abida
ASSESSING BIG DATA

ALGORITHMIC ACCOUNTABILITY

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

01IS15016A-F

Universität Osnabrück

Prof. Dr. Christoph Busch, Maître en Droit

ABIDA - ASSESSING BIG DATA

PROJEKTLAUFZEIT 01.03.2015-28.02.2019

Westfälische Wilhelms-Universität Münster,
Institut für Informations-, Telekommunikations- und
Medienrecht (ITM), Zivilrechtliche Abteilung

Karlsruher Institut für Technologie,
Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)

Leibniz Universität Hannover
Institut für Rechtsinformatik
(IRI)

Technische Universität Dortmund,
Wirtschafts- und Sozialwissenschaftliche
Fakultät (WiSo) Techniksoziologie

Ludwig-Maximilians-Universität München,
Forschungsstelle für Information, Organisation
und Management (IOM)

Wissenschaftszentrum
Berlin für Sozialforschung

ABIDA - Assessing Big Data

Über das Gutachten

Das Gutachten wurde im Rahmen des ABIDA-Projekts mit Mitteln des Bundesministeriums für Bildung und Forschung erstellt. Der Inhalt des Gutachtens gibt ausschließlich die Auffassungen der Autoren wieder. Diese decken sich nicht automatisch mit denen des Ministeriums und/oder der einzelnen Projektpartner.

ABIDA lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung.

www.abida.de

INHALTSVERZEICHNIS

EINFÜHRUNG

Mit der rasch voranschreitenden Digitalisierung von Wirtschaft und Gesellschaft dringen Algorithmen in immer mehr Lebensbereiche vor. Dies ist keine rein technologische Entwicklung, sondern führt zu einer Veränderung der Rahmenbedingungen des gesellschaftlichen Zusammenlebens.[1] Die zunehmende Bedeutung von algorithmenbasierten Entscheidungsprozessen (Algorithmic Decision Making, im Folgenden: ADM) weckt bei nicht wenigen Beobachtern die Sorge vor der Entstehung einer Wirtschafts- und Gesellschaftsordnung, die durch intransparente Algorithmen gesteuert wird („Black Box Society").[2] Diese Entwicklungen betreffen nicht nur Marktprozesse, sondern auch Fragen der sozialen Teilhabe und der demokratischen Willensbildung. So können etwa personalisierte Newsfeeds („content curation") in sozialen Netzwerken zu einer Fragmentierung des öffentlichen Diskurses führen.[3] Aktuell diskutiert wird auch der Einsatz von Filteralgorithmen zur Verhinderung von „hate speech" in sozialen Netzwerken.[4] Hier droht eine übermäßige Einschränkung der Meinungsfreiheit. In anderen Kontexten besteht die Gefahr digitaler Diskriminierung etwa durch den Einsatz von Scoring-Algorithmen im Online-Handel oder bei der Kreditvergabe.[5] Diesen Risiken stehen erhebliche Chancen für wirtschaftliche und gesellschaftliche Innovationen durch den Einsatz von Algorithmen gegenüber.

Vor dem Hintergrund dieser Entwicklungen geht die vorliegende Studie der Frage nach, auf welche Weise der Einsatz von Algorithmen transparent und verantwortlich gestaltet werden kann, damit die Interessen der unterschiedlichen Akteure in einer zunehmend durch algorithmenbasierte Entscheidungen geprägten Gesellschaft miteinander in Einklang gebracht werden. Im Mittelpunkt steht die Frage nach dem verantwortlichen und nachvollziehbaren Einsatz von Algorithmen („algorithmic accountability") und der Ausgestaltung des Regulierungsrahmens („governance of algorithms").[6] Die Untersuchung orientiert sich dabei an drei Leitfragen, anhand derer die Studie in drei Teile strukturiert wird:

- Leitfrage 1: Welche Konsequenzen hat der zunehmende Einsatz algorithmenbasierter Entscheidungen in unterschiedlichen sozialen Kontexten?
- Leitfrage 2: Bietet der geltende Regulierungsrahmen geeignete Instrumente zum Schutz der von ADM-Prozessen Betroffenen und für einen sachgerechten Interessenausgleich?

[1] *Leonie Beining*, Wie Daten und Algorithmen die Rahmenbedingungen für das Gemeinwohl verändern, Stiftung Neue Verantwortung (Juni 2017), S. 3.

[2] *Frank Pasquale*, The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge 2015; *Cathy O'Neil*, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, New York 2016.

[3] *Eli Pariser*, The Filter Bubble: What the Internet is Hiding from You, New York 2011.

[4] *Markus Beckedahl*, Algorithmen gegen den Hass, Süddeutsche Zeitung v. 29.7.2017, S. 9.

[5] *Thilo Weichert*, Scoring in Zeiten von Big Data, ZRP 2014, 168; zu den künftigen Vorgaben nach der DSGVO; *Flemming Moos/Tobias Rothkegel*, Nutzung von Scoring-Diensten im Online-Versandhandel: Scoring-Verfahren im Spannungsfeld von BDSG, AGG und DS-GVO, ZD 2016, 561.

[6] *Florian Saurwein/Natascha Just/Michael Latzer*, Governance of algorithms: options and limitations, Info 17(6), 35, 36 (2015).

- Leitfrage 3: Welche Handlungsoptionen bestehen für eine Ergänzung des Regulierungsrahmens, um bestehende Schutzlücken zu schließen und eine effektive „Algorithmic Accountabilty“ zu gewährleisten?

Leitfrage 1 wird schwerpunktmäßig in Teil 1 der Studie behandelt, der die rechtstatsächlichen Rahmenbedingungen einer Algorithmenregulierung ausleuchtet. Dazu werden zunächst einige ausgewählte tatsächliche Konstellationen analysiert, in denen derzeit und in naher Zukunft ADM-Prozesse eingesetzt werden. Ausgehend von einer überblicksartigen Bestandsaufnahme werden sodann die spezifischen Risiken und relevanten sozialen Kontexte skizziert.

In Teil 2 der Studie, der Leitfrage 2 behandelt, wird untersucht, ob das vorhandene Instrumentarium des europäischen und nationalen Regulierungsrahmens geeignet ist, die in Teil A der Studie identifizierten Interessen zu schützen und rechtliche Anforderungen durchzusetzen. Ein besonderer Fokus liegt dabei auf datenschutzrechtlichen Transparenzpflichten (Art. 13-15 DS-GVO) und dem Verbot automatisierter Einzelfallentscheidungen (Art. 22 DS-GVO).

Teil 3 der Studie untersucht, wie die vorhandenen Strukturen und Instrumente des Regulierungsrahmens ergänzt bzw. modifiziert werden könnten, um einen besseren Schutz der Interessen und eine effektivere Durchsetzung der rechtlichen Anforderungen an Algorithmen zu gewährleisten. Dabei werden neue rechtliche Erkenntnisse und Forschungen zum Regulierungsdesign berücksichtigt, um innovative Handlungsoptionen zu entwickeln. Die Studie schließt mit konkreten Handlungsempfehlungen für die Ergänzung des Regulierungsrahmens auf nationaler bzw. europäischer Ebene.

1 ANWENDUNGSFELDER, RISIKEN UND SOZIALE KONTEXTE ALGORITHMENBASIERTER ENTSCHEIDUNGSPROZESSE

1.1 ALGORITHMIC ACCOUNTABILITY

Das Konzept der „Algorithmic Accountability", das Gegenstand dieser Studie ist, bedarf der Erläuterung. Maßgeblich geprägt wurde der Begriff durch den amerikanischen Journalismusforscher *Nicholas Diakopolous*.[7] In seinem im Jahr 2014 veröffentlichten Beitrag „Algorithmic Accountability Reporting: On the Investigation of Black Boxes" legt *Diakopolous* dabei den Fokus auf die Rolle der Medien und deren Aufgabe, die Funktionsweise von Softwaresystemen mit gesellschaftlicher Relevanz als Recherchegegenstand zu verstehen, um so Transparenz zu schaffen. Inzwischen werden unter der Überschrift „Algorithmic Accountability" unterschiedliche technische,[8] rechtliche[9] und zivilgesellschaftliche[10] Ansätze diskutiert, die zu einem verantwortungsvollen und transparenten Einsatz von algorithmenbasierten Entscheidungsprozessen beitragen sollen.

Der Begriff „Algorithmus" bezeichnet in seinem ursprünglichen Sinne eine eindeutige Handlungsvorschrift zur Lösung eines bestimmten (mathematischen) Problems in einer endlichen Zahl definierter Einzelschritte. Ein bekanntes Beispiel bildet etwa der euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen.[11] Für die Nutzung in Computersystemen müssen die Schrittfolgen des Algorithmus in einen maschinenlesbaren, digitalen Computercode übersetzt werden.

In diesem Sinne kann als Ausgangspunkt in dieser Studie zunächst auf die Definition aus dem im Mai 2017 von der Association of Computing Machinery veröffentlichten „Statement on Algorithmic Transparency and Accountability" zurückgegriffen werden:

---

[7] *Nicholas Diakopoulos*, Algorithmic Accountability Reporting: On the Investigation of Black Boxes, Tow Center for Digital Journalism, 2014, http://towcenter.org/wp-content/uploads/2014/02/78524_Tow-Center-Report-WEB-1.pdf; siehe auch *Nicholas Diakopoulos*, Algorithmic accountability: Journalistic investigation of computational power structures, 3 Digital Journalism 398-415 (2015); siehe ferner *Alex Rosenblat*, *Tamara Kneese* and *Danah Boyd*, Algorithmic Accountability, A workshop primer produced for: The Social, Cultural & Ethical Dimensions of „Big Data" (March 17, 2014), https://ssrn.com/abstract=2535540.

[8] Siehe etwa *Joshua A. Kroll*, *Joanna Huey*, *Solon Barocas*, *Edward W. Felten*, *Joel Reidenberg*, *David G. Robinson* & *Harlan Yu*, Accountable Algorithms, 165 University of Pennsylvania Law Review, 633-705 (2017); *Reuben Binns*, Algorithmic Accountability and Public Reason, Philosophy & Technology (2017), https://doi.org/10.1007/s13347-017-0263-5.

[9] Vgl. *Sandra Wachter*, *Brent Mittelstadt & Luciano Floridi*, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, 7 International Data Privacy Law, 76-99 (2017); *Lilian Edwards* & *Michael Veale*, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16 Duke Law & Technology Review 18 (2017).

[10] Vgl. *Matthias Spielkamp*, AlgorithmWatch: What Role Can a Watchdog Organization Play in Ensuring Algorithmic Accountability?, in: Tania Cerquitelli, Daniele Quercia & Frank Pasquale (Hrsg.), Transparent Data Mining for Big and Small Data, 2017, S 207-215.

[11] Vgl. *Volker Heun*, Grundlegende Algorithmen: Einführung in den Entwurf und die Analyse effizienter Algorithmen, 2. Auflage, Wiesbaden 2013, S. 251 ff.

> „An algorithm is a self-contained step-by-step set of operations that computers and other ‚smart' devices carry out to perform calculation, data processing, and automated reasoning tasks."[12]

Angesichts der Vielfalt von Algorithmen und Anwendungsfeldern algorithmischer Systeme handelt es sich dabei um einen nicht leicht zu konturierenden Untersuchungsgegenstand.[13] Dazu trägt auch der Umstand bei, dass die heute in Computersystemen verwendeten Algorithmen nicht zwingend eine deterministische Struktur der Programmierung aufweisen, also einem vorher festgelegten Programm folgen. Zunehmend kommen sogenannte „selbstlernende" Algorithmen zum Einsatz, die dazu in der Lage sind, sich neuen Problemsituationen anzupassen.

Hinzu kommt, dass ein enges technisches Verständnis von Algorithmen als Computercode zu kurz greift, um die rechtlichen und gesellschaftlichen Auswirkungen des Einsatzes von Algorithmen zu beurteilen. Algorithmen, die etwa eingesetzt werden, um große Datenmengen („Big Data")[14] zu analysieren und dabei neue Korrelationen und bisher unbekannte Muster zu ermitteln, sind Bestandteil von soziotechnischen Systemen, die Wissen generieren und in (teil-)automatisierte Entscheidungsprozesse eingebunden sind. Für die Zwecke dieser Studie soll der Begriff des Algorithmus daher nicht nur in dem oben beschriebenen engen technischen Sinne verstanden werden, sondern darüber hinaus in seiner juristischen, sozialen und kulturellen Funktion erfasst werden. Im Anschluss an den amerikanischen Kommunikationswissenschaftler *Tarleton Gillespie* können Algorithmen dabei als spezielle Form bezeichnet werden, in der heute Wissen produziert und Entscheidungen getroffen werden.[15]

Der Begriff der „accountability" findet sich u.a. in der englischen Fassung von Art. 5 Abs. 2 DS-GVO. Dort bezieht er sich auf die Verantwortlichkeit des „data controller" für die Einhaltung der in Art. 5 Abs. 1 DS-GVO aufgeführten Grundsätze für die Verarbeitung personenbezogener Daten (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit). Die deutsche Fassung der DS-GVO umschreibt dies mit dem Begriff „Rechenschaftspflicht". Eine hieran anknüpfende, durchaus treffende Übersetzung des Kompositums „algorithmic accountability" lautet „Rechenschaft für Rechenverfahren".[16]

---

[12] Statement on Algorithmic Transparency and Accountability by ACM U.S. Public Policy Council, approved January 12, 2017 ACM Europe Policy Committee, approved May 25, 2017, https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf; siehe auch *Pedro Domingos*, The Master Algorithm: How the Quest for the Ultimate Learning Machine will Remake Our World, 2015, S. 1: „An algorithm is a sequence of instructions telling a computer what to do."

[13] So auch *Robert Seyfert*, *Jonathan Roberge*, Was sind Algorithmuskulturen, in: dies. (Hrsg.) Algorithmuskulturen: Über die rechnerische Konstruktion der Wirklichkeit, Transcript: Bielefeld 2017, S. 8.

[14] Der Begriff „Big Data" bezieht sich auf das Zusammenspiel von komplexen Analysealgorithmen und großen Datenmengen, die sich durch Datenvolumen (volume), Datenrate (velocity), Heterogenität (variety) und Datenqualität (veracity) von (früher) handelsüblichen Datenbanksystemen unterscheiden, vgl. *Volker Markl*, in: Hoeren (Hrsg.), Big Data und Recht, München 2014, S. 4; siehe auch *Viktor Mayer-Schönberger* & *Kenneth Cukier*, Big Data: Die Revolution, die unser Leben verändern wird, München 2013, S. 13 ff.

[15] *Tarleton Gillespie*, Algorithm, in: Benjamin Peters (ed.) Digital keywords: a vocabulary of information society and culture, Princeton University Press, 2016, S. 22.

[16] *Lorenz Matzat*, Rechenschaft für Rechenverfahren, Tendenz 2/2017, https://www.blm.de/infothek/magazin_tendenz/tendenz-2_2017/algorithmen-tendenz_2_17.cfm.

Art. 5 Abs. 2 DS-GVO bestimmt, dass der für die Datenverarbeitung Verantwortliche für die Einhaltung dieser Grundsätze „verantwortlich" ist und dies „nachweisen" können muss. Ein wesentlicher Ausdruck von „accountability" sind dementsprechend die umfangreichen Dokumentations- und Nachweispflichten in der DS-GVO, etwa die Verpflichtung zur Führung eines Verzeichnisses aller Verarbeitungstätigkeiten (Art. 30 DS-GVO) oder die im Rahmen der Datenschutz-Folgenabschätzung erforderliche Beschreibung und Bewertung der geplanten Verarbeitungsvorgänge (Art. 35 Abs. 7 DS-GVO).

Das Konzept der „algorithmic accountability", das im Folgenden zugrunde gelegt wird, geht allerdings in mehrfacher Weise über den Begriff der „accountability" i.S.v. Art. 5 Abs. 2 DS-GVO hinaus. Zum einen erschöpft sich ein verantwortungsvoller Umgang mit ADM-Systemen nicht allein in der Herstellung von Transparenz, sondern betrifft auch materielle Anforderungen im Sinne einer „ethics of algorithms".[17] Darüber hinaus beschränkt sich das Instrumentarium zur Verwirklichung von „algorithmic accountability" nicht auf rechtliche Vorgaben, sondern schließt auch technische Anforderungen („accountability by design") und zivilgesellschaftliche Ansätze ein.

1.2 BESTANDSAUFNAHME UND SYSTEMATISIERUNG

1.2.1 ANWENDUNGSFELDER VON ALGORITHMEN

Zu Beginn der Untersuchung ist zunächst eine rechtstatsächliche Bestandsaufnahme erforderlich. Dabei soll überblicksartig skizziert werden, in welchen Bereichen ADM-Systeme zum Einsatz kommen. Das Spektrum reicht von digitalen Geschäftsmodellen (z.B. Bewertungs- und Vergleichsplattformen,[18] Suchmaschinen,[19] Digitale Assistenten[20]) über das Gesundheitswesen (z.B. predictive medicine), das Personalwesen (z.B. People Analytics)[21] und soziale Netzwerke (z.B. personalisierte Newsfeeds) bis zur öffentlichen Verwaltung (z.B. automatisierte Besteuerungsverfahren).[22] Einige dieser Bereiche sollen nachfolgend exemplarisch anhand kurzer Case Studies näher beleuchtet werden.

---

[17] *Brent Mittelstadt* et al., The ethics of algorithms: Mapping the debate, Big Data & Society 1-21 (2016); siehe auch die von der amerikanischen Initiative „Fairness, Accountability and Transparency in Machine Learning" (fatml.org) entwickelten Prinzipen, anhand derer die gesellschaftlichen und ethischen Folgen von ADM-Prozessen beurteilt werden sollen: Verantwortlichkeit (responsibility), Erklärbarkeit (explainability), Genauigkeit (accuracy), Überprüfbarkeit (auditability) und Gerechtigkeit (fairness).

[18] *Christoph Busch*, Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy, in: De Franceschi (ed.), European Contract Law and the Digital Single Market: Implications of the Digital Revolution, Intersentia, Cambridge 2016, S. 223 ff.

[19] *Martin Eifert*, Rechenschaftspflicht für soziale Netzwerke und Suchmaschinen: Zur Veränderung des Umgangs von Recht und Politik mit dem Internet, NJW 2017, 1450.

[20] *Maurice Stucke/Ariel Ezrachi*, Is Your Digital Assistant Devious?, Oxford Legal Studies Research Paper No. 52/2016 (September 2016), verfügbar auf SSRN: https://ssrn.com/abstract=2828117.

[21] *Boris Dzida*, Big Data und Arbeitsrecht, NZA 2017, 541; *Christian Holthaus/Young-kul Park/Ruth Stock-Homburg*, People Analytics und Datenschutz – Ein Widerspruch?, DuD 2015, 676.

[22] *Mario Martini*, Wenn Maschinen entscheiden… – vollautomatisierte Verwaltungsverfahren und Persönlichkeitsschutz, NVwZ 2017, 681; siehe ferner zu „predictive policing" *Wolfgang Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), 1. Sogar in der Leitung von Unternehmen könnten Algorithmen schon bald eine wichtige Rolle spielen, vgl. *Florian Möslein*, Digitalisierung im Gesellschaftsrecht: Unternehmensleitung durch Algorithmen und künstliche Intelligenz? ZIP 2018, 204.

1.2.1.1. ONLINE-HANDEL

Algorithmen spielen heute im Online-Handel eine überragend wichtige Rolle. Im Mittelpunkt stehen dabei vor allem sog. Empfehlungssysteme. Dabei handelt es sich um algorithmische Entscheidungsunterstützungssysteme (*Decision Support Systems*), die dem einzelnen Kunden aus der großen Produktauswahl eines Online-Shops diejenigen Artikel präsentieren, für die das System eine hohe Kaufwahrscheinlichkeit berechnet hat. Der Einsatz von Empfehlungssystemen führt dazu, dass das Einkaufserlebnis für die einzelnen Kunden personalisiert wird. Ein Vorreiter dieser Methode war der Online-Händler Amazon.com. *Brent Smith* (Amazon) und *Greg Linden* (Microsoft) beschreiben das Geschäftsmodell des personalisierten Online-Kaufhauses treffend wie folgt:

> „For two decades now, Amazon.com has been building a store for every customer. Each person who comes to Amazon.com sees it differently, because it's individually personalized based on their interests. It's as if you walked into a store and the shelves started rearranging themselves, with what you might want moving to the front, and what you're unlikely to be interested in shuffling further away."[23]

Die technische Grundlage für die personalisierten Angebote bildet ein Empfehlungssystem, das im Wesentlichen auf einem patentierten[24], kollaborativen Filteralgorithmus basiert, der Produkte mit „verwandten" Produkten verknüpft (*item-based collaborative filtering algorithm*). Der Algorithmus hat dabei die Aufgabe für jedes Produkt p1 ein Produkt p2 zu ermitteln, das in der Vergangenheit häufig von Kunden gekauft wurde, die zuvor das Produkt p1 gekauft haben. Daraus leitet das System eine Empfehlung nach dem Muster „Kunden, die p1 gekauft haben, kaufen auch p2" ab. Das so konstruierte Empfehlungssystem von Amazon.com ist ein sehr leistungsfähiges Verkaufswerkzeug. Etwa 30 % der Seitenaufrufe bei Amazon.com sollen auf algorithmischen Produktempfehlungen beruhen.[25] Bei dem Streaming-Dienst Netflix, der ebenfalls ein sehr ausgefeiltes Empfehlungssystem verwendet, soll der Empfehlungsalgorithmus sogar für mehr als 80 % der abgespielten Filme verantwortlich sein.[26]

Die konsequente Weiterentwicklung dieses Geschäftsmodells beschreibt ein im Jahr 2012 von Amazon angemeldetes Patent[27] für ein algorithmisches System, das vorhersagt, welche Produkte von einem bestimmten Kunden in naher Zukunft voraussichtlich bestellt werden. Auf Grundlage dieser Prognose soll das Produkt bereits zu einem nahegelegenen Auslieferzentrum versandt werden, noch bevor der Kunde die Bestellung aufgibt (*anticipatory shopping*). Ein viel zitiertes Beispiel,[28] das die Möglichkeiten des algorithmischen *data mining* im Online-Handel veranschaulicht, handelt davon, dass der amerikanische Onli-

---

[23] *Brent Smith and Greg Linden*, Two decades of recommender systems at Amazon.com, 21 IEEE Internet Computing 12-18 (2017).

[24] *Greg Linden* et al., Collaborative Recommendations Using Item-to-Item Similarity Mappings, US Patent 6,266,649, to Amazon.com, Patent and Trademark Office, 2001 (led 1998); siehe auch *Greg Linden & Brent Smith*, Amazon.com Recommendations: Item- to-Item Collaborative Filtering, 7 IEEE Internet Computing 76–80 (2003).

[25] *A. Sharma, J.M. Hofman, D.J. Watts*, Estimating the Causal Impact of Recommendation Systems from Observational Data, Proc. 16th ACM Conf. Economics and Computation, 453-470 (2015).

[26] *C.A. Gomez-Uribe, N. Hunt*, The Netflix Recommender System: Algorithms Business Value and Innovation, ACM Trans. Management Information Systems, vol. 6, no. 4, pp. 1-19, 2016.

[27] *Joel R. Spiegel* et al. "Method and system for anticipatory package shipping." U.S. Patent No. 8,271,398. 18 Sep. 2012.

[28] *Charles Duhigg*, How Companies Learn Your Secrets, New York Times (16.2.2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

ne-Händler Target durch Analyse des Einkaufsverhaltens anhand scheinbar „unverdächtiger" Produkte (z.B. parfümfreie Körperlotion, bestimmte Nahrungsergänzungsmittel) nicht nur ermitteln konnte, dass eine bestimmte Kundin schwanger ist, sondern sogar in der Lage war, den Geburtstermin recht präzise zu berechnen. Der Online-Händler nutzte diese Informationen, um der Kundin personalisierte Werbebotschaften zu übermitteln.

Im Online-Handel werden Algorithmen nicht nur für Produktempfehlungen und personalisierte Werbung, sondern auch zur Preisgestaltung eingesetzt. Weit verbreitet ist das sog. *dynamic algorithmic pricing*. Dabei werten ADM-Systeme zahlreiche preisrelevante Informationen aus (z.B. die aktuelle Nachfragesituation und das Preissetzungsverhalten von Konkurrenten) und passen auf dieser Grundlage anschließend automatisch die eigenen Preise im Sekundentakt an die jeweilige Marktsituation an, um ihre Absatz- und Gewinnmöglichkeiten zu optimieren.[29] Nach einer Studie der Europäischen Kommission beobachten bereits heute über 50% der Onlinehändler die Preise ihrer Konkurrenten. 67% dieser Händler verwenden dabei eine automatische Preisanpassungssoftware. auf der Grundlage der erworbenen Informationen werden in den meisten Fällen (78%) die eigenen Preise sodann entweder manuell oder automatisch angepasst.[30]

1.2.1.2. PERSONALWESEN

Auch im Personalwesen gewinnen ADM-Systeme unter dem Stichwort „People Analytics" zunehmend an Bedeutung.[31] Aktuellen Studien zufolge wächst gerade vor dem Hintergrund des allgemeinen Fachkräftemangels sowohl bei deutschen als auch bei internationalen Unternehmen das Interesse an algorithmenbasierten Anwendungen zur Optimierung der Talentakquise im digitalen Recruiting.[32] Beispiele für den Einsatz von ADM-Systemen sind etwa Matching-Algorithmen zur Feststellung der Übereinstimmung von Bewerberprofil und Stellenausschreibung bzw. Unternehmenskultur, Such- und Filteralgorithmen für die gezielte Ansprache von neuen Mitarbeitern, die nicht aktiv auf Jobsuche sind (Headhunting 2.0), sowie verbesserte Suchalgorithmen für Job-Recommender. In den meisten Fällen dienen algorithmengestützte Anwendungen der Bewerbervorauswahl, die abschließende Einstellungsentscheidung verbleibt in der Hand der menschlichen Entscheider.

Algorithmenbasierte Entscheidungsunterstützung im Personalwesen wird derzeit vor allem in größeren Unternehmen eingesetzt. Dabei sind die Anwendungsfelder für Algorithmen unterschiedlich. Verbreitet sind insbesondere Systeme, die die Übereinstimmung formaler Bewerberkriterien (Ausbildung, Noten, Kompetenzen aus den Bereichen Sprache, Softwarekenntnisse etc.) mit der ausgeschriebenen Stelle abgleichen und Bewerber in Form einer Negativauswahl aussortieren, die die formalen Anforderungen nicht erreichen. Darüber hinaus überprüfen Unternehmen mit algorithmenbasierten Testverfahren auch

[29] *Martin Ebers*, Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten?, NZKart 2016, 554; siehe auch *Le Chen, Alan Mislove & Christo Wilson*, An Emipircal Analysis of Algorithmic Pricing on Amazon Marketplace, Proceedings of the 25th International Conference on World Wide Web (2016).

[30] Preliminary Report on the E-commerce Sector Inquiry, 15.9.2016, SWD (2016) 312 final, S. 53.

[31] Vgl. *Bertelsmann Stiftung* (Hrsg.), Wenn Maschinen Menschen bewerten: Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung, 2017, S. 22 ff.

[32] *Deloitte*, Neue Spielregeln im digitalen Zeitalter, Global Human Capital Trendstudie 2017, Deutschland Report, S. 3.

den „cultural fit“ des Bewerbers, also den Grad der Übereinstimmung zwischen den Bewerbern und dem Unternehmen in Bezug auf Denkmuster, Verhaltensweise, Normen und Werte (z.B. Führungskultur, Leistungsbereitschaft).[33] Eine Überprüfung des „cultural fit“ mittels psychometrischer Algorithmen erfolgt mitunter schon bevor die formale Eignung des Bewerbers überhaupt geprüft wurde.

Algorithmengestützte Verfahren zur Überprüfung der „kulturellen Passung“ werden nicht nur von Unternehmen, sondern auch von Online-Vermittlungsplattformen eingesetzt. So hat die Online-Jobbörse Stepstone angekündigt, im Laufe des Jahres 2018 solche „cultural fit“-Tests für unterschiedliche Unternehmen bereits für Bewerber anzubieten. Dadurch könne der potentielle Bewerber bereits bevor er Zeit und Mühe in das Verfassen einer Bewerbung investiert überprüfen, ob er zu dem Unternehmen und das Unternehmen zu ihm passen könnte. Zumeist ist der Matching-Algorithmus solcher Tests darauf ausgerichtet, Bewerber und Unternehmen zusammen zu führen, die über eine möglichst hohe Übereinstimmung verfügen („Supplementary Fit“) und nicht darauf, solche Mitarbeiter zu identifizieren, die über Eigenschaften verfügen, die im Unternehmen noch nicht in ausreichendem Maße vorhanden sind („Complementary Fit“). Einige Unternehmen und auch die Entwickler und Anbieter solcher Testsoftware geben jedoch zu bedenken, dass auf diese Weise „Querdenker“, die für die Innovationsstärke von Unternehmen notwendig sind, zumeist bereits im Vorfeld aussortiert werden.[34]

Automatisierte Empfehlungssysteme werden sowohl für Bewerber in Form von Job-Recommendern als auch für Unternehmen als Staff-Recommender am Markt angeboten. Aktuellen Studien zufolge setzen derzeit allerdings nur 3,5 % der Top-1000 Unternehmen Active-Sourcing-Anwendungen ein, 7 % planen den Einsatz für die Zukunft.[35] Die Such- und Filteralgorithmen gleichen dabei in der Regel die formale Qualifikation von Bewerbern und potenziellen Mitarbeitern mit den Qualifikationsprofilen aus Stellenanzeigen oder Suchaufträgen als best fit ab. Begrüßt wird die Nutzung der Informationen immer dann, wenn der Bewerber aktiv in die Nutzung einwilligt, wohingegen Skepsis bis hin zur Vermutung einer ggf. missbräuchlichen Nutzung insbesondere dann auf Seiten des potenziellen Mitarbeiters zu verzeichnen ist, wenn der Zugriff auf persönliche Online-Profile durch Active-Sourcing-Anwendungen geschieht. Knapp die Hälfte der Kandidaten begrüßt den automatisierten Zugriff der Anwendungen auf ihre Profile in sozialen Netzwerken bei Einwilligung, wohingegen mehr als ein Drittel der Kandidaten dies auch dann als problematisch ansehen.[36] Ein Drittel der Jobsuchenden veröffentlicht gezielt Informationen, insbesondere in Karrierenetzwerken, um von Empfehlungssystemen identifiziert zu werden.

Weiter verbreitet sind bereits Anwendungen im Bereich Performance Management, die eine detailgenaue Leistungsbeurteilung ermöglichen sollen. Ein bekanntes und zugleich kontroverses Beispiel sind et-

[33] Zum Begriff des „cultural fit“ siehe *Daniel M. Cable & Jeffrey R. Edwards*, Complementary and Supplementary Fit: A Theoretical and Empirical Integration, 89 Journal of Applied Psychology 822-834 (2004).

[34] Vgl. *Daniel M. Cable & Jeffrey R. Edwards*, Complementary and Supplementary Fit: A Theoretical and Empirical Integration, 89 Journal of Applied Psychology 822 ff. (2004).

[35] *Tim Weitzel*, *Sven Laumer*, *Christian Maier*, *Caroline Oehlhorn*, *Jakob Wirth & Christoph Weinert*, Active Sourcing und Social Recruiting. Ausgewählte Trends der Recruiting Trends 2017, Studie im Auftrag der Monster GmbH, Bamberg 2017, S. 22.

[36] *Weitzel* et al. (Fn. 35) 25.

wa die in den USA verwendeten algorithmengestützten Systeme zur Leistungsbeurteilung von Lehrern.[37] Auch zur Betrugsbekämpfung lassen sich algorithmengesteuerte Prozesse einsetzen. So wurde unlängst über Pläne der amerikanischen Investmentbank JP Morgan Chase berichtet, ihre Mitarbeiter mithilfe einer automatisierten Auswertung von E-Mails und sonstiger digitaler Kommunikation automatisiert auf verdächtige Verhaltensmuster zu überprüfen, um Verstöße gegen Risikostandards und Verhaltensrichtlinien aufzudecken.[38]

1.2.1.3. GESUNDHEITSWESEN

Für den Bereich des Gesundheitswesens sind eine Reihe von Anwendungsfeldern für ADM-Systeme zu nennen.[39] Das Spektrum reicht von Systemen zur algorithmenbasierten Entscheidungsunterstützung bei der Diagnose und Therapie von Krankheiten über mobile Anwendungen (Medical Apps) zur medizinischen Versorgung und Überwachung von Patienten bis zur Anwendung von Big-Data-Analysen und Machine Learning in der biomedizinischen Forschung.[40] Ein praktischer Anwendungsfall für den Einsatz von Machine Learning zu Diagnosezwecken ist etwa die Auswertung von Bilddaten mithilfe von neuronalen Netzen zur Identifikation von Melanomen.[41] Selbstlernende Algorithmen werden inzwischen zur Bildauswertung auch im Bereich der psychischen Gesundheit eingesetzt. So hat jüngst eine Forschergruppe untersucht, ob sich durch eine automatisierte Auswertung von Fotos, die über den Sharing-Dienst Instagram geteilt werden, prädiktive Marker für eine Depression identifizieren lassen.[42]

Ein viel diskutierter Anwendungsfall von Algorithmen für medizinische Zwecke ist die im Jahr 2008 von Google entwickelte Anwendung „Google Flu Trends", die zeitweise für über 25 Länder Vorhersagen zum Auftreten und zur Ausbreitung von Grippeerkrankungen berechnete.[43] Die Analyse-Software ermöglichte es, anhand von Google-Suchanfragen für 45 Suchbegriffe eine Korrelation mit dem Auftreten und der Ausbreitung von Influenza-Erkrankungen nachzuweisen. Die Vorhersagegenauigkeit, die die Anwendung für den Trainingsdatensatz erzielte, überzeugte nicht nur die Entwickler und die US-Seuchenbekämpfungsbehörde, sie stieß auch in der Öffentlichkeit auf großes Interesse. In den Folgejahren machte Google Flu Trends jedoch dadurch Schlagzeilen, dass Grippewellen in ihrer Intensität systematisch unter- bzw. häufiger noch überschätzt und auch die räumlichen Ausbreitungsmuster nur schlecht

---

[37] Vgl. *Cathy O'Neil*, Angriff der Algorithmen, Hanser: München 2017, S. 12-17.

[38] *Hugh Son*, JPMorgan algorithm knows you're a rogue employee before you do, Bloomberg Business, www.bloomberg.com/news/articles/2015-04-08/jpmorgan-algorithm-knows-you-re-a-rogue-employee-before-you-do; siehe dazu auch *Malcom Campbell-Verduyn*, *Marcel Goguen* & *Tony Porter*, Big Data and algorithmic governance: the case of financial practices, 22 New Political Economy, 219-236 (2017).

[39] Dazu ausführlich *Thilo Weichert*, Big Data im Gesundheitsbereich, ABIDA-Gutachten, 2018 sowie *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als individuelle Freiheitsgestaltung, 2017.

[40] Zu Einsatzmöglichkeiten selbstlernender Algorithmen in der Medizin siehe *Anton S. Becker* et al., Medicina ex Machina: Machine Learning in der Medizin, 107 Praxis: Schweizerische Rundschau für Medizin 19-23 (2018), https://doi.org/10.1024/1661-8157/a002920.

[41] *Andre Esteva* et al., Dermatologist-level classification of skin cancer with deep neural networks, 542 Nature 115-118 (2017).

[42] *A.G. Reece & C.M. Danforth*, Instagram photo reveal predictive markers of depression, 6 EPJ Data Science 15 (2017).

[43] *Mayer-Schönberger/Cukier* (Fn. 14) 7 ff.; siehe auch *Andrea Freyer Dugas* et al., Influenza forecasting with Google flu trends, PloS one (2013), https://doi.org/10.1371/journal.pone.0056176.

abgebildet wurden.[44] Letztlich wurde das Angebot Google Flu Trends wieder eingestellt. Als Gründe für das Scheitern werden u.a. genannt, dass der verwendete Algorithmus nicht „lernfähig" war, d.h. nicht in der Lage, sich auf veränderte Umweltbedingungen einzustellen. So blieben die Suchbegriffe, die in die Prognosen einfließen über die Zeit hinweg gleich. Auch verzichteten die Entwickler darauf, den verwendeten Datensatz zu korrigieren, wenn Suchanfragen in Bezug auf Influenza etwa nach einer Nachrichtensendung über eine aktuelle Grippeepidemie gehäuft auftraten. Das Beispiel von „Google Flu Trends" zeigt damit zugleich die Grenzen algorithmischer Analyseverfahren.

Ein Beispiel für den Einsatz von Algorithmen im Grenzbereich von Medizin und Lifestyle-Produkten sind sog. Fitnesstracker, die zur gesundheitlichen „Selbstvermessung" verwendet werden. Wie der Deutsche Ethikrat in seiner 2017 veröffentlichten Studie zu Big Data und Gesundheit anmerkt, hat der Trend zum *quantified self* durchaus etwas Zwiespältiges.[45] Einerseits können die Geräte und Apps einen gesunden Lebensstil fördern, „andererseits kann eine überzogene Selbstkontrolle mithilfe solcher Angebote zu einem übertriebenen, der Gesundheit abträglichen Optimierungsstreben sowie der Mediatisierung „natürlicher" Lebensvorgänge beitragen. Zudem ist zweifelhaft, ob Selbstvermessung tatsächlich immer Ausdruck persönlicher Souveränität oder eher eine Form selbstinduzierter Fremdbestimmung ist."[46] Hinzu kommt, dass derartige Fitnesstracker inzwischen auch von Krankenkassen im Rahmen von Bonusprogrammen eingesetzt werden.[47]

1.2.1.4. ÖFFENTLICHE VERWALTUNG

Die öffentliche Verwaltung setzt seit langem in unterschiedlicher Weise technische Hilfsmittel beim Erlass von Verwaltungsakten ein. Neuerdings gewinnen auch ADM-Prozesse als Instrument zur Verfahrensbeschleunigung und Kostenreduzierung im Verwaltungsverfahren an Bedeutung. Vorreiter ist hier das Steuerrecht.[48] Die rechtlichen Grundlagen für den vollständig automatisierten Erlass von Steuerbescheiden wurden unlängst durch das zum 1.1.2017 in Kraft getretene Gesetz zur Modernisierung des Besteuerungsverfahrens[49] geschaffen. Gemäß § 155 Abs. 4 S. 1 AO sind die Finanzämter künftig befugt, Steuerverwaltungsakte „ausschließlich automationsgestützt" zu erlassen, „soweit kein Anlass dazu besteht, den Einzelfall durch Amtsträger zu bearbeiten".

Für allgemeine Verwaltungsverfahren und das Sozialrecht sehen der auch Anfang 2017 eingefügte § 35a VwVfG bzw. § 31a SGB X ebenfalls die Möglichkeit vollautomatisierter Verwaltungsentscheidungen

---

[44] *David Lazer* et al., The parable of Google Flu: traps in big data analysis, 343 Science 1203-1205 (2014); siehe auch *Declan Butler*, When Google got flu wrong, 494 Nature 155 (2013).

[45] Vgl. zur „Quantified Self"-Bewegung *Gary Wolf*, The Data-Driven Life, New York Times Magazine (28.4.2010), http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html; siehe auch *Andreas Bernard*, Komplizen des Erkennungsdienstes: Das Selbst in der digitalen Kultur, Frankfurt am Main 2017, S. 97 ff.

[46] *Deutscher Ethikrat*, Big Data und Gesundheit – Datensouveränität als individuelle Freiheitsgestaltung, 2017, S. 20.

[47] Einige Krankenkassen fördern Fitness-Tracker, Wirtschaftswoche (13.8.2015), https://www.wiwo.de/finanzen/vorsorge/einige-krankenkassen-foerdern-fitness-tracker-bundesversicherungsamt-sollte-werbetraechtige-leistungen-verbieten/12174652.html.

[48] Siehe dazu *Julius Helbich*, Rechtsfragen der „automatisierten" Ermessensausübung im Steuerrecht, DStR 2017, 574 ff.; siehe auch *Nadja Braun Binder*, Vollautomatisierte Verwaltungsverfahren im allgemeinen Verwaltungsrecht? Der Gesetzentwurf zur Modernisierung des Besteuerungsverfahrens als Vorbild für vollautomatisierte Verwaltungsverfahren nach dem VwVfG, NVwZ 2016, 960.

[49] BGBl. I 2016, 1679.

vor.[50] Hier sind die Voraussetzungen jedoch enger als im Steuerrecht. Während die Abgabenordnung in engen Grenzen auch automatisierte Ermessensentscheidungen zulässt, kommt nach § 35a VwVfG ein vollständig automatisierter Erlass eines Verwaltungsaktes nur in Betracht, „sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht". Der vollständig automatisierte Erlass von Verwaltungsakten steht damit unter Gesetzesvorbehalt und kommt nur bei gebundenen Verwaltungsentscheidungen in Betracht. Für das Sozialrecht verlangt § 31a S. 2 SGB X, dass die Behörde beim Erlass automatisierter Entscheidungen die für den Einzelfall bedeutsamen tatsächlichen Angaben des Beteiligten berücksichtigt, die im automatischen Verfahren nicht ermittelt würden. Die Bearbeitung durch einen Menschen ist danach zwingend, wenn die anwendbare Rechtsnorm eine Ermessensentscheidung oder einen Beurteilungsspielraum vorsieht.[51]

Die Einschränkungen für den Erlass vollautomatisierter Verwaltungsakte in § 35a VwVfG und § 31a SGB X sollen die Gefahr reduzieren, dass durch automatisierte Verfahrensabläufe falsche Ergebnisse erzielt werden. Wie real eine solche Gefahr ist, zeigt ein aktueller australischer Fall.[52] So hat die australische Sozialhilfe-Agentur Centrelink zwischen Juni 2016 und März 2017 rund 200.000 automatisiert erstellte Bescheide verschickt und angeblich zu Unrecht erhaltene Sozialleistungen zurückgefordert. Wie sich später herausstellte, waren die Rückforderungsbeträge in 13.000 Fällen zu hoch berechnet. In 7.000 Fällen bestand gar keine rechtliche Grundlage für eine Rückforderung. Die Ursache der fehlerhaften Bescheide lag in Fehlern beim automatisierten Datenabgleich durch die Sozialhilfe-Agentur.

1.2.2 TYPEN ALGORITHMENBASIERTER ENTSCHEIDUNGEN

Der kurze Überblick über Anwendungsfelder algorithmenbasierter Entscheidungsprozesse verdeutlicht, dass Algorithmen inzwischen in einer Vielzahl unterschiedlicher sozialer Kontexte zum Einsatz kommen. Die oben genannten Beispiele zeigen auch, dass die jeweils eingesetzten Algorithmen unterschiedliche Funktionen erfüllen. In der Literatur wird dabei insbesondere zwischen *Priorisierungs-*, *Klassifizierungs-*, *Zuordnungs-* und *Filterprozessen* unterschieden.[53]

1.2.2.1. PRIORISIERUNG

Ein wichtiges Einsatzfeld von Algorithmen ist die Priorisierung von Informationen. Dabei geht es um die Bewertung von Elementen einer Menge anhand festgelegter Kriterien und anschließende Sortierung der

[50] Dazu näher *Heribert Schmitz/Lorenz Prell*, Neues zum E-Government: Rechtsstaatliche Standards für E-Verwaltungsakt und E-Bekanntgabe im VwVfG, NVwZ 2016, 1273.

[51] So die Gesetzesbegründung, BT-Drs. 18/8434, 120.

[52] Siehe dazu *Noëlle Rohde*, In Australien prüft eine Software die Sozialbezüge – und erfindet Schulden für 20.000 Menschen (25.10.2017), https://algorithmenethik.de/2017/10/25/in-australien-prueft-eine-software-die-sozialbezuege-und-erfindet-schulden-fuer-20-000-menschen/; siehe auch *Heiko Maas*, Zusammenleben in der digitalen Gesellschaft, DANA 2017, 156, 157.

[53] *Nicholas Diakopoulos*, Accountability in Algorithmic Decision Making, Communications of the ACM 59(2):56-62 (2016); siehe auch *Nicholas Diakopoulos/Oliver Deussen*, Brauchen wir eine Rechenschaftspflicht für algorithmische Entscheidungen?, Informatik Spektrum 2017, 362 (363); *World Wide Web Foundation*, Algorithmic Accountability: Applying the concept to different country contexts, Juli 2017, S. 7.

Elemente in einer eindeutigen Reihenfolge („Ranking"). Priorisierung hat dabei stets zur Folge, dass bestimmte Informationen zulasten anderer in den Vordergrund gestellt werden. In diesem Sinne beinhaltet eine Priorisierung auch immer eine Art von Selektion und Diskriminierung.[54] Klassische Beispiele sind die von Suchmaschinen zur Priorisierung von Webseiten eingesetzten Algorithmen, z.B. PageRank[55] (Google) und TrustRank (Yahoo), die auf die Eingabe von Suchbegriffen Online-Inhalte in einer nach Relevanz geordneten Ergebnisliste sortieren. Andere Beispiele sind etwa Rankings, wie sie etwa auf Vergleichsportalen (z.B. Tripadvisor, Jameda) gebildet werden. Mögliche Anknüpfungspunkte für eine Regulierung sind in diesen Fällen die Auswahl der Kriterien, anhand derer die Priorisierung erfolgt sowie die Gewichtung der einzelnen Kriterien.

1.2.2.2. KLASSIFIZIERUNG

Eine weitere wichtige Funktion von Algorithmen ist die Klassifizierung von Personen oder Inhalten anhand bestimmter Merkmale. Ähnlich wie bei der Priorisierung geht es auch diesen Fällen um die Sortierung von Elementen einer bestimmten Menge. Es wird jedoch keine eindeutige Reihenfolge für alle einzelnen Elemente gebildet, sondern lediglich eine Einteilung in bestimmte Klassen vorgenommen. Dabei kann die Einteilung der Klassen einerseits vorgegeben sein, andererseits ist es auch möglich, dass die Klassen nicht vorgegeben sind, sondern vom Algorithmus selbst gebildet werden. Die Zuordnung zu einer bestimmten Klasse steuert dabei in der Regel weitere Entscheidungen, etwa die Vergabe eines Kredits oder die Einräumung einer bestimmten Zahlungsmöglichkeit (z.B. Kauf auf Rechnung). Ebenfalls in diese Kategorie gehören Algorithmen, die zur Einteilung von Versicherungsnehmern in Risikoklassen verwendet werden.

1.2.2.3. ZUORDNUNG

In anderen Konstellationen werden Algorithmen eingesetzt, um Beziehungen zwischen unterschiedlichen Elementen (z.B. Personen und Informationen) herzustellen. Hierher gehören etwa der für das Empfehlungssystem von Amazon verwendete *item-based collaborative filtering algorithm* oder die Funktionsweise von Dating-Plattformen. Ein weiteres bekanntes Beispiel dafür ist die Autocomplete-Funktion, wie sie etwa von der Suchmaschine Google verwendet wird. Hier stellt ein Algorithmus eine Verknüpfung zwischen einem Suchbegriff und einem Ergänzungsvorschlag her. Als Ergänzung werden dabei Wortkombinationen vorgeschlagen, die zu dem fraglichen Suchbegriff von anderen Nutzern am häufigsten eingegeben wurden. Dies geschieht in der Erwartung, dass diese Wortkombinationen für den suchenden Internetnutzer hilfreich sein können, da sie – so die zugrundeliegende Annahme – einen inhaltlichen Bezug zu dem eingegebenen Suchwort aufweisen. Wird etwa bei der Eingabe des Namens einer Person der Ergänzungsbegriff „Betrug" vorgeschlagen, so kann dies als Hinweis auf ein strafrechtlich relevantes Verhalten der Person verstanden werden. Es kann aber auch sein, dass lediglich unzutreffende Gerüchte im Umlauf sind und andere Internetnutzer aus diesem Grund häufig die entsprechende Wortkombination in

[54] Diakopoulos/Deussen, (Fn. 53), 363.

[55] Vgl. *Larry Page* et al., The pagerank citation ranking: Bringing order to the web, Technical report, Stanford InfoLab (1999), http://ilpubs.stanford.edu:8090/422/1/1999-66.pdf.

die Suchmaschine eingeben. Hier besteht daher die Gefahr von schwerwiegenden Persönlichkeitsverletzungen.[56]

1.2.2.4. FILTERUNG

Eine wichtige Funktion erfüllen Algorithmen auch bei der Filterung von Inhalten. Hier geht es darum, einzelne Inhalte anhand bestimmter Kriterien zu berücksichtigen oder auszuschließen. Ein praktischer Anwendungsfall sind etwa die Spam-Filter von E-Mail-Programmen. Filteralgorithmen kommen auch bei Bewertungssystemen und bei Kommentarfunktionen auf Webseiten zum Einsatz (sog. Profanity-Filter). Weitere Beispiele sind Jugendschutzfilter, wie etwa NetNanny.

Übersicht: Funktionen von Algorithmen

Funktion	Anwendungsfeld	Beispiel
Priorisierung Zuweisung eines Rangs anhand vorab definierter Kriterien	Allgemeine Suchmaschinen	Google, Bing, Baidu
	Spezialisierte Suchmaschinen	Google Images, Shutterstock
	Meta-Suchmaschinen	Info.com
	Timelines in Sozialen Medien	Facebook, Twitter
Klassifizierung Gruppierung von Informationen	Reputationssysteme	Ebay, Uber, Airbnb
	Nachrichtenaggregatoren	Reddit, Digg
	Credit Scoring	Schufa, Creditreform, Credit Karma,
	Social Scoring	Klout, PeerIndex
Zuordnung Bestimmung von Verknüpfungen zwischen Personen und Informationen	Predictive Policing	PredPol
	Trend Scouting	Music Xray, Google Flu Trends
Filterung Auswahl und Ausschluss von Informationen	Spamfilter	Spamihilator
	Jugendschutz	Net Nanny
	Nachrichtenaggregatoren	Google News, Facebook News Feed

(Quelle: Eigene Darstellung nach World Wide Web Foundation, Algorithmic Accountability: Applying the concept to different country contexts, Juli 2017, S. 7)

[56] Vgl. *BGH*, Urt. v. 14.5.2013, VI ZR 269/12, NJW 2013, 2348; LG Wien, 24.11.2016, 13 Cg 16/16t-31, ZD 2017, 379; siehe auch *Georgios Gounalakis*, Rechtliche Grenzen der Autocomplete-Funktion von Google, NJW 2013, 2321 ff.

1.3 RISIKOANALYSE: KONSEQUENZEN DER VERWENDUNG VON ALGORITHMEN

Der Einsatz von ADM-Systemen ermöglicht nicht nur Effizienzgewinne, sondern geht auch einher mit dem Versprechen von Objektivität. *Bruno Lepri* et al. bringen dies auf die knappe Formel: „*Algorithmic decision-making processes might lead to more objective and thus potentially fairer decisions than those made by humans who may be influenced by greed, prejudice, fatigue, or hunger*".[57] Diese Einschätzung dürfte schon allein deshalb allzu optimistisch sein, weil bei der Gestaltung von ADM-Systemen stets bestimmte Wertungen einfließen[58] oder wie *Brent Mittelstadt* et al. es formulieren: „*Algorithms are inescapably value-laden.*"[59] Erschwerend kommt hinzu, dass die dem ADM-System zugrundeliegenden Wertungen in der „black box" versteckt sind und häufig sogar die Anwendung eines algorithmischen Entscheidungsprozesses für den Nutzer nicht erkennbar ist. Aus diesen Gründen ist der Einsatz von ADM-Systemen mit nicht unerheblichen Risiken für den Einzelnen und die Gesellschaft insgesamt verbunden. Dabei geht es nicht nur um handwerkliche Fehler bei der Programmierung von ADM-Systemen, sondern auch um grundsätzliche Gefahren und systembedingte Grenzen derartiger Systeme. Zu letzteren gehört der Umstand, dass aus den von einem Algorithmus ermittelten statistischen Zusammenhängen zwischen Variablen (Korrelationen) nicht ohne Weiteres auf Ursachen (kausale Effekte) oder Wirkmechanismen geschlossen werden kann. Drei Beispiele für Risiken, die mit dem Einsatz von ADM-Systemen verbunden sind, sollen nachfolgend kurz skizziert werden: das Auftreten algorithmischer Diskriminierungen, Manipulationsgefahren sowie die Entstehung von Filterblasen und Echokammern.

1.3.1 ALGORITHMISCHE DISKRIMINIERUNG

Wie der Überblick über die unterschiedlichen Anwendungsfelder und Typen algorithmenbasierter Entscheidungen gezeigt hat, werden ADM-Systeme häufig zur Klassifizierung eingesetzt, d.h. zur Zuordnung von Datenelementen zu bestimmten Gruppen: Programme zur Bilderkennung ordnen Objekte in unterschiedliche Kategorien, Programme zum Kredit-Scoring klassifizieren Verbraucher als kreditwürdig oder nicht kreditwürdig, Online-Persönlichkeitstests klassifizieren Stellenbewerber als geeignet oder ungeeignet und Programme, die von Gerichten zur Beurteilung des Rückfallrisikos von Straftätern eingesetzt werden, nehmen Einfluss auf die Entscheidung, ob eine Strafe zur Bewährung ausgesetzt wird oder nicht.

Bei solchen Klassifikationsentscheidungen können Diskriminierungen unterschiedlicher Art auftreten. Im Jahr 2016 hat beispielsweise das Nachrichtenportal ProPublica aufgedeckt, dass die in den USA zur Prognose des Rückfallrisikos von Straftätern eingesetzte Software COMPAS schwarze und weiße Häft-

[57] *Bruno Lepri*, *Nuria Oliver*, *Emmanuel Letouzé*, *Alex Pentland*, *Patrick Vinck*, Fair, Transparent, and Accountable Algorithmic Decision-making Processes Philos, Technol. (2017), https://doi.org/10.1007/s13347-017-0279-x.

[58] *Robert Seyfert & Jonathan Roberge*, Was sind Algorithmuskulturen, in: dies. (Hrsg.) Algorithmuskulturen: Über die rechnerische Konstruktion der Wirklichkeit, Transcript: Bielefeld 2017, S.24 sprechen daher von der „Legende algorithmischer Objektivität".

[59] *Brent Mittelstadt* et al., The ethics of algorithms: Mapping the debate, 3 Big Data & Society, 1-21 (2016).

linge unterschiedlich beurteilte.[60] Unter anderem wurde festgestellt, dass die Wahrscheinlichkeit, dass schwarze Häftlinge als hohes Risiko gekennzeichnet wurden, aber nicht wieder straffällig wurden, doppelt so hoch war wie bei weißen Häftlingen. Umgekehrt kam es bei weißen Häftlingen häufiger vor, dass sie als geringes Risiko eingestuft wurden, später jedoch wieder straffällig wurden.

Solche Verzerrungen im Output eines Algorithmus können unterschiedliche Ursachen haben. Eine simple Erklärung wäre, dass etwaige Vorurteile eines möglicherweise weißen Programmierers Eingang in das Design des Algorithmus gefunden haben.[61] Denkbar ist aber auch, dass sich die Verzerrung bereits in den Trainingsdaten findet, anhand derer das Programm gelernt hat, seine Prognosen zu treffen. Ergibt sich aus den historischen Trainingsdaten eine statistisch höhere Rückfallquote für schwarze Häftlinge, besteht die Gefahr, dass das Programm das entsprechende Muster aus der Vergangenheit erlernt und in die Zukunft projiziert.

Die Ursachen können aber noch komplexer sein, wie ein Beispiel diskriminierender Online-Werbung zeigt. Wissenschaftler der Carnegie Mellon University haben festgestellt, dass die Suchmaschine Google weiblichen Nutzern seltener Werbung für ein Führungskräftetraining zeigt als männlichen Nutzern.[62] Auch hier könnte man zunächst vermuten, dass Vorurteile der Programmierer die Ursache sind oder ein Trainingsdatensatz, aus dem das Programm lernt, dass Frauen (noch immer) unter Führungskräften unterrepräsentiert sind.

Zwei Wissenschaftlerinnen von der London Business School und der MIT Sloan School of Management haben jedoch Hinweise darauf gefunden, dass die ungleiche Werbung ihre Ursache möglicherweise in dem Auktionsmechanismus hat, den Google für den Verkauf der Werbeanzeigen verwendet.[63] Die Werbung wird in einem Auktionsverfahren den einzelnen Bietern zugeteilt, das eine optimale Preisbildung ermöglichen soll. Den Zuschlag für einen bestimmten Werbeplatz oder ein bestimmtes Zielpublikum erhält dabei jeweils der Bieter mit dem höchsten Angebot. Frauen im Alter zwischen 18 und 35 Jahren sind dabei eine besonders begehrte Zielgruppe. Dementsprechend ist Werbung, die Frauen dieser Altersgruppe angezeigt werden soll, teurer, als Werbung, die Männern gezeigt werden soll. Dies hat zur Folge, dass ein Bieter, der keine Präferenz für Männer oder Frauen als Zielgruppe angegeben hat, von anderen Bietern verdrängt wird, die explizit Frauen als Zielgruppe gewählt haben und bereit sind, dafür einen höheren Preis zu zahlen. Im Ergebnis führt dies dazu, dass die Werbung des Bieters, der keine Präferenz angegeben hat, mehr Männern als Frauen gezeigt wird. Hier zeigt sich, dass sich eine (scheinbare) Dis-

[60] *ProPublica*, Machine Bias (23.5.2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; siehe dazu auch *Matthias Spielkamp*, Sind Algorithmen die besseren Richter, Technology Review (16.10.2017), https://www.heise.de/tr/artikel/Sind-Algorithmen-die-besseren-Richter-3861814.html; *Ellora Thadaney Israni*, When an algorithm helps send you to prison, New York Times (26.10.2017), https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html.

[61] Vgl. *Kate Crawford*, Artificial Intelligence's White Guy Problem, New York Times (25.6.2016), http://nyti.ms/28YaKg7.

[62] *Amit Datta, M. C. Tschantz & Anupam Datta*, Automated experiments on ad privacy settings, Proceedings on Privacy Enhancing Technologies 92-112 (2015).

[63] *Anja Lambrecht and Catherine E. Tucker*, Algorithmic bias? An empirical study into apparent gender-based discrimination in the display of STEM career ads, Social Science Research Network (SSRN), August 2017.

kriminierung auch als unbeabsichtigter Nebeneffekt des Wettbewerbs um Werbekunden bzw. als Output eines ADM-Systems entstehen kann, das daraufhin optimiert ist, Werbung kosteneffizient zu verteilen.[64]

Die Beispiele zeigen, dass die Ursachen für algorithmische Diskriminierungen sehr vielfältig und komplex sein können. Dies macht zugleich deutlich, dass technische und institutionelle Maßnahmen zur Aufdeckung von Diskriminierungen, etwa „Algorithm Audits“[65] einen breiten Prüfradius vorsehen müssen, um unterschiedliche Ursachen zu ermitteln.

Die Bedeutung der Trainingsdaten als mögliche Ursache von Diskriminierungen zeigt noch ein weiteres Beispiel. Wird etwa ein ADM-System, das zur Bilderkennung eingesetzt werden soll, anhand eines Trainingsdatensatzes trainiert, der überwiegend Bilder hellhäutiger Personen enthält, führt dies (erwartungsgemäß) dazu, dass die erlernte Fähigkeit zur Bilderkennung bei dunkelhäutigen Personen schlechter ausfällt als bei hellhäutigen Personen. Besonders schwerwiegend wäre ein solcher Effekt etwa bei einem ADM-System, das zur Analyse medizinischer Bilddaten (z.B. zur Erkennung von Melanomen) eingesetzt werden soll und das anhand eines Trainingsdatensatzes trainiert wird, der überwiegend von hellhäutigen Patienten stammt. Dies könnte zur Folge haben, dass das Programm später bei dunkelhäutigen Patienten eine geringere Prognosegenauigkeit aufweist.[66]

1.3.2 MANIPULATIONSGEFAHREN

Neben der Gefahr von algorithmischen Diskriminierungen bestehen bei dem Einsatz von ADM-Systemen auch Manipulationsgefahren. Dies gilt insbesondere für Suchmaschinen und soziale Netzwerke, aber auch für Online-Shops und Plattformen der Sharing Economy. Mögliche Manipulationen können dabei sowohl intern (d.h. durch den Betreiber des ADM-Systems) als auch extern (d.h. durch Dritte) entstehen.

Ein Beispiel für eine (möglicherweise erfolgte) *interne* Manipulationen liefert die Google-Shopping-Entscheidung der EU-Kommission, bei der es u.a. um den Vorwurf geht, Google habe seinen eigenen Preisvergleichsdienst "Google Shopping" in den Suchergebnissen ganz oben oder sogar noch stärker hervorgehoben platziert, wodurch andere Vergleichsdienste herabgestuft worden seien.[67]

Beispiele für *externe* Manipulationen, die das Vertrauen in ADM-Systeme unterminieren können, sind etwa gefälschte Bewertungen (*fake reviews*) in Online Shops,[68] bestimmte Praktiken zur Suchmaschinenoptimierung sowie der Einsatz von Social Bots zur Beeinflussung der Meinungsbildung in sozialen Medien.[69] Die zuletzt genannten Beispiele betreffen zwar nicht Gefahrenquellen, die sich unmittelbar aus dem

---

[64] Siehe dazu auch *Amit Datta* et al., Discrimination in Online Advertising: A Multidisciplinary Inquiry Conference on Fairness, Accountability and Transparency, 2018, S. 20-34.

[65] Siehe dazu Abschnitt 3.4.1.

[66] *Joy Buolamwini* & *Timnit Gebru*, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, In: Conference on Fairness, Accountability and Transparency, 2018, S. 77-91.

[67] EU-Kommission, Entscheidung v. 27.6.2017, Case AT.39740 – Google Search (Shopping).

[68] Vgl. *Ben Edelman*, The market design and policy of online review platforms, 33 Oxford Review of Economic Policy 635 (2017); *Christoph Busch*, Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy, in: De Franceschi (ed.), European Contract Law and the Digital Single Market: Implications of the Digital Revolution, Intersentia, Cambridge 2016, S. 223 ff.

[69] Vgl. *Boris Paal/Moritz Hennemann*, Meinungsvielfalt im Internet: Regulierungsoptionen in Ansehung von Algorithmen, Fake News und Social Bots, ZRP 2017, 76.

Einsatz von ADM-Systemen ergeben. Die Besonderheit liegt vielmehr darin, dass ADM-Systeme einerseits mit der Erwartung der Objektivität verbunden sind und andererseits aufgrund ihrer Eigenschaft als „black box" die Feststellung von möglichen Manipulationen erheblich erschweren.

1.3.3 FILTERBLASEN UND ECHOKAMMERN

Eine weitere Gefahr ist die Entstehung algorithmisch erzeugter Filterblasen und Echokammern. Der von dem amerikanischen Internetaktivisten *Eli Pariser* geprägte Begriff der „Filterblase" bezeichnet geschlossene Kommunikationsräume in denen Personen nur noch Informationen erhalten, die ihrer Weltsicht entsprechen.[70] Die Gefahr von Filterblasen soll insbesondere in sozialen Netzwerken wie Facebook, LinkedIn oder Twitter bestehen, die ihren Nutzern einen personalisierten Newsfeed zur Verfügung stellen. Die Personalisierung zielt darauf, dass die angezeigten Nachrichten für den Nutzer möglichst interessant sind, damit er möglichst viel Zeit auf der Plattform verbringt.[71] Zu diesem Zweck lernen die Filteralgorithmen vom Verhalten des Nutzers dessen Präferenzen und liefern ihm entsprechende Nachrichten. Dies könnte, so die zugrundeliegende Überlegung, dazu führen, dass der Nutzer nur noch Nachrichten erhält, die einer bestimmten Weltsicht entsprechen. Diese Gefahr besteht insbesondere dann, wenn der personalisierte Newsfeed die wichtigste oder gar einzige Quelle ist, aus der sich ein Nutzer vorwiegend oder ausschließlich über politische und gesellschaftliche Themen informiert. Der verwandte Begriff der „Echokammer" beschreibt, wie der Austausch mit politisch Gleichgesinnten in sozialen Netzwerken ebenfalls zu einer Verengung der Weltsicht führen kann. Die Entstehung von Filterblasen und Echokammern kann Auswirkungen auf die politische Meinungsbildung haben. Der Einsatz algorithmischer Systeme als Vermittler personalisierter Informationen könnte so zu einer Zersplitterung von Öffentlichkeiten führen, das Meinungsklima verändern und Polarisierungstendenzen verstärken.

Es ist jedoch umstritten, wie stark der von *Pariser* beschriebene Effekt tatsächlich ist. Eine empirische Absicherung des Phänomens steht noch aus.[72] Einige Studien deuten darauf hin, dass die Angst vor Filterblasen möglicherweise übertrieben ist.[73] Zwar könnten soziale Netzwerke durch ihre Funktion als Informationsintermediäre die wahrgenommene Wichtigkeit bestimmter politischer Themen beeinflussen (Agenda-Setting-Funktion).[74] Die Entstehung von Filterblasen hängt jedoch stark davon ab, ob die Nutzer sich aus unterschiedlichen Informationsquellen informieren. Auch unabhängig vom individuellen Nutzungsverhalten sei weiterhin eine gemeinsame Themenagenda zu finden. In diese Richtung deuten auch

---

[70] *Eli Pariser*, The Filter Bubble: What The Internet Is Hiding From You, Penguin Press Limited, New York 2011; siehe auch *Seth Flaxman, Sharad Goel & Justin M. Rao*, Filter bubbles, echo chambers, and online news consumption, 80 Public Opinion Quarterly 298-320 (2016); *E. Bakshy, S. Messing & L. Adamic*, Exposure to ideologically diverse news and opinion on Facebook, 348 Science, 1130-1132, (2015); *Boris Paal & Moritz Hennemann*, Meinungsvielfalt im Internet: Regulierungsoptionen in Ansehung von Algorithmen, Fake News und Social Bots, ZRP 2017, 76.

[71] Der von Facebook zur Erstellung des Newsfeeds verwendete Algorithmus EdgeRank stellte bis 2013 auf drei zentrale Kriterien ab: (1) die persönliche Beziehung und die Intensität des Austauschs zu dem Nutzer, der die Nachricht teilt (affinity), (2) eine Gewichtung nach der vermuteten Bedeutung der Nachricht für den Empfänger (weight) wobei u.a. berücksichtigt wurde, ob eine Nachricht bereits viele Likes von anderen Nutzern erhalten hat, (3) Aktualität der Nachricht (time decay), vgl. *Josef Drexl*, Bedrohung der Meinungsvielfalt durch Algorithmen, ZUM 2017, 529 (532).

[72] So auch *Katharina A. Zweig, Oliver Deussen & Tobias Krafft*, Algorithmen und Meinungsbildung: Eine grundlegende Einführung, Informatik Spektrum 2017, 318 (324).

[73] *Birgit Stark*, Meinungsbildung im Netz: Die Macht der Algorithmen, MMR 2017, 721 (722).

[74] *Birgit Stark*, (Fn. 73) 722.

die Ergebnisse eines Crowdsourcing-Projekts, das die Initiative AlgorithmWatch vor der Bundestagswahl 2017 durchgeführt hat. Dabei wurde festgestellt, dass Suchergebnisse bei Suchanfragen zum Wahlprogramm der Parteien oder den Namen der Spitzenkandidaten von der Suchmaschine Google kaum personalisiert werden. Anzumerken bleibt, dass die Entstehung von Filterblasen nicht nur in Bezug auf Nachrichten und die politische Meinungsbildung möglich ist, sondern auch kulturelle Geschmacks- und Präferenzformungen betreffen kann, etwa durch Empfehlungsalgorithmen für Filme (z.B. Netflix) oder Musik (z.B. Spotify).[75]

1.4 SOZIALE KONTEXTE: INTERESSEN UND ANFORDERUNGEN DER STAKEHOLDER

Den Abschluss von Teil 1 der Studie bildet ein kurzer Überblick über soziale Kontexte und Diskurszusammenhänge, in die der Einsatz von Algorithmen eingebettet ist. Unterschiedliche Stakeholder artikulieren unterschiedliche Erwartungen in Bezug auf ADM-Systeme und legen dabei unterschiedliche Konzepte von „algorithmic accountability" zugrunde. Nachfolgend sollen beispielhaft einige Interessen und Anforderungen skizziert werden, die von Vertreten aus den Bereichen Politik, Wirtschaft, Programmierende und Verbraucherschützer geäußert werden.

1.4.1 POLITIK

Auf der politischen Ebene wurde die Debatte über einen verantwortlichen Umgang mit ADM-Systemen maßgeblich durch die im Juli 2017 von Bundesjustizminister *Heiko Maas* (SPD) erhobene Forderung nach einem Algorithmengesetz angestoßen.[76] Auch in den Wahlprogrammen der im Bundestag vertretenen Parteien für die Bundestagswahl 2017 finden sich Positionierungen zur Regulierung algorithmenbasierter Entscheidungen und dem damit verwandten Thema Künstliche Intelligenz (KI). In Bezug auf die mit ADM-Prozessen verbunden Chancen, die insbesondere in den Bereichen Smart City, intelligente Verkehrssteuerung und autonomes Fahren gesehen werden, gibt es eine weitgehende Übereinstimmung zwischen den Parteien. Gleiches gilt in Bezug auf die sozialen, umweltpolitischen und arbeitsmarktpolitischen Vorteile eines zunehmenden Einsatzes von KI, von Assistenzsystemen und algorithmenbasierten Entscheidungsunterstützungssystemen.

Die Risiken und damit auch die Notwendigkeit einer staatlichen Regulierung beurteilen die Parteien dagegen unterschiedlich. Divergenzen bestehen sowohl in Bezug auf die Sektoren in denen Regulierungsbedarf gesehen wird, als auch bei der Frage nach den geeigneten Regulierungsinstrumenten. Der Regulierungsbedarf und die Notwendigkeit einer staatlichen Marktaufsicht bzw. Marktlenkung werden insbesondere dort gesehen, wo die algorithmenbasierten Entscheidungen den Einzelnen betreffen (z.B. Kre-

[75] *Robert Seyfert & Jonathan Roberge*, Algorithmuskulturen: Über die rechnerische Konstruktion der Wirklichkeit, Transcript Verlag, 2017, S. 18.

[76] Rede des Bundesministers der Justiz und für Verbraucherschutz *Heiko Maas*, „Zusammenleben in der digitalen Gesellschaft – Teilhabe ermöglichen, Sicherheit gewährleisten, Freiheit bewahren" bei der Konferenz „Digitales Leben – Vernetzt. Vermessen. Verkauft? #Werte #Algorithmen #IoT" am 3.7.2017 in Berlin, http://www.bmjv.de/SharedDocs/Reden/DE/2017/07032017_digitales_Leben.html.

ditvergabe, Gewährung von Gesundheitsleistungen und sonstigen staatlichen Leistungen, individualisierte Preise, Abschluss und Ausgestaltung von Verträgen, insbesondere Versicherungen). Regulierungsbedarf wird auch in Bereichen gesehen, die für die gesellschaftliche Meinungsbildung besonders relevant sind.[77]

Die CDU konzentriert sich dabei in ihrem Wahlprogramm für die Bundestagswahl 2017 auf die Themen autonomes Fahren, intelligente Verkehrssteuerung und innere Sicherheit.[78] ADM-Systeme werden als grundsätzlich gesellschaftlich wünschenswert und durch die Politik zu fördern dargestellt. Der Bedarf nach Transparenz und staatlich gelenkter Kontrolle für ADM-Systeme wird zwar benannt, welche Strukturen geschaffen werden sollen oder müssen, um eine sachgerechte Regulierung sicherzustellen, bleibt jedoch offen. Ziel ist es in erster Linie eine diskriminierungsfreie Anwendung von Algorithmen sicherzustellen.[79]

Konkreter setzt sich die SPD insbesondere mit den zu schaffenden Strukturen für eine Kontrolle und Regulierung von Algorithmen auseinander. Sie fordert in ihrem Wahlprogramm[80] neben dem Vorstoß für ein digitales Gleichbehandlungsgesetz einen (behördlichen) Algorithmen-TÜV und eine Daten-Ethikkommission. Die missbräuchliche und diskriminierende Anwendung von Algorithmen solle so verhindert werden. Zu erreichen sei dies insbesondere durch eine Überprüfung der in algorithmenbasierten Entscheidungen einfließenden Daten und eine Stärkung des Grundsatzes der Datensparsamkeit.

Die FDP steht der Regulierung von ADM-Systemen und einer weitgehenden Transparenz von Algorithmen eher skeptisch gegenüber. Den Staat sehen die Liberalen in erster Linie in der Verantwortung, Leitplanken für die Anwendung von algorithmenbasierten Entscheidungen und künstlicher Intelligenz zu setzen und durch Medienbildung die Eigenverantwortung der Bevölkerung in Fragen der Digitalisierung zu fördern.[81] Detaillierte Zielvorstellungen finden sich im Wahlprogramm zum Thema Datenschutz.[82] Die FDP setzt sich für die Schaffung eines Einwilligungsmodells zur Nutzung personenbezogener Daten ein. Dieses soll dadurch ergänzt werden, dass der Einwilligende gegenüber staatlichen und privaten Stellen ein Recht auf Auskunft über die Nutzung und Auswertung seiner Daten bekommt. Nicht-personenbezogene Daten, die mit oder durch Maschinen erfasst werden, sollen nach dem Willen der FDP in Zukunft nicht mehr dem Maschinenhersteller oder dem Dienstleistungsanbieter allein zur Verfügung stehen, sondern explizit auch dem Nutzer der Maschine zur weiteren Verwendung frei zugänglich sein. Eine solche umfassende Datenportabilität ist derzeit bei einem Wechsel der Hardware oder des

---

[77] *Alexander von Humboldt Institut für Internet und Gesellschaft*, Wahlkompass Digitales, https://www.hiig.de/project/wahlkompass-digitales/.

[78] *CDU/CSU* (2017), Für ein Deutschland, in dem wir gut und gerne leben, Regierungsprogramm 2017-2021, S.51, 61, https://www.cdu.de/system/tdf/media/dokumente/170703regierungsprogramm2017.pdf?file=1.

[79] *Anita Klingel & Konrad Lischka*, Was die Wahlprogramme über Maschinen sagen, die Menschen bewerten, https://algorithmenethik.de/2017/09/11/was-die-wahlprogramme-ueber-maschinen-sagen-die-menschen-bewerten/.

[80] *SPD* (2017), Zeit für mehr Gerechtigkeit. Unser Regierungsprogramm für Deutschland, https://www.spd.de/fileadmin/Dokumente/Regierungsprogramm/SPD_Regierungsprogramm_BTW_2017_A5_RZ_WEB.pdf.

[81] *FDP* (2017), Denken wir neu. Das Programm der Freien Demokraten zur Bundestagswahl 2017: „Schauen wir nicht länger zu", S. 26, 28, https://www.fdp.de/sites/default/files/uploads/2017/08/07/20170807-wahlprogramm-wp-2017-v16.pdf.

[82] *FDP* (2017), S. 45-47, 75-76.

Dienstleisters nicht gesetzlich geregelt.

Zur Beantwortung der „Ethischen Fragen der digitalen Transformation“ wollen die Grünen durch den 19. Deutschen Bundestag eine Enquete-Kommission einrichten lassen.[83] Sie sehen einerseits den Staat in der Verantwortung Machtkonzentrationen und Diskriminierung im Zuge der Digitalisierung zu unterbinden und die Gesellschaft durch Bildung, Verbraucherschutz und an die gesellschaftlichen Implikationen der Digitalisierung angepassten Transparenzanforderungen zu befähigen, die Chancen der Digitalisierung für sich zu nutzen, und gleichzeitig die Risiken zu erkennen und zu bewerten. Für Social Bots soll eine Kennzeichnungspflicht eingeführt werden. Ein zentrales Ziel der digitalen Transformation muss es nach Auffassung der Grünen sein, „die ökologischen Chancen der Digitalisierung“ zu nutzen. Insbesondere im Bereich Mobilität sehen die Grünen entsprechende Potenziale.

Eine übergeordnete Auseinandersetzung mit den Fragen der Digitalisierung findet man im Wahlprogramm der Linken. Die linke Algorithmenpolitik formuliert, ebenso wie viele andere Parteien, den Anspruch, dass die automatisierte Auswertung großer Datenmengen dem Wohle der Allgemeinheit dienen solle. Den Einsatz von ADM-Systemen, die eine Bewertung des Individuums zum Ziel haben, wie etwa beim Kreditscoring, dem *predictive policing* oder der Gewährung von Leistungen der sozialen Sicherungssysteme, sehen die Linken kritisch und lehnen diese ab.[84] Zusammenfassend kann die Positionierung der Linken als weniger konkret und eher zurückhaltend beschrieben werden. Als Begründung für diese Haltung führen die Linken die große Komplexität der sich stellenden ethischen und sozialen Fragen an, deren Beantwortung nach Meinung der Linken nicht anhand von knappen Kernaussagen zum Beispiel in einem Wahlprogramm beantwortet werden können.

Das Wahlprogramm[85] der AfD enthält keine eindeutige Positionierung zu Fragen des Datenschutzes und zum digitalen Verbraucherschutz. Befürwortet wird allerdings der Einsatz von Videoüberwachung mit Gesichtserkennung zur Kriminalitätsbekämpfung.

1.4.2 WIRTSCHAFT

Stellvertretend für die deutsche Digitalwirtschaft setzt sich Bitkom in einem Positionspapier[86] für einen innovationsfreundlichen Regulierungsrahmen im Bereich der Anwendungen künstlicher Intelligenz und der Nutzung algorithmenbasierter Entscheidungssysteme ein. Der Digitalverband betont einerseits die Notwendigkeit einer digitalen Bildungsoffensive, sieht hier allerdings nicht nur die Information der breiten Bevölkerung im Mittelpunkt, sondern legt den Schwerpunkt vielmehr in die Aus- und Weiterbildung der Arbeitnehmer. Den Anspruch, die gesamte Bevölkerung in die Lage zu versetzen KI-Systeme „zu verstehen“ und algorithmenbasierte Entscheidungen nachzuvollziehen, um dieses Wissen in eine selbstbe-

[83] *Die Grünen* (2017), Zukunft wird aus Mut gemacht. Bundestagswahlprogramm 2017, S. 223.
[84] *Die Linke* (2017), Sozial. Gerecht. Frieden. Für Alle. Die Zukunft für die wir kämpfen. Langfassung des Wahlprogramms zur Bundestagswahl 2017, S. 122-124.
[85] *AfD* (2017), Programm für Deutschland, https://www.afd.de/wahlprogramm/.
[86] *Bitkom* (2017), Entscheidungsunterstützung mit Künstlicher Intelligenz - Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, https://www.bitkom.org/Bitkom/Publikationen/Entscheidungsunterstuetzung-mit-Kuenstlicher-Intelligenz-Wirtschaftliche-Bedeutung-gesellschaftliche-Herausforderungen-menschliche-Verantwortung.html

stimmte Anwendung und Nutzung solcher Systeme einfließen lassen zu können, hält Bitkom einerseits für unrealistisch und andererseits für nicht zielführend. Die Digitalwirtschaft setzt darauf, dass das Vertrauen in und damit auch die Akzeptanz von ADM-Systemen und KI dadurch entsteht, dass die Gesellschaft schrittweise an diese Innovationen herangeführt wird. Das bedeutet, dass die letzte Entscheidungsgewalt zum Beispiel beim autonomen Fahren beim Nutzer verbleibt. Außerdem fordert Bitkom Politik und Gesellschaft zu einem Dialog mit Wirtschaft und Wissenschaft über ethische Fragen algorithmenbasierter Entscheidungssysteme auf, die dann den Rahmen für die Entwicklung und Nutzung von KI-Anwendungen und ADM-Systemen bilden. Wie die Entwicklung, Nutzung und Weiterentwicklung von Anwendungen jenseits der gesellschaftlichen Akzeptanz verhindert werden sollen, lässt der Digitalverband offen. Er setzt offenbar auf eine Selbstverpflichtung seiner Mitglieder und sieht keinen staatlichen Regulierungsbedarf über die bestehenden gesetzlichen Regelungen hinaus. Bitkom geht sogar so weit, dass ein Abschmelzen des Schutzniveaus der Datenschutzgrundverordnung in Bereichen gefordert wird, in denen die Regelungen nicht dem Schutz der Privatsphäre dienen, sondern als Innovationshemmnis bei der weiteren Entwicklung algorithmenbasierter Entscheidungssysteme wirken.

Auch das Institut der deutschen Wirtschaft (IW Köln) spricht sich gegen eine Kontrolle von Algorithmen aus.[87] Es sieht die Aufgabe der Politik vielmehr darin, durch eine digitale Bildungsinitiative die Bevölkerung zu befähigen, digitale Geschäftsmodelle und algorithmenbasierte Entscheidungssysteme informiert und eigenverantwortlich zu nutzen. Eine Algorithmenkontrolle wird auf der einen Seite als nicht praktikabel zurückgewiesen, da sie sich als Standortnachteil für die deutsche Wirtschaft herausstellen und darüber hinaus ein Innovationshemmnis in Deutschland darstellen würde.

1.4.3 PROGRAMMIERENDE

Die Programmierenden nehmen bei der Gestaltung von ADM-Systemen und damit bei der praktischen Implementierung von „algorithmic accountability“ eine zentrale Rolle ein. Als soziale Gruppe – sofern man davon sprechen kann – ist der Kreis der Programmierenden allerdings sehr heterogen und es fällt schwer auszumachen, wer für „die“ Programmierenden spricht. Positionierungen von Teilgruppen finden u.a. an den Schnittstellen zur Wissenschaft statt.

Exemplarisch kann dafür das im August 2017 vor der Bundestagswahl von der Gesellschaft für Informatik e.V. herausgegebene Sonderheft der Zeitschrift „Informatik Spektrum“ zum Thema „Algorithmen und Meinungsbildung“ genannt werden. Darin behandelt werden u.a. das Thema „Microtargeting“ (die gezielte Ansprache von Personen und Gruppen) und die Frage, ob und wie weit die US-Wahl tatsächlich durch soziale Medien beeinflusst wurde. In zwei weiteren Beiträgen werden die wichtigsten netzpolitischen Akteure in Deutschland beschrieben und die Rolle von Informationsintermediären wie Facebook oder Google News und ihre mögliche Regulierung beleuchtet. Ebenfalls an der Schnittstelle zur Wissenschaft angesiedelt ist die amerikanische Initiative „Fairness, Accountability and Transparency in Machine Learning“, die fünf Prinzipen formuliert hat, anhand derer die gesellschaftlichen und ethischen Folgen von

[87] *Christian Rusche*, Gefahr für digitale Geschäftsmodelle (3.7.2017), https://www.iwkoeln.de/presse/iw-nachrichten/beitrag/christian-rusche-gefahr-fuer-digitale-geschaeftsmodelle-347922.html.

ADM-Prozessen beurteilt werden sollen: Verantwortlichkeit (responsibility), Erklärbarkeit (explainability), Genauigkeit (accuracy), Überprüfbarkeit (auditability) und Gerechtigkeit (fairness).

Vertreter von Programmierenden engagieren sich auch im Rahmen der Initiative AlgorithmWatch,[88] die sich das Ziel gesetzt hat, mit Mitteln der Zivilgesellschaft zur Verwirklichung von „algorithmic accountability" beizutragen und u.a. im Februar 2018 die Kampagne „OpenSchufa" gestartet hat. Zu erwähnen ist ferner der Chaos Computer Club, der auch als Sprachrohr der „Hacker-Community" dient, aus deren Reihen etwa die Forderung nach Widerstand gegen KI erhoben wurde.[89]

1.4.4 VERBRAUCHER

Der Verbraucherzentrale Bundesverband (VZBV) hat im Dezember 2017 ein Thesenpapier[90] zu algorithmenbasierten Entscheidungsprozessen vorgelegt, in dem u.a. die Forderung nach einem staatlich legitimierten Kontrollsystem erhoben wird, durch das relevante ADM-Systeme auf ihre Rechtskonformität hin überprüft werden sollen. Gefordert wird außerdem mehr Algorithmentransparenz, etwa die Offenlegung von Datenbasis, Entscheidungskriterien und Gewichtung bei ADM-Prozessen. Der VZBV spricht sich ferner für Regeln und Standards für die technische Gestaltung von ADM-Prozessen („Nachvollziehbarkeit by Design") aus. Darüber hinaus müsse eine Gefährdungshaftung für Algorithmen eingeführt werden. Ähnliche Forderungen hatte bereits im Dezember 2016 der Sachverständigenrat für Verbraucherfragen beim BMJV erhoben.[91]

1.5 ZUSAMMENFASSUNG

Im Zuge der rasch voranschreitenden Digitalisierung und Automatisierung dringen algorithmenbasierte Entscheidungsprozesse (ADM) in immer neue Felder vor. Der „algorithmic turn" erfasst praktisch alle Lebensbereiche. Die ADM-Systeme erfüllen dabei unterschiedliche Aufgaben. Das Spektrum reicht von Filterfunktionen über Klassifikationen und Rankings bis zum Matching von Personen und Informationen. Teilweise dienen ADM-Prozesse nur der Vorbereitung und Unterstützung menschlicher Entscheidungen, teilweise treffen sie auch selbst maschinelle Entscheidungen. Insbesondere in der Plattformökonomie – von Handelsplattformen bis zu Social Media – übernehmen ADM-Systeme eine wichtige Funktion als Informationsintermediäre. Damit kommt ihnen und ihren Betreibern eine wirtschaftliche und politische Schlüsselrolle zu.

Gleichzeitig sind ADM-Systeme anfällig für Fehler und systembedingte Risiken. Dies gilt etwa für Fälle algorithmischer Diskriminierung sowie interne und externe Manipulationen des ADM-Systems. Die Konsequenzen treffen nicht nur den Einzelnen, sondern die Gesellschaft insgesamt. Verschärft wird dieses

[88] Siehe dazu das ADM-Manifest von AlgorithmWatch, vhttps://algorithmwatch.org/de/.
[89] *Patrick Beuth*, Notwehr against the machine, Die ZEIT (28.12.2017), http://www.zeit.de/digital/internet/2017-12/34c3-chaos-computer-club-kuenstliche-intelligenz.
[90] *VZBV*, Algorithmenbasierte Entscheidungsprozesse (7.12.2017), https://www.vzbv.de/sites/default/files/downloads/2017/12/14/17-12-05_vzbv_thesenpapier_algorithmen.pdf.
[91] *SVRV*, Verbraucherrecht 2.0 (Dezember 2016), http://www.svr-verbraucherfragen.de/wp-content/uploads/Kurzfassung-Verbraucherrecht-2.0_Lösungsoptionen.pdf.

Problem dadurch, dass die ADM-Systeme für die von der Entscheidung Betroffenen als „black box“ erscheint und die Ursachen von Fehlleistungen daher nur schwer festzustellen sind. Ob etwa eine Diskriminierung aufgrund struktureller Verzerrungen in den Trainingsdaten liegt, an einem Programmierfehler oder an Wechselwirkungen mit anderen Systemen, ist häufig nur mit großem Aufwand feststellbar.

Auf politischer Ebene scheint es einen breiten Konsens zu geben, dass auf den zunehmenden Einsatz von ADM-Systemen eine regulatorische Antwort gefunden werden muss. Mit Blick auf die Auswahl der geeigneten Regulierungsinstrumente besteht jedoch bislang keine Einigkeit.

2 EIGNUNG DES GELTENDEN REGULIERUNGSRAHMENS

In Teil 2 der Studie steht die Frage im Vordergrund, inwieweit der bestehende Regulierungsrahmen geeignet ist den in Teil 1 beschriebenen Gefahren von ADM-Prozessen zu begegnen und die Interessen der Betroffenen zu schützen. Ziel ist es, die Leistungsfähigkeit des regulatorischen Instrumentariums zu überprüfen, um mögliche Schutzlücken und Durchsetzungsdefizite im geltenden Recht herauszuarbeiten.

Die Vorgaben des geltenden Rechts für ADM-Prozesse leiten sich bislang vor allem aus dem Datenschutzrecht ab. Im Folgenden wird dabei die ab dem 25.5.2018 geltende EU-Datenschutz-Grundverordnung (DS-GVO) herangezogen. Von besonderer Relevanz sind hierbei das Verbot automatisierter Einzelfallentscheidungen nach Art. 22 DS-GVO und die Transparenzgebote der Art. 13-15 DS-GVO. Eine wichtige flankierende Funktion kommt der Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen gem. Art. 35 DS-GVO und der damit verbundenen Konsultationspflicht nach Art. 36 DS-GVO zu sowie den Dokumentationspflichten nach Art. 30 DS-GVO. Weitere rechtliche Vorgaben können sich insbesondere aus dem Kartell- und Lauterkeitsrecht ergeben sowie aus dem Allgemeinen Gleichbehandlungsgesetz. Hinzu kommen weitere sektorspezifische Regelungen, von denen hier exemplarisch das Medizinprodukterecht und die Regelungen für den algorithmischen Handel mit Finanzinstrumenten beleuchtet werden soll.

2.1 DATENSCHUTZRECHT

2.1.1 VERBOT AUTOMATISIERTER EINZELFALLENTSCHEIDUNGEN

Der Einsatz von ADM-Systemen, die nicht nur dazu dienen, menschliche Entscheidungen vorzubereiten, sondern selbst maschinelle Entscheidung treffen, begründet die Gefahr, dass der Einzelne zum bloßen Objekt der anonymen Entscheidung einer Softwareanwendung degradiert wird.[92] Dieser Gefahr tritt Art. 22 Abs. 1 DS-GVO entgegen. Danach hat der Einzelne das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihm gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt. Bereits vor Erlass der Vorgängerregelung in Art. 15 DSRL wurde die Möglichkeit einer missbräuchlichen Verwendung von Computern bei der Entscheidungsfindung als eine der „Hauptgefahren der Zukunft“ angesehen.[93] Vor diesem Hintergrund sah der ursprüngliche Entwurf der EU-Kommission zur DS-GVO noch ein umfassendes Profiling-Verbot vor.[94] Danach sollten Maßnahmen, die auf einer automatisierten Datenverarbeitung beruhen und deren Zweck in der Auswertung bestimmter Merkmale der Person oder

[92] *Mario Martini*, JZ 2017, 1017 (1019 f.); *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 1, 11; ähnlich bereits *Dammann/Simitis* Art. 15 DSRL Rn. 2.

[93] *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 1 mit Verweis auf die Begründung der Kommission zu Art. 16 des geänderten Richtlinienvorschlags (ABl.EG Nr. C 311/30).

[94] Art. 20 Abs. 1 des Kommissionsentwurfs zur DSGVO, KOM (2012) 11 endg.

in der Analyse bzw. Voraussage persönlicher Eigenschaften besteht, unzulässig sein. Ein derart umfassendes Verbot, das zahlreiche auf Big Data Analytics beruhende Geschäftsmodelle in Frage gestellt hätte,[95] wurde nicht in die endgültige Fassung der DS-GVO übernommen. Art. 22 DS-GVO verbietet Profiling nicht generell, sondern nur automatisierte Entscheidungen, die auf Profiling beruhen und „ohne jegliches menschliches Eingreifen“[96] erfolgen.

2.1.1.1. ANWENDUNGSBEREICH

2.1.1.1.1. Ausschließlich automatisierte Entscheidung

Das Verbot aus Art. 22 Abs. 1 DS-GVO erfasst nur Entscheidungen, die „ausschließlich“ auf Grundlage einer automatisierten Verarbeitung, d.h. ohne jegliche menschliche Einflussnahme, erfolgen. Nicht erfasst werden damit Fallgestaltungen, bei denen ein Algorithmus lediglich unterstützend in die *Entscheidungsvorbereitung* eingebunden ist, die Entscheidung letztlich aber von einem Menschen gefällt wird.[97] Der Vorschlag des Europäischen Parlaments, auch „vorrangig“ automatisierte Entscheidungen in den Anwendungsbereich von Art. 22 DS-GVO aufzunehmen, wurde nicht in die endgültige Fassung der DS-GVO aufgenommen.[98] Die Beteiligung des Menschen darf sich allerdings nicht nur auf einen rein *formalen* Akt beschränken. Aus dem Anwendungsbereich von Art. 22 Abs. 1 DS-GVO fallen daher nur solche Konstellationen, die durch eine *inhaltliche* Mitverantwortung eines menschlichen Entscheidungsträgers geprägt sind.[99]

Wird etwa ein automatisiertes Verfahren zur Bonitätsprüfung eingesetzt, so kommt es darauf an, ob die darauf gestützte Bonitätseinstufung durch einen Sachbearbeiter mit Entscheidungsbefugnis inhaltlich überprüft wird. Wird der automatisiert ermittelte Score-Wert dagegen ohne weitere inhaltliche Prüfung übernommen, liegt eine ausschließlich automatisierte Entscheidung nach Art. 22 Abs. 1 DS-GVO vor.[100] Gleiches soll für ein Bewerberauswahlprogramm gelten, das anhand online eingegebener Bewerberdaten und auf Basis eines mit einem Computer geführten „Bewerbungsgesprächs“ entscheidet, welche Kandidaten in die nächste Runde kommen.[101] Nimmt das Computerprogramm dagegen nur ein Ranking der Bewerber vor, auf dessen Grundlage der Arbeitgeber entscheidet, welche Bewerber in Betracht kommen, greift das Verbot des Art. 22 Abs. 1 DS-GVO nicht ein.[102]

2.1.1.1.2. Profiling

Als besondere Fallgruppe der automatisierten Verarbeitung erwähnt Art. 22 Abs. 1 DS-GVO das Profi-

---

[95] So die Einschätzung von *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 9.
[96] Erwgr. 71 Unterabs. 1 S. 1 DSGVO.
[97] *Martini*, in: Paal/Pauly, 2. Auf. 2018, Art. 22 DSGVO Rn. 20; *Mario Martini/David Nink*, Wenn Maschinen entscheiden… - vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ Extra 10/2017, 1 (3).
[98] Vgl. *Schulz*, in: Gola, Art. 22 DSGVO Rn. 12.
[99] *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 15.
[100] *Schulz*, in: Gola, Art. 22 DSGVO Rn. 15; *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 16; *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 24; *Hladjk*, in: Ehmann/Selmayr, Art. 22 DSGVO Rn. 9; zur Anwendbarkeit von Art. 18 DSGVO auf Scoring-Verfahren siehe auch *Jürgen Taeger*, Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, 3 ff.
[101] *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 16; siehe auch *Hladjk*, in: Ehmann/Selmayr, Art. 22 DSGVO Rn. 9. („Online-Einstellungsverfahren ohne jegliches menschliches Eingreifen“).
[102] *Schulz*, in: Gola, Art. 22. DSGVO Rn. 13.

ling. Nach der Legaldefinition in Art. 4 Nr. 4 DS-GVO bezeichnet der Begriff Profiling „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen". Eine *Bewertung* von Persönlichkeitsmerkmalen liegt dann vor, wenn eine *Interpretation* der Daten erfolgt, um daraus eine Einschätzung etwa über die Kreditwürdigkeit, die Leistungsfähigkeit oder die Lebenserwartung abzuleiten.[103] Beispiele sind etwa Kreditscoring, Verfahren zur Auswahl von Organempfängern oder Verfahren zur Auswahl von Bewerbern.[104]

Besondere Vorgaben für das Profiling formuliert Art. 22 DS-GVO nicht.[105] Mündet das Profiling nicht in eine ausschließlich automatisierte Entscheidung, so richtet sich die Zulässigkeit des Profilings nach den allgemeinen Rechtfertigungsregeln, insbesondere Art. 6 und 9 DS-GVO, die allerdings keine besonderen Anforderungen für Profiling-Maßnahmen stellen.[106] Spezifische Anforderungen für das Profiling finden sich lediglich in Erwgr. 71 DS-GVO. Danach soll der Verantwortliche „geeignete mathematische oder statistische Verfahren für das Profiling verwenden" und „technische und organisatorische Maßnahmen treffen" um Transparenz, Richtigkeit und Diskriminierungsfreiheit der Datenverarbeitung zu ermöglichen.

Diese Vorgaben bleiben in mehrfacher Weise hinter § 28b BDSG a.F. zurück, der Vorgaben für Scoring (als Unterfall des Profilings) enthält.[107] Zum einen stellte § 28b BDSG a.F. auf ein „wissenschaftlich anerkanntes mathematisch-statistisches Verfahren" ab, während in Erwgr. 71 nur von „geeigneten mathematischen oder statistischen Verfahren" die Rede ist. Zum anderen finden sich die Anforderungen für das Profiling nicht im Text der Verordnung selbst, sondern lediglich in einem Erwägungsgrund. Die Erwägungsgründe von Richtlinien und Verordnungen entfalten jedoch keine bindende Wirkung.[108] Sie sind nicht selbst Rechtsquelle, sondern lediglich Rechtserkenntnisquelle und können bei der Auslegung des Normtextes herangezogen werden.[109] Damit bleibt weitgehend unklar, welche rechtliche Wirkung die Vorgaben aus Erwgr. 71 in Bezug auf Profiling entfalten.[110]

2.1.1.1.3. Rechtliche Wirkung oder erhebliche Beeinträchtigung

Eine Einschränkung erfährt der Anwendungsbereich von Art. 22 Abs. 1 DS-GVO dadurch, dass das Ver-

---

[103] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 21.

[104] *Schreiber*, in: Plath, 2. Aufl. 2016, Art. 4 DSGVO Rn. 16; *Hladjk*, in: Ehmann/Selmayr, Art. 22 DSGVO Rn. 7.

[105] *Peter Schantz*, NJW 2016, 1841 (1844) spricht daher treffend von einer „symbolischen" Erwähnung des Profiling in Art. 22 DSGVO; zustimmend *Schulz*, in: Gola, Art. 22 DSGVO Rn. 20; ähnlich *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 21.

[106] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 22.

[107] Zu § 31 BDSG n.F., der den Schutzstandard aus § 28b BDSG a.F. aufrechterhalten soll, siehe unten in Abschnitt 2.1.1.2.

[108] *Sandra Wachter*, *Brent Mittelstadt & Luciano Floridi*, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, 7 International Data Privacy Law, 76 (80); siehe auch *Tadas Klimas/Jurate Vaiciukaite*, 'The Law of Recitals in European Community Legislation' (2008) 15 ILSA Journal of International & Comparative Law 32.

[109] *EuGH*, Urt. v. 13.7.1989, Rs. 215/88 – Casa Fleischhandel/BALM, ECLI:EU:C:1989:331, Rn. 31: „Eine Begründungserwägung einer Verordnung kann zwar dazu beitragen, Aufschluß über die Auslegung einer Rechtsvorschrift zu geben, sie kann jedoch nicht selbst eine solche Vorschrift darstellen."

[110] Kritisch auch *Hans W. Micklitz*, Ungeheuerliche Neuigkeiten?, VuR 2017, 43 (46).

bot nur für Entscheidungen gilt, die gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Von einer „rechtlichen Wirkung" kann immer dann die Rede sein, wenn sich durch die Entscheidung die Rechtsposition des Betroffenen ändert.[111] Beispiele sind etwa der Erlass eines Verwaltungsaktes (z.B. Erteilung, Verweigerung oder Rücknahme einer Gewerbeerlaubnis[112]) oder die Entscheidung, ein Vertragsangebot zu unterbreiten oder einen Vertrag zu kündigen. Eine „erhebliche Beeinträchtigung" ist immer dann anzunehmen, wenn der Betroffene in seiner wirtschaftlichen oder persönlichen Entfaltung erheblich gestört wird. Beispiele sind etwa die Ablehnung eines Vertragsschlusses, die Verweigerung einer bestimmten Zahlungsart (z.B. PayPal) oder die Versagung eines günstigeren Zinssatzes.[113] Ob die Belästigung durch personalisierte Werbung dagegen erfasst wird, ist umstritten.[114] Gegen die Einbeziehung personalisierter Werbung in den Anwendungsbereich von Art. 22 DS-GVO spricht ein Umkehrschluss aus Art. 21 Abs. 2 DS-GVO, der dem Betroffenen ein Widerspruchsrecht gegen Direktwerbung einräumt und dementsprechend von einem an sich rechtmäßigen Verarbeitungsvorgang ausgeht.[115]

2.1.1.1.4. Minderjährigenschutz

Erwgr. 71 UAbs. 1 S. 5 DS-GVO stellt ergänzend klar, dass eine automatisierte Entscheidung im Einzelfall kein Kind betreffen „sollte". Im Text von Art. 22 DS-GVO findet sich diese Regelung nicht wieder. Im Vergleich zur Trilog-Fassung des entsprechenden Erwägungsgrundes, der noch vorsah, dass die Entscheidung kein Kind betreffen „darf", sieht die DS-GVO hier nur einen gelockerten Minderjährigenschutz vor.[116] Auch die Artikel-29-Datenschutzgruppe vertritt in ihrer Stellungnahme zum Profiling die Auffassung, dass die DS-GVO nicht ein „absolutes Verbot" von automatisierten Einzelfallentscheidungen in Bezug auf Kinder formuliert, spricht aber zugleich die Empfehlung aus, dass in Bezug auf Kinder nicht von den Ausnahmen des Art. 22 Abs. 2 DS-GVO Gebrauch gemacht werden sollte.[117]

2.1.1.2. AUSNAHMEN

Eine weitere Einschränkung des durch Art. 22 DS-GVO gewährleisteten Schutzes ergibt sich durch die in Abs. 2 der Vorschrift geregelten Ausnahmetatbestände. Nach Art. 22 Abs. 2 lit. a DS-GVO ist eine automatisierte Generierung von Einzelentscheidungen zulässig, wenn sie für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Voraussetzung ist dafür das Bestehen eines unmittelbaren sachlichen Zusammenhangs zwischen der Datenver-

---

[111] *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 24; *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 26.

[112] *Hladjk*, in: Ehmann/Selmayr, Art. 22 DSGVO Rn. 9.

[113] Vgl. Erwgr. 71 Unterabs. 1 S. 1; *Lisa Deuster*, Automatisierte Entscheidungen nach der DS-GVO, PinG 2016, 75 (76); *Born*, ZD 2015, 66 (69); *Martini*, in: Paal/Pauly, Art. 22 DSGVO Rn. 26.

[114] Dafür Thilo Weichert, Big Data im Gesundheitsbereich, ABIDA-Gutachten, 2018, S. 135; dagegen Martini, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 Rn. 23; zweifelnd Hladjk, in: Ehmann/Selmayr, Art. 22 Rn. 9.

[115] *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 26; *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 23; siehe auch Erwgr. 70 S. 1 DSGVO.

[116] Vgl. auch *Mario Martini/David Nink*, Wenn Maschinen entscheiden… - vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ-Extra 10/2017, 1(6).

[117] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3.10.2017, S. 26: Als Beispiel wird der Fall genannt, dass ein ADM-System in Online Games dazu dient, Spieler zu identifizieren, die eher geneigt sind, Geld auszugeben, um diesen Spielern vermehrt personalisierte Werbung zu zeigen.

wendung und dem konkreten Vertragszweck.[118] Hat die betroffene Person ausdrücklich eingewilligt, ist die automatisierte Einzelfallentscheidung gem. Art. 22 Abs. 2 lit. c DS-GVO zulässig. Wie auch sonst bei der Einwilligung ist hierbei erforderlich, dass der Betroffene in Kenntnis der Sachlage, also hinreichend informiert, und mit Einsichtsfähigkeit sein Einverständnis freiwillig erklärt hat.[119]

Eine zusätzliche Öffnungsklausel für die Mitgliedstaaten enthält Art. 22 Abs. 2 lit. b DS-GVO. Danach ist eine automatisierte Einzelfallentscheidung zulässig, wenn Rechtsvorschriften eines Mitgliedstaats dies erlauben und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten. Der deutsche Gesetzgeber hat von dieser Möglichkeit in § 37 Abs. 1 BDSG n.F. für die Leistungserbringung bei Versicherungsverträgen Gebrauch gemacht, sofern dem Leistungsbegehren des Betroffenen stattgegeben wird.[120] Als Beispiel nennt die Gesetzesbegründung den Fall der automatisierten Schadensregelung zwischen der Kfz-Haftpflichtversicherung des Schädigers und dem Geschädigten.[121] Erweitert wird die Ausnahmeregelung durch die in § 37 Abs. 2 BDSG n.F. geregelte Befugnis, bei automatisierten Entscheidungen nach Absatz 1 auch Gesundheitsdaten zu verarbeiten.

Ob die neu gefasste Regelung zum Scoring in § 31 BDSG n.F. (der im Wesentlichen § 28b BDSG a.F. entspricht) auf Art. 22 Abs. 2 lit. b DS-GVO gestützt werden kann, erscheint zweifelhaft. Die Öffnungsklausel knüpft an das grundsätzliche Verbot automatisierter Einzelentscheidungen in Art. 22 Abs. 1 DS-GVO an. Die Regelung in § 31 BDSG n.F. setzt jedoch gar keine automatisierte Einzelentscheidung voraus, sondern gilt auch für Scoring-Verfahren, die eine menschliche Entscheidung vorbereiten sollen. Auf die Öffnungsklausel aus Art. 22 Abs. 2 lit. b DS-GVO kann § 31 BDSG n.F. daher nicht gestützt werden. Auch die teilweise vertretene Argumentation,[122] dass es sich bei § 28b BDSG a.F. und § 31 BDSG n.F. nur um Konkretisierungen der Verarbeitung personenbezogener Daten „zur Wahrung berechtigter Interessen" i.S.d. Art. 6 Abs. 1 lit. f DS-GVO handele, dürfte wohl nicht tragfähig sein, da hierdurch zusätzliche nationale Anforderungen an eine rechtmäßige Datenverarbeitung gestellt werden, die in der DS-GVO – außer in den ausdrücklich zugelassenen Fällen – nicht vorgesehen sind.[123] Ob § 31 BDSG n.F. den Vorgaben des Unionsrechts genügt, ist daher zweifelhaft.[124]

2.1.1.3. BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN

Für besondere Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DS-GVO verschärft Art. 22 Abs. 4 DS-GVO das Verbot automatisierter Entscheidungen. Die Regelung gilt für Daten, aus denen die rassi-

[118] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 31.
[119] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 38.
[120] Im Referentenentwurf (Stand: 2. Ressortabstimmung, 11.11.2016) für die Neufassung des BDSG war noch eine deutlich weitergehende Ausnahme vom Verbot der automatisierten Einzelfallentscheidungen vorgesehen sowie Einschränkungen des Verbots für alle Vertragsarten. Ebenfalls nicht aufgegriffen wurde der Vorschlag des Bundesrates (BT-Drs. 18/11655, 41), eine Ausweitung des § 37 BDSG auf weitere Vertragsarten zu prüfen und die Regelung des § 6a Abs. 2 S. 1 Nr. 1 BDSG a.F. beizubehalten, vgl. *Gräber/Nolden* in: Paal/Pauly, 2. Aufl. 2018, § 37 BDSG Rn. 3.
[121] BT-Drs. 18/11325, 105.
[122] *Jürgen Taeger*, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, 72 (74).
[123] *Flemming Moos/Tobias Rothkegel*, Nutzung von Scoring-Diensten im Online-Versandhandel, ZD 2016, 561 (567).
[124] So auch *Martini* in: Paal/Pauly, 2. Aufl. 2018, Art. 22 DSGVO Rn. 44.

sche und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Eine automatisierte Einzelfallentscheidung auf Basis derartiger Daten ist auch dann untersagt, wenn sie ansonsten nach Art. 22 Abs. 2 DS-GVO ausnahmsweise zulässig wäre.

Der Rückausnahme zu Art. 22 Abs. 2 DS-GVO liegt der Gedanke zugrunde, dass in Bezug auf die besonders sensiblen Kategorien personenbezogener Daten ein besonderes Diskriminierungspotential besteht.[125] So betont Erwgr. 71 DS-GVO, dass im Interesse einer fairen und transparenten Datenverarbeitung verhindert werden soll, „dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben."

Relativiert wird das Verbot nach Art. 22 Abs. 4 DS-GVO durch zwei Rückausnahmen. Eine automatisierte Entscheidung auf Grundlage der besonders sensiblen Daten ist zum einen dann zulässig, wenn die betroffene Person in die Verarbeitung der Daten ausdrücklich eingewilligt hat (Art. 9 Abs. 2 lit. a DS-GVO) oder die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist (Art. 9 Abs. 2 lit. g DS-GVO). Ist die Verarbeitung der besonders schutzwürdigen Daten nach einer dieser beiden Ausnahmetatbestände zulässig, kommt es für die Zulässigkeit der darauf basierenden automatisierten Entscheidung darauf an, dass einer der Ausnahmetatbestände des Art. 22 Abs. 2 DS-GVO eingreift.

Die hohen Hürden für automatisierte Entscheidungen auf Grundlage besonders sensibler Daten dürfte vor allem bei Big-Data-Anwendungen praktische Schwierigkeiten bereiten. Sind in dem Datenbestand, der für die automatisierte Entscheidungsfindung herangezogen wird, Daten enthalten, aus denen „die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit"[126] hervorgehen, so steht zu befürchten, dass diese Daten den Datenbestand „infizieren" und eine ansonsten zulässige automatisierte Entscheidung unzulässig machen.[127] Im Ergebnis könnte sich damit eine Sperrwirkung gegenüber Datenbeständen und deren Verwertung ergeben, wenn sich daraus besondere Kategorien von personenbezogenen Daten i.S.d. Art. 9 Abs. 1 DS-GVO ableiten lassen.[128]

2.1.1.4. ANGEMESSENE SCHUTZMAßNAHMEN

In den Fällen, in welchen ausnahmsweise eine automatisierte Entscheidung nach Art. 22 Abs. 2 DS-GVO zulässig ist, ist die Ausnahme an die Bedingung geknüpft, dass flankierend „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person" getroffenen werden (Art. 22 Abs. 2 lit. b, Abs. 3 und Abs. 4 DS-GVO). Welchen Inhalt die „angemessenen Maßnahmen" haben müssen, wird in Art. 22 Abs. 3 DS-GVO nur angedeutet. Weitere Konkretisierungen

[125] *Buchner*, in: *Kühling/Buchner* Art. 22 DSGVO Rn. 44.
[126] Art. 9 Abs. 1 DSGVO.
[127] *Jochen Schneider*, ZD 2017, 303 (306).
[128] *Jochen Schneider*, ZD 2017, 303 (307).

der Mindestgarantien finden sich in Erwgr. 71 DS-GVO. Die DS-GVO verbindet dabei zwei sich wechselseitig ergänzende Ansätze: Grundrechtsschutz durch Verfahren („procedural fairness“) und Grundrechtsschutz durch Technik („fairness by design“).

2.1.1.4.1. Prozedurale Mindestgarantien

Art. 22 Abs. 3 DS-GVO verlangt zunächst explizit, dass der betroffenen Person „mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.“ Nach dem Wortlaut der Vorschrift besteht das Recht auf „Erwirkung des Eingreifens einer Person“ vorbehaltlos. Dies hätte zur Konsequenz, dass der Betroffene jederzeit die Möglichkeit hätte, ohne nähere Begründung einer automatisierten Datenverarbeitung zu widersprechen. Die Vorschrift soll jedoch gerade – unter strikter Wahrung prozeduraler und technischer Mindestgarantien – eine automatisierte Datenverarbeitung ermöglichen. Ein voraussetzungsloses „opt-out“ des Betroffenen würde diesem Ziel zuwiderlaufen. Überzeugender erscheint es, wenn man Art. 22 Abs. 3 DS-GVO dahingehend einschränkend auslegt, dass dem Betroffenen lediglich ein Recht eingeräumt wird, aus berechtigten Gründen im Einzelfall das Eingreifen einer Person zu verlangen.[129]

Als weiteren Bestandteil der prozeduralen Mindestgarantien nennt Erwgr. 71 UAbs. 1 S. 4 DS-GVO das Recht „auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung“.[130] Dem Betroffenen soll damit zum einen die Möglichkeit eingeräumt werden, die Besonderheiten des Einzelfalles vorzutragen, die bei einer schematisch verlaufenden automatisierten Entscheidung keine Berücksichtigung finden. Um sicherzustellen, dass die Spezifika des Einzelfalls auch in die Entscheidung einfließen, wird man verlangen müssen, dass die Besonderheiten des Einzelfalles einem Menschen vorgetragen werden.[131] Zudem muss für den Betroffenen ein „Remonstrationsrecht“[132] bestehen, d.h. es muss die Möglichkeit bestehen, eine inhaltliche Neubewertung zu verlangen.

2.1.1.4.2. Technische Maßnahmen

Ergänzt werden die prozeduralen Mindestgarantien durch technische und organisatorische Anforderungen, die ebenfalls dazu dienen, ein faires Verfahren sicherzustellen. So verlangt Erwgr. 71 UAbs. 2 S. 1 DS-GVO, dass „geeignete mathematische oder statistische Verfahren“ eingesetzt werden, um etwa Verzerrungen des Persönlichkeitsbildes zu verhindern, die von untauglichen Berechnungsmodellen ausgehen

---

[129] So auch *Mario Martini & David Nink*, Wenn Maschinen entscheiden… vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ 10/2017, 1 (4); siehe auch *Meg Leta Jones*, The right to a human in the loop: Political constructions of computer automation and personhood, 47 Social studies of science 216-239 (2017).

[130] Zur strittigen Frage, ob aus der Formulierung „Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung“ eine Pflicht zur Offenlegung von ADM-Prozessen abgeleitet werden kann, siehe unten Abschnitt 2.1.2.3.

[131] Ebenso *Mario Martini/David Nink*, NVwZ-Extra 10/2017, 1 (4), die darauf hinweisen, dass es dem Recht auf Darlegung des eigenen Standpunkts nicht genügt, wenn der Betroffene lediglich die Möglichkeit hat, aus einer enumerativen Liste vorformulierter Aussagen auszuwählen.

[132] So *Kamlah*, in: Plath, 2.Aufl. 2016, Art. 22 DSGVO Rn. 14.

können.[133] Darüber soll der für die Datenverarbeitung Verantwortliche „technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird."[134] Hierdurch soll insbesondere sichergestellt werden, dass eine Diskriminierung auf Basis besonders schutzwürdiger Daten verhindert wird.

Konkretisiert werden diese Anforderungen in der im Oktober 2017 veröffentlichten Stellungnahme[135] der Artikel-29-Datenschutzgruppe. Als Beispiele für mögliche Fehler oder Verzerrungen („bias") in den gesammelten Daten oder im automatisierten Entscheidungsverfahren werden dort fehlerhafte Klassifikationen sowie Bewertungen aufgrund unsicherer Prognosen genannt, die sich negativ auf Einzelne auswirken. Die Artikel-29-Datenschutzgruppe empfiehlt eine regelmäßige Überprüfung der verarbeiteten Datensätze, um Verzerrungen zu identifizieren und Methoden zu entwickeln, um Probleme (z.B. eine zu starke Berücksichtigung von Korrelationen) zu beseitigen. Ebenfalls angeregt wird der Einsatz von Audit-Algorithmen und die regelmäßige Überprüfung von ADM-Verfahren, einschließlich Profiling. Darüber hinaus spricht sich die Artikel-29-Datenschutzgruppe dafür aus, geeignete Maßnahmen und Verfahren einzuführen, um Fehler, Ungenauigkeiten oder Diskriminierungen auf der Grundlage von besonders sensiblen Daten zu vermeiden. Entsprechende Prüfroutinen sollten nicht nur in der Entwurfsphase, sondern auch begleitend zum Datenverarbeitungsprozess eingesetzt werden. Die Ergebnisse der Überprüfung sollen in das Systemdesign der ADM-Prozesse einfließen. Die Stellungnahme der Artikel-29-Datenschutzgruppe enthält darüber hinaus weitere Empfehlungen für „good practice suggestions" im Sinne der „angemessene Maßnahmen" nach Art. 22 DS-GVO.[136]

2.1.2 TRANSPARENZGEBOTE

Das Transparenzgebot aus Art. 5 Abs. 1 lit. a DS-GVO wird durch eine Reihe von Einzelregelungen in der

[133] *Mario Martini/David Nink*, NVwZ-Extra 10/2017, 4; vgl. auch *von Lewinski*, in: Wolff/Brink, BeckOK DatenschutzR, 19. Ed. (Stand: 1.2.2017), BDSG § 28b Rn. 1 f; zur Anwendbarkeit von Art. 22 DSGVO auf Scoring-Algorithmen s. *Martini*, in: Paal/Pauly, 2. Aufl. 2018, DS-GVO, Art. 22 Rn. 24; *Buchner*, in: Kühling/Buchner, DS-GVO, 2017, Art. 22 Rn. 38.

[134] Erwgr. 71 Unterabs. 2 S. 1 DSGVO.

[135] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3.10.2017, S. 16 f.

[136] In den Guidelines der Artikel-29-Datenschutzgruppe heißt es: „The following list, though not exhaustive, provides some good practice suggestions for controllers to consider when profiling: regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise; algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results;specific measures for data minimisation to incorporate clear retention periods for profiles and for any personal data used when creating or applying the profiles; using anonymisation or pseudonymisation techniques in the context of profiling; ways to allow the data subject to express his or her point of view and contest the decision; and a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries. Controllers can also explore options such as: certification mechanisms for processing operations; codes of conduct for auditing processes involving machine learning; ethical review boards to assess the potential harms and benefits to society of particular applications for profiling."

DS-GVO konkretisiert. An erster Stelle sind dabei die Informationspflichten aus Art. 13, 14 DS-GVO und das Auskunftsrecht der betroffenen Person aus Art. 15 DS-GVO zu nennen. Ob sich weitere Transparenzpflichten möglicherweise aus Art. 22 Abs. 3 i.V.m. Erwgr. 71 UAbs. 1 S. 4 DS-GVO ergeben, ist umstritten.

2.1.2.1. INFORMATIONSPFLICHTEN

Die Art. 13 und 14 DS-GVO verpflichten den Verantwortlichen, die betroffenen Personen über die Datenverarbeitung zu informieren. Artikel 13 DS-GVO regelt Art und Umfang der Informationspflichten für den Fall, dass die personenbezogenen Daten bei der betroffenen Person selbst erhoben werden, Art. 14 DS-GVO enthält eine entsprechende Regelung für den Fall, dass die Daten aus anderen Quellen erhoben wurden. Die Informationspflichten sollen sicherstellen, dass der Betroffene von der Datenverarbeitung und deren Reichweite erfährt, damit er seine Rechte effektiv wahrnehmen kann.[137] Im Falle einer automatisierten Entscheidungsfindung gem. Art. 22 Abs. 1 und 4 DS-GVO muss der Betroffene über die Anwendung des ADM-Systems informiert werden und „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" erhalten (Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DS-GVO).

In Bezug auf ADM-Systeme stellt sich dabei insbesondere die Frage, wie ein Ausgleich zwischen dem Recht des Betroffenen auf „aussagekräftige" Informationen und dem berechtigten Interesse des Verantwortlichen auf den Schutz seiner Geschäftsgeheimnisse gefunden werden kann. Die Verpflichtung, eine aussagekräftige Information zur involvierten Logik zu erteilen, bedeutet nicht, dass bei ADM-Prozessen der Algorithmus des Verfahrens mitgeteilt werden muss.[138] Diese Auslegung von Art. 13 Abs. 2 lit. f bzw. Art. 14 lit. g DS-GVO wird auf die im Oktober 2017 veröffentlichten Leitlinien der Artikel-29-Datenschutzgruppe gestützt. Darin heißt es, dass der Verantwortliche lediglich den Zweck („the rationale behind") und die Kriterien, die bei der Entscheidungsfindung berücksichtigt werden, offenlegen sollte, ohne den Algorithmus selbst preiszugeben.[139] Beispielsweise muss im Falle eines Kreditscorings, das in eine automatisierte Kreditentscheidung mündet, darüber informiert werden, dass eine (ermittelte) schlechtere Bonität zu Einschränkungen bei der Zahlungsweise führen kann.[140]

In der Literatur wird teilweise versucht die Begrenzung der Informationspflicht aus Art. 12 Abs. 1 DS-GVO herzuleiten, der als Grundregel für die Informationspflichten eine Information in verständlicher, klarer und einfacher Sprache verlangt. Da die Offenlegung eines komplexen Algorithmus nicht in klarer und einfacher Sprache erfolgen könne, sei sie auch nicht geschuldet.[141] Diese Argumentation kann nicht

---

[137] *Jan Philipp Albrecht/Florian Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 4 Rn. 4; siehe auch Erwgr. 60 DSGVO.

[138] *Paal*, in: *Paal/Pauly*, 2. Aufl. 2018, Art. 13 DSGVO Rn. 31.

[139] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October, p. 14.

[140] Beispiel nach *Peter Bräutigam/Florian Schmidt-Wudy*, Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung, CR 2015, 56 (61).

[141] So etwa *Knyrim*, in: Ehmann/Selmayr, Art. 13 DSGVO Rn. 53; ähnlich *Kai von Lewinski/Dirk Pohl*, Auskunfteien nach der europäischen Datenschutzreform, ZD 2018, 17 (22), der Art. 12 DSGVO zumindest eine Indizwirkung gegen die Offenlegung des Algorithmus entnehmen möchte.

überzeugen. Das Kriterium der „klaren und einfachen Sprache“ in Art. 12 Abs. 1 DS-GVO dient dem Schutz des Informationsberechtigten, nicht des Informationsverpflichteten. Wenn man aus der Formulierung „klare und einfache Sprache“ eine inhaltliche Begrenzung der Informationspflichten nach Art. 13, 14 DS-GVO herleiten wollte, würde man Art. 12 Abs. 1 DS-GVO entgegen seinem Schutzzweck gegen den Informationsberechtigten wenden. Auch die Leitlinien der Artikel-29-Datenschutzgruppe betonen, dass die Komplexität des Algorithmus für sich genommen kein Grund für eine Verweigerung der Offenlegung ist.[142]

Im Ergebnis ist die Feststellung, dass eine Offenlegung des Algorithmus nicht geschuldet ist, gleichwohl zutreffend. Das zentrale Argument ist der auch in Erwgr. 63 DS-GVO angesprochene Schutz von Geschäftsgeheimnissen. Würde man eine Offenlegung des Algorithmus verlangen, so drohe eine Offenbarung von Geschäftsgeheimnissen.[143] Für einen sachgerechten Ausgleich zwischen der Forderung nach Algorithmentransparenz und Geheimnisschutz kann dabei auch unter Geltung der DS-GVO weiterhin grundsätzlich auf die Rechtsprechung des BGH zum Scoring-Algorithmus der Schutzgemeinschaft für allgemeine Kreditsicherung („Schufa“) verwiesen werden.[144]

Mit seinem Grundsatzurteil vom 28.1.2014 hat der BGH den Umfang des Auskunftsanspruchs aus § 34 Abs. 4 BDSG a.F. konkretisiert. Den Hintergrund der Entscheidung bilden die durch den Gesetzgeber im Jahr 2009 in § 28b BDSG a.F. detailliert geregelten Zulässigkeitsvoraussetzungen für das Scoring. Flankiert wurden diese Regelungen durch entsprechende Auskunftsansprüche in § 34 Abs. 2, Abs. 4 BDSG a.F. Dadurch sollten ausweislich der Gesetzesbegründung die Rechte der Betroffenen gestärkt werden.[145]

Gegenstand des Rechtsstreits war insbesondere § 34 Abs. 4 S. 1 Nr. 4 BDSG a.F. Danach hat die Auskunftei einzelfallbezogen und nachvollziehbar zu erläutern, wie die im Wege des Scorings ermittelten Wahrscheinlichkeitswerte zustande gekommen sind. Weitgehend Einigkeit herrscht darüber, dass die Vorschrift keine Offenlegung der sogenannten Score-Formel, also der abstrakten Methode der Score-Wertberechnung, verlangt. Umstritten ist allerdings, ob ein Anspruch auf Auskunft über die Gewichtung[146] der in die Wahrscheinlichkeitsberechnung eingeflossenen Faktoren und die Bildung von Vergleichsgruppen[147] besteht.[148] Der BGH verneint dies mit der Begründung, dass der Gesetzgeber bei der

---

142 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October, p. 14 („Complexity is no excuse for failing to provide information to the data subject“).

143 *Paal/Hennemann*, in: Paal/Pauly, 2. Aufl. 2018, Art. 13 DSGVO Rn. 31; zum bisherigen Recht BGH MMR 2014, 489; siehe auch *Peter Bräutigam/Florian Schmidt-Wudy*, CR 2015, 56 (61).

144 *BGH*, NJW 2014, 1235: Gegen das Urteil des BGH ist eine Verfassungsbeschwerde unter dem Az. 1 BvR 756/14 beim BVerfG anhängig; s. auch *Thilo Weichert*, Scoring in Zeiten von Big Data, ZRP 2014, 168; zu den künftigen Vorgaben nach der DSGVO *Taeger*, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, 72; s. auch *Flemming Moos/Tobias Rothkegel*, Nutzung von Scoring-Diensten im Online-Versandhandel: Scoring-Verfahren im Spannungsfeld von BDSG, AGG und DS-GVO, ZD 2016, 561; *Rainer Metz*, Scoring: New Legislation in Germany (2012) 35 Journal of Consumer Policy, 297.

145 BT-Drs. 16/10529, 9.

146 Bejahend *Simitis/Dix*, § 34 BDSG Rn. 33, vgl. auch *Rainer Metz*, VuR 2009, 403 (406).

147 So etwa *Schmidt-Wudy*, § 34 BDSG Rn. 71.

Neufassung von § 34 Abs. 4 BDSG zwar einerseits die Transparenz bei Scoring-Verfahren erhöhen, zugleich aber die Geschäftsgeheimnisse der Auskunfteien schützen wollte.[149] Zu den nach dem gesetzgeberischen Willen geschützten Geschäftsgeheimnissen gehören nach Ansicht des BGH auch die in die Score-Formel eingeflossenen allgemeinen Rechengrößen, insbesondere die herangezogenen statistischen Werte und die Gewichtung der einzelnen Berechnungselemente.[150] Zur Begründung verweist der BGH u.a. darauf, dass ein Vorschlag des Bundesrates[151], auch eine Auskunftspflicht über die Reihenfolge der Gewichtung der Daten in § 34 BDSG aufzunehmen, nicht umgesetzt wurde.[152] Erforderlich ist daher nach Ansicht des BGH lediglich eine Auskunft über die in die Ermittlung des Scores eingeflossenen Datenarten und die personenbezogenen Daten, die konkret in die Score-Berechnung eingeflossen sind.

Ob diese Rechtsprechung auch unter der DS-GVO fortbestehen kann, ist umstritten.[153] Zwar ist anders als in § 34 Abs. 7 iVm § 33 Abs. 2 S. 1 Nr. 7 lit. b BDSG a.F. in den Art. 13 und 14 keine besondere Ausnahme für Geschäfts- und Betriebsgeheimnisse niedergelegt.[154] Eine Begrenzung der Informationspflicht könnte jedoch auf den Verhältnismäßigkeitsgrundsatz gestützt werden, der als allgemeiner Rechtsgrundsatz auch im Unionsrecht anerkannt ist.[155]

2.1.2.2. AUSKUNFTSRECHTE

Gemäß Art. 15 Abs. 1 DS-GVO hat der Betroffene das Recht, von dem Verantwortlichen Auskunft über den Zweck und die Reichweite der Datenverarbeitung zu verlangen. Der Auskunftsanspruch soll es dem Betroffenen insbesondere ermöglichen zu überprüfen, ob die Daten rechtmäßig verarbeitet werden.[156] Im Falle einer automatisierten Entscheidungsfindung gem. Art. 22 Abs. 1 und 4 DS-GVO muss die Auskunft auch „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ enthalten (Art. 15 Abs. 1 lit. h DS-GVO). Die Vorschrift greift die Formulierung aus Art. 13, 14 DS-GVO auf. Ebenso wie dort lässt der Wortlaut der Vorschrift erhebliche Auslegungsspielräume zu.[157]

Ein wesentlicher Unterschied zu den Informationspflichten nach Art. 13, 14 DS-GVO besteht darin, dass das Auskunftsrecht gem. Art. 15 DS-GVO seiner Zielsetzung nach eine bereits erfolgte Datenverarbei-

---

[148] Verneinend *OLG Nürnberg*, ZD 2013, 26 (27); *Oliver Heinemann/Florian Wäßle*, Datenschutzrechtlicher Auskunftsanspruch bei Kreditscoring: Inhalt und Grenzen des Auskunftsanspruchs nach § 34 BDSG, MMR 2010, 600 (602); *Plath/Kamlah*, BDSG § 34 Rn. 43.

[149] *BGH*, NJW 2014, 1235 Rn. 27.

[150] *BGH*, NJW 2014, 1235 Rn. 27.

[151] BT-Drs. 16/10529, 28 f.

[152] *BGH*, NJW 2014, 1235 Rn. 31.

[153] Bejahend etwa Paal/Hennemann, in: Paal/Pauly, 2. Aufl. 2018, Art. 13 Rn. 31; Franck, in: Gola, Art. 13 Rn. 26; Deuster, Automatisierte Entscheidungen nach der Datenschutz-Grundverordnung, PinG 2016, 75 (78); verneinend Alexander Roßnagel/Maxi Nebel/Philipp Richter, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455 (458); BeckOK Datenschutzrecht (Stand: 1.2.2018), Art. 15 Rn. 78.3; zweifelnd Schantz in: Schantz/Wolff, Das neue Datenschutzrecht, Rn. 744; Gerald Spindler, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937 (944).

[154] Am zukünftigen Schutz der Score-Formel zweifelnd daher *Niko Härting*, Datenschutz-Grundverordnung, 2016, Rn. 672.

[155] Vgl. *Axel Metzger*, Extra legem, intra ius: Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, Tübingen 2009, 362 ff.

[156] *Jan Philipp Albrecht/Florian Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 4 Rn. 9.

[157] *Schmidt-Wudy*, BeckOK Datenschutzrecht (Stand: 1.11.2017), Art. 15 DSGVO Rn. 78.

tung betrifft. Anders als bei Art. 13, 14 DS-GVO geht es hier nicht um Aufklärung ex ante, sondern um Transparenz ex post. Damit wäre es grundsätzlich möglich, aus Art. 15 DS-GVO eine Pflicht zur Erklärung der konkreten Entscheidung herzuleiten. Gleichwohl deutet der Wortlaut von Art. 15 DS-GVO, der lediglich eine Aufklärung über die „involvierte Logik" verlangt, eher darauf hin, dass lediglich eine abstrakte Information über die Systemfunktionalität geschuldet ist.[158]

2.1.2.3. ANGEMESSENE SCHUTZMAßNAHMEN

Sehr umstritten ist die Frage, ob eine Pflicht zur Offenlegung von ADM-Prozessen und ein damit korrespondierendes „Recht auf Erläuterung" auf Art. 22 Abs. 3 DS-GVO gestützt werden kann. Der Wortlaut der Vorschrift enthält keinen expliziten Hinweis auf ein derartiges Transparenzgebot, sondern verlangt lediglich, dass der Verantwortliche „angemessene Maßnahmen" trifft zum Schutz der Rechte und Freiheiten, sowie der berechtigten Interessen des Betroffenen. Erwgr. 71 UAbs. 1 S. 4 DS-GVO konkretisiert dies u.a. dahingehend, dass der Betroffene einen Anspruch auf „Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung" hat.

Ein Teil der Literatur leitet aus dieser Formulierung ein Recht auf Erläuterung („right of explanation") für automatisierte Entscheidungen ab.[159] Ob Erwgr. 71 UAbs. 1 S. 4 DS-GVO als Rechtsgrundlage für eine solche Transparenzpflicht herhalten kann, erscheint jedoch zweifelhaft.[160] Dagegen spricht zum einen der Umstand, dass von einem „Anspruch auf Erläuterung [...] der Entscheidung" lediglich in den Erwägungsgründen der DS-GVO, nicht jedoch im Verordnungstext selbst die Rede ist. Die Erwägungsgründe von Richtlinien und Verordnungen entfalten keine bindende Wirkung.[161] Sie sind nicht selbst Rechtsquelle, sondern lediglich Rechtserkenntnisquelle.[162] Gegen die Herleitung eines Rechts auf Erläuterung algorithmenbasierter Entscheidungen spricht ferner die Entstehungsgeschichte von Art. 22 Abs. 3 DS-GVO.[163] Während des Rechtsetzungsverfahrens hatte das Europäische Parlament vorgeschlagen, den Text der Vorschrift um einen ausdrücklichen Hinweis auf ein „right to obtain [...] explanation" zu ergänzen. Der Europäische Rat sprach sich demgegenüber dafür aus, diesen Passus lediglich in die Erwägungsgründe aufzunehmen. In ihrer Endfassung folgt die DS-GVO der Position des Rates. Dies spricht im Ergebnis dafür, dass aus Art. 22 Abs. 3 DS-GVO kein Recht auf Erläuterung hergeleitet werden kann.

2.1.3 DATENSCHUTZ-FOLGENABSCHÄTZUNG UND KONSULTATIONSVERFAHREN

Eine wichtige flankierende Funktion für die Kontrolle von ADM-Prozessen dürfte der Datenschutz-

---

158 So im Ergebnis auch *Wachter, Mittelstadt & Floridi*, (Fn. 9) 83.

159 *Bryce Goodman & Seth Flaxman*, European Union regulations on algorithmic decision-making and a" right to explanation", arXiv preprint arXiv:1606.08813 (2016).

160 Ebenso Wachter, Mittelstadt & Floridi, (Fn. 9) 80 (2017).

161 *Wachter, Mittelstadt & Floridi*, (Fn. 9) 80 (2017); siehe auch *Tadas Klimas & Jurate Vaiciukaite*, The Law of Recitals in European Community Legislation, (2008) 15 ILSA Journal of International & Comparative Law 32.

162 *EuGH*, Urt. v. 13.7.1989, Rs. 215/88 – Casa Fleischhandel/BALM, ECLI:EU:C:1989:331, Rn. 31: „Eine Begründungserwägung einer Verordnung kann zwar dazu beitragen, Aufschluß über die Auslegung einer Rechtsvorschrift zu geben, sie kann jedoch nicht selbst eine solche Vorschrift darstellen."

163 Siehe dazu *Wachter, Mittelstadt & Floridi*, (Fn. 9) 80 (2017).

Folgenabschätzung nach Art. 35 DS-GVO sowie dem in Art. 36 DS-GVO geregelten Konsultationsverfahren zukommen. Die Datenschutz-Folgenabschätzung ist Ausdruck der in Art. 5 Abs. 2 verankerten „Rechenschaftspflicht" (*accountability*). Danach hat der Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO die Einhaltung der DS-GVO nachzuweisen.[164]

Begründet die Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten der Betroffenen, so hat der Verantwortliche vorab eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 1 DS-GVO). Die Datenschutz-Folgenabschätzung soll nach dem Willen des europäischen Gesetzgebers die Funktion eines „Frühwarnsystems" erfüllen und dem Verantwortlichen eine eigenverantwortliche Risikoanalyse ermöglichen.[165] Dadurch soll die Gefahr von Persönlichkeitsverletzungen rechtzeitig erkannt und eingedämmt werden.[166]

Art. 35 Abs. 3 DS-GVO enthält eine nicht abschließende Liste von Regelbeispielen, aus denen sich ergibt, in welchen Konstellationen eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist. Nach Art. 35 Abs. 3 lit. a DS-GVO gehört hierzu unter bestimmten Umständen auch der Einsatz von ADM-Systemen. Dies soll dann der Fall sein, wenn eine systematische und umfassende Bewertung der Persönlichkeit auf der Basis automatisierter Datenverarbeitung erfolgt, die sodann als Grundlage von Entscheidungen mit Rechtswirkungen für den Einzelnen dient oder sich auf ähnliche Weise auf den Einzelnen auswirkt. Erfasst werden damit sowohl das in Art. 4 Nr. 4 DS-GVO definierte Profiling als auch Scoring-Verfahren, also Wahrscheinlichkeitsprognosen über zukünftiges Verhalten natürlicher Personen (z.B. automatisierte Bonitätsprüfungen) sowie Verfahren zur Festsetzung von personalisierten Preisen.[167] Nicht unter Art. 35 Abs. 3 lit. a DS-GVO fällt dagegen personalisierte Online-Werbung und das dafür erforderliche Tracking-Verfahren, da es hier an einer Entscheidung mit „Rechtswirkungen" fehlt.[168] Nach Auffassung der Artikel-29-Datenschutzgruppe erfasst Art. 35 Abs. 3 lit. a DS-GVO nicht nur Fälle, in denen ein Algorithmus die alleinige Entscheidung fällt, sondern – über den Anwendungsbereich von Art. 22 Abs. 1 DS-GVO hinaus – auch solche Konstellationen, in denen der Algorithmus nur vorbereitend zur Entscheidungsunterstützung eingesetzt wird.[169] Zur Begründung wird darauf verwiesen, dass Art. 35 Abs. 3 lit. a DS-GVO lediglich verlangt, dass sich die Bewertung auf eine automatisierte Entscheidung „gründet" (im Englischen: „based on").

Den Mindestinhalt der Datenschutz-Folgenabschätzung regelt Art. 35 Abs. 7 DS-GVO. Erforderlich ist u.a. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, einschließlich etwaiger vom Verantwortlichen verfolgter berechtigter Interessen (Art. 35 Abs. 7 lit. a DS-GVO). Die Dokumentation muss dabei so detailliert sein, dass der Verantwortliche (und gegebe-

---

164 *Nolte/Werkmeister*, in: Gola, Art. 35 DSGVO Rn. 2.

165 *Baumgartner*, in: Ehmann/Selmayr, Art. 35 DSGVO Rn. 2.

166 *Mario Martini/David Nink*, NVWZ-Extra 10/2017, 1 (7).

167 *Baumgartner*, in: Ehmann/Selmayr, Art. 35 DSGVO Rn. 21; siehe auch Article 29 Data Protection Working Party Guidelines on Data Protetion Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01 (4.10.2017), S. 9.

168 *Baumgartner*, in: Ehmann/Selmayr, Art. 35 DSGVO Rn. 21.

169 Article 29 Data Protection Working Party, Guidelines on Automated individual decision making and Profiling for the purposes of Regulation 2016/679, WP 251 (3.10.2017), S. 27.

nenfalls auch die Aufsichtsbehörde) anhand der Dokumentation die mit der Verarbeitung verbundenen Risiken identifizieren und bewerten kann, um geeignete Abhilfemaßnahmen zur Risikoreduzierung treffen zu können.[170] Erforderlich sind nicht nur Angaben zur verarbeiteten Kategorien personenbezogener Daten, sondern auch eine Beschreibung der „verwendeten IT-Systeme".[171] Unklar ist, inwieweit dies auch eine Dokumentation der verwendeten Algorithmen (etwa der Score-Formel) erfordert. Hierfür spricht, dass bei ADM-Prozessen eine Risikobewertung, wie sie Art. 35 Abs. 7 lit. c DS-GVO verlangt, ohne eine Dokumentation der den ADM-Prozessen zugrundeliegenden Algorithmen kaum möglich sein dürfte. Bei selbstlernenden Algorithmen dürfte darüber hinaus auch eine Dokumentation der Trainingsdaten erforderlich sein.

Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, besteht gem. Art. 36 Abs. 1 DS-GVO eine Pflicht zur Konsultation der Aufsichtsbehörde. Im Rahmen der Konsultation muss der Aufsichtsbehörde u.a. die nach Art. 35 DS-GVO erstellte Datenschutz-Folgenabschätzung vorgelegt werden (Art. 36 Abs. 3 lit. e DS-GVO). Darüber hinaus kann die Aufsichtsbehörde im Rahmen des Konsultationsverfahrens weitere Informationen anfordern (Art. 36 Abs. 3 lit. f i.Vm. Art. 58 Abs. 1 lit. a DS-GVO). Die Konsultationspflicht nach Art. 36 DS-GVO begründet zwar keinen Genehmigungsvorbehalt für risikoreiche Verarbeitungsvorgänge.[172] Durch das Konsultationsverfahren erlangt die Aufsichtsbehörde jedoch vorab Kenntnis von risikoträchtigen Datenverarbeitungen und erhält die Möglichkeit gezielt einzugreifen. Das Spektrum der möglichen Maßnahmen reicht von schriftlichen Empfehlungen zur Ausgestaltung der konkreten Verarbeitungen bis hin zu einem Verbot der konkreten Verarbeitungstätigkeit.[173] In der Praxis dürfte die Wirkung des Art. 36 DS-GVO einem „faktischen Genehmigungsvorbehalt" daher durchaus nahekommen.[174]

2.1.4 VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Nach Art. 30 Abs. 1 DS-GVO ist der Verantwortliche verpflichtet, ein umfassendes Verzeichnis der Datenverarbeitungstätigkeiten zu führen.[175] Eine entsprechende Dokumentationspflicht gilt gem. Art. 30 Abs. 2 DS-GVO auch für Auftragsverarbeiter.[176] Das Verzeichnis, das schriftlich oder in elektronischer Form zu führen ist, muss auf Anfrage der Aufsichtsbehörde vorgelegt werden (Art. 30 Abs. 4 DS-GVO). Die Pflicht zur Führung eines Verzeichnisses tritt an die Stelle der bisherigen Meldepflicht (Art. 18, 19 DS-RL), zugleich wird aber die inhaltliche Reichweite der Dokumentationspflichten erweitert. Die Rege-

[170] *Baumgartner*, in: Ehmann/Selmayr, Art. 35 DSGVO Rn. 32.
[171] So explizit *Baumgartner*, in: Ehmann/Selmayr, Art. 35 DSGVO Rn. 32.
[172] *Nolte/Werkmeister*, in: Gola, Art. 36 DSGVO Rn. 14.
[173] *Baumgartner*, in: Ehmann/Selmayr, Art. 36 DSGVO Rn. 1.
[174] So etwa *von dem Bussche*, in: Plath, 2. Aufl. 2016, Art. 36 DSGVO Rn. 2; ebenso *Baumgartner*, in: Ehmann/Selmayr, Art. 36 DSGVO Rn. 1.
[175] Dazu eingehend *Markus Schäffter*, Verfahrensverzeichnis 2.0, 2016.
[176] Einschränkungen der Dokumentationspflicht gelten gem. Art. 30 Abs. 5 DSGVO für Unternehmen und Einrichtung, die weniger als 250 Mitarbeiter beschäftigen.

lung soll eine effektive Datenschutzaufsicht bei gleichzeitiger Entbürokratisierung ermöglichen.[177] Sie ist Ausdruck des in Art. 5 Abs. 2 DS-GVO verankerten Accountability-Grundsatzes.[178]

In dem Verzeichnis sind die wesentlichen Informationen über die Datenverarbeitung (u.a. Zweck, Löschfristen, Empfänger) schriftlich zu dokumentieren. Art. 30 Abs. 1 S. 2 konkretisiert den Mindestinhalt des vom Verantwortlichen zu erstellenden Verzeichnisses.[179] Der Katalog der zu dokumentierenden Umstände weist eine gewisse strukturelle Ähnlichkeit auf mit den Transparenzgeboten aus Art. 13 Abs. 1 und Art. 14 Abs. 1 DS-GVO sowie mit den Auskunftsrechten nach Art. 15 DS-GVO.[180] In das Verzeichnis aufzunehmen sind u.a. Angaben über die „Kategorien personenbezogener Daten", die Gegenstand der Verarbeitung sind. Nicht ausreichend sind dabei ganz pauschale Angaben wie etwa „Kundendaten" oder „Patientendaten".[181] Um der Aufsichtsbehörde im Falle eines Auskunftsersuchens nach Art. 30 Abs. 4 DS-GVO eine effektive Überprüfung zu ermöglichen, sind vielmehr detailliertere Angaben erforderlich. Insbesondere muss aus den Angaben deutlich werden, ob besonders sensible Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO (z.B. ethnische Herkunft, politische Meinung, religiöse Überzeugung) verarbeitet werden.[182] Praktische Schwierigkeiten dürfte dies vor allem beim Einsatz von „Data Mining"-Verfahren bereiten, bei denen Algorithmen große Datenmengen nach Korrelationen und bislang unerkannten Mustern durchsuchen.

2.2 WETTBEWERBSRECHT

Weitere Anforderungen für ADM-Systeme ergeben sich aus dem Kartell- und Lauterkeitsrecht. Für das Lauterkeitsrecht sind die maßgeblichen Vorgaben dem nationalen Recht (UWG) zu entnehmen, auf kartellrechtlicher Seite werden in erster Linie die europäischen Regelungen einschlägig sein.

2.2.1 KARTELLRECHT

Vorgaben des Kartellrechts mit Relevanz für ADM-Systeme betreffen insbesondere den Einsatz von dynamischen Preisalgorithmen.[183] Dabei handelt es sich um Softwareanwendungen die es erlauben, Preisveränderungen auf dem Markt in Echtzeit zu beobachten. Auf diese Weise könne die Preise von Händlern überwacht und Abweichungen von unverbindlichen Preisempfehlungen binnen kürzester Zeit entdeckt werden. Eine solche automatisierte Preisüberwachung (*price monitoring*) ist für sich genommen

[177] *Klug*, in: Gola, Art. 30 DSGVO Rn. 1.
[178] *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 30 DSGVO Rn. 1; *Klug*, in: Gola, Art. 30 DSGVO Rn. 1.
[179] Für Auftragsverarbeiter ergibt sich der Mindestinhalt aus Art. 30 Abs. 2 DSGVO.
[180] *Martini*, in Paal/Pauly, 2. Aufl. 2018, Art. 30 DSGO Rn. 6.
[181] So aber offenbar *Klug*, in: Gola, Art. 30 DSGVO Rn. 6.
[182] In diesem Sinne auch *Martini*, in: Paal/Pauly, 2. Aufl. 2018, Art. 30 DSGO Rn. 10c.
[183] Dazu eingehend *Ariel Ezrachi/Maurice Stucke*, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy, Harvard University Press 2016; *dies.*, Algorithmic Collusion: Problems and Counter-Measures, OECD DAF/COMP/WD(2017)25 (Mai 2017); *OECD*, Algorithms and Collusion: Competition Policy in the Digital Age, 2017; siehe auch *Martin Ebers*, Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten?, NZKart 2016, 554 ff.; siehe ferner Boris Paal/Moritz Hennemann, Big Data as an Asset: Daten und Kartellrecht, ABIDA-Gutachten, 2018, S. 62 f.

nicht unzulässig.[184] Die durch das *price monitoring* gewonnenen Informationen können jedoch für vertikale Preisbindungen genutzt werden. Aus diesem Grund betrachten die Kartellbehörden den Einsatz von *web robots* zur Preisüberwachung mit einiger Skepsis.[185]

Mithilfe von Preisalgorithmen können Unternehmen nicht nur die Verkaufspreise der Händler überwachen, sondern auch die Preise der eigenen Wettbewerber. Dies ermöglicht es, die eigene Preisgestaltung automatisch an die Preise der Wettbewerber anzupassen (*dynamic algorithmic pricing*). Diese Vorgehensweise ist insbesondere im E-Commerce bereits heute weit verbreitet.[186] Kartellrechtlich bedenklich ist das *dynamic algorithmic pricing* dann, wenn es den Tatbestand einer Preisabsprache oder abgestimmten Verhaltensweise (§ 1 GWB; Art. 101 Abs. 1 AEUV) erfüllt. Unbedenklich ist es dagegen, wenn lediglich ein zulässiges stillschweigendes Parallelverhalten (*tacit collusion*) vorliegt.[187]

Ein praktischer Anwendungsfall eines kartellrechtlich unzulässigen *algorithmic pricing* ist der Einsatz von Preisalgorithmen, um eine zuvor getroffene Preisabsprache durchzusetzen. Ein viel zitiertes Beispiel für diese Fallgestaltung ist das in den USA aufgedeckte "Poster-Kartell".[188] Dabei hatten sich mehrere Händler von Postern darüber abgestimmt, zu welchen Preisen sie ihre Waren auf der Online-Plattform Amazon Marketplace anbieten würden. Zur Durchsetzung der Absprache wurde eine speziell zu diesem Zweck von einem der Händler entwickelte Preisanpassungssoftware eingesetzt. Ein anderes Beispiel betrifft den Fall, dass Wettbewerber auf Preisalgorithmen und Datensätze desselben Drittanbieters zurückgreifen. Dies ist insbesondere dann kartellrechtlich bedenklich, wenn die Preisvorschläge der Software auf dem Austausch wettbewerbssensibler Daten beruhen. In diesem Fall könnte die vom EuGH in *E-turas*[189] aufgestellte Vermutung greifen, dass sich die betreffenden Wirtschaftsteilnehmer aufgrund des gemeinsam genutzten IT-Systems an einer abgestimmten Verhaltensweise im Sinne des Art. 101 Abs. 1 AEUV beteiligt haben.[190]

2.2.2 LAUTERKEITSRECHT

Weder im deutschen noch im europäischen Lauterkeitsrecht finden sich bislang explizite Regelungen für ADM-Systeme. Sowohl das UWG als auch die UGP-Richtlinie (2005/29/EG) verfolgen vielmehr einen technikneutralen Ansatz. Gleichwohl lassen sich aus den Vorschriften des Lauterkeitsrechts einige spezifische Vorgaben für algorithmengestützte Geschäftspraktiken herleiten. Die Vorgaben des Lauterkeits-

[184] Näher dazu *Daniel Dohrn & Linda Huck*, Der Algorithmus als „Kartellgehilfe"? – Kartellrechtliche Compliance im Zeitalter der Digitalisierung, DB 2018, 173, 174 ff.

[185] Vgl. *EU-Kommission*, Commission's E-Commerce Sector Inquiry Staff Working Document, SWD(2017), 154 final; *Bundeskartellamt* und *Autorité de la concurrence*, Arbeitspapier Competition Law and Data, Mai 2016, S. 14 f.

[186] Nach einer Studie der EU-Kommission verwendeten im Jahr 2016 ca. 67% der Händler, die regelmäßig die Preise ihrer Händler beobachten, eine automatische Preisanpassungssoftware. In 78% der Fälle wurden die Preise auf Grundlage dieser Informationen manuell oder automatisch angepasst; siehe *EU-Kommission*, Commission's E-Commerce Sector Inquiry Staff Working Document, SWD(2017) 154 final, S. 51; siehe auch *Le Chen*, *Alan Mislove & Christo Wilson*, An Emipircal Analysis of Algorithmic Pricing on Amazon Marketplace, Proceedings of the 25th International Conference on World Wide Web (2016).

[187] *Dohrn/Huck*, DB 2018, 173 (176).

[188] Siehe dazu *Dohrn/Huck*, DB 2018, 173 (176 ff.); siehe auch *Johannes Ylinen*, Digital Pricing und Kartellrecht, NZKart 2018, 19 (20).

[189] *EuGH*, Rs. C-74/14 – Eturas, ECLI:EU:C:2016:42.

[190] Siehe dazu und zu weiteren Konstellationen *Ebers*, NZKart 2016, 554 (555).

rechts betreffen dabei insbesondere die Transparenz von ADM-Systemen und den Schutz vor Irreführungen.

Beispielsweise betonen die im Mai 2016 veröffentlichen Leitlinien der Europäischen Kommission für die Umsetzung und Anwendung der UGP-Richtlinie, dass die Nutzer von Suchmaschinen üblicherweise davon ausgehen, dass es sich bei den ihnen angezeigten Suchergebnissen um „natürliche" oder „organische" Ergebnisse handelt, die auf neutralen Kriterien beruhen.[191] Diese Verbrauchererwartung wird enttäuscht, wenn in der Liste der Suchergebnisse dadurch „gekaufte" Platzierungen manipuliert werden, die darauf beruhen, dass einzelne Unternehmen den Betreiber der Suchmaschine für eine bessere Platzierung in der Ergebnisliste bezahlt haben. Die UGP-Richtlinie verbietet zwar nicht die Aufnahme von bezahlten Suchergebnissen in die Liste, verlangt aber, dass dies gegenüber den Verbrauchern offengelegt wird. Andernfalls liege ein Verstoß gegen das Per-se-Verbot nach Nr. 11 Annex I UGP-Richtlinie vor.[192]

Für Bewertungsplattformen wie etwa Tripadvisor oder Jameda besteht aus lauterkeitsrechtlicher Sicht keine Pflicht zur Verwendung von Filteralgorithmen. In der Praxis werden entsprechende ADM-Systeme gleichwohl häufig eingesetzt, vor allem sog. Profanity-Filter, aber auch komplexe algorithmenbasierte Filtertechniken, die anhand von Textanalysen gefälschte Bewertungen ermitteln.[193] Die Rechtsprechung schafft für den Einsatz derartiger ADM-Systeme bislang günstige Rahmenbedingungen. So führt nach Ansicht des BGH der Einsatz eines automatischen Wortfilters für sich genommen nicht dazu, dass der Betreiber eines Hotelbewertungsportals seine neutrale Rolle verlässt und sich die in das Portal eingestellten Äußerungen zu eigen macht.[194]

2.3 NICHTDISKRIMINIERUNGSRECHT

In der Diskussion um eine Regulierung von ADM-Systemen spielt die Sorge vor der automatisierten Erstellung von Persönlichkeitsprofilen und einer daran anknüpfenden „algorithmischen Diskriminierung" eine zentrale Rolle.[195] Dementsprechend groß ist die Relevanz rechtlicher Diskriminierungsverbote für ADM-Systeme. Aus privatrechtlicher Perspektive gilt es jedoch zunächst daran zu erinnern, dass die Rechtsordnung für private Akteure nach herkömmlicher Auffassung keinen allgemeinen Grundsatz der Gleichbehandlung aufstellt. Gleichbehandlungspflichten sind vielmehr eine begründungsbedürftige Aus-

[191] Commission Guidance, S. 120; ähnliche Transparenzanforderungen formulieren die Leitlinien der Kommission für Vergleichsportale („Comparison tools") und verweisen dabei auf die von einer Multi-Stakeholder-Gruppe im Auftrag der Kommisison erarbeiteten „Key principles for comparison tools".

[192] Commission Guidance, S. 121.

[193] Vgl. *Huayi Li* et al, Analyzing and Detecting Opinion Spam on a Large-Scale Dataset via Temporal and Spatial Patterns, ICWSM 634-637 (2015); siehe dazu auch *Christoph Busch*, Crowdsourcing Consumer Confidence: How to regulate online rating and review systems in the collaborative economy, in: De Franceschi (ed.) European Contract Law and the Digital Single Market, Cambridge.

[194] *BGH*, Urt. v. 19.3.2015, I ZR 94/13, GRUR 2015, 1129 Rn. 35 – Hotelbewertungsportal.

[195] Siehe dazu bereits oben Abschnitt 1.3.1.; siehe auch *Peter Schaar*, Algorithmentransparenz, in: Alexander Dix et al. (Hrsg.), Informationsfreiheit und Informationsrecht Jahrbuch 2015, Berlin 2016, S. 23 (29 ff.).

nahme der Privatautonomie.[196] Die wichtigste spezialgesetzliche Konkretisierung privatrechtlicher Gleichbehandlungspflichten bildet das Allgemeine Gleichbehandlungsgesetz (AGG), das eine Reihe von beschäftigungsrechtlichen (§§ 6-18 AGG) und zivilrechtlichen (§§ 19-21 AGG) Benachteiligungsverboten enthält.[197]

Die Vorschriften des AGG sind technologieneutral konzipiert und erfassen daher grundsätzlich auch ADM-Prozesse.[198] Aus Sicht des AGG macht es keinen Unterschied, ob ein Verstoß gegen das Benachteiligungsverbot bei der Bewerberauswahl (§ 7 Abs. 1 i.V.m. § 6 Abs. 1 S. 2 AGG) durch einen Menschen oder ein automatisiertes E-Recruiting-System erfolgt. Gleichwohl wird derzeit sowohl aus der Politik [199] als auch von Teilen der Wissenschaft[200] die Forderung nach einer Anpassung des AGG bzw. der Einführung eines „digitalen AGG" erhoben.[201] Kritisiert wird unter anderem, dass das AGG aufgrund seines eingeschränkten sachlichen Anwendungsbereichs „zahlreiche spezialisierte Anwendungsfelder softwarebasierter Verfahren" nicht erfasse und daher nur einen eingeschränkten Schutz vor algorithmischer Diskriminierung bieten können.[202] So gelten die Benachteiligungsverbote des AGG vornehmlich für Arbeitsverhältnisse, Bildung und Sozialleistungen sowie für Güter und Dienstleistungen, die der allgemeinen Öffentlichkeit zur Verfügung stehen (§§ 2, 19 AGG). Für Verträge zwischen Privaten außerhalb des Arbeitsrechts gilt das AGG nur bei sog. Massengeschäften und Versicherungen (§ 19 Abs. 1 AGG).

Mögliche Defizite beim Schutz vor algorithmischen Diskriminierungen dürften sich jedoch weniger aus dem eingeschränkten Anwendungsbereich des AGG als vielmehr aus anderen Gründen ergeben. ADM-Systeme werden zumeist in Konstellationen zum Einsatz kommen, die unter den Begriff des „Massengeschäfts" i.S.v. § 19 Abs. 1 Nr. 1 AGG subsumiert werden können. Problematisch ist insoweit, dass der zunehmende Einsatz von ADM-Prozessen zur Generierung von personalisierten Angeboten zu einer Verschiebung des normativen Bezugsrahmens führen könnte (sog. Shifting-Baseline-Syndrom). Der Begriff des Massengeschäfts in § 19 Abs. 1 Nr. 1 AGG bezieht sich nämlich auf solche Schuldverhältnisse, die „typischerweise ohne Ansehen der Person zu vergleichbaren Bedingungen in einer Vielzahl von Fällen zustande kommen". Eine zunehmende Personalisierung von Verträgen könnte mittelfristig dazu führen, dass diese Typik de facto in immer mehr Bereichen verloren geht. Eine solche Veränderung im faktischen

---

196 *Block*, in: BeckOGK (Stand: 1.11.2017), § 1 AGG Rn. 2; eingehend dazu *Michael Grünberger*, Personale Gleichheit, Baden-Baden 2013, der zugleich ein Gegenmodell entwirft, nach welchem das Verhältnis von Grundsatz und Ausnahme umgekehrt wird. Danach ist im Ausgangspunkt jede Ungleichbehandlung rechtfertigungsbedürftig. Wichtigster Rechtfertigungsgrund ist dabei wiederum die Ausübung von Freiheitsrechten.

197 Hinzu kommen Diskriminierungsverbote, die an wirtschaftliche Machtstellung anknüpfen, etwa nach §§ 19 ff. GWB und § 826 BGB, vgl. *Wagner*, in: MüKoBGB, 7. Aufl. 2017, § 826 Rn. 200 ff.

198 Vgl. *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1021).

199 Maas fordert digitales Antidiskriminierung-Gesetz, FAZ, 3.7.2017, http://www.faz.net/aktuell/wirtschaft/unternehmen/maas-fordert-digitales-antidiskriminierung-gesetz-15088974.html; Auch der Entwurf eines Koalitionsvertrages zwischen CDU, CSU und SPD aus dem Februar 2018 geht darauf in Zeile 2097 f. ein: „Diskriminierungsverbote der analogen Welt müssen auch in der digitalen Welt der Algorithmen gelten."

200 *Mario Martini*, JZ 2017, 1017 (1021), der de lege ferenda eine Ergänzung des Katalogs der Anwendungsfälle des § 2 Abs. 1 AGG um eine Nr. 9 für Ungleichbehandlung zwischen Privaten erwägt, die auf einer algorithmenbasierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen.

201 Zum Stand der Diskussion siehe auch *Hubertus Gersdorf*, Brauchen wir ein digitales AGG?, NJW-Aktuell 31/2017, S. 3.

202 *Mario Martini*, JZ 2017, 1017 (1021), der de lege ferenda eine Ergänzung des Katalogs der Anwendungsfälle des § 2 Abs. 1 AGG um eine Nr. 9 für Ungleichbehandlung zwischen Privaten erwägt, die auf einer algorithmenbasierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen.

Marktverhalten darf jedoch im Ergebnis nicht zur Konsequenz haben, dass der durch das AGG gewährte Schutz ausgehöhlt wird. Der Begriff des „Massengeschäfts", durch welchen der Anwendungsbereich des zivilrechtlichen Diskriminierungsschutzes bestimmt wird, muss normativ und nicht durch eine Bezugnahme auf faktische Marktgegebenheiten festgelegt werden.

Praktisch bedeutsame Defizite im Schutz vor algorithmischen Diskriminierungen durch das AGG dürften sich darüber hinaus in erster Linie dadurch ergeben, dass der Einsatz von ADM-Systemen und die damit einhergehende Gefahr von Diskriminierungen in vielen Fällen für den Einzelnen nicht erkennbar ist. Hierbei handelt es sich in erster Linie um Nachweis- und Enforcement-Probleme, die zwar auch bei „analogen" Diskriminierungen auftreten, durch den massenweisen Einsatz von „unsichtbaren" ADM-Systemen an Bedeutung zunehmen dürften. Erschwert wird die Aufdeckung von Diskriminierungsfällen dadurch, dass eine algorithmische Diskriminierung nicht notwendigerweise an die im AGG genannten Diskriminierungsmerkmale anknüpfen muss. Vielmehr werden bei ADM-Prozessen Gruppenzugehörigkeiten aufgrund eines komplexen Merkmalsmix definiert.[203] Zwar erfasst das AGG auch mittelbare Diskriminierungen (§ 3 Abs. 2 AGG). Bei komplexen ADM-Prozessen dürfte die Zahl der berücksichtigten „neutralen" Merkmale jedoch schnell einen Umfang erreichen, der einen Nachweis der Diskriminierung erschwert.

2.4 SEKTORSPEZIFISCHE REGELUNGEN

Für den Einsatz von ADM-Systemen sind darüber hinaus sektorspezifische Regelungen zu beachten, die besonderen Gefährdungslagen Rechnung tragen. Beispielhaft sollen hier die Vorschriften im Bereich der Medizinprodukte und Finanzmarktregelungen für den Hochfrequenzhandel genannt werden.

2.4.1 MEDIZINISCHE ALGORITHMEN

Medizinische Entscheidungsunterstützungssysteme (*Decision Support Systems*), wie sie beispielsweise zur Interpretation radiologischer Bilddaten oder zur Beurteilung von Hautläsionen eingesetzt werden, unterliegen den Vorgaben des Medizinprodukterechts, sofern sie als Medizinprodukte i.S.d. § 13 Abs. 1 Medizinproduktegesetz (MPG) i.V.m. Anhang IV der Richtlinie 93/42/EWG klassifiziert werden.[204] Wie der EuGH jüngst entschieden hat, gilt dies etwa für eine Medical App, die es ermöglicht, Patientendaten zu nutzen, um Kontraindikationen, Wechselwirkungen zwischen Arzneimitteln und Überdosierungen festzustellen.[205] Eine Orientierungshilfe für die Beantwortung der Frage, unter welchen Voraussetzungen ein medizinisches *Decision Support System* als Medizinprodukt zu klassifizieren ist, bieten (rechtlich unverbindliche) Leitlinien der EU-Kommission.[206] Weiter konkretisiert wird der Regulierungsrahmen für den

---

[203] Vgl. Thilo Weichert, Big Data im Gesundheitsbereich, ABIDA-Gutachten, 2018, S. 101.

[204] Vgl. *Ulrich Gassner*, Software als Medizinprodukt – zwischen Regulierung und Selbstregulierung, MPR 2016, 109; siehe auch *Roderic Ortner / Felix Daubenbüchel*, Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918; *Jann Ferlemann*, Gesundheitsentscheidungen durch Algorithmen – rechtliche Rahmenbedingungen der Digitalisierung des Gesundheitswesens, NZS 2018, 56.

[205] *EuGH*, Urt. v. 7.12.2017, Rs. C-329/16 – Syndicat national de l'industrie des technologies médicales, ECLI:EU:C:2017:947, EuZW 2018, 166.

[206] MEDDEV 2.1/6 Qualification and Classification of stand alone software (Juni 2016); Manual on Borderline and Classification in the Community Regulatory Fremwork for Medical Version 1.18 (Dezember 2017).

Einsatz von medizinischen ADM-Systemen durch die ab Mai 2020 geltende EU-Medizinprodukte-Verordnung, die eine explizite Klassifizierungsregel für medizinische Stand-Alone-Softwares enthält.[207]

2.4.2 HOCHFREQUENZHANDEL

Detaillierte sektorspezifische Regelungen für den Einsatz von ADM-Systemen bestehen auch für den algorithmischen Handel (Art. 80 Abs. 2 S. 1 WpHG) und den Hochfrequenzhandel (§ 1 Abs. 1a S. 2 Nr. 4 lit. d KWG). Der algorithmische Handel macht ein immer wichtiger werdendes Segment des Börsenhandels aus, bei dem ADM-Systeme die Auftragsparameter (z.b. Kauf- und Verkaufszeitpunkt, Ordergröße) für Orders automatisch festlegen und Orders ohne menschliche Intervention platzieren. Der Begriff des Hochfrequenzhandels bezeichnet eine Unterkategorie des algorithmischen Handels, die sich durch eine hohe Anzahl von Auftragseingaben, -änderungen oder -löschungen innerhalb von Mikrosekunden auszeichnet.

Durch das im Jahr 2013 in Kraft getretene Hochfrequenzhandelsgesetz hat der Gesetzgeber Regelungen erlassen, die dazu dienen, systemischen Risiken des algorithmengesteuerten Wertpapierhandels zu begegnen, insbesondere der Gefahr von Kaskadeneffekten und möglichen Börsencrashs.[208] Die Tätigkeit von Hochfrequenzhändlern unterliegt danach einer Erlaubnispflicht nach dem KWG. Mit der Umsetzung der Zweiten Finanzmarktrichtlinie (MiFID II) wurde zum 3.1.2018 zusätzlich eine neue Anzeigepflicht für das Betreiben von algorithmischem Handel (Art. 80 Abs. 2 S. 1 WpHG) und den Betrieb eines direkten elektronischen Marktzugangs eingeführt (Art. 2 Abs. 30 WpHG).

Darüber hinaus sieht Art. 80 Abs. 2 WpHG eine Reihe von Organisationspflichten für Wertpapierdienstleistungsunternehmen vor, die algorithmischen Handel betreiben. So müssen angemessene System- und Risikokontrollen eingeführten werden und Notfallvorkehrungen getroffenen werden, um auf unvorhergesehene Störungen in den Handelssystemen reagieren zu können. Art. 80 Abs. 3 WpHG ergänzt diese Regelungen um detaillierte Dokumentationspflichten. Danach ist zum einen eine Dokumentation über die System- und Risikokontrollen und die getroffenen Notfallvorkehrungen anzufertigen. Sofern hochfrequente algorithmische Handelstechniken eingesetzt werden, besteht auch eine Dokumentationspflicht für die einzelnen Aufträge bzw. Auftragsstornierungen. Auf Verlangen sind diese Aufzeichnungen der BaFin herauszugeben. Nach § 16 Abs. 2 Nr. 3 BörsG besteht ferner eine Pflicht, algorithmisch generierte Aufträge zu kennzeichnen und den dabei verwendeten Algorithmus kenntlich zu machen.[209]

---

[207] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5.4.2017 über Medizinprodukte, ABl.EU L 117/1; siehe auch *Angela Graf*, Revision des europäischen Rechtsrahmens für Medizinprodukte: Einfluss auf die Klassifizierung von Medizinprodukten, PharmR 2017, 57.

[208] Siehe dazu *Ekkehard M. Jaskulla*, Das deutsche Hochfrequenzhandelsgesetz – eine Herausforderung für Handelsteilnehmer und Multilaterale Handelssysteme (MTF), BKR 2013, 221; *Jochen Kindermann / Benedikt Coridaß*, Der rechtliche Rahmen des algorithmischen Handels inklusive des Hochfrequenzhandels, ZBB, 178.

[209] Das Hessische Ministerium für Wirtschaft, Verkehr und Landesentwicklung hat als Börsenaufsichtsbehörde für die Frankfurter Wertpapierbörse Hinweise zur Kennzeichnung von Handelsalgorithmen gem. § 16 Abs. 2 Nr. 3 BörsG, § 33 Abs. 1 a WpHG, § 72 a Börsenordnung für die Frankfurter Wertpapierbörse, § 17a Börsenordnung für die Eurex Deutschland und die Eurex Zürich veröffentlicht (Stand: 22.9.2014); Danach ist für jeden Handelsalgorithmus ein eindeutiger numerischer Kennzeichnungschlüssel zu verwenden.

Ähnlich wie in § 22 DS-GVO unterscheiden auch die Vorschriften über den algorithmischen Handel zwischen ADM-Prozessen, die ohne eine menschliche Intervention ablaufen, und solchen, die eine menschliche Entscheidung lediglich unterstützen („human in the loop"). Nach den Erläuterungen[210] der BaFin zum Hochfrequenzhandelsgesetz gilt die Erlaubnispflicht demnach nicht für solche Algorithmen, die nur dazu dienen, den Händler auf das Vorliegen einer bestimmten Situation aufmerksam zu machen, sofern der Händler anschließend noch eigenständig eine Entscheidung treffen muss. Als Beispiel nennt die BaFin eine Chartsoftware, die so programmiert ist, dass sie immer dann einen akustischen oder visuellen Hinweis gibt, wenn der Kurs eines Finanzinstruments einen gleitenden Kursdurchschnitt schneidet ohne dabei automatisch eine weitere Entscheidung über Erteilung, Änderung oder Stornierung eines Auftrags zu treffen. Diese Differenzierung ist problematisch, da es durchaus naheliegend sein dürfte, dass insbesondere risikoaverse Menschen sich im Zweifel auf die Empfehlung des Algorithmus verlassen.

2.5 RECHTSDURCHSETZUNG BEI ADM-PROZESSEN

Algorithemenbasierte Entscheidungsprozesse stellen nicht nur das materielle Recht vor neue Herausforderungen, auch die Durchsetzung der materiellrechtlichen Vorgaben kann bei ADM-Systemen auf besondere Schwierigkeiten stoßen. Mögliche Durchsetzungsdefizite lassen sich exemplarisch am Beispiel der datenschutzrechtlichen Anforderungen für ADM-Systeme veranschaulichen.

2.5.1 INDIVIDUELLE RECHTSDURCHSETZUNG

Art. 77 DS-GVO bestimmt, dass sich betroffene Personen an die zuständige Aufsichtsbehörde wenden und geltend machen können, dass eine Datenverarbeitung gegen die DS-GVO verstößt. Das Beschwerderecht begründet jedoch keinen Anspruch auf Erlass einer konkreten Maßnahme, sondern lediglich darauf, dass die Aufsichtsbehörde den Fall nach pflichtgemäßem Ermessen prüft.[211] Zur Absicherung dieses Beschwerderechts gewährt Art. 78 Abs. 2 DS-GVO dem Betroffenen ein Recht auf einen gerichtlichen Rechtsbehelf für den Fall, dass sich die Behörde nicht mit der Beschwerde befasst, oder nicht binnen drei Monaten über den Stand oder das Ergebnis der Beschwerde unterrichtet. Als Ergänzung zur Möglichkeit einer Beschwerde bei den Aufsichtsbehörden und dem effektiven Rechtsschutz gegenüber der zuständigen Behörde bestimmt Art. 79 Abs. 1 DS-GVO, dass dem Betroffenen auch ein wirksamer gerichtlicher Rechtsbehelf gegen den Verantwortlichen oder den Auftragsverarbeiter zustehen muss.[212] Artikel 82 DS-GVO gewährt der betroffenen Personen einen Schadensersatzanspruch bei Datenschutzverstößen.

Auf den ersten Blick scheint das Instrumentarium des datenschutzrechtlichen Individualrechtsschutzes

[210] *BaFin*, Häufig gestellte Fragen (FAQs) zum Hochfrequenzhandelsgesetz (Stand: 28.2.2014), Nr. 22.
[211] *Pötters/Werkmeister*, in: Gola, Art. 77 DSGVO, Rn. 6; siehe auch Erwgr. 141 DSGVO.
[212] Ergänzt wird die Regelung durch Art. 79 Abs. 2 DSGVO, der bestimmt, dass die betroffene Person die Wahl hat, ob sie die Klage gegen den Verantwortlichen oder den Auftragsverarbeiter in dem Mitgliedstaaten dessen Niederlassung erhebt oder in ihrem Aufenthaltsstaat.

durchaus eindrucksvoll. Die bisherigen Erfahrungen im Bereich der individuellen Durchsetzung von Datenschutzvorschriften geben jedoch eher Anlass zur Skepsis. Bislang stößt die Effektivität des datenschutzrechtlichen Individualrechtsschutzes in der Praxis immer wieder an Grenzen. Dafür gibt es vielfältige Gründe, die nicht nur ADM-Prozesse betreffen, sondern auch für andere Konstellationen gelten.[213] Häufig scheitert die Rechtsdurchsetzung bereits daran, dass dem Einzelnen der Verstoß gegen Datenschutzrecht gar nicht bekannt ist. Dies gilt insbesondere in Fällen, in denen der Verantwortliche entgegen Art. 13, 14 DS-GVO den Betroffenen nicht oder nicht ausreichend über die Datenverarbeitung informiert hat. Ist dem Betroffenen der Datenschutzverstoß bekannt, so scheitert die Geltendmachung individueller Rechtsbehelfe nicht selten daran, dass aus Sicht des Einzelnen die Kosten einer gerichtlichen Rechtsdurchsetzung außer Verhältnis zu der häufig als gering empfundenen Rechtsbeeinträchtigung stehen („rationalen Desinteresse" oder „rationale Apathie").[214] Der tatsächliche Befund ist damit bei „persönlichkeitsrechtlichen Streuschäden"[215] ähnlich wie bei wirtschaftlichen Streuschäden.[216] Möglicherweise ist die rationale Apathie der Betroffenen bei Datenschutzverstößen sogar noch ausgeprägter, da diese häufig keine unmittelbar spürbaren Auswirkungen auf den Einzelnen haben.[217] Ein verstärkender Faktor könnte dabei das sog. *privacy paradox* sein. Der Begriff bezeichnet das in empirischen Untersuchungen zu beobachtende Auseinanderklaffen zwischen der abstrakten Wertschätzung der Nutzer für Datenschutz und ihrem konkreten Verhalten.[218] In prozessualer Hinsicht wird die Reichweite des Individualrechtsschutzes dadurch eingeschränkt, dass im Erfolgsfall das erstrittene Urteil nur *inter partes* wirkt und keine rechtliche Bindungswirkung gegenüber Dritten entfaltet.[219] In Betracht kommt allenfalls eine faktische Breitenwirkung.

Eine weitere Schwäche der Durchsetzung datenschutzrechtlicher Vorschriften im Wege des *private enforcement* folgt daraus, dass auf Geldersatz gerichtete Schadensersatzansprüche des Betroffenen in der Vergangenheit häufig daran scheiterten, dass die Rechtsprechung insoweit hohe Hürden aufstellt und eine Geldentschädigung bei Persönlichkeitsrechtsverletzungen nur gewährt, wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht in anderer Weise befriedigend ausgeglichen werden kann.[220] Mit Blick auf den *effet utile* der DS-GVO wird sich diese Einschränkung des An-

---

[213] Vgl. *Franziska Ritter/ Simon Schwichtenberg*, Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizites – neuer Weg, neue Chance, VuR 2016, 95, 96.

[214] Vgl. *Cseres* in: De Geest, Encyclopedia of Law and Economics, 2012, S. 192; siehe auch BT-Drs. 18/4631, S. 11 f.

[215] So treffend *Rupprecht Podszun/Michael de Toma*, Die Durchsetzung des Datenschutzes durch Verbraucherrecht, Lauterkeitsrecht und Kartellrecht, NJW 2016, 2987, 2989.

[216] Zu Durchsetzungsdefiziten bei Streuschäden vgl. *Gerhard Wagner*, Neue Perspektiven im Schadensersatzrecht, Verhandlungen des 66. DJT, Bd. 1, 2006, S. A 107 ff.; siehe auch die Nachweise bei *Brönneke* in: Schulte-Nölke/BMJV, Neue Wege zur Durchsetzung des Verbraucherrechts, 2017, S. 127, 135 ff.

[217] Vgl. *Gerald Spindler*, Verbandsklagen und Datenschutz – das neue Verbandsklagerecht: Neuregelungen und Probleme, ZD 2016, 114 (115).

[218] Vgl. *Susan Athey*, *Christian Catalini & Catherine Tucker*, The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, NBER Working Paper No. 23488, 2017, http://www.nber.org/papers/w23488; siehe auch *Jürgen Kühling & Mario Martini*: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448 (450).

[219] Franziska Ritter/Simon Schwichtenberg, VuR 2016, 95, 96.

[220] Grundlegend *BGH*, Urt. v. 14.2.1958, I ZR 151/56, BGHZ 26, 349; *BVerfG*, Urt. v. 14.2.1973, 1 BvR 112/65, NJW 1973, 1221; *BGH*, Urt. v. 15.11.1994, VI ZR 56/94, NJW 1995, 861; *BGH*, Urt. v. 5.12.1995, VI ZR 332/94, NJW 1996, 984; *BGH*, Urt. v. 5.10.2004, VI ZR 255/03, NJW 2005, 215; *BAG*, Urt. v. 19.2.2015, 8 AZR 1011/13, ZD 2015, 380; *Gola/Piltz*, in: Gola, Art. 82 DSGVO Rn. 12.

spruchs auf Geldentschädigung für Art. 82 DS-GVO möglicherweise nicht mehr aufrechterhalten lassen.[221]

In Bezug auf ADM-Prozesse dürften die hier beschriebenen Schwächen des datenschutzrechtlichen Individualrechtsschutzes besonders zum Tragen kommen. So wird gerade bei algorithmengestützten Prozessen die Kenntnis des Betroffenen von möglichen Datenschutzverstößen daran scheitern, dass er sich einer „black box" gegenübersieht. Selbst in Fällen, in denen der Einzelne einen Datenschutzverstoß vermutet, ist die Informationsgewinnung (gestützt etwa auf das Auskunftsrecht nach Art. 15 DS-GVO) hier besonders mühsam und erfordert technische Expertise, über die der Betroffene in vielen Fällen nicht verfügen wird.[222]

2.5.2 KOLLEKTIVE RECHTSDURCHSETZUNG

Die individuellen Rechtsbehelfe der Art. 77-79 DS-GVO werden ergänzt durch ein Verbandsbeschwerde- und ein Verbandsklagerecht (Art. 80 DS-GVO). Dadurch soll auf das immer wieder beklagte Vollzugsdefizit bei der Durchsetzung datenschutzrechtlicher Vorgaben reagiert werden.[223] Nach Art. 80 Abs. 1 DS-GVO können die Betroffenen etwa einen Verbraucherschutzverband damit beauftragen, ihre Rechte aus Art. 77 ff. DS-GVO im fremden Namen geltend zu machen. Auch mit der Geltendmachung von Schadensersatzansprüchen nach Art. 82 DS-GVO kann der Betroffene einen Verband beauftragen. Einen entsprechenden Anknüpfungspunkt bietet das Zivilprozessrecht in § 79 Abs. 2 Nr. 3 ZPO. Die Anwendung dieser Vorschrift hat sich in der Praxis jedoch als umständlich und wenig praktikabel erwiesen.[224]

Von größerer praktischer Relevanz dürfte das in Art. 80 Abs. 2 DS-GVO geregelte Recht der Verbände sein, im eigenen Namen die in Art. 77-79 DS-GVO geregelten Rechte geltend zu machen.[225] Der deutsche Gesetzgeber hat ein entsprechendes datenschutzrechtliches Verbandsklagerecht der Verbraucherverbände bereits im Februar 2016 durch eine Änderung des § 2 UKlaG eingeführt.[226] In seiner derzeitigen Fassung gilt dieses Verbandsklagerecht allerdings nicht bei allen Datenschutzverstößen, sondern nur bei Verletzung bestimmter Regeln des Datenschutzrechts (vgl. § 2 Abs. 2 S. 1 Nr. 11 UKlaG).[227] Darüber

---

[221] *Gola/Piltz*, in: Gola, Art. 82 DSGVO Rn. 13; siehe auch Erwgr. 141 S. 6 DSGVO, der einen „vollständigen und wirksamen Schadensersatz" verlangt.

[222] Ebenso *Gerald Spindler*, Verbandsklagen und Datenschutz – das neue Verbandsklagerecht: Neuregelungen und Probleme, ZD 2016, 114 (115).

[223] *Karg*, in: BeckOK Datenschutzrecht (Stand: 1.5.2017), Art. 80 DSGVO Rn. 1.

[224] Siehe etwa die Kritik an § 79 ZPO in der Stellungnahme des VZBV zum Diskussionsentwurf eines Gesetzes zur Einführung der Musterfeststellungsklage vom 27. Juli 2017 (29.9.2017), S. 7.

[225] Bei Art. 80 Abs. 2 DSGVO handelt es sich im Unterschied zu Art. 80 Abs. 1 DSGVO um eine Öffnungsklausel, d.h. das eigenständige Verbandsklagerecht bzw. -beschwerderecht besteht nur dann, wenn dies im Recht des jeweiligen Mitgliedstaates vorgesehen ist. Schadensersatzansprüche nach Art. 82 DSGVO können von den Verbänden nicht ohne einen konkreten Auftrag einer betroffenen Person geltend gemacht werden, vgl. *Werkmeister*, in: Gola, Art. 80 DSGVO Rn. 10.

[226] Vgl. *Gerald Spindler*, Verbandsklagen und Datenschutz – das neue Verbandsklagerecht: Neuregelungen und Probleme, ZD 2016, 114; *Axel Halfmeier*, Die neue Datenschutzverbandsklage, NJW 2016, 1126.

[227] Aus diesem Grund dürfte § 2 UKlaG in seiner derzeitigen Fassung die Vorgabe aus Art. 80 Abs. 1 DSGVO wohl nur unzureichend umsetzen, vgl. *Werkmeister*, in: Gola, Art. 80 DSGVO Rn. 18.

hinaus können Verbände unzulässige Datenschutzbestimmungen in AGB nach § 1 UKlaG angreifen.[228] Verstöße gegen das Datenschutzrecht können damit inzident im Rahmen der Inhaltskontrolle nach § 307 geltend gemacht werden.[229] Hinzu kommt die Möglichkeit einer Durchsetzung datenschutzrechtlicher Vorschriften über das UWG, insbesondere über die Scharniervorschrift des § 3a UWG.[230]

Bei ADM-Systemen ergeben sich spezifische Probleme, die eine kollektive Rechtsdurchsetzung durch Verbraucherverbände beeinträchtigt. Insbesondere die Möglichkeiten zur Personalisierung von Werbebotschaften, Angeboten und Preisen erschwert den klagebefugten Verbänden die Überwachung des Marktverhaltens. Zugespitzt formuliert: Erhält jeder Verbraucher eine andere Werbebotschaft, wird es ungleich schwieriger Datenschutzverstöße oder Fälle irreführender Werbung aufzuspüren. Auch die Verwendung der ADM-Prozesse für die Berechnung dynamischer und personalisierter Preise, die ebenfalls in naher Zukunft weiter an Bedeutung gewinnen dürfte, erschwert eine Marktkontrolle. Mit zunehmender Komplexität derartiger Systeme dürfte es für die Verbraucherverbände immer schwieriger werden, algorithmenbasierte Entscheidungen zu überprüfen. Erschwerend kommt hinzu, dass sich eine wirksame Überprüfung von ADM-Prozessen nicht auf die Prüfung des Programmcodes beschränken kann. Lernfähige Softwareanwendungen entwickeln ihre Analysefähigkeiten anhand von umfangreichen Trainingsdaten und sind in der Lage die gewonnenen Erkenntnisse durch Lerntransfer auf unbekannte Daten zu übertragen. Die Überprüfung lernfähiger Systeme erfordert daher möglicherweise auch den Zugriff auf die Trainingsdaten. Hinzu kommen schließlich weitere Hürden bei der gerichtlichen Geltendmachung, da die relevanten Algorithmen in aller Regel als Geschäftsgeheimnisse geschützt sein dürften, wie die Rechtsprechung des BGH zum Schufa-Algorithmus[231] oder die obergerichtliche Rechtsprechung zu den Rankingalgorithmen von der Bewertungsplattform „Yelp“[232] zeigt.

2.5.3 BEHÖRDLICHE RECHTSDURCHSETZUNG

Die behördliche Rechtsdurchsetzung des Datenschutzrechts durch die zuständigen Aufsichtsbehörden bildet die dritte Säule des Datenschutz-Enforcement. Die Behörden üben ihre Kontrollbefugnisse anlass- und verdachtslos aus und verfügen über ein breites Spektrum an Handlungsmöglichkeiten, das von Auskunftsrechten über Warnungen und Anordnungen bis zur Verhängung hoher Bußgelder reicht. Insbesondere der durch die DS-GVO erheblich erweiterte Bußgeldrahmen macht die behördliche Rechtsdurchsetzung jedenfalls auf dem Papier zum schärfsten Schwert im Vergleich zu den anderen Modalitäten der Rechtsdurchsetzung. Angesichts der Intransparenz von ADM-Systemen dürfte den behördlichen Untersuchungsbefugnissen, insbesondere den Auskunftsansprüchen nach Art. 58 Abs. 1 lit. e DS-GVO, eine zentrale Bedeutung für ein effektives Enforcement zukommen. Praktisch bedeutet der Auskunftsan-

[228] *LG Berlin*, Urt. v. 19.11.2013, 15 O 402/12, MMR 2014, 563; *OLG Koblenz*, Urt. v. 26.3.2014, 9 U 1116/13, ZD 2014, 524.
[229] *Werkmeister*, in: Gola, Art. 80 DSGVO Rn. 12.
[230] Dazu näher *Rupprecht Podszun/Michael de Toma*, NJW 2016, 2987 (2989 ff.); siehe auch *Markus Robak*, Neue Abmahnrisiken im Datenschutzrecht, GRUR-Prax 2016, 139.
[231] *BGH*, Urt. v. 28.1.2014, VI ZR 156/13, NJW 2014, 1235.
[232] *KG*, Urt. v. 10.12.2015, 10 U 26/15, MMR 2016, 352; *OLG Hamburg*, Urt. v. 10.11.2015, 7 U 18/15, MMR 2016, 355.

spruch, dass die Aufsichtsbehörde Einsicht nehmen kann in alle relevanten Unterlagen und Verzeichnisse, auch wenn diese Geschäftsgeheimnisse enthalten.[233] Damit ist es der Behörde grundsätzlich möglich, die „*black box*" des ADM-Systems zu öffnen. Darin liegt ein wesentlicher Unterschied zu den Möglichkeiten der individuellen und kollektiven Rechtsdurchsetzung. Inwieweit die Aufsichtsbehörden diese Möglichkeiten auch wahrnehmen können, hängt jedoch von deren finanzieller und personeller Ausstattung ab. Eine flankierende Rolle bei der behördlichen Durchsetzung datenschutzrechtlichen Anforderungen an ADM-Systeme könnte schließlich das Kartellrecht spielen.[234] Insbesondere das derzeit gegen Facebook geführte Verfahren des Bundeskartellamts[235] hat den Blick darauf gelenkt, dass Datenschutzverstöße auch kartellrechtlich relevant sein können. Aufgrund seiner großen juristischen und ökonomischen Kompetenz sowie seiner politischen Unabhängigkeit könnte das Bundeskartellamt bei der Ausgestaltung eines künftigen Durchsetzungsregimes für rechtliche Anforderungen an ADM-Systeme eine wichtige Rolle übernehmen.[236]

[233] *Eichler*, in: BeckOK DatenschutzR, Art. 58 DSGVO Rn. 13; *Selmayr*, in: Ehmann/Selmayr, Art. 58 DSGVO Rn. 16.

[234] Siehe dazu *Rupprecht Podszun/Michael de Toma*, Die Durchsetzung des Datenschutzes durch Verbraucherrecht, Lauterkeitsreht und Kartellrecht, NJW 2016, 2987 (2992).

[235] Siehe dazu die Pressemitteilung des BKartA v. 19.12.2017, „Vorläufige Einschätzung im Facebook-Verfahren: Das Sammeln und Verwerten von Daten aus Drittquellen außerhalb der Facebook Website ist missbräuchlich", http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Pressemitteilungen/2017/19_12_2017_Facebook.pdf?__blob=publicationFile&v=3.

[236] Kritisch dazu *Torsten Körber*, Das Bundeskartellamt auf dem Weg zur Digitalagentur?, WuW 2018, 173.

2.6 ZUSAMMENFASSUNG

Ein besonderes „Algorithmenrecht“ kennt das deutsche Privat- und Wirtschaftsrecht bislang nicht. Von zentraler Bedeutung für die Regulierung von ADM-Systemen ist vor allem das Datenschutzrecht. Hier finden sich spezielle Transparenzgebote und das Verbot automatisierter Einzelentscheidungen. Der Anwendungsbereich dieser Regeln ist jedoch schmal. Für Entscheidungsunterstützungssysteme (Decision Support Systems) finden diese Regeln keine Anwendung. Dadurch können Schutzlücken entstehen. Ob eine Schließung der Schutzlücken etwa beim Scoring durch den nationalen Gesetzgeber geschlossen werden kann (§ 31 BDSG n.F.) erscheint zweifelhaft. Hier wäre der europäische Gesetzgeber gefordert. Da eine Überarbeitung der DS-GVO in der nächsten Zeit wohl nicht auf der politischen Agenda steht, gilt es zunächst die vorhanden rechtlichen Möglichkeiten auszuschöpfen und das Instrumentarium der DS-GVO daraufhin zu überprüfen, inwieweit hier Ansatzpunkte für die Gewährleistung einer „Algorithmic Accountability“ bestehen. Eine wichtige Rolle als „Frühwarnsystem“ auch für ADM-Systeme dürfte dabei die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO spielen.

Andere Regelungen außerhalb des Datenschutzrechts, wie etwa das AGG und das UWG, zeichnen sich durch einen technologieneutralen Ansatz aus und finden daher auch ohne weiteres auf ADM-Systeme Anwendung. Ein Bedarf für ein „digitales AGG“ ist derzeit nicht erkennbar. Praktische Probleme haben ihre Ursache weniger im materiellen Recht als im Bereich der Rechtsdurchsetzung. Der Trend zur Personalisierung von Werbung, Angeboten, Preisen führt zu einer „Atomisierung“ der Geschäftspraktiken und erschwert die Marktkontrolle durch Verbraucherverbände. Dies könnte – wie in Teil 3 der Studie näher ausgeführt wird – eine Erweiterung behördlicher Aufsichtsbefugnisse erforderlich machen.

3 OPTIONEN FÜR EINE ERGÄNZUNG DES REGULIERUNGSRAHMENS

Angesichts der bislang nur fragmentarischen gesetzlichen Regelung werden zunehmend Forderungen laut, die eine Ergänzung des Regulierungsrahmens für ADM-Prozesse einfordern. Die Vorschläge reichen von moderaten Anpassungen des geltenden Rechts[237] über die Einrichtung eines „Algorithmen-TÜV"[238] bis hin zur Schaffung eines eigenständigen „Algorithmengesetzes"[239]. In der Tat stellt sich die Frage, inwieweit den Gesetzgeber angesichts der im ersten Teil der Studie beschriebenen Gefährdungslagen eine gesetzgeberische Handlungspflicht im Sinne einer Ausgestaltungs- und Gewährleistungsverantwortung für algorithmengesteuerte Entscheidungsprozesse trifft. Dabei gilt es, einen sachgerechten Ausgleich zu finden zwischen den konkurrierenden Zielen des Persönlichkeitsschutzes, dem Schutz der Betriebs- und Geschäftsgeheimnisse von Unternehmen sowie der Förderung digitaler Wertschöpfungspotenziale.[240] Die Aufgabe besteht damit auch in der richtigen Justierung von Innovationsoffenheit und Innovationsverantwortung.[241]

Vor diesem Hintergrund sollen im Folgenden einige Handlungsoptionen für eine Fortentwicklung des regulatorischen und institutionellen Rahmens entwickelt werden, die dazu beitragen könnten, den veränderten Bedingungen einer durch den Einsatz von Algorithmen geprägten Wirtschafts- und Gesellschaftsordnung Rechnung zu tragen. Das Spektrum der in Betracht kommenden Maßnahmen reicht von freiwilligen Standards,[242] über Zertifizierungsmodelle und andere Instrumente der Co-Regulierung bis hin zur Schaffung neuer behördlichen Kompetenzen für eine Kontrolle von Algorithmen sowie explizite Vorgaben für die Entwicklung von Algorithmen („accountability by design").[243] Ebenfalls in den Blick genom-

---

[237] Vgl. den Überblick bei *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 f.; siehe auch *Wolfgang Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017) 1 ff.

[238] *Heiko Maas*, Unsere digitalen Grundrechte, http://www.bmjv.de/SharedDocs/Interviews/DE/2015/-Namensartikel/12092015_DieZeit.html („Wir brauchen deshalb einen Algorithmen-TÜV, der die Lauterkeit der Programmierung gewährleistet und auch sicherstellt, dass unsere Handlungs- und Entscheidungsfreiheit nicht manipuliert wird."); ähnlich VZBV, Verbraucherpolitische Kernforderungen des Verbraucherzentrale Bundesverbands e.V. (vzbv) für die Legislaturperiode 2017 bis 2021 (Februar 2017), S. 7; *Klaus Müller*, Algorithmen Transparent gestalten, https://www.vzbv.de/sites/default/files/downloads/2017/12/13/17-12-08_veranstaltung_vzbv_algorithmen_rede_formatiert.pdf; Der im Februar 2018 veröffentlichte Entwurf eines Koalitionsvertrages zwischen CDU, CSU und SPD sieht die zeitnahe Einsetzung einer Daten-Ehtikkommission vor, „die Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlägt.", vgl. Entwurf des Koalitionsvertrages vom 7.2.2018, Zeile 2101 ff.

[239] *Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz*, Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt (Dezember 2016), S. 67 ff., http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_SVRV-.pdf.

[240] *Martini*, JZ 2017, 1017 (1019).

[241] *Hoffmann-Riem*, AöR 142 (2017), 1.

[242] Siehe etwa das „Statement on Algorithmic Transparency and Accountability" des US Public Policy Council of the Association for Computing Machinery (USACM), 2017.

[243] SVRV, Verbraucherrecht 2.0 (Dezember 2016), S. 64; s. auch *Gerald Spindler*, Regulierung durch Technik, Kurzgutachten für den Sachverständigenrat für Verbraucherfragen, Dezember 2016.

men wird die Möglichkeit einer zivilgesellschaftlich organisierten Algorithmen-Kontrolle (z.B. AlgorithmWatch), die eine Partizipation der technischen Community von Programmierenden ermöglicht.[244]

3.1 TRANSPARENZGEBOTE

3.1.1 TYPEN VON ALGORITHMENTRANSPARENZ

Zum Schutz des Einzelnen vor den möglichen Gefahren von ADM-Prozessen ist zunächst die Erweiterung bestehender und die Schaffung neuer Transparenzgebote zu erwägen. Vorgelagert ist dabei die Frage, welchem Zweck Transparenzanforderungen für ADM-Prozesse dienen sollen. Denn Transparenz ist nicht Selbstzweck, sondern ist jeweils in Bezug auf eine weitergehende gesetzgeberische Zielsetzung zu sehen. Je nach konkreter Zielsetzung ergeben sich dabei unterschiedliche Folgerungen für den Zeitpunkt der Information und die inhaltliche Reichweite der Transparenzpflichten.

Für die rechtspolitische Diskussion ist es hilfreich, dabei drei unterschiedliche Ziele von Algorithmentransparenz zu unterscheiden:[245] (1) Algorithmentransparenz kann zum einen dazu dienen, eine informierte Einwilligung zu ermöglichen. Dies erfordert eine Information *vor* einer automatisierten Entscheidung („Ex-ante-Transparenz"). (2) Algorithmentransparenz kann aber auch als Grundlage für die Geltendmachung von Rechtsbehelfen dienen, sofern durch die Entscheidung Rechte des Betroffenen verletzt wurden. Hierfür wäre eine Information *nach* der automatisierten Entscheidung ausreichend („Ex-post-Transparenz"). (3) Eine solche nachträgliche Information wäre ebenfalls ausreichend, wenn das Ziel der Transparenzregelung lediglich darin besteht, dem Betroffenen die Möglichkeit eines „opt-out" aus dem ADM-Prozess einzuräumen.

Wird eine Ex-ante-Transparenz vor einer automatisierten Entscheidung gefordert, kommt als Inhalt der Information nur eine abstrakte Beschreibung der allgemeinen Funktionsweise des Entscheidungssystems („Systemtransparenz") in Betracht, da eine konkrete Entscheidung ja gerade noch aussteht. Umgekehrt kann sich eine Ex-post-Transparenz nach einer automatisierten Entscheidung sowohl auf die abstrakte Systembeschreibung beziehen als auch auf eine konkrete Erläuterung der getroffenen Einzelfallentscheidung („Entscheidungstransparenz").[246] Nimmt man diese Überlegungen zusammen, so lassen sich drei verschiedenen Typen von Algorithmentransparenz unterscheiden:[247]

- Ex-ante-Systemtransparenz: Vorherige abstrakte Erläuterung der allgemeinen Systemfunktionalität

---

[244] Siehe etwa *Leonie Beining*, Wie Daten und Algorithmen die Rahmenbedingungen für das Gemeinwohl verändern, Stiftung Neue Verantwortung (Juni 2017).

[245] *Tae Wan Kim & Bryan Routledge*, Algorithmic transparency, a right to explanation and trust, Working Paper, Carnegie Mellon University, 2017, 2; *Sandra Wachter, Brent Mittelstadt & Luciano Floridi*, Why a Right to Explanation of Automated-Decision Making Does Not Exist in the General Data Protection Regulation, 7 International Data Privacy Law 76, 78 (2017).

[246] Wachter, Mittelstadt & Floridi, 7 International Data Privacy Law 76, 78.

[247] *Tae Wan Kim & Bryan Routledge*, Algorithmic transparency, a right to explanation and trust, Working Paper, Carnegie Mellon University, 2017, 4.

- Ex-post-Systemtransparenz: Nachträgliche abstrakte Erläuterung der allgemeinen Systemfunktionalität
- Ex-post-Entscheidungstransparenz: Nachträgliche konkrete Erläuterung der jeweiligen Einzelfallentscheidung

3.1.2 KENNZEICHNUNGSPFLICHTEN

Noch unterhalb der oben skizzierten Ebenen von System- und Entscheidungstransparenz wird als „erster Baustein" zur Herstellung von Algorithmentransparenz vorgeschlagen, den Einsatz von Algorithmen in persönlichkeitssensiblen Feldern zu kennzeichnen.[248] Dem liegt die Überlegung zugrunde, dass sich der Betroffene vor einer Benachteiligung durch ADM-Prozesse nur dann schützen und gegen Rechtsverletzungen nur verteidigen kann, die durch derartige algorithmengestützte Entscheidungen verursacht werden, wenn er darum weiß, dass er von einer solchen Entscheidung betroffen ist.

Anknüpfen lässt sich dabei an die bestehenden Transparenzgebote des Datenschutzrechts. So sehen Art. 13 Abs. 2 lit. f. und Art. 14 Abs. 2 lit. g DS-GVO schon jetzt eine Pflicht zur Information über das Bestehen einer „automatisierten Entscheidungsfindung" vor. Wie oben näher erläutert, knüpft diese Hinweispflicht aber an die engen Tatbestandsvoraussetzungen des Art. 22 Abs. 1 DS-GVO an und gilt daher nur für Fälle, in denen die Entscheidung „ausschließlich" automatisiert getroffen wird. Auf Fallgestaltungen, in denen ein Algorithmus lediglich zur Entscheidungsvorbereitung oder –Unterstützung eingesetzt wird (Decision Support Systems), finden die genannten Transparenzgebote der DS-GVO keine Anwendung.

Gerade in Fällen, in denen die Letztentscheidung von einem Menschen auf Grundlage eines algorithmengestützten Verfahrens getroffen wird, dürfte jedoch ein besonderer Aufklärungsbedarf bestehen. Durch die Einschaltung eines Menschen als (scheinbar) letztes Glied der Entscheidungskette wird es für den Betroffenen noch viel weniger erkennbar, dass er möglicherweise Objekt einer maschinell vorgeprägten Entscheidung ist als in solchen Fällen, in denen der Betroffene direkt einer „Entscheidungsmaschine" ausgesetzt ist. Dies dürfte etwa der Fall sein, wenn ein Arzt einem Patienten eine Diagnose stellt, ohne offenzulegen, dass diese ganz maßgeblich auf der algorithmischen Auswertung radiologischer Bilddaten beruht. In derartigen Fällen besteht die Gefahr, dass sich der menschliche Entscheider ganz auf die Empfehlung des ADM-Systems verlässt ohne dies dem Betroffenen mitzuteilen und die maschinell getroffene Entscheidung dadurch den Anschein einer menschlichen Entscheidung hat.

Konstellationen, in denen die Einbindung eines Menschen in den Entscheidungsprozess lediglich einen formalen Charakter hat und der Mensch nur Sprachrohr des Algorithmus ist, fallen zwar unter Art. 22 Abs. 1 DS-GVO und damit auch unter die Informationsgebote aus Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2

[248] So etwa *VZBV*, Algorithmenbasierte Entscheidungsprozesse (7.12.2017), S. 9; ebenso *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1020); in diese Richtung auch *Gerald Spindler*, Zukunft der Digitalisierung – Datenwirtschaft in der Unternehmenspraxis, DB 2018, 41, 46.

lit. g DS-GVO.[249] Ob im konkreten Fall eine solche Konstellation vorliegt oder nicht, wird für den Betroffenen in vielen Fällen aber gerade nicht erkennbar sein.

Bei der Ausgestaltung einer entsprechenden Kennzeichnungspflicht sollten verhaltenswissenschaftliche Erkenntnisse zu den Grenzen des verbraucherrechtlichen Informationsmodells und die zweifelhafte Wirksamkeit detaillierter Aufklärungspflichten berücksichtigt werden.[250]

Anknüpfend an Art. 12 Abs. 7 DS-GVO, der fakultativ die Verwendung standardisierter Bildsymbole (Piktogramme) für die nach Art. 13, 14 DS-GVO bereitzustellenden Informationen vorsieht, könnte auch die Kennzeichnung von ADM-Prozessen durch eingängige Symbole erfolgen.[251]

Ob der Einzelne von einer solchen Kennzeichnungspflicht tatsächlich einen Nutzen hat, wäre noch empirisch zu validieren. Zweifel ergeben sich insbesondere im Hinblick auf das in der Literatur unter dem Schlagwort „privacy paradox" beschriebene Phänomen.[252] So geben zwar viele Verbraucher in Umfragen an, dass ihnen der Schutz der Privatsphäre besonders wichtig ist, jedoch sind nur wenige Verbraucher bereit, für ein Mehr an Datenschutz im Online-Handel einen höheren Preis zu zahlen.[253] In gleicher Weise könnte der Fall eintreten, dass der Hinweis auf das Bestehen eines ADM-Prozesses schlicht ignoriert wird. Dies bedeutet allerdings nicht zwingend, dass ein solcher Hinweis ohne Funktion wäre. Auch wenn der Einfluss auf die informierte Entscheidung des Einzelnen gering bleibt, könnte ein solcher Hinweis einen Anstoß für das Tätigwerden zivilgesellschaftlicher Kontrollinstanzen (z.B. Verbraucherverbände oder Organisationen wie AlgorithmWatch) geben.

3.1.3 ERLÄUTERUNGSPFLICHTEN

Noch weiter gehen Überlegungen, die auf eine Begründungspflicht für algorithmenbasierte Entscheidungen zielen. So hat etwa der Staatssekretär im BMJV *Gerd Billen* im Februar 2018 vorgeschlagen, bei ADM-Prozessen eine kurze Erklärung („one pager") zu verlangen, „mit standardisierten Basisinformatio-

[249] *Buchner*, in: Kühling/Buchner, Art. 22 DSGVO Rn. 15.

[250] Vgl. zu den Grenzen des verbraucherrechtlichen Informationsmodells *Omri Ben-Shahar & Carl Schneider*, More than you wanted to know, Princeton 2014; siehe auch *Christoph Busch*, The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data, in: Christian Twigg-Flesner (ed.), Research Handbook on EU Consumer and Contract Law, Cheltenham 2016, 221; *Oren Bar-Gill & Omri Ben-Shahar*, Regulatory techniques in consumer protection: a critique of European consumer contract law, CML Rev. 2013, 109.

[251] In diese Richtung auch *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1020); zu den standardisierten Bildsymbolen nach Art. 12 Abs. 7 DSGVO siehe *Knyrim*, in: Ehmann/Selmayr, Art. 13 DSGVO, Rn. 8 ff.

[252] Vgl. *Susan Athey/Christian Catalini/Catherine Tucker*, The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, NBER Working Paper No. 23488, 2017, http://www.nber.org/papers/w23488; dazu *Tobias Dienlin/Sabine Trepte*, Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviours, European Journal of Social Psychology 45 (2015) 285 (286 f.); Sonja *Utz/Nicole Krämer*, The privacy paradox on social network sites revisited: The role of individual characteristics and group norms, Journal of Psychosocial Research on Cyberspace, 3(2), article 2, verfügbar unter: https://cyberpsychology.eu/article/view/4223/3265; *Monika Taddicken*, The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure, J Comput-Mediat Comm, 19: 248; siehe auch *Martini*, JZ 2017, 1017 (1019).

[253] *Alastair Beresford/Dorothea Kübler/Sören Preibusch*, Unwillingness to pay for privacy: a field experiment, SFB 649 discussion paper, No. 2011-010.

nen über das Zustandekommen eines Ergebnisses und die Datengrundlage".[254] In der Literatur ist die Frage nach einem Recht auf Erklärung („right to explanation") für ADM-Prozesse Gegenstand einer kontroversen Debatte. Dabei geht es nicht nur um die sehr umstrittene rechtsdogmatische Frage, ob sich aus den Vorschriften der DS-GVO ein Recht auf Erklärung der algorithmischen Entscheidung herleiten lässt,[255] sondern auch um die grundsätzliche und eher rechtspolitische Frage, ob eine Erklärung algorithmischer Entscheidungen sinnvoll ist. Aktuelle Studien zur Effektivität komprimierter und standardisierter Datenschutzinformationen (sog. privacy nutrition labels) deuten eher darauf hin, dass solche verkürzten Informationen (etwa in Form eines „one-pager") nur wenig zum Verständnis der Betroffenen beitragen[256]

Erläuterungspflichten, etwa im Sinne einer Offenlegung des Programmcodes, der einem ADM-Prozess zugrunde liegt, gegenüber den Nutzern oder der Öffentlichkeit erscheint nicht sinnvoll. Eine solche Form von technischer Algorithmentransparenz würde die Geschäftsmodelle der Betreiber ernsthaft gefährden und wäre nicht mit dem Schutz von Geschäftsgeheimnissen vereinbar.[257] Die Offenlegung der Algorithmen wäre eine Einladung zur Manipulation der ADM-Systeme, etwa durch „Search Engine Optimization" bei Suchmaschinen oder durch die Umgehung von Spam-Filtern bei E-Mail-Programmen.[258]

Diskutiert werden derzeit eine Reihe von anderen Ansätzen, die eine Erklärung algorithmenbasierter Entscheidungen ohne eine Offenlegung des Programmcodes ermöglichen. So wird beispielweise vorgeschlagen, ADM-Prozesse durch sogenannte „kontrafaktische Erklärungen" (*counterfactual explanations*) zu erläutern.[259] Dabei soll nicht offengelegt werden, warum eine bestimmte Entscheidung getroffen wurde (etwa die Ablehnung eines Kreditantrages), sondern unter welchen Bedingungen die Entscheidung anders ausgefallen wäre (also der Kredit gewährt worden wäre).

3.2 ACCOUNTABILITY BY DESIGN

In Anlehnung an das bereits seit den 1990er Jahren bekannte Konzept des Datenschutzes durch Technikgestaltung („privacy by design")[260] lassen sich auch rechtliche Vorgaben für eine „Algorithmic Accoun-

[254] Rede von *Gerd Billen*, Staatssekretär im Bundesministerium der Justiz und für Verbraucherschutz, bei der gemeinsamen Konferenz des Bundesministeriums der Justiz und Verbraucherschutz sowie des bitkom „Künstliche Intelligenz – Dein Freund und Helfer?" zum Safer Internet Day am 6.2.2018 in Berlin, http://www.bmjv.de/SharedDocs/Reden/DE/2018/020618_Billen_SID.html.

[255] Siehe dazu bereits oben Abschnitt 2.1.2.

[256] Siehe etwa *Omri Ben-Shahar/Adam Chilton*, Simplification of Privacy Disclosures: An Experimental Test, 45:S2 Journal of Legal Studies, S41-S67 (2016); siehe auch Sara Elisa Kettner, Christian Thorun, and MaxVetter, Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz, ConPolicy-Studie 2018.

[257] *Lilian Edwards & Michael Veale*, Slave to the algorithm? Why a ‚right to an explanation' is probably not the remedy you are looking for, 16 Duke Law & Technology Review 18, 43 (2017).

[258] *Joshua Kroll* et al., Accountable Algorithms, 165 University of Pennsylvania Law Review, 633, 654 (2017); *Jürgen Kühling & Nicolas Gauß*, Suchmaschinen – eine Gefahr für den Informationszugang und die Informationsvielfalt?, ZUM 2007, 881 (889).

[259] *Sandra Wachter, Brent Mittelstadt & Christ Russell*, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR (October 6, 2017), Harvard Journal of Law & Technology, Forthcoming, verfügbar auf SSRN: https://ssrn.com/abstract=3063289.

[260] *Ann Cavoukian*, Ann. "Privacy by design" Take the challenge, Information and privacy commissioner of Ontario, Canada (2009).

tability“ durch technische Anforderungen an die Gestaltung von ADM-Systemen verwirklichen („accountability by design“).[261] Je nachdem in welchem Bereich man den Schwerpunkt beim Konzept der *accountability* setzt, lassen sich dabei unterschiedliche Ansätze unterscheiden, wie die folgenden Beispiele zeigen.

3.2.1 INTERPRETABILITY BY DESIGN

Geht man davon aus, dass *accountability* im Sinne einer „Rechenschaftspflicht“ zwingend voraussetzt, dass das ADM-System „berechenbar“ und seine Funktionsweise erklärbar sein muss (sei es gegenüber den Nutzern oder einer Aufsichtsbehörde), könnten die Anwender von ADM-Systemen verpflichtet werden, nur solche Algorithmen einzusetzen, bei denen es möglich ist, die Gründe für eine Entscheidung *ex post* festzustellen. Im Umkehrschluss würde dies bedeuten, dass der Einsatz eines opaken Algorithmus, der auch für den Anwender selbst eine „black box“ ist, unzulässig wäre. Während das Erfordernis einer *interpretability by design* bei konventionell programmierter Software noch relativ leicht zu erfüllen sein dürfte, erreichen moderne selbstlernende Algorithmen, wie etwa neuronale Netze, einen Komplexitätsgrad, die an dieser regulatorischen Hürde scheitern würden.[262] Eine mögliche Lösung versprechen hier neuere Forschungsansätze, die darauf zielen, *explainable artificial intelligence* (XAI) zu entwickeln. Dabei handelt es sich um selbstlernende Systeme, die nicht nur den gewünschten Output liefern, sondern auch selbst erklären, auf welchen Input sie das Ergebnis zentral stützen.[263] Zusätzlich erschwert wird die „Erklärbarkeit“ algorithmenbasierter Entscheidungen dadurch, dass viele ADM-Systeme zukünftig nicht mehr isoliert agieren, sondern mit anderen Systemen vernetzt werden, etwa als Bestandteil von Smart Grids oder im Falle von Verkehrstelematik-Systemen.[264] „Algorithmic Accountability“ im Sinne einer Nachvollziehbarkeit von ADM-Prozessen setzt in diesen Fällen voraus, dass alle Einzelsysteme den Anforderungen einer *interpretability by design* genügen.

3.2.2 LEGALITY AND ETHICS BY DESIGN

Während die Forderung nach einer „eingebauten“ Erklärbarkeit von ADM-Prozessen lediglich einen formalen Aspekt der Rechtmäßigkeit algorithmischer Systeme betrifft und gewissermaßen einen *due (algorithmic) process* sicherstellen soll, geht die Forderung nach einer automatischen Berücksichtigung materi-

---

[261] Siehe etwa *VZBV*, Algorithmen basierte Entscheidungsprozesse (7.12.2017), S. 12.

[262] Vgl. *Timo Rademacher*, Predictive Policing im deutschen Polizeirecht, AöR 142 (2017) 366 (377).

[263] Aus der inzwischen sehr umfangreichen Literatur zu diesem Thema siehe etwa *Zachary C. Lipton*, The Mythos of Model Interpretability, (2016) ICML Workshop on Human Interpretability in Machine Learning, arXiv:1606.0490; *Marco Tulio Ribeiro, Sameer Singh & Carlos Guestrin*, Why Should I Trust You?: Explaining the Predictions of Any Classifier, (2016) Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 1135; *Andreas Henelius* et al., A Peek Into the Black Box: Exploring Classifiers by Randomization, (2014) 28 Data Mining and Knowledge Discovery 1503; *Anupam Datta, Shayak Sen & Yair Zick*, Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems, (2016) Proceedings of the 2016 IEEE Symposium on Security and Privacy 598; *Philip Adler* and others, Auditing Black-Box Models for Indirect Influence, (2016) Proceedings of the 2016 IEEE 16th International Conference on Data Mining (ICDM) 1; *Tim Miller*, Explanation in artificial intelligence: Insights from the social sciences, arXiv preprint arXiv:1706.07269 (2017); Finale Doshi-Velez & Been Kim A roadmap for a rigorous science of interpretability, arXiv preprint arXiv:1702.08608 (2017).

[264] Vgl. *Julian Reichwald & Dennis Pfisterer*, Autonomie und Intelligenz im Internet der Dinge, CR 2016, 208 (211).

eller Rechtmäßigkeitsanforderungen[265] („legality by design“) und ethischer Standards bei der Technikgestaltung („ethics by design“) noch einen Schritt weiter.[266] So hat etwa die vom BMVI eingesetzte Ethikkommission „Automatisiertes und vernetztes Fahren“ jüngst die Forderung erhoben, dass bei der Programmierung selbstfahrender Fahrzeuge der Grundsatz beachtet werden müsse, dass der Schutz menschlichen Lebens in einer Rechtsgüterabwägung höchste Priorität habe. Die Programmierung der Steueralgorithmen sei daher im Rahmen des technisch Machbaren so anzulegen, dass im Konflikt Tier- oder Sachschäden in Kauf zu nehmen seien, wenn dadurch Personenschäden vermeidbar seien.[267]

Andere Überlegungen für normativ „aufgeladene“ ADM-Systeme zielen darauf, die Gefahr von algorithmischen Diskriminierungen durch Technikgestaltung zu reduzieren. Im Wesentlichen geht es dabei um technische Vorkehrungen, die dafür sorgen sollen, dass bestimmte Variablen (z.B. ethnische Herkunft, Religion) im ADM-Prozess unberücksichtigt bleiben, auch wenn diese statistisch betrachtet einen prädiktiven Wert haben.[268] Bei der Umsetzung dieses Ansatzes ergeben sich allerdings dadurch Schwierigkeiten, dass die im Datensatz vorhandenen „erlaubten“ Variablen möglicherweise versteckte Hinweise auf die „verbotenen“ Variablen enthalten. Dies kann dazu führen, dass ein Data-Mining-Algorithmus diese Korrelationen berücksichtigt, wodurch indirekte Diskriminierungen entstehen können.[269]

3.2.3 SERENDIPITY BY DESIGN

Technikgestaltung kann nicht nur zur Herstellung von Transparenz oder zum Schutz von Individualrechtsgütern eingesetzt werden. Zu erwägen wäre, ob man auch den gesellschaftlichen Risiken einer „Algorithmenkultur“ durch Vorgaben für das Design von ADM-Prozessen begegnen könnte. Unter dem Schlagworten *serendipity by design*[270] und *diversity by design*[271] wird diskutiert, ob das vielfach beklagte Phänomen der Echokammern und Filterblasen in sozialen Medien dadurch abgemildert werden könnte, dass in die für die Erstellung der *newsfeeds* verwendeten Algorithmen ein „Zufallselement“ eingebaut wird, durch das die Nutzer gelegentlich mit einer Nachricht konfrontiert werden, die nicht ihrem üblichen Präferenzprofil entspricht. Auf diese Weise, so die zugrundliegende Überlegung, könnten Offenheit und

---

[265] Ein weiteres Anwendungsbeispiel ist der „Einbau“ kartellrechtlicher Regeln in Preissoftware, um unzulässige abgestimmte Verhaltensweisen zu unterbinden, vgl. *Simonetta Vezzoso*, Competition by Design (28.11.2017), prepared for presentation at 12th ASCOLA Conference, Stockholm University, 15-17 June 2017, https://ssrn.com/abstract=2986440.

[266] Siehe etwa *Ronald Leenes & Rederica Lucivero*, Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design, 6 Law, Innovation and Technology, 193-220 (2016); kritisch *Wolfgang Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), 1 (35).

[267] Bericht der *Ethikkommission* „Automatisiertes und vernetztes Fahren“ (Juni 2017), S. 11.

[268] Zu den unterschiedlichen Methoden der „non-discrimination by design“ siehe *Hans Lammerant, Peter Blok & Paul de Hert*, Big data en gelijke behandeling, in: Peter Blok (ed.), Big data & het recht, Sdu Uitgevers 115 (131).

[269] *Lilian Edwards & Michael Veale*, Slave to the algorithm? Why a ‚right to an explanation' is probably not the remedy you are looking for, 16 Duke Law & Technology Review 18, 29 (2017).

[270] *Urbano Reviglio*, Serendipity by Design? How to Turn from Diversity Exposure to Diversity Experience to Face Filter Bubbles in Social Media, in: Kompatsiaris et al. (eds.), International Conference on Internet Science, INSCI 2017, Springer 2017, 281-300.

[271] *Natali Helberger*, Diversity by design, 1 Journal of Information Policy 1, 441-469 (2011); *dies.*, Merely Facilitating or Actively Stimulating Diverse Media Choices? Public Service Media at the Crossroad, 9 International Journal of Communication 1324-1340 (2015); siehe auch *Nikolaus Pöchhacker* et al., Interventionen in die Produktion algorithmischer Öffentlichkeiten: Recommender Systeme als Herausforderung für öffentlich-rechtliche Sendeanstalten, 18 kommunikation@gesellschaft, 25 (2017), https://www.ssoar.info/ssoar/handle/document/51500.

Neugier gefördert und das Entstehen von Filterblasen verhindert werden.[272] Das Beispiel zeigt, welche vielfältigen Möglichkeiten sich für die Regulierung eines „verantwortungsvollen" Algorithmendesigns bieten. Kritisch ließe sich allerdings anmerken, dass hier möglicherweise die Grenze zu einer paternalistischen Algorithmenregulierung überschritten wird.[273]

3.3 PRÄVENTIVE KONTROLLE VON ALGORITHMEN

3.3.1 ZULASSUNGSVERFAHREN

Für besonders gefahrgeneigte Anwendungsfelder, die besonders persönlichkeitssensibel sind oder bei denen schwere Schäden für sonstige wichtige Rechtsgüter drohen, ist die Einführung einer präventiven Zulassungskontrolle („premarket approval") von ADM-Systemen denkbar.[274] Entsprechende Zulassungsverfahren gelten schon heute aufgrund des Medizinproduktegesetzes für bestimmte medizinische Softwareanwendungen.[275] Dieses Modell könnte als Vorbild für einen sektorübergreifenden Regulierungsansatz oder jedenfalls für weitere, ebenfalls besonders sensible Bereiche dienen. In Betracht kommt eine präventive Zulassungskontrolle etwa für sicherheitsrelevante ADM-Prozesse bei autonomen Systemen, beispielsweise hoch- und vollautomatisierte Fahrzeuge.[276] Bei der Frage nach der Erforderlichkeit einer Ex-ante-Kontrolle sollte nach unterschiedlichen Gefährdungslagen differenziert werden. Ein mögliches Modell für eine nach Risikoklassen gestufte Regulierung liefert etwa die im Mai 2017 in Kraft getretene und ab Mai 2020 anwendbare EU-Medizinprodukte-Verordnung (MPVO).

Für die Frage, unter welchen Voraussetzungen eine im medizinischen Bereich eingesetzte Software überhaupt als Medizinprodukt zu klassifizieren ist und damit den strengen regulatorischen Anforderungen des Medizinprodukterechts unterliegt, unterscheidet die MPVO zwischen Software, die vom Hersteller speziell für medizinischen Zwecke (z.B. Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten) vorgesehen ist und solcher Software, die lediglich für allgemeine Zwecke in Einrichtungen des Gesundheitswesens eingesetzt wird (z.B. Software zur Patientenverwaltung, Bettendisposition, Abrechnung oder Terminsteuerung in Krankenhäusern) sowie Software, die lediglich im Lifestyle-Bereich eingesetzt wird.[277]

Ist die Software hiernach als Medizinprodukt i.S.v. Art. 2 Nr. 1 MPVO anzusehen, so sieht Anhang VIII

---

[272] *Paul Resnick, R. Kelly Garrett, Travis Kriplean, Sean A. Munson & Natalie Jomini Stroud*, Bursting your (filter) bubble : Strategies for promoting diverse exposure, in: Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion, CSCW 13, 95-100 (2013); *Rikiya Takahashi & Shunan Zhang*, Towards Bursting Filter Bubble via Contextual Risks and Uncertainties. arXiv preprint arXiv:1706.09985 (2017).

[273] Vgl. *Luciano Floridi*, Tolerant paternalism: pro-ethical design as a resolution of the dilemma of toleration, 22 Science and Engineering Ethics 1669–1688 (2016).

[274] Vgl. *Andrew Tutt*, An FDA for Algorithms 69 Admin. L. Rev. 83 (2017); *Martini*, JZ 2017, 1017 (2021).

[275] Siehe dazu bereits Abschnitt 2.4.1.

[276] Eine ensprechende Empfehlung hat jüngst die vom Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) eingesetzte „Ethikkommission Automatisiertes und Venetztes Fahren" ausgesprochen, vgl. den Bericht der *Ethikkommission* (Juni 2017), S. 10: „Die Gewährleistungsverantwortung für die Einführung und Zulassung automatisierter und vernetzter Systeme im öffentlichen Verkehrsraum obliegt der öffentlichen Hand. Fahrsysteme bedürfen deshalb der behördlichen Zulassung und Kontrolle."

[277] Vgl. Erwgr. 19 MPVO.

der Verordnung eine spezielle Klassifizierungsregel für die Einstufung in unterschiedliche Risikoklassen vor (Regel 11).[278] Danach wird medizinische Software je nach Gefahrenpotential in unterschiedliche Risikoklassen eingestuft. Maßgeblich ist, welche Konsequenzen die Entscheidung haben kann, die mit Unterstützung der Software getroffen werden soll. Liefert die Software Informationen, die zu einer Entscheidung herangezogen werden, die den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person hervorrufen kann, so erfolgt eine Einstufung in die höchste Risikoklasse (Klasse III). Geht es um Entscheidungen mittlerer Tragweite, die etwa eine schwerwiegende Verschlechterung des Gesundheitszustandes oder einen chirurgischen Eingriff zur Folge haben können, wird die Software in eine mittlere Risikoklasse (Klasse II b) eingestuft. Dient die Software lediglich der Kontrolle von physiologischen Prozessen erfolgt eine noch niedrigere Einstufung (Klasse IIa), es sei denn die Software ist für die Kontrolle von vitalen physiologischen Parametern bestimmt (dann Klasse IIb). Andere medizinische Softwareprodukte werden in die niedrigste Risikoklasse (Klasse I) eingeordnet.

Zum Prüfungsumfang eines Zulassungsverfahrens sollte nicht nur der Programmcode des ADM-Systems gehören. In die Prüfung einzubeziehen sind auch die Trainingsdaten, anhand derer etwa ein Bilderkennungsalgorithmus gelernt hat, bestimmte Objekte zu identifizieren. Besondere Schwierigkeiten ergeben sich bei Zulassungsverfahren für selbstlernende Systeme. Derartige Systeme verändern sich im laufenden Betrieb und passen sich an die veränderte Umwelt an. Die im Zeitpunkt der Zulassung überprüften Eigenschaften des Systems stellen daher nur eine „Momentaufnahme“ dar. Im Beispielfall eines hochautomatisierten Fahrzeugs könnte dies etwa bedeuten, dass sich die Fahrzeugdynamik an den jeweiligen Fahrer anpasst.[279] Dies hätte zur Konsequenz, dass sich die ADM-Systeme der individuellen Fahrzeuge mit zunehmendem Betrieb unterscheiden und möglicherweise immer weiter von dem im Rahmen der Zulassungskontrolle überprüften Zustand entfernen. Die Ethikkommission des BMVI zieht daraus den Schluss, dass ein Einsatz von selbstlernenden Systemen beim gegenwärtigen Stand der Technik nur bei nicht unmittelbar sicherheitsrelevanten Funktionen denkbar ist.[280] Solange nicht sichergestellt werden kann, dass selbstlernende Algorithmen grundlegende Anforderungen an ADM-Systeme auch dann noch erfüllen, wenn sie sich im Wechselspiel mit Umwelteinflüssen verändern, wird man diese Einschätzung auch auf andere sensible Bereiche (z.B. Pflegeroboter) übertragen müssen. Aus dem dynamischen Charakter selbstlernender ADM-Systeme folgt zudem, dass derartige Systeme nicht nur einer Zulassungskontrolle unterliegen sollten, sondern zusätzlich einer kontinuierlichen Fehlerkontrolle.

3.3.2 ALGORITHMIC IMPACT ASSESSMENT

Als milderes Mittel im Vergleich zu einem präventiven Zulassungsverfahren könnte in weniger gefahrge-

[278] Die Klassifizierungsregel Nr. 11 gilt nur für die sogenannte Stand-Alone-Software, die nicht Bestandteil eines Medizinprodukt ist, sondern ein eigenständiges Medizinprodukt i.S.v. Art. 2 Nr. 1 MPVO darstellt. Ist die Software Bestandteil eines Medizinprodukts (z.B. Steuerungssoftware für EKG-Gerät), wird die Software automatisch derselben Klasse zugeordnet wie das Produkt, vgl. *Angela Graf*, Revision des europäischen Rechtsrahmens für Medizinproduzkte: Einfluss auf die Klassifzierung von Medizinprodukten, PharmR 2017, 57 (59); siehe auch *Peter von Czettritz/Tanja Strelow*, „Beam me up, Scotty“ – die Klassifzierung von Medical Apps als Medizinprodukte. PharmR 2017, 433 (435).

[279] Bericht der *Ethikkommission des BMVI* (Juni 2017), S. 30.

[280] Bericht der *Ethikkommission des BMVI* (Juni 2017), S. 30.

neigten Konstellationen eine Verpflichtung zur Durchführung einer Algorithmen-Folgenabschätzung (*algorithmic impact assessment*) nach dem Vorbild der in Art. 35 DS-GVO geregelten Datenschutz-Folgenabschätzung (oder auch als deren Bestandteil) eingeführt werden.[281] Der Mehrwert einer solchen Algorithmen-Folgenabschätzung im Vergleich zu dem Verfahren nach Art. 35 DS-GVO könnte darin liegen, dass nicht nur die datenschutzrechtlichen Aspekte der ADM-Prozesse analysiert werden, sondern auch darüber hinaus gehende gesellschaftliche Folgen des Einsatzes von Algorithmen (etwa die Entstehung von Filterblasen und Echokammern oder mögliche Autonomieverluste) berücksichtigt werden könnten.

3.4 MARKTBEGLEITENDE KONTROLLE

Die bisher erörterten Regulierungsansätze könnten um unterschiedliche Formen der marktbegleitenden Algorithmenkontrolle ergänzt werden. In Betracht kommen zum einen eine *externe* Kontrolle einzelner ADM-Systeme im Rahmen eines „Algorithm Auditing" und anlassbezogene Sektoruntersuchungen. Zum anderen könnte erwogen werden, in den Unternehmen, die ADM-Systeme einsetzen, *interne* Prozesse für ein adäquates Risikomanagement einzuführen, deren Einhaltung durch einen Algorithmenbeauftragten überwacht wird.

3.4.1 ALGORITHM AUDITING

Eine präventive Kontrolle von ADM-Systemen ist weder in allen Bereich erforderlich, noch ist sie für sich genommen ausreichend, um eine sachgerechte Algorithmenregulierung zu gewährleisten. Bei ADM-Systemen, die entweder eine besonders große Reichweite haben (z.B. Suchmaschinen) oder mit Gefahren für wichtige Rechtsgüter verbunden sind (z.B. autonome Fahrzeuge), ist daher zusätzlich eine „begleitende Fehlerkontrolle"[282] erforderlich. Dies ist schon deshalb geboten, weil selbstlernende Algorithmen im laufenden Betrieb ihre Struktur verändern und daher einer regelmäßigen Überprüfung bedürfen.

Die Durchführung der Algorithmenprüfung könnte dabei entweder eine Behörde oder eine beliehene Stelle (wie etwa der TÜV) übernehmen. Ob die Schaffung einer eigenständigen „Digitalagentur" für diese Zwecke sinnvoll ist,[283] erscheint eher zweifelhaft. Naheliegender dürfte es sein, Behörden, die bereits für bestimmte Sektoren zuständig sind, etwa die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Bundesnetzagentur (BNetzA) mit dieser Aufgabe zu betrauen, da hier bereits sektorspezifische Expertise vorhanden ist, die für die Bewertung der Risiken von ADM-Verfahren hilfreich sein dürfte. Für Bereiche, die bislang nicht einer sektorspezifischen Behördenaufsicht unterliegen, könnte die Algorithmenprüfung etwa dem Bundeskartellamt (BKartA) übertragen werden. Erforderlich wäre dafür der Aufbau entsprechender technologischer Expertise, etwa durch die Einführung eines „Chief Technology Officer"

---

[281] Einen entsprechenden Vorschlag hat kürzlich das AI Now Institute der New York University für ADM-Prozesse vorgelegt, die von öffentlichen Stellen eingesetzt weren, vgl. *AI Now Institute*, Algorithmic Impact Assessments: Toward Accountable Automation in Public Agencies (21.2.2018), https://medium.com/@AINowInstitute/-algorithmic-impact-assessments-toward-accountable-automation-in-public-agencies-bd9856e6fdde.

[282] *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1021).

[283] So die Forderung des *SVRV*, Verbraucherrecht 2.0, S. 69 ff.

nach dem Vorbild der amerikanischen Federal Trade Commission (FTC).[284]

Inhaltlich sollte sich das Audit-Verfahren nicht allein auf den Computercode des ADM-Systems beschränken. Es ist nämlich nicht zu erwarten, dass Verstöße gegen gesetzliche Diskriminierungsverbote dort in Maschinensprache auffindbar sind, etwa nach dem folgenden Muster:[285]

```
if ($race = NOT_CAUCASIAN) then { illegal_discrimination() };
```

Erforderlich ist vielmehr ein erweiterter Prüfradius, der bei lernenden Algorithmen auch die Trainings- und Testdaten umfasst, um etwaige Verzerrungen festzustellen, die der Algorithmus aus der Datenbasis erlernt haben könnte (Input-Monitoring).[286] Die Überprüfung der ADM-Systeme setzt dabei voraus, dass die Trainings- und Testdaten dokumentiert und die Programmabläufe des ADM-Systems protokolliert werden. Auf Basis dieser Daten könnte sodann mittels Kontrollalgorithmen der Output des ADM-Systems auf etwaige Konstruktionsfehler überprüft werden (Black-Box-Experimente).[287] Um dies zu gewährleisten müsste die „auditability" im System eingebaut sein.[288] In diesem Sinne gehört die „auditability" zu den Grundprinzipien der „algorithmic accountability".[289] Um die Belastung kleinerer Unternehmen durch übermäßige Dokumentationspflichten zu vermeiden, sollte der Umfang der zu protokollierenden Daten dabei nach dem jeweiligen Gefahrenpotential des ADM-Systems skaliert werden.

3.4.2 SEKTORUNTERSUCHUNGEN

Als flankierende Maßnahme wäre zu erwägen, dass die zuständige Aufsichtsbehörde die Befugnis zur Durchführung von Sektoruntersuchungen erhält, um verbreitete Rechtsverstöße durch den Einsatz von ADM-Systemen aufzudecken. Als Vorbild könnte dabei die im Jahr 2017 mit der 9. GWB-Novelle neu geschaffene Befugnis des Bundeskartellamts zur Durchführung verbraucherrechtlicher Sektoruntersuchungen nach § 32e Abs. 5 und 6 GWB dienen. Danach können Ermittlungen eingeleitet werden „bei

---

[284] Vgl. *Rupprecht Podszun*, The Digital Economy: Three Chances for Competition Law, 23 Maastricht Journal of European and Comparative Law, 747, 750 (2016).

[285] Beispiel nach *Christian Sandvig* et al., Auditing algorithms: Research methods for detecting discrimination on internet platforms, Data and discrimination: converting critical concerns into productive inquiry (2014): 1-23.

[286] *Brent Mittelstadt*, Automation, Algorithms, and Politics| Auditing for Transparency in Content Personalization Systems, International Journal of Communication, 2016, 10. Jg., S. 12; *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1022); zum möglichen Prüfungsumfang siehe auch *Katharina Anna Zweig*, Arbeitspapier: Überprüfbarkeit von Algorithmen (7.7.2016), https://algorithmwatch.org/de/zweites-arbeitspapier-ueberpruefbarkeit-algorithmen/.

[287] Zu möglichen Auditmethoden siehe *Katharina Anna Zweig*, Wo Maschinen irren können: Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung, Arbeitspapier der Bertelsmann-Stiftung, Februar 2018; *Philip Adler* et al., Auditing Black-box Models for Indirect Influence, IEEE International Conference on Data Mining, December 2016; *Pauline T. Kim*, Auditing Algorithms for Discrimination, 166 University of Pennsylvania Law Review Online, 189-203 (2017); siehe ferner die verfügbaren Informationen unter: http://auditingalgorithms.science. In den USA bieten inzwischen bereits private Dienstleister die Durchführung von Algorithm Audits an, siehe etwa *O'Neil*, Risk Consulting and Algorithmic Auditing, http://www.oneilrisk.com/.

[288] *Information Commissioner's Office*, Big Data, Artificial Intelligence, Machine Learning and Data Protection, para. 190.

[289] *Nicholas Diakopoulos & Sorelle Friedler*, How to Hold Algorithms Accountable, MIT Technology Review (17.11.2016), https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/; Als Grundprinzipien der Algorithmic Accountability werden dort genannt: Responsibility, Explainability, Accuracy, Auditability, Fairness.

begründetem Verdacht des Bundeskartellamts auf erhebliche, dauerhafte oder wiederholte Verstöße gegen verbraucherrechtliche Vorschriften, die nach ihrer Art oder ihrem Umfang die Interessen einer Vielzahl von Verbraucherinnen und Verbrauchern beeinträchtigen". Das Amt hat bereits erste Sektoruntersuchungen auf Grundlage der neuen Befugnis eingeleitet. Beide Untersuchungen betreffen Geschäftsmodelle, bei denen auch Algorithmen eine wesentliche Rolle spielen.[290]

3.4.3 ALGORITHMENBEAUFTRAGTER

Um die effektive Verwirklichung der „Algorithmic Accountability" auch innerhalb eines Unternehmens abzusichern, kommt zusätzlich die Einrichtung eines internen Algorithmenbeauftragten[291] (oder „Algorithmikers"[292]) in Betracht. Nach dem Vorbild des Datenschutzbeauftragten (Art. 37 bis 39 DS-GVO) könnte der Algorithmenbeauftragte die ADM-Prozesse sowohl im Interesse des Anwenders als auch der betroffenen Nutzer überwachen. Ferner könnte der Beauftragte als Ansprechpartner für die Aufsichtsbehörde im Rahmen des Algorithmic Impact Assessment oder bei der Durchführung eines Algorithm Auditing fungieren.[293]

3.5 SELBSTREGULIERUNG

Als eine mögliche Alternative oder Ergänzung zu einer behördlichen Algorithmenkontrolle kommen Instrumente der Selbst- und Ko-Regulierung in Betracht.[294] Eine Möglichkeit wäre etwa die Zertifizierung von Algorithmen auf Basis freiwilliger „Algorithmic Accountability Standards", die von den Normungsorganisationen erarbeitet werden könnten (DIN, CEN, ISO etc.). Ein Vorbild für ein derartiges Modell bietet die DS-GVO, die einen Rechtsrahmen für europaweit einheitliche Zertifizierungsverfahren im Bereich des Datenschutzes und der Datensicherheit vorsieht (Art. 42 DS-GVO).[295] Verknüpft werden könnte ein solcher Ansatz mit Gütesiegeln, durch welche die Qualität der ADM-Systeme bewertet wird.

Denkbar wäre es auch, das im Bereich der Produktsicherheit seit langer Zeit angewendete Modell des „New Approach" auf algorithmenbasierte Entscheidungen zu übertragen.[296] Diesem Ansatz folgend könnten etwa per Gesetz festgelegte grundlegende Anforderungen an den Einsatz von Algorithmen

---

[290] Bundeskartellamt, Pressemitteilung vom 24.10.2017 (Einleitung Sektoruntersuchung Vergleichsportale), Pressemitteilung vom 13.12.2017 (Einleitung Sektoruntersuchung Smart-TV); siehe auch *Torsten Körber*, Das Bundeskartellamt auf dem Weg zur Digitalagentur?, WuW 2018, 173.

[291] So etwa *VZBV*, Algorithmenbasierte Entscheidungsprozesse (7.12.2017), S. 15.

[292] *Viktor Mayer-Schönberger/Kenneth Cukier*, Big Data: Die Revolution, die unser Leben verändern wird, München 2013, S. 228 f.; zustimmend *Wolfgang Schulz & Kevin Dankert*, Die Macht der Informationsintermediäre, 2016, S. 75 f., http://library.fes.de/pdf-files/akademie/12408.pdf.

[293] Zu weiteren Aufgaben siehe *Wolfgang Schulz & Kevin Dankert* (Fn. 282).

[294] Vgl. *Gerald Spindler/Christian Thorun*, Die Rolle der Ko-Regulierung in der Informationsgesellschaft: Handlungsempfehlung für eine digitale Ordnungspolitik, MMR Beilage, Heft 6, 1-28.

[295] Vgl. *Sebastian Kraska*, Datenschutz-Zertifizierungen in der EU-Datenschutzgrundverordnung, ZD 2016, 153 (154).

[296] *Christoph Busch*, Towards a „New Approach" in European Consumer Law: Standardisation and Co-Regulation in the Digital Single Market, (2016) Journal of European Consumer and Market Law, 197; s. auch zu einem ähnlichen Ansatz bei ODR-Systemen *Christoph Busch & Simon Reinhold*, Standardisation of Online Dispute Resolution Services: Towards a More Technological Approach, (2015) Journal of European Consumer and Market Law 50-58.

durch freiwillige Standards in technischer und rechtlicher Hinsicht konkretisiert werden. Die Verknüpfung zwischen den beiden Normebenen würde durch eine Konformitätsvermutung erfolgen.

Als weiteres Vorbild für ein hybrides Regulierungsmodell könnte § 161 Abs. 1 S. 1 AktG dienen. Danach erklären Vorstand und Aufsichtsrat börsennotierter Gesellschaften jährlich, dass den Empfehlungen der „Regierungskommission Deutscher Corporate Governance Kodex" entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden und warum nicht („comply or explain"). In ähnlicher Weise könnte der Gesetzgeber die Anwender besonders persönlichkeitssensibler ADM-Systeme verpflichten, sich zu einem „Algorithmic Accountability Code" zu erklären.[297]

Inzwischen gibt es bereits einige Vorbilder für einen „Algorithmic Accountability Standards" bzw. einen „Algorithmic Accountability Code". Beispielhaft kann das Statement on Algorithmic Transparency and Accountability der Association of Computing Machinery genannt werden, das sieben „Principles for Algorithmic Transparency and Accountability" festlegt: (1) Awareness, (2) Access and redress, (3) Accountability, (4) Explanation, (5) Data Provenance, (6) Auditability, (7) Validation and Testing.[298] Auf der Grundlage dieser Prinzipien ließe sich möglicherweise auch eine Berufsethik für Entwickler algorithmenbasierter Entscheidungssysteme entwickeln.[299]

3.6 HAFTUNGSRECHT

Nur kurz angerissen werden kann hier die Frage nach der Haftung für Schäden, die durch fehlerhafte ADM-Systeme entstehen. Ob das Produkthaftungsrecht Anwendung findet, soll nach herkömmlicher Lesart davon abhängen, ob die Software „verkörpert" ist oder nicht.[300] Nach einer neueren Ansicht ist diese Differenzierung willkürlich und in der digitalen Welt nicht mehr zeitgemäß.[301] Noch weiter geht der rechtspolitische Vorschlag, eine vom Fehlerbegriff des ProdHaftG unabhängige echte Gefährdungshaftung für Algorithmen einzuführen[302] In diese Richtung weist auch eine vom französischen *Conseil d'Etat* im Juli 2017 vorgelegten Studie[303] die einen Vorschlag für eine Algorithmenhaftung enthält. Danach soll der Nutzer („utilisateur"), der einen Algorithmus für die Zwecke seiner Tätigkeit als Sachhalter („gardien de la chose") angesehen werden und der Halterhaftung nach Art. 1242 Code civil unterworfen wer-

[297] Ähnlich bereits *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1023).
[298] Ähnliche Grundsätze enthalten die „Principles for Accountable Algorithms" der von Wissenschaftlern und Praktikern gegründeten Initiative „Fairness, Accountability and Transparency in Machine Learning" (FAT/ML): Responsibility, Explainability, Accuracy, Auditability, Fairness.
[299] Vgl. *Christoph Kerkmann*, Microsoft will den moralischen Programmierer, Handelsblatt (23.1.2018), http://www.handelsblatt.com/my/unternehmen/it-medien/furcht-vor-kuenstlicher-intelligenz-microsoft-will-den-moralischen-programmierer/20877112.html.
[300] Siehe zum Meinungsstand *Förster*, in. BeckOK § 2 ProdHG Rn. 22 f.
[301] *Gerhard Wagner*, MüKoBGB, § 2 ProdHG Rn. 17 f.
[302] Dafür *VZBV*, Algorithmenbasierte Entscheidungsprozesse, S. 14; ähnlich *Martini*, JZ 2017, 1017 (1022); allgemein zur Frage einer Gefährdungshaftung bei technischen Innovationen *Herbert Zech*, Gefährdungshaftung und neue Technologien, JZ 2013, 21 ff.
[303] *Conseil d'État*, Puissance publique et plateformes numériques: accompagner l'"ubérisation", La Documentation Française, 2017.

den.[304] Bei der Delegation von unternehmerischen Entscheidungen an ADM-Systemen kommt auch eine Haftung aufgrund algorithmenspezifischer Organisationspflichten (z.b. Gewährleistung der Systemstabilität, Dokumentation der Entscheidungen), die in Analogie zu § 33 Abs. 1a WpHG entwickelt werden könnten.[305] Zu klären wäre ferner, inwieweit prozessrechtliche Flankierungen erforderlich wären, etwa die Einführung eines in-camera-Verfahrens, um den Schutz von Geschäftsgeheimnissen zu gewährleisten.[306]

3.7 ZIVILGESELLSCHAFTLICHE ALGORITHMENKONTROLLE

Eine wichtige flankierende Funktion bei der Algorithmenkontrolle kommt schließlich Initiativen aus der Zivilgesellschaft zu. Als prominentes Beispiel kann hier die Ende 2015 gegründete Initiative AlgorithmWatch genannt werden, die u.a. im Rahmen eines Crowdsourcing-Projekts vor der Bundestagswahl 2017 untersucht hat, inwieweit Suchergebnisse bei Suchanfragen zum Wahlprogramm der Parteien oder den Namen der Spitzenkandidaten von der Suchmaschine Google personalisiert werden. Ein weiteres Vorhaben von AlgorithmWatch ist das im Februar 2018 gestartete Projekt „OpenSchufa", das darauf gerichtet ist, die Score-formel der Wirtschaftsauskunftei Schufa durch *reverse engineering* zu überprüfen. Das Projekt ist zugleich ein Beispiel für die Überprüfung von Algorithmen im Wege der umstrittenen Methode des *black box tinkering*.[307] Weitere Initiativen, die an der Schnittstelle von Zivilgesellschaft und Wissenschaft angesiedelt sind, sind etwa das französische Projekt „TransAlgo"[308] und die amerikanische Initiative „Fairness, Accountability and Transparency in Machine Learning"[309] (FAT/ML).

Zivilgesellschaftliche Initiativen können einen wichtigen Beitrag zur Verwirklichung von „algorithmic accountability" im Sinne eines „regulatory crowdsourcing" leisten. Dabei sind die Akteure jedoch auf die Partizipation vieler Betroffener angewiesen. Beispielhaft zeigt sich dies an den Aufrufen von AlgorithmWatch zu „Datenspenden" im Rahmen des bereits erwähnten Projekts zur Untersuchung von Filterblasen vor der Bundestagswahl 2017. In anderen Fällen bewegen sich derartige Initiativen in einem rechtlichen Graubereich, wenn etwa Daten mittels „Screenscraping" erhoben werden. Die Möglichkeiten der zivilgesellschaftlichen Algorithmenkontrolle sind daher begrenzt und können nur eine – wichtige – ergänzende Funktion erfüllen.

---

[304] Kritisch dazu *Florence G'sell*, Le Conseil d'État et les plateformes: de l'"ubérisation" à un programme d'action – A propos de l'étude annuelle 2017 du Conseil d'État, La Semaine juridique, Édition générale, N. 43, 23 Octobre 2017, S. 1926 (1928).

[305] So etwa Florian Möslein, Digitalisierung im Gesellschaftsrecht: Unternehmensleitung durch Algorithmen und künstliche Intelligenz? ZIP 2018, 204 (211).

[306] Vgl. *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1022).

[307] Vgl. *Maayan Perel & Niva Elkin-Koren*, Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement, 69 Florida Law Review 181 (2017).

[308] https://www.inria.fr/en/news/news-from-inria/transalgo.

[309] https://www.fatml.org.

ZUSAMMENFASSUNG UND RECHTSPOLITISCHE EMPFEHLUNGEN ZUM THEMA „ALGORITHMIC ACCOUNTABILITY“

Der Ausgangspunkt für die vorliegende Studie zum Thema „Algorithmic Accountability“ liegt in der zunehmenden Bedeutung algorithmenbasierter Entscheidungsprozesse (Algorithmic Decision Making, kurz: ADM) in der digitalisierten Wissensgesellschaft und Wirtschaft. Vor diesem Hintergrund wird in dieser Studie der bestehende normative Rahmen für ADM-Prozesse aufgearbeitet. Die Grundlage der juristischen Analyse bildet dabei zunächst eine überblicksartige rechtstatsächliche Bestandsaufnahme (Teil 1). Die sich daran anschließende juristische Analyse skizziert die rechtlichen Vorgaben für ADM-Prozesse und zeigt zugleich rechtliche und technische Grenzen der vorhandenen Regulierungsinstrumente und mögliche Schutzlücken auf (Teil 2). Hieran anknüpfend werden sodann rechtspolitische Handlungsoptionen herausgearbeitet, die sowohl rechtliche, technische und institutionelle Ansätze miteinander verbinden (Teil 3). Insgesamt lassen sich die wesentlichen Untersuchungsergebnisse wie folgt zusammenfassen:

I. Bedeutung algorithmenbasierter Entscheidungsprozesse

Im Zuge der rasch voranschreitenden Digitalisierung und Automatisierung dringen ADM-Systeme in immer neue Felder vor. Der „algorithmic turn“ erfasst praktisch alle Lebensbereiche. Die ADM-Systeme erfüllen dabei unterschiedliche Aufgaben. Das Spektrum reicht von Filterfunktionen über Klassifikationen und Rankings bis zum Matching von Personen und Informationen. Teilweise dient das ADM nur der Vorbereitung und Unterstützung menschlicher Entscheidungen, teilweise treffen ADM-Systeme auch selbst maschinelle Entscheidungen. Insbesondere in der Plattformökonomie – von Handelsplattformen bis zu Social Media – übernehmen ADM-Systeme eine wichtige Funktion als Informationsintermediäre. Damit kommt ihnen und ihren Betreibern eine wirtschaftliche und politische Schlüsselrolle zu.

Gleichzeitig sind ADM-Systeme anfällig für Fehler und systembedingten Risiken. Dies gilt etwa für Fälle algorithmischer Diskriminierung sowie interne und externe Manipulationen des ADM-Systems. Die Konsequenzen treffen nicht nur den Einzelnen sondern die Gesellschaft insgesamt. Verschärft wird dieses Problem dadurch, dass die ADM-Systeme für die von der Entscheidung Betroffenen als „black box“ erscheinen und die Ursachen von Fehlleistungen daher nur schwer festzustellen sind. Ob etwa eine Diskriminierung aufgrund struktureller Verzerrungen in den Trainingsdaten liegt, an einem Programmierfehler oder an Wechselwirkungen mit anderen Systemen, ist häufig nur mit großem Aufwand feststellbar.

Auf politischer Ebene scheint es einen breiten Konsens zu geben, dass auf den zunehmenden Einsatz von ADM-Systemen eine regulatorische Antwort gefunden werden muss. Mit Blick auf die Auswahl der geeigneten Regulierungsinstrumente besteht jedoch keine Einigkeit.

II. Regulierungsrahmen und mögliche Schutzlücken

Ein besonderes „Algorithmenrecht“ kennt das deutsche Privat- und Wirtschaftsrecht bislang nicht. Von zentraler Bedeutung für die Regulierung von ADM-Systemen ist vor allem das Datenschutzrecht. Hier finden sich spezielle Transparenzgebote und das Verbot automatisierter Einzelentscheidungen. Der Anwendungsbereich dieser Regeln ist jedoch schmal. Für Entscheidungsunterstützungssysteme (Decision Support Systems) finden diese Regeln keine Anwendung. Dadurch können Schutzlücken entstehen. Ob eine Schließung der Schutzlücken etwa beim Scoring durch den nationalen Gesetzgeber geschlossen werden kann (§ 31 BDSG n.F.) erscheint zweifelhaft. Hier wäre der europäische Gesetzgeber gefordert. Da eine Überarbeitung der DS-GVO in der nächsten Zeit wohl nicht auf der politischen Agenda steht, gilt es zunächst die vorhanden rechtlichen Möglichkeiten auszuschöpfen und das Instrumentarium der DS-GVO daraufhin zu überprüfen, inwieweit hier Ansatzpunkte für die Gewährleistung einer „Algorithmic Accountability“ bestehen. Eine wichtige Rolle als „Frühwarnsystem“ auch für ADM-Systeme dürfte die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO spielen.

Andere Regelungen außerhalb des Datenschutzrechts, wie etwa das AGG und das UWG, zeichnen sich durch technologieneutralen Ansatz und finden daher auch ohne weiteres auf ADM-Systeme Anwendung. Ein Bedarf für ein „digitales AGG“ ist derzeit nicht erkennbar. Praktische Probleme haben ihre Ursache weniger im materiellen Recht als im Bereich der Rechtsdurchsetzung. Der Trend zur Personalisierung von Werbung, Angeboten, Preisen führt zu einer „Atomisierung“ der Geschäftspraktiken und erschwert die Marktkontrolle durch Verbraucherverbände. Dies könnte eine Erweiterung behördlicher Aufsichtsbefugnisse erforderlich machen.

III. Rechtspolitische Handlungsempfehlungen

Statt eines breitflächigen Algorithmengesetzes sollten vorhandene Kontroll- und Aufsichtsmöglichkeiten behutsam erweitert werden Die Kontrolldichte sollte dabei nach dem Grad der Gefährdung und dem Rang der gefährdeten Rechtsgüter abgestuft werden. Sinnvoll erscheint ein Regulierungsmix aus behördlicher Kontrolle, zivilrechtlichen Rechtsbehelfen und Selbstregulierung.

1. Transparenzgebote

ADM-Prozesse sollten jedenfalls in sensiblen Bereichen einer Kennzeichnungspflicht unterliegen.[310] Weitergehende Erläuterungspflichten stoßen bei komplexen ADM-Systemen an Grenzen. Eine mögliche Lösung bieten neuere Forschungsansätze für *explainable artificial intelligence* (XAI).[311] Unabhängig von der technischen Machbarkeit ist der Mehrwert eines algorithmischen Informationsmodells, das dem Vorbild des viel kritisierten verbraucherrechtlichen Informationsmodells folgt, eher zweifelhaft. Transparenzgebote allein können jedenfalls einen verantwortungsvollen Umgang mit ADM-Systemen im Sinne einer „Algorithmic Accountability“ nicht sicherstellen.

[310] Siehe dazu Abschnitt 3.1.
[311] Siehe dazu Abschnitt 3.2.1.

2. Accountability by Design

Sinnvoll dürfte es sein, nach dem Vorbild von „privacy by design“ regulatorische Vorgaben für ADM-Systeme bereits im Rahmen der Technikgestaltung zu berücksichtigen und soweit möglich von vornherein in die ADM-Systeme einzubauen.[312] Insbesondere sollten ADM-Systeme so gestaltet werden, dass ein anlassbezogenes oder regelmäßiges „Algorithm Auditing“ technisch möglich ist („auditability by design“).[313] Bei besonders gefahrträchtigen Anwendungen könnte darüber hinaus verlangt werden, dass auch andere normative Vorgaben bei der Entwicklung von ADM-Systemen berücksichtigt werden („legality by design“).[314]

3. Präventive Kontrolle

Besonders gefahrträchtige ADM-Systeme sollten einer Vorabgenehmigung unterliegen.[315] Bei selbstlernenden Systemen, die sich im Laufe des Betriebs an ihre Umwelt anpassen, ist eine einmalige präventive Kontrolle jedoch nicht ausreichend. Als milderes Mittel zum Genehmigungsverfahren käme eine ADM-Folgenabschätzung (Algorithmic Impact Assessment) in Betracht, das über die Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) hinaus die zu erwartenden rechtlichen und gesellschaftlichen Auswirkungen des ADM-Systems prüft und dokumentiert.[316]

4. Marktbegleitende Kontrolle

Als Ergänzung zur präventiven Kontrolle sollte eine marktbegleitende Aufsicht für kritische ADM-Systeme eingeführt werden.[317] In Betracht kommen sowohl eine *externe* Kontrolle einzelner ADM-Systeme im Rahmen eines „Algorithm Auditing“ und anlassbezogene Sektoruntersuchungen. Zum anderen könnte erwogen werden, in den Unternehmen, die ADM-Systeme einsetzen, *interne* Prozesse für ein adäquates Risikomanagement einzuführen, deren Einhaltung durch einen Algorithmenbeauftragten überwacht wird.[318]

5. Selbstregulierung und Zivilgesellschaft

Private Selbstregulierung in Form von Selbstverpflichtungen, Branchenkodizes, Gütesiegeln und vor allem DIN/EN/ISO-Normen können die zuvor genannten Ansätze begleiten und unterstützen.[319] Nach

[312] Siehe dazu Abschnitt 3.2.
[313] Siehe dazu Abschnitt 3.4.1.
[314] Siehe dazu Abschnitt 3.2.2.
[315] Siehe dazu Abschnitt 3.3.1.
[316] Siehe dazu Abschnitt 3.3.2.
[317] Siehe dazu Abschnitt 3.4.1.
[318] Siehe dazu Abschnitt 3.4.3.
[319] Siehe dazu Abschnitt 3.5.

dem Vorbild des im Produktsicherheitsrecht seit langem etablierten „New Approach“ wäre es denkbar ADM-Systeme, die einer harmonisierten europäischen Norm entsprechen mit einer Konformitätsvermutung zu versehen. Eine flankierende Rolle kommt zivilgesellschaftlichen Initiativen wie etwa AlgorithmWatch zu.[320]

[320] Siehe dazu Abschnitt 3.7.

LITERATURVERZEICHNIS

Alle Internetquellen wurden zuletzt am 28.2.2018 abgerufen.

Adler et al. Auditing Black-box Models for Indirect Influence, IEEE International Conference on Data Mining, December 2016, http://sorelle.friedler.net/papers/auditing_icdm_2016.pdf.

AI Now Institute, Algorithmic Impact Assessments: Toward Accountable Automation in Public Agencies (21.2.2018), https://medium.com/@AINowInstitute/algorithmic-impact-assessments-toward-accountable-automation-in-public-agencies-bd9856e6fdde.

Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Baden-Baden 2017.

Athey/Catalini/Tucker, The Digital Privacy Paradox: Small Money, Samll Costs, Small Talk, NBER Working Paper No. 23488 (2017), http://www.nber.org/papers/w23488.

Bakshy/Messing/Adamic. Exposure to ideologically diverse news and opinion on Facebook. 348 Science, 1130-1132, (2015).

Bar-Gill/Ben-Shahar, Regulatory techniques in consumer protection: a critique of European consumer contract law, CML Rev. 2013, 109.

Beckedahl, Algorithmen gegen den Hass, Süddeutsche Zeitung v. 29.7.2017, S. 9.

Becker et al., Medicina ex Machina: Machine Learning in der Medizin, 107 Praxis: Schweizerische Rundschau für Medizin 19-23 (2018), https://doi.org/10.1024/1661-8157/a002920.

Beining, Wie Daten und Algorithmen die Rahmenbedingungen für das Gemeinwohl verändern, Stiftung Neue Verantwortung (Juni 2017).

Ben-Shahar/Schneider, More than you wanted to know, Princeton 2014.

Ben-Shahar/Chilton, Simplification of Privacy Disclosures: An Experimental Test, 45:S2 Journal of Legal Studies, S41-S67 (2016).

Beresford/Kübler/Preibusch, Unwillingness to pay for privacy: a field experiment, SFB 649 discussion paper, No. 2011-010.

Bernard, Komplizen des Erkennungsdienstes: Das Selbst in der digitalen Kultur, Frankfurt am Main 2017.

Bertelsmann Stiftung (Hrsg.) Wenn Maschinen Menschen bewerten: Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung, 2017.

Beuth, Notwehr against the machine, Die ZEIT (28.12.2017), http://www.zeit.de/digital/internet/2017-12/34c3-chaos-computer-club-kuenstliche-intelligenz.

Binns, Algorithmic Accountability and Public Reason, Philosophy & Technology (2017) https://doi.org/10.1007/s13347-017-0263-5.

Bitkom, Entscheidungsunterstützung mit Künstlicher Intelligenz - Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung (2017), https://www.bitkom.org/Bitkom/Publikationen/Entscheidungsunterstuetzung-mit-Kuenstlicher-Intelligenz-Wirtschaftliche-Bedeutung-gesellschaftliche-Herausforderungen-menschliche-Verantwortung.html.

BMVI (Hrsg.), Bericht der Ethikkommission Automatisiertes und vernetztes Fahren (Juni 2017), https://www.bmvi.de/SharedDocs/DE/Publikationen/G/bericht-der-ethik-kommission.pdf?__blob=publicationFile

Born, Bonitätsprüfungen im Online-Handel - Scorewert-basierte automatisierte Entscheidung über das Angebot von Zahlungsmöglichkeiten, ZD 2015, 66.

Braun Binder, Vollautomatisierte Verwaltungsverfahren im allgemeinen Verwaltungsrecht? Der Gesetzentwurf zur Modernisierung des Besteuerungsverfahrens als Vorbild für vollautomatisierte Verwaltungsverfahren nach dem VwVfG, NVwZ 2016, 960.

Bräutigam/Schmidt-Wudy,CR 2015, 56.

Bundeskartellamt und Autorité de la concurrence, Arbeitspapier Competition Law and Data, Mai 2016.

Buolamwini/Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Conference on Fairness, Accountability and Transparency, 2018, S. 77.

Busch/Reinhold, Standardisation of Online Dispute Resolution Services: Towards a More Technological Approach, (2015) Journal of European Consumer and Market Law 50.

Busch, Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy, in: De Franceschi (ed.), European Contract Law and the Digital Single Market: Implications of the Digital Revolution, Intersentia, Cambridge 2016, S. 223.

Busch, The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data, in: Christian Twigg-Flesner (ed.), Research Handbook on EU Consumer and Contract Law, Cheltenham 2016, S. 221.

Busch, Towards a „New Approach" in European Consumer Law: Standardisation and Co-Regulation in the Digital Single Market (2016) Journal of European Consumer and Market Law 197.

Butler, When Google got flu wrong. 494 Nature 155 (2013).

Cable/Edwards, Complementary and Supplementary Fit: A Theoretical and Empirical Integration, 89 Journal of Applied Psychology 822 (2004).

Campbell-Verduyn/Goguen/Porter, Big Data and algorithmic governance: the case of financial practices, 22 New Political Economy, 219 (2017).

Cavoukian, "Privacy by design" Take the challenge. Information and privacy commissioner of Ontario, Canada (2009).

CDU/CSU (2017) Für ein Deutschland, in dem wir gut und gerne leben, Regierungsprogramm 2017-2021, https://www.cdu.de/system/tdf/media/dokumente/170703regierungsprogramm2017.pdf?file=1

Chen/Mislove/Wilson, An Empirical Analysis of Algorithmic Pricing on Amazon Marketplace, Proceedings of the 25th International Conference on World Wide Web, 1339 (2016).

Conseil d'État, Puissance publique et plateformes numériques: accompagner l'"ubérisation", La Documentation Française, 2017.

Crawford, Artificial Intelligence's White Guy Problem, New York Times (25.6.2016), http://nyti.ms/28YaKg7.

von Czettritz/Strelow, „Beam me up, Scotty" – die Klassifzierung von Medical Apps als Medizinprodukte. PharmR 2017, 433.

Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997.

Datta et al. Discrimination in Online Advertising: A Multidisciplinary Inquiry, 81 Proceedings of Machine Learning Research 1 (2018).

Datta/Sen/Zick, 'Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems' (2016) Proceedings of the 2016 IEEE Symposium on Security and Privacy 598.

Datta/Tschantz/Datta, Automated experiments on ad privacy settings, Proceedings on Privacy Enhancing Technologies 92 (2015).

De Geest, Encyclopedia of Law and Economics, Cheltenham 2012.

Deloitte, Neue Spielregeln im digitalen Zeitalter, Global Human Capital Trendstudie 2017, Deutschland Report, [ohne Ort] 2017.

Deuster, Automatisierte Entscheidungen nach der Datenschutz-Grundverordnung, PinG 2016, 75.

Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als individuelle Freiheitsgstaltung, Berlin 2017.

Diakopoulos/Deussen, Brauchen wir eine Rechenschaftspflicht für algorithmische Entscheidungen?, Informatik Spektrum 2017, 362.

Diakopoulos, Algorithmic Accountability Reporting: On the Investigation of Black Boxes, Tow Center for Digital Journalism, 2014, http://towcenter.org/wp-content/uploads/2014/02/78524_Tow-Center-Report-WEB-1.pdf.

Diakopoulos, Algorithmic accountability: Journalistic investigation of computational power structures, 3 Digital Journalism 398 (2015).

Diakopoulos, Accountability in Algorithmic Decision Making, 59 Communications of the ACM 56 (2016).

Diakopoulos/Friedler, How to Hold Algorithms Accountable, MIT Technology Review (17.11.2016), https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/.

Die Grünen, Zukunft wird aus Mut gemacht, Bundestagswahlprogramm 2017.

Die Linke, Sozial. Gerecht. Frieden. Für Alle. Die Zukunft für die wir kämpfen, Langfassung des Wahlprogramms zur Bundestagswahl 2017.

Dienlin/Trepte, Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors, 45 European Journal of Social Psychology 285 (2015).

Dohrn/Huck, Der Algorithmus als „Kartellgehilfe"? – Kartellrechtliche Compliance im Zeitalter der Digitalisierung, DB 2018, 173.

Domingos, The Master Algorithm: How the Quest for the Ultimate Learning Machine will Remake Our World, New York 2015.
Doshi-Velez/Kim A roadmap for a rigorous science of interpretability. arXiv preprint arXiv:1702.08608 (2017).
Drexl, Bedrohung der Meinungsvielfalt durch Algorithmen, ZUM 2017, 529.
Dugas et al, Influenza forecasting with Google flu trends, PloS one (2013), https://doi.org/10.1371/journal.pone.0056176.
Duhigg, How Companies Learn Your Secrets, New York Times (16.2.2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
Dzida, Big Data und Arbeitsrecht, NZA 2017, 541.
Ebers, Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten? NZKart 2016, 554.
Edwards/Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16 Duke Law & Technology Review 18 (2017).
Ehmann/Selmayr/Albrecht (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München 2017.
Eifert, Rechenschaftspflicht für soziale Netzwerke und Suchmaschinen: Zur Veränderung des Umgangs von Recht und Politik mit dem Internet, NJW 2017, 1450.
Esteva et al. Dermatologist-level classification of skin cancer with deep neural networks, 542 Nature 115 (2017).
Ezrachi/Stucke, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy, Harvard University Press, Cambridge 2016.
Ezrachi/Stucke, Algorithmic Collusion: Problems and Counter-Measures, OECD DAF/COMP/WD(2017)25 (Mai 2017).
FDP (2017) Denken wir neu. Das Programm der Freien Demokraten zur Bundestagswahl 2017: „Schauen wir nicht länger zu“, https://www.fdp.de/sites/default/files/uploads/2017/08/07/20170807-wahlprogramm-wp-2017-v16.pdf.
Ferlemann, Gesundheitsentscheidungen durch Algorithmen – rechtliche Rahmenbedingungen der Digitalisierung des Gesundheitswesens, NZS 2018, 56.
Flaxman/Goel/Rao, Filter bubbles, echo chambers, and online news consumption, 80 Public Opinion Quarterly 298 (2016).
Floridi, Tolerant paternalism: pro-ethical design as a resolution of the dilemma of toleration, 22 Science and Engineering Ethics 1669 (2016).
G’sell, Le Conseil d’État et les plateformes: de l’“ubérisation“ à un programme d’action – A propos de l’étude annuelle 2017 du Conseil d’État, La Semaine juridique, Édition générale, N. 43, 23 Octobre 2017, S. 1926.
Gassner, Software als Medizinprodukt – zwischen Regulierung und Selbstregulierung, MPR 2016, 109.
Gersdorf, Brauchen wir ein digitales AGG?, NJW-Aktuell 31/2017, 3.
Gillespie, Algorithm, in: Peters (ed.) Digital keywords: a vocabulary of information society and culture, Princeton University Press, Princeton 2016.
Gola (Hrsg.) Datenschutz-Grundverordnung, Kommentar, München 2017.
Gomez-Uribe/Hunt, The Netflix Recommender System: Algorithms Business Value and Innovation, ACM Trans, 6 Management Information Systems 1 (2016).
Goodman/Flaxman, European Union regulations on algorithmic decision-making and a" right to explanation", arXiv preprint arXiv:1606.08813 (2016).
Gounalakis, Rechtliche Grenzen der Autocomplete-Funktion von Google, NJW 2013, 2321.
Graf, Revision des europäischen Rechtsrahmens für Medizinprodukte: Einfluss auf die Klassifizierung von Medizinprodukten, PharmR 2017, 57.
Grünberger, Personale Gleichheit, Baden-Baden 2013.
Halfmeier, Die neue Datenschutzverbandsklage, NJW 2016, 1126.
Heinemann/ Wäßle, Datenschutzrechtlicher Auskunftsanspruch bei Kreditscoring: Inhalt und Grenzen des Auskunftsanspruchs nach § 34 BDSG, MMR 2010, 600
Helberger, Diversity by design, 1 Journal of Information Policy 1, 441 (2011).
Helberger, Merely Facilitating or Actively Stimulating Diverse Media Choices? Public Service Media at the Crossroad, 9 International Journal of Communication 1324 (2015).
Helbich, Rechtsfragen der „automatisierten“ Ermessensausübung im Steuerrecht, DStR 2017, 574.
Henelius et al. ‘A Peek Into the Black Box: Exploring Classifiers by Randomization’ 28 Data Mining and Knowledge Discovery 1503 (2014).

Heun, Grundlegende Algorithmen: Einführung in den Entwurf und die Analyse effizienter Algorithmen, 2. Auflage, Wiesbaden 2013.

Hoeren (Hrsg.), Big Data und Recht, München 2014.

Hoffmann-Riem, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017) 1.

Holthaus/Park/Stock-Homburg, People Analytics und Datenschutz – Ein Widerspruch?, DuD 2015, 676.

Israni, When an algorithm helps send you to prison, New York Times (26.10.2017), https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html.

Jaskulla, Das deutsche Hochfrequenzhandelsgesetz – eine Herausforderung für Handelsteilnehmer und Multilaterale Handelssysteme (MTF), BKR 2013, 221.

Jones, The right to a human in the loop: Political constructions of computer automation and personhood, 47 Social studies of science 216 (2017).

Kettner/Thorun/Vetter, Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz (2018), https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf.

Kerkmann, Microsoft will den moralischen Programmierer, Handelsblatt (23.1.2018), http://www.handelsblatt.com/my/unternehmen/it-medien/furcht-vor-kuenstlicher-intelligenz-microsoft-will-den-moralischen-programmierer/20877112.html.

Kim, Auditing Algorithms for Discrimination, 166 University of Pennsylvania Law Review Online, 189 (2017).

Kim/Routledge, Algorithmic transparency, a right to explanation and trust, Working Paper, Carnegie Mellon University (June 2017).

Kindermann/Coridaß, Der rechtliche Rahmen des algorithmischen Handels inklusive des Hochfrequenzhandels, ZBB, 178.

Klimas/Vaiciukaite, The Law of Recitals in European Community Legislation, 15 ILSA Journal of International & Comparative Law 32 (2008)

Klingel/Lischka, Was die Wahlprogramme über Maschinen sagen, die Menschen bewerten, https://algorithmenethik.de/2017/09/11/was-die-wahlprogramme-ueber-maschinen-sagen-die-menschen-bewerten/.

Körber, Das Bundeskartellamt auf dem Weg zur Digitalagentur?, WuW 2018, 173.

Kraska, Datenschutz-Zertifizierungen in der EU-Datenschutzgrundverordnung, ZD 2016, 153.

Kroll/Hue/Barocas/Felten/Reidenberg, Robinson & Yu, 165 Accountable Algorithms, University of Pennsylvania Law Review, 633 (2017).

Kühling/Gauß, Suchmaschinen – eine Gefahr für den Informationszugang und die Informationsvielfalt?, ZUM 2007, 881.

Kühling/Martini: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448.

Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München 2017.

Lambrecht/Tucker, Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads (November 30, 2017), https://ssrn.com/abstract=2852260

Lammerant/Blok/de Hert, Big data en gelijke behandeling, in: Blok (ed.) Big data & het recht. Sdu Uitgevers 115 (131).

Lazer et al. The parable of Google Flu: traps in big data analysis. 343 Science 1203 (2014).

Leenes/Lucivero, Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design, 6 Law, Innovation and Technology, 193 (2016).

Lepri, Oliver, Letouzé, Pentland & Vinck, Fair, Transparent, and Accountable Algorithmic Decision-making ProcessesPhilos. Technol. (2017). https://doi.org/10.1007/s13347-017-0279-x.

von Lewinski/Pohl, Auskunfteien nach der europäischen Datenschutzreform, ZD 2018, 17.

Li et al, Analyzing and Detecting Opinion Spam on a Large-Scale Dataset via Temporal and Spatial Patterns, ICWSM 634 (2015).

Linden/Smith, Amazon.com Recommendations: Item- to-Item Collaborative Filtering, 7 IEEE Internet Computing 76 (2003).

Linden et al., Collaborative Recommendations Using Item-to-Item Similarity Mappings, US Patent 6,266,649, to Amazon.com, Patent and Trademark Office, 2001 (filed 1998).

Lipton, The Mythos of Model Interpretability, ICML Workshop on Human Interpretability in Machine Learning, arXiv:1606.0490 (2016).
Maas, Unsere digitalen Grundrechte (10.12.2015), http://www.bmjv.de/SharedDocs/Interviews/DE/2015/Namensartikel/12092015_DieZeit.html.
Maas, Zusammenleben in der digitalen Gesellschaft, DANA 2017, 156.
Martini/Nink, Wenn Maschinen entscheiden... vollautomatisierte Verwaltungsverfahren und Persönlichkeitsschutz, NVwZ 2017, 681 [Kurzfassung]
Martini/Nink, Wenn Maschinen entscheiden... vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ-Extra 10/2017, 1.
Martini, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017.
Matzat, Rechenschaft für Rechenverfahren, Tendenz 2/2017, https://www.blm.de/infothek/magazin_tendenz/tendenz-2_2017/algorithmen-tendenz_2_17.cfm.
Mayer-Schönberger/Cukier, Big Data: Die Revolution, die unser Leben verändern wird, München 2013.
Metz, Scoring: New Legislation in Germany (2012) 35 Journal of Consumer Policy, 297.
Metzger, Extra legem, intra ius: Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, Tübingen 2009.
Micklitz, Ungeheuerliche Neuigkeiten? VuR 2017, 43.
Miller, Explanation in artificial intelligence: Insights from the social sciences, arXiv preprint arXiv:1706.07269 (2017).
Mittelstadt et al. The ethics of algorithms: Mapping the debate. 3 Big Data & Society, 1 (2016).
Mittelstadt, Automation, Algorithms, and Politics| Auditing for Transparency in Content Personalization Systems, 10 International Journal of Communication 12 (2016).
Moos/Rothkegel, Nutzung von Scoring-Diensten im Online-Versandhandel: Scoring-Verfahren im Spannungsfeld von BDSG, AGG und DS-GVO, ZD 2016, 561.
Möslein, Digitalisierung im Gesellschaftsrecht: Unternehmensleitung durch Algorithmen und künstliche Intelligenz? ZIP 2018, 204.
O'Neil, Angriff der Algorithmen, Hanser: München 2017.
O'Neil, Weapons of Math Destruction: How Big Data Increases Inequlity and Threatens Democracy, Crown, New York 2016.
OECD, Algorithms and Collusion: Competition Policy in the Digital Age, 2017.
Ortner/Daubenbüchel, Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918.
Paal/Hennemann, Meinungsvielfalt im Internet: Regulierungsoptionen in Ansehung von Algorithmen, Fake News und Social Bots, ZRP 2017, 76.
Pall/Hennemann, Big Data as an Asset: Daten und Kartellrecht, ABIDA-Gutachten, 2018.
Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2. Auflage, München 2018.
Page/Brin/Motwani/Winograd, The pagerank citation ranking: Bringing order to the web. Technical report, Stanford InfoLab (1999), http://ilpubs.stanford.edu:8090/422/1/1999-66.pdf.
Pariser, The Filter Bubble: What The Internet Is Hiding From You, New York 2011.
Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Cambridge 2015.
Perel/Elkin-Koren, Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. 69 Florida Law Review 181 (2017).
Plath (Hrsg.), BDSG/DSGVO, Kommentar, 2. Auflage, Köln 2016.
Pöchhacker et al., Interventionen in die Produktion algorithmischer Öffentlichkeiten: Recommender Systeme als Herausforderung für öffentlich-rechtliche Sendeanstalten, 18 kommunikation@ gesellschaft, 25 (2017), https://www.ssoar.info/ssoar/handle/document/51500.
Podszun/de Toma, Die Durchsetzung des Datenschutzes durch Verbraucherrecht, Lauterkeitsrecht und Kartellrecht, NJW 2016, 2987.
Podszun, The Digital Economy: Three Chances for Competition Law, 23 Maastricht Journal of European and Comparative Law, 747 (2016).
ProPublica, Machine Bias (23.5.2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
Rademacher, Predictive Policing im deutschen Polizeirecht, AöR 142 (2017) 366.
Reece/Danforth, Instagram photo reveal predictive markers of depression, 6 EPJ Data Science 15 (2017).
Reichwald/Pfisterer, Autonomie und Intelligenz im Internet der Dinge, CR 2016, 208.

Resnick/Garrett/Kriplean/Munson/Stroud, Bursting your (filter) bubble : Strategies for promoting diverse exposure, in: Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion, CSCW 95 (2013).

Reviglio, Serendipity by Design? How to Turn from Diversity Exposure to Diversity Experience to Face Filter Bubbles in Social Media, in: Kompatsiaris et al. (eds.) International Conference on Internet Science, INSCI 2017, Springer 2017, 281.

Ribeiro/Singh/Guestrin, 'Why Should I Trust You?: Explaining the Predictions of Any Classifier', Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 1135 (2016).

Ritter/Schwichtenberg, Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizites – neuer Weg, neue Chance, VuR 2016, 95.

Rohde, In Australien prüft eine Software die Sozialbezüge – und erfindet Schulden für 20.000 Menschen (25.10.2017), https://algorithmenethik.de/2017/10/25/in-australien-prueft-eine-software-die-sozialbezuege-und-erfindet-schulden-fuer-20-000-menschen/.

Rosenblat/Kneese/Boyd, Algorithmic Accountability, A workshop primer produced for: The Social, Cultural & Ethical Dimensions of „Big Data" (17.3.2014), https://ssrn.com/abstract=2535540.

Roßnagel/Nebel/Richter, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455.

Rusche, Gefahr für digitale Geschäftsmodelle (3.7.2017), https://www.iwkoeln.de/presse/iw-nachrichten/beitrag/christian-rusche-gefahr-fuer-digitale-geschaeftsmodelle-347922.html.

Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt (Dezember 2016), http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_SVRV-.pdf.

Sandvig et al., Auditing algorithms: Research methods for detecting discrimination on internet platforms, in: Data and discrimination: converting critical concerns into productive inquiry 1 (2014).

Saurwein/Just/Latzer, Governance of algorithms: options and limitations, 17 Info 35 (2015).

Schaar, Algorithmentransparenz, in: Alexander Dix et al. (Hrsg.) Informationsfreiheit und Informationsrecht Jahrbuch 2015, Berlin 2016, S. 23.

Schäffter, Verfahrensverzeichnis 2.0, Datenschutzdokumentation konform zur EU-Datenschutzgrundverordnung gestalten, [ohne Ort] 2016.

Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841.

Schantz/Wolff, Das neue Datenschutzrecht, München 2017.

Schmitz/Prell, Neues zum E-Government: Rechtsstaatliche Standards für E-Verwaltungsakt und E-Bekanntgabe im VwVfG, NVwZ 2016, 1273.

Schneider, Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus? Überlegungen, wie weit die Untersagung bei besonderen Datenkategorien reicht, ZD 2017, 303.

Schulte-Nölke/BMJV (Hrsg.), Neue Wege zur Durchsetzung des Verbraucherrechts, Berlin 2017.

Schulz/Dankert, Die Macht der Informationsintermediäre (2016) http://library.fes.de/pdf-files/akademie/12408.pdf.

Seyfert/Roberge, Was sind Algorithmuskulturen, in: dies. (Hg.) Algorithmuskulturen: Über die rechnerische Konstruktion der Wirklichkeit, Transcript: Bielefeld 2017.

Sharma/Hofman/Watts, Estimating the Causal Impact of Recommendation Systems from Observational Data, in: Proceedings of the 16th ACM Confererence on Economics and Computation, 453 (2015).

Smith/Linden, Two decades of recommender systems at Amazon. com." 21 IEEE Internet Computing 12 (2017).

Son, JPMorgan algorithm knows you're a rogue employee before you do, Bloomberg Business (8.4.2015), www.bloomberg.com/news/articles/2015-04-08/jpmorgan-algorithm-knows-you-re-a-rogue-employee-before-you-do.

SPD (2017) Zeit für mehr Gerechtigkeit. Unser Regierungsprogramm für Deutschland, https://www.spd.de/fileadmin/Dokumente/Regierungsprogramm/SPD_Regierungsprogramm_BTW_2017_A5_RZ_WEB.pdf.

Spiegel et al., Method and system for anticipatory package shipping, U.S. Patent No. 8,271,398. 18 Sep. 2012.

Spielkamp, AlgorithmWatch: What Role Can a Watchdog Organization Play in Ensuring Algorithmic Accountability?, in: Cerquitelli, Quercia & Pasquale (Hrsg.), Transparent Data Mining for Big and Small Data, 2017, S. 207.

Spielkamp, Sind Algorithmen die besseren Richter, Technology Review (16.10.2017), https://www.heise.de/tr/artikel/Sind-Algorithmen-die-besseren-Richter-3861814.html.

Spindler, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937.

Spindler, Regulierung durch Technik, Kurzgutachten für den Sachverständigenrat für Verbraucherfragen (Dezember 2016), http://www.svr-verbraucherfragen.de/wp-content/uploads/Spindler-Gutachten.pdf.

Spindler, Verbandsklagen und Datenschutz – das neue Verbandsklagerecht: Neuregelungen und Probleme, ZD 2016, 114.

Spindler/Thorun, Die Rolle der Ko-Regulierung in der Informationsgesellschaft: Handlungsempfehlung für eine digitale Ordnungspolitik, MMR-Beilage, Heft 6/2016, 1.

Spindler, Zukunft der Digitalisierung – Datenwirtschaft in der Unternehmenspraxis, DB 2018, 41

Stark, Meinungsbildung im Netz: Die Macht der Algorithmen, MMR 2017, 721.

Stucke/Ezrachi, Is Your Digital Assistant Devious?, Oxford Legal Studies Research Paper No. 52/2016 (September 2016), https://ssrn.com/abstract=2828117.

Taddicken, The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure, 19 Journal of Computer Mediated Communication, 248 (2014).

Taeger, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, 72.

Taeger, Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, 3.

Takahashi/Zhang, Towards Bursting Filter Bubble via Contextual Risks and Uncertainties. arXiv preprint arXiv:1706.09985 (2017).

Tutt, An FDA for Algorithms 69 Admin. L. Rev. 83 (2017).

Utz/Krämer, The privacy paradox on social network sites revisited: The role of individual characteristics and group norms, 3 Journal of Psychosocial Research on Cyberspace 2 (2009), <https://cyberpsychology.eu/article/view/4223/3265>.

Vezzoso, Competition by Design (28.11.2017). Prepared for Presentation at 12th ASCOLA Conference, Stockholm University, 15-17 June 2017, https://ssrn.com/abstract=2986440.

VZBV, Algorithmenbasierte Entscheidungsprozesse (7.12.2017), https://www.vzbv.de/sites/default/files/downloads/2017/12/14/17-12-05_vzbv_thesenpapier_algorithmen.pdf.

Wachter/Mittelstadt/Floridi, Why a Right to Explanation of Automated-Decision Making Does Not Exist in the General Data Protection Regulation, 7 International Data Privacy Law 76 (2017).

Wachter/Mittelstadt/Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR (October 6, 2017). Harvard Journal of Law & Technology (forthcoming), https://ssrn.com/abstract=3063289.

Wagner, Neue Perspektiven im Schadensersatzrecht, Verhandlungen des 66. DJT, Gutachten A, Bd. 1, München 2006.

Weichert, Scoring in Zeiten von Big Data, ZRP 2014, 168.

Weichert, Big Data im Gesundheitsbereich, ABIDA-Gutachten, 2018.

Weitzel/Laumer/Maier/Oehlhorn/Wirth/Weinert, Active Sourcing und Social Recruiting. Ausgewählte Trends der Recruiting Trends 2017, Studie im Auftrag der Monster GmbH, Bamberg 2017.

Wolf, The Data-Driven Life, New York Times Magazine (28.4.2010), http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html.

Wolff/Brink (Hrsg.) BeckOK Datenschutzrecht, 22. Edition (Stand: 1.11.2017), München 2017.

World Wide Web Foundation, Algorithmic Accountability: Applying the concept to different country contexts (Juli 2017), http://webfoundation.org/docs/2017/07/Algorithms_Report_WF.pdf.

Ylinen, Digital Pricing und Kartellrecht, NZKart 2018, 19.

Zech, Gefährdungshaftung und neue Technologien, JZ 2013, 21.

Zweig, Arbeitspapier: Überprüfbarkeit von Algorithmen (7.7.2016), https://algorithmwatch.org/de/zweites-arbeitspapier-ueberpruefbarkeit-algorithmen/.

Zweig/Deussen/Krafft, Algorithmen und Meinungsbildung: Eine grundlegende Einführung, Informatik Spektrum 2017, 318.

Zweig, Wo Maschinen irren können – Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung, Arbeitspapier der Bertelsmann-Stiftung, Februar 2018; https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WoMaschinenIrrenKoennen.pdf.