SABINE SCHÄUFLER

Regulierung von Systemen Künstlicher Intelligenz durch die DSGVO

Schriften zum Recht der Digitalisierung
28

Mohr Siebeck

Schriften zum Recht der Digitalisierung

Herausgegeben von
Florian Möslein, Sebastian Omlor und Martin Will

28

Sabine Schäufler

Regulierung von Systemen Künstlicher Intelligenz durch die DSGVO

Mohr Siebeck

Sabine Schäufler, geboren 1989; Studium der Rechtswissenschaft in München und Bordeaux; 2016 Erste Juristische Staatsprüfung; Referendariat in München und Luxemburg; 2018 Zweite Juristische Staatsprüfung; wissenschaftliche Mitarbeiterin am Lehrstuhl für Staats- und Verwaltungsrecht, Europarecht und Völkerrecht an der Eberhard Karls Universität Tübingen; 2023 Promotion; Richterin auf Probe am Bayerischen Verwaltungsgericht Augsburg.
orcid.org/0009-0006-4323-5549

D21

ISBN 978-3-16-163315-7 / eISBN 978-3-16-163316-4
DOI 10.1628/978-3-16-163316-4

ISSN 2700-1288 / eISSN 2700-1296 (Schriften zum Recht der Digitalisierung)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.

Publiziert von Mohr Siebeck Tübingen 2024. www.mohrsiebeck.com

Das Buch wurde auf alterungsbeständiges Werkdruckpapier gedruckt.

Printed in Germany.

Für Heinz und Marianne Menzel

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2023 von der Juristischen Fakultät der Eberhard-Karl-Universität Tübingen als Dissertation angenommen. Für die Drucklegung ist die bis Juni 2023 veröffentlichte Literatur und Rechtsprechung berücksichtigt worden.

Mein besonderer Dank gilt meinem Doktorvater und akademischen Lehrer Herrn Prof. Dr. Martin Nettesheim für seine hervorragende Betreuung. Er hat mich zu jeder Zeit des Promotionsprozesses fachlich wie persönlich engagiert gefördert und unterstützt und mir die Freude am rechtswissenschaftlichen Denken und Arbeiten vermittelt. Für die wertschätzende Zusammenarbeit und die mir gewährte akademische Freiheit an seinem Lehrstuhl bin ich sehr dankbar.

Herrn Professor Dr. Jochen von Bernstorff, LL.M., danke ich für die rasche Erstellung des Zweitgutachtens und für die wertvollen Anmerkungen in seinem Gutachten. Herrn Professor Dr. Stefan Thomas danke ich für die freundliche und anregende Leitung der Disputatio. Den Herausgebern danke ich herzlich für die freundliche Aufnahme in die Schriftenreihe zum Recht der Digitalisierung.

Danken möchte ich überdies Frau Professorin Dr. Michèle Finck, LL.M., in deren Seminar ich meine Thesen vorstellen durfte. Von ihrem persönlichen Feedback und den Anregungen der SeminarteilnehmerInnen habe ich sehr profitiert. Gedankt sei auch Frau Professorin Dr. Iris Eisenberger M.Sc. (LSE) und Herrn Dr. Nikolaus Pöchhacker für die konstruktive Diskussion meines Forschungsprojekts in ihrer Arbeitsgruppe. Herr Professor Dr. Dres. h.c. Hans-Jürgen Papier hat während meiner Tätigkeit als Hilfskraft an der Ludwig-Maximilans-Universtität München mein Interesse an der Rechtswissenschaft maßgeblich geweckt und mich vielseitig gefördert. Dafür bin ich sehr dankbar.

Zahlreiche Personen haben mich während der Erstellung der Arbeit begleitet und zum Gelingen dieser Arbeit beigetragen. Einige möchte ich beispielhaft erwähnen. Zu großem Dank verpflichtet bin ich Herrn PD Dr. Andreas Kulick, der mir zu jeder Zeit mit wertvollem Rat und einem offenen Ohr zur Seite stand. Meinen KollegInnen am Lehrstuhl und an der Juristischen Fakultät danke ich für ihre Unterstützung jeglicher Art und für die äußerst vergnügliche gemeinsame Zeit. Besonders danken möchte ich meinen KollegInnen Herrn Laurenz Eichhorn, Herrn Christoph Fischer, Frau Marie-Sophie Müller und Frau Leonie Schmitt für unzählige erkenntnisreiche Gespräche. Mein herzlicher Dank gilt überdies Frau Dr. Tamara Schneider für ihre Ermutigung und

ihre praktische Hilfestellung. Meinen ehemaligen KollegInnen an der Ludwig-Maximilians-Universität Herrn Dr. Julian Eibl, Frau Veronika Foerst, Herrn Dr. Stefan Herrmann, Herrn Prof. Dr. Michael W. Müller, M.A., LL.M., und Herrn Dr. Markus Vordermayer, LL.M., danke ich für viele hilfreiche Denkanstöße und ihren stetigen Zuspruch. Nicht genug danken kann ich Frau Dr. Corinne Dialer, Herrn Christoph Fischer, Herrn Dr. Stefan Herrmann, Herrn Markus Schäufler, Herrn Dr. Markus Vordermayer, LL.M., und Frau Imogen Willers für ihr wertvolles Feedback zu meiner Arbeit und ihren stetigen Rückhalt. Herrn Uwe Geis-Schroer, Herrn Lars-Henrik Kahle, Herrn Lino Santuario und Frau Maria Vrettou danke ich für ihre lektorierende Unterstützung. Nicht zuletzt möchte ich Frau Julia Wagner vom Dekanat der Juristischen Fakultät für ihre zuvorkommende Begleitung des Promotionsprojekts danken. Frau Dr. Julia Caroline Scherpe-Blessing LL.M. und dem gesamten Team des Mohr Siebeck Verlags danke ich für ihre engagierte Begleitung des Veröffentlichungsprozesses.

Besonderer Dank gebührt meiner Familie. Mir ist bewusst, wie privilegiert ich bin, dass ich eine Doktorarbeit habe verfassen dürfen. Ohne ihr Zutrauen und ihre Unterstützung wäre dies nicht möglich gewesen. Schließlich möchte ich meinen Wahlgroßeltern, Heinz und Marianne Menzel, von ganzem Herzen danken. Sie haben weit früher und beständiger an die Vollendung dieses Projekts geglaubt als ich selbst und mich immer wieder neu motiviert. In ihrem Optimismus, ihrer Neugier und ihrem Humanismus sind sie mir großes Vorbild. Ihnen ist dieses Buch gewidmet.

Tübingen, November 2023 *Sabine Schäufler*

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA	anderer Ansicht
ABl.	Amtsblatt der Europäischen Union
ACM	Association of Computing Machinery
AcP	Archiv für die civilistische Praxis
AfP	Zeitschrift für Medien- und Kommunikationsrecht (zuvor: Archiv für Presserecht)
AöR	Archiv des öffentlichen Rechts
aE	am Ende
aF	alte Fassung
Artikel 29 Datenschutzgruppe	Gremium der unabhängigen Datenschutzbeauftragten der EU-Mitgliedstaaten und des europäischen Datenschutzbeauftragten nach Art. 29 DSRL
B2b	Business-to-Business
B2c	Business-to-Consumer
BB	Betriebsberater
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
BKR	Zeitschrift für Banken- und Kapitalmarktrecht
BT-Drs.	Bundestags-Drucksache
BTLJ	Berkeley Technology Law Journal
Cal. L. Rev.	California Law Review
Cam. L. rev.	Cambridge Law Review
CBLR	Columbia Business Law Review
CLSR	Computer Law and Security Review
Colum. Sci. & L. Rev.	Columbia Science and Technology Law Review
CR	Computer und Recht
CRi	Computer und Recht International
Datenschutzkonferenz	Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder
DMA	Digital Markets Act (Gesetz über digitale Märkte), Verordnung (EU) 2022/1925, ABl. L 265, 1
DPD	Data Protection Directive
DS	Data Science (Zeitschrift)
DSA	Digital Services Act (Gesetz über digitale Dienste), Verordnung (EU) 2022/2065, ABl L 277, 1

DSGVO	Datenschutzgrundverordnung, Verordnung (EU) 2016/679, ABl. L 119, 1
DSK	siehe Datenschutzkonferenz
DSRL	Datenschutzrichtlinie, Richtlinie EG 95/46, ABl. L 281, 31
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
EDPL	European Data Protection Law Review
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA	Europäischer Datenschutzausschuss
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention
E-Privacy-RL	Richtlinie 2002/58/EG des Europäischen Parlaments und desRates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutz-Richtlinie für elektronische Kommunikation), ABl. L 201 S. 37.
Erwgr.	Erwgrund/Erwgründe
Et al.	Et alii
EuCML	Journal of European Consumer and Market Law
Flo. L. Review	Florida Law Review
GDPR	General Data Protection Regulation (siehe DSGVO)
GrCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GLTR	Georgetown Law Technology Review
Harv. Law Review	Harvard Law Review
Harv. J. L. Technol.	Harvard Journal of Law and Technology
HS.	Halbsatz
ICC	International Review of Intellectual Property and Competition Law
ICLQ	International and Comparative Law Quarterly
iCS	Information, Communication and Society (Zeitschrift)
IDIS	Identity in the Information Society (Zeitschrift)
IDPL	International Data Privacy Law
IJAFRC	International Journal of Advance Foundation and Research in Computer
Int. J. Commun.	International Journal of Communication
Int. J. Hum. Comp.	International Journal of Human-Computer studies
Int. J. Inf. Technol.	International Journal of Law and Information Technology
IntTeR	Zeitschrift für Innovations- und Technikrecht
J. Consum. Policy	Journal of Consumer Policy
JAISE	Journal o Ambient Intelligence and Smart Environments
JIPITEC	Journal of Intellectual Property, Information Technology and Electronic Commerce
JZ	JuristenZeitung
KI-Gesetz-E	Vorschlag der Europäischen Kommission für eine Verordnung zur Festlegung harmoniiserter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz), COM/2021/206 final
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift

Northwest J. Tech. & Intell. Prop	Northwestern Journal of Technology and Intellectual Property
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZZ	Neue Züricher Zeitung
OECD	Organisation for Economic Co-operation and Development
PIMS	Personal Information Management System
Proc. IEEE	Proceedings of the Institute of Electrical and Electronics Engineers (Zeitschrift des Institute of Electrical and Electronics Engineers)
RDi	Recht Digital
RDV	Recht in der Datenverarbeitung (Zeitschrift)
Rich. J. L. Techn.	Richmond Journal of Law and Technology
RW	Rechtswissenschaft (Zeitschrift)
SSRN Journal	Social Science Research Network Journal
SZ	Süddeutsche Zeitung
U. Pa. L Rev.	University of Pennsylvania Law Review
VuR	Verbraucher und Recht
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
Yale J. L. & Tech.	Yale Journal of Law and Technology
Yale L. J.	Yale Law Journal
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZD	Zeitschrift für Datenschutz
ZEuP	Zeitschrift für Europäisches Privatrecht
ZfDR	Zeitschrift für Digitalisierung und Recht
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZGE	Zeitschrift für geistiges Eigentum
ZJS	Zeitschrift für das Juristische Studium
ZöR	Zeitschrift für öffentliches Recht
ZParl	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht

Siehe zu weiteren gängigen Abkürzungen Kirchner/Böttcher (Begr.), Abkürzungsverzeichnis der Rechtsprache, 10. Aufl. 2021, Berlin/Boston 2021

Einführung

A. Einleitung

Die Technologie der Künstlichen Intelligenz[1] erlebt aktuell mit der Verbreitung Maschineller Lernverfahren[2] einen neuen Frühling.[3] Selbstlernende Algo-

---

[1] Die Künstliche Intelligenz (KI) beschreibt einen interdisziplinären Forschungsbereich an der Schnittstelle von Kybernetik, Informatik und Computerwissenschaft, mit dem Ziel, ein System zu schaffen, das intelligent, rational und eigenständig Probleme lösen und agieren kann. Als Geburtsstunde gilt die im Jahr 1956 von John McCarthy und Marvin Minsky veranstaltete interdisziplinäre Konferenz „Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI)" des Massachusetts Institute of Technology (MIT), siehe die Konferenzankündigung. Siehe eingehend zur Geschichte der KI-Forschung *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 17–27; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 7–14. Dabei hat man fünf Bereiche intelligenten Verhaltens definiert, durch deren Automatisierung Künstliche Intelligenz hergestellt werden soll: logisches Schließen, Suchen, Planen, Wissen und Lernen, vgl. etwa die Gliederungen in den Lehrbüchern *Russell/Norvig*, Artificial Intelligence, [4]2021; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021. Sie stellen zugleich die historischen Entwicklungsstufen dieses Forschungsbereichs dar.

[2] Erste Ansätze dazu waren theoretisch bereits in den 1950er Jahren entwickelt worden. Aufgrund fehlender Datenmengen und unzureichender Soft- und Hardware konnten diese aber praktisch nicht realisiert werden. Vgl. *Skansi*, Introduction to deep learning, 2018, S. 8–11; *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 9 f.; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 105. Mit der Digitalisierung Ende des 20. Jahrhunderts änderten sich diese Ausgangsbedingungen grundlegend: Die hohe und kostengünstige Speicherfähigkeit und Rechenkraft der Hardware, die Verfügbarkeit großer Datenmengen (Big Data) und leistungsstarke Algorithmen ermöglichten die Erforschung und Entwicklung Maschineller Lernverfahren. Eingehend *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), 429; *Alpaydın*, Machine learning, 2021, S. 129 f. Siehe auch die Studie von *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 5 f.

[3] Vgl. *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 27. Siehe auch *Bringsjord/Govindarajulu*, in: Zalta (Hrsg.), The Stanford Encyclopedia of Philosophy, 2020, 4.1: „A huge part of AI's growth in applications has been made possible through invention of new algorithms in the subfield of machine learning". Von einem „new spring" sprechen auch *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 9.

rithmen[4] erschließen Anwendungsbereiche, die sich bislang nicht mit zufriedenstellenden Ergebnissen automatisieren ließen,[5] etwa die Bild- und Spracherkennung,[6] die Übersetzung[7] oder die Erstellung von Texten.[8] Verwendungsmöglichkeiten derartiger Algorithmen sind zahllos; sie kommen überall dort zum Einsatz, wo sich Dienste und Leistungen informationstechnisch abbilden lassen.[9] Von besonderem Interesse sind dabei Systeme der Künstlichen Intelligenz, die mehr oder weniger autonom mit dem Menschen interagieren. Die folgende Arbeit betrachtet eine bestimmte Art derartiger Systeme, nämlich personalisierte autonome Systeme. Diese bieten NutzerInnen personalisierte Leistungen an oder treffen automatisiert Entscheidungen über Personen. Anwendungsbeispiele sind Systeme, die die Angebote von Streamingdiensten nach

---

[4] Beim Maschinellen Lernen wird menschliches Lernen imitiert; Lösungsstrategien werden nicht vorgegeben, vielmehr leitet ein System durch Beobachtung der Umwelt selbst Regeln ab und entwickelt diese beständig fort. Bei selbstlernenden Algorithmen erfolgt dies durch Analyse von Daten. Siehe hierzu eingehend unter Kapitel 1 A. II.

[5] Mit tradierten, d.h. auf logischen Regeln gestützten wissensbasierten Systemen und Expertensystemen, auch als Good Old-Fashioned Artificial Intelligence (GOFAI) bezeichnet, so *Dignum*, Responsible Artificial Intelligence, 2019, S. 13, erzielte man zunächst gute Ergebnisse, siehe hierzu etwa *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 22–24; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 314–343; *Nebel/Wölfl*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 27 Man scheiterte aber in hochkomplexen Bereichen, in denen sich keine logischen, präzisen und statischen Regeln finden lassen, vgl. *Alpaydın*, Machine learning, 2021, S. 16. Dies führte zu einem Winter in der KI-Forschung.

[6] Tradierte Methoden, insbesondere wissensbasierte Systeme, kommen an Grenzen, da sich für Bilder und Sprache keine eindeutigen und abschließenden Regeln finden lassen. Vgl. *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 12; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 338–340. Ausführliche Darstellung auch bei *Menzel*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 601.

[7] Anschaulich *Lewis-Kraus*, The Great A.I. Awakening, The New York Times Magazine 18.12.2016, https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html., der die technische Entwicklungsgeschichte anhand des Übersetzungsprogramms von Google nachzeichnet.

[8] Siehe eingehend zum automatisierten Texterstellungsprogramm ChatGPT *Schwartmann*, Wenn Maschinen die Macht übernehmen, FAZ 25.02.2023, https://www.faz.net/einspruch/chatgpt-wenn-maschinen-die-macht-uebernehmen-18629187.html.; *Roose*, The Brilliance and Weirdness of ChatGPT, The New York Times 07.12.2022, https://www.nytimes.com/2022/12/05/technology/chatgpt-ai-twitter.html.

[9] Siehe nur die beispielhaften Aufzählungen bei *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 1 f., die unter anderem Luftfahrt, Energiesektor, Automobilindustrie, Medizintechnik, öffentliche Verwaltung, Gesundheitswesen und Bildung bis hin zu Mode und Tourismus aufführt.

persönlichen Präferenzen filtern,[10] personalisierte Werbeanzeigen schalten[11] oder BewerberInnen für einen Arbeitsplatz auswählen.[12] Derartige autonome Systeme kommen in der Privatwirtschaft bereits vielfach zum Einsatz, sie gestalten wesentlich die modernen Bedingungen der Kommunikation, Information, sozialen Interaktion und des Marktes.[13] Unternehmerische, individuelle und gesamtgesellschaftliche Interessen treffen aufeinander und werfen vielfältige Regulierungsfragen auf. Autonomen Systemen kommt ein bedeutender wirtschaftlicher Wert zu. Sie haben Geschäftsmodelle entstehen lassen und effektivieren unternehmerische und industrielle Prozesse.[14] Autonome Systeme versprechen überdies Steigerungen der Effektivität, Sicherheit, Konvenienz und Präzision von Diensten, Entscheidungen und Leistungen.[15] Dies ist die eine Seite. Auf der anderen Seite wirken autonome Systeme auf vielfältige Weise nachteilig auf Marktbedingungen, Freiheit, Gleichheit und Würde ein.[16] Beispielhaft sollen einige Phänomene vorgestellt werden: Wenn etwa Unternehmen einseitig Vertragsinhalte vorgeben und sich VerbraucherInnen aufgrund der Intransparenz und Determiniertheit algorithmischer Entscheidungsfindung nicht mehr in den Vertragsaushandlungsprozess einbringen können, ist

---

[10] Siehe etwa für die Videostreaming-Plattform Netflix *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like.; *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18.

[11] Vgl. *Wågström*, Why Behavioral Advertising Should Be Illegal, Forbes 05.05.2019, https://www.forbes.com/sites/forbestechcouncil/2019/03/05/why-behavioral-advertising-should-be-illegal.; *Ebers*, MMR 21 (2018), 423–428.

[12] *Kuner*, Und raus bist du!, FAZ 09.08.2021, https://www.faz.net/aktuell/karriere-hochschule/buero-co/ki-im-bewerbungsprozess-und-raus-bist-du-17471117.html.; *Redding*, Künstliche Intelligenz im Bewerbungsprozess, Tagesspiegel 19.07.2021, https://www.tagesspiegel.de/wirtschaft/ki-guckt-mit-4264693.html.

[13] Siehe zum Einsatz von Künstlicher Intelligenz für personalisierte Dienste *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 17. Vgl. Allgemein zum Einsatz personalisierter Systeme *Lorentz*, Profiling, 2019, S. 11–25.

[14] *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 2.

[15] Siehe allgemein zu Vorteilen von Systemen Maschinellen Lernens für Individuen, Unternehmen, Staat und Gesamtgesellschaft, *dies.*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 2 f. Sie nennt unter anderem eine Verbesserung des Gesundheitswesens, kostengünstige und effektive öffentliche Dienstleistungen wie Verkehr, Bildung oder Energie sowie die Leistungskraft der Technik bei der Verwirklichung ökologischer Nachhaltigkeitsziele.

[16] Siehe eingehend zu Risiken und Beeinträchtigungen konkreter rechtlich geschützter Interessen in Kapitel 2 der Arbeit. Vgl. allgemein zu Risiken von Systemen Künstlicher Intelligenz *dies.*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 12–15.

dies abträglich für die allgemeine Wohlfahrt.[17] Besonders auf sozialen Netzwerken musste man feststellen, dass autonome Systeme Diskussionsräume fragmentieren[18] und Menschen in Filterblasen festhalten.[19] Desinformation und Hassrede sind die Folge. Darüber hinaus ist zu beobachten, dass selbstlernende Algorithmen in hohem Maße diskriminierungsanfällig sind.[20] Autonome Systeme vermögen überdies, präzise intime Persönlichkeitsmerkmale, etwa den emotionalen Zustand einer Person, aufzudecken und in Form personalisierter Werbung wirkmächtig die Konsumentscheidung von VerbraucherInnen zu beeinflussen.[21] Vor allem stellt der Umstand vor Herausforderungen, dass Ergebnisse und Verfahren bestimmter selbstlernender Algorithmen menschlich nicht mehr verständlich sind.[22] Es ist unklar, inwieweit ein freiheitliches Leben in Würde gelingen kann, wenn Entscheidungen, Steuerungen und Leistungen für die betroffene Person nicht mehr vorhersehbar und nachvollziehbar sind.[23] Auch im Hinblick auf bestimmte Werte werden autonome Systeme teils sehr

[17] Vgl. zu verschiedenen Ursachen von Wohlfahrtsverlusten durch Einsatz von Algorithmen in der Privatwirtschaft *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 226–227, 233, 237–240. Siehe zu Wohlfahrtsverlusten spezifisch für die personalisierte Preisbildung *Tillmann/Vogt*, VuR 33 (2018), 447, 448 f.; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 405 f.

[18] Siehe hierzu Kapitel 2 C. II. 2. Hierfür ist der Begriff der Echokammern geprägt worden, siehe grundlegend *Sunstein*, Republic.com 2.0, 2007, S. 65; *Sunstein*, Echo chambers, 2001.

[19] Siehe hierzu Kapitel 2 C. IV. 2. b). Grundlegend zum Phänomen der Filterblase *Pariser*, The filter bubble, 2011.

[20] Siehe hierzu Kapitel 2 C. 1. Vgl. umfassend zu verschiedenen Formen und Ursachen *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019, S. 3–7; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 10–14; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 104–109.

[21] Eingehend hierzu unter Kapitel 2 C. IV. 2. c). Siehe auch *Berger*, Vermarktete Facebook die Gefühle seiner Nutzer?, Heise Online 02.05.2017, https://www.heise.de/newsticker/meldung/Internes-Papier-Vermarktete-Facebook-die-Gefuehle-seiner-Nutzer-3701195.html.; *Wågström*, Why Behavioral Advertising Should Be Illegal, Forbes 05.05.2019, https://www.forbes.com/sites/forbestechcouncil/2019/03/05/why-behavioral-advertising-should-be-illegal. Differenzierend zu verschiedenen Einsatzmöglichkeiten von Künstlicher Intelligenz im Marketingbereich, darunter auch die Nutzung zur Emotionserkennung für die Gestaltung von Werbemaßnahmen, *Huang/Rust*, Journal of the Academy of Marketing Science 49 (2021), 30–50.

[22] Eingehend hierzu Kapitel 2 A. II. 2. c) sowie Kapitel 4 D. IV. 1.

[23] Eingehend hierzu unter anderem unter Kapitel 2 C. II. 3., III. 2., IV. 1. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 29–33. Vgl. allgemein auch *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 13.

kritisch bewertet und Regulierungen eingefordert.[24] Im Zentrum stehen Überlegungen, wie das Verhältnis von Mensch und Maschine richtigerweise auszugestalten ist. Dystopische Vorstellungen von der Unterwerfung des Menschen durch die Maschine prägen vielfach den Diskurs.[25] Auf der anderen Seite wird befürchtet, dass bei einer allzu ausgreifenden Regulierung die Vorteile autonomer Systeme für Individuum und Gesellschaft ungenutzt bleiben könnten[26] und man im internationalen „race for AI" Wettbewerbsnachteile erleiden könnte.[27]

[24] Als maßgebliche Werte werden etwa benannt die menschliche Autonomie, menschliche Aufsicht und Kontrolle, Sicherheit und Robustheit, Fairness, Privatheit, Transparenz bzw. Erklärbarkeit oder Rechenschaft (Accountability). Vgl. auf internationaler Ebene *Extended Working Group on Ethics of Artificial Intelligence*, Preliminary Study on the technical and legal aspects relating to the desirability of a standard-setting instrument on the ethics of artificial intelligence, World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), 21.03.2019; auf europäischer Ebene *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, Europäische Kommission, 10. April 2019, S. 17 f.; auf nationaler Ebene *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 43–48; mit ausgewählten Anwendungsbeispielen *Deutscher Ethikrat*, Mensch und Maschine, 20.03.2023. Vgl. überdies die Darstellungen in der Literatur, etwa *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1; *Hagendorff*, Minds and Machines 30 (2020), 99–120. Auch die *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 2; *Europäische Kommission*, Künstliche Intelligenz für Europa, 25.04.2018, S. 17–19 betont die Notwendigkeit einer Abstützung der Künstlichen Intelligenz auf Werten.

[25] Vgl. *Russell/Dewey/Tegmark*, AI Magazine 36 (2015), 105, 111 f.; *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 366–369; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 110.

[26] So etwa *Erdélyi/Goldsmith*, Regulating Artificial Intelligence, 22.05.2020, S. 3.

[27] Siehe etwa *Kerkmann*, Künstliche Intelligenz: Wirtschaft warnt vor „massiven Einschränkungen" durch AI Act, Handelsblatt 6.1.2022, https://www.handelsblatt.com/technik/it-internet/eu-regulierung-kuenstliche-intelligenz-wirtschaft-warnt-vor-massiven-einschraenkungen-durch-ai-act/28850684.html. Deutlich *Werner*, Robotergehirne brauchen Regeln, SZ 16.03.2018, https://www.sueddeutsche.de/digital/kuenstliche-intelligenz-robotergehirne-brauchen-regeln-1.3907264: „Wegen all der Rhetorik um die Robokalypse ist die Gefahr einer Überregulierung noch größer als die Gefahr der KI selbst". Ein maßvolles legislatives Vorgehen mahnt auch *Reed*, Philos Trans A Math Phys Eng Sci 376 (2018), 1–12 an. Die Problematik der Überregulierung der Technik verweist auf den grundlegenden Konflikt der Technikregulierung, nämlich den richtigen Ausgleich zwischen Innovationssteuerung und -förderung zu finden. Grundlegend *Hoffmann-Riem*, AöR 131 (2006), 255, 265–268.

In diesem herausfordernden Regulierungsumfeld werden derzeit auf nationaler,[28] europäischer[29] und internationaler Ebene[30] bestehende Regelungen geprüft und verschiedene Regulierungsprojekte im Hinblick auf autonome Systeme angestoßen.[31] Vielfach ist man dabei der Ansicht, dass bestehende Regelungen nicht ausreichend sind, mehr noch: dass diese innovationshinderlich wirken. Die Europäische Union (EU) hat die Regulierung in ihre geoökonomische Strategie zur Künstlichen Intelligenz integriert: Sie will mit einer Regulierung eine „AI made in Europe"[32] schaffen und sich so auf dem Weltmarkt eine Vorreiterrolle sichern.[33] In Brüssel wird derzeit am Entwurf einer spezifi-

[28] Vgl. etwa für die Bundesrepublik Deutschland *Bundesregierung*, Strategie Künstliche Intelligenz der Bundesregierung, November 2018, S. 38–41; *Bundesregierung*, Strategie Künstliche Intelligenz der Bundesregierung, Dezember 2020, S. 24–26. Siehe instruktiv die Übersicht zu verschiedenen nationalen Regulierungsinitiativen *Campbell*, Artificial Intelligence: An overview of state initatives, FutureGrasp, 2019; *NíFhaoláin/Hines/Nallur*, in: Longo/Rizzo/Hunter u.a. (Hrsg.), Artificial Intelligence and Cognitive Science, 2020, S. 133.

[29] Siehe zu derartigen Bestrebungen der Einführung einer KI-Regulierung bereits *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 10–30.

[30] Vgl. etwa zu Initiativen der OECD *Council on Artificial Intelligence*, Recommendation of the Council on Artificial Intelligence, OECD Legal Instruments, 2022.

[31] Plakativ wird das „race to AI" umgewandelt zu einem „race of AI regulation", so *Smuha*, Law Innov. Technol. 13 (2021), 57–84.

[32] In der Europäischen Union wurde der Begriff der „vertrauenswürdigen Künstlichen Intelligenz" (trustworthy AI) geprägt, so etwa *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 12. Eingehend zu einem solchen Konzept auch *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, Europäische Kommission, 10. April 2019, S. 6.

[33] Siehe hierzu eingehend *Cooman*, Market and Competition Law Review 6 (2022), 49, 50 f.; *Kerkmann*, Künstliche Intelligenz: Wirtschaft warnt vor „massiven Einschränkungen" durch AI Act, Handelsblatt 6.1.2022, https://www.handelsblatt.com/technik/it-internet/eu-regulierung-kuenstliche-intelligenz-wirtschaft-warnt-vor-massiven-einschraenkungen-durch-ai-act/28850684.html. Siehe auch *Europäische Kommission*, Begründung Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 21.04.2021, S. 7, 10, 12. Vgl. zur geostrategischen Erwägungen der Einführung einer regulierten Künstlichen Intelligenz auch *Bundesregierung*, Strategie Künstliche Intelligenz der Bundesregierung, Dezember 2020, S. 2: „Verantwortungsvolle und gemeinwohlorientierte Entwicklung und Anwendung von KI-Systemen soll zu einem integralen Bestandteil und damit Markenzeichen einer ‚AI Made in Europe' gemacht werden". Einen Überblick über aktuelle geostrategische Investitionen in die Entwicklung von Künstlicher Intelligenz weltweit bieten *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 7.

schen KI-Regelung gearbeitet,[34] aber auch kritisch geprüft, inwieweit der geltende europäische Regulierungsrahmen hinreichend oder sogar hinderlich ist.[35]

Ein unionales Rechtsinstrument, mit dem bereits aktuell autonome Systeme reguliert werden können, ist die DSGVO. Sie sieht sich in besonderem Maße dem Vorwurf ausgesetzt, veraltet zu sein[36] und die EU im internationalen Wettbewerb um die Künstliche Intelligenz zurückzuwerfen.[37] Datenschutzskeptiker verweisen darauf, dass die DSGVO in technischer, ökonomischer und gesellschaftlicher Hinsicht nicht mehr dem heutigen Stand entspricht. Das Datenschutzrecht datiert aus den 1970er Jahren, einer Zeit, in der Großrechner nur einzeln verbreitet waren und das Internet noch nicht existierte. Die DSGVO öffnet sich zwar gewissen technischen Änderungen,[38] übernimmt aber im Wesentlichen den tradierten datenschutzrechtlichen Besitzstand.[39] Mit den Herausforderungen autonomer Systeme, insbesondere den hohen Datenmengen, der Unvorhersehbarkeit von Datenverarbeitungsergebnissen sowie dem Um-

---

[34] Siehe zum Entwurf der Europäischen Kommission für ein Gesetz zur Künstlichen Intelligenz eingehend Kapitel 3 B. II. 2. c) bb), zu einer Bewertung Kapitel 5 C II. Vgl. anschaulich zur Entwicklung einer unionalen Strategie zur Regulierung der Künstliche Intelligenz *Andraško/Mesarčík/Hamuľák*, AI and Society 36 (2021), 623–636.

[35] Vgl. *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 11 f.

[36] So *Veil*, NVwZ 37 (2018), 686, 695 f. Vgl. auch bereits für Big-Data-Analysen *Zarsky*, Setton Hall Law Review 47 (2017), 995–1020 In der Tendenz kritisch auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 306, 311.

[37] *Wallace*, Europe is about to lose the global AI race – thanks to GDPR, Euractive 25.5.2018, https://www.euractiv.com/section/data-protection/opinion/europe-is-about-to-lose-the-global-ai-race-thanks-to-gdpr; *Chivot/Castro*, The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy, 13.5.2019; *Jamison*, European Commission's AI Regulations Would Limit Possibility, American Enterprise Institute, 27.02.2020 (https://www.aei.org/articles/european-commissions-ai-regulations-would-limit-possibility); *Humerick*, Santa Clara High Technology Law Review 34 (2018), 393, 416. Siehe überdies die Studie von *Jia/Jin/Wagman*, Marketing Science 40 (2021), 661–684, durchgeführt am Illinois Institute of Technology, die ein Absinken von Investitionen in datengetriebene Technologien in der Europäischen Union im unmittelbaren Anschluss an die Einführung der DSGVO beobachten; sie werten allerdings allein Daten bis April 2019 aus.

[38] Das Gesetzgebungsverfahren wurde am 27.4.2016 mit Unterzeichnung des Europäischen Parlaments und des Rats abgeschlossen. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Albrecht*, Einleitung Rn. 184.

[39] Deutlich etwa *Martini*, Blackbox Algorithmus, 2019, S. 159: „Die Grundausrichtung des Datenschutzrechts entstammt der Ära der Lochkarten". Vgl. mit anschaulicher Übersicht der aus der Datenschutzrichtlinie übernommenen Regulierungsinstrumente Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Albrecht*, Einleitung Rn. 184, 212 sowie der neu eingefügten Regulierungsinstrumente, die nur eine moderarte Reform des Datenschutzrechts erkennen lassen, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 214.

stand, dass die eigentliche Gefährdung in den Algorithmen liegt, kann die DSGVO, so die These der Skeptiker, schon konzeptionell nicht zurechtkommen. Die technikneutrale Ausgestaltung der DSGVO, die auf Daten, nicht auf Verarbeitungstechniken und Anwendungen fokussiert, habe zudem zur Konsequenz, dass die eigentlichen Regulierungsfragen autonomer Systeme nicht spezifisch adressiert werden können.[40] Andere sehen in der DSGVO besondere Chancen zur Regulierung autonomer Systeme:[41] Sie ermögliche eine Regulierung an der Quelle selbstlernender Algorithmen[42] und erlaube mit ihrem technik-, anwendungs- bzw. schutzgutübergreifenden Regulierungsansatz eine verklammernd-globalisierte Adressierung der verschiedenen durch die Künstliche Intelligenz aufgeworfenen Regulierungsfragen.[43] Der technikneutrale Regulierungsansatz, so die Erwartung, befähigt die DSGVO, auch Regulierungsfragen autonomer Systeme zu adressieren.[44]

Die vorliegende Arbeit soll diese Thesen mit Leben füllen. Ihr Ziel ist es, durch Prüfung einzelner Rechtsinstrumente spezifisch darzulegen, inwieweit die DSGVO sinnvoll zur Regulierung autonomer Systeme beitragen, also Gefährdungen eindämmen und zugleich technische Entwicklung ermöglichen kann. Die Arbeit wird dabei zu dem Ergebnis kommen, dass die DSGVO vielfach an Grenzen kommt, dass sie aber auch einige sinnvolle Regulierungsak-

---

[40] Explizit *European Parliamentary Research Service*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Juni 2020, S. 35: „[T]he GDPR is focussed on the challenges emerging for the Internet – which were not considered in the 1995 Data Protection Directive, but were well present at the time when GDPR was drafted – rather than on new issues pertaining to AI, which only acquired social significance in most recent years". Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 306; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 5; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 7.

[41] So auch die Europäische Kommission, siehe etwa *Europäische Kommission*, Künstliche Intelligenz für Europa, 25.04.2018, S. 17.

[42] Vgl. auch *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 114.

[43] Die DSGVO wird auch als Querschnittsmaterie oder Schnittstellenrecht bezeichnet. Siehe etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 159. Zur Technikneutralität siehe Erwägungsgrund 15 S. 1 der DSGVO: „Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen".

[44] So etwa *Martini*, Blackbox Algorithmus, 2019, S. 157 f. Explizit auch *Andraško/Mesarčík/Hamuľák*, AI and Society 36 (2021), 623, 633. In diese Richtung auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 99. Siehe allgemein zu dieser Erwartung hinsichtlich des technikneutralen Regulierungsansatzes *Reding*, ZD 2 (2012), 195, 198; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 6. Ausführlich hierzu auch unter Kapitel 4 A. I. 2. c).

zente setzt. Die Arbeit soll bei einer bloßen Bestandsaufnahme und Kritik nicht stehen bleiben. Ihr Anliegen ist es, auch Optionen vorzustellen, wie aufgedeckte Regulierungsschwächen durch Reformen der DSGVO überwunden werden könnten. Am Ende soll die Untersuchung auch aufzeigen, was die DSGVO nicht regeln kann, wo also eigenständige Regelungen autonomer Systeme geboten sind. Um das Ergebnis vorwegzunehmen: Über die DSGVO ist eine echte Regulierung Maschineller Lernverfahren und der selbstlernenden Algorithmen nicht möglich. Sie muss auch dort scheitern, wo Verarbeitungsergebnisse menschlich nicht nachvollziehbar sind. Hier bedarf es eigenständiger, dann nicht-datenschutzrechtlicher Rechtsinstrumente.

B. Untersuchungsziele, Forschungsfrage und Erkenntnisinteressen

Die Arbeit hat damit vier Untersuchungsziele: eine Anwendung der DSGVO auf autonome Systeme, eine reflektive Kritik dieser datenschutzrechtlichen Regulierung, eine Darlegung der Innovationsfähigkeit der DSGVO sowie schließlich die Aufdeckung von Regulierungsaufträgen jenseits der DSGVO. Die Arbeit fokussiert dabei auf die Rechtsinstrumente des Zweckfestlegungs-, Rechtmäßigkeits- und Transparenzgrundsatzes. Sie nimmt eine freiheitsspezifische Perspektive ein, untersucht die DSGVO also im Hinblick auf Gefährdungen menschlicher Autonomie, bezieht dabei aber auch Diskriminierungen durch autonome Systeme ein.[45]

Typisch für autonome Systeme ist die Personalisierung, die über Profilbildungen technisch realisiert wird, sowie die Automatisierung von Anwendungen. Die Arbeit verspricht Erkenntnisse darüber, wie die Vorschriften der DSGVO zu allgemeinen Datenverarbeitungen, Profilbildung und automatisierter Entscheidung zusammenwirken und wie diese spezifisch durch den Einsatz selbstlernender Algorithmen herausgefordert sind.

C. Methode

Es ist Anliegen dieser Arbeit, zu klären, was die DSGVO zu einer guten Regulierung autonomer Systeme beitragen kann und soll. Maßgeblich ist, ob es der DSGVO rechtstatsächlich gelingt, die maßgeblichen Interessenskonflikte zu einem angemessenen Ausgleich zu führen. Der Bewertungsmaßstab der Arbeit

[45] Was damit im Einzelnen gemeint ist, soll ausführlich in Kapitel 2 IV. dargelegt werden.

ist der einer normativen Angemessenheit bzw. Rationalität.[46] Um Fragen verfassungsgemäßer Gebotenheit geht es dagegen nicht.

D. Rechtspraktische Bedeutung

Die vorliegende Arbeit soll Gesetzgeber und Rechtsanwender Direktiven an die Hand geben, wie autonome Systeme sinnvollerweise datenschutzrechtlich einzufassen sind. Die Arbeit soll überdies aufzeigen, wo Raum und Bedarf für den Erlass spezifischer Regelungen für autonome Systeme ist. Aufgrund des gewählten Bewertungsmaßstabs erheben die Vorschläge keinen Anspruch auf Verbindlichkeit, sie verstehen sich allein als Handlungsoptionen. Die Untersuchung soll auch betroffenen Personen eröffnen, welchen Schutz sie von der DSGVO erwarten können und welchen nicht, hinsichtlich welcher Schutzbedürfnisse sie also im rechtspolitischen Diskurs auf weitergehende Regelungen hinwirken müss(t)en. Die Arbeit versteht sich als Beitrag zur allgemeinen Diskussion über eine gute bzw. optimale Regulierung autonomer Systeme.

E. Gang der Untersuchung

Zunächst bedarf es eines Verständnisses von dem technischen Untersuchungsgegenstand dieser Arbeit. Autonome Systeme sollen im ersten Kapitel definiert und in ihrer Funktionsweise vorgestellt werden. Dabei ist auch auf technische Details des Maschinellen Lernverfahrens einzugehen. Abschließend sollen vier Referenzbeispiele dargestellt werden, die im Weiteren zur Veranschaulichung und Gegenprüfung der Thesen dienen, nämlich Informationsfilterdienste, personalisierte Werbemaßnahmen, automatisierte Kreditentscheidungssysteme sowie die personalisierte Preisgestaltung.

Das zweite Kapitel beschäftigt sich mit den soziokulturellen Bewertungen autonomer Systeme. Damit sollen präzise die Interessenskollisionen, die autonome Systeme hervorrufen, offengelegt werden. Die Chancen und Risiken autonomer Systeme werden vorgestellt, die Prämissen und Maxime, die hinter den Gewichtungen von Chancen und Risiken und damit den Bewertungen autonomer Systeme stehen, aufgezeigt, und schließlich konkrete Vulnerabilitätsphänomene dargelegt, auf die im öffentlichen Diskurs maßgeblich die Forderungen nach Regulierung gestützt werden. Autonomiegefährdungen und Diskriminierungen durch autonome Systeme, auf denen der Fokus dieser Arbeit liegt, sollen hier näher erläutert werden.

---

[46] Siehe Kapitel 3 A.

Zur Regulierung autonomer Systeme werden derzeit verschiedene Ansätze vorgeschlagen. Um diese allgemeine Regulierungsdebatte soll es im dritten Kapitel gehen. Dabei soll zunächst dargelegt werden, wie sich der Anspruch einer sinnvollen bzw. guten oder optimalen Regulierung zu einem rechtsnormativen Maßstab formt, wie sich also normative Angemessenheit und Klugheit einer Regulierung definieren lassen. Dies stellt den Bewertungsmaßstab dar, anhand dessen im Weiteren die DSGVO kritisch geprüft wird. Im Anschluss soll ein Überblick über wesentliche, derzeit diskutierte Regulierungsvorschläge gegeben werden und auch bereits eine erste Einordnung des Regulierungsbeitrags der DSGVO erfolgen.

Im vierten Kapitel sollen dann Anwendungsbereich und Regulierungszugriff der DSGVO, Zweckmäßigkeits- und Rechtmäßigkeitsgrundsatz sowie Transparenzgrundsatz im Hinblick auf autonome Systeme analysiert und kritisch bewertet werden. Die DSGVO kann und soll nach dem gesetzgeberischen Entwurf nicht sämtliche Regulierungsfragen autonomer Systeme lösen. Wichtig ist daher ein Verständnis vom normativen Regulierungsbeitrag der DSGVO. Dieser ergibt sich aus den grundlegenden Zielen und Vorverständnissen des Datenschutzrechts, auf die zunächst einzugehen ist. Dies leitet dann auch die Auslegung der zu untersuchenden Rechtsinstrumente an. Im Weiteren soll geklärt werden, welche Regulierungszugriffe die DSGVO grundsätzlich für die einzelnen technischen Verarbeitungsabläufe autonomer Systeme bietet. Sodann soll der Frage nachgegangen werden, unter welchen Umständen diese Verarbeitungsverfahren zulässig sind und welche Informationspflichten für diese jeweils bestehen. Im Anschluss soll dann bewertet werden, ob die Zulässigkeitsanforderungen und Informationspflichten praktikabel sind und ob damit die Regulierungsbedarfe autonomer Systeme in gelungener Weise beantwortet sind. Die Untersuchung wird zu dem Ergebnis kommen, dass allein der Zweckfestlegungsgrundsatz gute Lösungen bietet, während Rechtmäßigkeits- und Transparenzgrundsatz insbesondere aufgrund der fehlenden Nachvollziehbarkeit autonomer Systeme an Grenzen geführt werden.

Abschließend sollen in einem fünften Kapitel rechtliche Möglichkeiten zur Überwindung der aufgezeigten Regulierungsdefizite der DSGVO vorgestellt werden. Nur teilweise lassen sich diese dem normativen Regulierungsauftrag der DGSVO zuordnen. Innovationspotentiale der DSGVO betreffen vor allem die eigenständigen Vorschriften zur Profilbildung sowie die Einführung eines Rechts auf Erklärung. Die DSGVO bietet für die fehlende Nachvollziehbarkeit autonomer Systeme keine Lösung, auch Fragen der Regulierung des Maschinellen Lernverfahrens liegen außerhalb ihres Regulierungsauftrags. Hier sind eigenständige, technikspezifische Regelungen gefordert, deren möglicher Inhalt kurz skizziert werden soll.

Ein Fazit fasst am Ende die wesentlichen Erkenntnisse der Untersuchung zusammen.

F. Themeneingrenzung

Autonome Systeme werden allein in ihrer Nutzung im Privatbereich betrachtet. Der Einsatz autonomer Systeme durch den Staat wirft komplexe Fragen auf, die eigenständiger Untersuchung bedürfen. Gegenstand der Arbeit ist zudem allein das unionale Datenschutzrecht; soweit die DSGVO Öffnungen für nationale Datenschutzregelungen vorsieht, sind diese nicht Gegenstand dieser Untersuchung.

Die Arbeit fokussiert auf beobachtete, als regulierungsbedürftig erkannte Fehlentwicklungen autonomer Systeme. Sie ist dabei auf empirische Erkenntnisse und interdisziplinäre Einordnungen angewiesen. Teilweise liegen zu bestimmten Anwendungen noch keine Langzeitstudien vor,[47] teilweise liefern Studien ambivalente Ergebnisse.[48] Die Untersuchung kann es nicht leisten, diese realwissenschaftliche Forschungslücken zu schließen. Sie stützt sich auf die vorhandene Empirik und analysiert Ursachen und Zusammenhänge, soweit dies für die Forschungsfrage dienlich ist.

Diese Arbeit fokussiert auf Maschinelle Lernverfahren als der Teil des Forschungsbereichs der Künstlichen Intelligenz. Autonome Systeme im Sinne dieser Arbeit sind damit solche des Maschinellen Lernens. Es handelt sich dabei

---

[47] Das Fehlen von Langzeitstudien im Bereich von Empfehlungssystemen betont auch *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019, S. 19. *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 9 weisen darauf hin, dies im Rahmen von Informationsfilterdiensten, dass sich die tatsächlichen Effekte autonomer Systeme auf die Lebenswirklichkeit des Einzelnen und der Gesellschaft zum aktuellen Zeitpunkt nur bedingt prognostizieren lassen.

[48] Siehe hierzu unter Kapitel 2 C. Herausfordernd ist auch, dass Einwirkungen auf die Willens- und Entscheidungsbildung des Menschen nur begrenzt empirisch präzise belegt werden können und Studienergebnisse Raum für verschiedene Schlussfolgerungen lassen. Siehe etwa *Stark/Magin/Jürgens*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 20, 71 hinsichtlich der Erforschung von Suchmaschinennutzung: „Angesichts der Tatsache, dass es dabei um unbewusst ablaufende Prozesse geht und dass soziale Erwünschtheit die Antworten beeinflusst haben könnte, wäre es sicherlich gewinnbringend, die gewonnenen Erkenntnisse experimentell und/oder mittels Blickaufzeichnungsstudien zu validieren.“. Herausfordernd ist auch, dass es vielfach an Bemessungskriterien fehlt, da man für die neue Technologie noch keine eigenen Maßstäbe gefunden hat, so auch *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 5. Problematisch können auch kulturell bedingte Verzerrungen sein, hierauf weisen *Bakshy/Messing/Adamic*, Science 348 (2015), 1130, 1131 hin.

um eine Form der schwachen[49] Künstlichen Intelligenz.[50] Ob und inwieweit autonome Systeme als intelligent gelten können, ist für das Forschungsziel dieser Arbeit nicht von Interesse. Ebenso stehen rechtliche Fragen, die sich mit Blick auf eine „echte", sogenannte starke Künstlichen Intelligenz[51], oder eine die menschliche Intelligenz übertreffende, sogenannte Superintelligenz,[52] stellen, jenseits des Forschungsauftrags dieser Arbeit. Die Arbeit beschäftigt sich vielmehr mit einer ganz bestimmten Anwendung selbstlernender Algorithmen und fragt konkret, was die DSGVO zu ihrer Regulierung beitragen kann.

---

[49] Gängig sind die Begriffe narrow oder weak artificial intelligence. Siehe die Darstellungen bei *Bringsjord/Govindarajulu*, in: Zalta (Hrsg.), The Stanford Encyclopedia of Philosophy, 2020, 8.1; *Dignum*, Responsible Artificial Intelligence, 2019, S. 15 f.; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 981.

[50] So die einhellige Meinung, siehe nur *Wischmeyer*, AöR 143 (2018), 1, 3 f.; *Martini*, Blackbox Algorithmus, 2019, S. 25; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 3. Hervorgehoben wird, dass wesentliche Aspekte der menschlich-natürlichen Intelligenz, insbesondere Intuition und Unterbewusstsein, nicht abgebildet werden können, siehe *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 985 f. Zur Unfähigkeit des Einbezugs von „common sense", siehe *Görz/Braun/Schmid*, in: dies. (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 1, 10; *Martini*, Blackbox Algorithmus, 2019, S. 60, zur Intuition *Hoffmann-Riem*, AöR 142 (2016), 1, 30. Andere verweisen darauf, dass autonomen Systemen intelligenzkonstitutive Eigenschaften wie Selbstbewusstsein und Fähigkeit zu kritischer Selbstdistanz fehlen, so *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 4; *Görz/Braun/Schmid*, in: dies. (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 1, 6; *Bringsjord/Govindarajulu*, in: Zalta (Hrsg.), The Stanford Encyclopedia of Philosophy, 2020, 8.1. Auch auf das Fehlen von Kreativität wird hingewiesen, so *Görz/Braun/Schmid*, in: dies. (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 1, 6. Ob und wann eine starke Künstliche Intelligenz erzeugt werden kann, ist letztlich eine philosophische Frage, siehe hierzu eingehend *Bringsjord/Govindarajulu*, in: Zalta (Hrsg.), The Stanford Encyclopedia of Philosophy, 2020, 8, 9.

[51] Zum Begriff der starken Künstlichen Intelligenz *Wang*, J. Artif. Gen. 10 (2019), 1, 15. Auch die Bezeichnung general artifical intelligence wird geführt. Vgl. auch *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 221–232; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 1004 f.

[52] Grundlegend *Bostrom*, Superintelligence, 2014. Auch von technischer Singularität ist die Rede, so etwa *Vinge*, The coming technological singularity, San Diego State University, 01.12.1993; *Kurzweil* (Hrsg.), The age of intelligent machines, 1990; *Kurzweil*, The singularity is near, 2005.

Kapitel 1

Phänomenologie und technische Funktionsweise autonomer Systeme

Die technischen Untersuchungsgegenstände dieser Arbeit sind autonome Systeme, die auf der Technologie Künstlicher Intelligenz aufbauen. Es handelt sich dabei um informationstechnische Konstrukte, die auf eigenständige Aktion und auf die Interaktion mit dem Menschen ausgerichtet sind. Zunächst sollen grundlegend die Funktionselemente derartiger autonomer Systeme vorgestellt werden (A.). Die Künstliche Intelligenz ist Schlüsseltechnologie autonomer Systeme und Zielpunkt der Arbeit, ihre Historie, technische Funktionsweise und Definition soll im Anschluss vorgestellt werden (B.). Zur technischen Realisierung autonomer Systeme als personalisiert-automatisierte Assistenzsysteme in dem hier beschriebenen Sinne bedarf es der Profilbildung und der Integration des Profils in eine automatisierte Entscheidungs- und Steuerungsarchitektur. Darin werden die spezifischen Einsatzbereiche der Künstlichen Intelligenz bei der Konstruktion autonomer Systeme deutlich (C.). Die technischen Verfahren derartiger autonomer Systeme sind komplex, die Anwendungsfelder vielfältig. Zur Veranschaulichung und zur Prüfung der rechtlichen Thesen dieser Arbeit sollen vier Referenzbeispiele dienen, die abschließend genauer dargestellt werden (D.).

A. Charakterisierung und technische Funktionsweise autonomer Systeme

Zunächst sollen autonome Systeme im Verständnis dieser Arbeit kurz definiert werden (I.). Im Anschluss soll die Technik der Künstlichen Intelligenz als Schlüsseltechnologie autonomer Systeme in ihrer grundlegenden Funktionsweise vorgestellt werden (II.). Die Untersuchung konzentriert sich auf zwei Arten autonomer Systeme, nämlich Systeme der Ambient Intelligence sowie automatisierte Entscheidungssysteme (III.).

I. Definition und Merkmale autonomer Systeme

Für autonome Systeme werden verschiedene Definitionen vorgeschlagen.[1] In dieser Arbeit geht es um autonome Systeme, die zur Interaktion mit dem Menschen bestimmt sind. Der Begriff der autonomen Systeme wird demnach enggeführt auf personalisierte autonome Systeme. Für die Definition dieser autonomen Systeme bietet sich eine Übertragung der Definition der sogenannten Ambient Intelligence (Umgebungsintelligenz) – hierzu noch genauer unten[2] – an, denn diese wird durch personalisierte autonome Systeme technisch realisiert. Zur Charakterisierung der Ambient Intelligence werden gemeinhin fünf Elemente hervorgehoben:[3] das Umwelt- und Kontextbewusstsein (Wahrnehmung), die eigeninitiative Handlungsfähigkeit (Autonomie bzw. Responsivität), die Anpassung an unterschiedliche Anwendungsbereiche und individuelle Bedürfnisse (Adaptabilität), die Antizipierung präferierter Ergebnisse und Entwicklungen (Antizipativität) sowie im Rahmen personalisierter Anwendungen die selbstadaptive Anpassung an individuelle Fähigkeiten und Vorlieben von NutzerInnen (Personalisierung).[4] Von besonderer Bedeutung ist dabei die Lernfähigkeit der Systeme, die ihnen eine beständige Anpassung an veränderte Umstände über die Zeit erlaubt (Lernfähigkeit).[5] Je nach Anwendungskontext sind die verschiedenen Elemente unterschiedlich stark ausgeprägt.

---

[1] Vgl. etwa *Wahlster*, Informatik Spektrum 40 (2017), 409, 410 f., der die Merkmale Entscheidungs-, Selbstlern- und Selbsterklärungsfähigkeit, die Resilienz, Kooperativität, Ressourcenadaption und Proaktivität benennt. Siehe auch *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859, 872, 861-862, die die Fähigkeit zur Interaktion, Kooperation, Lernfähigkeit und Problemlösungskompetenz herausstellen. *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 40–42 machen als konstitutive Elemente von „intelligent agents" das Umweltbewusstsein, die Lernfähigkeit und die Autonomie aus. *Hoffmann-Riem*, AöR 142 (2016), 1, 30 benennt die Fähigkeit zur Wahrnehmung, Schlussfolgerung und zur Kommunikation und Kooperation.

[2] Siehe Kapitel 1 A. III. 1.

[3] Einen Überblick über verschiedene Definitionsansätze der Ambient Intelligence bieten *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 278.

[4] Vgl. *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 278; *Gams/Gu/Härmä u.a.*, JAISE 11 (2019), 71, 76; *Sadri*, ACM Computing Surveys 43 (2011), 1, 2 f. Ähnlich die Zusammenstellungen bei *Chin/Callaghan/Allouch*, JAISE 11 (2019), 45, 52 f.; *Pantoja/Viterbo/Seghrouchni*, in: Jezic/Chen-Burger/Kusek (Hrsg.), Agents and Multi-agent Systems: Technologies and Applications 2019, 2020, S. 57, 60 f.

[5] *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859, 861; *Wahlster*, Informatik Spektrum 40 (2017), 409, 410.

II. Künstliche Intelligenz als Schüsseltechnologie autonomer Systeme: Maschinelle Lernverfahren und technische Grundlagen

Kerntechnologie autonomer Systeme ist die Informations- und Computertechnologie, vor allem die Datenverarbeitungs- und Algorithmentechnik.[6] Für die Automatisierung und Personalisierung autonomer Systeme erweist sich dabei die Technik der Künstlichen Intelligenz als besonders effektiv. Während man in einfach gelagerten Fällen mit der klassischen Programmierung gute Ergebnisse erzielt,[7] kommt man in komplexeren Umgebungen, die multivariable Problemlösungen voraussetzen, nicht weiter,[8] so etwa bei der Bild- und Spracherkennung,[9] aber auch bei der Medien- und Informationsfilterung[10] oder

---

[6] Zu dieser Einordnung siehe für autonome Systeme *Wahlster*, Informatik Spektrum 40 (2017), 409, 411–415; *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 131–141; *Damm/Kalmar*, Informatik Spektrum 40 (2017), 400, 406 f.; für intelligente Agenten *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 47–49 „agent program"; für die Ambient Intelligence hierzu noch unter Kapitel 1 A II. 1. genauer – *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 282–284.

[7] Vgl. *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 135, die verschiedene informationstechnische Methoden zur Umsetzung autonomer Systeme vorstellen.

[8] Die Notwendigkeit der Techniken der Künstlichen Intelligenz bzw. des Maschinellen Lernens für die technische Realisierung autonomer Systeme streichen heraus *Damm/Kalmar*, Informatik Spektrum 40 (2017), 400, 406; *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 131; *Wahlster*, Informatik Spektrum 40 (2017), 409, 414 f. Siehe auch umfassend *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859. Vgl. zur Anwendung von Verfahren der Künstlichen Intelligenz in Applikationen der Ambient Intelligence *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 289; *Aztiria/Augusto/Orlandini* (Hrsg.), State of the art in AI applied to ambient intelligence, 2017; *Ramos/Augusto/Shapiro*, IEEE Intelligent Systems 23 (2008), 15–18; *Gams/Gu/Härmä u.a.*, JAISE 11 (2019), 71–86 Eine präzise Darstellungen der Technologien der Künstlichen Intelligenz für einzelne Anwendungsszenarien der Ambient Intelligence bietet *Sadri*, ACM Computing Surveys 43 (2011), 1, 6–47. Für automatisierte Entscheidungen sehr allgemein *Martini*, Blackbox Algorithmus, 2019, S. 22; *Davenport/Harris*, MIT Sloan Management Review 46 (2006), 1, 6. Siehe zum Einsatz Künstlicher Intelligenz bei der Kreditvergabe, *Sadok/Sakka/El Maknouzi*, Cogent Economics and Finance 10 (2022), 1–12.

[9] Eingehend *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859, 863–869.

[10] Siehe etwa zur Verbesserung der Empfehlungssysteme des Streamingdienstes Spotify durch den Einsatz Maschineller Lernverfahren *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html. Siehe im Einzelnen noch unten Kapitel 1 C. I.

bei der personalisierten Preisbildung.[11] Hier bieten Algorithmen aus Maschinellen Lernverfahren, die derzeit erfolgreichste Methode im Forschungsbereich der Künstlichen Intelligenz, gute Lösungen. Zugleich erlauben diese Verfahren ein höheres Maß an Automatisierung, als dies bislang möglich war, eben da die Systeme Algorithmen eigenständig bilden. Das Maschinelle Lernverfahren ist damit Kerntechnologie autonomer Systeme. Untersuchungsgegenstand dieser Arbeit sind solche autonomen Systeme, die sich Maschineller Lernverfahren bedienen. Im Folgenden sollen Ansätze, Methoden und Verarbeitungsverfahren des Maschinellen Lernverfahrens vorgestellt werden; dies bildet die Grundlage für die spätere datenschutzrechtliche Untersuchung autonomer Systeme. Beim Maschinellen Lernverfahren wird menschliches Lernen imitiert (1.), verschiedene Repräsentationsformen und Ansätze sind dabei üblich (2.).

[11] Siehe etwa *Wallace*, Using AI for Dynamic Pricing, 20.9.2019 (https://opendatascience.com/using-ai-for-dynamic-pricing-the-smarking-example/); *Pearson*, Personalizing Price With AI: How Walmart, Kroger Do It, Forbes 7.9.2021, https://www.forbes.com/sites/bryanpearson/2021/09/07/personalizing-price-with-ai-how-walmart-kroger-do-it/?sh=5b7f06732eb2. Ausführlich unten Kapitel 1 C. III. 2.

1. Grundlegende Funktionsweise und Ansätze des Maschinellen Lernens

Ziel des Maschinellen Lernens ist die eigenständige Erarbeitung von Problemlösungen und -strategien durch ein System anhand eines algorithmischen Verfahrens. Lösungsmethoden sollen nicht menschlich vorgegeben (oder aus Vorprogrammiertem abgeleitet) werden, vielmehr soll der Lösungsweg durch das System selbst erarbeitet und implementiert werden. Das Maschinelle Lernen ist ein induktiv-datenbasiertes Lernen: In Daten werden Muster erkannt und hieraus Regeln abgeleitet, die dann zu einem Algorithmus[12] , d.h. einer durch das System berechenbaren Handlungsanweisung, geformt werden.[13] Wird dann im Anwendungsfall ein bislang unbekannter Input in das System eingegeben, soll dieses eine zutreffende Zuordnung vornehmen. Der Lösungsalgorithmus wird so vom System „eigenständig" gebildet, das System programmiert sich gleichsam selbst.[14] Je umfassender die Daten sind, desto präzisere Regeln können abgeleitet werden. Das Maschinelle Lernen hat damit seine Grundlagen in klassischen Datenanalysemethoden, etwa der Statistik, dem Data Mining sowie der Data Science,[15] und ist, soweit große Datenmengen verarbeitet werden, eine Form der Big-Data-Analyse.[16] Es geht dabei nicht um das Aufdecken potentiell interessanter Zusammenhänge in den Daten – so das Data Mining[17] oder Predictive Analytics[18] –, sondern um die Entwicklung einer algorithmischen Lösung für ein bestimmtes Anwendungsproblem anhand der Daten.[19] Dass Daten brauchbare Angaben für diese Lösung enthalten, ist dabei vorausgesetzt – dies gilt für Maschinelle Lernverfahren nach tradierten Methoden ebenso wie für solche des Deep Learnings.[20] Das Maschinelle Lernverfahren ist nicht statisch, vielmehr setzt es sich beständig fort, indem die Daten und Rückmeldungen aus der Anwendungsumgebung als neue Lerndaten dienen. Die Systeme schreiben die Algorithmen somit eigenständig kontinuierlich fort.[21]

2. Methoden und Darstellungsformen des Maschinellen Lernens

Differenzieren lassen sich Maschinelle Lernverfahren nach der Art der Darstellung (a) sowie der Lernmethode (b). Das von den Systemen entwickelte

---

[12] Algorithmen sind präzise Arbeits- bzw. Berechnungsanweisungen zur Lösung eines konkreten Problems. Sie enthalten eine Abfolge von Anweisungen zur Umwandlung von Eingaben (Problem) in erwünschte Ausgaben (Lösung, Ergebnis). Die Abbildung dieser Einzelschritte wird als Funktion bezeichnet. Vgl. hierzu eingehend *Martini*, Blackbox Algorithmus, 2019, S. 17 f.; *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 43; *Dignum*, Responsible Artificial Intelligence, 2019, S. 3. Der Algorithmus grenzt sich von einer bloßen mathematischen Rechenregel dadurch ab, dass er tatsächlich in einer endlichen Zeit durch ein maschinelles System berechnet werden kann. Der Algorithmus muss für das System lesbar sein und also in einer bestimmten formalen Sprache (sogenannte Programmiersprache) vorliegen. Der in die Programmiersprache umgesetzte, d.h. von einem Com-

puter ausführbare Algorithmus wird als Programm bezeichnet. Siehe hierzu *Broy/Kuhrmann*, Einführung in die Softwaretechnik, 2021, S. 18. Informationen, d.h. Zustände, die nicht einen konkreten (Rechen-)Auftrag, sondern einen bestimmten Sinngehalt aufweisen, werden in Form von Daten in die formale Sprache übersetzt, liegen also in einer bestimmten, der Programmiersprache entsprechenden Zeichenfolge vor. In Digitalcomputern sind Daten als binäre Signale dargestellt, vgl. *Ernst/Schmidt/Beneken*, Grundkurs Informatik, [7]2020, S. 12; *Broy/Kuhrmann*, Einführung in die Softwaretechnik, 2021, S. 132 f. Die Darstellung der konkreten Daten und Algorithmen als eine bestimmte, in der Programmiersprache festgelegte Abfolge von Zeichen wird als Code bezeichnet. Demgegenüber beschreibt die Software die Gesamtheit aller Programme und Daten, die zur Lösung eines Problems notwendig sind, und zwar in der für das System lesbaren Form. Siehe *Broy/Kuhrmann*, Einführung in die Softwaretechnik, 2021, S. 17 f.

[13] Anschauliche Definition bei *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 651: „[A] computer observes some data, builds a model based on that date, and uses the model as both a hypothesis about the world and a piece of software that can solve problems". Siehe auch *Alpaydın*, Machine learning, 2021, S. 14-18, 25–27. Vgl. auch *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 8; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 201; *Goodfellow/Bengio/Courville*, Deep learning, 2016, S. 1; *Dignum*, Responsible Artificial Intelligence, 2019, S. 22 f.

[14] *Dignum*, Responsible Artificial Intelligence, 2019, S. 22; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 274. Dies wird auch unter dem Schlagwort zusammengefasst „Der Algorithmus wird nicht mehr programmiert, sondern trainiert", so *Stiemerling*, CR 2015, 762, 763.

[15] *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, 429; *Alpaydın*, Machine learning, 2021, S. 32 f. Gerade bei tradierten Lernverfahren sind die technischen Methoden von klassischer Datenanalyse und Maschinellem Lernverfahren vielfach ähnlich.

[16] Siehe anschaulich die Übersicht bei *Brühl*, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt, S. 3.

[17] Beim Data Mining geht es um die strukturierende Analyse von Datenmengen zur menschlichen Wissensgewinnung und -darstellung, vgl. *Beierle/Kern-Isberner*, Methoden wissensbasierter Systeme, [6]2019, S. 146. Ziel ist es, einen Datensatz nach Mustern und Zusammenhängen zu analysieren, ohne dass eine Frage oder ein Anwendungsfall feststeht, ja ohne dass überhaupt klar ist, ob sich eine Frage oder ein Anwendungsfall ergeben wird. Erst bei Vorliegen des Ergebnisses des Data Minings kann entschieden werden, ob die Erkenntnisse brauchbar sind und wie sie verwendet werden könnten. Ein Supermarktbetreiber könnte etwa den Datensatz zum Kaufverhalten seiner Kunden nach bestimmten Merkmalen (features), zB nach der Tageszeit, dem Geschlecht oder dem Wohnort, untersuchen. Dabei könnte aufgedeckt werden, dass bestimmte Produktvorlieben bestimmter Personen zu bestimmten Tageszeiten bestehen. Der Betreiber könnte diese Erkenntnis für personalisierte Werbemaßnahmen oder die Produktplatzierungen im Supermarkt nutzen. Das Ergebnis des Data Minings könnte aber auch sein, dass keinerlei Zusammenhänge bestehen. Plakativ *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 6: „Data mining provides its users with answers to questions they did not know to ask". Das Data Mining dient damit der Vorbereitung zielorientierter Datenanalyse wie Predictive Analytics oder Maschineller Lernverfahren, bei denen vorab feststehen muss, dass der Datensatz relevantes Wissen, d.h. Muster für einen bestimmten Anwendungsfall oder ein bestimmtes Ziel enthält. Knowledge Discovery in Databases

Wissen lässt sich so systematisieren (c). Für die Auswahl eines Maschinellen Lernverfahrens in der Praxis sind verschiedene Kriterien maßgeblich (d).

a) Lernmethoden: überwachtes, nicht überwachtes und bestärkendes Lernen

Beim Maschinellen Lernen werden drei Methoden unterschieden: das überwachte (*supervised,* Lernen mit Lehrer*)*, das unüberwachte (*unsupervised,* Lernen ohne Lehrer*)* und das bestärkende Lernen (*reinforcement learning)*, wobei auch hybride Methoden zur Anwendung kommen.[22] Beim überwachten Lernen ist das erwünschte Ergebnis (Output) bzw. die Struktur, Gruppierung und Klassifizierung der Daten (sogenanntes Label) vorgegeben, allein der Weg zwischen Input und Output bzw. die Verbindungen zwischen den Datengruppierungen ist unbekannt.[23] Dagegen geht es beim unüberwachten Lernen darum,

---

(KDD) und Data Mining werden oftmals synonym verwendet oder wechselweise als Überbegriffe bzw. Teilverfahren verwendet. In der informationstechnischen Forschung bzw. Praxis werden die Begrifflichkeiten nicht trennscharf auseinandergehalten und vielfach synonym verwendet. Siehe ausführlich zu all dem *Alpaydın*, Machine learning, 2021, S. 2 f.; *Beierle/Kern-Isberner*, Methoden wissensbasierter Systeme, [6]2019, S. 145–160; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 195–197; *Brühl*, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt; *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 6 f.

[18] Sollen anhand der Erkenntnisse aus den Daten Prognosen angestellt werden, wird von Predictive Analytics gesprochen, *Brühl*, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt, S. 4. Es handelt sich somit um einen dem Data Mining nachgelagerten Analyseprozess, denn es ist vorausgesetzt, dass die Daten Aussagen über zukünftiges Verhalten oder erwartbare Entwicklungen enthalten.

[19] *Brühl*, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt, S. 5; *Alpaydın*, Machine learning, 2021, S. 40. Plakativ *Domingos*, Communications of the ACM 2012 (2012), 78: „Machine learning systems automatically learn programs from data".

[20] Vgl. *Alpaydın*, Machine learning, 2021, S. 28–30. Siehe auch, dort für tradierte Lernmethoden, *Domingos*, Communications of the ACM 2012 (2012), 78, S. 80, 82–83.

[21] *Alpaydın*, Machine learning, 2021, S. 27–28, 41.

[22] Statt vieler *Goodfellow/Bengio/Courville*, Deep learning, 2016, S. 101–104; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 653; *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 430–432. Instruktive Übersicht verschiedener Methoden *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 10.

[23] *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 10; *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 430 f.; *Alpaydın*, Machine learning, 2021, S. 46–51; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 653–657. Ist die Anzahl der Label gering, wird dies als Klassifikation bezeichnet (zB Spam – keine Spam), geht es um die Einordnungen in kontinuierliche Größen (Skalen oder

in einem unstrukturiert-chaotischen Datensatz Muster, Strukturen und Zusammenhänge aufzudecken.[24] Typischer Anwendungsfall ist das Clustering (Cluster-Analyse), bei der die Trainingsdaten in verschiedene Vergleichsgruppen eingeordnet werden,[25] oder Association Rules (Assoziationsregelanalyse), bei der einzelne Merkmale in einem Trainingsdatensatz zueinander in Verbindung gesetzt werden.[26] Beim bestärkenden Lernen wird für das Erreichen eines Zwischen- oder Endziels eine positive (Belohnung – *reward*) oder negative (Strafe – *penalty*) Rückmeldung ausgegeben. Anhand dieser Rückmeldung soll eine Strategie (*policy*) zur Erzielung einer maximalen Belohnung entwickelt werden.[27] In diesem Verfahren geht es um die Entwicklung einer optimalen Lösungsstrategie. Es ähnelt damit dem überwachten Lernen, es werden aber nicht Vorgaben für einzelne Datenzuordnungen gemacht, sondern für eine Folge von Aktionen.[28] Für die jeweiligen Verfahren stehen unterschiedliche Lernmethoden bzw. -stile zur Verfügung.[29] Aus diesen ergibt sich dann der Ablauf des Maschinellen Lernverfahrens, das typischerweise aus fünf Schritten besteht: der Aufbereitung der Daten, dem Einspeisen der Daten, dem Training des Mo-

---

Vektoren), spricht man von Regression, vgl. *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 431; *Domingos*, Communications of the ACM 2012 (2012), 78.

[24] *Goodfellow/Bengio/Courville*, Deep learning, 2016, S. 102; *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 431; *Alpaydın*, Machine learning, 2021, S. 143–152.

[25] *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 244-243; *Alpaydın*, Machine learning, 2021, S. 144; *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 431.

[26] *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 431. Typischer Anwendungsfall sind Empfehlungssysteme beim Online-Handel anhand von Warenkorbanalysen. Untersucht wird dabei, welche Produkte typischerweise gemeinsam gekauft werden (Kunden, die das Produkt A gekauft haben, haben auch das Produkt B gekauft, nicht aber Produkt C). Dies lässt Prognosen darüber zu, ob eine Person, die Produkt A gekauft hat, auch Produkt B (Wahrscheinlichkeit hoch) oder Produkt C (Wahrscheinlichkeit niedrig) kaufen wird. Siehe hierzu auch, wenngleich nicht spezifisch auf Maschinelle Lernverfahren bezogen, *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 12 f.

[27] Ausführlich *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 351–377; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 789–822; *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 432 f.

[28] *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 431 f.

[29] Einen anschaulichen Überblick über Verfahren, Methoden und Stile und deren Einsatz in der Praxis bieten *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 10 f. Siehe für überwachte Lernverfahren *Domingos*, Communications of the ACM 2012 (2012), 78, 79.

dells, der Evaluation und Anpassung des Modells und der Nutzung.[30] Maßgeblich für die Auswahl der Lernmethode und -stile ist etwa der Anwendungszweck, die Größe, Qualität und Zusammensetzung der verfügbaren Daten, das menschliche Wissen in einem Anwendungsfeld, aber auch ökonomische Erwägungen und sonstige Faktoren.[31] Wichtig ist dabei stets die strikte Trennung zwischen Trainings- und Test- bzw. Anwendungsdaten, da andernfalls die Treffsicherheit und Tauglichkeit des erlernten Algorithmus nicht geprüft werden kann.[32]

b) Deep Learning und künstliche neuronale Netze

Bei hochkomplexen Problemstellungen kommt man mit tradierten Datenanalysemethoden nicht weiter. Dies gilt vor allem bei der Sprach-, Text- oder Bilderkennung: Ein Datenset an Sprachbeispielen, Texten oder Bildern lässt sich mit simplen statistisch-mathematischen Regeln nicht beschreiben.[33] Aber auch Produktangebote von Online-Händlern oder Medien- und Informationsangebote von Online-Plattformen oder Streamingdiensten können nicht mehr über einfache logische Regeln strukturiert werden.[34] Um in derartigen Datensets Muster zu erkennen, bedarf es eines multikonzeptionalen und multidimensionalen Ansatzes.[35] Aus den Trainingsdaten werden mehrere algorithmische Einzelfunktionen abgeleitet und in einer bestimmten Hierarchie in mehreren Schichten (Layers) geordnet und miteinander verbunden. Das Regelset wird „tief", daher wird diese Methodik als Deep Learning (tiefes Lernen) bezeich-

---

[30] Siehe beispielhaft die Darstellung der einzelnen Verfahrens- und Verarbeitungsschritte eines überwachten Maschinellen Lernverfahrens *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 434–445.

[31] *Dies.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 433 f.

[32] *Domingos*, Communications of the ACM 2012 (2012), 78, 79.

[33] *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning); *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 750, 782–783.

[34] Vgl. hierzu *LeCun/Bengio/Hinton*, Nature 521 (2015), 436. Siehe zum Einsatz von Deep-Learning-Verfahren bei Produktempfehlungen bei Amazon *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning) sowie beim Streamingdienst Spotify *Hajek*, So funktioniert die Erfolgsformel von Spotify, Wirtschafts-Woche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html. Zum Einsatz von Deep Learning bei der Erstellung des NewsFeed-Algorithmus auf Facebook siehe *Meta AI*, The new AI-powered feature designed to improve Feed for everyone, 5.10.2022 (https://ai.facebook.com/blog/facebook-feed-improvements-ai-show-more-less).

[35] Die theoretischen Ansätze hierzu waren bereits in den 1940er Jahren entwickelt worden, konnten dort aber aufgrund der geringen Datenmenge und Rechenleistung von Computern praktisch nicht umgesetzt werden, vgl. *Görz/Braun/Schmid*, in: dies. (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 1, 5 f.; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 750.

net.[36] Die derzeit erfolgreichste Methode zur Auswahl und Anordnung dieser Funktionen bzw. Schichten sind künstliche neuronale Netze (KNN, artificial neuronal networks),[37] die inspiriert sind vom Aufbau des natürlichen Gehirns.[38] Das Lernverfahren erfolgt hier in einem multiiterativen Ausprobierprozess, bei dem allein das erwünschte Ergebnis vorgegeben wird. Das System nimmt so lange Änderungen an den einzelnen Funktionen und deren Verbindungen zueinander sowie den Schichten – auch deren Anzahl – vor, bis das erwünschte Ergebnis mit hinreichender Wahrscheinlichkeit korrekt ausgegeben wird.[39] Der

---

[36] *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning); *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 750. Vgl. auch *Alpaydın*, Machine learning, 2021, S. 129.

[37] Einzelne Funktionen, d.h. Teilalgorithmen (Künstliche Neuronen) werden dabei über Knotenpunkte (Nods, Künstliche Synapsen) miteinander verbunden. Die Teilalgorithmen werden auf Schichten (Layers) abgebildet, die in bestimmten Hierarchien geordnet sind. Ausgehend von einem Input gibt der Teilalgorithmus bei Erreichen eines bestimmten Schwellenwerts einen Output von einer gewissen Intensität an den nachfolgenden Teilalgorithmus, damit also die nachfolgende Schicht, weiter. Die Intensität dieses Outputs wird als Gewicht bezeichnet. Jeder Teilalgorithmus in jeder Schicht „gewichtet" also den Input. Der letzte Teilalgorithmus in der letzten Schicht (Output Layer) gibt das finale Gewicht und damit das Ergebnis aus. Im Trainingsverfahren ermittelt üblicherweise jede Schicht eine bestimmte Eigenschaft in den Trainingsdaten. Das Trainingsverfahren ist beendet, wenn das künstliche neuronale Netz, d.h. sämtliche Schichten und Teilalgorithmen in ihrer Gesamtheit, den erwünschten Output, etwa das Erkennen eines Bildes, mit hinreichender Treffsicherheit ausgibt. Die Leistungskraft des künstlichen neuronalen Netzes bestimmt sich nach der Art und Anzahl der Teilalgorithmen und Schichten, deren Verbindungen und der Intensität (Gewichte) der Outputs der Teilalgorithmen. Diesem Verfahren liegt die Erkenntnis zugrunde, dass für komplexe Problemstellungen Lösungen nicht durch eine einzelne lineare Lösungsfunktion, sondern nur durch mehrere, präzise aufeinander abgestimmte Lösungsfunktionen erzielt werden können. Vielschichtige, komplexe und unstrukturierte Trainingsdatensätze können nur durch diese Kombination von Lösungsfunktionen präzise abgebildet werden. Siehe eingehend zu künstlichen neuronalen Netzen, ihrem Aufbau, Konzept und Erstellungsverfahren *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 429, 445–461; *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 509; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 285–349; *Alpaydın*, Machine learning, 2021, S. 105–142; *Skansi*, Introduction to deep learning, 2018; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 750–782; *LeCun/Bengio/Hinton*, Nature 521 (2015), 436–444.

[38] Das natürliche Gehirn dient dabei nur als Modell zur Ausgestaltung des Lösungsalgorithmus, auf welche Weise also Teilalgorithmen ausgestaltet, miteinander verbunden und geschichtet werden können; eine tatsächliche Nachbildung eines natürlichen Gehirns ist nicht beabsichtigt. So auch *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 750: „[…] [T]he resemblance to real neural cells and structures is superficial".

[39] Eingehend *Burrell*, Big Data and Society 3 (2016), 5–7; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 751; *LeCun/Bengio/Hinton*, Nature 521 (2015), 436–438. Wird etwa ein künstliches neuronales Netz zur Bilderkennung von Hunden eingesetzt, erhält das neuronale Netz im Trainingsprozess verschiedene Bilder von Tieren. Ordnet das System wäh-

Lösungsalgorithmus ist am Ende das künstliche neuronale Netz insgesamt, d.h. ein komplexes algorithmisches Konstrukt (sog. Neuronenmodell). Es wird beständig fortentwickelt, Anwendungsdaten dienen dann zugleich als Trainingsdaten.[40] Je mehr Einzelfunktionen (Neuronen) das künstliche neuronale Netz enthält, desto präzisere Ergebnisse lassen sich erzielen. Auch die Anzahl der Schichten ist entscheidend.[41] Besonders leistungsstarke künstliche neuronale Netze enthalten eine Vielzahl derartiger Neuronen, dann im Millionen- oder Milliardenbereich.[42]

c) Symbolische und subsymbolische Lernmethoden

Beim Maschinellen Lernen kommen tradierte, d.h. mathematische und statistische Datenanalysemethoden zum Einsatz. Das Erlernte ist explizit in Form von formalen Symbolen, logischen Regeln oder graphischen Abbildungen dargestellt, es ist mathematisch nachweisbar, sprachlich fassbar und für den Menschen erkläbar.[43]

---

rend dieses Trainingsverfahrens das Bild von einer Katze fälschlicherweise als das eines Hundes ein, erhält es als Rückmeldung „inkorrekt", jedoch keine Vorgabe, welche Teilalgorithmen und Verbindungen in welcher Schicht im Einzelnen auf welche Weise zu ändern sind. Das System passt dann in einem zufälligen Ausprobierverfahren Teilalgorithmen, vor allem deren Gewichte, in den einzelnen Schichten an und testet dann erneut, wie die Rückmeldung ausfällt. Dies erfolgt so oft und so lange, bis es als Rückmeldung „korrekt" erhält.

[40] *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning).

[41] Unterschieden werden Input Layer und Output Layer (Eingabe- und die Ausgabeschichten) sowie die Schichten dazwischen, die als Hidden Layers bezeichnet werden. Es gibt jeweils nur eine Input und Output Layer, es kann also nur die Anzahl der Hidden Layers erhöht werden. Die Leistungskraft des künstlichen neuronales Netzes steigt mit der Anzahl der Neuronen in den jeweiligen Schichten und mit der Anzahl der Schichten. Bei einfachen Anwendungen reichen bereits wenige oder gar nur eine Hidden Layer aus, komplexere Problemstellungen verlangen mehrere Layers. Es ist dann auch von tiefen künstlichen neuronalen Netzen die Rede, so *Brühl*, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt, S. 8. Die passende Anzahl von Schichten und Einzelfunktionen ist Gegenstand fortlaufender Forschung. Vgl. *Ertel*, Grundkurs Künstliche Intelligenz, ^{5}2021, S. 326–329; *Burrell*, Big Data and Society 3 (2016), 5 f.; *Russell/Norvig*, Artificial Intelligence, ^{4}2021, S. 759.

[42] *Brühl*, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt, S. 6.

[43] Siehe zu derartigen Verfahren eingehend *Bauckhage/Hübner/Hug u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 429, 461–475; *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 11. Siehe zur Unterscheidung symbolischer und subsymbolischer Lernverfahren anschaulich *Bhatia*, Understanding the difference between Symbolic AI and Non Symbolic AI, Analytics India Magazine 27.12.2017, https://analyticsindiamag.com/understanding-difference-symbolic-ai-non-symbolic-ai/.
Vgl. auch *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen

Diese Verfahren werden als symbolische[44] oder auch als Top-down-Lernverfahren[45] bezeichnet. Beim Deep Learning ist das gefundene Regelwerk ein komplexes, mehrschichtiges algorithmisches Konstrukt. Es enthält keine (menschlich) erkennbaren oder logischen symbolischem Verbindungen, Strukturen, Gruppierungen oder Darstellungen.[46] Dieses Lernverfahren wird daher auch als subsymbolisch[47] oder konnektionistisch[48] bezeichnet, auch von Bottom-up-Algorithmen ist die Rede.[49]

d) Entscheidungskriterien für die Auswahl des Maschinellen Lernverfahrens

In manchen Anwendungskonstellationen, etwa der Sprach- oder Bilderkennung, sind Automatisierungen allein mit Methoden des Deep Learnings möglich, in anderen ermöglichen sie gegenüber klassischen Lernmethoden detailgenauere und akkuratere Ergebnisse.[50] Kredit-Scorings oder personalisierte Werbemaßnahmen sind dann noch passgenauer möglich. Für die Auswahl zwischen Deep-Learning-Methoden und klassischen Lernverfahren sind verschiedene Faktoren entscheidend.[51] Maschinelle Lernverfahren anhand klassischer Methoden verlangen eine Vorstrukturierung der Daten: Dass diese ein Muster enthalten, muss vorab bekannt sein, ebenso wie gewisse Kenntnisse über die Merkmale der Daten.[52] Dieses Lernverfahren ist auch mit wenigen Daten mög-

---

und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 11, 44; *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning).

[44] Vgl. auch *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 11, 44; *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning); *Bhatia*, Understanding the difference between Symbolic AI and Non Symbolic AI, Analytics India Magazine 27.12.2017, https://analyticsindiamag.com/understanding-difference-symbolic-ai-non-symbolic-ai/.

[45] *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432.

[46] In diesen Bereich fallen insbesondere künstliche neuronale Netze vgl. *Goodfellow/Bengio/Courville*, Deep learning, 2016, S. 1 f.; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 750. So auch *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 308 f.

[47] *Döbel/Leis/Vogelsang u.a.*, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, 2018, S. 44.

[48] *Alpaydın*, Machine learning, 2021, S. 116–118.

[49] *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432.

[50] *Heller*, Was ist Deep Learning?, Computerwoche 27.08.2022, https://www.computerwoche.de/a/was-ist-deep-learning,3549921.; *Alpaydın*, Machine learning, 2021, S. 127.

[51] Siehe instruktiv die Übersicht zu den Charakteristika von Maschinellen Lernverfahren und Deep Learning *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning).

[52] *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning); *Domingos*, Communications of the ACM 2012 (2012), 78, 82 f.

lich.[53] Demgegenüber ist beim Deep Learning eine Vorstrukturierung der Daten nicht notwendig, dort ist eine originär maschinelle Regelfindung aus einem chaotischen Datensatz möglich.[54] Auch ein bestimmtes Anwendungsziel muss vorab nicht festgelegt sein, das Ergebnis kann für verschiedene Anwendungen genutzt werden.[55] Überdies ist der Automatisierungsgrad höher, da ein menschliches Eingreifen im Lernverfahren nicht notwendig ist, zudem die menschliche Prüfung nur das Ergebnis, nicht auch die einzelnen Regeln oder den inneren Aufbau erfasst.[56] Dieses Lernverfahren verlangt allerdings große Datenmengen, überdies eine hohe Rechenleistung sowie Hardwareausstattung.[57] Zudem sind diese Lernverfahren deutlich zeitintensiver als tradierte Methoden.[58] In Bereichen, in denen das Deep Learning nicht funktionsnotwendig ist, sondern nur bessere Ergebnisse erzielt, wird sich ein Unternehmer für den Einsatz derartiger Lernverfahren nur entscheiden, wenn sich der Daten-, Ressourcen- und Zeiteinsatz amortisiert bzw. gegenüber tradierten Lernverfahren geringer ist.[59] Ob ein Deep-Learning-Verfahren in der jeweiligen Anwendung zum Ein-

---

[53] *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning).

[54] *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning); *Alpaydın*, Machine learning, 2021, S. 127–129; *LeCun/Bengio/Hinton*, Nature 521 (2015), 436.

[55] *Alpaydın*, Machine learning, 2021, S. 127.

[56] *Heller*, Was ist Deep Learning?, Computerwoche 27.08.2022, https://www.computerwoche.de/a/was-ist-deep-learning,3549921. Anschaulich *Alpaydın*, Machine learning, 2021, S. 129: „Once we have data – and today we have ‚big' data – and sufficient computation available – and today we have data centers with thousands of processors – we just wait and let the learning algorithm discover all that is necessary by itself". Ähnlich *LeCun/Bengio/Hinton*, Nature 521 (2015), 436 „The key aspect of deep learning is that these layers of features are not designed by human engineers: they are learned from data using a general-purpose learning procedure".

[57] *Heller*, Was ist Deep Learning?, Computerwoche 27.08.2022, https://www.computerwoche.de/a/was-ist-deep-learning,3549921.; *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning). Siehe auch *Domingos*, Communications of the ACM 2012 (2012), 78, 83: „In most of computer science, the two main limited resources are time and memory. In machine learning, there is a third one: training data".

[58] Lernverfahren nach klassischen Lernmethoden dauern Minuten bis Stunden, Deep-Learning-Methoden bis zu Wochen oder sogar Monaten. Vgl. *Heller*, Was ist Deep Learning?, Computerwoche 27.08.2022, https://www.computerwoche.de/a/was-ist-deep-learning,3549921.; *Wuttke*, Machine Learning vs. Deep Learning (https://datasolut.com/machine-learning-vs-deep-learning).

[59] Der Zeit- und Ressourcenaufwand eines Maschinellen Lernverfahrens mit klassischen Methoden ist nicht notwendig geringer als derjenige des Deep Learnings, denn bei klassischen Methoden bedarf es der Vorstrukturierung der Daten sowie eine intensivere menschliche Begleitung des Lernprozesses. Ob dieser Aufwand dann höher ist als beim Deep Learning, lässt sich nur im Einzelfall bestimmen. Vgl. zu diesen Überlegungen *Heller*, Was ist

satz kommt, ist am Ende nicht nur eine technische, sondern vor allem auch eine wirtschaftliche Frage. Mit einer immer weiteren Verbesserung der Methoden, Rechenleistung und Hardware und der Verfügbarkeit großer Datenmengen ist es freilich denkbar, dass der Ressourceneinsatz für Deep-Learning-Verfahren in Zukunft deutlich sinken und dann auch diese Methoden umfassend(er) Verbreitung finden werden.

III. Eingrenzung des Untersuchungsgegenstands: autonome Systeme der Ambient Intelligence und automatisierte Entscheidungssysteme

Anwendungskonstellationen autonomer Systeme sind vielfältig. Die folgende Untersuchung konzentriert sich auf zwei Einsatzbereiche, die datenschutzrechtlich von besonderer Relevanz sind: erstens personalisierte Dienste, derer sich die Person zu eigenen Zwecken bedient (Mensch-Maschine-Interaktion), zweitens personalisierte Dienste, derer sich eine Person, um eine Entscheidung über einen Dritten zu treffen (Mensch-Maschine-Mensch-Interaktion). Der erstgenannte Einsatzbereich erfasst insbesondere Anwendungen der Ambient Intelligence (Umgebungsintelligenz) (1.), die zweitgenannte Konstellation die Automatisierung von Entscheidungen[60] (2.).

1. Autonome Systeme als automatisierte Steuerungssysteme und technische Umsetzung einer Ambient Intelligence

Autonome Systeme versprechen, als persönliche Assistenten umfassend Alltagsaufgaben des und für den Einzelnen zu automatisieren. Anwendungsbeispiele sind etwa Informationsempfehlungssysteme, Smart Home Anwendungen, autonome Fahrzeuge oder Assistenzsysteme wie Alexa.[61] Viele Alltagsaufgaben verlangen komplexere Lösungsstrategien, zudem können Anpassungen an Bedürfnisse, Vorlieben und Kompetenzen der einzelnen Person notwendig oder effizienzsteigernd sein, siehe hierzu sogleich.[62] Autonome Systeme kommen mit diesen Anforderungen zurecht. Sie erweitern damit den Bereich von Alltagsaufgaben, die automatisiert werden können. Damit sind bedeutende Fortschritte im interdisziplinären Forschungsbereich der Ambient Intelligence

---

Deep Learning?, Computerwoche 27.08.2022, https://www.computerwoche.de/a/was-ist-deep-learning,3549921.

[60] Mit dieser Bezeichnung ist noch nichts darüber gesagt, ob diese auch automatisierte Entscheidungen im Sinne des Art. 22 DSGVO darstellen. Hierauf ist noch vertieft unter Kapitel 4 B. III. 3. b) einzugehen.

[61] Siehe eingehend *Prasad*, „Ambient intelligence" will accelerate advances in general AI, Amazon Science, 21.01.2021 (https://www.amazon.science/blog/ambient-intelligence-will-accelerate-advancements-in-general-ai).

[62] Kapitel 1 B. I.

(Umgebungsintelligenz) möglich,[63] mit der das Idealbild einer Welt automatisiert-personalisierter Assistenzsysteme beschrieben wird.[64] Assistenzsysteme wie Alexa oder Siri gelten (derzeit) als Prototypen der Ambient Intelligence.[65] Zur technischen Umsetzung bedarf es der umfassenden Integration informationstechnischer Systeme in die Alltagsumgebung des Einzelnen.[66] Der Anspruch ist dabei, nicht allein den digitalen Bereich, sondern auch die analoge Welt zu automatisieren. Hierfür bedarf es der Installation von Aktuatoren und Sensoren[67] sowie der Virtualisierung sämtlicher physischer Alltagsgegenstände, etwa durch RFID-Technologie,[68] und der Vernetzung (Internet of

---

[63] Erste Ideen zur Ambient Intelligence entstammen den 1990er Jahren, siehe zur Historie *Aarts/Encarnação*, in: dies. (Hrsg.), True Visions, 2006, S. 1, 6–8. Siehe auch das von 2002 bis 2006 laufende Forschungsprogramm der Europäischen Union „Information Society Technologies", eingehend *Burgelman/Punie*, in: Aarts/Encarnação (Hrsg.), True Visions, 2006, S. 17 Aus der umfassenden Literatur zur Ambient Intelligence siehe beispielhaft *Coutaz/Crowley*, in: Calvary/Delot/Sedes u.a. (Hrsg.), Computer Science and Ambient Intelligence, 2013, S. 1; *Sadri*, ACM Computing Surveys 43 (2011), 1–66 Siehe zu aktuellen Forschungsinitiativen *Chatzigiannakis/Ruyter/Mavrommati* (Hrsg.), Ambient Intelligence, 2019; *Julián/Carneiro/Alonso u. a.* (Hrsg.), Ambient Intelligence—Software and Applications—13th International Symposium on Ambient Intelligence, 2023.

[64] *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 278 sprechen von einem „electronic butler".

[65] Vgl. etwa *Prasad*, „Ambient intelligence" will accelerate advances in general AI, Amazon Science, 21.01.2021 (https://www.amazon.science/blog/ambient-intelligence-will-accelerate-advancements-in-general-ai). Siehe auch *Gams/Gu/Härmä u.a.*, JAISE 11 (2019), 71, 74.

[66] Ziel ist die Automatisierung und Personalisierung der gesamten Lebensumwelt des Einzelnen. Hierauf deutet der Teilbegriff „Ambient" der Ambient Intelligence hin, *Aarts/Encarnação*, in: dies. (Hrsg.), True Visions, 2006, S. 1, 2. Vgl. auch *Sadri*, ACM Computing Surveys 43 (2011), 1, 2. Jeder Alltagsgegenstand kann dann in ein Assistenzsystem eingebunden sein, etwa der Kühlschrank, der Kalender oder das Fahrzeug, vgl. *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277 f. Hierzu bedarf es der Implementierung von (unsichtbaren) Mikrocomputern in die zu automatisierenden Alltagsgegenstände. Diese sollen langfristig Computer, Laptops oder Smarthphones ersetzen. Die Ambient Intelligence beruht auf bzw. ist teilweise identisch mit Bestrebungen des Ubiquitous Computing (Rechnerallgegenwart), vgl. hierzu grundlegend *Weiser*, Scientific American 265 (1991), 94–104.

[67] Für autonome Systeme *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 859, 898 f.; *Wahlster*, Informatik Spektrum 40 (2017), 409, 411 f.; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, ^{2}2019, S. 158. Für die Ambient Intelligence *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 280–282; *Sadri*, ACM Computing Surveys 43 (2011), 1, 39; *Augusto/Mccullagh*, Computer Science and Information Systems 4 (2007), 1, 8–11.

[68] Vgl. *Pantoja/Viterbo/Seghrouchni*, in: Jezic/Chen-Burger/Kusek (Hrsg.), Agents and Multi-agent Systems: Technologies and Applications 2019, 2020, S. 57, 62–65; *Sadri*, ACM Computing Surveys 43 (2011), 1, 2 f.; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, ^{2}2019, S. 159.

Things).[69] Die Ambient Intelligence findet demnach zwischen Online- und Offline-Welten bzw. gleichzeitig in beiden statt.[70] Autonome Systeme können daher auch Daten in der analogen Welt aufzeichnen.[71] Dies erhöht den Umfang verfügbarer Daten für das Trainingsverfahren und die Profilerstellung.[72] Diese informationstechnischen Systeme sollen zudem fähig sein, eigenständig und pro- und selbstadaptiv auf die Umwelt und die Bedürfnisse der NutzerInnen zu reagieren.[73] Hierzu bedarf es dann, nämlich bei komplexeren Aufgabenstellungen, der Technologie des Maschinellen Lernens.[74] Dies verweist zurück auf die umfassende Verbreitung autonomer Systeme im Lebensalltag des Einzelnen: Erst die Verfügbarkeit großer Datenmengen aus den digitalen und analogen Einsatzbereichen erlaubt es autonomen Systemen, eigenständig Regeln für die jeweiligen Anwendungen zu finden.[75]

---

[69] Vgl. hierzu eingehend *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 164; *Nürnberger/Bugiel*, DuD 40 (2016), 503; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 157–165. Siehe auch *Chin/Callaghan/Allouch*, JAISE 11 (2019), 45–69; *Boehme-Neßler*, DuD 40 (2016), 419, 420 f.

[70] Hierfür wurde der Begriff der Onlife-Welten geprägt. Zu diesem Begriff grundlegend *Floridi* (Hrsg.), The Onlife Manifesto, 2015. Siehe auch *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 41 f.; *Hoffmann-Riem*, AöR 142 (2016), 1, 5 f. Auch von cyberphysischen Systemen (CPS) ist die Rede, so etwa *Taha/Taha/Thunberg*, Cyber-Physical Systems: A Model-Based Approach, 2021; *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 143; *Wahlster*, Informatik Spektrum 40 (2017), 409; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 170–174.

[71] Vgl. eingehend *Storr/Storr*, in: Corrales/Fenwick/Forgó (Hrsg.), New Technology, Big Data and the Law, 2017, S. 65; *Lorentz*, Profiling, 2019, S. 45 f.; *Boehme-Neßler*, DuD 40 (2016), 419, 420.

[72] Hierauf ist noch zurückzukommen. Siehe Kapitel 4 B. II.

[73] Dies wird im Teilbegriff der „intelligence" der Ambient Intelligence deutlich, *Aarts/Encarnação*, in: dies. (Hrsg.), True Visions, 2006, S. 1, 2; *Augusto/Mccullagh*, Computer Science and Information Systems 4 (2007), 1, 3–5; *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 279; *Sadri*, ACM Computing Surveys 43 (2011), 1, 2.

[74] Siehe eingehend etwa *Aztiria/Augusto/Orlandini* (Hrsg.), State of the art in AI applied to ambient intelligence, 2017; *Gams/Gjoreski* (Hrsg.), Artificial Intelligence and Ambient Intelligence, 2021; *Gams/Gu/Härmä u.a.*, JAISE 11 (2019), 71, 73–75. Siehe auch *Prasad*, „Ambient intelligence" will accelerate advances in general AI, Amazon Science, 21.01.2021 (https://www.amazon.science/blog/ambient-intelligence-will-accelerate-advancements-in-general-ai). Aus der älteren Literatur *Ramos/Augusto/Shapiro*, IEEE Intelligent Systems 23 (2008), 15–18.

[75] Vgl. zu diesen Zusammenhängen auch *Prasad*, „Ambient intelligence" will accelerate advances in general AI, Amazon Science, 21.01.2021 (https://www.amazon.science/blog/ambient-intelligence-will-accelerate-advancements-in-general-ai).

Teilweise werden diese Anwendungen auch als Smart Technologies bezeichnet.[76]

2. Autonome Systeme als automatisierte Entscheidungssysteme

Autonome Systeme fungieren überdies als automatisierte Entscheidungssysteme.[77] Hier sind es dann Dritte, die sich der Automatisierungstechnologie bedienen, um mit dem Menschen interagieren zu können.[78] Dies betrifft etwa automatisierte Kreditentscheidungen oder Versicherungsprämienberechnung. Hier passt sich nicht die Alltagsumgebung bzw. einzelne Alltagsgegenstände

---

[76] *Hildebrandt*, Smart technologies and the end(s) of law, 2016. Die Begrifflichkeit des „Smart" weist darauf hin, dass die Systeme fähig sind, kognitiv anspruchsvolle Aufgaben eingeständig zu lösen. Teilweise ist auch von Smart Systems, etwa Smart Home, Smart City, Smart Health oder Smart Energie, die Rede. Bei diesen Systemen ist eine Personalisierung nicht unbedingt notwendig, bereits mit einer Automatisierung lassen sich gut Lösungen erzielen, siehe hierzu sogleich unter Kapitel 1 B. I. Auch der Einsatz selbstlernender Algorithmen ist nicht stets erforderlich oder wirtschaftlich rentabel. Smart Technologies bzw. Smart Systems sind damit nicht identisch mit autonomen Systemen im Sinne dieser Arbeit; autonome Systeme stellen sich vielmehr als Unterkategorie von Smart Technologies dar. Sie beschreiben die Anwendungskonstellationen, in denen Personalisierung notwendig oder erwünscht und die Verwendung selbstlernender Algorithmen notwendig ist.

[77] Diese werden auch als automated-decision-making applications, automated-decision-making systems oder automated-decision-making processes (ADM) bezeichnet, siehe nur *Davenport/Harris*, MIT Sloan Management Review 46 (2006), 1–10; *Power*, What is decision automation?, DSSResources, 19.12.2018; *Zarsky*, Science, Technology, & Human Values 41 (2016), 118–132 In der deutschen Übersetzung ist dann von automatisierten Entscheidungssystemen bzw. -verfahren die Rede, siehe etwa *Ernst*, JZ 72 (2017), 1026; *Martini*, Blackbox Algorithmus, 2019, S. 28; *Martini/Nink*, NVwZ 36 (2017), 1–14 Auch die Begriffe algorithmische oder algorithmenbasierte Entscheidungsverfahren werden verwendet, so *Ernst*, JZ 72 (2017), 1026–1036; *Martini*, JZ 72 (2017), 1017, 1020, 2021. Hiervon zu unterscheiden ist der rechtliche Term der automatisierten Entscheidung nach Art. 22 DSGVO. Ob eine automatisierte Entscheidung eines autonomen Systems auch eine solche im Rechtssinne darstellt, soll in Kapitel 4 B. III. 3. b) geklärt werden.

[78] Die Assistenz autonomer Systeme erfolgt also zugunsten eines Dritten, vgl. *Davenport/Harris*, MIT Sloan Management Review 46 (2006), 1, 2: „Automated decision-making applications, however, are designed to minimize human involvement in an ongoing decision-making process". Zu diesem Anwendungsbereich autonomer Systeme siehe auch *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 46–48; *Wahlster*, Informatik Spektrum 40 (2017), 409–418; *Nürnberger/Bugiel*, DuD 40 (2016), 503–506. Ohne eine Beschränkung auf die Verwendung durch den Nutzer oder Dritte konzipieren auch *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 859, 859–862, 872 Assistenzsysteme bzw. „smart agents". Auch der Begriff des (Software)Agenten ist nicht auf eine bestimmte Verwendungskonstellation beschränkt, siehe hierzu *Ertel*, Grundkurs Künstliche Intelligenz, ^{5}2021, S. 19–22; *Hoffmann-Riem*, AöR 142 (2016), 1, 30.

automatisiert an den Einzelnen an – so die Ambient Intelligence[79], vielmehr wird eine Entscheidungsfrage automatisiert auf eine Person zugeschnitten. Auch hier geht es also um eine automatisiert-personalisierte Interaktion mit einer bestimmten Person, wenngleich im Drittinteresse.[80]

IV. Zusammenfassung und Themeneingrenzung

Autonome Systeme sollen eine Automatisierung der Interaktion mit Einzelpersonen ermöglichen. Mit der Technologie des Maschinellen Lernens als Teilbereich der Künstlichen Intelligenz erzielt man dabei besonders gute Ergebnisse; sie ermöglicht die eigenständige Entwicklung von Lösungen in komplexen Anwendungskonstellationen. Die Arbeit konzentriert sich auf autonome Systeme, bei denen Maschinelle Lernverfahren zum Einsatz kommen. Beim Maschinellen Lernen leiten Systeme aus Daten anhand unterschiedlicher Verfahren – überwacht, unüberwacht oder bestärkend – algorithmische Regeln ab. Dies kann durch klassische Methoden erfolgen, bei denen Algorithmen in symbolischer Form vorliegen. In hochkomplexen Umgebungen erweisen sich Deep-Learning-Methoden als besonders erfolgreich. Die Algorithmen stellen sich hier als vielschichtig geordnete Konstruktion in Form künstlicher neuronaler Netze dar, d.h. in subsymbolischer Form. Die Auswahl zwischen klassischen und Deep-Learning-Verfahren bestimmt sich nach dem Anwendungsbereich, der Verfügbarkeit von Daten, Rechenleistung und Hardware sowie nach wirtschaftlichen Gesichtspunkten. Nach ihrem Anwendungszweck lassen sich zwei Typen autonomer Systeme unterscheiden: Solche, die von der Einzelperson eingesetzt werden (automatisierte Steuerungssysteme), und solche, die durch Dritte für Maßnahmen gegenüber der Einzelperson eingesetzt werden (automatisierte Entscheidungssysteme). Beide Arten autonomer Systeme – bezeichnet als Steuerungssysteme einerseits, Entscheidungssysteme andererseits – sollen im Weiteren untersucht werden.

---

[79] Automatisierte Entscheidungssysteme werden überwiegend nicht als Anwendungen der Ambient Intelligence verstanden, vgl. etwa die Darstellungen bei *Cook/Augusto/Jakkula*, Pervasive and Mobile Computing 5 (2009), 277, 288–292; *Gams/Gu/Härmä u.a.*, JAISE 11 (2019), 71–86, bei denen derartige Systeme fehlen. AA *Friedewald/Vildjiounaite/Punie u.a.*, Telematics and Informatics 24 (2007), 15–29; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 27 f., die auch automatisierte Entscheidungssysteme zur Ambient Intelligence zählen. Siehe insbesondere *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 428, 432, die zwischen der Automatisierung von Entscheidungen *anstelle* der Person (Ambient Intelligence im klassischen Sinne, also Steuerungen von Geräten, Webseiten etc.) und *über* die Person (automatisierte Entscheidungen) unterscheiden („decisions for us", „decisions about us") und beide als Anwendungen der Ambient Intelligence verstehen.

[80] Ähnlich die Erwägungen bei *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428.

B. Automatisierung und Personalisierung durch autonome Systeme

Autonome Systeme, wie sie Gegenstand dieser Arbeit sind, sind solche, die zur Interaktion mit dem Menschen konzipiert sind. Hierfür bedarf es der Automatisierung der Systeme. In bestimmten Anwendungskonstellation lässt sich die Effektivität und Kundenzufriedenheit steigern, wenn die autonomen Systeme individualisiert, d.h. die angebotenen Dienste, Programme oder Produkte an eine ganz bestimmte Person und deren Bedürfnisse, Präferenzen oder Fähigkeiten angepasst werden. Es bedarf dann zusätzlich einer Personalisierung. Hierfür sind, wie noch zu zeigen ist, Erkenntnisse über betroffene Personen notwendig, die in Benutzerprofilen abgebildet sind. Autonome Systeme können diese Profilerstellung automatisieren. Mithilfe der Benutzerprofile können dann die Lösungsalgorithmen personalisiert werden und so eine an die betroffene Person individuell angepasste Steuerung oder Entscheidung ausgeben werden.

Nachfolgend soll zunächst vorgestellt werden, dass und bei welchen autonomen Systemen ein Personalisierungsbedarf besteht und in welcher Intensität (I.). Im Anschluss sollen das technische Verfahren zur Realisierung dieser Personalisierung erörtert und dabei auch verschiedene Personalisierungsgrade vorgestellt werden (II.). Des Weiteren soll dann näher das Verfahren der Automatisierung der Profilbildung durch autonome Systeme dargestellt und dabei auch auf den Begriff und mögliche Inhalte des Profils eingegangen werden (III.). Abschließend soll erläutert werden, wie der Lösungsalgorithmus eines autonomen Systems gebildet und personalisiert und so eine automatisierte Anwendung ausgelöst wird (IV.).

I. Einsatzbereiche und Abstufung personalisierter autonomer Systeme

Autonome Systeme im Sinne dieser Arbeit bieten personalisierte Dienste an. Personalisierungen und Individualisierung autonomer Systeme sind in einzelnen Anwendungsbereichen essentiell, in anderen steigern sie die Effektivität einer Anwendung (1.). Je nach Anwendung unterscheidet sich der notwendige Personalisierungsgrad. Die Arbeit konzentriert sich auf personalisierte autonome Systeme, die auf eine bestimmte Person angepasst, d.h. individualisiert sind (2.).

1. Effektivitätsgewinne durch Personalisierung

In vielen Anwendungsbereichen autonomer Systeme bedarf es keiner Anpassung an die betroffene Person, bereits mit der Automatisierung erzielt man gute Ergebnisse. Vielfach sind individuelle Bedürfnisse und Kompetenzen für die Leistungskraft des Systems irrelevant oder die Bedürfnisse oder Kompetenzen

betroffener Personen sind so vergleichbar, dass sich über eine allgemeine Programmierung bereits der Personalisierungsbedarf abdecken lässt. So ist etwa bei autonomen Fahrzeugen, Sprachassistenten, oder Informationsfilterdiensten[81] eine Anpassung auf die NutzerInnen nicht notwendig, um gute Ergebnisse zu erzielen. In anderen Konstellationen, bei denen das Ergebnis eng mit Bedürfnissen oder Vorlieben betroffener Personen verknüpft ist, bedarf es dagegen einer Integration von Persönlichkeitseigenschaften in die Funktionsweise, etwa bei automatisierten Entscheidungen. Vielfach werden bereits generaltypisch-standardisierte Anpassungen, d.h. bloße Personalisierungen anhand generalisierbarer Bedürfnisse, Vorlieben oder Kompetenzen ausreichend sein. In anderen Bereichen bedarf es dagegen einer präzisen Adaption gerade an die betroffene Person, also einer Individualisierung. Dies betrifft Anwendungen, in denen die Eigenschaften der Einzelperson die Funktionsweise maßgeblich bestimmen und sich die anwendungsbezogenen Bedürfnisse von NutzerInnen wesentlich unterscheiden. Um diese soll es in dieser Arbeit gehen. Angesprochen sind damit hyperpersonalisierte Dienste, wie etwa persönliche Assistenten. Dort wird man nur zufriedenstellende Ergebnisse erzielen, wenn die Systeme fähig sind, sich spezifisch an die Eigenschaften gerade der betroffenen Person anzupassen.[82] Bei anderen Diensten ist die Personalisierung zwar nicht funktionsnotwendig, wirkt aber erheblich effizienzsteigernd.[83] Vor allem bei Empfehlungssystemen für Musik- und Videoplattformen[84] oder für News-

---

[81] Siehe auch *Finck/Biega*, Technology and Regulation 2021, 44, 50. Zu Suchdiensten Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 27; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 42, 62.

[82] Eingehend zu Ausgestaltungen, Charakteristika und aktuellen Angeboten personalisierter Assistenten auf dem Markt *Knote/Janson/Eigenbrod u.a.*, The What and How of Smart Personal Assistants, Multikonferenz Wirtschaftsinformatik 2018, 06.03.2018, S. 1083. Siehe zum Personalisierungsbedarfdes Assistenzsystems Alexa *Prasad*, „Ambient intelligence" will accelerate advances in general AI, Amazon Science, 21.01.2021 (https://www.amazon.science/blog/ambient-intelligence-will-accelerate-advancements-in-general-ai): „AI's ability to conform to customers as opposed to the other way around differentiates it from other technological advancements". *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 23 zufolge ist „personalised profiling [...] the *conditio sine qua non* of Ambient Intelligence (AmI), the vision of a networked environment that monitors its users and adapts its services in real time, permanently learning to anticipate the user's preferences in order to adapt to them".

[83] Siehe allgemein *Hengst/Grua/el Hassouni u.a.*, DS 2020, 1. Vgl. auch bereits *Myers/Berry/Blythe u.a.*, AI Magazine 28 (2007), 47, 53.

[84] Siehe hierzu etwa *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like; *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18; *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streaming dienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

Feeds sozialer Netzwerke,[85] bei der Produktsuche beim Online-Shopping[86] sowie bei der personalisierten Werbemaßnahmen[87] ließ sich beobachten, dass betroffene Personen umso besser angesprochen werden können, je präziser sie an das Interesse der betroffenen Person angepasst sind.[88] Bei automatisierten Entscheidungen geht es meist um Risikobewertungen von Personen, etwa beim Kredit-Scoring. Diese sind umso präziser, je umfassender und detailgenauer die Systeme risikorelevante Merkmale der spezifischen Person erfassen.[89] Auch die Individualisierung der Preisbildung verspricht gegenüber einer bloßen gruppenbezogenen Anpassung (mehr) wirtschaftliche Vorteile.[90] In den später noch zu erläuternden Referenzbeispielen soll genauer auf derartige Dienste und deren Individualisierungsbedarf eingegangen werden.[91]

2. Abstufung der Personalisierung autonomer Systeme und Themeneingrenzung

Damit lassen sich drei Arten autonomer Systeme ausmachen: Solche, die keiner Personalisierung bedürfen (generelle bzw. nicht-personalisierte autonome

---

[85] Siehe unten Kapitel 1 C. I. Eingehend zum Newsfeed von Facebook *Fagganella*, Your Feed is All You: The Nuanced Art of Personalization at Facebook, 18.08.2016 sowie die Beschreibungen zur Funktionsweise des Newsfeeds durch Facebook selbst unter *Meta AI*, The new AI-powered feature designed to improve Feed for everyone, 5.10.2022 (https://ai.facebook.com/blog/facebook-feed-improvements-ai-show-more-less).

[86] Ausführlich *Wood*, A New Kind of E-Commerce Adds a Personal Touch, New York Times 13.08.2014, https://www.nytimes.com/2014/08/14/technology/personaltech/data-driven-shopping-with-the-personal-touch.html. Siehe auch die Studie von McKinsey& Company, wonach 71 % der Befragten eine Personalisierung der Suche in einem Online-Handel erwarten und die Personalisierung maßgeblich die Kaufentscheidung oder Weiterempfehlung des Online-Handels beeinflusst, *Arora/Ensslen/Fiedler u.a.*, The value of getting personalization right – or wrong – is multiplying, 12.11.2021.

[87] Siehe unten Kapitel 1 C. II.

[88] *Smith*, A.I. Here, There, Everywhere, The New York Times 23.02.2021, https://www.nytimes.com/2021/02/23/technology/ai-innovation-privacy-seniors-education.html. kommt sogar zu dem Ergebnis: „Our interactions with the technology will become increasingly personalized".

[89] Siehe unten Kapitel 1 C III. 1. Zur Bedeutung der Profilbildung für automatisierte Entscheidungssysteme siehe auch *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 112: „In the data economy, many companies try to gain a competitive edge by extracting profiles and other hidden knowledge from large amounts of data via data mining and machine learning […]. Profiles extracted from large datasets are often regarded as useful knowledge for subsequent decision-making […]". Vgl. überdies *Lorentz*, Profiling, 2019, S. 11–12, 20–24. Siehe auch bereits *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 19: „Besides individuation, profiling mainly aims for risk-assessment and/or assessment of opportunities of individual subjects".

[90] Anschaulich *Hofmann*, WiRO 62 (2016), 1074, 1079 f.

[91] Siehe unten Kapitel 1 C.

Systeme), solche, die einer generell-typisierten Personalisierung bedürfen (standardisiert personalisierte autonome Systeme), und solche, die einer präzisen Personalisierung, dann also Individualisierung bedürfen (individualisiert personalisierte autonome Systeme).[92] Es hängt von der Anwendung ab, ob und in welchem Maße Personalisierungen erfolgen. Auch sind dabei wirtschaftliche Gesichtspunkte relevant, da die Umsetzung der Personalisierung, wie noch zu zeigen ist, ressourcenintensiv ist und der notwendige Ressourceneinsatz mit der Intensität der erwünschten Personalisierungsgrades steigt. Die Untersuchung betrachtet autonome Systeme, die individualisiert sind.

II. Technische Umsetzung der Personalisierung

Zur Personalisierung eines autonomen Systems bedarf es (unterschiedlich stark) personalisierter Algorithmen (1.). Die Automatisierung der Profilerstellung verspricht Qualitätsgewinne und Leistungssteigerungen autonomer Systeme (2.).

1. Personalisierung von Algorithmen durch Profile

Zur Integration von Nutzereigenschaften in den Lösungsalgorithmen sind verschiedene Verfahren gängig.[93] Typischerweise erfolgt die Personalisierung, indem benutzerrelevante Informationen in einen Lösungsalgorithmus Eingang finden. Die Persönlichkeitsmerkmale stellen also Entscheidungsparameter im Lösungsalgorithmus dar. Zusätzlich bedarf es dann Erkenntnisse über die betroffene Person.[94] Diese Erkenntnisse werden in einer Merkmalsmatrix dargestellt und in Form von Benutzerprofilen abgespeichert und so dauerhaft verfügbar gemacht.[95] Je nach Personalisierungsbedarf gestaltet sich der Detailgrad

---

[92] Der Unterschied zwischen standardisierter und individualisierter Personalisierung ist vor allem im Marketingbereich aufgearbeitet worden. Siehe zur Differenzierung etwa *Kwon/Kim*, Electronic Commerce Research and Applications 11 (2012), 101, 103; *Arora/Dreze/Ghose u.a.*, Marketing Letters 19 (2008), 305, 310 f.

[93] Siehe allgemein zur Funktionsweise personalisierter Systeme *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 330 f. Vgl. zu den einzelnen Problemen, für die ein autonomes System Lösungen finden muss, *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859, 875. Siehe zum Aufbau autonomer Systeme auch *Wahlster*, Informatik Spektrum 40 (2017), 409, 412–415; *Fachforum Autonome Systeme im Hightech-Forum*, Autonome Systeme, Deutsche Akademie der Technikwissenschaften; Hightech Forum, April 2017, S. 134.

[94] Vgl. *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859, 883 f.; *Wahlster*, Informatik Spektrum 40 (2017), 409, 414; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 113. Die Kenntnisse über die einzelnen NutzerInnen sind damit Teil des notwendigen Wissens zu einem Problem bzw. einer Aufgabe.

[95] *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 66. Siehe auch *Piao/Breslin*, User Modeling and User-Adapted Interaction

des Profils: Es kann generalisiert-typisierte Merkmale enthalten oder anwendungsrelevante Eigenschaften einer ganz bestimmten Person.[96] Hierauf ist noch zurückzukommen.[97] Für die Personalisierung bedarf es zusätzlich eines Verfahrens zur Zuordnung dieser Erkenntnisse zu einem bestimmten Nutzer.[98] So ist es sichergestellt, dass ein Nutzer bei Aufruf eines Dienstes ein auf ihn zugeschnittenes Angebot erhält, d.h. Algorithmus und Person im Einzelfall gekoppelt sind. Dies erfolgt über Identifizierungsverfahren, die es erlauben, das gespeicherte Benutzerprofil einer Person zuzuordnen. Typischerweise werden hierzu Logins oder BenutzerIDs, wie etwa der IP-Adresse genutzt.[99] Die personalisierte Ausgabe des Systems erfolgt dann dadurch, dass das Benutzerprofil durch den Lösungsalgorithmus verarbeitet wird.[100]

2. *Erstellung von Profilen durch autonome Systeme*

Anwendungsrelevante Benutzermerkmale können unmittelbar durch einen menschlichen Experten einprogrammiert oder direkt beim Nutzer erfragt werden (explizite Profilbildung).[101] Mit einer Automatisierung der Profilerstellung erzielt man jedoch bessere Ergebnisse (a)), mitunter führt allein die Verwendung Maschineller Lernverfahren zu guten Lösungen (b)).

---

28 (2018), 277, 280: „A user model is a (data) structure that is used to capture certain characteristics about an individual user". Noch präziser *Kunaver/Požrl*, Knowledge-Based Systems 123 (2017), 154, 155 f.: „The user model can be an independent data structure separate from the algorithm itself, a part of the algorithm itself or it can simply be presented as a collection of user's past actions in the form of a vector of item-rating pairs".

[96] Siehe hierzu auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 99.

[97] Zur Typisierung von Profilen zwischen generell-stereotypen und individuellen siehe unten Kapitel 1 B. III. 1. b).

[98] Vgl. *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 48 f.; *Lorentz*, Profiling, 2019, S. 47.

[99] Siehe eingehend zu verschiedenen technischen Möglichkeiten der Identifizierung *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 48–69; *Lorentz*, Profiling, 2019, S. 47–52.

[100] Siehe hierzu noch ausführlich unter Kapitel 1B. IV.

[101] *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 333; *Mitchell/Caruana/Freitag u.a.*, Communications of the ACM 37 (1994), 80, 81. Siehe auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, S. 8. Auch Likes sind explizite Rückmeldungen, vgl. *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like.

a) Automatisierung der Profilerstellung

Eine explizite Profilerstellung erfordert die Mitarbeit der NutzerInnen und deren Bereitschaft, zutreffende und ausführliche Angaben zu machen – und dies, während der gesamten Lebensdauer eines Systems.[102] Dies ist anspruchsvoll und nicht immer im Interesse der betroffenen Person, etwa bei automatisierten Entscheidungen. Auch für den Verantwortlichen ist dies ressourcenintensiv, muss er doch Persönlichkeitsmerkmale umfassend und fortlaufend aufnehmen und abspeichern. Demgegenüber lassen sich effektivere und präzisere Lösungen erreichen, wenn das Profil vom autonomen System selbst, d.h. automatisiert erstellt wird.[103] Dies erfolgt regelmäßig, indem aus beobachtetem Nutzerverhalten auf anwendungsrelevante Persönlichkeitsmerkmale geschlossen wird (implizite bzw. induktive Profilbildung,[104] verhaltensbezogene[105] oder lernende[106] Profilbildung).[107] Dies beruht auf der Annahme, dass persönliche

---

[102] Vgl. *Bozdag*, Ethics Inf. Technol 15 (2013), 209, 217; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 333 f.; *Mitchell/Caruana/Freitag u.a.*, Communications of the ACM 37 (1994), 80, 81.

[103] *Gasson/Browne*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 58, 59; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 19 bezeichnen dies als „automated profiling", *Nabeth*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 30, 33 als „autonomic profiling".

[104] *Frias-Martinez/Chen/Liu*, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), 734; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331; *Kanoje/Girase/Mukhopadhyay*, IJAFRC 2014, 120; *Rich*, Cognitive Science 3 (1979), 329, 332; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 202. Siehe daher auch die Definition des Profilings bei *Zukerman/Albrecht*, User Modeling and User-Adapted Interaction 11 (2001), 5: „The user-profiling or user-modeling task involves inferring unobservable information about users from observable information about him/her, for example their actions or utterances". Dies beruht auf der Annahme, dass persönliche Eigenschaften überwiegend gleich bleiben, sodass aus vergangenem auf zukünftiges Verhalten geschlossen werden kann, vgl. *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 337.

[105] *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, 47 „behavioural profiling".

[106] *Mitchell/Caruana/Freitag u.a.*, Communications of the ACM 37 (1994), 80, 82 „learning apprentice".

[107] Siehe auch *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 32; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 334 f. In der Praxis kommen auch hybride Methoden zum Einsatz. Bestimmte Daten, etwa das Alter oder bestimmte Interessen, werden direkt abgefragt, weitere Aspekte des Profils anhand beobachteten Verhaltens abgeleitet, vgl. *Frias-Martinez/Chen/Liu*, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), 734; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 334 f.; *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, 47. Vgl. für die Plattform Netflix *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like.

Eigenschaften gleich bleiben, sodass aus vergangenem Verhalten bzw. Persönlichkeitsmerkmalen auf gegenwärtige und zukünftige Verhaltensweisen bzw. Persönlichkeitsmerkmale geschlossen werden kann.[108] Aus dem Anklicken eines Informationsangebots wird dann etwa auf das Interesse an diesem Medieninhalt geschlossen. In der Praxis werden explizite und implizite Profilbildungsmaßnahmen häufig kombiniert.[109]

b) Automatisierung der Profilerstellung durch Maschinelle Lernverfahren

In bestimmten Anwendungsfällen erlaubt allein die Automatisierung der Profilerstellung eine technische Realisierung autonomer Systeme, nämlich dort, wo sich Zusammenhänge, d.h. Regeln zwischen Persönlichkeitsmerkmalen, Funktionselementen und erwünschten Ausgaben eines Dienstes aus einem Datensatz menschlich nicht mehr erkennen lassen. Hier kann man allein mit Maschinellen Lernverfahren gute Ergebnisse erzielen.[110] Dies ist vor allem bei Informationsfilterdiensten der Fall. Seit dort Maschinelle Lernverfahren zum Einsatz kommen, lassen sich deutliche Qualitätssteigerungen der automatisierten Empfehlungen verzeichnen.[111] Auch bei Kredit-Scorings anhand umfangreicher, unstrukturierter Datensätze erlaubt allein der Einsatz von Maschinellen

---

[108] *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 337; *Martini*, Blackbox Algorithmus, 2019, S. 4, 30.

[109] *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, S. 8.

[110] Siehe allgemein *LeCun/Bengio/Hinton*, Nature 521 (2015), 436–444.

[111] Zum Einsatz von Maschinellen Lernverfahren bei der Profilbildung siehe etwa *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 330; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 205. Hierin zeigt sich die Fortentwicklung der Künstlichen Intelligenz: Während dieses Wissen anfänglich detailreich von NutzerInnen vorgegeben werden musste (user-programming approach), kann auf nächster Stufe maschinelles Wissen über die Person in das System eingespeichert werden (knowledge-engineering approach). Beim Maschinellen Lernen kann die Profilbildung vollständig durch das System erfolgen werden (machine learning approach), vgl. *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331. Ähnliche Abstufungen bei *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 27–29. Zum Einsatz Maschineller Lernverfahren der Filmplattform Netflix siehe *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like, der Musikplattform Spotify *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html. Zum Einsatz im Newsfeed von Facebook *Meta AI*, The new AI-powered feature designed to improve Feed for everyone, 05.10.2022 (https://ai.facebook.com/blog/facebook-feed-improvements-ai-show-more-less).

Lernverfahren die Ableitung einer Scoreformel.[112] Hierauf ist noch zurückzukommen.[113]

3. Ergebnis und Themeneingrenzung: Automatisierte Profilerstellung als Funktionselement autonomer Systeme

Die automatisierte Profilerstellung unter Einsatz Maschineller Lernverfahren ist damit wesentlicher Teil der Funktionsweise autonomer Systeme in der Konzeption dieser Arbeit. Dabei unterscheiden sich die Inhalte der zu erstellenden Profile, je nachdem, ob eine Typisierung ausreichend oder eine Individualisierung eines Dienstes erwünscht ist. Die Arbeit konzentriert sich auf solche Systeme, die eine Individualisierung, dann also ein individuelles Profil voraussetzen. Welche Profile auf welche Weise durch autonome Systeme erstellt werden, soll im Anschluss im Einzelnen geklärt werden.

III. Automatisierung der Profilerstellung

Profile können unterschiedliche Inhalte haben. Um zu verdeutlichen, um welche Profile es im Rahmen dieser Arbeit geht, soll zunächst der Begriff des Benutzerprofils bzw. der Profilbildung kurz definiert und typische Inhalte eines Benutzerprofils vorgestellt werden (1.). Im Fokus dieser Arbeit stehen Individualprofile. Deren automatisierte Erstellung erfolgt, wie beschrieben, durch Ableitungen anhand beobachteten Nutzerverhaltens. Noch weitreichendere Erkenntnisse erlaubt dabei die Kombination von Gruppen- und Individualprofilen (2.). Dieses Verfahren soll näher erläutert werden (3.).

1. Definition des Profils und der Profilbildung sowie typische Profilinhalte

Im Nachfolgenden soll das Benutzerprofil bzw. die Profilerstellung definiert (a)) und zwischen Gruppen- und Individualprofilen unterschieden werden (b)). Abschließend sollen typische Inhalte von Profilen beschrieben werden (c)).

a) Arbeitsdefinition von Profil und Profilbildung

Für das Profil und die Profilbildung gibt es keine allgemeingültige Definition, der Begriff variiert mit dem Anwendungsbereich und -ziel.[114] In der Regel be-

---

[112] *Wang/Xiao*, Applied Sciences 12 (2022), 1; *Shi/Tse/Luo u.a.*, Neural Computing and Applications 34 (2022), 14327 f.

[113] Siehe unter Kapitel 1 C.

[114] Zur Unbestimmtheit des Begriffs des Profils siehe auch *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, 17 f.; *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 41 f.; *Lorentz*, Profiling, 2019, S. 119 f. Herausfordernd ist dabei, dass die Profilbildung (Profiling) ein rechtlicher Term ist, etwa der DSGVO, siehe dort Art. 4 Nr. 4 DSGVO. Auch die Definition des rechtlichen Terms bereitet Schwierigkeiten, siehe hierzu Kapitel 4 B. II 1. a).

zeichnet das Profil die Zusammenstellung von anwendungsrelevanten Eigenschaften über eine Person(engruppe), um diese zu beschreiben und mit dieser zu interagieren.[115] Die Profilbildung ist dann also die Erstellung dieses Wissens über eine Person. Bei der automatisierten, datenbasierten Profilerstellung kommt ein weiterer wesentlicher Aspekt hinzu: Durch die Datenanalyse ist es möglich, anwendungsrelevante Eigenschaften aus den vorhandenen Daten (sogenannte Rohdaten) abzuleiten, etwa Vorlieben oder Interessen, Verhaltensweisen, Kompetenzen oder Fähigkeiten. Darin liegen gerade Zweck und Mehrgewinn der automatisierten Profilerstellung. Es geht also nicht allein um eine bloße Sammlung und Speicherung bereits bekannter Einzelinformationen, sondern um einen über die Rohdaten hinausgehenden Erkenntnisgewinn über die betroffene Person(engruppe).[116] Dieser Erkenntnisgewinn soll die spezifische Anwendung ermöglichen, also etwa eine Kreditentscheidung oder die Anzeige eines Produktvorschlags. Die Profilbildung im Rahmen dieser Arbeit wird daher verstanden als automatisierte Ableitung von anwendungsrelevanten Persönlichkeitsmerkmalen einer bestimmten Person(engruppe) aus Rohdaten, dies mit dem Ziel der Verwendung für eine Entscheidung oder Maßnahme für diese Person(engruppe).[117]

---

[115] Vgl. etwa den Eintrag Profiling, in: Oxford University Press (Hrsg.), The Oxford English dictionary, [2]2023, mit interdisziplinärer sowie historischer Nachzeichnung des Begriffsverständnisses, dabei insbesondere die Definition unter 5.a.: „recording, itemization, or analysis of a person's known psychological, intellectual, and behavioural characteristics, esp. as documentation used (in schools, businesses, etc.) in the assessment of an individual's capabilities“. In *Dudenredaktion*, Profiling, Duden Online-Wörterbuch, 2023 wird Profiling als „für bestimmte Zwecke (z. B. zur Arbeitsvermittlung oder bei der Tätersuche) nutzbare Erstellung des Gesamtbildes einer Persönlichkeit“ verstanden. Vgl. auch die Definition bei *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 42 f., der die Merkmale Einmaligkeit (das Profil wird einer bestimmten Person zugeschrieben), Passivität (das Profil erstellen andere, nicht die betroffene Person) und Nachhaltigkeit (Profile werden beständig fortentwickelt und korrigiert, nicht aber gelöscht). Siehe auch *Lorentz*, Profiling, 2019, S. 33–34, 119.

[116] So auch *Lorentz*, Profiling, 2019, S. 120–122; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 538. Besonders im Online-Marketing wird diese Unterscheidung offenbar: Das Aufzeichnen von Daten wird dort als Tracking, die Analyse zur Erstellung eines Werbekundenprofils als Profiling bezeichnet. Beide stellen unterschiedliche (datenschutz-)rechtliche Fragen. Siehe zu dieser Differenzierung *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 71–74; *Lutz*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 203, Rn. 81. Zur Definition des Webtrackings siehe *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 48.

[117] Ähnliche Definionen bei *Lorentz*, Profiling, 2019, S. 33 f.; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 536. Siehe auch *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331; *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 35. Siehe auch *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 194; *Zukerman/Albrecht*, User Modeling and User-Adapted Interaction 11 (2001), 5: „User profiling implies inferring unobservable information about users from observable information about them, that is, their actions or ut-

Die Begriffe der Profilbildung und des Profilings sollen dabei synonym verwendet werden.[118]

b) Individual- und Gruppenprofile

Bezugsobjekt des Profils kann eine Gruppe sowie eine Individualperson sein. Grundlegend zu differenzieren sind daher Gruppen- und Individualprofile.[119] Gruppenprofile enthalten stereotype Eigenschaften einer Nutzergemeinschaft oder Untergruppe einer Nutzergemeinschaft.[120] Ist nur eine Personalisierung, nicht aber eine Individualisierung eines Dienstes beabsichtigt, kann bereits ein Gruppenprofil ausreichend sein. Individualprofile bilden dagegen allein die Persönlichkeitseigenschaften einer bestimmten Einzelperson ab.[121] Gruppenprofile können aber auch dazu dienen, Individualprofile zu erstellen. Im Gruppenprofil werden dann die Informationen über eine Nutzergemeinschaft so strukturiert, dass hieraus Erkenntnisse über einzelne Gruppenmitglieder, d.h. Einzelpersonen gewonnen werden können.[122] Das Gruppenprofil unterteilt die Nutzergemeinschaft in Vergleichsgruppen (auch: Kategorien) und weist denen bestimmte Attribute (auch: Prädikatoren) zu, etwa das Alter, Geschlecht oder die Vorliebe für ein Produkt. Diese Attribute werden dann zueinander in eine stochastische Verbindung gesetzt (Korrelationen).[123] Hierauf ist noch zurückzukommen. Dabei lassen sich distributive Gruppenprofile unterscheiden, bei denen sämtliche Gruppenmitglieder eine Eigenschaft teilen, und nicht-distributive, bei denen nur einzelne Gruppenmitglieder eine bestimmte Eigenschaft

---

terances". Ähnlich *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, 17–20.

[118] Zu dieser deutschen Übersetzung des Begriffs des Profilings siehe auch *Lorentz*, Profiling, 2019, S. 133 f.

[119] Vgl. hierzu eingehend *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 434. Siehe auch *Lorentz*, Profiling, 2019, S. 119 f.

[120] *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20; *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 40 f. Vgl. auch *Lorentz*, Profiling, 2019, S. 119.

[121] So auch *Lorentz*, Profiling, 2019, S. 119, die ebenso den Begriff des Individualprofils vorschlägt. Vgl. auch *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 40, der ebenso von „individual profiling" spricht.

[122] *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 536; *Lorentz*, Profiling, 2019, S. 35–37. Siehe bereits *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 21 f.; *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 42 f.

[123] *Lorentz*, Profiling, 2019, S. 68 f.; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 73 f. Siehe auch bereits *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20. *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, S. 35–36, 41.

aufweisen.[124] Bei distributiven Profilen passt das Gruppenprofil in seiner Gesamtheit, d.h. sämtliche Attribute auf das einzelne Gruppenmitglied, bei nicht-distributiven Profilen sind nur einzelne Attribute zutreffend.[125] In der Praxis sind nicht-distributive Profile am meisten verbreitet; dass alle Gruppenmitglieder alle Attribute teilen, ist eher selten.[126]

c) Typische Inhalte des Profils

Der Inhalt des Profils hängt vom jeweiligen Analyse- und Anwendungsziel ab.[127] Anwendungsrelevante Merkmale sind dabei vor allem solche deskriptiver, analytischer oder prädiktiver Natur.[128] Das Profil ordnet die anwendungsrelevanten Persönlichkeitsmerkmale und setzt sie zueinander bzw. zur Anwendung in Verbindung, ist dann also analytischer Art. Gruppenprofile sind typischerweise Profile mit analytischem Inhalt.[129] Das individuelle Profil einer Person soll antizipativ Anpassungen entsprechend ihrer Präferenzen oder Bedürfnisse vornehmen, so etwa bei Empfehlungssystemen. Dies verlangt eine Prognose ihrer Präferenzen und Bedürfnisse. Individuelle Profile weisen daher vielfach einen prädiktiven Inhalt auf.[130] In Anwendungen, in denen eine Entscheidung über eine Person getroffen werden soll, können prädiktive Aussagen um

---

[124] Eingehend *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 21. Siehe auch *Lorentz*, Profiling, 2019, S. 69.

[125] Vgl. auch *Lorentz*, Profiling, 2019, S. 69.

[126] *Lorentz*, Profiling, 2019, S. 69; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 21.

[127] Zu typischen Inhalten siehe die Darstellungen bei *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 194–200; *Webb/Pazzani/Billsus*, User Modeling and User-Adapted Interaction 11 (2001), 19, 20; *Frias-Martinez/Chen/Liu*, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), 734, 735; *Lorentz*, Profiling, 2019, S. 73; *Rao/Schaub/Sadeh*, What do they know about me? Contents and Concerns of Online Behavioral Profiles, Carnegie Mellon University Pittsburgh, 04.06.2015, S. 3–6.

[128] Vgl. zu derartigen Inhalten von Profilen *Europäischer Datenschutzausschuss*, S. 5: „Aspekte der Persönlichkeit oder des Verhaltens von Personen sowie ihre Interessen und Gewohnheiten [lassen sich] feststellen, analysieren und vorhersagen". Allgemein für die Big-Data-Analyse *Hoffmann-Riem*, AöR 142 (2016), 1, 7 f.; *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 11. Siehe auch die Definition des Profilings in Art. 4 Nr. 4 DSGVO, in der explizit auf die Evaluation, die Analyse und die Prognose von Persönlichkeitsmerkmalen abgestellt wird.

[129] Vgl. *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20. Siehe auch *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 10 f.

[130] *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 536; *Nabeth*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 30, 31; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 22. *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 51 sprechen sogar von „prediction models". Siehe auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, S. 8.

evaluative Informationen ergänzt werden, wenn etwa bestimmte Persönlichkeitsmerkmale als vorteilhaft oder nachteilig bewertet werden, so beim Kredit-Scoring.[131] Darüber hinaus enthält das individuelle Profil häufig auch deskriptive Beschreibungen, die für die Analyse, Prädiktion oder Evaluation notwendig sind. Hierzu zählen etwa demographische Angaben, aber auch Informationen zum Gesundheits- oder emotionalen Zustand.[132] Liegen hierzu keine Informationen vor, sondern sind diese anhand automatisierter Profilbildungsverfahren und Wahrscheinlichkeitsannahmen errechnet – hierzu sogleich –, sind diese deskriptiven Merkmale ihrerseits prädiktiver Natur.[133]

2. *Verfahren der automatisierten Profilbildung*

Die automatisierte Profilerstellung erfolgt über Auswertung von beobachtetem Verhalten einer Einzelperson oder Nutzergemeinschaft (a)). Weitaus umfassendere Erkenntnisse bei gleichzeitig geringem Bedarf an Informationen der betroffenen Person erlaubt eine Profilerstellungsmethode, bei der Gruppen- und Individualprofilbildung kombiniert werden ((bb).

a) Einstufiges Profilbildungsverfahren

Bei der direkten[134] oder auch content-based (inhaltsbezogenen)[135] oder personalisierten[136] Profilbildung werden allein Daten einer Person ausgewertet. Notwendig ist hier zunächst die Aufzeichnung von Nutzerverhalten,[137] sodann die Datenauswertung, aus der dann weitere anwendungsrelevante Informationen abgeleitet werden können.[138] Die Profilbildung besteht hier regelmäßig aus

---

[131] Vgl. *Lorentz*, Profiling, 2019, S. 12. Ebenso *Schermer*, CLSR 27 (2011), 45, 50: „Predictive data mining is particularly suited for making decisions in concrete cases".

[132] Siehe hierzu *Lorentz*, Profiling, 2019, S. 37–38, 72.

[133] Vgl. *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 11; *Lorentz*, Profiling, 2019, S. 37–38, 72; *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7.

[134] *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 41 f.

[135] Diese Bezeichnung wird im Rahmen von Vorschlagssoftware und personalisierter Informationssoftware gewählt, vgl. *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 337 „content-based".

[136] *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 22.

[137] *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 71 f.; *Lorentz*, Profiling, 2019, S. 41–59; *Härting*, CR 4 (2014), 528, 530 f.

[138] *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 73 f.; *Härting*, CR 4 (2014), 528, 531. Vgl. auch *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 35; *Mitchell/Caruana/Freitag u.a.*, Communications of the ACM 37 (1994), 80, 82.

zwei Verarbeitungsprozessen: die Datenakquise und die Datenauswertung.[139] Das Profil der Person steht hier unmittelbar am Ende des Datenauswertungsprozesses, es findet also nur eine Datenauswertung statt.[140]

b) Zweistufiges Profilbildungsverfahren

Die Erkenntnisse sind hier gleichwohl begrenzt auf solche Merkmale und Verhaltensweisen, die über die betroffene Person aufgezeichnet werden (können). Weitaus umfassendere Einblicke verspricht der Einbezug von Daten Dritter (indirekte,[141] stereotype[142] oder collaborative (kollaborative)[143] Profilbildung).[144] Sie sind in der Praxis vorherrschend.[145] Bei einem solchen Profilbildungsverfahren werden zunächst die Daten einer Nutzergruppe ausgewertet,

---

[139] So etwa *Härting*, CR 4 (2014), 528, 529–531; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 71–74; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 536–538. Ähnlich *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 114, die als dritte Verarbeitungsphase die Profilverwendung benennen.

[140] *Lorentz*, Profiling, 2019, S. 33 f. spricht von zweiphasiger Profilbildung, da nur zwei Verarbeitungsprozesse – die Datensammlung und *eine* Datenauswertung – erfolgen.

[141] So etwa *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 41–43.

[142] *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 335 f.; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 205.

[143] Die Begrifflichkeit des kollaborativen Profilings (collaborative filtering) werden vor allem bei Vorschlagssoftware oder personalisierten Informationen verwendet. Vgl. nur *Eke/Norman/Shuib u.a.*, IEEE Access 7 (2019), 144907, 144917; *Frias-Martinez/Chen/Liu*, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), 734, 735; *Zukerman/Albrecht*, User Modeling and User-Adapted Interaction 11 (2001), 5, 7.

[144] Teilweise wird unter Profilbildung allein diese Methode verstanden, vgl. etwa *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20; *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 48–53.

[145] So auch *Lorentz*, Profiling, 2019, S. 35; *Edwards/Veale*, SSRN Journal 2017, 35. So auch für den Streamingdienst Netflix *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like., und Spotify, so *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

typisierbare Nutzereigenschaften generalisiert und hieraus ein Gruppenprofil, auch als Modell[146] bezeichnet, gebildet.[147]
In einem zweiten Schritt wird eine Person einer Gruppe zugeordnet und dann die gesamten Gruppeneigenschaften auf diese übertragen.[148] Dies erfolgt über die Eingabe eines Anwendungsdatums in das Modell. Dieses zweistufige Profilbildungsverfahren beruht auf der Prämisse, dass Menschen und Situationen einander ähneln, Menschen bestimmte Eigenschaften teilen und sich in bestimmten Situationen auf vergleichbare Weise verhalten.[149]

Diese Methode hat den Vorteil, dass detailreiche Erkenntnisse über eine Person gewonnen werden können, obschon zu ihr nur wenige Rohdaten[150] vorlie-

---

[146] Zu diesem Begriff siehe *Lorentz*, Profiling, 2019, S. 35. *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 335 f.; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 205 bezeichnen diese als Stereotype. *Gasson/Browne*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 58, 59 sprechen von Generalisierung. In der informationstechnischen Literatur wird vielfach nicht zwischen Profil und Modell differenziert, der Begriff des Modells vielfach zur Beschreibung des Profils verwendet, vgl. etwa *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 51; *Dudley/Kristensson*, ACM Transactions on Interactive Intelligent Systems 8 (2018), 1 f.; *Eke/Norman/Shuib u.a.*, IEEE Access 7 (2019), 144907, 144917; *Frias-Martinez/Chen/Liu*, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), 734, 735; *Piao/Breslin*, User Modeling and User-Adapted Interaction 28 (2018), 277, 279 f., umgekehrt der Begriff der Profilbildung bzw. des Profilings für die Erstellung des Modells genutzt, so etwa *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 19; *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 48–53.

[147] Von statistischen Profilen sprechen *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 113. Es handelt sich dabei also um Gruppenprofile, siehe hierzu ausführlich *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 35 f.; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20.

[148] Eingehend *Lorentz*, Profiling, 2019, S. 35–31; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 335 f.; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 113 f.

[149] Die Wahrscheinlichkeitsberechnungen sind in der Praxis häufig diffiziler, da nicht notwendig davon ausgegangen werden kann, dass alle Mitglieder einer Gruppe tatsächlich dieselben Eigenschaften aufweisen; siehe zu distributiven und nicht distributiven Gruppenprofilen bereits oben Kapitel 1 B. III. 1. b) sowie *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 21. Hier müssen dann Untergruppen gebildet werden oder die gruppenabweichenden Merkmale durch anderer Gruppenzuordnungen ergänzt werden, vgl. auch *Lorentz*, Profiling, 2019, S. 69.

[150] Der Begriff der Rohdaten wird gewählt, um klar zwischen den direkten von der Person bereitgestellten Daten und den Daten, die durch die Profilbildung erzeugt werden, zu differenzieren. Dieselbe Begrifflichkeit verwendet *Lorentz*, Profiling, 2019, S. 39, 75. Auch die Begriffe volunteered bzw. observed data im Gegensatz zu inferred data (im Deutschen dann: direkt übermittelte, erhobene im Gegensatz zu abgeleiteten und hergeleiteten Daten) sind gebräuchlich, vgl. *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 32;

gen.[151] Darüber hinaus ist die zweistufige, gruppenbezogene Methodik der Profilbildung auch deshalb besonders interessant, da hier mit den Daten einer Personengruppe eine große Datenmenge mit einer hohen Anzahl verschiedener Persönlichkeitsmerkmale vorliegt. Dies erlaubt die Anwendung von Datenanalysemethoden zur Aufdeckung bislang unerkannter Zusammenhänge und Erkenntnisse über Persönlichkeitsmerkmale der Personengruppe.[152] Umso höher sind dann die Erkenntnismöglichkeiten über eine Einzelperson. In einem bekannten Fall konnte so eine Supermarktkette anhand der Analyse der Kaufhistorie ihrer Kunden auf die Schwangerschaft einer Einzelkundin schließen.[153]

Beim zweistufigen Profilbildungsverfahren finden im Ergebnis zwei Profilbildungen statt: Die Gruppenprofilbildung, hier bezeichnet als Modellbildung und die Individualprofilbildung, hier bezeichnet als Profilbildung.

Besonders präzise Ergebnisse sind mit hybriden Verfahren möglich, bei denen ein- und zweistufige Profilbildungsverfahren kombiniert werden.[154] Die weitere Untersuchung konzentriert sich auf das zweistufige Profilbildungsverfahren.

3. Technische Funktionsweise des zweistufigen Profilbildungsverfahrens

Beim zweistufigen Profilbildungsverfahren findet auf der Modellbildungsebene eine Big-Data-Analyse statt (a)). Hierbei kommen Maschinelle Lernverfahren zur Anwendung (b)). Im Anschluss wird in der Inferenzphase aus dem Modell ein individuelles Profil gebildet (c)).

Wachter/Mittelstadt, CBLR 2019, 494, 516; *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 8. Siehe auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 8. *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 113 unterscheiden declared und inferred data.

[151] *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 112; *Lorentz*, Profiling, 2019, S. 36–38; *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 22 f. Zum Einsatz dieser Verfahren beim Scoring *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 280.

[152] So auch *Lorentz*, Profiling, 2019, S. 35 f.; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 538. Vgl. auch *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 48 f.

[153] *Duhigg*, How Companies Learn Your Secrets, The New York Times Magazine 16.02.2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Siehe zu diesem Beispiel auch ausführlich *Lorentz*, Profiling, 2019, S. 36 f.

[154] Vgl. *Eke/Norman/Shuib u.a.*, IEEE Access 7 (2019), 144907, 144917; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 338; *Zukerman/Albrecht*, User Modeling and User-Adapted Interaction 11 (2001), 5, 15.

a) Modellbildung als Big-Data-Analyse

Auf Stufe der Modellbildung werden in den Datensätzen Muster erkannt.[155] Die Modellbildung ist im Ergebnis nichts anderes als eine Big-Data-Analyse,[156] auch Maschinelle Lernverfahren[157] – hierzu sogleich genauer – kommen zur Anwendung. Der jeweilige Anwendungskontext, die verfügbaren Daten, aber auch wirtschaftliche Gesichtspunkte bestimmen dabei über die Auswahl der Analysemethodik.[158] Typisch ist etwa die Bildung von Vergleichsgruppen.[159] Für diese vordefinierten Vergleichsgruppen werden bestimmte Merkmale als gruppentypisch erkannt, die dann eine Zuordnung einer Person zu einer bestimmten Gruppe erlauben. Diese Merkmale werden als Prädikatoren bezeichnet.[160] Ein derartiger Prädikator ist etwa der Wohnort, das Alter oder ein bestimmtes Produkt. Ein anderes Verfahren sind Association Rules. Vordefinierte Vergleichsgruppen gibt es hier nicht, vielmehr werden anhand der Analyse von Verbindungen und Beziehungen einzelner Parameter Gruppen gebildet. Diese Methode ist besonders bei der Warenkorbanalyse (welche Produkte werden typischerweise zusammen gekauft) gängig.[161] Das Ergebnis des Modellbildungsverfahrens ist eine komplexe Matrix, in der das mathematisch-stochastische Gerüst der Vergleichsgruppen, deren Verbindung zueinander und

---

[155] Vgl. auch *Lorentz*, Profiling, 2019, S. 37; *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 48 f. Zur Big-Data-Analyse *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 3–5; *Martini*, DVBl 129 (2014), 1481, 1482 f.; *Roßnagel*, ZD 3 (2013), 562.

[156] Eingehend *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 48–53; *Lorentz*, Profiling, 2019, S. 60–72; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 205–211; *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 71–79. Zu Verfahren der Big-Data-Analyse *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 9–16; *Hoffmann-Riem*, in: ders. (Hrsg.), Big Data, 2018, S. 11, 20 f.

[157] Der Einsatz Maschineller Lernverfahren ist auch im implizit-direkten Profilbildungsverfahren denkbar. Dann erfolgt der Maschinelle Wissensgewinn anhand der Daten der Einzelperson. Das System entwickelt hieraus ein Muster und also Regelset aus den anwendungsrelevanten Merkmalen, etwa dem Interesse einer betroffenen Person. Die algorithmischen Erkenntnismöglichkeiten sind hier aber weitaus geringer, schon allein deshalb, da weit weniger Daten zur Verfügung stehen, aber auch deshalb, da der Aussagegehalt der Trainingsdaten geringer ist, denn diese beinhalten allein Informationen zur Einzelperson.

[158] *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 51.

[159] *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 10; *Lorentz*, Profiling, 2019, S. 68 f.

[160] *Lorentz*, Profiling, 2019, S. 36. Vgl. auch *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 10 f.

[161] Siehe hierzu *Lorentz*, Profiling, 2019, S. 69 f.; *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 12 f.; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 207–209; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 73.74; *Tene/Polonetsky*, Northwest. J. Technol. Intellect. Prop. 11 (2013), 239, 270.

die Prädikatoren in formaler Sprache abgebildet sind.[162] Diese Matrix ist zugleich das algorithmische Regelwerk für die Profilerstellung.

b) Insbesondere: Modellbildung durch Maschinelle Lernverfahren

Bei der Datenauswertung im Rahmen der Modellbildung kommen Verfahren des Maschinellen Lernens zum Einsatz (aa)). Typischerweise werden dabei fünf Verarbeitungsschritte durchlaufen (bb)). Je nach gewähltem Verfahren unterscheiden sich die Respräsentationsformen des Modells (cc)).

aa) Maschinelle Lernverfahren in der Modellbildung

Maschinelle Lernverfahren bei der Modellbildung versprechen ein hohes Maß an Automatisierung, Präzision und Erkenntnistiefe.[163] Algorithmen des Maschinellen Lernens können die Daten anhand einer Vielzahl von Parametern parallel analysieren, vor allem können sie Muster in den Daten erkennen, die in der menschlichen Analyse unentdeckt blieben. Zudem erlauben sie eine dynamische Anpassung und beständige Fortentwicklung der Anwendungen.[164] Sie kommen in der Praxis daher zunehmend zum Einsatz.[165]

---

[162] *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 336 f. Vgl. auch *Lorentz*, Profiling, 2019, S. 36.

[163] Zum Einsatz von Maschinellen Lernverfahren bei der Profilbildung siehe etwa *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 330; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 205. Zum Einsatz Maschineller Lernverfahren durch Netflix siehe *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like., der Musikplattform Spotify *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

[164] Siehe zu diesen Vorteilen *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 333. Noch deutlicher, wenngleich nicht explizit zu personalisierten autonomen Systemen im Sinne dieser Arbeit, *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 859, 860: „Klar scheint vor allem zu sein, dass für die Realisierung von Assistenzsystemen KI-Verfahren benötigt werden".

[165] *Lorentz*, Profiling, 2019, S. 64 f.; *Eke/Norman/Shuib u.a.*, IEEE Access 7 (2019), 144907, 144915 f. Siehe für Streamingdienste *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like.; *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18; *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html. Für die Erstellung von Kreditscores *Shi/Tse/Luo u.a.*, Neural Computing and Applications 34 (2022), 14327–14339; *Wang/Xiao*, Applied Sciences 12 (2022), 1–14 Siehe hierzu auch bereits *Fawcett/Provost*, in: Simoudis/Han/Fayyad (Hrsg.), Proceedings / Second International Conference on Knowledge Discovery & Data Mining, 1996, S. 8.

Das Modell ist die algorithmische Lösungsstrategie zur Erstellung des Profils. Das Profilbildung ist also das Problem, für das das autonome System anhand Maschineller Lernverfahren eigenständig eine Lösung entwickeln soll. Hierfür kommen überwachte, nicht überwachte, hybride und verstärkende Methoden des Maschinellen Lernens zum Einsatz. Überwachte Verfahren setzen voraus, dass bereits Grundkenntnisse zum Datensatz vorliegen, etwa zu den einzelnen Gruppen.[166] Es geht dann vornehmlich um das Auffinden von Prädikatoren für die Zugehörigkeit zu einer Gruppe, die eine präzise Zuordnung eines unbekannten Falles in diese Gruppe erlaubt. Ähnlich ist dies beim bestärkenden Lernverfahren, bei dem zumindest bekannt sein muss, welche Gruppierungen bzw. Ausgaben erwünscht sind und welche nicht.[167] Beim unüberwachten Lernverfahren kann dagegen ohne Kenntnisse über Strukturen des Datensatzes ein Algorithmus über die anwendungsrelevanten Nutzereigenschaften gebildet werden.[168] Diese Lernverfahren sind besonders in Umgebungen sinnvoll, in denen sich Strukturen und Zusammenhänge zwischen einzelnen Persönlichkeitsmerkmalen menschlich nicht erkennen lassen, etwa bei Empfehlungssystemen[169] oder der personalisierten Werbung.[170]

---

[166] *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 50 f.; *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 67; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 344–351. Im Rahmen eines Kredit-Scoring sind etwa die Gruppen „Personen, die den Kredit bedient haben" und „Personen, die zahlungspflichtig geblieben sind" gegeben. Es werden dann Eigenschaften ermittelt, die die Personen in dieser Gruppe jeweils teilen. So kann etwa das Einkommen, das vorhandene Vermögen oder das Alter, aber auch der Bildungsabschluss, der Wohnort oder der Familienstatus als Prädikator herausgearbeitet werden. Siehe hierzu eingehend *Bao/Lianju/Yue*, Expert Systems with Applications 128 (2019), 301, 302.

[167] Vgl. zum bestärkenden Lernen bei der Modellbildung *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 67. Siehe allgemein zum Einsatz des Reinforcement Learnings bei Empfehlungssystemen *Afsar/Crump/Far*, Reinforcement learning based recommender systems: A survey, 15.01.2021.

[168] Siehe auch bereits *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 48 f.; *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 67; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 352 f.

[169] Für welche Beiträge, Musiktitel oder Filme eines Streamingdienstes oder einer Online-Plattform typischerweise ein einheitliches Interesse besteht, wie diese also in Interessensgruppen geordnet werden können, ist für den Menschen regelmäßig nicht erkennbar. Siehe zum Einsatz unüberwachter Lernverfahren bei Empfehlungssystemen *Cintia Ganesha Putri/Leu/Seda*, Symmetry 12 (2020), 185–212 Siehe zu Streamingdiensten *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

[170] Besonders für die Warenkorbanalyse erweisen sich unüberwachte Lernverfahren als besonders ergiebig, siehe etwa *Liu*, Using Unsupervised Learning to Detect Purchase Prefe-

Bei den klassischen Maschinellen Lernverfahren muss aber vorab bekannt sein, dass sich aus den Daten brauchbare Muster zu Nutzerverhalten abstrahieren lassen. Dem Maschinellen Lernverfahren geht damit stets eine Voranalyse im Rahmen des Data Minings vor. Anders ist dies bei modernen Maschinellen Lernverfahren, dem Deep Learning. Hier kann ganz ohne Vorstrukturierung ein algorithmisches Modell in Form eines künstlichen neuronalen Netzes entwickelt werden.[171] Diese Methodik ist allerdings, wie ausgeführt,[172] daten- und ressourcenintensiv. In der Praxis wird man sie nur einsetzen, wo klassischen Maschinellen Lernverfahren nicht ausreichen oder jedenfalls Modelle des Deep Learnings deutlich bessere Ergebnisse erzielen, die sich wirtschaftlich verwerten lassen.[173]

bb) Verfahrensschritte bei der Modellbildung

Das Maschinelle Lernverfahren – wie im Übrigen auch die klassische Big-Data-Analyse – gliedert sich üblicherweise in fünf Schritte:[174] Die Problemdefinition, die Datenauswahl, die Datenaufbereitung, darunter die Datenaufspaltung in Trainings- und Testdaten, die Analyse, die Evaluation, Verifikation bzw. Testung.[175] Eine menschliche Gegenprüfung gewährleistet die Akkura-

---

rences in Retail Stores, Medium, 08.01.2019 (https://medium.com/@tianjiaoliu2012/using-unsupervised-learning-to-detect-purchase-preferences-in-retail-stores-7e5cd592c7ee). Zur Verwendung beim Kredit-Scoring siehe *Bao/Lianju/Yue*, Expert Systems with Applications 128 (2019), 301–315 Das Kredit-Scoring erfolgt typischerweise als überwachtes Lernverfahren, da hier die Gruppeneinteilung – kreditwürdig oder nicht – bereits vorgegeben ist, also allein Prädikatoren zu ermitteln sind.

[171] Zum Einsatz von Deep Learning bei Empfehlungssystemen *Liu/Wu*, in: Kim/Joukov (Hrsg.), Information Science and Applications 2017, 2017, Bd. 424, S. 451; *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18 sowie beim Kredit-Scoring *Wang/Xiao*, Applied Sciences 12 (2022), 1–14. Siehe allgemein zur Verwendung von Deep-Learning-Verfahren bei der Modellbildung bereits *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 77 f.; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 351 f.; *Paradarami/Bastian/Wightman*, Expert Systems with Applications 83 (2017), 300–313.

[172] Siehe oben Kapitel 1 A. II. 2. d).

[173] Vgl. auch *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html. Zum Einsatz von Deep Learning durch Netflix siehe *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18.

[174] Innerhalb dieser fünf Schritte laufen tatsächlich eine Vielzahl einzelner Verarbeitungsprozesse ab. Zudem müssen nicht notwendig alle Verarbeitungsschritte durchlaufen werden. Die Einteilung ist daher im Sinne einer idealisierten Strukturierung zu verstehen, nicht als akkurate Beschreibung der tatsächlichen technischen Geschehnisse.

[175] *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 50–52. Vgl. auch *Lorentz*, Profiling, 2019, S. 66–72. Siehe zu den Phasen

tesse des gebildeten Modells im Hinblick auf seine Funktionstauglichkeit und Ergebnisrichtigkeit.[176] Die Auswahl des Modells ist durchaus anspruchsvoll, vor allem bei unüberwachten Lernverfahren, da nicht alle aufgefundenen Muster und Verbindungen tatsächlich von Relevanz sind.[177] Das Modell kann durch weitere Aspekte angereichert und so präziser gestaltet werden. Der Trainingsprozess ist dabei kontinuierlich und iterativ: Die Anwendungsdaten aus der Profilbildung dienen zugleich als Trainingsdaten des Modells.[178] So können immer neue Muster in den Daten erkannt und das Modell flexibel gehalten, erweitert, präzisiert und an Änderungen der Umwelt angepasst werden.

cc) Repräsentationsformen zwischen symbolischen und subsymbolischen Lernverfahren

Das Modell ist am Ende ein algorithmisches Konstrukt. Das gewählte Lernverfahren entscheidet über die Repräsentation des Modells. Bei tradierten, symbolischen Lernverfahren ist das Modell in menschlich auslesbarer formaler Symbolsprache und logischen Regeln dargestellt. Vergleichsgruppen und Prädikatoren liegen hier vor und können eingesehen werden. Anders ist dies bei subsymbolischen Methoden. Hier ist das Modell ein komplexes, vielstufiges geschachteltes algorithmisches Konstrukt, das menschlich erkennbare Gruppierungen, Prädikatoren oder Verbindung nicht enthält.

---

der Big-Data-Analyse *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 300–302; *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 8–16.

[176] Geprüft wird das Model, zumindest soweit es symbolischen Methoden entstammt, im Hinblick auf Wahrheitsgehalt, Relevanz, Nützlichkeit oder Plausibilität, vgl. hierzu *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 52 f.; *Frias-Martinez/Chen/Liu*, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), 734, 736; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 355. Maschinelle Lernverfahren sind technikbedingt fehleranfällig, die Kontrolle ist daher besonders wichtig. Typisch sind etwa Phänomene des Overfittings, bei dem das Modell unzutreffend Muster erkennt oder den Trainingsdatensatzes umfassend imitiert (auswendig lernt), sowie des Underfittings, bei dem das Modell zu grobschlächtig und oberflächlich gerät und relevante Variablen nicht abgebildet sind. *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 52. Eingehend zum Overfitting siehe *Domingos*, Communications of the ACM 2012 (2012), 78, 80 f.; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 663 f., zum underfitting *Alpaydın*, Machine learning, 2021, S. 40.

[177] Vgl. hierzu, wenngleich im Rahmen der Big-Data-Analyse, *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 13; *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 33 f.

[178] *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 353; *Canhoto/Backhouse*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 47, 53; *Lorentz*, Profiling, 2019, S. 40 f.

c) Profilerstellung und Inferenzphase

Auf Stufe der Profilbildung wird das Modell auf die Einzelperson angewendet.[179] Dies wird auch als Inferenz bezeichnet.[180] Dies geschieht durch Eingabe eines Einzeldatums in das Modell.[181] Meist ist für eine klare Zuordnung die Eingabe mehrerer Einzeldaten notwendig, etwa das Alter und der Wohnort oder mehrere Produktangebote. Entspricht dieses Einzeldatum einem Prädikator, wird die Person der oder den zugehörigen Vergleichsgruppen zugeordnet und die Merkmale der Vergleichsgruppe auf diese Person übertragen. Bei Association Rules werden die mit einem Merkmal (statistisch) eng verbundenen Merkmale ausgegeben, also etwa Produkte, die mit dem gekauften in enger Verbindung stehen.[182]

Den Inferenzbildungen anhand des Modells liegen Wahrscheinlichkeitsberechnungen zugrunde:[183] Aus dem Prädikator wird die Wahrscheinlichkeit der Gruppenzugehörigkeit, aus der Gruppenzugehörigkeit die Wahrscheinlichkeit des Vorliegens eines Attributs der Gruppe berechnet, aus einem Attribut die Wahrscheinlichkeit der Zugehörigkeit weiterer Attribute. Die Zuordnungen

---

[179] *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 42 f.; *Lorentz*, Profiling, 2019, S. 72 f.; *van Otterlo*, in: Hildebrandt/Vries (Hrsg.), Privacy, due process and the computational turn, 2013, S. 41, 50. *Rich*, Cognitive Science 3 (1979), 329, 345 ff. spricht dann von user synopsis. Hier wird auch teilweise von Inferenzbildung gesprochen, so etwa *Lorentz*, Profiling, 2019, S. 73. Vgl. auch *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 43 f.

[180] So etwa *Lorentz*, Profiling, 2019, S. 35; *Wachter/Mittelstadt*, CBLR 2019, 494, 506, siehe auch *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 112. Vgl. auch *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 537. Der Term „Inferenzbildung" wird auch für Ableitung einer anwendungsrelevanten Eigenschaft aus individuell beobachtetem Nutzerverhalten, d.h. bei der direkten impliziten Profilbildung verwendet, vgl. etwa *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 112; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 330; *Piao/Breslin*, User Modeling and User-Adapted Interaction 28 (2018), 277, 280; *Wachter/Mittelstadt*, CBLR 2019, 494–620; *Zukerman/Albrecht*, User Modeling and User-Adapted Interaction 11 (2001), 5.

[181] Wie bei der Modellbildung werden dort die Verfahrensschritte der Datenauswahl, der Vorbereitung, der Analyse – hier durch das Modell – und der Testung und Evaluation durchlaufen. Siehe auch *Lorentz*, Profiling, 2019, S. 72 f.; *Jaquet-Chiffelle*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 34, 41–43.

[182] *Anrig/Browne/Gasson*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 65, 73; *Lorentz*, Profiling, 2019, S. 69 f. Allgemein zur Big-Data-Analyse *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 11–14.

[183] Vgl. auch *Lorentz*, Profiling, 2019, S. 73; *Wachter/Mittelstadt*, CBLR 2019, 494, 509. Siehe auch *Bygrave*, Data protection law, 2002, S. 309.

sind daher potentiell unzutreffend, etwa wenn fehlerhaft eine Einordnung erfolgt („false positives") oder gerade nicht („false negatives").[184]

Die errechneten Profilinhalte werden auch als Output-Daten,[185] abgeleitete bzw. hergeleitete Daten,[186] neu generierte Daten[187] oder inferierte Daten[188] bezeichnet.[189]

d) Vorverfahren: Datenakquise zur Erstellung von Trainings- und Anwendungsdaten

Sowohl die Modellbildung als auch die Profilbildung setzen eine Datenerhebung voraus.[190] Die zu erhebenden Daten unterscheiden sich bei der Modell- und Profilbildung: Dort sind es Trainingsdaten, hier sind es Anwendungsdaten, dort stammen sie von einer Vielzahl von Nutzern, hier allein vom einzelnen NutzerInnen.[191] Wie beschrieben erfolgt die Datenakquise selten durch Direkteingabe der NutzerInnen,[192] sondern mittels Datenaufzeichnung durch das

---

[184] Wird etwa eine hohe Wahrscheinlichkeit errechnet, dass eine Person vermögend ist, ist sie es aber tatsächlich nicht, spricht man von false positives. Wird dagegen eine geringe Wahrscheinlichkeit für ein hohes Vermögen berechnet, ist die Person aber doch vermögend, wird dies als false negative bezeichnet. Siehe hierzu *Martini*, Blackbox Algorithmus, 2019, S. 55.

[185] *Lorentz*, Profiling, 2019, S. 72.

[186] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 8.

[187] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 10; *Lorentz*, Profiling, 2019, S. 72.

[188] *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 112; *Wachter/Mittelstadt*, CBLR 2019, 494–620; *Kreitz/Frank*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 143; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 537; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 113.

[189] Hierdurch wird begrifflich verdeutlicht, dass anhand der Verarbeitung des oder der Rohdaten darüber hinausgehende, neue Erkenntnisse über eine Person gewonnen werden.

[190] Im Ergebnis finden so drei relevante Datenverarbeitungen durch autonome Systeme statt: Datenakquise, Modellbildung und Profilbildung. So auch *Lorentz*, Profiling, 2019, S. 38; *Schreurs/Hildebrandt/Kindt u.a.*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 241, 246–256. Mit anschaulicher Übersicht *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 327 f. Ähnlich *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 114., die aber Modell- und Profilbildung als einen einheitlichen Verarbeitungsprozess erkennen.

[191] Vgl. *Lorentz*, Profiling, 2019, S. 35, 72.

[192] Möglich ist dies etwa durch Eingabefelder in Apps oder in Kundenaccounts, vgl. *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 224 f. Siehe auch *Giesbrecht*, This is

System selbst, üblicherweise während der Nutzung eines konkreten Dienstes. Typisch sind etwa Tracking-Maßnahmen (auch bezeichnet als Consumer Tracking[193] oder Web Tracking[194]), bei denen die Zugangsgeräte, etwa das Smartphone oder der Laptop, Verhaltensweisen aufzeichnen, so etwa das Aufrufen von Webseiten, Browsing-Verhalten, Likes oder das Anklicken von Angeboten.[195] Im analogen Raum erfolgt dies über Sensoren, etwa Wearables,[196] Smart-Home-Einrichtungen oder sonstige Smarte Alltagsgeräte.[197] Möglich ist

---

how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like. Bei Kreditverträgen sind auch Selbstauskünfte oder Abfragen bei Schuldnerverzeichnissen möglich, vgl. hierzu *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 288 f.

[193] Das Browsing-Verhalten kann etwa Cookies oder IP-Adressen ausgelesen werden, vgl. *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 19 f. Demographische Informationen können insbesondere über Kontodaten erhoben werden, vgl. *ders.*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 19. In der real-physischen Welt bedarf es des Einsatzes von Hardwareelementen, etwa Sensoren, und von Programmen für die Übersetzung der aufgezeichneten analogen Phänomene ins Digitale, etwa durch maschinelles Sprachverständnis, vgl. auch *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 112; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 333 f.; *Miller*, J. Law Technol. Policy 2014, 41, 45. Auch Kundenkarten oder Payback-Systeme können Verhalten in der analogen Welt digital abspeichern, siehe *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 227; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 114. Schließlich können auch Interaktionen mit dem System selbst aufgezeichnet werden, wenn etwa durch das System erarbeitete Lösungen angenommen, abgelehnt oder geändert werden, vgl. *Mitchell/Caruana/Freitag u.a.*, Communications of the ACM 37 (1994), 80, 84 f.

[194] Siehe zu diesem Begriff *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 48–50; *Lorentz*, Profiling, 2019, S. 47.

[195] Vgl. ausführlich *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 51–70; *Lorentz*, Profiling, 2019, S. 44 f. Nicht ganz klar ist die Abgrenzung zum Profiling: Teilweise wird das Tracking synonym zur Profilbildung, teilweise als technische Methode der Identifizierung von Daten, d.h. der Zuordnung von aufgezeichnetem Verhalten zu einer Person, teilweise in der Nachverfolgung der Verhaltensweisen einer bestimmten Person im Netz verstanden. Das Tracking ist überzeugenderweise nicht gleichbedeutend der Profilbildung, es kann vielmehr Teil hiervon sein. Das Nachverfolgen einer Person setzt freilich die Identifizierung dieser Person voraus, sodass im Ergebnis die beiden letztgenannten Aspekte vom Trackingbegriff erfasst sind. So auch *Lorentz*, Profiling, 2019, S. 47 f.; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 48–50.

[196] Insbesondere Informationen zu körperlichen Merkmalen und Zuständen können über Wearables oder Quantified-Self-Technologien erhoben werden, zB Schrittzähler, aufgezeichnet werden, vgl. *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 240.

[197] Siehe hierzu *Härting*, CR 4 (2014), 528, 530; *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 159; *Tene/Polonetsky*, Northwest. J. Technol. Intellect. Prop. 11 (2013), 239, 240. Siehe auch im Rahmen personalisierter Werbung *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting,

auch – gerade für die Modellbildung – der Erwerb von Daten durch Drittanbieter.[198]

IV. Automatisierung der Anwendung

Das Profil allein löst aber noch nicht eine automatisierte Steuerung oder Entscheidung aus. Es bedarf daher, wie oben bereits beschrieben, eines Lösungsalgorithmus und dessen Anwendung.[199] Dies erfolgt regelmäßig durch Verarbeitung des Profils sowie gegebenenfalls weiterer Daten. Profilbildungs- und Profilverwendungsverfahren[200] sind dabei zu unterscheiden (1.). Die Regelbildung im Lösungsalgorithmus erfolgt durch stochastische Verknüpfung von bestimmten Inputs mit erwünschten Outputs (2.). Auch bei der Erstellung des Lösungsalgorithmus können Maschinelle Lernverfahren zum Einsatz kommen (3.).

1. Differenzierung von Profilbildung und Profilverwendung

Je nach Methode der Personalisierung unterscheidet sich das Verfahren der Integration des Profils in den Lösungsalgorithmus. Benutzerprofil und Lösungs-

---

2015, S. 33. Vgl. auch *Lorentz*, Profiling, 2019, S. 45–46, 55–56. Gerade darin zeigt sich ein Verschwimmen der Welten zwischen Online und Offline.

[198] Hierfür haben sich eigene Märkte herausgebildet, auf denen Datenhändler (Data Broker) die selbst aus verschiedenen Quellen erhobenen oder ihrerseits aus Drittquellen erworbenen Daten zum Kauf anbieten. Siehe hierzu eingehend die Studie *Federal Trade Commission*, Data Brokers, Mai 2014. Vgl. auch *Lorentz*, Profiling, 2019, S. 56–59; *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 301. Siehe allgemein zur Monetarisierung von Daten und zur Entstehung von Datenmärkten *Zuboff*, The age of surveillance capitalism, 2019; *West*, Business and Society 58 (2019), 20–41.

[199] Wenngleich es hier um individualisierte autonome Systeme geht, lässt sich dem Folgenden auch die Funktionsweise personalisierter sowie genereller autonomer Systeme entnehmen: Die Personalisierung mittels eines generalisiert-typisierten Profils erfolgt ähnlich; bei nicht-profilbasierten autonomen Systemen entfällt die vorherige Stufe der Profilbildung und die nachfolgende Stufe der Personalisierung. Es wird dann nur ein Lösungsalgorithmus gebildet und angewandt.

[200] Da der Begriff der Profilanwendung häufig für die Erstellung des konkreten Profils – im zweistufigen Profilbildungsverfahren also für die Erstellung des konkreten Profils aus dem Modell – genutzt wird, vgl. etwa *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 8; *Lorentz*, Profiling, 2019, S. 35–41, 72–73; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 55, wird zur Klarstellung der Verfahrensschritt der Auslösung der Steuerungsarchitektur der Umgebungsintelligenz mittels des Profils der Term der Profilverwendung genutzt. Die englische Begrifflichkeit ist hier präziser: Während die Profilerstellung und -anwendung als Profile Application bezeichnet wird, wird die automatisierte Entscheidung bzw. Steuerung durch die Profilverwendung als Profile Use bezeichnet, vgl. mit anschaulicher Übersicht *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 327 f.

algorithmus und auch deren Erstellungsverfahren lassen sich technisch nicht immer klar trennen, die einzelnen dabei stattfindenden Verarbeitungsprozesse gehen vielfach ineinander über.[201] Entsprechend vielfältig sind die Vorschläge zu Abstrahierungen, Untergruppierungen und Bezeichnungen. Gemeinhin wird der Prozess der Profilerstellung und derjenige der Bildung des Lösungsalgorithmus unterschieden,[202] ebenso der Prozess der Profilerstellung und der Profilverwendung.[203] Denn die Verarbeitungsziele, Daten, Algorithmen und Outputs unterscheiden sich wesentlich.[204] Je nach Automatisierungsgrad des Systems wird diese Lösung unmittelbar operativ umgesetzt, etwa ein Medieninhalt bei einem Suchdienst angezeigt, oder es bedarf für die Umsetzung der Beteiligung eines Menschen, so etwa bei der automatisierten Kreditvergabe, bei der das System lediglich einen Entscheidungsvorschlag ausgibt.

2. Grundlegende Funktionsweise des Lösungsalgorithmus

Algorithmische Lösungsverfahren basieren wesentlich auf konditionalen Verbindungen („wenn-dann“).[205] Der Lösungsalgorithmus muss damit ein Regelwerk enthalten, das die Profilinhalte mit einer spezifischen Ausgabe in eine konditionale Beziehung setzt, etwa das Interesse an einem Produkt mit einer entsprechenden Werbemaßnahme.[206] Notwendig ist dabei die Bestimmung von Schwellenwerten: Erst wenn dieser erreicht ist, wird der erwünschte Output,

---

[201] *Lorentz*, Profiling, 2019, S. 74. Vgl. auch *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 32.

[202] So auch *Lorentz*, Profiling, 2019, S. 34, 73–74; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 114. Implizit kommt diese Unterscheidung darin zum Ausdruck, dass Arbeiten, die sich mit der Profilbildung beschäftigen, keine Ausführungen zur Profilverwendung enthalten, siehe etwa *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 71–75; *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 78–81. Letztlich kommt diese Unterscheidung auch in Art. 22 DSGVO zum Ausdruck, in der zwischen Profiling und automatisierter Entscheidung differenziert wird. In der Praxis gehen Profilbildung und -verwendung häufig ineinander über, so *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 32, vgl. auch *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331.

[203] *Lorentz*, Profiling, 2019, S. 73 f.

[204] Bei der Profilbildung geht es darum, anwendungsbezogenes, maschinell lesbares Wissen über eine bestimmte Person zu bilden, siehe *Lorentz*, Profiling, 2019, S. 33; *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331. Bei der Profilverwendung bzw. der Umsetzungsphase ist Ziel die Ausgabe einer konkreten Entscheidung oder Steuerung. Vgl. hierzu auch *Lorentz*, Profiling, 2019, S. 73 f.

[205] Siehe allgemein zur Funktionsweise algorithmischer Lösungsmechanismen *Martini*, Blackbox Algorithmus, 2019, S. 19 f.

[206] Vgl. *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331. Siehe auch *Lorentz*, Profiling, 2019, S. 74; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 88.

etwa eine Werbeanzeige, ausgegeben.[207] Kommen in einer Anwendung mehrere Outputs in Betracht, muss zusätzlich eine Priorisierung der Outputs erfolgen.[208] Komplexer stellt sich die Situation dar, wenn neben dem Profil weitere Variablen berücksichtigt werden sollen. Der Lösungsalgorithmus muss all diese Entscheidungsvariablen mit dem erwünschten Output in eine stochastische Beziehung setzen.[209] Je mehr Variablen und je diffiziler deren Verhältnisse zueinander sind, desto komplexer gestaltet sich das algorithmische Konstrukt.

3. Erstellung des Lösungsalgorithmus durch Maschinelle Lernverfahren

Der Lösungsalgorithmus kann menschlich vorgegeben werden. Dabei ist vor allem die Definition von Schwellenwerten notwendig, ab dem eine bestimmte Ausgabe erfolgen soll.[210] Der Algorithmus kann aber auch in einem Maschinellen Lernverfahren gebildet werden.[211] Wiederum entscheidet die Komplexi-

---

[207] In einem klassischen Algorithmus würde etwa programmiert, dass bei Anhören des Musiktitels A als nächstes der Musiktitel B ausgegeben wird. Hier gibt es keine Wahrscheinlichkeiten, sondern absolute Angaben. Ein Algorithmus der Künstlichen Intelligenz berechnet dagegen aus einem großen Datensatz, mit welcher Wahrscheinlichkeit eine Person, die Musiktitel A angehört hat, einen anderen Musiktitel anhört, und formt hieraus Regeln. Das System kann dann im konkreten Fall ermitteln, dass eine Person, die den Musiktitel A gehört hat, mit großer Wahrscheinlichkeit auch ein Interesse an Musiktitel B hat. Nach dieser Berechnung wird die Person aber auch ein Interesse an Musiktitel C haben, allerdings nur zu 30 %. Durch die Vorgabe eines Schwellenwerts ist dann sichergestellt, dass nur das zutreffend(st)e Ergebnis ausgegeben wird. Auch dieses muss nicht notwendig tatsächlich zutreffend sein, denn es handelt sich weiterhin nur um eine stochastische Annäherung. Siehe hierzu auch Kapitel 2 A III. 2. a).

[208] Im genannten Beispielsfall errechnet das System ein Interesse für Musiktitel B von 90 %, Musiktitel C von 30 % und Musiktitel D von 50 %. Das Ranking sichert dann ab, dass – je nach Anwendung – entweder nur der Musiktitel mit der höchsten Wahrscheinlichkeit, dann also Musiktitel B angezeigt wird (Selektionsdienst), oder die Musiktitel in der Reihenfolge B, D, C angezeigt werden (Ranking- oder Selektionsdienst). Zum Unterschied zwischen Selektions- und Rankingdiensten siehe unten unter D. 1.

[209] Vgl. *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 331.

[210] So kann etwa bei automatisierten Werbemaßnahme bestimmt werden, dass ab einem Interesse von 90 % („if“) für ein Produkt eine entsprechende Werbeanzeige geschaltet wird („then“). Siehe auch *Lorentz*, Profiling, 2019, S. 74. Bei einer automatisierten Kreditvergabe könnte definiert werden, dass bei einer Rückzahlungswahrscheinlichkeit von 80 % („if“) ein Kredit vergeben wird („then“). Dabei handelt es sich um sogenannte Cut-Off-Werte: Unterhalb dieser erfolgt eine Versagung des Kredits, oberhalb eine Zusage. Vgl. hierzu *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 206. Siehe auch *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 278–284.

[211] Siehe zum Einsatz von Maschinellen Lernverfahren bei autonomen Systemen eingehend mit verschiedenen Anwendungsbeispielen *Kraus/Ludwig/Minker u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 859, 862–872. Die

tät der Sachlage, inwieweit der Einsatz Maschineller Lernverfahren und auch welches Maschinelle Lernverfahren, tradiert oder Deep Learning, sinnvoll ist. Je mehr Ausgabemöglichkeiten und Entscheidungsvariablen zu berücksichtigen sind, desto ergiebiger ist der Einsatz der Maschinellen Lernverfahren. Die Fähigkeit Maschineller Lernverfahren, in komplexen Umgebungen Regeln zu erkennen und sich dynamisch fortzuentwickeln, ist hier von besonderem Wert. In sehr unklaren und dynamischen Umgebungen, etwa bei Informationsfilterdiensten, erzielt man mit Deep-Learning-Verfahren besonders gute Ergebnisse.[212] Entscheidend sind aber auch hier wirtschaftliche Gesichtspunkte, insbesondere die Verfügbarkeit von Daten, Hardware und Fachpersonal sowie der notwendige Aufwand.[213]

V. Zusammenfassung und Themeneingrenzung

Die Automatisierung autonomer Systeme erfordert allein einen Lösungsalgorithmus, in bestimmten Anwendungsbereichen erlaubt aber erst eine Personalisierung des Dienstes gute Lösungen. Bereits die typisiert-generalisierte Anpassung kann ausreichend sein. Die Untersuchung konzentriert sich aber auf solche Anwendungen, die eine Adaption gerade auf eine bestimmte betroffene Person, d.h. eine Individualisierung erfordern. Diese erfolgt durch Integration von Persönlichkeitsmerkmalen in den Lösungsalgorithmus. Hierfür werden Benutzerprofile erstellt. Der Einsatz autonomer Systeme bei der Profilerstellung erlaubt nicht nur eine Automatisierung, sondern auch eine besondere Präzision und Tiefe der Wissensbildung über die betroffene Person. Besonders gute Ergebnisse erzielt man in einem zweistufigen Profilbildungsverfahren. Dort wird zunächst ein Gruppenprofil – Modell – erstellt und hieraus ein Individualprofil – Profil – gebildet. Durch Zuordnung der Person zu einer Ver-

---

Trainingsdatensätze werden dabei vielfach mit denen der Modellbildung identisch sein, das Training erfolgt aber mit anderem Ziel: Während beim Modell die Verknüpfung von Persönlichkeitseigenschaften im Vordergrund steht, geht es beim Entscheidungsmodell um die Verbindung von Persönlichkeitseigenschaften mit einer Ausgabe. Es geht also nicht darum, inwieweit der Wohnort mit der Vermögenslage korreliert, sondern wie die Vermögenslage mit der Kreditvergabe oder -ablehnung in Verbindung steht.

[212] Siehe hierzu *Godoy/Amandi*, Knowledge Engineering Review 20 (2005), 329, 353 f.; *Schiaffino/Amandi*, in: Bramer (Hrsg.), Artificial intelligence, 2009, S. 193, 211; *Paradarami/Bastian/Wightman*, Expert Systems with Applications 83 (2017), 300–313 Vgl. zum Einsatz von Maschinellen Lernverfahren bei Spotify *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html. sowie bei Netflix *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18.

[213] Vgl. *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

gleichsgruppe im Modell lassen sich die Attribute der Vergleichsgruppe auf die Person übertragen und so ergänzende und umfassende Erkenntnisse über die Person bilden. Bei der Modellbildung kommen Verfahren des Maschinellen Lernens zum Einsatz und erlauben die Aufdeckung neuartiger, für den Menschen bislang nicht erkenntlicher Zusammenhänge in den Daten. Je nach gewählter Methode unterscheidet sich die Repräsentationsform des Modells als symbolisches oder subsymbolisches algorithmisches Konstrukt. Eine Anwendung eines autonomen Systems wird dann über die Eingabe des Profils in einen Lösungsalgorithmus automatisiert. Dieser kann seinerseits in einem Maschinellen Lernverfahren gebildet werden. Zu unterscheiden ist damit die Profilbildungsebene, bei der Erkenntnisse über die betroffene Person gebildet werden, und die Profilverwendungsebene, bei der das Profil und andere Daten in den Lösungsalgorithmus eingesetzt und so eine Entscheidung oder Steuerung ausgelöst wird.

C. Vorstellung von Anwendungsszenarien als Referenzbeispiele

Die Innovation autonomer Systeme ist bereits in technischer Hinsicht anspruchsvoll, vor allem aber ist unklar, welche realen Veränderungen ihre Etablierung im Lebensalltag des Einzelnen auslösen wird. Zur Veranschaulichung und Gegenprüfung der folgenden Ausführungen sollen daher Referenzbeispiele dienen. Ausgewählt werden vier Konstellationen, bei denen gerade die Individualisierung notwendig bzw. wirtschaftlich interessant und daher die Erstellung eines Individualprofils gängig ist. Die Beispielsfälle sollen nachfolgend in ihrer typischen, auf dem Markt angebotenen Ausgestaltung vorgestellt werden: Informationsfiltersysteme (I.), personalisierte Werbemaßnahmen (II.) und automatisierte Vertragsgestaltung, dabei die Kreditvergabe und die personalisierte Preisbildung (III.).

I. Informationsfilterdienste: Vorschlagssysteme und Suchmaschinen

Auf verschiedenen informations- und kommunikationsbezogenen Online-Plattformen[214] (Suchmaschinen, soziale Netzwerke, Video-Sharing-Dienste), bei Streamingdiensten,[215] teilweise auch bei Online-Auftritten von Tageszei-

[214] Der Begriff der Online-Plattform erfasst unspezifisch jede Internetseite, auf der bestimmte Dienstleistungen angeboten werden. Neben Kommunikation und Information werden etwa auch Waren, Zahlungssysteme oder kreative Inhalte ausgetauscht. Siehe hierzu *Europäische Kommission*, Online-Plattformen im digitalen Binnenmarkt, 25.05.2016, S. 2.

[215] Siehe für den Streamingdienst Netflix (Film und Serien) *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like; *Steck/Baltrunas/Elahi u.a.*, AI Magazine 42 (2022), 7–18; für den Streaming-

tungen oder Fernsehprogrammen (Mediathek)[216] werden zunehmend autonome Systeme in der hier beschriebenen Art eingesetzt.[217] Autonome Systeme sollen die Informations-, Kommunikations- und Medienangebote nach den persönlichen Präferenzen der NutzerInnen automatisiert filtern. Ziel ist es, die Fülle digitalisierter Medienangebote, Informationen und Meinungsbeiträge für den menschlichen Nutzer in besonders ansprechender Art aufzubereiten.[218] In einer Welt, in der sich der Informations- und Meinungsaustausch und Medienkonsum zunehmend in die digitale Welt verlagert,[219] kommt autonomen Systemen für die Präferenz-, Meinungs- und Wertebildung, die Information und den öffentlichen Diskurs eine besondere Rolle zu.[220]

---

dienst Spotify (Musik und Podcasts) *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streaming dienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

[216] Vgl. *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 66 f. Siehe zu empirischen Studien zu verschiedenen Filtermethoden bei unterschiedlichen Medienanbietern *Grafanaki*, Rich J. L. Techn. 24, 1, 36 f.; *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019.

[217] Siehe hierzu auch Kapitel 3 B. I. 1. a).

[218] Siehe nur *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 28; *Flamme*, MMR 24 (2021), 770; *Martini*, Blackbox Algorithmus, 2019, S. 213.

[219] Aus einer Studie der Medienanstalten von 2020 lässt sich ein solcher Trend ablesen: 44,6 % der Personen über 14 Jahre nutzt das Internet für die persönliche Information, vgl. *Die Medienanstalten*, Mediengewichtungsstudie 2020-I, Kantar Media Research, 2020, S. 7). Damit stellt das Internet 2020 erstmals das Medium mit dem größten Gewicht für die Meinungsbildung dar, vgl. *dass.*, Mediengewichtungsstudie 2020-I, Kantar Media Research, 2020, S. 8, 10, 24, 26. Dabei lässt sich ein Generationenschnitt erkennen: Für die Altersgruppe zwischen 14–29 Jahren (70,7 %) sowie zwischen 30–49 Jahre (54,3 %) ist das Internet das am meisten genutzte Medium für die Informationsbeschaffung (70,7 %). vgl. *dass.*, Mediengewichtungsstudie 2020-I, Kantar Media Research, 2020, S. 18, 25, 27. Der Trend zum digitalen Informations- und Meinungsbezug und -austausch dürfte sich also noch weiter steigen. Ähnliche Trends lassen sich für das Internet als Unterhaltungsmedium ausmachen *dass.*, Mediengewichtungsstudie 2020-I, Kantar Media Research, 2020, S. 43–47. Zu vergleichbaren Ergebnissen kommen, dabei mit differenziertem Ansatz zwischen informierenden und unterhaltenden Medienangeboten, *Breunig/Handel/Kessler*, Media Perspektiven 2020, 602–625 Vgl. auch *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, 293; *Stark/Magin/Jürgens*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 20, 22–24, die weitere Studien zur Bedeutung zum digitalen Informationsbezug und Meinungsaustausch zitieren.

[220] Siehe nur *Martini*, Blackbox Algorithmus, 2019, S. 99–100, 213–215. Im Einzelnen unter Kapitel 3 B. I. 1. a). Im Detail werfen automatisierte Informationsfilterdienste vielschichtige, komplexe Fragen auf, die sich je nach Informationsangebot und Filtermethode unterscheiden. Sie stehen nicht im Fokus dieser Arbeit. Aus der umfassenden Literatur siehe etwa *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017; *Kellner*, Die

Diese Filterdienste lassen sich grundsätzlich unterscheiden nach dem Informations- und Kommunikationsangebot sowie der Filtermethodik. Allgemeine Suchdienste bereiten regelmäßig die Gesamtheit der indexierten Informations- und Kommunikationsbeiträge des Internets[221] auf,[222] während soziale Netzwerke und Video-Sharing-Dienste die von NutzerInnen oder Dritten auf der Plattform generierten Inhalte vermitteln.[223] Diese Online-Plattformen filtern vorwiegend fremde Beiträge, nur teilweise erstellen sie auch selbst Inhalte.[224] Sie dienen wesentlich als Schaltstelle zwischen Kommunikations- bzw. Informationssender und -rezipient („Intermediäre", „Gatekeeper").[225] Aufgrund der im Internet nicht mehr überschaubaren Informationsflut bieten sie den NutzerInnen überhaupt erst die Möglichkeit, für sie relevante Informationen zu konsumieren.[226] Demgegenüber vermitteln Streamingdienste und Mediatheken al-

---

Regulierung der Meinungsmacht von Internetintermediären, 2019; *Schulz/Dankert*, Die Macht der Informationsintermediäre, Friedrich-Ebert-Stiftung.

[221] Suchmaschinen bilden nur einen Teil des im Internet verfügbaren Informationsmaterials ab. Von den Suchmaschinen erfasst wird nur das sogenannte „sichtbare Internet" (Visible Web). Informationen aus dem Deep Web oder dem Darknet tauchen in den gängigen Suchdiensten daher nicht auf. Zudem können nur Informationen aus Internetseiten aufgefunden werden, die von der Suchmaschine mittels sogenannter Crawler indexiert wurden. Nicht indexiert werden etwa Internetseiten, die nicht über einen Link verfügen oder nicht in Textform oder in einem unbekannten Datenformat dargestellt sind. Vgl. *Martin-Jung*, Wie die Google-Suche funktioniert, SZ 210.3.2022, https://www.sueddeutsche.de/wirtschaft/google-suche-wie-funktioniert-1.5549584, eingehend auch *Dörr/Natt*, ZUM 58 (2014), 829, 829, 831; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 101; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 81 f. Dabei gibt es auch Suchmaschinen mit einem begrenzten Suchangebot, etwa Hotelsuchmaschinen wie www.booking.com. Diese bleiben in der vorliegenden Untersuchung außer Betracht. Siehe hierzu *Dörr/Natt*, ZUM 58 (2014), 829, 833.

[222] Ausführlich zur Funktionsweise *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 68–77.

[223] Eingehend zur Ausgestaltung verschiedener sozialer Netzwerke und Video-Sharing-Plattformen *dies.*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 31–39. Vgl. auch *Dörr/Natt*, ZUM 58 (2014), 829, 831; *Flamme*, MMR 24 (2021), 770.

[224] Vgl. *Dörr/Natt*, ZUM 58 (2014), 829, 831 f.; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 52–54.

[225] Siehe zu diesen Begriffen nur *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 40–43; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, 75 f.; *Danckert/Mayer*, MMR 13 (2010), 219, 220; *Dörr/Natt*, ZUM 58 (2014), 829, 831; *Drexl*, ZUM 61 (2017), 529, 536. Die Bezeichnung „Intermediär" stellt die Vermittlerrolle zwischen Beitragssender (NutzerInnen oder Dritte) und Beitragsempfänger (NutzerInnen) in den Vordergrund, während mit dem Begriff „Gatekeeper" veranschaulicht wird, dass die Online-Plattformen darüber entscheiden, welche Informationen die Bevölkerung erreicht und welche nicht.

[226] *Flamme*, MMR 24 (2021), 770; *Dörr/Natt*, ZUM 58 (2014), 829, 830 f.

lein ein selbst erstelltes, dann also auch begrenztes Medienangebot. Um Kommunikationsermöglichung geht es hier nicht. In der Filtermethodik lassen sich Such- und Empfehlungsdienste unterscheiden. Manche Online-Plattformen verwenden beide Techniken.[227] Suchdienste setzen eine Anfrage des Nutzers voraus, während Empfehlungssysteme eigeninitiativ Informationsangebote unterbreiten.[228] Suchdienste lassen sich nochmals differenzieren in Selektionsdienste, bei denen allein eine spezifische Ausgabe erfolgt, und Ranking- bzw. Sortierungsdienste, bei denen verschiedene Ausgaben in einer bestimmten Reihenfolge angezeigt werden.[229] Auch Kombinationen zwischen Selektion und Ranking sind gängig.[230]

Die Personalisierung ist nur eine von verschiedenen Filtermethoden. Filterkriterien können auch die Beliebtheit eines Beitrags oder dessen Aktualität sein.[231] Zur personalisierten Filterung wird das Verhalten der Nutzer einer Plattform durch den Betreiber aufgezeichnet, hieraus werden dann Modelle

---

[227] So etwa soziale Netzwerk, siehe eingehend für Facebook *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 40–43. Auch GoogleNews ist ein Empfehlungssystem, das neben dem Suchfeld von Google eigeninitiativ Beiträge vorschlägt, vgl. hierzu *dies.*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 71 f.

[228] Siehe zu Empfehlungssystemen eingehend *Shi*, Recommendation Systems: A Review, Towards Data Science 03.02.2020, https://towardsdatascience.com/recommendation-systems-a-review-d4592b6caf4b. Vgl. auch *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 85. Bei der Mehrheit der sozialen Netzwerke liegt der Schwerpunkt auf der Empfehlung, vgl. eingehend zu einzelnen Diensten *dies.*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 40–46.

[229] Vgl. *Müller-Terpitz*, ZUM 64 (2020), 365; *Schulz/Dankert*, Die Macht der Informationsintermediäre, Friedrich-Ebert-Stiftung, S. 35. Siehe eingehend zur Funktionsweise von Ranking-Diensten *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 83 f.

[230] So kombinieren vor allem Suchdienste Selektions- und Rankingmerkmale, siehe *Müller-Terpitz*, ZUM 64 (2020), 365; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 106. Anschaulich zur Filtermethode verschiedener gängiger Online-Plattformen *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 38.

[231] Siehe zu verschiedenen Filtermethoden und Relevanzkriterien eingehend für Suchmaschinen *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 83 f., für verschiedene Online-Plattformen *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 40–46. Bekannt ist vor allem der Page-Rank-Algorithmus von Google, bei dem das höchste Ranking die Beiträge mit den meisten Klickzahlen erhalten. Siehe auch zu älteren, weiterhin genutzten Techniken *Introna/Nissenbaum*, The Information Society 16 (2000), 169, 174 f. Empirische Nachweise zu den Filtermethoden verschiedener Medienanbieter bieten *Grafanaki*, Rich J. L. Techn. 24, 1, 36 f.; *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019.

und Profile in der hier beschriebenen Art gebildet. Das Profil beinhaltet die Interessen und Vorlieben des Nutzers, auf dessen Grundlage die automatisierte Auswahl von Medienangeboten der Plattform – je nach Funktion dann in Form einer Selektion, eines Rankings oder einer Empfehlung – erfolgt.[232] Bei Musik- und Videostreamingdiensten ist die Personalisierung der Empfehlungssysteme bekannt; sie macht gerade die Attraktivität des Dienstes aus.[233] Demgegenüber ist bei Online-Plattformen und Suchdiensten vielfach unklar, ob und in welchem Umfang dort personalisierte Filtermethoden zum Einsatz kommen. Da diese Filtermethodik das Geschäftsmodell der Unternehmen darstellt, sind Unternehmen äußerst zurückhaltend, diese offenzulegen.[234] Die unterschiedlichen Filtermethoden können ganz eigene Fragen aufwerfen. Im Rahmen dieser Untersuchung soll es allein um personalisierte Verfahren gehen.

---

[232] *Müller-Terpitz*, ZUM 64 (2020), 365; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 83 f.; *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 18–22; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 91. Typischerweise ist bei Vorschlagssystemen die Personalisierung höher, so *Shi*, Recommendation Systems: A Review, Towards Data Science 03.02.2020, https://towardsdatascience.com/recommendation-systems-a-review-d4592b6caf4b. Siehe eingehend zur technischen Funktionsweise etwa *Giesbrecht*, This is how Netflix's top-secret recommendation system works, Wired 22.08. 2017, https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like.; *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html; *Ali/El Desouky/Saleh*, Inf Softw Technol. 6 (2016), 1–6; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 83–85.

[233] Vgl. nur für den Streamingdienst Spotify *Hajek*, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018, https://www.wiwo.de/technologie/digitale-welt/streamingdienst-boersengang-so-funktioniert-die-erfolgsformel-von-spotify/21121318.html.

[234] Beim Suchalgorithmus von Google sollen unter den etwa 200 verschiedenen Filtermethoden etwa 11 % auf Personalisierung beruhen, bei sozialen Netzwerken und Nachrichtenseiten sind (noch) keine Zahlen bekannt, vgl. *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 7. Es lässt sich jedoch eine klarer Trend hin zu verstärktem Einsatz von Personalisierungsalgorithmen bei Suchmaschinen ausmachen, vgl. auch *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 21 f. Siehe dezidiert zu Personalisierungsalgorithmen für Filterdienste *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 114 f.; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 90 f.; *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 4.

II. Personalisierte Werbung: Online Behavioural Targeting

Autonome Systeme können eingesetzt werden, um die Werbeansprache der NutzerInnen zu individualisieren:[235] Die einzelnen NutzerInnen erhalten eine eigene, an sie und ihre spezifische Situation angepasste Werbeanzeige, sowohl was den Inhalt, als auch was die Form, etwa die äußere Ausgestaltung, den Zeitpunkt und den Werbekanal (Webseiten, Apps oder E-Mails) anbelangt.[236] Auch die Personalisierung von Kundenbindungsprogrammen lässt sich hierzu zählen, etwa wenn spezifisch auf das Nutzerinteresse angepasste Rabatte oder Gutscheine übersandt werden.[237] Die Individualisierung der Werbung verspricht besondere wirtschaftliche Gewinne. Studien zufolge erreicht die personalisierte Werbung die KundInnen besonders gut.[238] Dabei ist der Werbeeffekt umso höher, je besser die Werbemaßnahme auf die betroffene Person und ihre situativen Interessen und Bedürfnisse angepasst ist. Der Zweck der Personali-

---

[235] Nur beim Online-Behavioural-Targeting wird ein Profil im Sinne dieser Arbeit gebildet, dies anhand des beobachteten Nutzerverhaltens, also implizit, siehe eingehend hierzu *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 86–91; *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, S. 5; *Dornis*, ZfPW 8 (2022), 310, 313 f.; *Ebers*, MMR 21 (2018), 423 f. Möglich sind personalisierte Werbemaßnahmen aber auch ohne ein solches Profil, etwa anhand der von den NutzerInnen bereitgestellten Informationen, sowie anhand des Besuchs und Verhaltens der NutzerInnen auf einzelnen besuchten Webseiten (sogenannte kontextbezogene oder segmentierende Werbung), siehe hierzu *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 86; *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, S. 5. Hierbei werden keine, jedenfalls keine detailreichen oder langfristigen Profile über die betroffene Person gebildet. Sie bleiben daher in der Untersuchung außer Betracht.

[236] Siehe eingehend zur personalisierten Werbemaßnahmen *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 221–230; *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 47–51; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 80–82. Vgl. auch Ausführlich zum Einsatz personalisierter Marketingstrategien in sozialen Netzwerken siehe *Krönke*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 145, 147–152.

[237] Siehe zu verschiedenen Ausgestaltungsformen *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 221–230; *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 47–51; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 80–82 Vgl. hierzu auch *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, 201–205.

[238] Siehe etwa die Studie von *Goldfarb/Tucker*, Management Science 57 (2011), 57–71 sowie von *Matz/Konsinksi/Nave u.a.*, Proceedings of the National Academy of Sciences of the United States of America 114 (2017), 12714–12719; zum emotional Targeting siehe *Otamendi/Sutil Martín*, Frontiers in psychology 11 (2020), 1–12 Vgl. eingehend mit Erläuterung verschiedener Hintergründe *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 84 f. VerbraucherInnen empfinden personalisierte Werbung vielfach als angenehmer im Vergleich zu unspezifischen Werbemaßnahmen. Vgl. hierzu auch bereits *Bygrave*, Data protection law, 2002, S. 313.

sierung ist damit die Steigerung der Wirkkraft von Werbemitteln.[239] Zugleich können Ressourcen für breit gestreute, dabei wirkungsarme bzw. wirkungsärmere Streuwerbung eingespart werden.[240] Für betroffene Personen bietet die Personalisierung entscheidende Vorteile, da sie nicht mit für sie irrelevanten Werbeinformationen belastet werden, zudem die Masse an Produktangeboten und -informationen, mit der die betroffene Person in einem Online-Markt konfrontiert ist, durch die Personalisierung in besonders ansprechender Weise gefiltert wird.[241] Die Individualisierung erfordert detailreiche, vor allem aber auch dynamische Profile. Für Unternehmen besonders interessant sind Kenntnisse zu manipulationssensiblen Persönlichkeitsmerkmalen, etwa Suchtverhalten oder emotionalen Vulnerabilitäten (Emotional Targeting).[242] Die Werbewirkung lässt sich zudem steigern, wenn die Werbung in Echtzeit an situativ bestehende Vorlieben, Bedürfnisse oder Sensibilitäten angepasst wird. [243] Über autonome Systeme lässt sich beides umsetzen. In der Praxis fallen die Unternehmen, die Online-Werbeplätze bereitstellen, Akteure, die Werbeprofile erstellen und Werbemaßnahmen auswählen, sowie Anbieter, die ihr Produkt bewerben wollen, häufig auseinander.[244] Dies wirft komplexe datenschutzrecht-

---

[239] *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 9; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 83–85.

[240] Plakativ *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 81 „Aus Sicht der Internetökonomie gehört die Massenwerbung der Vergangenheit an". Vgl. auch *Lorentz*, Profiling, 2019, S. 13; o.A., Verbraucherrecht 2.0, Dezember 2016, S. 59.

[241] Vgl. *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 82 f.; *Galli*, in: Ebers/Gamito (Hrsg.), Algorithmic Governance and Governance of Algorithms, 2021, S. 109, 110.

[242] *Otamendi/Sutil Martín*, Frontiers in psychology 11 (2020), 1–12 Siehe auch *Lorentz*, Profiling, 2019, S. 15 f.; *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 227 f.; *Dornis*, ZfPW 8 (2022), 310, 314. Vgl. auch zur gezielten Manipulation durch personalisierte Werbung *Mik*, Law Innov. Technol. 8 (2016), 1, 14, 22–24; *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 996; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 234–238 sowie *Sartor*, New aspects and challenges in consumer protection, Europäisches Parlament, April 2020, S. 14 f.

[243] Eingehend zur Effektivität situativ und kontextuell angepasster personalisierter Werbemaßnahmen *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1033, 1047-1049. Mit Beispielsfällen *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 231 f.

[244] Anbieter von Online-Inhalten, etwa Webseiten oder Apps, weisen Bildräume aus, auf denen Werbung geschaltet werden kann. Diese stellen die sogenannten Werbenetzwerkbetreibern (ad network agencies) zur Verfügung. Die Werbenetzwerkbetreiber sammeln Daten zu Nutzerverhalten auf den Webseiten und Apps, die dem Werbenetzwerk angehören oder mit diesem kollaborieren, auch können sie Daten von sonstigen Drittunternehmen erwerben. Hieraus bilden sie Profile, wählen entsprechende Werbeangebote aus und schalten diese auf den Seiten der Anbieter der Online-Inhalte frei. Die konkreten Werbeangebote stammen von werbebetreibenden Unternehmen, die sie diesen zur Verfügung stellen; sie sind auf den Servern der Werbenetzwerkbetreiber gespeichert. Die Werbenetzwerkbetreiber dienen so als Schnittstelle zwischen Anbietern von Online-Inhalten und werbebetreibenden Unternehmen. Je größer das Werbenetzwerk ist, d.h. mit je mehr Webseiten- und App-Betreibern es zu-

liche Fragen auf, die für die folgende Untersuchung nicht von Relevanz sind. Unterstellt wird daher vereinfacht, dass Datensammlung, Werbeprofilerstellung und Werbeschaltung durch eine Stelle erfolgen.[245]

III. Vertragsgestaltungen

Autonome Systeme unterstützen bzw. ersetzen vielfach den menschlichen Entscheider. Typische Anwendungsfälle sind das Kreditvergabeverfahren (1.) sowie die personalisierte Preisbildung (2.).[246]

1. Automatisierte Kreditvergabe

Bei der Kreditvergabe können autonome Systeme anhand des Verhaltens der KreditbewerberInnen besonders akkurat Risikoeinschätzungen hinsichtlich der Rückzahlungs- bzw. Zahlungsausfallwahrscheinlichkeit der einzelnen KreditbewerberInnen berechnen und damit besonders präzise dessen Kreditwürdigkeit (Bonität) bestimmen.[247] Diese Wahrscheinlichkeit zum zukünftigen Zah-

---

sammenarbeitet, desto umfassender ist das Datenmaterial und desto detailgenauer können die Profile ausfallen. Je mehr Online-Inhalteanbieter mit dem Werbenetzwerk kooperieren, desto weiter ist auch die Reichweite einer personalisierten Werbeanzeige. Für einen Kunden können dann über mehrere Webseiten und Geräte hinweg individuell angepasste Werbeanzeigen geschaltet werden. Vgl. eingehend zu diesen Mechanismen *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 16–17, 31–33; *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, S. 5 f.; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 58 f.; *Galli*, in: Ebers/Gamito (Hrsg.), Algorithmic Governance and Governance of Algorithms, 2021, S. 109, 113 f.

[245] Insbesondere stellen sich Fragen der Verantwortlichkeit. Siehe eingehend zu den datenschutzrechtlichen Fragen dieser Konstellation *Artikel 29 Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 145–147.

[246] In Abgrenzung zu Smart Contracts geht es dabei nicht um die Abbildung des Vertrags in einem Programmcode – dies erfolgt über die Blockchain-Technologie –, sondern um die Automatisierung des Vertragsschlusses. Diese Automatisierungen gehen dem Smart Contract in der Regel vor. Auch Smart Contracts sind automatisiert, allerdings hinsichtlich der Vertragserfüllung, nicht hinsichtlich des Zustandekommens des Vertrages. Zur umfassenden Literatur zu Smart Contracts siehe einführend *Heckelmann*, NJW 71 (2018), 504–510; *Paulus/Matzke*, ZfPW 4 (2018), 432–465; *Kipker/Birreck/Niewöhner u.a.*, MMR 23 (2020), 509–513; *Finck*, Int. Data Priv. Law 9 (2019), 78–94.

[247] Dies wird auch als „behavioural scoring" bezeichnet, siehe etwa *Kennedy/Mac Namee/Delany u.a.*, Expert Systems with Applications 40 (2013), 1372–1380 Auch bei Dauerschuldverhältnissen, etwa der Miete, oder sonstigen Risikogeschäften im Online-Handel kommen derartige Prognoseverfahren zum Einsatz, vgl. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 99; *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, [2]2022, S. 369, 287–290; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6 Rn. 35.

lungsverhalten einer Person wird in einem Zahlenwert angegeben (Score).[248] Indem der errechnete Score unmittelbar mit einer Zu- oder Absage oder bestimmten Vertragsbedingungen (etwa Kreditzins, erforderliche Sicherheiten, Laufzeit) verbunden wird, kann die Kreditvergabe sogar umfassend automatisiert werden.[249] Denkbar sind auch Ausgestaltungen, in denen das autonome System einen Entscheidungsvorschlag erarbeitet, der noch der menschlichen Umsetzung bedarf.[250] Derzeit (noch) am meisten verbreitet ist das Kredit-Scoring, bei dem lediglich der Score errechnet wird, der dann – neben anderen Faktoren – die Grundlage für eine menschliche Entscheidung bildet.[251] Um den individuellen Kreditscore (auch Scorewert) berechnen zu können, bedarf es einer sogenannten Scorecard (auch Scoreformel), in der sämtliche für die Wahrscheinlichkeitsberechnung relevanten Merkmale, etwa Einkommen, Kredithistorie oder Vermögensstand, ihr Verhältnis zueinander und deren Gewicht in einem statistischen Modell abgebildet sind.[252] Um den individuellen Score zu erhalten, werden die Daten eines Kunden in die Scoreformel eingegeben und so die Bonitätswerte errechnet.[253] Für Erstellung der Scorecard werden Daten von Kunden, die einen Kredit erhalten bzw. nicht erhalten haben, nach Mustern durchsucht und so Kriterien für die Rückzahlung bzw. Nichtrückzahlung abgeleitet.[254] Maschinelle Lernverfahren kommen dabei zunehmend zum Ein-

---

[248] *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 206; *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, ²2022, S. 369, 277.

[249] *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 210; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 29. Siehe auch mit Beispielen aus der Praxis *Miller*, Is an Algorithm Less Racist Than a Loan Officer?, The New York Times 18.09.2020, https://www.nytimes.com/2020/09/18/business/digital-mortgages.html. Dies ist insbesondere bei Cut-off-Scores der Fall, bei denen ab Unterschreitung eines bestimmten Scores eine Absage, bei Überschreiten eine Zusage erteilt wird.

[250] *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 210.

[251] Vgl. etwa *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, S. 206, 210; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 29. Vielfach ist in der Praxis der Kreditscore das maßgebliche Entscheidungskriterium.

[252] Siehe eingehend *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 205 f. Üblicherweise werden dabei den einzelnen Merkmalen bestimmte Punktwerte zugewiesen, siehe hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6 Rn. 35–36

[253] *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 206; *Weichert*, ZRP 47 (2014), 168; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6 Rn. 33.

[254] *Weichert*, ZRP 47 (2014), 168; *Martini*, DVBl 129 (2014), 1481, 1485 f.; *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 206.

satz.[255] Die Individualisierung ist dabei von besonderem wirtschaftlichen Wert: Mit dem Detailgrad der Scorecard steigt die Treffgenauigkeit der Prognose. Kreditunternehmen greifen daher umfassend auf Konten- und Zahlungsabwicklungsdaten von Kunden zu.[256] Dabei hat man erkannt, dass sich letztlich jeder Verhaltensweise bzw. jedem Persönlichkeitsmerkmal eine Aussage über die ökonomische Zuverlässigkeit einer Person entnehmen lässt („All data are credit data").[257] Unternehmen haben daher auch ein Interesse an Datenbeständen sozialer Netzwerke oder sonstiger Online-Plattformen (sogenanntes Social Scoring).[258] Vielfach nimmt eine Kreditanstalt das Scoring nicht selbst vor (internes Scoring), sondern beauftragt Drittunternehmen (Auskunfteien) mit der Erstellung der Scorings (externes Scoring).[259] Die einzelnen Kreditanstalten leiten ihre Kundendaten an diese Auskunftei weiter, sodass ein umfassender, kreditinstitutsübergreifender Datensatz entsteht. Anhand dieses Datensatzes

---

[255] Vgl. *Sadok/Sakka/El Maknouzi*, Cogent Economics and Finance 10 (2022), 1–12; *Dushimimana/Wambui/Lubega u.a.*, Journal of Risk and Financial Management 13 (2020), 180; *Miller*, Is an Algorithm Less Racist Than a Loan Officer?, The New York Times 18.09.2020, https://www.nytimes.com/2020/09/18/business/digital-mortgages.html.

[256] *Miller*, Is an Algorithm Less Racist Than a Loan Officer?, The New York Times 18.09.2020, https://www.nytimes.com/2020/09/18/business/digital-mortgages.html.Siehe zu typischerweise erhobenen Daten *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 207. Vgl. auch *Weichert*, ZRP 47 (2014), 168 f. Siehe allgemein zum Mehrgewinn einer Big-Data-Analyse beim Kredit-Scoring *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, [2]2022, S. 369, 280–282.

[257] So das Zitat des früheren Google-CEOs Douglas Merrill: „We feel like all data is credit data, we just don't know how to use it yet", zitiert nach *Hardy*, Just the Facts. Yes, All of Them., The New York Times 24.03.2012, https://archive.nytimes.com/query.nytimes.com/gst/fullpage-9A0CE7DD153CF936A15750C0A9649D8B63.html. Vgl. auch *Weichert*, ZRP 47 (2014), 168, 169; *Helfrich*, ZD 3 (2013), 473–474.

[258] Dies ist bereits vielfach gängige Praxis, vgl. *Kosta*, Social credits and security: embracing the world of ratings, Kaspersky Daily (https://www.kaspersky.com/blog/social-credits-and-security); *Kert*, Facebook can now be your only source of credit information, 10.01.2014 (https://www.bigdatascoring.com/another-breakthrough-in-social-media-credit-scoring). Siehe hierzu auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 96 f.; *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, [2]2022, S. 369, 294. In Deutschland ist diese Praxis (noch) nicht verbreitet. Vgl. auch *Helfrich*, Kreditscoring und Scorewertbildung der SCHUFA, 2010; *Lorentz*, Profiling, 2019, S. 21 f. Das Social Scoring ist nicht zu verwechseln mit dem Social Credit System, bei dem sämtliche Persönlichkeitsmerkmale ausgewertet und positiv oder negativ bewertet werden, um so zur Grundlage (staatlicher) Entscheidungen oder Sanktionen gemacht zu werden. Siehe hierzu genauer unter Kapitel 2 C. II. 1.

[259] *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 206; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 29; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 115. Siehe auch § 31 Abs. 2 BDSG. In Deutschland nimmt dies überwiegend die Wirtschaftsauskunftei SCHUFA vor.

erstellt die Auskunftei dann die Scorecard. Auf Anfrage einer Kreditanstalt berechnet die Auskunftei den Score eines Kunden und übermittelt diesen an die Kreditanstalt, die anhand dessen – typischerweise durch einen Menschen – über die Kreditvergabe entscheidet.

2. *Personalisierte Preisgestaltung*

Bei der personalisierten Preisbildung[260] wird die individuelle Zahlungsbereitschaft ermittelt, d.h. die Wahrscheinlichkeit, dass der Kunde das Produkt zu dem angebotenen Preis erwerben wird.[261] Das System kann dann lediglich einen Preisvorschlag errechnen, den die Parteien noch verhandeln können, oder die Preisgestaltung vollständig übernehmen, dann also den KundInnen den errechneten Preis anbieten, den diese, je nach Fallgestaltung, noch ablehnen können oder auch nicht.[262] Auch individualisierte Angebote oder Preisrabatte sind so möglich.[263] Nach ökonomischen Studien führt die personalisierte Preisgestaltung zu einer Gewinnsteigerung für die Unternehmen, da bei einem passgenauen Preis die KundInnen eher zu einem Kauf bereit sind, zudem die Preise in der Summe häufig höher ausfallen als bei generalisierenden Preisen.[264] Die

---

[260] Zu diesem Begriff *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403–410; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 224. Auch von algorithmic prizing oder Preisdifferenzierung ist die Rede, so *Zuiderveen Borgesius*, European Business Law Review 31 (2020), 401, 404. In den Wirtschaftswissenschaften wird dies als Preisdiskriminierung ersten Grades bezeichnet, siehe *Miller*, J. Law Technol. Policy 2014, 41; *Schneiders*, Jeder kriegt einen eigenen Preis, FAZ 08.04.2015, https://www.faz.net/aktuell/finanzen/meine-finanzen/geld-ausgeben/dynamische-preise-das-ende-des-einheitspreises-13522679.html. Preisdiskriminierungen zweiten Grades sind dann solche, die an sachbezogenen Kriterien, etwa der Verfügbarkeit der Ware, anknüpfen; Preisdiskriminierungen dritten Grades solche, die nach bestimmten Gruppen von Konsumenten differenzieren, etwa Studierende oder Senioren, vgl. *Miller*, J. Law Technol. Policy 2014, 41, 55; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 224. Es geht damit um einen individuell zugeschnittenen Preis, nicht um eine Preisgestaltung anhand einer allein oberflächliche(re)n gruppenbezogenen Verbrauchersegmentierung. Zu dieser Differenzierung siehe auch *Ban/Keskin*, Management Science 67 (2021), 5549; *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 705.

[261] *Dornis*, ZfPW 8 (2022), 310, 312; *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 705.

[262] Auch Kombinationen mit Informationsfilterdiensten sind möglich: Denkbar ist etwa, dass höherpreisige Angebote in Suchmaschinendiensten weiter oben platziert werden, um die Aufmerksamkeit besonders auf diese zu lenken. Es wird als Suchdiskriminierung oder price steering bezeichnet, vgl. *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 404; *Dornis*, ZfPW 8 (2022), 310, 315.

[263] *Miller*, J. Law Technol. Policy 2014, 41, 46; *Schneiders*, Jeder kriegt einen eigenen Preis, FAZ 08.04.2015, https://www.faz.net/aktuell/finanzen/meine-finanzen/geld-ausgeben/dynamische-preise-das-ende-des-einheitspreises-13522679.html; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 405.

[264] Vgl. umfassend zu den Vorteilen personalisierter Preisbildung, die vorwiegend für die Unternehmen bestehen *Zuiderveen Borgesius*, European Business Law Review 31

Berechnung der Zahlungsbereitschaft erfolgt, wie das Kredit-Scoring, durch Erstellung eines statistischen Modells anhand von Nutzerdaten.[265] In diesem Modell werden durch Datenanalyse verschiedene Parameter ermittelt, die für eine besonders hohe oder niedrige Zahlungsbereitschaft sprechen. Über die Eingabe individueller Daten in dieses Modell ist dann eine Einstufung des individuellen Preises zwischen Preisminima und Preismaxima für ein Produkt möglich. Wie bei der automatisierten Kreditvergabe sind umso tiefer gehende Erkenntnisse möglich, je mehr Aktivitäten und Persönlichkeitsmerkmale in diesem Datensatz abgebildet sind.[266] So kann etwa aus dem Zugangsort[267] oder dem Zugangsgerät[268] auf die Finanzkraft und damit höhere Zahlungsbereitschaft eines Kunden geschlossen werden. Bei Flugreisen sind relevant die Reisegewohnheiten und -umstände – wer üblicherweise Sonntagabend einen Flug bucht, wird dies auch zu einem höheren Preis tun, wer als Geschäftskunde fliegt, zahlt in der Regel mehr als ein Privatreisender.[269] Für Unternehmen besonders relevant sind dabei, wie auch bei der personalisierten Werbung, Erkenntnisse über akute, auch emotionale Bedarfe an einem Produkt, die eine erhöhte Zahlungsbereitschaft erwarten lassen.[270] Maschinelle Lernverfahren erlauben dabei die Aufdeckung zahlreicher Kriterien zur Zahlungsbereitschaft,

---

(2020), 401, 404; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 225–227; *Dornis*, ZfPW 8 (2022), 310, 314 f.; *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 708–714. Auf Verbraucherseite besteht insbesondere die Gefahr der Verdrängung zahlungsschwacher VerbraucherInnen aus dem Markt.

[265] Siehe zum technischen Verfahren ausführlich *Shiller*, Personalized Price Discrimination Using Big Data, Brandeis University, 29.07.2019, S. 9–22. Siehe auch *Miller*, J. Law Technol. Policy 2014, 41, 44–49, 58–62. Vgl. auch *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 404.

[266] *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 700.

[267] So fiel etwa die Gebühr für die Hochschulzulassung bei Aufruf der Seite mit einer asiatischen IP-Adresse deutlich höher aus, vgl. *Angwin/Mattu/Larson*, The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review, 01.09.2015. Weitere Beispiele bei *Miller*, J. Law Technol. Policy 2014, 41, 52; *Zuiderveen Borgesius*, European Business Law Review 31 (2020), 401, 404 f.

[268] Unterschiedliche Preise können etwa daran festgemacht werden, ob Zugriffe über das Smartphone oder den Computer erfolgen, vgl. *Zuiderveen Borgesius*, European Business Law Review 31 (2020), 401, 405. Auch die Marke des Zugangsgeräts kann maßgeblich sein. Beobachtbar ist etwa, dass mancherorts für Apple-NutzerInnen höhere Preise festgelegt wurden als für NutzerInnen anderer Hersteller, vgl. *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 404; *Mattioli*, On Orbitz, Mac Users Steered to Pricier Hotels, The Wall Street Journal 23.08.2012, https://www.wsj.com/articles/SB10001424052702304458604577488822667325882.

[269] *Elliott*, Your Very Own Personal Air Fare, The New York Times 09.08.2005, https://www.nytimes.com/2005/08/09/business/your-very-own-personal-air-fare.html.

[270] *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 29.

umso präziser fallen dann die Prognosen aus.[271] Auch die Ermittlung situativer Produktabhängigkeiten lässt sich so akkurat prognostizieren. Vor allem aber erlauben diese Verfahren eine echte Dynamisierung, da sie auf individuelle Erwerbssituationen und verändertes Kaufverhalten flexibel eingehen können.

Der Einsatz Maschineller Lernverfahren erlaubt zudem eine vollständige Automatisierung der Preisgestaltung. In Abgrenzung zur personalisierten Preisbildung wird dies als dynamische oder algorithmische Preisgestaltung bezeichnet. Die Preisbildung ist ein komplexer Prozess, in die verschiedene Faktoren, nicht nur die Zahlungsbereitschaft, sondern etwa auch die Marktlage oder die Verfügbarkeit eines Produkts, und dies mit ganz unterschiedlichem Gewicht einfließen. Eine technische Unterstützung ist für Unternehmen daher besonders attraktiv.[272] Maschinelle Lernverfahren können aus den verschiedenen Parametern, zu denen auch die Zahlungsbereitschaft zählt, eine konkrete Strategie formen und Preise akkurat, dynamisch, ressourcenschonend und äußerst schnell berechnen.[273] Inwieweit und auf welche Weise derzeit Mechanismen personalisierter Preisgestaltung tatsächlich eingesetzt werden, ist vielfach unklar, da Unternehmen mit Hinweis auf ihre Geschäftsgeheimnisse die Modalitäten ihrer Preisbildung nicht offenlegen.[274]

---

[271] *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 701. Eingehend zu verschiedenen Methoden Maschineller Lernverfahren *Shiller*, Personalized Price Discrimination Using Big Data, Brandeis University, 29.07.2019; *Ban/Keskin*, Management Science 67 (2021), 5549–5568 Siehe zum Einsatz Maschineller Lernverfahren bei der Berechnung von Flugticketpreisen *Weed*, In the Race for Cheap Airfare, It's You vs. the Machine, New York Times 28.01.2020, Section B, S. 4.

[272] *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 702. Hier ist dann der Begriff der dynamischen oder algorithmischen Preisbildung passender. Diese Differenzierung nehmen auch *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697–719; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403 f. vor.

[273] *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 702, 704; *Calvano/Calzolari/Denicolò u.a.*, Review of Industrial Organization 55 (2019), 155, 160–165.

[274] Vgl. *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 404 f.; *Miller*, J. Law Technol. Policy 2014, 41, 51. Vor allem in der Flugindustrie sind derartige Methoden bekannterweise vielfach verbreitet, zunehmend kommen sie auch in der Hotellerie oder der Versicherungsbranche zum Einsatz, *Calvano/Calzolari/Denicolò u.a.*, Review of Industrial Organization 55 (2019), 155, 156. Im Online-Handel dürften personalisierte Preisbildungen bereits aktuell vielerorts Verwendung finden, wohingegen sie im analogen Markt erst ganz allmählich eingesetzt werden, vgl. *Zuiderveen Borgesius*, European Business Law Review 31 (2020), 401, 406; *Miller*, J. Law Technol. Policy 2014, 41, 48; vgl. auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 225. Erste Studien benennen *Seele/Dierksmeier/Hofstetter u.a.*, Journal of Business Ethics 170 (2021), 697, 701 f.; sie kommen zu dem Ergebnis, dass die Verfahren im Online-Handel vordringlich sind.

D. Ergebnis

Untersuchungsgegenstand dieser Arbeit sind personalisierte autonome Systeme. Dies sind solche, die mit einem mit zur Interaktion mit einer Person bestimmt sind und dabei ein Mindestmaß an Wahrnehmung, Autonomie, Adaptabilität, Antizipativität, Personalisierung und Lernfähigkeit aufweisen. Zwei Anwendungsformen autonomer Systeme werden untersucht: Solche, die zur direkten Interaktion mit einer Person bestimmt sind (automatisierte Steuerung), und solche, die indirekt im Drittinteresse eine Interaktion mit einer Person durchführen (automatisierte Entscheidung). Das Maschinelle Lernen ist dabei Schlüsseltechnologie zur Realisierung derartiger Systeme. Zum Einsatz kommen überwachte, nicht überwachte und bestärkende Lernverfahren sowie symbolische, d.h. menschlich verständliche Methoden sowie subsymbolische, d.h. menschlich nicht nachvollziehbare Verfahren, insbesondere in Gestalt des Deep Learnings. In bestimmten Anwendungsbereichen erzielen autonome Systeme besonders gute Ergebnisse, wenn sie individualisiert sind. Auf diese konzentriert sich die vorliegende Untersuchung. Hierzu bedarf es einer Personalisierung des Lösungsalgorithmus; dies erfolgt durch den Einbezug von Benutzerprofilen. Ein Profil ist die Zusammenstellung anwendungsrelevanter Persönlichkeitsmerkmale. Je nach Anwendung sind diese deskriptiver, analytischer oder prädiktiver Natur. Das Profil ist damit mehr als die bloße Addition verfügbarer Persönlichkeitsmerkmale, es enthält ein oder mehrere über die verfügbaren Informationen hinausgehende Aussagen. Die Automatisierung der Profilerstellung durch autonome Systeme erlaubt ein hohes Maß an Eigenständigkeit, Präzision und Detailtiefe dieser Profile und dies auch dann, wenn zu der Einzelperson nur wenige Informationen vorliegen. Die automatisierte Profilbildung erfolgt über ein zweistufiges Verfahren, bei dem zunächst ein Gruppenprofil (Modell) anhand eines Datensatzes erstellt wird, in den verschiedene NutzerInnen ihre Daten gegeben haben. Der Einsatz Maschineller Lernverfahren bei dieser Analyse ermöglicht die Aufdeckung bislang unerkannter Zusammenhänge von anwendungsrelevanten Persönlichkeitsmerkmalen. In komplexen Umgebungen, in denen sich klare Strukturen und Verbindungen zwischen Persönlichkeitsmerkmalen und erwünschtem Output menschlich nicht erkennen lassen, können autonome Systeme so gute Lösungen herbeiführen. Das individuelle Profil wird gebildet, indem ein oder mehrere Rohdaten in das Modell eingegeben werden. Durch Zuordnung in die Vergleichsgruppen im Modell können neue Erkenntnisse über die Person inferiert werden. Zum Auslösen einer automatisierten Entscheidung oder Steuerung bedarf es eines Lösungsalgorithmus. Dieser kann seinerseits in einem Maschinellen Lernverfahren gebildet werden. Über die Eingabe des Profils in den Lösungsalgorithmus gibt dieser, gegebenenfalls unter Verarbeitung weiterer Anwendungsdaten, einen bestimmten Output aus. Je nach Anwendung folgt hieraus unmittelbar eine Interaktion mit der Einzelperson oder es bedarf eines Tätigwerdens eines Menschen.

Ob und in welchem Umfang und mit welchem Verfahren Maschinelle Lernverfahren bei der Konstruktion autonomer Systeme zum Einsatz kommen, ist neben der technischen auch eine wirtschaftliche Frage, da Maschinelle Lernverfahren, vor allem solche des Deep Learnings, ressourcenintensiv sind.

Für die folgende Untersuchung dienen vier Anwendungskonstellationen als Referenzbeispiele, nämlich die Informationsfilterung, die personalisierte Werbung, die automatisierte Kreditvergabe sowie die personalisierte Preisgestaltung. Sie dienen der Veranschaulichung und Prüfung der zu entwickelnden These.

Kapitel 2

Soziokulturelle Bewertungen und Begründung von Regulierungsbedarfen

In der Gesellschaft werden autonome Systeme unterschiedlich bewertet. Beobachtbar ist dabei, dass die Technik überwiegend als gefährlich eingeordnet wird und, teils strikte, Regulierung eingefordert wird. Autonome Systeme sind aber, wie jede Technik, weder gut noch schlecht, noch sind sie neutral.[1] Wenn am Ende autonome Systeme befürwortet oder abgelehnt werden, für keine oder für strikte Regulierung eingetreten wird, so liegen die Gründe dafür in bestimmten Grundüberzeugungen gegenüber der Technik und der Verantwortungsverteilung zwischen Staat und Individuum. Das folgende Kapitel soll einen Überblick über die Bewertung autonomer Systeme in der Gesellschaft geben. Hierzu sollen sowohl die Chancen und Risiken autonomer Systeme vorgestellt als auch die grundlegenden Überzeugungen aufgedeckt werden, die einer Befürwortung oder Ablehnung autonomer Systeme zugrunde liegen. Die Risiken autonomer Systeme wirken auf verschiedene Weise nachteilig auf einzelne Interessensfelder und begründen so Konflikte mit denjenigen, die Vorteile aus der Anwendung autonomer Systeme ziehen. Dies sind vorwiegend Unternehmen, die autonome Systeme wirtschaftlich verwerten. Hier formen sich aus den generellen befürwortenden bzw. ablehnenden Haltungen konkrete Interessenskonflikte, die nach Ausgleich verlangen. Im liberalen Verfassungsstaat erfolgt dies durch den demokratisch legitimierten Gesetzgeber. Diese Interessenkonflikte begründen also die Regulierungsbedarfe, auf die Regulierungsvorgaben eine Antwort geben sollen. Sie bilden damit die Grundlage für die spätere Bewertung der DSGVO.

Zunächst sollen die Chancen und Risiken autonomer Systeme vorgestellt und dabei auch darauf eingegangen werden, inwieweit es sich bei den Wirkungen und Auswirkungen autonomer Systeme überhaupt um neuartige Phänomene handelt (A.). Im Anschluss sollen die Prämissen und Grundüberzeugungen erläutert werden, die hinter der Befürwortung oder Ablehnung autonomer Systeme stehen (B.). Abschließend erfolgt eine Darstellung der tatsächlichen Effekte autonomer Systeme auf ausgewählte Interessensfelder (C.).

---

[1] So das berühmte Schlagwort von *Kranzberg*, Technology and Culture 27 (1986), 544, 547: „Technologie ist weder gut noch böse, noch ist sie neutral“.

A. Neuartigkeit sowie Chancen und Risiken autonomer Systeme

Vielfach wird davon ausgegangen, dass autonome Systeme etwas noch nie Dagewesenes sind, die durch sie ausgelösten Phänomene neuartig. Gerade deshalb werden autonome Systeme als besonders risikoreich eingeschätzt. Dies ist allerding nur bedingt richtig. Es lohnt daher, sich zunächst zu vergegenwärtigen, inwieweit autonome Systeme tatsächlich eine disruptive Technik darstellen (I.). Dies schärft den Blick, welche Chancen und Risiken autonome Systeme ganz spezifisch hervorrufen (II.).

I. Neuartigkeit und Disruptivität autonomer Systeme

Kritisch bewertet wird vor allem der Umstand, dass autonome Systeme umfassend und detailreich Profile von Einzelpersonen erstellen und auf deren Grundlage in intransparenter Weise Entscheidungen treffen. Dies ist aber kein neuartiges Phänomen (1.). Die Profilbildung und Regelfindung durch autonome Systeme unterscheidet sich aber in bestimmten Merkmalen von der menschlichen Regelfindung sowie von derjenigen nach tradierten informationstechnischen Verfahren (2.).

1. Profilbildung als natürlicher Prozess und Mensch als Blackbox

Wer Profilbildungen und ihre Verwendung durch autonome Systeme per se für schädlich hält, verkennt, dass der Mensch schon immer in einer Welt lebt, in der er permanent von anderen bewertet und analysiert wird.[2] Um mit anderen Menschen interagieren und kommunizieren zu können, bedarf der Mensch einer Vorstellung vom Gegenüber. Auch im wirtschaftlichen Bereich hat es Profilbildungen schon immer gegeben, etwa im Bereich der Kundenbestandspflege.[3] Auch die Stereotypisierung, bei autonomen Systemen also die Erstellung von Modellen und Einordnung der betroffenen Person in das Modell, ist nichts Neues. Aufgrund begrenzter Ressourcen, insbesondere der Grenzen menschlich-kognitiver Fähigkeiten, bedarf der Mensch der Komplexitätsre-

[2] Eingehend *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 51; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 25–27; *Schauer*, Profiles, Probabilities, and Stereotypes, 2006; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 431. Siehe auch *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 32. Noch allgemeiner, dann hinsichtlich der gesamten Umwelt, *Purtova*, Law Innov. Technol. 10 (2018), 40, 52: „People measured and quantified the world long before the Digital Age, eg in the form of maths and language".

[3] So auch *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 34 f. Vgl. auch *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, 201 f.

duktion.[4] In der Interaktion mit dem Gegenüber erfolgt dies über die Verwendung von Stereotypen.[5] Die Intransparenz der Profilbildung, ebenso wie die der Profilverwendung, ist darüber hinaus ein Umstand, mit dem der Mensch schon immer konfrontiert war: Die Inhalte und Zuordnungskriterien der menschlichen Profilbildung treten überwiegend nicht nach außen, häufig sind sie nicht einmal der profilbildenden Person selbst bewusst,[6] auch die Regeln und Mechanismen, die einen Menschen bei einer Entscheidung oder Interaktion mit einem Mitmenschen anleiten, sind überwiegend intransparent. Auch der Mensch ist eine „Blackbox".[7] Hierauf ist noch zurückzukommen.[8]

2. Eigenheit und Neuartigkeit von Regelbildungen durch autonome Systeme

Die Stereotypisierung durch autonome Systeme, d.h. die Modellbildung anhand Maschineller Lernverfahren, sowie die Regelfindung, d.h. die Erstellung eines Lösungsalgorithmus durch Maschinelle Lernverfahren, und die Anwendung der Stereotype und Entscheidungsregeln weisen jedoch auch Unterschiede zu dem auf, womit der Mensch bisher konfrontiert war, und zwar im Vergleich zum Menschen (a)) sowie im Vergleich zu tradierten informationstechnischen Automatisierungsverfahren (b)).

a) Abgrenzung zu menschlichem Wissen

Maschinelle Regelbildung lässt sich anhand von fünf Wesensmerkmalen[9] von menschlichem Wissen abgrenzen. Erstens ist das maschinelle Wissen überwiegend prognostisch-prädiktiver Natur. Denn um eine Automatisierung von Entscheidungen und Steuerungen zu ermöglichen, ist maßgeblich, welche Verhaltensweisen und Persönlichkeitsmerkmale eine Person in der (nahen) Zukunft

---

[4] Ausführlich *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 51 f.; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 25–27; *Schauer*, Profiles, Probabilities, and Stereotypes, 2006, S. 6–7, 75–78.

[5] Inhalte und Zuordnungskriterien dieser Stereotype beruhen auf individuellen Erfahrungen, Werteüberzeugungen oder sonstigen Voreinstellungen. Siehe eingehend zu verschiedenen Einordnungen von Personen in bestimmte Profile und ihren Ursachen *Schauer*, Profiles, Probabilities, and Stereotypes, 2006; vgl. generell zu den Grundlagen der Profilbildung *ders.*, Profiles, Probabilities, and Stereotypes, 2006, S. 9–17. Siehe auch *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 51, 88; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 436.

[6] Vgl. *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 27.

[7] Vgl. *Wischmeyer*, AöR 143 (2018), 1, 54; *Bonezzi/Ostinelli/Melzner*, Journal of experimental psychology 151 (2022), 1–9.

[8] Siehe unter Kapitel 5 B. III. 2. a).

[9] Ähnliche Ansätze bei *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 94–98, der auf prädiktive, segmentierende und emergente Ableitungen, dann allerdings mittels Techniken der Big-Data-Analyse, verweist.

aufweisen wird.[10] Zweitens ist es stochastisch-mathematischer Natur, es beruht auf komplexen Wahrscheinlichkeitsrechnungen.[11] Drittens ist es datenbasiert-korrelativ, es wird anhand der Mustererkennung im Datensatz ohne kausal-logische Hypothesenfundierung gebildet.[12] Viertens ist es klassifizierend-stereotypisierend: Erkenntnisse über die Einzelperson werden allein anhand gruppenbezogener Merkmale im Modell gebildet.[13] Fünftens ist es intransparent: Aufgrund von Geheimhaltung der Unternehmen[14] sowie aufgrund technischer Überforderung bleiben Profilinhalte gerade für die betroffene Person intransparent.[15] Maschinelle Lernverfahren sind zudem menschlich nur begrenzt verständlich, hierzu sogleich noch genauer.[16]

b) Neuartigkeit gegenüber tradierten Datenauswertungsverfahren

Maschinelle Lernverfahren sind Big-Data-Datenauswertung. Anders als bei tradierten Datenanalysemethoden liegt das Ziel aber nicht in einem menschlichen, sondern einem maschinellen Wissensgewinn:[17] Anhand Maschineller Lernverfahren sollen autonome Systeme eigenständig algorithmische Lösungsstrategien entwickeln, die ihnen dann eine Problemlösung im Einzelfall erlauben. Auch hier lassen sich fünf Kriterien benennen, anhand derer Maschinelle Lernverfahren von tradierten Auswertungsverfahren differenziert werden können. Erstens sind Maschinelle Lernverfahren gegenüber tradierten Auswertungsmethoden eigenständiger. Schon das Ergebnis ist menschlich nicht vorgegeben, aber auch die menschliche Einflussnahme im Lern-, d.h. Auswer-

---

[10] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 94 f.; *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 36; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 430 f.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10.

[11] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 94; *Martini*, Blackbox Algorithmus, 2019, S. 5, 20, 22.

[12] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 94 f.; *Martini*, Blackbox Algorithmus, 2019, S. 22, 60; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432.

[13] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 97 f.; *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 35 f.; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 52–58, 236; *Just/Latzer*, Media, Culture & Society 39 (2017), 238, 247 f.

[14] Eingehend hierzu *Martini*, Blackbox Algorithmus, 2019, S. 33; *Dornis*, ZfPW 8 (2022), 310, 313.

[15] *Martini*, Blackbox Algorithmus, 2019, S. 41 f.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10.

[16] Siehe unter Kapitel 2 A II. 2. c).

[17] Vgl. auch *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 573; *Purtova*, Law Innov. Technol. 10 (2018), 40, 52 f.

tungsprozess ist zurückgenommen.[18] Zweitens sind Maschinelle Lernverfahren dynamisch, der Auswertungs- und Algorithmenbildungsprozess ist niemals abgeschlossen.[19] Drittens ist das Ergebnis des Maschinellen Lernverfahrens, d.h. das selbsterlernte Regelwerk, nurmehr bedingt menschlich verständlich, nämlich nur dann nicht, wenn subsymbolische Verfahren, insbesondere künstliche neuronale Netze zum Einsatz kommen.[20] Viertens ist das Maschinelle Lernverfahren nur bedingt beeinflussbar. Der Maschinelle Lernprozess soll gerade eigenständig ablaufen, bestimmte äußere Einflussnahmen können Systemstörungen herbeiführen.[21] Ohnehin setzt eine gezielte Einflussnahme ein Mindestmaß an Verständnis des Regelwerks voraus. Fünftens ist die Analysekraft Maschineller Lernverfahren im Vergleich zu tradierten Analyseverfahren bedeutend höher.[22] Dies steigert die Erkenntnismöglichkeiten über betroffene Personen und erlaubt tiefgehende Einblicke in Persönlichkeitsaspekte betroffener Personen.[23] Auch der Zeitaufwand für die Analysen ist verkürzt. Dies erlaubt personalisierte Anwendungen instantan und in Echtzeit.[24]

II. Chancen und Risiken maschineller Wissensbildung und Verwendung

Autonome Systeme bieten verschiedene Chancen für Individuum und Gesamtgesellschaft, warten aber auch mit einigen Risiken auf. Je nach Anwendungsbereich wirken sich Chancen und Risiken unterschiedlich aus, führen dann zu echten Vor- oder Nachteilen. Nachfolgend sollen typisiert-generell die Chancen (1.) oder Risiken (2.) dargelegt werden. Dabei soll nur auf wesentliche As-

---

[18] *Martini*, Blackbox Algorithmus, 2019, S. 42; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 431 f. Siehe auch *Alpaydın*, Machine learning, 2021, S. 129. Die menschliche Involvierung im Lernprozess unterscheidet sich danach, welches Lernverfahren – supervised, unsupervised oder reinforcement learning gewählt wird. Siehe hierzu oben Kapitel 1 A. II. 2.

[19] Vgl. *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10; *Wischmeyer*, AöR 143 (2018), 1, 13. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 42; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 430.

[20] Siehe hierzu bereits unter Kapitel 1 A. II. 2. c) sowie noch ausführlich unter Kapitel 2 A. II. 2. c).

[21] Vgl. *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 367.

[22] *Martini*, Blackbox Algorithmus, 2019, S. 4, 21; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432 f.

[23] *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10; *Dornis*, ZfPW 8 (2022), 310, 312 f.

[24] Diesen Aspekt betonen auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 435; *Martini*, Blackbox Algorithmus, 2019, S. 5; *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 59; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 110; *Roßnagel*, DuD 40 (2016), 561, 563. Siehe auch für den Anwendungsbereich autonomer Fahrzeuge *Nürnberger/Bugiel*, DuD 40 (2016), 503, 504; für die Informationsfilterung *Just /Latzer*, Media, Culture & Society 39 (2017), 238, 247.

pekte eingegangen werden, die Darstellung erhebt keinen Anspruch auf Vollständigkeit.

1. Technikbedingte Chancen autonomer Systeme

Das maschinelle Wissen zeichnet sich nicht nur durch ein erhöhtes Maß an Richtigkeit und Objektivität (a)) und an Transparenz und Kontrollfähigkeit aus (b)). Es erschließt zudem neue Erkenntnisquellen (c)). Die auf dieses Wissen gestützten Entscheidungen und Steuerungen versprechen bessere, sicherere, gerechtere und effektivere Lösungen,[25] ein hohes Maß an Sicherheit von Anwendungen[26] und insgesamt eine Steigerung der Lebensqualität durch Effizienz-, Effektivitäts und Konvenienzgewinne.[27]

---

[25] *Ernst*, JZ 72 (2017), 1026, 1028; *Rademacher*, AöR 142 (2017), 366, 391. Sehr allgemein zu den Vorteilen von Systemen der Künstlichen Intelligenz *Martini*, Blackbox Algorithmus, 2019, S. 14–16; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 986 f.; *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 2. Siehe allgemein zu Potentialen der Künstlichen Intelligenz, aktuelle wirtschaftliche, soziale oder ökologische Konflikte zu lösen *Chui/Harryson/Manyika u.a.*, Applying AI for Social Good, McKinsey Global Institute, Dezember 2018.

[26] *Europäische Kommission*, Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss, Europäische Kommission, 19.02.2020, S. 3; *High-Level Expert Group on Artificial Intelligence*, A defintion of AI: Main capabilites and disciplines, Europäische Kommission, 8. April 2019, S. 42; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 986; *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 2. Siehe auch *Roßnagel*, DuD 40 (2016), 561, 562.

[27] Siehe etwa zu Konvenienzsteigerungen der Ambient Intelligence *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 60; *Roßnagel*, DuD 40 (2016), 561, 562 f. Vgl. zu den Vorteilen im Konsumbereich *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 244. Vor allem die Nutzung autonomer Systeme als persönliche Assistenten verspricht Steigerungen der Lebensqualität, siehe hierzu *Eaton*, Artificial Intelligence Makes the Phone a Personal Assistant, The New York Times 18.05.2016, https://www.nytimes.com/2016/05/19/technology/personaltech/artificial-intelligence-makes-the-phone-a-personal-assistant.html.; *Waters*, Artificial intelligence: A virtual assistant for life, Financial Times 22.2.2015, https://www.ft.com/content/4f2f97ea-b8ec-11e4-b8e6-00144feab7de. Möglich sind auch Automatisierungen im Bereich der Pflege, *Stone/Brooks/Brynjolfsson u.a.*, Artificial Intelligence and Life in 2030, September 2016, S. 30 f.; *Sönnichsen*, Mein Helfer, der Pflege-Roboter, Tagesschau 10.03.2020, https://www.tagesschau.de/inland/pflege-roboter-101.html. Optimierungsoptionen werden auch im Bildungssektor gesehen, siehe hierzu *Stone/Brooks/Brynjolfsson u.a.*, Artificial Intelligence and Life in 2030, September 2016, S. 31; *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 7.

a) Objektivität, Akkuratesse und Gleichbehandlung

Die Erstellung von Modellen, Profilen und Entscheidungsregeln erfolgt allein daten- und algorithmenbasiert, die Ergebnisse sind nicht, jedenfalls nicht unmittelbar, durch subjektive Voreinstellungen, Diskriminierungen und Erwartungshaltungen gelenkt und verzerrt.[28] Einmal entwickelt, erlaubt der Algorithmus aufgrund seiner Determiniertheit keinen Einbezug sachfremder Erwägungen.[29] Dies verspricht objektive und neutrale Ergebnisse. Die Rechenleistung autonomer Systeme übersteigt die menschlich-kognitive, auch unterliegt diese keinen natürlich-situativen Beeinträchtigungen, etwa aufgrund von Ermüdung oder individuellen Aufmerksamkeitsdefiziten.[30] Fehlerhafte Ergebnisse, wie sie dem Menschen etwa aufgrund von Rechenfehlern, Ungenauigkeiten oder Unvollständigkeiten unterlaufen, sind damit ausgeschlossen. Der generalisierende Ansatz der zweistufigen Profilbildung, in der die Ähnlichkeit von Personen und Anwendungsszenarien in den Vordergrund gestellt ist, kann zu einer faireren und gerechteren Behandlung führen, eine gerechte(re) Verteilung von Gütern bewirken und so insgesamt die Verbraucherwohlfahrt stärken.[31]

b) Plastizität sowie Einwirkungs- und Gestaltungsmöglichkeit

Im Vergleich zu tradierten Entscheidungsprozessen, etwa Marktmechanismen und menschlichen Entscheidungsverfahren, bieten autonome System ein erhöhtes Maß an Transparenz und Plausibilität.[32] Verwendete Daten, Verfahren

---

[28] *Wischmeyer*, AöR 143 (2018), 1, 16; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 104; *Bull*, Der Staat 58 (2019), 57, 75. Für algorithmische Systeme allgemein *Martini*, Blackbox Algorithmus, 2019, S. 47.

[29] *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 365. Wenn auch nur für nicht-lernende Algorithmen *Ernst*, JZ 72 (2017), 1026, 1027 f.

[30] *Wischmeyer*, AöR 143 (2018), 1, 16; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 104. Nicht beschränkt auf Maschinelle Lernverfahren *Ernst*, JZ 72 (2017), 1026, 1027 f.; *Wischmeyer*, AöR 143 (2018), 1, 16; *Martini*, Blackbox Algorithmus, 2019, S. 47. Siehe auch *Roßnagel*, DuD 40 (2016), 561, 562.

[31] Ausführlich zu Erwartungen einer gesteigerten Verbraucherwohlfahrt bei der personalisierten Preisbildung *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 437; *Miller*, J. Law Technol. Policy 2014, 41, 62; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 405 f.; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 225–227; *Ernst*, JZ 72 (2017), 1026, 1034, die dies gleichwohl allesamt im Ergebnis ablehnen. Aufgrund der noch darzulegenden Diskriminierungs- und Segmentierungseffekte ist eher zu erwarten, dass benachteiligte Personengruppen, insbesondere zahlungsschwache Personen, aus dem Markt gedrängt werden.

[32] Für sämtliche den Menschen umgebende Entscheidungs- und Steuerungsstrukturen *Wischmeyer*, AöR 143 (2018), 1, 45; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 80, für den menschlichen Entscheidungsprozess *Ernst*, JZ 72 (2017), 1026, 1029; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 997. Erklärungsmodelle und Studien, weshalb an algorithmische Entscheidungen dennoch höhere Transparenzanforderungen als an menschlichen Entscheidungen gestellt werden, bieten

und die Algorithmen insgesamt sind vollständig[33] und dauerhaft abgespeichert, sie können jederzeit ausgelesen werden. Auch Modell- und Lösungsalgorithmus, das Profil sowie das finale Ergebnis, d.h. der Quellcode und die Datenmatrizen, sind umfassend einsehbar.[34] Zudem sind sämtliche Bestandteile der Entscheidungsverfahren und -ergebnisse autonomer Systeme beeinflussbar und jederzeit abänderbar. Trainingsdaten können ausgewechselt, Parameter in den Algorithmen gelöscht oder Ergebnisse berichtigt werden.[35]

c) Zugang zu neuen und erweiterten Wissensquellen

Das zweistufige Profilbildungsverfahren ermöglicht Erkenntnisse über eine Person jenseits der über sie bzw. von ihr verfügbaren Daten.[36] Zudem erschließen autonome Systeme über das Maschinelle Lernverfahren im Modell neue Erkenntnisquellen. Die algorithmische Auswertung lässt Strukturen in den Daten, damit also Zusammenhänge zwischen Persönlichkeitsmerkmalen erkennen, die dem Menschen verborgen bleiben.[37] Darüber ermöglicht der datenbasiert-korrelative Lernansatz den Zugang zu einer neuen Form des Wissens. Dieses ist nicht theoriengestützt-deduktiv, sondern datenbasiert-induktiv, findet seine epistemische Aufladung also in der Generalisierung der Datenstruktur.[38] Die aufgefundenen Muster können als Grundlage für menschlichen Er-

---

Bonezzi/Ostinelli/Melzner, Journal of experimental psychology 151 (2022), 1–9 Sie arbeiten vor allem das Merkmal der Ähnlichkeit heraus: Mit der Entscheidung eines Menschen kann sich eine Person eher identifizieren, da diese auf Prozesse und Muster gestützt ist, die denjenigen ähneln, die die betroffene Person selbst für eine Entscheidungsfindung nutzen würde, eben da diese menschlich sind. Mit einer algorithmischen Entscheidung, die ganz anderen Mechanismen folgt, ist eine solche Identifikation nicht möglich. Es sind dann derartige Projektionen, die für eine höhere Akzeptanz menschlicher Entscheidungen sorgen.

[33] Anders als bei klassischen Steuerungsmethoden gibt es keine unbewussten Anteile der Entscheidung(sfindung), auch Möglichkeiten der Verschleierung bestehen nicht: Sämtliche Elemente der Ergebnisfindung und Inhalte des Ergebnisses liegen in Form von Daten bzw. Algorithmen vor, siehe hierzu *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 997.

[34] *Dies.*, Artificial Intelligence, [4]2021, S. 997.

[35] So auch *Rademacher*, AöR 142 (2017), 366, 392; *Wischmeyer*, AöR 143 (2018), 1, 45. Für den Bereich klassischer Algorithmen *Ernst*, JZ 72 (2017), 1026, 1027. Plakativ *Lessig*, Code, [2]2006, S. 6: „Code is never found; it is only ever made, and only ever made by us […] a code of cyberspace, defining the freedoms and controls of cyberspace, will be built". *Martini*, Blackbox Algorithmus, 2019, S. 49: „Künstliche Intelligenz gibt nicht vorrangig Algorithmen die Kontrolle, sondern denen, die sie entwickeln".

[36] Siehe hierzu oben Kapitel 1 B. III. 2. b) sowie Kapitel 1 B. III. 3. c).

[37] *Wischmeyer*, AöR 143 (2018), 1, 16; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432; *Martini*, Blackbox Algorithmus, 2019, S. 13 f.; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 76.

[38] Eine ähnliche Differenzierung trifft *Rademacher*, AöR 142 (2017), 366, 374. Auch ist denkbar, dass sich noch nachträglich Hypothesen finden lassen. So auch *Ernst*, JZ 72 (2017), 1026, 1030: „Selbst wenn der sachliche Grund für einen Zusammenhang nicht erkennbar

kenntnisgewinn dienen, wenn sich zu diesem eine logische bzw. kausale Verknüpfung finden lässt. Die Datenkorrelation kann so als Ausgangspunkt für menschliches Wissen dienen.[39] Derartiges Wissen könnte zudem auch ohne eine menschliche Theorieaufladung brauchbar sein, soweit man auf menschlich kausal-rationale Abstützung verzichtet und etwa allein die Ergebnisrichtigkeit bzw. das Funktionsoptimum zum Validierungs- und Kontrollkriterium macht.[40] Derzeit ist aber noch unklar, ob und in welchen Bereichen dies sinnvoll ist. Hierauf ist noch zurückzukommen.[41]

2. *Technikbedingte Risiken autonomer Systeme*

Als Gefährdungsmomente der Wissensbildung und -verwendung durch autonome Systeme werden erkannt die Anfälligkeit der Systeme für Fehler, Diskriminierungen und verzerrende Ergebnisse (a)), die systemimmanenten Beschränkungen bei der Erfassung der (Um-)Welt und des Menschen (b)), die Intransparenz und fehlende Nachvollziehbarkeit (c)), sowie die Beschränktheit der Einwirkungs- und Abänderungsmöglichkeiten (d)). Dies setzt sich dann in

---

sein sollte, bedeutet dies nicht, dass dieser nicht möglicherweise existiert". Ähnlich *Wischmeyer*, AöR 143 (2018), 1, 14 f.: „Ob wir *à la longue* in größerem Umfang als bisher statistische Korrelationen als Erklärungen, d. h. als Nachweis kausaler oder anderer Gesetzmäßigkeiten akzeptieren werden, auch wenn uns ein Verständnis der dahinter stehenden ‚Theorie' fehlt, sei hier dahingestellt".

[39] Angedeutet bei *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 61: „Even if the concrete connection identified by an automated system cannot be understood by a human observer, the result may nevertheless be true but so far just has not been recognizable for humans". Vgl. auch *Anderson*, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, Wired 23.06.2008, https://www.wired.com/2008/06/pb-theory: „Scientists are trained to recognize that correlation is not causation, that no conclusions should be drawn simply on the basis of correlation between X and Y (it could just be a coincidence). Instead, you must understand the underlying mechanisms that connect the two. Once you have a model, you can connect the data sets with confidence".

[40] Plakativ *Domingos*, Communications of the ACM 2012 (2012), 78, 86: „Many researchers believe that causality is only a convenient fiction". So auch bereits *Anderson*, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, Wired 23.06.2008, https://www.wired.com/2008/06/pb-theory: „Petabytes allow us to say: ‚Correlation is enough'. We can stop looking for models. We can analyze the data without hypotheses about what it might show. We can throw the numbers into the biggest computing clusters the world has ever seen and let statistical algorithms find patterns where science cannot". Ähnlich *Purtova*, Law Innov. Technol. 10 (2018), 40, 53: „[W]e can no longer say that some data has no meaning […]. [I]t is safer to assume that all data […] potentially has meaning, even if not for humans". Kritisch hierzu *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 25– 26, 37–40.

[41] Letztlich ist dies eine Frage, in welchem Rahmen menschliche Verständlichkeit autonomer Systeme gefordert ist. Siehe hierzu Kapitel 5 B. III. 2. c).

den Entscheidungen oder Steuerungen fort, die fehlerhaft, diskriminierend, inakzeptabel, intransparent und nicht anfecht- oder abänderbar sind.

a) Fehlerhaftigkeit, insbesondere Diskriminierungsanfälligkeit

Die stochastisch-mathematischen Methoden der Wissensbildung durch Maschinelle Lernverfahren sind fehleranfällig. Typische Phänomene sind unzutreffende Treffer (false positive) oder unzutreffende Nichttreffer (false negative)[42] sowie sonstige unzutreffende statistische Annäherungen.[43] Ganz grundlegend kann man die Prämisse der Profilbildung anzweifeln, dass nämlich die Analyse vergangenen Verhaltens tatsächlich belastbare Aussagen über zukünftige Verhaltensweisen oder Persönlichkeitseigenschaften zulässt.[44]

Die Ergebnisse der Maschinellen Lernverfahren sind von der Qualität der Trainingsdaten abhängig (Garbage-in-garbage-out-Prinzip).[45] In den Daten angelegte Unrichtigkeiten,[46] vor allem aber sozionormativ inakzeptable Verzerrungen wie Diskriminierungen[47] schlagen auf Modelle und Lösungsalgorith-

---

[42] *Bygrave*, Data protection law, 2002, S. 309. Siehe hierzu Kapitel 1 B. III. 3. c).

[43] *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 4 f.; *Wischmeyer*, AöR 143 (2018), 1, 24. Siehe zu Fehlern des Profils auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 433–435.

[44] *Hildebrandt*, in: Deakin/Markou (Hrsg.), Is law computable?, 2020, 78: „[C]ode-driven normativity scales the past; it is based on insights from past decisions and cannot reach beyond them". In diese Richtung auch *Miller*, J. Law Technol. Policy 2014, 41, 95: „[T]he outrage over sorting comes from the feeling that individuals are held unreasonably or unfairly accountable for past behavior or social status". Siehe hierzu auch eingehend *Nissenbaum*, Privacy in context, 2010, S. 208. Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 4.

[45] Eingehend zu diesem Phänomen *Rademacher*, AöR 142 (2017), 366, 376; *Wischmeyer*, AöR 143 (2018), 1, 23; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 83; *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, Europäische Kommission, 10. April 2019, S. 22 f.; *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 231.

[46] Problematisch sind etwa unzutreffende, unvollständige oder irrelevante Daten, vgl. *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 231 f.; siehe auch bereits *Bygrave*, Data protection law, 2002, S. 309. Verschiedene Fehler und ihre Ursachen, etwa Falschangaben von NutzerInnen, präsentieren *Rao/Schaub/Sadeh*, What do they know about me? Contents and Concerns of Online Behavioral Profiles, Carnegie Mellon University Pittsburgh, 04.06.2015, S. 9.

[47] Die gesammelten Daten selbst können Vorprägungen enthalten, da bestimmte Gruppen mit positiven oder negativen Eigenschaften konnotiert sind (als Input Bias, auch als Historical Bias oder Social Bias bezeichnet), vgl. *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 105; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 167; *Martini*, Blackbox Algorithmus, 2019, S. 50 f.; *Russell/Norvig*, Artificial Intelligence, ^{4}2021, S. 995 f. Auch kann es zu Diskriminierungen kommen, da bestimmte Personen(gruppen) in einem Daten-

men, damit am Ende auch auf das gebildete Profil und die Einzelentscheidung durch (sogenannter Maschineller Bias).[48] Auch Vorprägungen der am Trainingsverfahren beteiligten menschlichen Akteure können in das Maschinelle Lernverfahren einfließen.[49] Hierauf ist noch zurückzukommen.[50] Schließlich kann die klassifizierende Regelfindungsmethodik Maschineller Lernverfahren problematisch sein, wenn diese zu unerwünschten Segmentierungen jenseits von Diskriminierungsmerkmalen führt, etwa nach dem Einkommen oder dem

satz unter- oder überrepräsentiert sind (sog. sampling oder representation bias), siehe hierzu *Martini*, Blackbox Algorithmus, 2019, S. 50 f.; *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1147; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 105; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 995. Einen technischen Einblick bieten *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019, S. 7–9. So wurde etwa bei der Spracherkennungssoftware von Google festgestellt, dass diese für Minderheitengruppen weniger gut funktionieren, da diese in den Trainingsdaten unterrepräsentiert sind, siehe *Bender/Gebru/McMillan-Major u.a.*, in: Coscia (Hrsg.), Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2021, S. 610, 614 f. Als Präzedenz- und Referenzfall gilt die Prognosesoftware COMPAS, die in den USA zur Entscheidung über die Kautionshöhe und die Entlassung aus der Untersuchungshaft eingesetzt wurde. Eine Analyse im Auftrag von ProPublica 2016 offenbarte eine strukturelle nachteilige Analyseausgabe des algorithmischen Entscheidungsprogramms zulasten einer bestimmten ethnischen Zugehörigkeit, da die verwendeten Trainingsdaten die menschlichen Diskriminierungen widerspiegelten, siehe hierzu *Larson/Mattu/Kirchner, Lauren Kirchner, Angwin, Julia*, How We Analyzed the COMPAS Recidivism Algorithm, ProPublica, 23.05.2016. Zu diesem und weiteren Beispielen *Hacker*, Common Mark. Law Rev 55 (2018), 1143–1145; *Martini*, Blackbox Algorithmus, 2019, S. 53–58; *Steege*, MMR 22 (2019), 715, 716, 718–720, ein Beispiel aus dem Recruiting-Bereich stellt *Dastin*, Amazon scraps secret AI recruiting tool that showed bias against women, Reuters 11.10.2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. vor.

[48] Zum Begriff siehe etwa *Martini*, Blackbox Algorithmus, 2019, S. 47; *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019.

[49] Im Rahmen des Trainings selbstlernender Algorithmen wird etwa der gesamte Trainingsprozess menschlich vorgegeben (überwachtes Lernen, verstärkendes Lernen) oder das Ergebnis menschlich als tauglich oder untauglich bewertet (unüberwachtes Lernen). Darin fließen menschlich-subjektive Bewertungen ein. Vgl. *Wischmeyer*, AöR 143 (2018), 1, 28; *Martini*, Blackbox Algorithmus, 2019, S. 48 f.; *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 23; *Burrell*, Big Data and Society 3 (2016), 3, siehe auch bereits *Bygrave*, Data protection law, 2002, S. 309. Ausführliche Darstellung verschiedener Ursachen und der Art und Weise der menschlichen Vorprägungen in die Technik bei *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 7. Anschaulich Olga Russakovska zitiert nach *Smith*, Dealing With Bias in Artificial Intelligence, The New York Times 19.11.2019, https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html:„There's no balanced representation of the world and so data will always have a lot of some categories and relatively little of others. […] I don't think it's possible to have an unbiased human, so I don't see how we can build an unbiased A.I. system".

[50] Siehe unten Kapitel 2 C. II. 1.

Bildungsstand.[51] Darüber hinaus sind Funktionsstörungen autonomer Systeme, sowohl in der Hard- als auch der Software möglich,[52] auch manipulativ-schadhafte Einwirkungen Dritter sind denkbar.[53]

b) Beschränktheit auf generalisierbare, mathematisch darstellbare Aspekte

Die Wissensbildung autonomer Systeme erfolgt durch Mustererkennung in Daten einer Vielzahl von NutzerInnen oder Anwendungen, es ist per se ein stereotypes und generalisierendes Wissen. Raum für Einzelfallbetrachtungen, Abweichungen oder atypische Fallgestaltungen gibt es nicht.[54] Im Übrigen können autonome Systeme die Umwelt nur erfassen und Probleme nur lösen, soweit diese mathematisch erfass- und berechenbar, algorithmisierbar und in formale Sprache übertragbar sind.[55] Die Datenabhängigkeit führt dazu, dass As-

[51] Vgl. *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 34. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 97 f.

[52] Vgl. Darstellung bei *Castelluccia/Le Métayer*, Understanding algorithmic decision-making, Europäisches Parlament, März 2019, S. 33–37.

[53] Vgl. *Wischmeyer*, AöR 143 (2018), 1, 17. Siehe hierzu auch *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 20; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 45. Vor allem bei Künstlichen Neuronalen Netzen ist es möglich, durch geringfügige Änderungen des Trainingsmaterials das Modell so zu verändern, dass es falsche Ergebnisse ausgibt, vgl. *Nürnberger/Bugiel*, DuD 40 (2016), 503, 504. Bei einem Bilderkennungssystem, das Katzenbilder erkennen soll, könnte etwa auf sämtlichen Katzenbildern im Trainingsmaterial ein – für den Menschen – nicht erkenntlicher Pixel angebracht werden. Das System wird dann nur solche Abbildungen als Katzenbilder erkennen, die diesen Pixel enthalten.

[54] *Ernst*, JZ 72 (2017), 1026, 1028; *Hill*, in: Hill/Schliesky (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, 2015, S. 267, 274 beschreibt das vielzitierte Problem des „Schwarzen Schwans" nach *Taleb/Proß-Gill*, Der schwarze Schwan, 2008: Auch höchst unwahrscheinliche Phänomene sind möglich, jedoch nicht in der künstlich geschaffenen digital-algorithmisierten Welt. Vgl. zur fehlenden Berücksichtigungsfähigkeit des Einzelfalls auch *Bull*, Der Staat 58 (2019), 57, 76.

[55] *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 36: „[Data analyis] forces our mind to think in terms of specific formats and to qualify our experience in machine-understandable language". *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 678: „Data mining can only address problems that lend themselves to formalization". Normative oder graduelle Wertungen oder nicht triviale Abwägungsentscheidungen, die nicht als absolute Zahlen darstellbar sind, können durch Systeme Künstlicher Intelligenz nicht vorgenommen werden, vgl. im Rahmen des Predictive Policings *Rademacher*, AöR 142 (2017), 366, 383 f.

pekte keine Berücksichtigung finden können, die nicht in Daten darstellbar[56] oder nicht im Trainingsdatensatz repräsentiert sind[57].

c) Intransparenz und mangelnde Nachvollziehbarkeit

Inhalte des Profils sowie Parameter der konkreten Entscheidung oder Steuerung sind für die betroffene Person in der Regel nicht erkenntlich. Verschiedene Gründe sind hierfür ursächlich.[58] Hierzu zählen etwa die fehlende fachliche Expertise der VerbraucherInnen (technische Illiteralität, technical illiteracy),[59] sowie die technische Komplexität der Auswertungsmethodik und die Masse an Daten und Verarbeitungsverfahren, die menschliches Denkvermögen übersteigen.[60] Problematisch ist bei autonomen Systemen aber vor allem, dass

---

[56] Problematisch ist dies etwa bei sozialen, emotionalen, intuitiven und sonstigen unbewussten Merkmalen. Vgl. *Hoffmann-Riem*, AöR 142 (2016), 1, 30; *Martini*, Blackbox Algorithmus, 2019, S. 59 f. Siehe auch *Nürnberger/Bugiel*, DuD 40 (2016), 503, 504; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 985 f. Es ist aber durchaus denkbar, dass diese Aspekte in der Zukunft Berücksichtigung finden können. So erzielt man derzeit etwa im Bereich der emotionalen Künstlichen Intelligenz vielversprechende Ergebnisse, siehe etwa *Kreye/Hunger*, Künstliche Intelligenz: die Entschlüsselung unserer Gefühle, SZ 22.01.2023, https://www.sueddeutsche.de/projekte/artikel/politik/kuenstliche-intelligenz-gefuehle-roboter-e936533/?reduced=true.

[57] *Mayer-Schönberger/Cukier/Mallett*, Big Data, 2013, S. 38–44; *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 37. Ausdrücklich *Hill*, in: Hill/Schliesky (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, 2015, S. 267, 274: „[…] Entscheidungen ergeben sich auch nur aus dem, was bereits im System angelegt ist". Siehe auch *Binns*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 130, 132: „One cannot always draw samples from all logically possible populations for various societal, economic, or even biological reasons. For instance, there may not be data on the population of prisoners who were deemed 'high risk' but were released; or of those with low credit scores who were nevertheless given loans; or of pregnant males (except in rare circumstances)". Im Rahmen des Predictive Policing: *Rademacher*, AöR 142 (2017), 366, 383.

[58] Siehe hierzu auch unter Kapitel 4 D. IV. 1.

[59] *Martini*, Blackbox Algorithmus, 2019, S. 41; *Wischmeyer*, AöR 143 (2018), 1, 46 f.; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 80; *Burrell*, Big Data and Society 3 (2016), 4. Vgl. auch *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 22. Der Einblick in das Maschinelle Lernverfahren nützt dem durchschnittlichen Laien auch deshalb wenig, da darin nicht eine bestimmte Lösungsmethode oder ein konkreter Algorithmus erkenntlich wird, sondern eine – sich zudem beständig fortentwickelnde – Lernarchitektur dargelegt ist. Ohne hinreichende fachliche Kenntnisse wird der Laie damit wenig anfangen können.

[60] *Wischmeyer*, AöR 143 (2018), 1, 46; *Martini*, Blackbox Algorithmus, 2019, S. 41 f.; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 80 f. Die Logik eines Maschinellen Lernverfahrens und eines gebildeten Algorithmus nachzuvollziehen, ist, da Daten und Algorithmen ausgelesen werden können, zwar möglich,

diese eine nicht überwindliche Intransparenz aufweisen, da sie menschlich unverständlich sind. Dies betrifft zum einen korrelativ-datenbasierte Musterbildungen, die ohne eine logisch-kausale Theorie für den Menschen willkürlich erscheinen.[61] Wenn etwa das autonome System einen Zusammenhang zwischen einer Filmvorliebe und einer Kreditausfallwahrscheinlichkeit herstellt, ist dies mit kausal-logischen Begründungsanforderungen unvereinbar.[62] Zum anderen und vor allem betrifft dies subsymbolische Lernverfahren, in dem sich die gefundene Regel als künstliches neuronales Netz darstellt. Es enthält keine für den Menschen verständliche Parameter oder Gewichtungen mehr, erst recht dann keine logisch-kausalen Verbindungen.[63] Auch ein Experte – dabei selbst derjenige, der das Trainingsverfahren geleitet hat – kann in diesen Fällen nicht nachvollziehen, weshalb ein autonomes System ein bestimmtes Ergebnis ausgegeben hat und kann Input und Output weder im Vor- noch im Nachhinein zusammenführen.[64] Letztlich ist die fehlende Nachvollziehbarkeit darauf zu-

---

verlangt aber einen hohen Ressourcen- und Zeiteinsatz, so auch *Burrell*, Big Data and Society 3 (2016), 4 f. Notwendig ist sowohl ein Verständnis für die Daten als auch den Algorithmus, dies erhöht die Verständnisanforderungen. Siehe *dies.*, Big Data and Society 3 (2016), 5: „While datasets may be extremely large but possible to comprehend and code may be written with clarity, the interplay between the two in the mechanism of the algorithm is what yields the complexity (and thus opacity)".

[61] Es wird dann auch von Apophänie, Cluster-Illusion oder *Cum-hoc-ergo-propter-hoc*-Fehlschluss oder schlicht von willkürlichem Maschinenwissen gesprochen, so *Martini*, Blackbox Algorithmus, 2019, S. 60. Eingehend zu diesem Phänomen auch *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 67 f.; *Domingos*, Communications of the ACM 2012 (2012), 78, 86. Siehe auch mit weiteren Beispielen *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 17, 20; *Rademacher*, AöR 142 (2017), 366, 375.

[62] Anders zu bewerten ist der Fall, in dem das System einen Zusammenhang zwischen dem Kauf von Filzpads für Stuhlbeine und der Kreditwürdigkeit errechnete. Derartige Filzpads werden üblicherweise genutzt, um Parkettböden zu schonen. Personen, die Filzpads erwerben, haben also erstens einen Parkettboden, den sich eher vermögende Personen leisten können, und gehen zweitens gewissenhaft mit den in ihrem Besitz oder Eigentum befindlichen Sachen um. Beide Aspekte können so tatsächlich als logisch-rationale Kriterien dienen, die für eine hohe Wahrscheinlichkeit der Kreditbedienung sprechen. Vgl. zu diesem Beispiel *Strahilevitz*, Harv. L. Rev. 126 (2013), 2010, 2023.

[63] Siehe bereits oben Kapitel 1 A. II. 2. c). Siehe überdies *Martini*, Blackbox Algorithmus, 2019, S. 43 f.; *Wischmeyer*, AöR 143 (2018), 1, 47; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 81. Präzise spricht *Burrell*, Big Data and Society 3 (2016), 2 von einer „opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human scale reasoning and styles of semantic interpretation". Siehe auch *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 16, 22.

[64] *Burrell*, Big Data and Society 3 (2016), 9; *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 573; *Purtova*, Law Innov. Technol. 10 (2018), 40, 53. Explizit *Russell/Norvig*, Artificial Intelligence,

rückzuführen, dass menschliche und maschinelle Regelfindung unterschiedlich funktionieren: hier hypothesenbasiert-kausal, dort datenbasiert-korrelativ.[65] Hinzu kommt, dass das Maschinelle Wissen sich beständig fortentwickelt und nicht statisch bleibt: Die Offenlegung des Algorithmus oder der algorithmischen Struktur liefert daher keine (dauerhaft) zutreffenden Erkenntnisse.[66] Diese unüberwindliche Intransparenz wird als Blackbox-Phänomen bezeichnet.[67] Auch von opaker Künstlicher Intelligenz (opaque Artificial Intelligence) im Gegensatz zu transparenter (transparent Artificial Intelligence) ist die Rede.[68]

d) Determiniertheit

Algorithmische Entscheidungsstrukturen sind zudem determiniert. Eine Profilbildung oder automatisierte Entscheidung bzw. Steuerung läuft nach der gefundenen algorithmischen Regel ab, ohne dass Aspekte jenseits der Programmierung einfließen können, neue Merkmale hinzukommen oder bestehende wegfallen können und schließlich, ohne dass Ausnahmen möglich sind.[69] Die algorithmische Struktur gibt dann auch vor, welche Ergebnisse und damit Entscheidungsinhalte und Verhaltensoptionen möglich sind. Einwirkungen, Abänderungen und Abweichungen in der Profilbildung und in der Entscheidung oder Steuerung sind nur möglich, wenn dies technisch umsetzbar und eigens vorgesehen ist.[70]

---

[4]2021, S. 759: „[D]eep networks may form internal layers whose meaning is opaque to humans, even though the input is still correct".

[65] Maschinelle bzw. autonome Systeme „denken" also anders als Menschen. Grundlegend zu diesem Bild *Burrell*, Big Data and Society 3 (2016). Siehe auch *Purtova*, Law Innov. Technol. 10 (2018), 40, 52 f.

[66] *Martini*, Blackbox Algorithmus, 2019, S. 42; *Wischmeyer*, AöR 143 (2018), 1, 47.

[67] Grundlegend *Pasquale*, The Black box society, 2015. Siehe auch *Hoffmann-Riem*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 1, 17; *Wischmeyer*, AöR 143 (2018), 1, 8; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75; *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 16. Vielfach werden sämtliche Intransparenzformen unter den Begriff der „Blackbox" gefasst. Allein die letztgenannten sind neuartig und für Maschinelle Lernverfahren typisch, nur diese sind unüberwindlich. Der Begriff sollte daher nur für diese Formen der Inkomprehensibilität verwendet werden. Ähnlich das Verständnis bei *Burrell*, Big Data and Society 3 (2016), 2; *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 575.

[68] Vgl. *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 759; *Burrell*, Big Data and Society 3 (2016), 5.

[69] *Ernst*, JZ 72 (2017), 1026, 1027 f. Plakativ *Hildebrandt*, in: Deakin/Markou (Hrsg.), Is law computable?, 2020, 78: „[C]ode-driven normativity freezes the future; it cannot adapt to unforeseen circumstances due to the disambiguation that is inherent in code".

[70] *Ernst*, JZ 72 (2017), 1026, 1027.

B. Voreinstellungen und Prämissen für soziokulturelle Bewertungen autonomer Systeme

Die soeben dargelegten Chancen und Risiken autonomer Systeme werden in der Gesellschaft unterschiedlich bewertet und gewichtet. Im Meinungsspektrum stehen sich als Extreme gegenüber Stimmen, die für einen umfassenden Einsatz autonomer Systeme werben und die Regulierung den freien Märkten überlassen wollen, und Ansätze, die autonome Systeme ablehnen und für eine strikte Regulierung eintreten. Die Einstellungen entlang dieses Meinungsspektrums haben ihre Ursache in unterschiedlichen Prognosen und Bewertungen autonomer Systeme. Im Kern geht es also um divergierende Risikoeinschätzungen. Auf einer tieferen bzw. generelleren Ebene ist für die jeweilige Auffassung auch entscheidend, welche Vorstellung von der richtigen Verteilung staatlicher und individueller Verantwortung vorherrscht, welche normativen Erwartungen also an den liberalen Verfassungsstaat im Umgang mit Risikoszenarien herangetragen werden.

Um die befürwortenden wie ablehnenden Positionen im öffentlichen Diskurs angemessen berücksichtigen zu können, ist es wichtig, sich die hinter den Risikobewertungen und den Forderungen nach staatlichem Einschreiten stehenden Grundüberzeugungen zu vergegenwärtigen. Die Untersuchung kann es nicht leisten, diese umfassend darzustellen. Im Folgenden sollen daher nur skizzenhaft die Grundüberzeugungen vorgestellt werden, die hinter den Risiko- und Verantwortungsbewertungen von Personen, die sich für keine oder geringe Regulierungen autonomer Systeme aussprechen (I.), und solcher, die für Verbote oder strikte Regulierung eintreten (II.).

I. Chancenkonzentrierende, interventionsablehnende Ansätze

Autonome Systeme werden in der Gesellschaft teilweise umfassend begrüßt. Derartige Ansichten stützen sich teilweise auf eine optimistische Grundeinstellung oder stellen eine utilitaristische Gesamtschau an (1.), andere halten Risiken für marginal, da sie die Disruptionskraft autonomer Systeme grundlegend in Zweifel ziehen (2.). Die Ablehnung staatlicher Intervention wird auch darauf gestützt, dass dem Einzelnen eine hohe Selbstschutz- und Resilienzfähigkeit zugeschrieben wird (3.).

1. Technikoptimismus und Utilitarismus

In einer technikoptimistischen Sicht herrscht die Erwartung vor, dass autonome Systeme sämtliche kognitiv anspruchsvolle Aufgaben eigenständig erfüllen, immer weitere Anwendungsbereiche erschließen und in Industrie und Alltags-

leben umfassend Verwendung finden werden.[71] Dies ist verbunden mit Überzeugung, der der Einsatz autonomer Systeme zu einer im Ergebnis besseren, bequemeren, gerechteren und sicheren Welt,[72] zu mehr ökonomischem Wohlstand[73] und zu mehr ökologischer Nachhaltigkeit[74] führen wird. Diese Vorteile überwiegen in einer utilitaristischen Gesamtschau etwaige Nachteile und werden als hinnehmbar betrachtet.[75] (Ausgreifende) regulative Beschränkungen autonomer Systeme werden kritisch gesehen, können diese doch dazu führen, dass die Vorteile autonomer Systeme für Individuum und Gesamtgesellschaft ungenutzt bleiben.[76] Aufgabe des Staates ist es in dieser Perspektive allein, ei-

---

[71] So etwa die Modellstudie von *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 3, wonach bis zum Jahr 2030 70 % der Unternehmen Systeme der Künstlichen Intelligenz einsetzen werden. Auch die *Europäische Kommission*, Künstliche Intelligenz für Europa, Europäische Kommission, 25.04.2018, S. 1 f. geht von einer immer weiteren Verbreitung der Künstlichen Intelligenz in Wirtschaft und Gesellschaft aus.

[72] Siehe etwa *McKnight*, Life in 2050: How Will AI Shape the Future?, InformationWeek 02.09.2022, https://www.informationweek.com/ai-or-machine-learning/life-in-2050-how-will-ai-shape-the-future. Auch die *Europäische Kommission*, Künstliche Intelligenz für Europa, Europäische Kommission, 25.04.2018, S. 1 f. fokussiert für die Entwicklung ihrer geoökonomischen Strategie zur Künstlichen Intelligenz allein auf die Vorteile der Künstlichen Intelligenz. Siehe allgemein auch die Studie von *Chui/Harryson/Manyika u.a.*, Applying AI for Social Good, McKinsey Global Institute, Dezember 2018, dort explizit *dies.*, Applying AI for Social Good, McKinsey Global Institute, Dezember 2018, S. i: „Artificial intelligence, while not a silver bullet, could contribute to the multi-pronged efforts to tackle some of the world's most challenging social problems".

[73] Der Modellstudie von *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 3 zufolge lässt der Einsatz von Künstlicher Intelligenz in der Privatwirtschaft ein Wirtschaftswachstum von 13 Milliarden $ und eine Steigerung des weltweiten BIP von 1,2 % pro Jahr bis 2030 erwarten. Die ökonomischen Potentiale betont auch die *Europäische Kommission*, Künstliche Intelligenz für Europa, Europäische Kommission, 25.04.2018, S. 1.

[74] Siehe zum weltweiten Einsatz von Künstlicher Intelligenz mit dem Ziel des Umwelt- und Klimaschutzes in der Privatwirtschaft *Chui/Hall/Mayhew u.a.*, The state of AI in 2022 – and a half decade in review, McKinsey & Company, Dezember 2022, S. 8.

[75] Vgl. zu derartigen Erwägungen in der Strategie der Europäischen Kommission zur Künstlichen Intelligenz *Europäische Kommission*, Künstliche Intelligenz für Europa, Europäische Kommission, 25.04.2018, S. 17–20.

[76] *Erdélyi/Goldsmith*, Regulating Artificial Intelligence, 22.05.2020, S. 3: „Inadequate regulatory interventions and protracted periods of uncertainty during regulatory adjustments may also irreversibly destroy society's trust in new technologies. This, in turn, may thwart their societal adoption or even annihilate entire emerging markets, withholding potentially substantial benefits from society". Ebenso *Gurkaynak/Yilmaz/Haksever*, CLSR 32 (2016), 749, 758. Siehe auch Christian Borggreen, Vizepräsedent CCIA Europa, zum Entwurf der Europäischen Kommission für ein KI-Gesetz: „For example, an AI application that detects the spreading of the coronavirus might have to wait months before it could be used in Europe", zitiert nach *Espinoza/Murgia*, The four problems with Europe's vision of AI, Finan-

nen fairen Zugang zu autonomen Systemen für alle zu garantieren,[77] sowie die (nur) in Einzelfällen bestehenden und empirisch erwiesenen[78] unzumutbaren Risiken autonomer Systeme einzudämmen.[79]

2. *Grundlegende Innovationsskepsis*

Vereinzelt wird die Innovationskraft autonomer Systeme bzw. der Künstlichen Intelligenz umfassend in Zweifel gezogen. Das Maschinelle Lernen wird als ein vorübergehender Hype gedeutet[80] und das Leistungspotential der Künstlichen Intelligenz als marketingstrategisches Story-telling betrachtet.[81] Herausgestellt werden die faktischen Leistungsgrenzen verschiedener Anwendungen

---

cial Times 26.02.2020, https://www.ft.com/content/6759046a-57bf-11ea-a528-dd0f971febbc. So auch *Jamison*, European Commission's AI Regulations Would Limit Possibility, American Enterprise Institute, 27.02.2020 (https://www.aei.org/articles/european-commissions-ai-regulations-would-limit-possibility): „The EC's attempts to keep AI safe will also keep it from being as effective as it can be".

[77] *Yu*, Flo. L. Rev. 72 (2020), 331, 343–354. Siehe hierzu auch *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 13.

[78] Auf diesen Aspekt weist *Reed*, Philos Trans A Math Phys Eng Sci 376 (2018), 1, 2 hin: „Regulation cannot control unknown risks, and devising a regulatory mandate on the basis of speculative risks seems unlikely to produce successful results".

[79] Allein einen Schutz gegen die bewusst schädliche Verwendung von Künstlicher Intelligenz fordern etwa *Brundage/Avin/Clark u.a.*, The Malicious Use of Artificial Intelligence, 20.02.2018. Eine zurückhaltende regulative Eindämmung inakzeptabler Risiken fordert auch *Reed*, Philos Trans A Math Phys Eng Sci 376 (2018), 1, 2. In diese Richtung auch die *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 12: „Der Schwerpunkt eines Regulierungsrahmens sollte auf der Frage liegen, wie die Gefahr potenzieller und vor allem der schwersten Schäden minimiert werden kann".

[80] Eingehend *Gellert*, Int. Data Priv. Law 11 (2021), 196, 206. Siehe auch *Martin-Jung*, Künstliche Intelligenz wird überschätzt, SZ 30.11.2018, https://www.sueddeutsche.de/digital/kuenstliche-intelligenz-digitalgipfel-regierung-algorithmen-1.4233675: „Die Technologie […] leidet an Kinderkrankheiten". Vor allem die (derzeitige) Begrenztheit der Technik und ihrer Einsatzfelder wird in den Vordergrund gestellt, so etwa *ders.*, Künstliche Intelligenz wird überschätzt, SZ 30.11.2018, https://www.sueddeutsche.de/digital/kuenstliche-intelligenz-digitalgipfel-regierung-algorithmen-1.4233675.

[81] *Delko*, Hype und Realität in den Strassen von San Francisco, NZZ 09.08.2018, https://www.nzz.ch/finanzen/hype-und-realitaet-in-den-strassen-von-san-francisco-ld.1407930. Tatsächlich behaupten Unternehmen vielfach, Künstliche Intelligenz, d.h. dann Maschinelle Lernverfahren einzusetzen, um ihre Produkte attraktiver erscheinen zu lassen. Vgl. etwa die Studie im Auftrag von McKinsey *Bughin/Hazan/Ramaswamy u.a.*, Artificial Intelligence – the next digital frontier?, McKinsey Global Institute, Juni 2017, S. 13–19, wonach lediglich 20 % von 3000 befragten Unternehmen tatsächlich Künstliche Intelligenz zu einem bedeutenden Umfang verwenden.

autonomer Systeme.[82] Der Erwartung einer umfassenden Implementierung autonomer Systeme im Alltag wird dann entgegengetreten, ebenso der Technik eine echte Automatisierung bzw. Autonomisierung von Einzelaufgaben nicht zugetraut, da die begrenzte Leistungsfähigkeit autonomer Systeme stets eine menschliche Gegenkontrolle oder menschliche Assistenz erforderlich machen wird. Etwaige Risiken autonomer Systeme werden sich in dieser Perspektive dann gar nicht erst realisieren oder jedenfalls keine wesentlichen Schäden herbeiführen.

3. Herausstellen von Selbstverantwortung und Befürchtung paternalistischer Übergriffe

Andere erkennen die Risiken autonomer Systeme zwar an, trauen dem Einzelnen aber zu und fordern von diesem, sich den Gefährdungen autonomer Systeme selbst zu erwehren. Resilienzfähigkeit und Medienkompetenz müssten daher gestärkt werden,[83] was aber nicht notwendig und nicht nur durch den Staat erfolgen müsse. Regulative Zurückhaltung wird vor allem aus einer Grundüberzeugung liberaler Staatlichkeit gefordert. In einem Umfeld der Unsicherheit und Dynamik ist demnach der Einzelne gefordert, eigene Vorstellungen vom richtigen Umgang mit der neuen Technologie zu entwickeln. Ein Staat, der dem Einzelnen diese Aufgabe abnimmt oder ihn in eine bestimmte Richtung lenkt, verhält sich dieser Überzeugung zufolge paternalistisch und freiheitsfeindlich.[84] Staatliches Einschreiten sei zwar nicht ausgeschlossen, be-

---

[82] Siehe zum Texterstellungsprogramm ChatGPT *Chomsky/Roberts/Watumull*, The False Promise of ChatGPT, The New York Times 08.03.2023, https://www.nytimes.com/2023/03/08/opinion/noam-chomsky-chatgpt-ai.html.; *Stern*, Don't be deluded by the exaggerated claims made for AI, Financial Times 27.02.2023, https://www.ft.com/content/dc7d6217-a7ba-451a-a18f-d55356c7fae3. Vgl. mit Verweis auf die überzogenen Erwartungen hinsichtlich anderer technischer Erfindungen wie dem Internet *Taub*, New technology, same old blind spot?, The New York Times 17.02.2023, https://www.nytimes.com/2023/02/17/world/new-technology-same-old-blind-spot.html.

[83] So etwa *Gigerenzer*, Technik braucht Menschen, die sie beherrschen, Spektrum 12.11.2015, https://www.spektrum.de/kolumne/technik-braucht-menschen-die-sie-beherrschen/1375950; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 113. Dies wird unter dem Stichwort der „AI literacy" diskutiert, siehe hierzu *Yi*, European Journal of Bioethics 12 (2021), 353–368; *Ng/Leung/Chu u.a.*, Computers and Education: Artificial Intelligence 2 (2021), 1–11.

[84] Explizit zur Regulierung Künstlicher Intelligenz *Layton*, The Authoritarian Paternalism of EU Tech Policy, 13.03.2020 (https://www.aei.org/technology-and-innovation/the-authoritarian-paternalism-of-eu-tech-policy). In einem erweiterten Verständnis von Paternalismus wird auch kritisiert, wenn im Bereich der Künstlichen Intelligenz technische Experten und nicht betroffene Laien Risikobewertungen vornehmen, siehe hierzu mit entsprechender Kritik am Entwurf für ein KI-Gesetz, *Laux/Wachter/Mittelstadt*, Regulation & Governance 17 (2023), 1, 5. Vgl. für die Digitaltechnik und begleitende Datenschutzregulierung *Krönke*, Der Staat 55 (2016), 319–351; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015,

schränke sich aber auf die Gewährleistung von Grundbedingungen, die es dem Einzelnen ermöglichen, diese anspruchsvolle Aufgabe zu erfüllen.[85] In dieser Sichtweise wird die Freiheit vor der Sicherheit priorisiert. [86]

II. Risikozentrierte, interventionistische Ansätze

Personen, die die Einführung autonomer Systeme grundlegend ablehnen oder für strikte(re) Regulierung eintreten, stützen sich auf ein Weltbild dystopisch-technikpessimistischer Prägung (1.) und tragen idealisierend-moralische Erwartungen an die Technik heran (2.). Sie weisen ein hohes Sicherheitsbedürfnis auf und haben wenig Vertrauen in die Selbstschutzfähigkeit des Einzelnen (3.).

S. 362–366; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 202–204. Deutlich darin *Krönke*, Der Staat 55 (2016), 319, 350: „Als ein Leitgedanke personaler Autonomie wurde herausgearbeitet, dass der Einzelne in der Betätigung seiner Wertungen über das für seine eigene Person Gute oder Schlechte, Gesunde oder Ungesunde, Vernünftige oder Unvernünftige prinzipiell keinen Beschränkungen unterworfen werden darf und insbesondere keinem Zwang zu einer – wie auch immer bestimmbaren – objektiven Rationalität unterliegt". Siehe allgemein zu regulatorischem Paternalismus in Risikokonstellationen *Ogus*, in: Hopt (Hrsg.), Corporate governance in context, 2005, S. 302.

[85] Vgl. *Krönke*, Der Staat 55 (2016), 319, 339. Siehe ausführlich zur nicht-paternalistischem staatlichen Unterstützungsleistungen im Selbstdatenschutz und zur Abgrenzung von unzulässigem paternalistischen Eingreifen *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 362–375 Eine Regulierung muss dann vornehmlich auf Transparenz und auf Kontrollmöglichkeiten durch die NutzerInnen abstellen. In diese Richtung geht auch der Regulierungsansatz Künstlicher Intelligenz in Finnland, der die Herstellung der Medienkompetenz ins Zentrum stellt, siehe hierzu *Mocker*, Digitale Mündigkeit – Warum Finnland für Deutschland ein Vorbild ist, Gewerblicher Rechtsschutz und Urheberrecht 24.6.2019, https://www.handelsblatt.com/meinung/gastbeitraege/expertenrat/mocker/expertenrat-valerie-mocker-digitale-muendigkeit-warum-finnland-fuer-deutschland-ein-vorbild-ist/24479592.html.

[86] Siehe allgemein zum Verhältnis von Sicherheit und Freiheit im liberalen Verfassungsstaat *Di Fabio*, NJW 61 (2008), 421, 422; *Isensee*, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982 – erweiterte Fassung, 1983, S. 21–26. Sicherheit und Freiheit werden dabei als sich ergänzende Grundsätze verstanden, die erst in der Komplementarität echte Freiheit ermöglichen. Absolute Sicherheit im Sinne eines Ausschlusses jeglichen Risikos im privaten Bereich kann es demnach in einem liberalen Verfassungsstaat nicht geben, *Isensee*, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982 – erweiterte Fassung, 1983, S. 41 f.

1. Dystopie und Technikpessimismus

Manche treten autonomen Systemen mit einer prinzipiell technikpessimistischen Grundhaltung entgegen.[87] Auch sie sind, wie technikoptimistische Auffassungen, der Ansicht, dass autonome Systeme umfassend Verbreitung finden werden, bewerten diesen Umstand aber gegenteilig: Autonome Systeme werden, so die Erwartung, vor allem zu schädlichen Zielen eingesetzt werden,[88] doch auch bei Verwendung zu gemeinwohlverträglichen Zwecken wird es unvermeidlich zu Beeinträchtigungen von Interessen, ethischen Prinzipien und Rechtsgütern kommen.[89] Mit Sorge blicken manche auch auf sozioökonomische Veränderungen, die mit der zunehmenden Automatisierung der Lebenswelt einhergehen: Sie befürchten den Verlust von Arbeitsplätzen[90] oder die Benachteiligung oder den Ausschluss von Bevölkerungsgruppen, die nicht die Fähigkeit oder Bereitschaft mitbringen, diesen technischen Wandel mitzugehen.[91] Autonome Systeme schüren überdies Befürchtungen vor einem Kontrollverlust des Menschen gegenüber der Maschine,[92] von einer Ausrottung der Menschheit

---

[87] So auch *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 355. Dabei hat die Bevölkerung Deutschlands den Ruf, besonders technologiekritisch zu sein, vgl. *Hilgendorf*, in: Spiecker gen. Döhmann/Wallrabenstein (Hrsg.), IT-Entwicklungen im Gesundheitswesen: Herausforderungen und Chancen, 2016, S. 75, 79 ff. Siehe auch *Kleine*, in: Zoglauer/Weber/Friesen (Hrsg.), Technik als Motor der Modernisierung, 2018, S. 57.

[88] *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 987; *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 355. Ein typisches dystopisches Szenario ist etwa die Entwicklung eines Social Credit Systems. Vgl. auch *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 269–273; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 990. Problematisiert wird auch die Entwicklung automatisierter bzw. autonomer Waffensysteme, die dann als Massenvernichtungswaffen genutzt werden könnten, siehe hierzu *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 987–990.

[89] *Fast/Horvitz*, Long-Term Trends in the Public Perception of Artificial Intelligence, 02.12.2016, S. 967; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 987–1000.

[90] Siehe auch *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 31 f., 998; *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 40; *Palka*, Digitalisierung gefährdet Millionen von Jobs – welche besonders betroffen sind, Handelsblatt 26.4.2018, https://www.handelsblatt.com/unternehmen/management/digitaletransformation/oecd-studie-zur-zukunft-des-arbeitsmarktes-digitalisierung-gefaehrdet-millionen-von-jobs-welche-besonders-betroffen-sind/21217278.html. Siehe hierzu auch die Studie *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 42–44 zu Veränderung der Arbeitswelt, wonach die Anzahl der Arbeitsplätzen, die eine hohe technische Kompetenz voraussetzen, bis 2030 auf mehr als 50 % steigen wird, während Tätigkeiten, die nur geringer technischer Expertise bedürfen, auf 30 % sinken werden. Dies wirkt sich nicht nur nachteilig auf die Verfügbarkeit von Arbeitsplätzen in Bereichen einfach gelagerter Tätigkeiten aus, sondern auch auf die Lohngestaltung.

[91] Vgl. *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 227–229.

[92] Vgl. *Fast/Horvitz*, Long-Term Trends in the Public Perception of Artificial Intelligence, 02.12.2016, S. 966 f.: „The fear of loss of control, for example, has become far more

durch die Maschine,[93] von einem Übergang in eine transhumanistische Welt,[94] von der Obsolenz des Menschen[95] und vom Ende des menschlichen (intellektuell-kognitiven) Primats.[96]

2. *Idealisierung und Moralisierung*

Andere sehen in der Etablierung autonomer Systeme eine Möglichkeit zur Errichtung einer gerechteren, faireren und sichereren Welt.[97] Dieses Idealbild

---

common in recent years – more than triple what it was as a percentage of AI articles in the 1980s". Siehe auch *Russell/Dewey/Tegmark*, AI Magazine 36 (2015), 105, 111 f.; *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 366–369; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 110. Dies wird vor allem im Rahmen der „Superintelligenz", also der Entwicklung einer Generellen oder Starken Künstlichen Intelligenz diskutiert, siehe etwa *Bostrom*, Superintelligence, 2014, S. 127–144; *Russell*, Human compatible, 2019. Siehe auch *Bauberger/Beck/Burchardt u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 907, 916–917, 930–932. Siehe auch die Forderungen nach Kontrolle bzw. menschlicher Aufsicht bei *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 19 f., sowie zur Kontrolle von Algorithmen im Allgemeinen *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 77.

[93] Siehe hierzu *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 1001. Siehe auch *Wilson*, Robocalypse, 2011.

[94] Konkrete Szenarien einer transhumanistischen Welt präsentiert *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 227–232. Vgl. auch *Bauberger/Beck/Burchardt u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 907, 929. Zum – auch rechtlichen – Transhumanismus siehe auch eingehend *Kersten*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 315.

[95] *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 12.

[96] *Simanowski*, Wir halten uns für den Endpunkt der Schöpfung. Doch vielleicht ist der Mensch nur ein Zwischenwirt der Vernunft, NZZ 16.10.2020, https://www.nzz.ch/feuilleton/hegel-und-kuenstliche-intelligenz-willensfreiheit-anders-denken-ld.1581396.; *Markoff*, Scientists Worry Machines May Outsmart Man, The New York Times 25.07.2009, https://www.nytimes.com/2009/07/26/science/26robot.html.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 12. Dies wird vor allem im Rahmen der „technischen Singularität" diskutiert, vgl. grundlegend *Kurzweil*, The singularity is near, 2005. Siehe auch *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 227; *Bauberger/Beck/Burchardt u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 907, 930. Es wird auch von „Robopokalypse" oder „Transhumanismus" gesprochen, siehe ausführlich zu all dem *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 1001–1005.

[97] So etwa *Meckel*, Ist Künstliche Intelligenz die bessere Demokratin?, Handelsblatt 21.7.2022, https://www.handelsblatt.com/meinung/kolumnen/kreative-zerstoerung/kolumne-kreative-zerstoerung-ist-kuenstliche-intelligenz-die-bessere-demokratin/28519292.html; *Beschorner/Meckel*, Mut zum Träumen, Die Zeit 1.7.2018, https://www.zeit.de/2018/27/kuenstliche-intelligenz-roboter-utopie-kulturpessimismus. Eine Utopie einer Welt Künstlicher Intelligenz entwirft *Hannig*, Pantopia, März 2022.

wird dann zur normativen Vorgabe gemacht, hinter der die Technik nicht zurückbleiben darf. Bislang hingenommene Unzulänglichkeiten, Defizite oder Unannehmlichkeiten sind dieser Ansicht zufolge in der neuen Welt nicht akzeptabel.[98] Dies lässt sich etwa für die Bewertung der Intransparenz autonomer Systeme beobachten: Hier ist man nicht bereit, die fehlende menschliche Nachvollziehbarkeit von Entscheidungen hinzunehmen, obschon diese auch bei menschlichen Entscheidungen bestehen.[99] In ähnliche Richtung geht es, wenn Systeme Künstlicher Intelligenz erst dann als akzeptierfähig anerkannt werden, wenn diese selbst – nicht (allein) ihre Entwickler, Hersteller oder Betreiber – „ethisch" sind und also ethisch-moralisch für richtig befundene Lösungen finden und umsetzen.[100] Darin kann man auch den allgemeinen Trend zur Moralisierung in der öffentlichen Debatte erkennen: Autonome Systeme werden abgelehnt, da sie oder ihre Ergebnisse schlicht als moralisch verwerflich bewertet werden.[101]

---

[98] *Nürnberger/Bugiel*, DuD 40 (2016), 503, 504: „Interessanterweise haben wir an Algorithmen höhere ethische Ansprüche als an uns selbst". Vgl. auch *Wischmeyer*, AöR 143 (2018), 1, 45. Siehe allgemein zu diesem Phänomen *Bull*, Der Staat 58 (2019), 57, 98.

[99] Vgl. *Wischmeyer*, AöR 143 (2018), 1, 44 f.; *Bonezzi/Ostinelli/Melzner*, Journal of experimental psychology 151 (2022), 1 f.

[100] Gefordert wird also die Entwicklung einer Maschinenethik, d.h. einer Ethik, die unabhängig und neben die Menschenethik tritt, vgl. *Simanowski*, Wir halten uns für den Endpunkt der Schöpfung. Doch vielleicht ist der Mensch nur ein Zwischenwirt der Vernunft, NZZ 16.10.2020, https://www.nzz.ch/feuilleton/hegel-und-kuenstliche-intelligenz-willensfreiheit-anders-denken-ld.1581396. Ziel ist die Konstruktion von „moralischen Künstlichen Agenten" (Artificial Moral Agents – AMA), vgl. grundlegend *Wallach/Allen*, Moral machines, 2009. Siehe zur Forderung der Entwicklung ethischer Systeme der Künstlichen Intelligenz auch *Floridi/Sanders*, Minds and Machines 14 (2004), 349–379; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1; *Müller*, in: The Metaphysics Research Lab, Stanford University (Hrsg.), The Stanford Encyclopedia of Philosophy, 2020, 1.1. Andernorts wird von „Artificial Morality" gesprochen, siehe *Misselhorn*, Maschinenethik und „Artificial Morality", Bundeszentrale für politische Bildung, 2.2.2018, S. 3. Es geht dabei nicht um die Konstruktion von Systemen, die selbst ein moralisch-ethisches Bewusstsein haben können – dies ist (zumindest derzeit) technisch nicht möglich –, sondern um eine möglichst effektive Einprogrammierung solcher Wertvorstellungen in die Systeme, siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 61; *Misselhorn*, Maschinenethik und „Artificial Morality", Bundeszentrale für politische Bildung, 02.02.2018, S. 5 f.

[101] Siehe allgemein zum Phänomen der Moralisierung *Sprenger*, Ohne Moral geht es nicht. Aber wir moralisieren alles – und das ist falsch, NZZ 11.04.2018, https://www.nzz.ch/feuilleton/bekenne-du-schlechter-mensch-ld.1375392. Handlungen werden demnach nicht anhand ihrer realen Vor- oder Nachteile bewertet, sondern danach, ob sie nach der eigenen (Moral-)Vorstellung gut oder schlecht sind. Vgl. speziell für den Bereich der Technikethik bzw. der Ethisierung der Technik *van den Daele*, in: Bogner (Hrsg.), Ethisierung der Technik – Technisierung der Ethik, 2013, S. 29.

3. Hohe Risikosensibilität und Bedenken hinsichtlich Selbstschutzfähigkeit

Auch ein erhöhtes Sicherheitsbedürfnis und eine geringe Fehler- und Risikotoleranz können Ursache dafür sein, dass autonome Systeme abgelehnt oder eine strikte Regulierung eingefordert wird.[102] Eine Geringhaltung des Risikos ist demnach nicht ausreichend, ein gutes Leben gibt es nur, wo Risiken gänzlich ausgeschlossen sind („Null-Risiko-Politik").[103] Dem liegen Überzeugungen zugrunde, wie sie typisch für die Risikogesellschaft sind.[104] Verbunden ist diese Risikosensibilität typischerweise mit einer geringem Vertrauen in die Steuerungsmechanismen des Marktes[105] und in die Existenz und Bereitschaft zum Einsatz von Selbstschutz- und Resilienzmechanismen des Einzelnen.[106]

---

[102] Einer Studie des *Verbands der TÜV e. V.*, Verbraucher:innen wollen Sicherheit und Transparenz bei Künstlicher Intelligenz, Verband der TÜV e. V., 27.01.2020, S. 35 zufolge fordern 40 % der Befragten eine Fehlerfreiheit von 100% ein, nur 17 % halten Fehler für hinnehmbar. Dabei ist die Fehlertoleranz abhängig vom Einsatzgebiet: Bei Anwendungen mit geringem Risiko sind 45 % bereit, Fehler zu tolerieren. Auffällig ist zudem, dass der Begriff der Sicherheit vielfach sehr weit definiert wird, so etwa die *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 15: „KI-Systeme sollten Schäden weder verursachen noch verschärfen oder sich auf andere Art und Weise auf Menschen negativ auswirken".

[103] *Bucheli*, Wir sind auf dem besten Weg, in der Null-Risiko-Gesellschaft zu versauern, NZZ 19.02.2020, https://www.nzz.ch/feuilleton/der-mensch-ist-ein-nervenbuendel-unterwegs-in-die-null-risiko-zone-ld.1540844.

[104] Siehe hierzu grundlegend *Beck*, Risikogesellschaft, 1968; *Bonß*, Vom Risiko, 1995. Siehe hierzu auch *Bucheli*, Wir sind auf dem besten Weg, in der Null-Risiko-Gesellschaft zu versauern, NZZ 19.02.2020, https://www.nzz.ch/feuilleton/der-mensch-ist-ein-nervenbuendel-unterwegs-in-die-null-risiko-zone-ld.1540844; *Bucheli*, Willkommen in der Angsthasengesellschaft, NZZ 07.07.2018, https://www.nzz.ch/feuilleton/die-angsthasengesellschaft-liefert-sich-als-williges-opfer-dem-populismus-aus-ld.1403475.

[105] Dies wird besonders auf die Erfahrungen im Hinblick auf die (anfängliche) Nicht-Regulierung des Internets und den nachteiligen Folgen dessen gestützt. So etwa *Roose*, We Need to Talk About How Good A.I. Is Getting, The New York Times 24.08.2022, https://www.nytimes.com/2022/08/24/technology/ai-technology-progress.html: „We could end up with a repeat of what happened with social media companies after the 2016 election – a collision of Silicon Valley power and Washington ignorance, which resulted in nothing but gridlock and testy hearings". Ebenso *MacCarthy*, AI needs more regulation, not less, Brookings, 09.03.2020 (https://www.brookings.edu/research/ai-needs-more-regulation-not-less): „The calls for modest regulation that lets industry take the lead are part of a failed regulatory philosophy, one that saw its natural experiment over the past several decades come up lacking. AI is too important and too promising to be governed in a hands-off fashion, waiting for problems to develop and then trying to fix them after the fact". Siehe auch *Pichai*, Why Google thinks we need to regulate AI, Financial Times 20.01.2020, https://www.ft.com/content/3467659a-386d-11ea-ac3c-f68c10993b04.

[106] Nach der Studie des *Verbands der TÜV e. V.*, Verbraucher:innen wollen Sicherheit und Transparenz bei Künstlicher Intelligenz, Verband der TÜV e. V., 27.01.2020, S. 40 sehen 62 % der Befragten die Verantwortung für die sichere Ausgestaltung bei den Herstellern von Produkten und Anwendungen der Künstlichen Intelligenz. Vgl. auch *Nemitz*, Philos

Echten Schutz können in dieser Betrachtung daher nur andere, vornehmlich dann der Staat bieten. In einer Welt komplexer Techniken und diffuser Risiken ist, so die Ansicht, der Einzelne strukturell überfordert und der Staat in die Verantwortung gerufen.[107] In dieser Perspektive gewährleistet die staatliche Intervention freiheitsnotwendige Sicherheit, die freiheitsfeindliche paternalistisch-bevormundende Wirkung wird nicht wahrgenommen oder jedenfalls als hinnehmbar erachtet. Sicherheit wird hier vor der Freiheit priorisiert.[108]

C. Konkrete Vulnerabilitätsphänomene autonomer Systeme

Im Folgenden soll dargelegt werden, wie sich die oben beschriebenen Risiken auf Interessen und Rechte Einzelner auswirken und so Bedarf für legislatives Einschreiten begründen. Sie lassen sich in vier Interessensgruppen aufteilen: Auswirkungen auf den Markt, die Gesamtgesellschaft, die Persönlichkeit und Würde und schließlich die individuelle Freiheit. Diese Vulnerabilitätsphänomene sind es, die der Gesetzgeber adressieren und mit kollidierenden Interessen in einen angemessenen Ausgleich bringen muss. Sie bilden damit die Grundlage für die anschließende kritische Prüfung der DSGVO. Die Untersuchung soll sich dabei auf Autonomiegefährdungen und Diskriminierungen be-

---

Trans A Math Phys Eng Sci 376 (2018), 7: „It is clear […] that AI cannot and will not serve the public good without strong rules in place. […] Over and over society has confirmed the experience that law, and not the absence of law, relating to critical technology serves the interests of the general public".

[107] Entsprechend herrschen in den aktuellen Regulierungsentwürfen, etwa dem Vorschlag der EU-Kommission für eine KI-Verordnung, zentrale, durch den Staat vorgegebene Regulierungsinstrumente vor. Dass Künstliche Intelligenz für die VerbraucherInnen „vertrauenswürdig" ist, so die *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 9 f., eine Aufgabe des Staates, nicht der Unternehmen. Plakativ das Zitat eines Siemens-Mitarbeiters zur Strategie der EU-Kommission hinsichtlich der Künstlichen Intelligenz: „Das aktuelle Weißbuch der EU-Kommission vermittelt den Eindruck, dass Vertrauen in KI nur durch eine Regulierung und Zertifizierung erreicht werden kann", zitiert nach *Siebenhaar*, EU-Parlament will Überregulierung von KI verhindern, Handelsblatt 19.10.2020, https://www.handelsblatt.com/politik/international/kuenstliche-intelligenz-eu-parlament-will-ueberregulierung-von-ki-verhindern/26281962.html. Auch im Datenschutzrecht lassen sich in der Rechtswissenschaft zunehmend Forderungen nach mehr zentralisierten, objektivrechtlichen Schutz beobachten, siehe hierzu eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 181–184.

[108] Siehe zum Verhältnis von Freiheit und Sicherheit im liberalen Verfassungsstaat bereits oben unter Kapitel 2 B. I. 3. Kritisch zu einer Priorisierung der Sicherheit etwa *Di Fabio*, NJW 61 (2008), 421, S. 422, 425; *Isensee*, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982 – erweiterte Fassung, 1983, S. 41 f.

schränken. Was damit konkret gemeint ist, soll der nachfolgende Abschnitt verdeutlichen.

Risikoanlagen und Anwendungsfelder autonomer Systeme sind äußert divers, entsprechend vielgestaltig sind diese Gefährdungsszenarien.[109] Es kann daher nur ein Ausschnitt der Problemfelder präsentiert werden. Betrachtet werden dabei allein ordnungsgemäß funktionierende Systeme; Gefährdungslagen aufgrund unbeabsichtigter Fehler oder bewusst schädlicher Zugriffe durch Dritte bleiben außer Betracht.

Zunächst sollen nachteilige Effekte für den Markt (I.), anschließend für die Gesamtgesellschaft (II.), sodann für die Persönlichkeit (III.) und schließlich die Autonomie (IV.) dargelegt werden.

I. Markteffekte: Machtasymmetrien und Verbraucherwohlfahrtsverluste

Der Einsatz autonomer Systeme kann zu Machtasymmetrien und Wohlfahrtsverlusten führen, dies im einzelnen rechtsgeschäftlichen Verhältnis (1.), aber auch in der Marktarchitektur insgesamt (2.).

1. Wohlfahrtsverluste in der Vertragsgestaltung

Der Einsatz autonomer Systeme lässt Informationsasymmetrien zulasten der VerbraucherInnen entstehen. Autonome Systeme verschaffen den betreibenden Unternehmen umfassendes Wissen über VerbraucherInnen, während diese umgekehrt nicht in selbem Maße über Kenntnisse über die Unternehmen verfügen.[110] Ihnen ist zudem nicht bekannt, welche Erkenntnisse die Unternehmen über sie haben, dies sowohl aufgrund der Intransparenz der autonomen Sys-

---

[109] Einen Überblick über verschiedene Regulierungsbedarfe von Profilbildungsmaßnahmen bieten *Hildebrandt/Gutwirth* (Hrsg.), Profiling the European Citizen, 2008, S. 241–364, von Algorithmen im Allgemeinen *Martini*, Blackbox Algorithmus, 2019, S. 27–112 mit anschaulicher Tabelle, von Systemen Künstlicher Intelligenz *Wischmeyer/Rademacher* (Hrsg.), Regulating Artificial Intelligence, 2020. Vgl. zu verschiedenen Konstellationen der Steuerung durch Algorithmen auch *Hoffmann-Riem*, AöR 142 (2016), 1, 11–20.

[110] Siehe umfassend zu all dem *Mik*, Law Innov. Technol. 8 (2016), 1, 12–14. Vgl. auch *Sartor*, New aspects and challenges in consumer protection, Europäisches Parlament, April 2020, S. 18; *Martini*, Blackbox Algorithmus, 2019, S. 63; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 224 f.; *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 229 f.; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 108; *Paal*, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), 43, 49; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 406; *Schermer*, CLSR 27 (2011), 45, 47. Vgl. auch *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 308–309, 318.

teme[111] wie auch aufgrund unternehmerischer Geheimhaltung.[112] Die ungleiche Verteilung von Wissen über den Vertragspartner stärkt die Verhandlungsposition der Unternehmen und schwächt diejenige der VerbraucherInnen.[113] Informationsasymmetrien entstehen zudem durch die Intransparenz der algorithmischen Entscheidungsarchitekturen, die die Verhandlungsposition von VerbraucherInnen beeinträchtigen kann: Kennen sie Entscheidungsparameter und -regeln nicht, können sie keinen Einfluss auf die Vertragsgestaltung nehmen,[114] jedenfalls sind sie in der Durchsetzung ihrer Interessen erheblich beeinträchtigt.[115] Hinzu kommt, dass aufgrund der Determiniertheit der algorithmischen Entscheidungsfindung VerbraucherInnen daran gehindert sind, sich in den

---

[111] Sehr allgemein im Hinblick auf Smarte Technologien *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 67–68, 71, 93. Explizit *dies.*, Smart technologies and the end(s) of law, 2016, S. 68: „The power of definition shifts from a multiplicity of others – with whom [the person] can interact and discuss, whose interpretations she can question and reject – to an anonymous infrastructure that seems to know things about her without giving her a clue as to the how or the why" und weiter *dies.*, Smart technologies and the end(s) of law, 2016, S. 71: „There is no reciprocity. […] because we don't know how [the algorithms] interpret us". Auf das Problem mangelnder Transparenz weisen auch hin *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 10. Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 28 f.; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 63 f.

[112] *Dornis*, ZfPW 8 (2022), 310, 313.

[113] So ausdrücklich *Schermer*, CLSR 27 (2011), 45, 47: „Information asymmetries may influence the level playing field between government and citizens, and between businesses and consumers, upsetting the current balance of power between different parties". Vgl. auch *Dornis*, ZfPW 8 (2022), 310, 312 f.; *Bull*, Der Staat 58 (2019), 57, 89 f. Siehe auch *Paal*, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), 43, 49; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 406; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 222; *Mik*, Law Innov. Technol. 8 (2016), 1, 12–14. Eine gestörte Vertragsparität aufgrund des überlegenen Wissens der Unternehmen erkennt auch *Hofmann*, WiRO 62 (2016), 1074, 1081: „Kennt der Unternehmer den Verbraucher durch die Möglichkeiten der Digitaltechnik gleichsam besser als dieser sich selbst, liegt darin mehr als nur das generelle Ungleichgewicht zwischen unterschiedlich starken Wirtschaftssubjekten".

[114] Zur Entstehung von Machtasymmetrien allgemein siehe *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 61 f.; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 437; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 36, 38; *Yeung*, iCS 20 (2017), 118, 123. Zur Auswirkung für den Anwendungsfall personalisierter Preisbildung: *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 406: „Im Unterschied zum ‚Feilschen' in der analogen Einkaufswelt findet kein Verhandeln auf Augenhöhe statt, sondern auf Basis einer Informationsasymmetrie zugunsten des Unternehmers. […] Mangels Kenntnis der relevanten Kriterien kann zudem nicht nachgeprüft werden, ob die Anwendung eines Algorithmus in unzulässiger Weise eine Übervorteilung darstellt".

[115] *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 999; *Ernst*, JZ 72 (2017), 1026, 1034; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 222, 239; eher kritisch *Zarsky*, Theoretical Inquiries in Law 20 (2019), 157, 172 f.

Verhandlungsprozess einzubringen.[116] Hierfür müssten technische Einwirkungsoptionen vorgesehen sein und die VerbraucherInnen über entsprechende technische Fertigkeiten verfügen.[117] Am Ende findet so gar keine Verhandlung mehr statt. Zu befürchten ist dann, dass Unternehmen einseitig ihre Interessen durchsetzen und die Gemeinwohlfahrt leidet.[118] Dass eine einseitige Wissens- und Machtverteilung ganz generell gemeinwohlschädliche Verschiebungen der Märkte zulasten der VerbraucherInnen erwarten lassen, ist ein Gemeinplatz.[119]

2. Wohlfahrtsverluste aufgrund monopolartig strukturierter Datenmärkte

Digitale Märkte sind derzeit monopolartig strukturiert.[120] Dies lässt erwarten, dass auch autonome Systeme nur von einigen wenigen Akteure bereitgestellt werden, die allein über die notwendige Datenmenge, Hardware und fachperso-

---

[116] *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 406. Ebenso *Schneiders*, Jeder kriegt einen eigenen Preis, FAZ 08.04.2015, https://www.faz.net/aktuell/finanzen/meine-finanzen/geld-ausgeben/dynamische-preise-das-ende-des-einheitspreises-13522679.html: „Es wird wieder gefeilscht. Allerdings ohne, dass wir etwas davon mitbekommen: Das Verhandeln übernehmen jetzt Algorithmen". Vgl. auch *Ernst*, JZ 72 (2017), 1026, 1034. *Dornis*, ZfPW 8 (2022), 310, 315 prognostiziert sogar einen „death of contract".

[117] Dies kann dazu führen, dass sich technisch versierte und informierte VerbraucherInnen über entsprechende technische Vorkehrungen eine bessere Behandlung erstreiten können, während die anderen einen automatisierten Vertrag oder eine automatisierte Entscheidung hinnehmen müssen. Dies kann zu einer Ungleichbehandlung von Konsumenten führen. Siehe zu diesen Überlegungen hinsichtlich des Anwendungsbeispiels personalisierter Preise *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 227, allgemein *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1026. Siehe auch *Zarsky*, Science, Technology, & Human Values 41 (2016), 118, 124 f.

[118] *Paal*, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), 43, 48 f.; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 225–227. So auch *Mik*, Law Innov. Technol. 8 (2016), 1, 20 f.; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 121.

[119] *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 308; *Hoffmann-Riem*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 1, 17 f.; *Schermer*, CLSR 27 (2011), 45, 47. Zu Wohlfahrtsverlusten durch personalisierte Preisbildung siehe eingehend *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 224–227; *Ernst*, JZ 72 (2017), 1026, 1034; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 405 f. Vgl. auch *Zuboff*, The age of surveillance capitalism, 2019, die den Übergang in einen „Überwachungskapitalismus" (surveillance capitalism) erkennt. Ihr zufolge lassen die neuen Datenaufzeichnungs- und -auswertungssysteme einen neuen Markt, den Überwachungsmarkt entstehen, auf dem das Wissen über das (zukünftige) Verhalten der Konsumenten das maßgebliche Kapital darstellt.

[120] Einführend in die Thematik *Clement/Schreiber/Bossauer u. a.* (Hrsg.), Internet-Ökonomie, 2019; *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft, 18.10.2017. Vgl. auch *Hoffmann-Riem*, in: ders. (Hrsg.), Big Data, 2018, S. 11, 38–40. Siehe zu institutionsökonomischen Erwägungen *Akerlof*, The Quarterly Journal of Economics 84 (1970), 488–500.

nelle Ausstattung verfügen, während Konkurrenten den Wettbewerbsnachteil einer zu geringen datenmäßigen, algorithmischen und personellen Ausstattung kaum aufholen können.[121] Zusätzlich lässt sich beobachten, dass die „High Performer" im Bereich der Künstlichen Intelligenz prozentual deutlich größere Summen in die Entwicklung und den Einsatz von Künstlicher Intelligenz investieren als ihre Marktkonkurrenten.[122] Dies vergrößert noch weiter den Innovationsvorsprung dieser „High Performer". VerbraucherInnen mangelt es dann an Alternativangeboten, über die sie ihre Interessen (besser) verfolgen könnten.[123] Die umfassenden Kenntnisse über den Einzelnen liegen dann zudem in der Hand einiger weniger, die diese zu eigenen, wirtschaftlichen Zielen einsetzen können und erwartbar werden.[124]

---

[121] Eingehend *Hennemann*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 361, 367–370 (er unterscheidet „competiton *for* AI", d.h. die Entwicklung der Technik, und „competition with AI", d.h. die Vermarktung der Technik). Von einer Monopolstellung einzelner Unternehmen im Hinblick auf Künstliche Intelligenz gehen auch *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 4, 38–41 in ihrer Modellstudie bis 2030 aus. Die aktuelle globale wettbewerbliche Situation hinsichtlich der Künstlichen Intelligenz stellt *Walch*, Why The Race For AI Dominance Is More Global Than You Think, Forbes 9.2.2020, https://www.forbes.com/sites/cognitiveworld/2020/02/09/why-the-race-for-ai-dominance-is-more-global-than-you-think/?sh=5b6030d121ff vor: Zu den maßgeblichen Unternehmen gehören etwa Amazon, Apple, Meta (ehemals Facebook), Google, IBM und Microsoft für den amerikanischen und europäischen Markt oder Alibaba, Baidu, Tencent und Huawei Technologies für den chinesischen Markt. *Webb*, The Big Nine, 2019 macht neun relevante Unternehmen aus dem amerikanischen und chinesischen Markt aus: Alibaba, Amazon, Apple, Baidu, Meta (ehemals Facebook), Google, IBM, Microsoft und Tencent. Siehe zu Wettbewerbsvorsprüngen entwickelter Länder des globalen Nordens gegenüber weniger entwickelten Länder die Modellstudie von *Bughin/Seong/Manyika u.a.*, Modeling the Impact of AI on the World Economy, September 2018, S. 3–4, 30–37.

[122] Siehe eingehend hierzu die Studie von *Chui/Hall/Mayhew u.a.*, The state of AI in 2022 – and a half decade in review, McKinsey & Company, Dezember 2022, S. 12. Die Bereitschaft zur Investition ist der Studie zufolge zwischen den verschiedenen Unternehmen auf dem Markt ähnlich verteilt, allerdings sind Marktführer im Bereich der Entwicklung und Erforschung von Künstlicher Intelligenz bereit, deutlich höhere Summen (20 % und mehr des Budgets) einzusetzen. Dies führt dazu, so die Studie, dass die „Global Players" auch für Fachpersonal deutlich attraktiver sind, während andere Unternehmen teilweise Schwierigkeiten haben, Fachpersonal anzuwerben.

[123] So auch *Paal*, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), 43, 49.

[124] *Hennemann*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 361, 370–373; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 110–112; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 36; *Yeung*, iCS 20 (2017), 118, 123. Diese Problematik deuten auch an *Hoffmann-Riem*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 1, 17 f.; *Martini*, Blackbox Algorithmus, 2019, S. 62 f.

II. Gesamtgesellschaftlich-kollektive Phänomene: (Real-)Diskriminierung, Fragmentierung und Fairness

Autonome Systeme können unmittelbare und mittelbare Diskriminierungen sowie Ungleichbehandlungen hervorrufen (1.), sozialschädliche Fragmentierungs- und Segmentierungseffekte freisetzen (2.) und materielle Vorstellungen von Gerechtigkeit und Fairness beeinträchtigen (3.).

1. Diskriminierungen, Realdiskriminierungen und Ungleichbehandlungen

Autonome Systeme können diskriminierend wirken (a)) und Ungleichbehandlungen herbeiführen (b)).

a) Diskriminierungen durch autonome Systeme

Die Gruppenbildungen im Modell können inakzeptable Vorprägungen der menschlich-analogen Welt enthalten.[125] In die Daten,[126] die Datenauswahl[127] oder das Algorithmentraining[128] fließen derartige Verzerrungen zugunsten oder

---

[125] Vgl. umfassend die Darstellung zu verschiedenen Formen und Ursachen des Maschinellen Bias bei *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019, S. 3–7; *Smith*, Dealing With Bias in Artificial Intelligence, The New York Times 19.11.2019, https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html.; *Ntoutsi/Fafalios/Gadiraju u.a.*, Bias in Data-driven AI Systems, 14.01.2020; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 10–14; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 104–109.

[126] Hier sind bereits in den Daten bestimmte Personengruppen mit spezifischen positiven oder negativen Eigenschaften konnotiert, etwa Männer mit einem höheren Gehalt als Frauen. Zum Input bzw. Historical Bias oder Social Bias siehe *Martini*, Blackbox Algorithmus, 2019, S. 50–58; *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1148; *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 680 f.; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 105; *Russell/Norvig*, Artificial Intelligence, ^{4}2021, S. 995 f.; *Bauberger/Beck/Burchardt u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 907, 918 f.

[127] Hier sind Minderheiten im Datensatz unterrepräsentiert, etwa in einem Datensatz für eine Bewerberauswahl Personen einer bestimmten Ethnie, sodass das Modell diese nicht zutreffend abbilden kann. Zum Sampling oder zur Representation siehe *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1148; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 105; *Bender/Gebru/McMillan-Major u.a.*, in: Coscia (Hrsg.), Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2021, S. 610; *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 684–688.

[128] Vorprägungen der am Trainingsverfahren beteiligten menschlichen Akteure fließen zwangsläufig in das Trainingsverfahren ein. Siehe hierzu *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1147; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 106; *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 681–684, 688–690; *Bauberger/Beck/Burchardt u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch

zulasten bestimmter Personen(gruppen) ein und werden dort repliziert und verstärkt. Problematisch ist dabei vor allem, dass Ergebnisse autonomer Systeme diskriminierend wirken, obschon diese nicht unmittelbar an bekannte Diskriminierungsmerkmale, etwa das Alter oder das Geschlecht, anknüpfen. Häufig sind nämlich vermeintlich neutrale Kriterien, etwa der Wohnort, mit Diskriminierungsmerkmalen verbunden (sogenannte Proxies).[129] Das Löschen von Diskriminierungsmerkmalen genügt daher nicht, um die Diskriminierungen durch autonome Systeme zu unterbinden.[130] Ohnehin sind diese Diskriminierungen im algorithmischen Konstrukt nicht erkennbar, eben da die Kriterien nach außen hin objektiv erscheinen.[131] Bei menschlich nicht nachvollziehbaren Modell- und Problemlösungsalgorithmen werden sich die Ursachen von Diskriminierungen überhaupt nicht mehr aufdecken und damit effektiv beseitigen lassen.[132] Herausfordernd ist zudem, dass die (Real-)Diskriminierungsfreiheit eine sozionormative Richtigkeitsvorgabe darstellt, die sich nur schwer in eine

---

der Künstlichen Intelligenz, [6]2021, S. 907, 918 f. Plakativ *Martini*, Blackbox Algorithmus, 2019, S. 48 f. „[Algorithmen] sind typischerweise den Zielvorstellungen ihrer Schöpfer, insbesondere legitimen wirtschaftlichen Ertragszielen, verschrieben und daher auch nur so wertfrei bzw. wertbeladen wie der ergebnisorientierte Korridor, den sie ihnen belassen". Olga Russakovska weist darauf hin, dass programmierende Personen überwiegend männlichen Geschlechtes sind und aus bestimmten sozioökonomisch und sozionormativ geprägten Umfeldern stammen, deren Vorstellungen dann in die Algorithmen einfließen, vgl. *Smith*, Dealing With Bias in Artificial Intelligence, The New York Times 19.11.2019, https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html. Auch ein intentionales Aufrechterhalten oder Einfügen von Diskriminierungen durch die den Algorithmus trainierende Stelle ist denkbar, hierzu *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 692 f.

[129] Dem Wohnort kann Diskriminierungsrelevanz zukommen, wenn dort typischerweise bestimmte ethnische Personengruppen wohnen. Zu diesem und weiteren Beispielen siehe *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1148 f.; *Martini*, Blackbox Algorithmus, 2019, S. 52; *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 691 f.; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 107–109. Siehe auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 194.

[130] *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 993; *Martini*, Blackbox Algorithmus, 2019, S. 240–242; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 108.

[131] Die diskriminierende Wirkung entsteht oftmals auch erst aus einer Kombination verschiedener vermeintlich neutraler Kriterien, *Mann/Matzner*, Big Data and Society 6 (2019), 1, 5. Zu den Beweisschwierigkeiten derartiger Diskriminierungen siehe ausführlich *Barocas/Selbst*, Cal. L. Rev. 104 (2016), 671, 701–714. Letztlich kann so jedes Unterscheidungsmerkmal ein Proxy darstellen, so auch *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1153; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 116–118.

[132] Siehe zu den Herausforderungen des Nachweises algorithmischer Diskriminierungen allgemein *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2019, S. 106.

algorithmische Regel fassen lässt. Technisch läuft alles richtig, allein sozionormativ sind die Ergebnisse unerwünscht.[133]

b) Ungleichbehandlung durch autonome Systeme und Social-Credit-System

Die Klassifizierungen im Modell bzw. Lösungsalgorithmus, in denen typisiert bestimmte Eigenschaften mit bestimmten vorteilhaften oder nachteiligen Ergebnissen verknüpft werden, kann zudem zu strukturellen Benachteiligungen von Personen(gruppen) führen, die nicht über die Diskriminierungsmerkmale abgedeckt sind.[134] Befürchtet wird vor allem eine Benachteiligung finanziell schwacher Personengruppen. Auch hier sind es letztlich die in den Daten, aber auch den Vorprägungen der Akteure angelegten Vorurteile, die sich dann in den Modellen bzw. Lösungsalgorithmen wiederfinden (maschineller Bias).[135] Problematisch sind dabei die selbstbestärkenden Effekte Maschineller Lernverfahren: In den Profilverwendungen werden Daten produziert, die dann als neue Trainingsdaten dienen, in diesen Profilverwendungen werden aber gerade die strukturellen Benachteiligungen bedient.[136] Mit der zunehmenden Verbrei-

---

[133] Vgl. zu diesen Schwierigkeiten *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 993; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 108 f. Wenn etwa eine Frau aufgrund systematischer Benachteiligung ein niedrigeres Gehalt erhält als ein Mann, ist sie weniger kreditwürdig. Dies ist in einem mathematischen Modell ein korrektes, aber in einer sozionormativen Wertung nicht akzeptierfähiges Ergebnis.

[134] Siehe aus der Fülle der Literatur *Eubanks*, Automating inequality, January 2018 sowie *Martini*, Blackbox Algorithmus, 2019, S. 49 f.; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 9; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 5; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 225 f.; *Zarsky*, Science, Technology, & Human Values 41 (2016), 118, 123–127; *Miller*, J. Law Technol. Policy 2014, 41, 93. Siehe auch *Madden/Gilman/Levy u.a.*, Washington University Law Review 95 (2017), 53–125 mit Zitierung zahlreicher Studien zur Benachteiligung von Personen mit geringem Einkommen. Siehe grundlegend zu Stigmatisierungseffekten durch Datenanalyseverfahren *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 97: „Der Zweck solcher Vorhersagen ist Selektion. Mittelbar schafft die datenbasierte Selektion soziale Ränge, Stigmatisierung und Entindividualisierung, weil der Einzelne im Wesentlichen durch eine statistische Regelmäßigkeit identifiziert wird und falsch-positive Identifikationen statistisch nicht auszuschließen sind".

[135] Vgl. bereits für Big-Data-Analysen *Tene/Polonetsky*, Northwest. J. Technol. Intellect. Prop. 11 (2013), 239, 254.

[136] Erteilt ein autonomes System bestimmten Personen aufgrund ihrer Gruppenzugehörigkeit keinen Kredit, erhält es im Weiteren die Rückmeldung, dass diese Personengruppe mit einer hohen Wahrscheinlichkeit keinen Kredit zugeteilt bekommt. So bestätigt sich fortlaufend die aufgefundene algorithmische Regel. Das autonome System prüft eben immer nur die statistische Richtigkeit eines Ergebnisses, nicht seine sozionormative Akzeptierfähigkeit. Siehe hierzu *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1150; *Martini*, Blackbox Algorithmus, 2019, S. 49 f.; *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019, S. 7; *Tischbirek*, in: Wischmeyer/Rade-

tung der Systeme und des Einsatzes ähnlicher Algorithmen in verschiedenen Anwendungen steht zu befürchten, dass diese Effekte bereichs- und anwendungsübergreifend wirken und sich verstärken.[137] Am Ende könnte dies zu einer Welt führen, in der die gesamte Lebensführung des Einzelnen einem Bewertungsregime zugeführt wird, anhand dessen über die Zuteilung von Vor- und Nachteilen entschieden wird (Social-Credit-System).[138]

2. *Fragmentierung und Segmentierung*

Der gruppenbezogen-klassifizierende Ansatz autonomer Systeme kann schließlich gesellschaftliche Fragmentierungs- und Segmentierungseffekte freisetzen. Dies kann zu gesellschaftlichen Spaltungen führen.[139] In einer Welt umfassender Verbreitung autonomer Systeme erhält jede Person entsprechend

---

macher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 105; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 60; *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 112, 113.

[137] Vor allem die Erstellung ähnlicher Klassifizierungen von autonomen Systemen in verschiedenen Anwendungsbereichen ist dann problematisch. Dann besteht die Gefahr, dass bestimmte Personen(gruppen) bereichs- und marktübergreifend eine nachteilige Behandlung erfahren, etwa keinen Kredit und keine Wohnungszusage erhalten, zudem höhere Versicherungsprämien zahlen müssen. Diese ökonomische Segmentierung der Gesellschaft in Gruppen, aus denen die Individuen nicht mehr austreten können, entspricht dann den für die Kommunikation im digitalen Raum konstatierten Echokammern, hierauf weist zutreffend hin *Ernst*, JZ 72 (2017), 1026, 1028 f. Vgl. zu diesen Effekten auch *Martini*, Blackbox Algorithmus, 2019, S. 54; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 5; *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 230.

[138] Grundlegend *Lyon*, Surveillance as social sorting, 2003. Vgl. für Systeme der Künstlichen Intelligenz *Mainzer*, Künstliche Intelligenz – Wann übernehmen die Maschinen?, [2]2019, S. 269–273; *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 990; *Mann/Matzner*, Big Data and Society 6 (2019), 1, 2. Zur Gefahr der Entwicklung derartiger Systeme im Bereich der Preisdiskriminierung siehe *Miller*, J. Law Technol. Policy 2014, 41, 93. Siehe auch *Citron/Pasquale*, The Washington Law Review 89 (2014), 1–33 Vor allem die Nutzung eines derartigen umfassenden Bewertungssystems im staatlichen Bereich wird als Grenzüberschreitung wahrgenommen, siehe etwa *Mozur*, Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras, New York Times 08.07.2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 56.

[139] *Baur*, Algorithmic decision-making and social division, 21.2.2019 (https://dorotheabaur.medium.com/algorithmic-decision-making-and-social-division-acknowledging-the-political-context-of-ai-e071e34524bb). Eingehend auch *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 120–122. Für den Bereich der Informationsfilterung *Just/Latzer*, Media, Culture & Society 39 (2017), 238, 246 f.: „The governing character of algorithms, their role in reality construction, makes them a source and factor of social order".

ihrem Profil bestimmte Informationen, bekommt bestimmte Produkte angeboten oder zahlt einen bestimmten Preis, lebt also umfassend in der Realität ihrer Vergleichsgruppe.[140] Ein Ausbruch oder Wechsel aus diesen Gruppen ist nicht möglich, solange dies technisch nicht vorgesehen ist.[141] Selbstbestärkende Effekte des Maschinellen Lernverfahrens lassen eine Verstärkung dieser gruppenspezifischen Einordnungen befürchten (Lock-in-Effekt).[142] Dem Einzelnen sind diese gruppenspezifischen Realitätsgestaltungen nicht bewusst und Merkmale „seiner" Realität bzw. der anderer nicht bekannt.[143] Die Kluften zwischen den Gruppen könnten sich vertiefen, da es an Berührungspunkten, Begegnungsmomenten und Kommunikationsmöglichkeiten zwischen den Gruppen fehlt. Wenn der Einzelne die Realitäten anderer Personen(gruppen) nicht kennt, mag es ihm zudem an Verständnis für die Lebensweise, Einstellungen und Herausforderungen anderer Personen(gruppen) fehlen.

Derartige Phänomene lassen sich schon aktuell im Bereich der Informations- und Kommunikationskultur auf Online-Plattformen und sozialen Netzwerken beobachten, auf denen sich zunehmend hermetisch abgeschlossene Kommunikationsräume herausbilden und verstärkt Radikalisierungen und Verrohungen auftreten (Echokammern).[144] Denkbar sind aber auch Ghettoisie-

---

[140] Von einer „algorithmic reality construction" sprechen *Just/Latzer*, Media, Culture & Society 39 (2017), 238, 246.

[141] Notwendig ist zudem eine entsprechende technische Expertise. Die Spaltungseffekte werden dann für technisch versierte Personen nicht gelten, entsprechend verlaufen dann auch gesellschaftliche Spaltungslinien zwischen technisch kompetenten und technisch nicht kompetenten Personen, vgl. *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 226, 233.

[142] *Miller*, J. Law Technol. Policy 2014, 41, 60; *Martini*, Blackbox Algorithmus, 2019, S. 50.

[143] Treffend für Informationsfilterdienste *Leerssen*, Algorithm Centrism in the DSA's Regulation of Recommender Systems, Verfassungsblog, 29.03.2022: „The black box metaphor does not go far enough, because with recommender systems not only the algorithm but even the basic outputs are obscure. […] The result, in short, is that we lose the collective ability to see what others are seeing".

[144] Zu sogenannten Echokammern siehe grundlegend *Sunstein*, Republic.com 2.0, 2007, S. 65; *Sunstein*, Echo chambers, 2001.Siehe beispielhaft zu diesen Effekten aus der umfassenden Literatur *Kersting/Mehl*, ZParl 49 (2018), 586, 588, 590–591 „homophile Diskussionszusammenhänge"; *Vīķe-Freiberga/Däubler-Gmelin/Hammersley u.a.*, A free and pluralistic media to sustain European democracy, High Level Group on Media Freedomand Pluralism, Januar 2013, S. 27 „insulated communities as isolated subsets". Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 100. Nach der aktuellen Studienlage sind diese Phänomene nicht zweifelsfrei belegt. In Bezug auf die Echokammern liefern durchgeführte Studien keine eindeutigen Ergebnisse, vgl. *Liesem*, AfP 51 (2020), 277, 279. Von einem Vorliegen derartiger Fragmentierungseffekte gehen aus *An/Quercia/Crowcroft*, in: Schwabe (Hrsg.), Proceedings of the 22nd international conference on World Wide Web companion, 2013, S. 51; *Bessi/Zollo/Del Vicario u.a.*, PloS one 11 (2016), e0159641; *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 188. Ablehnend aufgrund unzureichender empirischer Nachweise äußern sich dagegen *Cornils*, AfP 49 (2018), 377, 380 f.; *Ingold*, MMR 23

rungseffekte, wenn Personen nur die ihrer Vergleichsgruppe entsprechenden Wohnungsmiet- und -kaufanzeigen oder -angebote erhalten.[145] Auch eine Spaltung der Märkte erscheint möglich: Jede Personengruppen erhält dann auf segmentierten Märkten nur die ihr zugeordneten Produkte, die für Mitglieder einer anderen Gruppe nicht zugänglich sind.[146] Dabei handelt es sich nicht um völlig neuartige Phänomene, zudem nicht solche, die per se inakzeptabel oder unzumutbar sein müssen.[147] Es ist dann aber die umfassende Verbreitung der Systeme, vor allem aber die Intransparenz und Unabänderbarkeit der gruppenbezogenen Einteilung, die eine Intensivierung der tradierten Segmentierungseffekte befürchten lässt.[148]

3. Gefährdungen materieller Gerechtigkeit und Fairness

Im Hinblick auf materielle Gleichbehandlung und Fairness sind vor allem automatisierte Entscheidungen problematisch. Unzutreffende Zuordnungen im Profil können zu fehlerhaften Entscheidungen führen.[149] In atypischen, über-

---

(2020), 82, 83 f.; *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 5 f.; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 5–6, 10. Vgl. auch beispielhaft die unklaren Ergebnisse bei *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 179–186.

[145] Derartige Effekte können auch deshalb entstehen, da der Wohnort zum maßgeblichen Kriterium gemacht wird: Personen mit Wohnsitz in einem bestimmten Gebiet erhalten dann ähnliche Informations- oder Vertragsangebote oder auch eine Vertragszusage. Vgl. *Baur*, Algorithmic decision-making and social division, 21.2.2019, https://dorotheabaur.medium.com/algorithmic-decision-making-and-social-division-acknowledging-the-political-context-of-ai-e071e34524bb.

[146] Vgl. *Miller*, J. Law Technol. Policy 2014, 41, 94 f., der in den US-amerikanischen Märkten derartige Effekte bereits beobachtet.

[147] Dies stellen auch *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 121 fest.

[148] So auch, obschon hinsichtlich Diskriminierungen durch Algorithmen, *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 167: „Im Gegensatz zu vorurteilsbehafteten Entscheidungen einzelner Menschen besteht bei algorithmischen Systemen aber die Gefahr, dass der einem System inhärente Effekt über eine skalenmäßig große Anwendung des Systems eine Breitenwirkung entfaltet, die einzelne menschliche Entscheider nie erreichen könnten". Ebenso *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 121: „In a ubiquitous-computing environment where profiling is an important requirement, exclusion and discrimination of people increases to disturbing levels". Sie problematisieren dann auch die Intransparenz und fehlende Einwirkungsmöglichkeit, siehe *dies.*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 122 f. Siehe auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 237 f.

[149] Siehe umfassend zu den verschiedenen Fehlerquellen und der Inakzeptabilität fehlerhafter Ergebnisse *Zarsky*, Science, Technology, & Human Values 41 (2016), 118, 127 f.; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 36 f.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic

raschenden oder individualistischen Fallkonstellationen liefern autonome Systeme keine brauchbaren Ergebnisse.[150] Vor allem stellen sich Fragen prozeduraler Gerechtigkeit und Fairness automatisierter Entscheidungen,[151] insbesondere aufgrund der Intransparenz des Entscheidungsverfahrens und der Unverständlichkeit des Entscheidungsergebnisses[152] sowie der Determiniertheit der Entscheidungsfindung.[153]

III. Persönlichkeitskonstitutive Belastungen: Fremddarstellung und Fremdeinblicke

Problematisch im Hinblick auf die Persönlichkeitskonstitution sind unzutreffende und entindividualisierende Darstellungen im Profil (1.) sowie Einblicke in die Persönlichkeit ohne oder gegen den Willen der betroffenen Person (2.).

1. Unzutreffende und entindividualisierende Darstellungen

Die freiheitliche Persönlichkeitskonstitution kann beeinträchtigt sein, wenn der Einzelne es hinnehmen muss, dass er im Profil fehlerhaft dargestellt wird.[154] Problematisch ist es überdies, dass der Einzelne aufgrund des zweistufigen

---

regulation, 2019, S. 21, 31 f. Nicht nur fehlerhafte Profilzuordnungen aufgrund false positives oder negatives sind angesprochen, sondern auch aufgrund fehlenden oder unzureichenden Kontextbezugs unzutreffende Klassifizierungen, vgl. *Zarsky*, Science, Technology, & Human Values 41 (2016), 118, 127 f.; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 36 f.

[150] Eingehend *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016; *Ernst*, JZ 72 (2017), 1026, 1028; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 60 f.; ebenso *Leese*, Security Dialogue 45 (2014), 494, 506. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 97.

[151] *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 25 f. Siehe auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 437; *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 100–102, die allerdings allein auf staatliche Entscheidungen durch autonome Systeme fokussieren.

[152] Siehe nur *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 28 f.; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 61 f. Vgl. auch *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019, S. 7; vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 62, 236.

[153] Vgl. allgemein zu den Beeinträchtigungen der Verfahrensgerechtigkeit durch automatisierte Entscheidungen *Zarsky*, Science, Technology, & Human Values 41 (2016), 118, 128–130; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 87; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 437 f. Für die personalisierte Preisbildung *Miller*, J. Law Technol. Policy 2014, 41, 95.

[154] So auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 433 f.; *Hildebrandt/Gutwirth*, in: dies. (Hrsg.), Profiling the European Citizen, 2008, S. 365, 366; *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 112, 113.

Profilbildungsverfahren, in der die Vergleichbarkeit mit anderen maßgeblich ist, nicht mehr in seiner Individualität wahrgenommen wird.[155] Einige erkennen darin den Übergang in eine Welt, in der die Menschen nicht mehr als Subjekte, sondern als generalisierte, austauschbare Datenmatrizen wahrgenommen und behandelt werden.[156] Mit einer Wert- und Rechtsordnung, die die Individualität des Einzelnen in den Vordergrund stellt, ist dies nicht vereinbar.

2. *Informationsemergenzen ohne den Willen der betroffenen Person*

Das zweistufige Profilbildungsverfahren erlaubt Einblicke in die Persönlichkeit jenseits des Rohdatums und damit jenseits dessen, was die betroffene Person freigegeben hat. Problematisch sind dann Konstellationen, in denen Aspekte aufgedeckt werden, die die betroffene Person gar nicht teilen wollte, d.h. Inferenzen gegen ihren Willen gebildet werden,[157] sowie Konstellationen, in denen die betroffene Person aufgrund der Intransparenz des Profils weder im Vor- noch im Nachhinein wissen kann, welche Informationen über sie gewonnen werden, d.h. Inferenzen ohne ihren Willen gebildet werden.[158]

---

[155] *Ernst*, JZ 72 (2017), 1026, 1028, 1030; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 10; *Wischmeyer*, AöR 143 (2018), 1, 29; *Martini*, Blackbox Algorithmus, 2019, S. 30 f. Nach *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 93 führt dies zur Wahrnehmung der Menschen als „dividuals" (im Gegensatz zu individuals), da jede Person in ihre Eigenschaften aufgeteilt (divided) wird und den Menschen (similes) zugeordnet wird, mit denen sie aufgrund dieser Eigenschaft vergleichbar ist. Diese similes stehen im digitalen Raum dann als Stellvertreter für das eigene Selbst.

[156] *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 35: „How can we ensure that individuals are not viewed only as temporary digital data aggregates exploitable en masse on an industrial scale but as subjects of law in their own right". So auch *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 30; *Schermer*, CLSR 27 (2011), 45, 47. In diese Richtung auch *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 61; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 112.

[157] Vgl. *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 305 f.; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 441; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 116; *Manheim/Kaplan*, Yale J.L. & Tech. 21 (2019), 106, 119–129; *Martini*, DVBl 129 (2014), 1481, 1483; *Martini*, Blackbox Algorithmus, 2019, S. 91 f.; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 107, 109; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 36. Siehe hierzu auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 45.

[158] *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 318; *Hildebrandt/Gutwirth*, in: dies. (Hrsg.), Profiling the European Citizen, 2008, S. 365, 366; *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 37; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 61. Angedeutet auch bei der *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 45. Vgl. auch eingehend *Solove*, The digital person, 2004, S. 51–53.

IV. Autonomiegefährdungen: Verhaltenssteuerung, willensbildungsbezogene Phänomene und Abschreckungseffekte

Autonome Systeme können auf verschiedene Weise autonomiegefährdende Effekte freisetzen. Unterscheiden lassen sich dabei Phänomene der Beschränkung der äußeren Autonomie, die sich vor allem im Phänomen des „Code is law" realisieren (1.), sowie der Einwirkung auf die innere Autonomie, dann also die (unbewusste) Einflussnahme auf die Willens-, Meinungs- und Entscheidungsfindung (2.). Auf diese zweitgenannte Fallgruppe konzentriert sich die folgende Arbeit.

1. Beeinträchtigungen äußerer Freiheit: Verhaltenssteuerung und Code is law

In einer Welt, die algorithmisch bestimmt ist, geben autonome Systeme faktisch sämtliche Handlungsoptionen vor, denn was nicht programmiert ist, ist technisch nicht realisierbar.[159] Dies galt bisher für die Online-Welt, in einer Verschränkung analog-digitaler Realität kann dies aber auf die gesamte Lebenswirklichkeit des Einzelnen ausgreifen.[160] Algorithmen können dann genutzt werden, um menschliches Verhalten effektiv zu steuern.[161] Darin liegt dann eine Beeinträchtigung äußerer Verhaltensfreiheit: Der betroffenen Person wird von Dritten die Möglichkeit der Wahrnehmung einer gewünschten Ver-

---

[159] *Hoffmann-Riem*, AöR 142 (2016), 1, S. 8–11, 34–36; *Boehme-Neßler*, NJW 70 (2017), 3031, 3033. Siehe zur Techniksteuerung allgemein *Spiekermann/Pallas*, Poiesis & Praxis 4 (2006), 6, 10. Für den Bereich der Informationsfilterung *Hill*, in: Hill/Schliesky (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, 2015, S. 267, 279; *Just/Latzer*, Media, Culture & Society 39 (2017), 238, S. 239–242, 246–247. Erscheint ein Artikel in einem Suchprogramm oder auf einer Webseite nicht, besteht keine Option zur Kommentierung eines Beitrages, ist ein bestimmtes Produkt, etwa Betäubungsmittel, nicht im Online-Handel verfügbar, wird ein Kredit nicht zugeteilt, sind entsprechende Informations-, Kommunikations-, Erwerbs- oder Vertragsabschlusswünsche faktisch nicht realisierbar. Siehe zu weiteren Beispielen *Hoffmann-Riem*, AöR 142 (2016), 1, 11–19; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 5.

[160] Vgl. *Boehme-Neßler*, ZöR 64 (2009), 145, 149 f. Anschaulich spricht *Hoffmann-Riem*, AöR 142 (2016), 1, 5 von einer „omnipräsente[n] Basisinfrastruktur". Hier ist etwa denkbar, dass ein autonomes Fahrzeug sich nicht starten lässt, wenn eine Person nicht angeschnallt ist; ein Smarter Kühlschrank das Bestellen von Junkfood nicht zulässt.

[161] Es ist der Umstand des Steuerungsvorsatzes (intention), der aus der bloßen Technikgestaltung eine Techniksteuerung macht, vgl. *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 5. Steuerungsakteure sind die Entwickler, Hersteller oder Betreiber oder andere menschliche Akteure, die den Inhalt der Algorithmen vorgeben. Auch Algorithmen sind damit soziale, nicht rein technische Konstrukte. Siehe hierzu eingehend *Buchholtz*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 175, 183; *Hoffmann-Riem*, AöR 142 (2016), 1, 28–31.

haltensweise genommen.[162] Steuerungsakteur ist damit, wer den Inhalt der Algorithmen vorgibt.[163] Sind dies private Akteure, besteht die Befürchtung, dass diese eigene Wertvorstellungen definieren und wirkungsvoll durchsetzen könnten und sich so in Konkurrenz zum gesellschaftlich-konsentierten, vor allem rechtlichen Wertesystem stellen und dieses wirkungsvoll verdrängen.[164] Dies ist unter dem Stichwort „code is law"[165] oder auch „Algocracy"[166] bekannt

---

[162] *Hoffmann-Riem*, AöR 142 (2016), 1, 35; *Rouvroy*, Studies in Ethics, Law, and Technology 2 (2008), 1, 17; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10. Plakativ *Spiekermann/Pallas*, Poiesis & Praxis 4 (2006), 6, 10: „Technology Paternalism is not matter of obedience as is the case with human interfaces. Instead ist is a matter of total compliance. The risk exists that humans may have to subdue to the machine". Teilweise wird dies auch als Technologiepaternalismus bezeichnet. Hervorgehoben wird dadurch, dass die autonomen Systeme zu besseren, sichereren oder gesünderen Entscheidungen für den Einzelnen führen können – auch wenn dies die betroffene Person gar nicht möchte oder für sich anders definiert, was gut, sicher oder gesund ist. Siehe hierzu *Spiekermann/Pallas*, Poiesis & Praxis 4 (2006), 6–18; *Rouvroy*, Studies in Ethics, Law, and Technology 2 (2008), 1, 17; in diese Richtung auch *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 63 f.

[163] *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 5: „Critical to all these systems is the ned for some kind of system ‚director' (or ‚regulator') to determine the overarching goal of the regulatory system".

[164] Im Privatverhältnis besteht dagegen die Gefahr, dass die Programmierung an wirtschaftlichen Zielvorstellungen der Unternehmen ausgerichtet ist und sich das algorithmische Normsystem in Konkurrenz zum gesellschaftlich konsentierten setzt. *Boehme-Neßler*, NJW 70 (2017), 3031, 3035; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 238; *Just/Latzer*, Media, Culture & Society 39 (2017), 238, 249 f.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 9 f. Vgl. auch eingehend die Darstellungen zu den unterschiedlichen Zielen, Inhalten, Entstehung, Formen und Durchsetzung staatlichen Rechts und privater, code-basierter Normierung *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 143–158; *Hoffmann-Riem*, AöR 142 (2016), 1, 25–36.

[165] Grundlegend *Lessig*, Code, [2]2006, der sich dabei auf die Idee der „Lex Informatica" von Joel Reidenberg stützt, siehe *Reidenberg*, Texas Law Review 76 (1998), 553–593 Ausführlich *Hoffmann-Riem*, AöR 142 (2016), 1, 8; *Hill*, in: Hill/Schliesky (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, 2015, S. 267; *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 169–172; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 8–13. Siehe auch *Boehme-Neßler*, NJW 70 (2017), 3031, 3033; *Wischmeyer*, AöR 143 (2018), 1, 20–23. Dies ist kein neues Phänomen des algorithmisierten Zeitalters: Ganz allgemein kommt der Technik ein steuernder Charakter zu, wo sie Handlungen einerseits ermöglicht, andererseits verhindert. Dies wird auch als Technosteuerung, Technoregulation oder normative Technik bezeichnet, so auch *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 11; *Hoffmann-Riem*, AöR 142 (2016), 1, 11. Siehe allgemein zur Technosteuerung bzw. Technokratie die Beiträge in *Brownsword/Scotford/Yeung* (Hrsg.), The Oxford handbook of law, regulation, and technology, 2017, S. 705 ff.; *Brownsword/Yeung* (Hrsg.), Regulating technologies, 2008, S. 49 ff. sowie *Leenes*, Legisprudence 5 (2011), 143–169.

[166] Grundlegend *Aneesh*, Sociological Theory 27 (2009), 347–370. Denselben Begriff nutzt *Martini*, Blackbox Algorithmus, 2019, S. 9.

geworden.[167] Problematisch ist dabei, dies unterscheidet autonome Systeme von anderen technischen Anwendungen, dass diese in sensible, letztlich sogar in sämtliche Lebensbereiche vordringen und so eine wirkmächtige Steuerungsarchitektur errichten können, die sich neben die tradierten Steuerungsarchitekturen Netzwerk, Hierarchie, Verhandlung und Markt stellt.[168] Soweit sich autonome Systeme von der menschlichen Vorgabe entfernen, könnten sie sogar eigene Steuerungsinhalte entwickeln,[169] die aufgrund der fehlenden Nachvollziehbarkeit menschlich nicht mehr kontrolliert werden könnten. Dann, so die Befürchtung, entstünde eine originär maschinelle Techniksteuerungsinfrastruktur.[170]

2. Beeinträchtigungen innerer Freiheit: verhaltensökonomische Phänomene, präemptive Effekte, Manipulation und Abschreckungswirkung

Die Einwirkungen autonomer Systeme auf die innere Autonomie des Menschen, d.h. seine Willens- und Entscheidungsfreiheit, stellen sich als äußerst vielfältig und diffus dar. Die Studienlage lässt hier vielfach (noch) keine eindeutigen Erkenntnisse zu. Herausgegriffen werden vier Konstellationen, in denen sich Einwirkungen auf die Willens- und Entscheidungsfreiheit schon aktuell beobachten lassen: die Ausnutzung verhaltensökonomischer Effekte (a)), die präemptiv-selektive Realitätsgestaltung (b)), manipulative Übergriffe (c)) sowie Abschreckungs- und Hemmeffekte (d)). Dass diese Einflussnahmen tatsächlich als Autonomiegefährdungen zu qualifizieren sind, ergibt sich aus der Eigenart und Neuartigkeit der autonomen Systeme (e)).

---

[167] Auch andere Bezeichnungen sind geläufig, etwa „Verhaltenssteuerung durch Algorithmen", so *Hoffmann-Riem*, AöR 142 (2016), 1–42, „algorithmic regulation", so *Yeung/Lodge* (Hrsg.), Algorithmic regulation, 2019, oder „governance by algorithms", so *Just/Latzer*, Media, Culture & Society 39 (2017), 238–258; *Ebers/Gamito* (Hrsg.), Algorithmic Governance and Governance of Algorithms, 2021. Siehe zu diesem Phänomen auch *Lenk*, Verwaltung und Management 22 (2016), 225, 231 f. Die Herausforderungen einer derartigen, in Konkurrenz zum staatlichen Recht tretenden Normordnung sind vielfältig. Siehe aus der umfassenden Literatur beispielhaft *Boehme-Neßler*, NJW 70 (2017), 3031–3037; *Hoffmann-Riem*, AöR 142 (2016), 1, 25–36; *Yeung/Lodge* (Hrsg.), Algorithmic regulation, 2019. Die These, dass mittels Algorithmen Verhalten gesteuert werden kann, wird interdisziplinär kontrovers diskutiert, eine Darstellung der Gegenthesen mit zahlreichen Nachweisen aus der Literatur bietet *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 5 f.

[168] *Hoffmann-Riem*, AöR 142 (2016), 1, 10.

[169] *Just/Latzer*, Media, Culture & Society 39 (2017), 238, 252.

[170] Definiert etwa ein künstliches neuronales Netz, wer einen Kredit erhält, legt es gutes, d.h. kreditwürdiges, und schlechtes, d.h. kreditunwürdiges Verhalten fest und nimmt damit auch eine normative Wertung vor. Siehe hierzu etwa *dies.*, Media, Culture & Society 39 (2017), 238, 252 f., die diese Gefahr allerdings noch nicht realisiert sehen, da die autonomen Systeme weiterhin vom Menschen steuerbar sind: „[R]eality construction, both via […] algorithmic selection, is a co-production of humans and technology".

a) Verhaltensökonomische Phänomene bei Empfehlungssystemen

Vor allem bei Empfehlungs- und Rankingsystemen in Informationsfilterdiensten lässt sich beobachten, dass NutzerInnen typischerweise die automatisierten Vorschläge übernehmen, statt eigeninitiativ nach alternativen Informationsangeboten zu suchen.[171] Ähnliche Effekte lassen sich bei Entscheidungsassistenzsystemen beobachten, die für einen menschlichen Entscheider einen Entscheidungsvorschlag erarbeiten. Dort wird dieses Phänomen als „Automation Bias" bezeichnet.[172] Verschiedene Ursachen werden hierfür diskutiert, vor allem verhaltensökonomisch sind diese Phänomene umfassend aufgearbeitet worden. Nach dortigen Erkenntnissen ist der Mensch in komplexen Entscheidungssituationen geneigt, sich von irrationalen Anreizen leiten zu lassen, sich dann also auf diffuse Vertrauenszuschreibungen, Intuitionen oder Emotionen zu stützen.[173] Der algorithmische Vorschlag ist ein solcher Anreiz, dem eine hohe Objektivität, Akkuratesse und Relevanz zugeschrieben wird.[174] Wenn das au-

---

[171] Siehe zu verschiedenen Studien im Bereich der Informationsfilterung, wonach NutzerInnen die Vorschläge in der Tendenz übernehmen, sie nicht kritisch überprüfen und auch keine Suche nach Alternativen betreiben *Magin/Steiner/Stark*, Media Perspektiven 2019, 421–429; *Stark/Magin/Jürgens*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 20, 54–49. Siehe allgemein zu diesen Effekten, vor allem auch bei automatisierten Entscheidungs(assistenz)systemen *Martini*, DVBl 129 (2014), 1481, 1488: „[Der Algorithmus] verleitet zu einem blinden Glauben in die Analyserichtigkeit und -redlichkeit". Vgl. zu diesem Phänomen auch *Hoffmann-Riem*, AöR 142 (2016), 1, 11–14; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 230; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 105 f.

[172] *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 228; *Goddard/Roudsari/Wyatt*, Journal of the American Medical Informatics Association 19 (2012), 121–127.

[173] So wird etwa dem statistisch-mathematischen Ansatz der Künstlichen Intelligenz ein höheres Vertrauen gegenüber gebracht als dem menschlichen Entscheidungs- oder Aktionsträger, wie verschiedene Studien nahelegen, vgl. das bei *Martini*, Blackbox Algorithmus, 2019, S. 48 geschilderte Experiment am Georgia Institute of Technology: In der Versuchskonstellation führte ein Roboter die Versuchspersonen durch einen Versuchsraum. Der Roboter war dabei so programmiert, dass er zahlreiche Fehler, zB Irrwege, machte. Nach einer ersten Interaktionsphase, in denen den Versuchspersonen die Fehleranfälligkeit des Roboters bewusstgemacht wurde, folgte das eigentliche Experiment. Im Versuchsraum wurde ein Feuer simuliert; die Versuchspersonen sollten sich möglichst schnell aus dem Raum retten. Hierzu konnten die Versuchspersonen entweder der angebrachten Notausgangbeschilderung folgen oder sich der Führung durch den (bekanntermaßen fehleranfälligen) Roboter überlassen. Der überwiegende Anteil der Versuchspersonen vertraute dem Roboter. Vgl. *Robinette/Li/Allen u.a.*, 2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI) 2016, 101–108 Vgl. auch die Studie bei *Borenstein/Wagner/Howard*, IEEE Robot. Automat. Mag. 25 (2018), 46–54.

[174] Siehe ausführlich *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 235–237. Mit einigen Beispielen *Ebers*, MMR 21 (2018), 423, 424. Studien haben dies vielfach bestätigt, siehe zu personalisierter Werbung auf sozialen Netzwerken etwa *Matz/Konsinksi/Nave u.a.*, Procee-

tonome Systeme ohnehin gute oder sogar bessere Ergebnisse erzielt als der Mensch, erscheint es nicht rational, den Aufwand eigener Suche oder kritischer Prüfung des Vorschlags zu erbringen.[175] Überdies können Trägheitseffekte wirken.[176] Der Mensch ist generell, vor allem aber in herausfordernden Entscheidungssituationen, geneigt, im Status quo zu verharren. Die Entscheidungsoption ist dann die attraktivste, die mit der geringsten Zustandsänderung verbunden ist – dies ist die Übernahme des Vorschlags. Die Abwahl und Abänderung des algorithmischen Vorschlags, ja bereits die Suche nach Alternativen ginge mit einer Zustandsänderung einher.

Personalisierte Dienste wie Informationsfilterdienste oder personalisierte Werbemaßnahmen bedienen zudem Selbstbestärkungseffekte. Nach verhaltensökonomischen Erkenntnissen übt das Bekannte für den Menschen einen hohen Anreiz aus, während Unbekanntes und Widersprechendes als irritierend und unattraktiv wahrgenommen werden. Informations-, Erwerbs- und Handlungsangebote, die den bestehenden Interessen, Vorlieben und Weltkonzeptionen entsprechen, erreichen den Einzelnen damit besonders gut und besser als hiervon abweichende Angebote.[177] Die Anreizwirkung autonomer Systeme ist

---

dings of the National Academy of Sciences of the United States of America 114 (2017), 12714–12719.

[175] In diese Richtung *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 60: „If, however, the individual chooses an alternative option, there is a risk that this will result in higher costs or will require a larger effort. These alternatives therefore tend not to be pursued further". Kausalitätsbeziehungen kehren sich gewissermaßen um: Die NutzerInnen sind mit den Angeboten zufrieden, da sie davon ausgehen, diese böten die besten Ergebnisse. Vgl. unter Heranziehung empirischer Studien *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), 298 f.

[176] *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 107 f. Untersucht worden ist dieses Phänomen vor allem im Bereich der Informationsfilterung. Vgl. etwa die Studien bei *Magin/Steiner/Stark*, Media Perspektiven 2019, 421–429; *Stark/Magin/Jürgens*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 20, 54–49. Siehe zu diesen Effekten auch *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, 266–267, 294; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 78, sowie bereits *Introna/Nissenbaum*, The Information Society 16 (2000), 169, 174, jeweils mit Zitierung weiterer Studien. Eingehend zu den Trägheitseffekten menschlicher Entscheidungsfindung *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 263–267, 370–373; *Samuelson/Zeckhauser*, Journal of Risk and Uncertainty 1 (1988), 7–59.

[177] In der internationalen Forschung wird dies als „homophily" bezeichnet. Vgl. ausführlich etwa *Halberstam/Knight*, J. Public Econ. 143 (2016), 73–88; *McPherson/Smith-Lovin/Cook*, Annual Review of Sociology 27 (2001), 415–444; *Retica*, Homophily, New York Times Magazine 10.12.2006, https://www.nytimes.com/2006/12/10/magazine/10Section2a.t-4.html. Diese Theorie wurde bereits in den 1950er Jahren entwickelt, es handelt sich um nicht um ein völlig neues Phänomen. Siehe zu diesen Effekten durch personalisierte Waren-

daher umso stärker, je präziser der Vorschlag auf individuelle Bedürfnisse angepasst ist.[178]

b) Selektiv-präemptive Realitätsgestaltung und -wahrnehmung

Wenn der Einzelne überwiegend den Vorschlag von Empfehlungs- und Rankingsystemen übernimmt, im Übrigen Selektionsdienste über den faktischen Zugang des Einzelnen zu Informations- und Kommunikationsangeboten entscheiden, bestimmen autonome Systeme am Ende, welche Informationen und Meinungsbeiträge eine Person erreichen. Verlagern sich Information und Kommunikation zunehmend in den digitalen Raum, bestimmten autonome Systeme so wesentlich, wie eine Person die Welt wahrnimmt und wie sie sich selbst wahrnehmen muss.[179] Dies kann manipulativ genutzt werden, hierzu sogleich. Bei einem ordnungsgemäß funktionierenden autonomen System ist allein die Personalisierung maßgebliches Filterkriterium. Auch dies kann aber problematisch sein. Denn in dieser Weltwahrnehmung werden bestehende persönliche Ein- und Vorstellungen fortlaufend bedient und verstärkt, während neuartige und kreative Impulse fehlen.[180] Dies kann Selbstbestärkungs- und Radikalisie-

angebote *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 236 f. Für die Informationsfilterung *Hoffmann-Riem*, AöR 142 (2016), 1, 13 f.

[178] *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 107 f. *Yeung*, iCS 20 (2017), 118–136; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 35 spricht daher von einem „Hypernudging", das bei besonders tiefgehender und präziser Personalisierung erfolgt.

[179] *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 23, 31–33, 33–34 sprechen von der gezielten Gestaltung der „Entscheidungsarchitektur" sowie von „Mediatisierung" der NutzerInnen, wo die Online-Plattformen die Brillen („eye glasses") bilden, mit denen diese auf die digitale Welt blicken. Ebenso *Wischmeyer*, AöR 143 (2018), 1, 21: „Im Internet […] sorgen intelligente Algorithmen dafür, dass jeder Nutzer eine ganz eigene Wahrnehmungssphäre und einen eigenen differenzierten Handlungsraum zugewiesen bekommt". Für Marktbedingungen *Mik*, Law Innov. Technol. 8 (2016), 1, 19 „The extreme effect of personalisation is that each online consumer sees a customised view of the marketplace". *Just /Latzer*, Media, Culture & Society 39 (2017), 238–258 bezeichnen dies als „Realitätsgestaltung". Plakativ auch *Rouvroy*, Studies in Ethics, Law, and Technology 2 (2008), 1, 14: „What is crucial here is that these systems construct or produce the meaning of [...] events and, on that basis, frame the user's environment in ways that in turn impact on his self-perception, choices, preferences and behaviours, interfering, potentially at the deepest level, with the effective exercise by individuals of their capacity for self-determination". Vgl. zu diesen Wirkeffekten selektiver Realitätswahrnehmung und -gestaltung auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 234–236; *Lobe*, Lieber Computer, sag mir, wen ich heiraten soll, FAZ 14.09.2016, https://www.faz.net/aktuell/feuilleton/debatten/die-macht-der-datenkonzerne-und-algorithmen-14433947.html.; *Martini*, Blackbox Algorithmus, 2019, S. 100–102.

[180] *Grafanaki*, Rich J. L. Techn. 24, 1, 21 f.; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 306 f.; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 9; *Dornis*, ZfPW 8 (2022), 310, 315. Vgl. auch *Rouvroy*,

rungseffekte freisetzen. Hatespeech, Fakenews oder Desinformation, wie sie seit einiger Zeit in sozialen Netzwerken zu beobachten sind, werden gerade auch auf die personalisierte Filterung zurückgeführt.[181] Dort ist für das Phänomen personalisierter Perspektiveneinengung der Begriff der Filterblase (Filter Bubble) geprägt worden.[182]

In einer Welt autonomer Systeme könnten sich diese Mechanismen auf die gesamte Werte-, Präferenz- und Persönlichkeitsbildung erstrecken.[183]

Ein Ausbruch aus dieser selektiven Wahrnehmung ist zwar möglich – die betroffene Person kann Alternativen im digitalen oder analogen Bereich fin-

---

Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 37; *Nürnberger/Bugiel*, DuD 40 (2016), 503, 504. Siehe auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 235.

[181] Eingehend hierzu *Schimmele*, Staatliche Verantwortung für diskursive Integrität in öffentlichen Räumen, 2019, S. 34 f.; *Nolte*, ZUM 21 (2017), 552–564; *Oswald*, in: Grabenwarter/Holoubek/Leitl-Staudinger (Hrsg.), Regulierung von Kommunikationsplattformen, 2022, S. 67 Vgl. auch *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 17. Diese Erscheinungen sind Gegenstand interdisziplinärer Forschung, die Ursachen sind noch nicht ganz eindeutig geklärt, vgl. eingehend *Ingold*, MMR 23 (2020), 82, 83 f. Dabei ist Konsens, dass zumindest auch die Personalisierung der Filterung ursächlich ist. Vgl. nur *Martini*, Blackbox Algorithmus, 2019, S. 100 f.; *Dörr/Natt*, ZUM 58 (2014), 829, 837; *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 4; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 110; *Liesem*, AfP 51 (2020), 277, 278. Siehe auch *Menczer Filippo/Hills*, Die digitale Manipulation, Spektrum 02.04.2021, https://www.spektrum.de/news/wie-algorithmen-uns-manipulieren/1849438.

[182] Der Einzelne nimmt die Welt in dieser Blase wahr, in der bestehende Ansichten immerfort bestärkt und widersprechende, kreative Impulse unterdrückt werden. Grundlegend *Pariser*, The filter bubble, 2011. Diese Konzeption wird vielfach aufgegriffen und befürwortet; aus der Fülle der Literatur siehe etwa *Brkan*, SSRN Journal 9.4.2019, 1, 3; *Carson*, Journal of Science Policy and Governance 7 (2015), 1, 7–9; *Liesem*, AfP 51 (2020), 277, 278; *Vīķe-Freiberga/Däubler-Gmelin/Hammersley u.a.*, A free and pluralistic media to sustain European democracy, High Level Group on Media Freedomand Pluralism, Januar 2013, S. 27 sowie *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98; *Moeller/Helberger*, Beyond the filter bubble: concepts, myths, evidence and issues for future debates, University of Amsterdam, 2018; *Müller-Terpitz*, ZUM 64 (2020), 365–374 Die Existenz und Wirkkraft derartiger „Filterblasen" ist allerdings äußerst umstritten, durchgeführte Studien liefern keine eindeutigen Ergebnisse. Kritisch etwa *Cornils*, AfP 49 (2018), 377, 380 f.; *Ingold*, MMR 23 (2020), 82, 83 f.; *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 5 f.; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 5–6, 10; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 126–128.

[183] *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 235–237. Wenn eine Person etwa allein Werbeangebote zu sportlichen Aktivitäten erhält, wird sie womöglich nie erfahren, dass auch die Musik oder die Kunst Möglichkeiten der Persönlichkeitsentfaltung bieten. Siehe zu einem ähnlichen Beispiel *dies.*, ZfPW 5 (2019), 220, 236.

den, den Vorschlag eines Empfehlungssystems muss sie nicht annehmen. Dies setzt aber Reflexion und Eigeninitiative voraus. Die beschriebenen verhaltensökonomische Effekte erschweren dies.[184] Problematisch ist zudem, dass die Steuerungen durch autonome Systeme eigeninitiativ-prädiktiv erfolgen. Noch bevor die betroffene Person entscheiden kann, ob sie eine bestimmte Anwendung nutzen, etwa einen Informationsbeitrag wahrnehmen möchte, ist ihr diese bereits automatisiert angeboten worden.[185] Die offene (und herausfordernde) Frage nach Vorlieben, Wünschen oder Handlungsoptionen aus einer Vielfalt an Möglichkeiten wandelt sich zu einer geschlossenen nach der Annahme oder Ablehnung des Outputs des autonomen Systems.[186] Dies ist etwas grundlegend anderes.[187] Hinzu kommt, dass aufgrund der instantanen Anpassung des autonomen Systems an Vorlieben und Wünschen in Echtzeit die Zeitspanne für Selbstreflexion und kritische Prüfung der algorithmischen Perspektivenverengung verkürzt und damit erschwert wird.[188] Die Prädiktion wird am Ende zur Präemption.[189]

---

[184] *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 60 f.

[185] *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 34. Ähnlich *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 235, die von einem „passiven Zugang zur Realität" sprechen.

[186] Siehe auch *Rouvroy*, Studies in Ethics, Law, and Technology 2 (2008), 1, 16: „When individual desires, preferences, and choices are always already framed by the technology, when, in other words, no elsewhere exists from where individuals could contest what is proposed or imposed on them through the AmI technologies, how can individual autonomy be preserved?".

[187] Siehe nur *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 235: „Der natürliche Prozess des flexiblen Umgangs mit bestehenden Präferenzen und ihrer kreativen Weiterentwicklung steht still". Vgl. auch *Mik*, Law Innov. Technol. 8 (2016), 1, 22: „It is one thing to decide not to explore all possibilities, it is yet another not to know that many possibilities exist". Ähnlich *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1004: „The difference […] lies in the consumer's inability to adopt a critical frame of mind prior to entering the marketplace".

[188] Vgl. *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 60, 69, 91–92. Ebenso *Grafanaki*, Rich J. L. Techn. 24, 1, 30; ähnlich *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 37; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 58. Beobachtet wird dies vor allem im Bereich personalisierter Werbung, dann für die Entwicklung von Konsumwünschen.

[189] Vgl. *Hildebrandt*, Smart technologies and the end(s) of law, 2016, S. 57– 61, 68– 69 Ebenso *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 34.

c) Manipulative Übergriffe

Die beschriebenen verhaltensökonomischen sowie präemptiven Effekte können durch Dritte gezielt zur Willensbeeinflussung eingesetzt werden.[190] Die Kenntnis von den Vorlieben der NutzerInnen erlaubt Dritten, Produkte oder Dienstleistungen, aber auch (politische) Überzeugungen auf solche Weise zu präsentieren, dass sie für die einzelnen NutzerInnen besonders attraktiv erscheinen.[191] Dies betrifft vor allem den Bereich der Werbung.[192]

---

[190] Vgl. *Sartor*, New aspects and challenges in consumer protection, Europäisches Parlament, April 2020, S. 14; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 58; *Yeung*, iCS 20 (2017), 118, 123 f. Siehe auch *Ebers*, MMR 21 (2018), 423, 424, spezifisch für Informationsfilterdienste *Dörr/Natt*, ZUM 58 (2014), 829, 840; *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, 269. Ausführlich *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 234–240. Es geht darum, „die Konsumenten systematisch auszubeuten, indem (Unternehmen) diese in strategisch errichtete Rationalitätsfallen lenken", so *dies.*, ZfPW 5 (2019), 220, 231. Ausführlich auch *Mik*, Law Innov. Technol. 8 (2016), 1, 16–18; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 91. Siehe zum Einsatz der Verfahren während des US-Wahlkampfs 2016 ausführlich *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 9–12. Derartige Verfahren werden auch als „persuasion profiling" bezeichnet, so eingehend vgl. *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, S. 1033, 1047– 1049. Ganz generell wird bezweifelt, ob die automatisierte Personalisierung überhaupt je ohne Drittinteressen stattfinden kann, da die autonomen Systeme von Unternehmen bereitgestellt werden, die stets eigene wirtschaftliche Ziele verfolgen, und wenn diese nur darin liegen, die betroffene Person im eigenen Dienst „festzuhalten", so *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, S. 34– 35, 127– 128; ähnlich *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 230–232.

[191] *Calo*, Geo. Wash. L. Rev. 82 (2014), 995 entwickelt hieraus, basierend auf den Arbeiten von *Hanson/Kysar*, Harv. L. Rev. 112 (1999), 1420–1572, eine Theorie der digitalen Marktmanipulation. Ausdrücklich *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1010: „By identifying the factors related to these deviations (from the rational model by the consumers), the firm can watch for those factors to align again and target the consumer when she is vulnerable". So kann etwa durch selektive Vorschläge von Produkten oder durch deren priorisierte Platzierung in Suchanfragen auf die Wahrnehmung und Bewertung des Produkts durch die Konsumenten eingewirkt werden, vgl., *Mik*, Law Innov. Technol. 8 (2016), 1, 27; *Sartor*, New aspects and challenges in consumer protection, Europäisches Parlament, April 2020, S. 14; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 230–233.

[192] Vgl. *Bozdag*, Ethics Inf. Technol 15 (2013), 209, 220; *Ebers*, MMR 21 (2018), 423–428 Ausführlich zum Einsatz personalisierter Marketingstrategien in sozialen Netzwerken *Krönke*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 145, 147–152. Eine empirische Studie zur Wirkmacht personalisierter Werbemaßnahmen bieten *Matz/Konsinksi/Nave u.a.*, Proceedings of the National Academy of Sciences of the United States of America 114 (2017), 12714–12719 Die Ausnutzung von Verhaltensirrationalitäten kann eine Methode des Nudgings sein, es gibt also Überschneidungen zwischen Profilbildung und Nudging, so auch *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 58. Es wird auch von „Big Nudging" (eine Kombination von Big Data und Nudging) oder „Hybernudging" gesprochen, vgl. etwa *Helbing*, „Big

Die Profilbildung kann überdies manipulationssensible Erkenntnisse aufdecken, die es Unternehmen erlaubt, wirkungsstarke Entscheidungsirrationalitäten auszunutzen.[193] Es geht um Kenntnisse über emotionale Schwächen, psychisch belastende Situationen, physische Anfälligkeiten oder lebenssituationsbedingte, situative Absenkungen von Resilienzmechanismen. Unternehmen könnten diese Kenntnisse nutzen, um wirkungsstarke Werbung zu schalten.[194]

d) Hemm- und Einschüchterungseffekte

Dass die intransparente und unkontrollierbare Erfassung von Persönlichkeitsmerkmalen ebenso wie eine intransparente und unkontrollierbare Entscheidungsarchitektur allgemeine Hemm- und punktuelle Einschüchterungseffekte freisetzen können, ist, wenngleich teilweise umstritten,[195] zumindest im staatlichen Kontext überwiegend anerkannt.[196] Zunehmend wird vorgebracht, dass

---

Nudging" – zur Problemlösung wenig geeignet, Spektrum der Wissenschaft 12.11.2015, https://www.spektrum.de/kolumne/big-nudging-zur-problemloesung-wenig-geeignet/1375930.; *Yeung*, iCS 20 (2017), 118–136 Ähnlich *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1001 „market manipulation is, essentially, nudging for profit". *Büchi/Fosch-Villaronga/Lutz u.a.*, The chilling effects of algorithmic profiling, März 2020, S. 12 bezeichnen dies als „automated manipulation".

[193] Vgl. *Mik*, Law Innov. Technol. 8 (2016), 1, 14, 22–24 („idiosyncratic vulnerabilities"). Siehe auch *Sartor*, New aspects and challenges in consumer protection, Europäisches Parlament, April 2020, S. 14 f.; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 232. Weitere Beispiele, die teilweise bereits zum Einsatz kommen, bei *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 996; *Ebers*, MMR 21 (2018), 423, 424; o.A., Verbraucherrecht 2.0, Dezember 2016, S. 59. Anders als bei der Ausnutzung von verhaltensökonomisch bedingten Selbstbestärkungseffekten reizen diese Einwirkungen Konsumwünsche an, die nicht notwendig den Interessen und Vorlieben der betroffenen Person entsprechen. Mit verschiedenen Anwendungsbeispielen *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 234–238.

[194] Vgl. für personalisierte Werbemaßnahmen *Danckert/Mayer*, MMR 13 (2010), 219; *Dörr/Natt*, ZUM 58 (2014), 829, 838; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 72 f.; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 92 f.; *Paal*, ZRP 48 (2015), 34, 35; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 9. Siehe auch *Kreile/Thalhofer*, ZUM 58 (2014), 629; vgl auch bereits *Introna/Nissenbaum*, The Information Society 16 (2000), 169, 174 f.

[195] Ablehnend etwa, insbesondere aufgrund fehlender empirischer Nachweise, – wenngleich hinsichtlich staatlicher Datenverarbeitung – *Büchi/Fosch-Villaronga/Lutz u.a.*, The chilling effects of algorithmic profiling, März 2020, S. 11; *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 283–286; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 45–54. Für die Datenverarbeitung durch Private dürften diese Erwägungen dann erst recht gelten. Siehe hierzu etwa *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 59 f.

[196] Siehe eingehend die Untersuchung zur Anerkennung von Abschreckungseffekten in der deutschen und amerikanischen Verfassungsrechtsprechung *Staben*, Der Abschreckungseffekt auf die Grundrechtsausübung, 2017. Siehe darin die Studien zu Abschreckungseffek-

diese auch im Verhältnis zwischen Privaten wirken könnten, zumindest dann, wenn autonome Systeme umfassend Verbreitung finden und damit allgemein über die Verteilung von Gütern auf dem Markt entscheiden. Problematisiert wird dabei insbesondere, wenn autonome Systeme über den Zugang zu essentiellen Gütern der Daseinsvorsorge oder zu Gütern von hoher individueller Bedeutung.[197] Schon die Intransparenz, Unausweichlichkeit und Unabänderbarkeit der Entscheidungen bzw. Steuerungen autonomer Systeme per se könnte dann, so wird befürchtet, ein allgemeines freiheitsfeindliches Gefühl der Hilflosigkeit und des Ausgeliefertseins auslösen.[198] Wenn eine konkrete Entscheidung unverständlich, unabänderbar und unanfechtbar ist, begründet dies für die betroffene Person eine kafkaeske[199] Situation der Ohnmacht.[200] Das Bewusstsein von der permanenten, aber intransparent bleibenden Aufzeichnung, Analyse und Bewertung einer jeden Verhaltensweise kann zudem Einschüchterungseffekte freisetzen.[201] Auch punktuelle Freiheitsbeeinträchtigungen sind

---

ten im Online-Bereich *ders.*, Der Abschreckungseffekt auf die Grundrechtsausübung, 2017, S. 158–160, 165. Siehe für den europäischen Raum *Pech*, The Concept of Chilling Effect, Open Society European Policy Institute, 2021.

[197] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 265 f. Ähnliche Überlegungen bei *Martini*, Blackbox Algorithmus, 2019, S. 196, der diese Überlegungen im Rahmen der Ausweitung von Transparenzpflichten hinsichtlich autonomer Systeme anstellt.

[198] *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 61, 68; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 87; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 265 f. Eingehend *Solove*, The digital person, 2004, S. 47–51.

[199] Zu dieser Metapher ausführlich *Solove*, The digital person, 2004, S. 27–55. Siehe zu diesem Bild im Rahmen des Datenschutzrechts Kapitel 4 A II. 2. a).

[200] So etwa *Ernst*, JZ 72 (2017), 1026, 1030. Dies wird vielfach als „Computer says no"-Dystopie beschrieben, so *Martini*, Blackbox Algorithmus, 2019, S. 170. Das Bild entstammt der Comedy-Serie „Little Britain", in der ein Mitarbeiter verschiedene Anfragen einer Person in einen PC eingibt. Die Ausgabe des PCs ist dabei überwiegend negativ, auch bei Umständen, die klar für eine positive Entscheidung sprächen. Der Bankmitarbeiter lehnt dann die Anfrage ab und teilt als Begründung allein mit: „Computer says no".

[201] *Ernst*, JZ 72 (2017), 1026, 1035; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 307 f.; *Martini*, Blackbox Algorithmus, 2019, S. 50; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 59; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 109; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 36. So auch *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 105–106, 109: „Zu erwarten ist infolgedessen tendenziell eine Entwicklung hin zu mehr Unauffälligkeit und Angepasstheit der Nutzer im Netz". *Wachter/Mittelstadt*, CBLR 2019, 494, 512 befürchten ein „self-censorship". Ähnlich *Härting*, CR 4 (2014), 528, 532 „diffuse Bedrohlichkeit" der systematischen Erfassung der betroffenen Person. Mit Anwendungsbeispiel des Gesundheitsmonitorings *Delisle/Weyer*, in: Kolany-Raiser/Heil/Orwat u.a. (Hrsg.), Big Data und Gesellschaft, 2018, S. 84, 97 f. Diese sprechen von einer „Normierung des Alltags".

denkbar, wenn betroffene Personen bestimmte Handlungen unterlassen[202] oder vornehmen[203], da sie spätere, vor allem wirtschaftliche Nachteile befürchten. Ob und inwieweit diese Effekte tatsächlich bestehen, ist höchst umstritten.[204]

e) Autonomiegefährdung durch Eigenart und Neuartigkeit der Einflussnahme durch autonome Systeme

Die profilgestützte Automatisierung erweist sich als zweischneidiges Schwert:[205] Einerseits macht die algorithmische Personalisierung dem Einzelnen die digitale Realität mit ihren zahlreichen Informations-, Kommunikations- und Handlungsoptionen überhaupt erst zugänglich[206] und stärkt und er-

---

[202] Vgl. *Martini*, Blackbox Algorithmus, 2019, S. 50; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 306; *Roßnagel*, DuD 40 (2016), 561, 563. In diese Richtung auch *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 60 f. Ähnliche Überlegungen stellt *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 36 f. an. Siehe auch *Lobe*, Lieber Computer, sag mir, wen ich heiraten soll, FAZ 14.09.2016, https://www.faz.net/aktuell/feuilleton/debatten/die-macht-der-datenkonzerne-und-algorithmen-14433947.html.

[203] Sehr allgemein *Roßnagel*, DuD 40 (2016), 561, 563. Hier ist das Gesundheitsmonitoring, etwa über Fitness-Wearables, ein gängiges Beispiel, vgl. hierzu *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 100; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 59. Eine Autonomiegefährdung ist dies freilich nur, wenn das Verhalten, zu dem angereizt werden soll, nicht dem Willen der betroffenen Person entspricht. Bei Fitness-Wearables in ihrer üblichen Nutzung ist es vielfach aber gerade der Wunsch der NutzerInnen, gesünder und bewegungsaktiver zu leben. Dieser Fall stellt dann allerdings keine Autonomiegefährdung dar. Zu dieser Differenzierung siehe auch *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 100: „It would […] not just be a self-imposed tool for regulation and governing our behaviour, It would be one whose software and programming is controlled by third parties. It would not be entirely *ours*; it would be *theirs* as well". (mit Hervorhebung im Original).

[204] Kritisch etwa *Shiller*, Personalized Price Discrimination Using Big Data, Brandeis University, 29.07.2019, S. 3 f., der zudem darauf hinweist, dass aufgrund der Verhaltensirrationalitäten von VerbraucherInnen selbst bei Kenntnis günstiger Verhaltensweisen nicht notwendig eine Verhaltensänderung zu erwarten ist. Kritisch aufgrund fehlender empirischer Nachweise auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 219–322, der Abschreckungseffekte allerdings im Verhältnis zwischen VerbraucherInnen (c2c) und nicht, wie in der Perspektive dieser Arbeit, zwischen Unternehmern und VerbraucherInnen (b2c) untersucht.

[205] So auch *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 100, 106; für den Bereich der Informations- und Meinungspersonalisierung *Vīķe-Freiberga/Däubler-Gmelin/Hammersley u.a.*, A free and pluralistic media to sustain European democracy, High Level Group on Media Freedomand Pluralism, Januar 2013, S. 30 f. Ebenso *Bozdag*, Ethics Inf. Technol 15 (2013), 209, 221.

[206] *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 100; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 34. Vgl. auch *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 9 sowie *Mik*, Law Innov. Technol. 8 (2016), 1, 21.

weitert Selbstentfaltungsmöglichkeiten,[207] andererseits beschränkt sie diese. Das eine vom anderen abzugrenzen, fällt schwer.[208] Umso anspruchsvoller gestaltet sich dies, da die Studienlage noch unklar ist, und vielfach weiterhin analoge Alternativangebote zur Verfügung stehen.[209] Überdies ist der Einzelne mit derartigen Einflussnahmen durchaus vertraut: Algorithmenbasierte personalisierte Informations-, Waren- und Dienstleistungsangebote, Werbemaßnahmen oder Entscheidungen sind nichts eigentlich Neues.[210] Ohnehin ist der Mensch schon immer verschiedenen äußeren Einflussnahmen auf seine Willensbildung ausgesetzt, ohne dass er sich als unfrei begreifen würde.[211] Dass die Einwirkungen durch autonome Systeme tatsächlich autonomiegefährdend und ablehnungswürdig sind, bedarf daher besonderer Begründung.

Der Fokus ist daher auf die Eigenart und Neuartigkeit der Einwirkung durch autonome Systeme zu richten.[212] Tatsächlich stellt sich die Einflussnahme in Tiefe und Breite der Einflussnahme anders dar als das, womit der Einzelne bislang konfrontiert war: Autonome Systeme analysieren die betroffene Person in einer Detailtiefe, wie dies bislang nicht möglich war.[213] Sie passen die Umgebung, etwa Informationen oder Warenangebote, in Echtzeit an diese Erkenntnisse an, wirken so situativ-kontextuell und in Echtzeit und unterbinden so Momente der Selbstreflexion und -distanz.[214] Nicht einzelne, situative Reize

---

[207] So auch *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 110.

[208] Ebenso *Mik*, Law Innov. Technol. 8 (2016), 1, 21: „[T]he line between facilitating and reducing choice is difficult to draw". Differenzierungsansätze bei *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 12–29; *Zarsky*, Theoretical Inquiries in Law 20 (2019), 157, 168–172. Siehe zu diesem Abgrenzungsproblem auch *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 43 f.; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 232–233, 237–240; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 112.

[209] Ähnlich *Grafanaki*, Rich J. L. Techn. 24, 1, 37; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 239.

[210] *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 109; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 237.

[211] So auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 237; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 64; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 110; *Yeung*, iCS 20 (2017), 118, 129.

[212] So auch *Grafanaki*, Rich J. L. Techn. 24, 1, 42; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 110. Siehe hierzu bereits oben Kapitel 2 A. I. 2.

[213] *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 58; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 10; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 107 f.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 36; *Yeung*, iCS 20 (2017), 118, 122. Siehe auch o.A., Verbraucherrecht 2.0, Dezember 2016, S. 58 f. sowie *Mik*, Law Innov. Technol. 8 (2016), 1, 14, 27.

[214] *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 110 f.; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 34; *Mik*, Law Innov. Technol. 8 (2016), 1, 15. Zur personalisierten Werbung *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 31 f.: „Unlike traditional advertisements, which were static and disseminated en

wirken auf den Einzelnen ein, vielmehr sind es permanente, ubiquitäre, systematische Einflussnahmen einer umfassend automatisierten Umwelt, denen der Einzelne ausgesetzt ist.[215] All dies erfolgt in einer Umgebung der Intransparenz. Betroffene Personen wissen häufig nicht, dass überhaupt Profilbildungen und profilbasierte Automatisierungen stattfinden.[216] Zudem wirken die Einflussnahmen subtil und knüpfen vielfach an unterbewusst ablaufende, irrationale Mechanismen menschlicher Willensbildung an.[217] Vor allem aber sind Parameter dieser Einflussnahme, d.h. Profilinhalte und Variablen des Lösungsalgorithmus für die betroffene Person überwiegend aus geschäftlichen, bei autonomen Systemen aber vor allem aus technischen Gründen intransparent und nicht nachvollziehbar.[218] Schließlich sind die personalisierten Angebote nur von der einzelnen Person insoweit beeinflussbar und abänderbar, als dies technisch möglich und von Seiten der Unternehmen vorgesehen, d.h. einprogrammiert ist und der Einzelne die technische Expertise und Bereitschaft zur aktiven

masse, digitally-mediated platforms, such as websites and social media applications, constitute dynamic, interactive, intrusive, and personalized choice architectures".

[215] So auch *Mik*, Law Innov. Technol. 8 (2016), 1, S. 24, 27; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 98, 108–109, 110. Ebenso *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 238–240, die den Vergleich zu CO^2-Emissionen ziehen: Erst die quantitative Verbreitung belastender Einwirkungen führt zur eigentlichen Schädigung geschützter Rechtsgüter. Sie weisen dann darauf hin, dass die Gefährdungen der Privatautonomie mit einer allmählichen Verlagerung des Handels in die digitale „smarte" und damit umfassend personalisierte Welt zunehmen werden. Dieses Bild prägen auch *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 230: „Like global warming, erosion of the democratic commons would not result from any single AI system, but form an accumulation of algorithm-based decision increasingly replacing human-based decision-making in different contexts […]. A view of risk that ignores social impacts or focuses only on individual machine learning applications and overlooks the cumulative impact on society will fall short". Ebenso *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 34: „Furthermore, because information technology mediates so much of so many people's lives, the reach of online manipulation is virtually limitless. […] Unlike ‚offline manipulation', which is constrained by the manipulator's ability to understand and influence a finite number of other people, online manipulation is practically unbounded". Ähnlich *Grafanaki*, Rich J. L. Techn. 24, 1, 36.

[216] *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 1, 12. Für den Bereich personalisierter Werbung *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 33 f. Sie weisen auch darauf hin, dass selbst die Kenntnis vom manipulativen Einsatz derartiger algorithmischer Systeme deren Wirksamkeit kaum beeinträchtigt. Siehe allgemein zu den Gefahren bei einer Verwechslung autonomer Systeme mit menschlichen Entscheidern *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 33.

[217] *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 66; *Yeung*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 21, 35. Ebenso *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 111 f.: „[A]lgorithmic tools tend towards personalisation […] rather than outright manipulation".

[218] *Yeung*, iCS 20 (2017), 118, 124. Für den Bereich personalisierter Werbung *Susser/Roessler/Nissenbaum*, GLTR 4 (2019), 1, 33 f.

Beteiligung mitbringt.[219] Dass autonome Systeme damit grundlegend anders zu bewerten sind als tradierte Methoden der Personalisierung, erscheint daher richtig.[220] Diese Erwägungen gelten dann auch für die übrigen Vulnerabilitätsphänomene, wie sie hier beschrieben wurden. Auch diese stellen sich teilweise als bekannte Phänomene dar, erhalten dann aber aufgrund der Eigenart autonomer Systeme eine andere, neuartige Intensität und Qualität.

Die Abgrenzung zwischen akzeptabler Einflussnahme und inakzeptabler Autonomiegefährdung durch die Personalisierung lässt sich allerdings nur im Einzelfall bestimmen.[221] Maßgebliche Kriterien sind dann etwa der Personalisierungsgrad, der Anwendungsbereich, die typische Nutzung, die Intention des Herstellers, aber auch die Resilienzfähigkeit und das Risikobewusstsein des Einzelnen. In dieser Abwägungsentscheidung entscheidend ist am Ende aber die jeweilige Vorstellung von Autonomie und Resilienzfähigkeit.

V. Zusammenfassung und Themeneingrenzung

Die technikbedingten Risiken autonomer Systeme führen zu Veränderungen der Marktbedingungen zulasten von VerbraucherInnen, bewirken unerwünschte Klassifizierungen in der Gesamtgesellschaft und gefährden materielle Vorstellungen von Gerechtigkeit und Fairness, sie können die Grundbedingungen der Persönlichkeitskonstitution beeinträchtigen, Verhaltenssteuerung bewirken und auf vielfältige Weise die Willens- und Entscheidungsfreiheit des Menschen verkürzen. Vielfach knüpfen autonome Systeme zwar an bekannte Erscheinungen an, sie verstärken diese jedoch und begründen teilweise neue Gefährdungen. Analysekraft, Instantanität, Ubiquität, Intranspa-

---

[219] *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 106 f.

[220] So auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 237–239. *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 37 „[Legal Systems] must prevent people being locked into ‚categories' or ‚profiles' they know nothing about and which they are unable to challenge. […] Subjects are shown no respect if we do not at the same time respect their capacity for reticence, for reservation, for not doing what the algorithms predict and their ability to say, for themselves, what prompts them to act". Ähnlich *Grafanaki*, Rich J. L. Techn. 24, 1, 39 „Personalization algorithms are not inherently good or bad; the design choices behind them are what drives their impact". *Zuboff*, The age of surveillance capitalism, 2019 entwickelt hieraus die These, dass die Weltordnung algorithmischer Systeme mit den bisherigen Konzepten nicht mehr fassbar ist. Nicht das Wissen über den Einzelnen ist Ziel und Gefahr dieser neuen Welt, sondern die Verhaltensbeeinflussung des Einzelnen anhand dieses Wissens. *dies.*, The age of surveillance capitalism, 2019, S. 8: „[I]t is no longer enough to automate information flows *about* us; the goal is now to *automate* us" (Hervorhebung im Original). Befürwortend *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 113 f.; *Yeung*, iCS 20 (2017), 118, 130.

[221] So auch *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 65; *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 104.

renz und Determiniertheit führen dazu, dass sich die Auswirkungen und Wirkungen autonomer Systeme auf die beschriebenen Interessensfelder anders darstellen als das Bekannte. Dies erlaubt vor allem im Hinblick auf Autonomiegefährdungen eine Abgrenzung akzeptabler von inakzeptabler Einflussnahme. Die Nachteile wirken am Ende vor allem auf VerbraucherInnen, die personalisierte Dienste nutzen oder einer automatisierten Entscheidung unterworfen sind. Der Interessenskonflikt besteht damit maßgeblich zwischen Unternehmern, d.h. Herstellern und Anbietern oder Verwendern autonomer Systeme, und VerbraucherInnen. Zwischen diesen Personengruppen muss der Staat vermitteln.

Die folgende Untersuchung beschränkt die Perspektive auf Beeinträchtigungen innerer Autonomie, sucht also danach, inwieweit die DSGVO Schutz- und Ausgleichsmechanismen für die oben beschriebenen Beeinträchtigungen bereithält. Sie nähert sich der menschlichen Autonomie dabei phänomenologisch. Maßgeblich ist im Übrigen, auf welche Weise das Datenschutzrecht menschliche Autonomie schützt und begreift. Hierauf ist noch ausführlich einzugehen.[222] Eine allgemeine Definition und Beschreibung menschlicher Autonomie im Allgemeinen ist dagegen für das Erkenntnisinteresse dieser Arbeit nicht förderlich und unterbleibt daher. [223]

Berücksichtigt werden sollen im Folgenden auch Diskriminierungen, wenngleich der Schwerpunkt auf den Autonomiegefährdungen liegen wird. Denn menschliche Freiheit und Diskriminierungsschutz bedingen sich gegenseitig.[224] In einer Welt, in der Personen(-gruppen) aufgrund inakzeptabler Differenzierung nur bestimmte Informationen erhalten, wirtschaftliche Nachteile erleiden, während andere bevorteilt werden, und ganz allgemein in eigenen Realitäten leben (müssen), kann sich niemand als frei begreifen.[225]

---

[222] Siehe Kapitel 4 A. II.

[223] Aus der umfassenden Literatur zur Definition und den Inhalten menschlicher Autonomie siehe etwa *Betzler* (Hrsg.), Autonomie der Person, 2013; *Bobbert/Werner*, in: Lenk/Duttge/Fangerau (Hrsg.), Handbuch Ethik und Recht der Forschung am Menschen, 2014, S. 105; *Rössler*, Autonomie, 2017; *Seidel*, Deutsche Zeitschrift für Philosophie 59 (2011), 897–915 Vgl. auch die Darstellungen bei *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 102–104; *Yeung*, iCS 20 (2017), 118, 128 f. mit zahlreichen weiteren Nachweisen. Siehe auch unter Kapitel 4 A. II. 1.

[224] Vgl. zu den Wechselwirkungen von Gleichheitsgebot bzw. Diskriminierungsverbot und Freiheitsrechten, wenngleich zum Grundgesetz, Dürig/Herzog/Scholz, GG/*Kirchhof*, Art. 3 Abs. 1 Rn. 228; Dürig/Herzog/Scholz, GG/*Langenfeld*, Art. 3 Abs. 3 Rn. 19. Allgemein stehen diese daher in Idealkonkurrenz, vgl. hierzu Jarass, GRCh/*Jarass*, Art. 20 Rn. 6; Meyer/Hölscheidt, GRCh/*Hölscheidt*, Art. 21 Rn. 31.

[225] Dies hat auch der Uniongesetzgeber erkannt und hat in verschiedenen Vorschriften der DSGVO auf Diskriminierungseffekte Bezug genommen, insbesondere in Art. 9, Art. 22 Abs. 4 DSGVO. Vgl. hierzu auch *Martini*, Blackbox Algorithmus, 2019, S. 80–82.

D. Ergebnis

Autonome Systeme automatisieren menschlich-kognitive Prozesse, ihre Mechanismen und Verfahren sind daher bekannte Phänomene: Profilbildungen und profilgestützte Entscheidungen nimmt auch der Mensch vor. Sie stellen sich dann aber insoweit als neuartige Erscheinungen dar, als dass das maschinelle Wissen, d.h. das durch autonome Systeme gebildete Profil bzw. die profilbasierte algorithmische Lösung, stochastisch-mathematisch, datenbasiert-korrelativ, klassifizierend-stereotyp und intransparent ist. Gegenüber tradierten Big-Data-Auswertungsverfahren grenzt sich das Maschinelle Lernverfahren dadurch ab, dass es eigenständig, dynamisch, menschlich unverständlich, nur bedingt beeinflussbar, und im Hinblick auf Ressourceneinsatz, Zeit und Inhalt analysestärker ist. Autonome Systeme versprechen ein hohes Maß an Objektivität, Akkuratesse und Gleichmäßigkeit, an Transparenz und Beeinflussbarkeit sowie an Zugang zu umfassenden Wissensquellen. Darin liegen ihre Chancen. Ihre Risiken liegen in einer hohen Fehler- und Diskriminierungsanfälligkeit, in ihrer Beschränkung auf mathematisch Berechen- und Darstellbares, in ihrer Intransparenz und fehlenden Nachvollziehbarkeit sowie in der Determiniertheit. Dass autonome Systeme dann befürwortet oder abgelehnt werden, ist zurückzuführen auf bestimmte Einstellungen gegenüber Technik, Risiko und staatlicher Verantwortung. Technikoptimistische oder innovationsskeptische Überzeugungen, die zudem die Selbstverantwortung betonen, kollidieren mit technikpessimistischen Ansichten und solchen, die an autonomen Systemen idealisierende oder moralisierende Anforderungen stellen oder umfassende staatliche Verantwortung einfordern. Die beschriebenen Risiken wirken nachteilig auf verschiedene Interessensbereiche. Autonome Systeme können wohlfahrtsschädliche Machtasymmetrien auf den Märkten begründen oder vertiefen. Auf gesamtgesellschaftlicher Ebene sind Diskriminierungen und Ungleichbehandlungen zu befürchten sowie Segmentierungen und Fragmentierungen zwischen einzelnen Personengruppen, die das Modell vorgibt. Die Fehleranfälligkeit und nur beschränkte Abbildbarkeit von Einzelfallumständen in automatisierten Entscheidungsprozessen sowie die Intransparenz und Determiniertheit autonomer Systeme können zu Beeinträchtigungen materieller Fairness und Gerechtigkeit führen. Unzutreffende und entindividualisierende Darstellungen können Grundbedingungen freier Persönlichkeitskonstitution aufheben, ebenso wie unerwünschte oder ungewollte Einblicke in die Persönlichkeit, wie sie durch die zweistufige Profilbildung möglich sind. Die intransparente und deterministische Vorgabe von Handlungsoptionen kann die Verhaltensfreiheit verkürzen. Autonome Systeme können verhaltensökonomische Effekte bedienen, eine präemptive Realitätsgestaltung vornehmen, manipulative Übergriffe ermöglichen sowie Hemm- und Einschüchterungseffekte freisetzen. Dabei ist es die Neuartigkeit der Einflussnahme durch autonome Systeme, anhand derer eine hinnehmbare Einwirkung von einer inakzeptablen Autonomiegefährdung ab-

gegrenzt werden kann. Die Arbeit fokussiert auf Beeinträchtigungen der inneren Autonomie, berücksichtigt aber auch Diskriminierungen. Das Interesse am Schutz vor Autonomiegefährdungen und Diskriminierungen ist auszugleichen mit Interessen, vor allem von Unternehmen, an der freien Entwicklung, Nutzung und wirtschaftlichen Verwertung autonomer Systeme sowie mit dem allgemeinen Interesse an einer Ermöglichung und Förderung autonomer Systeme. Diesen Interessensausgleich herbeizuführen, ist Aufgabe des Rechts. Derzeit werden verschiedene Regulierungsinstrumente diskutiert, die dies leisten sollen. Dies ist Gegenstand des anschließenden Kapitels. Auch die DSGVO wird daran zu messen sein, ob ihr dieser Interessensausgleich gelingt. Dies ist dann Gegenstand des 4. Kapitels.

Kapitel 3

Regulierungsansätze für autonome Systeme

Vor dem Hintergrund der beschriebenen Vulnerabilitätsphänomene ist gemeinhin Konsens, *dass* diese neuartige Technologie der autonomen Systeme reguliert werden muss.[1] *Wie* diese Regulierung aussehen sollte, wird dagegen sehr unterschiedlich gesehen. Die Frage nach dem *Wie* der Regulierung eröffnet verschiedene rechtliche Forschungsfelder. So stellen sich etwa Fragen der rechtsnormativen Gebotenheit und Zulässigkeit derartiger Regulierung. Um diese soll es hier nicht gehen. Im Fokus dieser Arbeit steht vielmehr die Frage, wie eine Regulierung autonomer Systeme besonders gut bzw. optimal erfolgen kann. Im liberalen Verfassungsstaat gibt es hierzu keine verbindlichen Vorgaben, vielmehr muss der Gesetzgeber nach Regeln legislativer Klugheit abwägen und entscheiden. Dies lässt Raum für ganz unterschiedliche Wertungen. Entsprechend vielgestaltig sind die derzeit diskutierten Ansätze zur sinnvollen Regulierung autonomer Systeme. Ziel des folgenden Kapitels ist es, einen Überblick über diese allgemeine Regulierungsdebatte zu geben. Dieser Überblick vermittelt nicht nur ein grundlegendes Verständnis dafür, wie eine gute Regulierung autonomer Systeme (derzeit) verstanden wird, sie führt überdies vor Augen, welchen Beitrag die DSGVO zur Regulierung autonomer Systeme erbringen kann und soll. Dies ist wichtig, um die DSGVO im nachfolgenden Kapitel 4 einer angemessenen Bewertung zuzuführen sowie im 5. Kapitel Innovationspotentiale der DSGVO auszuloten.

Zunächst soll aber der Bewertungsmaßstab dieser Arbeit näher präzisiert und also verdeutlicht werden, was in der nachfolgenden Untersuchung mit der Maxime einer „guten" Regulierung autonomer Systeme gemeint ist (A.). Im Anschluss soll dann eine Darstellung wesentlicher Regulierungsansätze in Bezug auf autonome Systeme erfolgen (B.). Dies erlaubt eine erste Einordnung, was die DSGVO zur Regulierung autonomer Systeme beitragen kann und soll (C.).

---

[1] Einen Überblick über verschiedene internationale und nationale Regulierungsprojekte bieten *NíFhaoláin/Hines/Nallur*, in: Longo/Rizzo/Hunter u.a. (Hrsg.), Artificial Intelligence and Cognitive Science, 2020, S. 133; *Campbell*, Artificial Intelligence: An overview of state initatives, FutureGrasp, 2019.

A. Gute Regulierung autonomer Systeme als Bewertungsmaßstab

Untersuchungsziel der Arbeit ist es, aufzudecken, inwieweit die DSGVO sinnvolle Schutzmaßnahmen gegen die in Kapitel 2 dargelegten Gefährdungen bereithält und, soweit Defizite festgestellt werden, welche Anpassungen der DSGVO geboten sind. Diese Forschungsfragen haben eine normative Ausrichtung: Es geht nicht allein darum, wie sich die Regulierung darstellt, sondern wie sie bestenfalls aussehen *sollte*. Der rechtswissenschaftliche Forschungsauftrag besteht in der Erarbeitung von Empfehlungen für eine gelungene Technikregulierung (I.). Als inhaltliche Kriterien für eine „gute" bzw. „optimale" Regulierung sollen dabei wirkungs- sowie sozialethisch orientierte Merkmale dienen (II.).

I. Gute Regulierung als rechtswissenschaftlicher Untersuchungsauftrag

Der Fokus dieser Untersuchung liegt nicht auf den verfassungsgemäßen Grenzen einer Regulierung autonomer Systeme, vielmehr richtet er sich auf den von der Verfassungsordnung eröffneten Gestaltungsspielraum. Es geht um die rechtswissenschaftliche Aufarbeitung und Bewertung legislativer Handlungsoptionen innerhalb dieses Spielraums. Der Bewertungsmaßstab ist dabei kein juristischer im technischen Sinne, denn um Rechtmäßigkeitskriterien geht es nicht. Ziel ist vielmehr, eine möglichst gute oder gar optimale Regulierung zu finden, d.h. eine solche, die die aufgeworfenen Regulierungsfragen einer angemessenen Lösung zuführt.[2,3] An dieser Maxime ist bestehendes oder zu

[2] Diese Fragestellung ist Gegenstand der Gesetzgebungslehre, einem Teilbereich der Rechtswissenschaft. Siehe eingehend zur historischen Entwicklung *Emmenegger*, Gesetzgebungskunst, 2020; *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 8–69. Siehe auch *Meßerschmidt*, ZJS 1 (2008), 111, 113–116 Grundlegend die Beiträge von *Karpen*, in: Schreckenberger (Hrsg.), Grundfragen der Gesetzgebungslehre, 2000, S. 11; *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006; *Karpen*, Gesetzgebungs-, Verwaltungs- und Rechtsprechungslehre, 1989. Die Gesetzgebungslehre sieht ihren Auftrag darin, Gesetzgebungsverfahren sowie äußere und innere Aspekte der Gesetzesgestaltung (gemeint sind: formelle und inhaltliche Aspekte eines Gesetzes) einerseits zu erfassen und zu beschreiben, andererseits gute legislative Praktiken und Lösungen zu entwickeln und dem Gesetzgeber vorzuschlagen, siehe *Meßerschmidt*, ZJS 1 (2008), 111, S. 112 f., 118 f.; *Müller*, in: Akyürek (Hrsg.), Staat und Recht in europäischer Perspektive, 2006, 503. Eingehend *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 35–37; *Karpen*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 1, 3, der Gesetzgebungstaktik (Gesetzgebungsverfahren), Gesetzgebungsanalytik (inhaltliche Gestaltung des Gesetzes) und Gesetzgebungstechnik (äußerliche Gestaltung des Gesetzes) unterscheidet. Zur damit praktischen Bedeutung der Gesetzgebungslehre, d.h. ihrer beratend-reformatorischen Zielsetzung siehe etwa *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 48: „Ziel der Gesetzgebungslehre ist die Verbesserung der Gesetze und ihrer Wirkung".

schaffendes Recht zu prüfen. Der Bewertungsmaßstab ist damit eine normative Angemessenheit im Sinne legislativer Klugheit und Rationalität.[4] Die nach diesem Maßstab optimale Lösung muss dann nicht notwendig in einem legislativen Tätigwerden liegen. Auch die Nichtregulierung, d.h. die gezielte gesetzgeberische Zurückhaltung, kann einen Konfliktfall gut bzw. optimal auflösen.[5]

Am Ende dieses rechtswissenschaftlichen Untersuchungsauftrags stehen Handlungsempfehlungen für den Gesetzgeber,[6] die aber keinen Verbindlichkeitsanspruch erheben können.[7] Denn apriorische Richtigkeitsvorstellungen,

---

[3] Die rechtswissenschaftliche Innovationsforschung beschäftigt sich mit dieser Frage spezifisch im Hinblick auf die Technikregulierung. Grundlegend zu diesem Forschungsbereich *Hoffmann-Riem*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 11; *Hoffmann-Riem*, AöR 131 (2006), 255–277 Siehe auch *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273; *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993; *Roßnagel*, in: Breuer/Kloepfer/Marburger u.a. (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, 1994, S. 425; *Roßnagel*, in: Hof/Wegenroth (Hrsg.), Innovationsforschung, ^{2}2010, S. 9. Zum Forschungsauftrag der Entwicklung besonders guter Technikregulierung *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273, 280 f.; *Hoffmann-Riem*, AöR 131 (2006), 255, 271–274. Siehe zu typischen Forschungsfragen und -aufträgen *Hoffmann-Riem*, AöR 131 (2006), 255, 273 f.; *Hoffmann-Riem*, in: Hof/Wegenroth (Hrsg.), Innovationsforschung, ^{2}2010, S. 387, 396 f.

[4] Die Begriffe der „guten" bzw. „optimalen" Gesetzgebung sind damit keine rechtsförmlichen, sondern Hilfsbegriffe, denn sie benennen Orientierungsmaßstäbe nicht-rechtlicher Natur, so *Smeddinck*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 69, Rn. 33. Zur Abgrenzung von Verfassungsmäßigkeit – dies ist nicht Gegenstand der Gesetzgebungslehre – und normativer Klugheit – dies ist Gegenstand der Gesetzgebungslehre, siehe *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 72 f.; *Voermans*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 17, 25 f. Zum Begriff der Gesetzgebungsklugheit siehe *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 36; *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn.70; zu dem der Rationalität *Steinbach*, Rationale Gesetzgebung, 2017; *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 80–99.

[5] Vgl. *Voermans*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 17, 31.

[6] *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 36: „Die Gesetzgebungslehre […] versteht sich aber seit je in besonderem Maße als wissenschaftliche Anleitung der gesetzgeberischen Praxis".

[7] Die Gesetzgebungslehre bewegt sich, vor allem soweit inhaltliche Fragen guter Gesetzgebung angesprochen sind, nahe an der Rechtspolitik. Seit jeher ist daher umstritten, ob es sich überhaupt um eine Wissenschaft handelt, siehe nur *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 70–75; unter Darstellung der geschichtlichen Hintergründe *Emmenegger*, Gesetzgebungskunst, 2020, S. 291–296. Inwieweit die Anregungen der Gesetzgebungslehre auch rechtsnormative Gebote mit Verbindlichkeitsanspruch sein können, ist Gegenstand kontroverser Debatte. Es geht dann um eine verfassungsgemäße Verpflichtung des Gesetzgebers zu guter bzw. optimaler Gesetzgebung. Nach *Müller*, in: Akyürek (Hrsg.), Staat und Recht in europäischer Perspektive, 2006, S. 503, 508 f. soll zu-

wie eine gute bzw. optimale (Technik-)Regulierung aussehen muss, gibt es im liberalen Verfassungsstaat nicht, [8] ja nicht einmal, was eine „gute" bzw. „optimale" Technik ausmacht.[9] Dies kann und wird man ganz unterschiedlich sehen.[10] Im demokratischen Rechtsstaat ist am Ende allein entscheidend, welcher Vorschlag sich im politischen Diskurs durchsetzt.[11] Dieser Diskurs darf nicht, auch nicht von Seiten der Rechtswissenschaft, verkürzt werden. Sehr wohl aber kann sie sich als gleichberechtigte Stimme in den Diskurs zur richtigen (Technik-)Regulierung einbringen.[12] Darin liegt der Auftrag dieser Arbeit.

---

mindest ein „Mindestmaß" an Rationalität von Verfassungs wegen geboten sein. So auch *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 39: „Aber der Gesetzgeber verfassungsunterworfen, schuldet dem Bürger nicht einfach ‚das Gesetz', sondern ‚ein gutes Gesetz'". Ähnlich *Blum*, Wege zu besserer Gesetzgebung, 2004, S. 19: „Nicht jedes ‚vermurkste' Gesetz ist verfassungswidrig". Kritisch *Karpen*, in: Schreckenberger (Hrsg.), Grundfragen der Gesetzgebungslehre, 2000, S. 11, 23. Zurückhaltend auch *Meßerschmidt*, ZJS 1 (2008), 224: „[D]ie prozedurale und materielle Rationalitätspflicht des Gesetzgebers […] [würde] zur [sic] einer Depossedierung des politisch verantwortlichen parlamentarischen Gesetzgebers durch das Bundesverfassungsgericht in weiten Teilen führen".

[8] Siehe hierzu *Meßerschmidt*, ZJS 1 (2008), 111, 118; *Mödinger*, Bessere Rechtsetzung, 2020, S. 37 f. Siehe auch *Blum*, Wege zu besserer Gesetzgebung, 2004, S. 12.

[9] Die Verfassung gibt nur ein Rahmenprogramm vor, vgl. hierzu etwa *Hoffmann-Riem*, AöR 131 (2006), 255, 266 f.; *Boehme-Neßler*, Unscharfes Recht, 2008, S. 62. Siehe auch eingehend *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273, 290–292.

[10] Treffend *Blum*, Wege zu besserer Gesetzgebung, 2004, S. 9: „Da es sich bei der Beantwortung der Frage nach ‚guter', ‚weniger guter' und ‚besserer' Gesetzgebung um wertende Betrachtungen handelt, wird man sich eingestehen müssen: Einschätzungen hierüber befinden sich stets auf schwankendem Boden und sind stark abhängig von Erfahrungen und dem daraus gewonnenen Verständnis des Beurteilenden. Gleiches gilt für die aus diesen Einschätzungen gewonnenen Empfehlungen". Eine Systematisierung von politisch definierten Zielen des Technikrechts nimmt *Eisenberger*, Innovation im Recht, 2016, S. 20–36 vor. Sie macht sieben Regulierungsziele aus: Rationalisierung, Gefahrenabwehr, Risikovorsorge, Innovationsförderung, Ethisierung, Sozio-Ökonomisierung und Demokratisierung.

[11] Das majoritäre Gesetzgebungsverfahren wird im demokratischen Verfassungsstaat als Garant für die Entwicklung eines „guten" Gesetzes gesehen. Rationalität und Majorität gehen also Hand in Hand, vgl. *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 83 f.; *Karpen*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 1, 3.

[12] *Meßerschmidt*, ZJS 1 (2008), 224, 228–230; *Müller*, in: Akyürek (Hrsg.), Staat und Recht in europäischer Perspektive, 2006, S. 503, 514. Vgl. auch *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 91. Unter Nachzeichnung der historischen Entwicklung dieses Verständnisses der Gesetzgebungslehre *Emmenegger*, Gesetzgebungskunst, 2020, S. 287–296 Auch die rechtswissenschaftliche Innovationsforschung sieht ihren Auftrag in der Beratung – nicht in der Vorwegbindung – des Gesetzgebers, eingehend *Hoffmann-Riem*, AöR 131 (2006), 255, 271 f.; *Roßnagel*, in: Breuer/Kloepfer/Marburger u.a. (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, 1994, S. 425, 435–440; vgl. auch *Schulze-Fielitz*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Inno-

II. Materielle Bewertungsmaßstäbe guter Regulierung

Wann ist ein Gesetz gut bzw. optimal?[13] Da es dabei nicht um Fragen der Rechtmäßigkeit oder Rechtswidrigkeit geht, kann das Recht hierauf keine Antworten geben.[14] Eine Vielzahl an Bemessungskriterien ist denkbar, etwa solche ökonomischer, ethischer oder soziologischer Natur.[15] Die vorliegende Untersuchung beschränkt sich auf zwei Aspekte: Die tatsächliche Wirksamkeit und die materielle Sachgerechtigkeit.

Gemeinhin wird ein Gesetz als gut bewertet, wenn es tatsächlich gut funktioniert, d.h. die intendierte (Verhaltens-)Steuerung in der Rechtswirklichkeit erbringt.[16] Für das Technikrecht lässt sich spezifizieren: Ein Technikgesetz ist gut, wenn es die Technik in der intendierten Weise tatsächlich zu steuern vermag.[17] Der Fokus richtet sich damit auf die Rechtspraxis und die Rechtsfolgen-

---

vationsforschung, 1998, S. 291, 304; *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273, 282 f.

[13] Neben diesem inhaltlichen Aspekt geht es auch um Fragen der optimalen äußerlichen Gestaltung eines Gesetzes, etwa der sprachlichen Fassung oder der Verwendung von Verweisungen, sowie eines effektiven Gesetzgebungsprozesses. Diese stehen aber nicht im Fokus dieser Arbeit. Zur äußeren Gestaltung siehe etwa *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 100–131; *Duprat/Xanthaki*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 109; *Hernández Ramos/Heydt*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 129, zum Gesetzgebungsverfahren siehe beispielhaft *Drinóczi*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 33 Umfassend zu den verschiedenen Aspekten guter Gesetzgebung und ihrer Systematisierung *Mödinger*, Bessere Rechtsetzung, 2020, S. 27–33.

[14] Vgl. *Emmenegger*, Gesetzgebungskunst, 2020, S. 291.

[15] Zur interdisziplinären Inspiration der Gesetzgebungslehre siehe *Meßerschmidt*, ZJS 1 (2008), 224, 225; *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 74 f.; *Karpen*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 1, 3. Vgl. auch *Emmenegger*, Gesetzgebungskunst, 2020, S. 163–183. Dies verlangt eine besondere interdisziplinäre Sensibilität der Gesetzgebungslehre. Defizite erkennt *Meßerschmidt*, ZJS 1 (2008), 224, 225: „Juristen [neigen] dazu, Erkenntnisse der Nachbarwissenschaften entweder zu ignorieren oder aber in advokatorischer oder ideologischer Manier als Versatzstücke in ihre Argumentation einzubauen". Zu weiteren Kriterien inhaltlich guter Gesetze siehe ausführlich *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 38–41.

[16] Dieser Aspekt zählt gemeinhin zum Kernelement eines guten Gesetzes, siehe nur *Müller*, in: Akyürek (Hrsg.), Staat und Recht in europäischer Perspektive, 2006, S. 503, 504; *Mödinger*, Bessere Rechtsetzung, 2020, S. 33; *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 35; *Smeddinck*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 69, Rn. 10–20; *Zamboni*, in: Jung/Jung-Müller-Dietz-Neumann (Hrsg.), Recht und Moral, 1991, S. 109, 97. Die Effektivität als Merkmal führt auch *Wischmeyer*, AöR 143 (2018), 1, S. 19, 43, 52–54 an.

[17] Siehe nur *Hoffmann-Riem*, in: Hof, Wegenroth Hg, S. 387, 388; *Hoffmann-Riem*, AöR 131 (2006), 255, 267, 271; *Hoffmann-Riem*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 11, 15, 20–21. Siehe auch *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273,

seite, der Ansatz ist soziologisch-ökonomisch inspiriert.[18] Eine Regulierung ist zudem nur dann gut, wenn das Gesetz den adressierten Konflikt auflöst, d.h. einen gerechten und fairen Ausgleich zwischen kollidierenden Interessen findet.[19] Im Technikrecht ist der Anspruch, einen idealen Ausgleich von Innovationsermöglichung und Eindämmung von Risiken, d.h. Innovationsbehinderung zu finden.[20] Im Fokus dieser Arbeit stehen die in Kapitel 2 geschilderten

---

280 f.: „Aufgabe der rechtswissenschaftlichen Innovationsforschung ist es mithin, […] darzulegen, ob und ggf. in welcher Weise die gewünschten Effekte einfacher, zielgerecht(er) und ‚nebenwirkungsärmer' erreicht werden können, sowie Konzepte und Instrumentarien für weiter politische Einwirkung auf Innovationsprozesse mit dem [sic] Mitteln des Rechts zu erstellen". Zur Rechtsfolgenorientierung des Technikrechts siehe etwa *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993. In der rechtswissenschaftliche Innovationsforschung wird dies auf das Schlagwort „[technische] Innovation durch Recht" gebracht, siehe etwa *Hoffmann-Riem*, in: Schulte/Di Fabio (Hrsg.), Technische Innovation und Recht, 1997, S. 3. Vgl. auch *Schuppert*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 171; *Reich*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 330; *Trute*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 208. Das Recht kann freilich nur Impulse für die technischen Entwicklung setzen, diese aber nicht selbst vornehmen, so auch *Hoffmann-Riem/Fritzsche*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsverantwortung, 2009, S. 12, 13 f.; *Schulze-Fielitz*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 291, 294. Treffend *Hoffmann-Riem*, Die Verwaltung 33 (2000), 155, 159: „Innovationen lassen sich nicht ergebnisorientiert konditional programmieren". Diese auf reale Steuerungseffekte fokussierende Betrachtung und Bewertung des Rechts ist steuerungswissenschaftlich inspiriert und damit Teil der sogenannten Neuen (Verwaltungs-)Rechtswissenschaft, siehe hierzu eingehend *Hoffmann-Riem*, AöR 131 (2006), 255, 268; *Hoffmann-Riem*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 11, 20; *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273, 281–283. Zur Neuen (Verwaltungs-)Rechtswissenschaft siehe ausführlich *Voßkuhle*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, [2]2012, Bd. 1, 1–71.

[18] Zur Bedeutung der Soziologie für die Gesetzgebungslehre siehe *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 37 f.; *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 74. Die (sozialwissenschaftliche) Gesetzesfolgenforschung ist daher wesentlicher Bestandteil der Gesetzgebungslehre, siehe *Smeddinck*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 69, Rn. 45–46. Zu ökonomischen Bewertungsmaßstäben siehe eingehend *Voermans*, in: Karpen/Xanthaki/Mader u.a. (Hrsg.), Legislation in Europe, 2017, S. 17, 30 f.

[19] *Kluth*, in: Kluth/Krings/Augsberg u.a. (Hrsg.), Gesetzgebung, 2014, S. 3, Rn. 85. Vgl. auch *Karpen*, Gesetzgebungslehre – neu evaluiert, 2006, S. 35 „(Das Gesetz) ist Ausformung der Rechtsidee – es soll ‚gerecht' sein". Von „gerechte(r), effektive(r) und effiziente(r) Normierung" spricht *Müller*, in: Akyürek (Hrsg.), Staat und Recht in europäischer Perspektive, 2006, S. 503, 513, von „Sachangemessenheit" *Blum*, Wege zu besserer Gesetzgebung, 2004, S. 12. Zur Rationalität als Maßstab siehe *Steinbach*, Rationale Gesetzgebung, 2017.

[20] Spezifisch für die Regulierung autonomer Systeme *Martini*, Blackbox Algorithmus, 2019, S. 360; *Hoffmann-Riem*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial

Autonomiegefährdungen und Diskriminierungen. Damit lässt sich präzisieren: Eine Regulierung autonomer Systeme ist gelungen, wenn sie es leisten kann, diese Gefährdungen effektiv zu unterbinden, dabei aber zugleich die Nutzung und Entwicklung autonomer Systeme zu ermöglichen. Dieses Verständnis guter Gesetzgebung ist sozialethisch geprägt. Diese Anforderung führt zurück zur erstgenannten: Die Regulierung ist nur gut, wenn sie diesen Interessensausgleich auch in der Praxis tatsächlich herbeizuführen vermag.

B. Ansätze einer guten Regulierung autonomer Systeme

Über eine sinnvolle Regulierung autonomer Systeme wird bereits seit einiger Zeit auf nationaler, europäischer und internationaler Ebene nachgedacht. Ziel dieses Abschnitts ist es, einen Überblick über zentrale Regulierungsansätze zu verschaffen. Unterscheiden lassen sich tradierte Ansätze, die in autonomen Systemen lediglich neuartige Erscheinungen bekannter Phänomene erkennen und bestehende Regelungsansätze heranziehen (I.) und innovative Ansätze, die autonome Systeme als disruptiv-neuartige Erscheinungen einordnen und eigenständige, technikspezifische Regelungen fordern, dies teils mit neuartigen Regulierungsansätzen (II.). Am Ende sind die Regulierungsansätze sehr unterschiedlich, lassen aber auch gewisse übereinstimmende Merkmale erkennen (III.). Die folgende Darstellung beschränkt sich auf die im öffentlichen Diskurs vorherrschenden Ansätze.

I. Tradiert-punktuelle Regulierungsansätze

Regulierungsvorschläge erfolgen im Bereich der Informations- und Meinungsfreiheit (1.), der Privatautonomie und dem Verbraucherschutz (2.), dem Antidiskriminierungsrecht (3.), dem Privatheitsschutz (4.) sowie mit Blick auf die Herstellung von materieller Gerechtigkeit und Fairness, insbesondere Verfahrensgerechtigkeit, (5.), sowie auf die Menschenwürde (6.).

Intelligence, 2020, S. 1, 5; *Smuha*, Law Innov. Technol. 13 (2021), 57, 60 f. Allgemein zu diesem Doppelziel im Technikrecht *Eisenberger*, Innovation im Recht, 2016, S. 28–30, 75–80; *Hoffmann-Riem*, AöR 131 (2006), 255, 258–261, 271–272; *Hoffmann-Riem*, in: Hoffmann-Riem/Schneider (Hrsg.), Rechtswissenschaftliche Innovationsforschung, 1998, S. 11, 19 f.; *Kloepfer/Franzius*, Technik und Recht im wechselseitigen Werden, 2002, S. 105–107; *Boehme-Neßler*, Unscharfes Recht, 2008, S. 60 f.; *Scherzberg*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 273, 291 f.; *Roßnagel*, in: Breuer/Kloepfer/Marburger u.a. (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, 1994, S. 425, S. 426, 429. Hier setzt vielfach die Kritik am klassischen Technikrecht an, das häufig einseitig als innovationshemmend wahrgenommen wird, so *Hoffmann-Riem*, AöR 131 (2006), 255, 258–259, 261.

1. Meinungs- und Informationsfreiheit: Plattform- und Suchmaschinenregulierung und Digital Services Act

Unter der Perspektive der Meinungs- und Informationsfreiheit rücken Anwendungen autonomer Systeme in den Fokus regulativer Steuerung, die Informations- und Kommunikationsinhalte für NutzerInnen automatisiert aufbereiten.[21] Von besonderer Bedeutung sind dabei Online-Plattformen, die fremde Beiträge – solcher der NutzerInnen oder Dritter – vermitteln.[22] Typisch für die Plattformökonomie ist das monopolartige Marktdesign,[23] Lock-in-Effekte bestärken diese Monopolisierungstendenzen.[24] Verlagern sich Information und Kommunikation zunehmend in den digitalen Raum, fungieren die Plattform-

[21] Vermittlungsdienste sollen die kognitiv überfordernde Informationsflut im digitalen Raum für die NutzerInnen verfügbar machen. Siehe dazu bereits Kapitel 1 C. I. *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 28; *Flamme*, MMR 24 (2021), 770; *Martini*, Blackbox Algorithmus, 2019, S. 213. Neben der Personalisierung gibt es verschiedene Filterkriterien, etwa nach der Popularität oder Aktualität eines Beitrags, die aber im Folgenden außer Betracht bleiben.

[22] Nur teilweise erstellen diese auch eigene Beiträge, vgl. *Dörr/Natt*, ZUM 58 (2014), 829, 831 f.; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 52–54.

[23] Der Marktanteil von Google in Deutschland bei der Desktopsuche liegt im November 2022 bei 80 %, bei der mobilen Suche bei 96, 33 %, so *Statistika*, Marktanteile von ausgewählten Suchmaschinen bei der Desktop-Suche und bei der mobilen Suche in Deutschland im November 2022, Dezember 2022. Das Soziale Netzwerk Facebook rangiert im Januar 2022 mit einer Anzahl von 2.910 Millionen monatlichen NutzerInnen an erster Stelle, gefolgt von YouTube mit 2.562 Millionen aktiven NutzerInnen. Instagram ist mit 1.478 Millionen NutzerInnen auf dem dritten Platz, Twitter belegt mit 436 Millionen NutzerInnen den 15. Platz, siehe *dies.*, Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Januar 2022, Januar 2022. Im November 2022 verbuchte Facebook – gemessen an den Page Views – einen Marktanteil von 67,13 % unter den Sozialen Netzwerken, gefolgt von Twitter mit einem Marktanteil von 10.30 % und Instagram mit einem Marktanteil von 9,65 %, siehe *dies.*, Marktanteile von Social-Media-Seiten nach Seitenabrufen weltweit bis November 2022. Nach einer Umfrage von Statistika ist das beliebteste Soziale Netzwerk in Deutschland im Jahr 2022 YouTube, gefolgt von Facebook und Instagram, siehe *dies.*, Beliebteste soziale Netzwerke in Deutschland im Jahr 2022, November 2022. Siehe zur Marktstruktur der Online-Plattformen auch eingehend *Dörr/Natt*, ZUM 58 (2014), 829, 833 f.

[24] Diese beschreiben das Phänomen, dass zwar Alternativen faktisch verfügbar wären, diese aber für NutzerInnen nicht attraktiv sind. Der Effekt lässt sich vor allem auf Sozialen Netzwerken beobachten: Die Mehrheit der NutzerInnen ist auf einer bestimmten Online-Plattform vertreten und verwendet nur diese. Liegt die Attraktivität einer Online-Plattform gerade in der Erreichbarkeit möglichst vieler NutzerInnen, besteht wenig Anreiz, ein alternatives Netzwerk zu nutzen, bei dem nur wenige Personen Mitglieder sind. Siehe etwa *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 57–59. Bei Suchmaschinen entsteht dieser „Lock-in"-Effekt aufgrund des besonderen Vertrauens, das dem bekannten – dann also marktbeherrschenden Suchdienst – entgegengebracht wird und das bei alternativen Suchdiensten fehlt. Vgl. eingehend *Dörr/Natt*, ZUM 58 (2014), 829, 834 f.

betreiber als „Intermediäre“ und „Gatekeeper“:[25] Die Online-Plattformen entscheiden letztlich, welche Informationen und Kommunikationsinhalte von der breiten Bevölkerung konsumiert werden.[26] Online-Plattformen wird daher eine besondere Verantwortung für die Information, Willens- und Wertebildung und Meinungspluralität zugesprochen.[27]

Dieser auf automatisierter Filterung beruhende Informations- und Kommunikationsaustausch im Netz lässt grundlegende Änderungen des Informations- und Kommunikationsverhaltens der NutzerInnen erkennen.[28] Desinformation und Hassrede sowie Radikalisierungen und Polarisierungen,[29] aber auch wirkmächtige Manipulationen[30] sind Phänomene, die gemeinhin als problematisch bewertet werden. Ursachen und Zusammenhänge sind vielfach unklar. Es besteht aber Konsens, dass zumindest auch die Personalisierung der Filterung ur-

---

[25] Zu diesen Begriffen siehe nur *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 40–43; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, 75 f.; *Danckert/Mayer*, MMR 13 (2010), 219, 220; *Dörr/Natt*, ZUM 58 (2014), 829, 831. Anschaulich spricht *Drexl*, ZUM 61 (2017), 529, 536 von einem „digitalen Kiosk“.

[26] Siehe nur *Koreng*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 245, 253 f.; *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, S. 262–263, 299-300; *Martini*, Blackbox Algorithmus, 2019, S. 99 f.

[27] Vgl. *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, S. 263–267, 306 f.; *Danckert/Mayer*, MMR 13 (2010), 219, 220 f.; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 29 f.

[28] Die Wirkungen auf das Meinungsbild der NutzerInnen gestalten sich bei Suchdiensten, die eine Eigeninitiative der NutzerInnen voraussetzen, anders als bei Empfehlungssystemen, die eigeninitiativ Medienbeiträge anbieten. Auch die Art der Online-Plattform ist entscheidend. Vielfach wird daher bei der Erarbeitung von Regulierungsinstrumenten zwischen Such- und Empfehlungssystemen sowie zwischen einzelnen Anbietern differenziert. Eine Differenzierung zwischen Selektions- und Rankingdiensten nehmen etwa vor *Müller-Terpitz*, ZUM 64 (2020), 365; ähnlich *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 85. *Dörr/Natt*, ZUM 58 (2014), 829, 833 unterscheiden verschiedene Typen von Suchdiensten.

[29] Siehe hierzu nur *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 17.

[30] Siehe nur *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 16 f.; *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 75, 90. Eingehend auch *Menczer Filippo/Hills*, Die digitale Manipulation, Spektrum 02.04.2021, https://www.spektrum.de/news/wie-algorithmen-uns-manipulieren/1849438.

sächlich ist.[31] Wie in Kapitel 2 bereits dargelegt wurde,[32] befördert die Personalisierung verhaltensökonomische Anreize und Selbstbestärkungseffekte[33] sowie Fragmentierungen der Realitäts- und Diskursräume (Filter Bubbles[34] und Echokammern[35]).[36]

---

[31] Ebenso *Martini*, Blackbox Algorithmus, 2019, S. 100 f.; *Dörr/Natt*, ZUM 58 (2014), 829, 837; *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 4; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 110; *Liesem*, AfP 51 (2020), 277, 278. Siehe auch *Menczer Filippo/Hills*, Die digitale Manipulation, Spektrum 02.04.2021, https://www.spektrum.de/news/wie-algorithmen-uns-manipulieren/1849438.

[32] Siehe eingehend Kapitel 2 C II. 2, IV. 2. Inwieweit die automatisierte Selektion von Medieninhalten sich tatsächlich nachteilig auf die Meinungsbildung auswirkt, ist empirisch noch nicht zweifelsfrei belegt. So ist schon unklar, inwieweit die personalisierte Filterung überhaupt zu einem selektiv-einseitigen Medienangebot führt. Studienergebnisse weisen teilweise darauf hin, dass den NutzerInnen tatsächlich ein äußerst vielseitiges Inhalts- und Meinungsspektrum angeboten wird, vgl. *Brkan*, SSRN Journal 9.4.2019, 1, 3, so auch *Bakshy/Messing/Adamic*, Science 348 (2015), 1130, 1131 f. Verschiedene Studien zur Testung des Personalisierungsgrades (untersucht wurde, inwieweit die Suchanfragen unterschiedlicher NutzerInnen zu unterschiedlichen Ergebnissen führen), liefern ambivalente Ergebnisse, vgl. etwa *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 128 f.; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 70 f. Weitere Forschungsbedarfe erkennen auch *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 8 f.

[33] Siehe bereits die Nachweise unter Kapitel 2 C IV. 2. a). Vgl. auch *Drexl*, ZUM 61 (2017), 529, 533 f.; *Flamme*, MMR 24 (2021), 770, 774.

[34] Eingehend *Pariser*, The filter bubble, 2011. Siehe auch *Dörr/Natt*, ZUM 58 (2014), 829, 837; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 111. Weitere Nachweise in Kapitel 2 C. IV. 2 b).

[35] Grundlegend *Sunstein*, Republic.com 2.0, 2007, S. 65; *Sunstein*, Echo chambers, 2001. Weitere Nachweise in Kapitel 2 C. II 2.

[36] Die tatsächliche Existenz derartiger Phänomene ist realwissenschaftlich noch nicht eindeutig geklärt, Studien liefern ambivalente Ergebnisse. Befürwortend *An/Quercia/Crowcroft*, in: Schwabe (Hrsg.), Proceedings of the 22nd international conference on World Wide Web companion, 2013, S. 51; *Bessi/Zollo/Del Vicario u.a.*, PloS one 11 (2016), e0159641; *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 188. In der Tendenz auch *Flaxman/Goel/Rao*, Public Opinion Quarterly 80 (2016), 298, 317–319 Kritisch aufgrund der unklaren Studienlage *Cornils*, AfP 49 (2018), 377, 380 f.; *Ingold*, MMR 23 (2020), 82, 83 f.; *Stark*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 1, 5 f.; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 5–6, 10; *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 98, 126–128. Auch *Stark/Magin/Jürgens*, Ganz meine Meinung?, August 2017, S. 179–186 kommen nicht zu eindeutigen Ergebnissen. Dabei ist zu berücksichtigen: Die Durchführung aussagekräftiger Untersuchungen ist äußerst voraussetzungsvoll. Ausgangspunkte, Parameter und Kausalitätsbeziehungen der Meinungsbildung sind derart komplex, das Nutzungsverhalten und die technische Funktionsweise der verschiedenen Filterdienste so divers, dass verallgemeinerbare und eindeutige Aussagen nur bedingt möglich sein werden, so auch *Bakshy/Messing/Adamic*, Science 348 (2015), 1130 f.;

Personalisierte Filterungen werden zunehmend auch auf Streamingdiensten, Mediatheken oder Online-Auftritten von Tageszeitungen eingesetzt. Fragen der Meinungs- und Informationsfreiheit stellen sich hier in weit geringerem Maße, da diesen keine Intermediärfunktion zukommt.[37]

a) Plattformregulierung zur Regulierung autonomer Systeme

Regulative Gegenmaßnahmen setzen vor allem bei den Online-Plattformen an. Eine Regulierung autonomer Systeme ist damit nur teilweise verbunden. Diskutiert werden etwa kartell- und marktrechtliche Maßnahmen,[38] Löschungs- und Moderationspflichten[39] sowie Neutralitätsgebote und Diskriminierungs-

---

Ignatidou, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019, S. 19. Zur methodischen Kritik an den durchgeführten Studien aufgrund mangelnder Differenzierung siehe etwa *Cornils*, AfP 49 (2018), 377, 380; *Ingold*, MMR 23 (2020), 82, 83 f., sowie *Stark/Stegmann*, Are Algorithms a Threat to Democracy?, AW AlgorithmWatch gGmbH, 26.05.2020, S. 22; so auch *Flaxman/Goel/Rao*, Public Opinion Quarterly 80 (2016), 298, 307–318; *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019, S. 19. Auch ist fraglich, inwieweit eine unterschiedliche nationale Prägung einer Verallgemeinerung der Studienergebnisse entgegensteht; dies heben hervor *Stöcker/Lischka*, in: Mohabbat-Kar/Thapa/Parycek (Hrsg.), (Un) berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Juni 2018, S. 364, 385 f.; *Zuiderveen Borgesius/Trilling/Möller u.a.*, Internet Policy Rev. 5 (2016), 1, 8. Auch die Verflechtungen mit analogen oder digitalen Alternativangeboten sind unklar, vgl. die Studienergebnisse bei *Welbers/Opgenhaffen*, New Media & Society 20 (2018), 4728, 4743–4745, so auch *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019, S. 19. Problematisch ist zudem, dass die Terme und Phänomene von Filterblasen und Echokammern teilweise ganz unterschiedlich verstanden werden, vgl. *Stark/Stegmann*, Are Algorithms a Threat to Democracy?, AW AlgorithmWatch gGmbH, 26.05.2020, S. 22.

[37] So auch *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 27.

[38] Siehe etwa *Dörr/Natt*, ZUM 58 (2014), 829, 842–844; *Paal*, ZRP 48 (2015), 34, 35 f. Da das Kartellrecht allein den Schutz des freien Wettbewerbs zum Ziel hat, ergeben sich gewisse Irritationen und Inkohärenzen, wenn dieses als meinungs- und informationssicherndes Rechtsinstrument dienen soll. Problematisch ist überdies, dass es um die Beschränkung von Meinungsmacht geht, während das Kartellrecht auf Marktmacht abstellt. Kritisch etwa *Danckert/Mayer*, MMR 13 (2010), 219–222; *Koreng*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 245, 255; *Paal/Heidtke*, ZUM 64 (2020), 230, 237; *Schmid/Braam/Mischke*, MMR 23 (2020), 19, 20; *Schwartmann/Hermann/Mühlenbeck*, MMR 22 (2019), 498, 499; *Cornils*, AfP 49 (2018), 377, 387; *Dörr/Natt*, ZUM 58 (2014), 829, 843 f.

[39] Im deutschen Recht umgesetzt im NetzDG, zur Regelung auf unionaler Ebene – dem DSA – siehe sogleich. Löschende Inhalte sind dabei solche, die gegen Strafvorschriften verstoßen – relevant sind damit insbesondere die Ehrverletzungsdelikte nach §§ 185 ff. StGB sowie der Tatbestand der Volksverhetzung nach § 130 StGB. Eine Auflistung relevanter Straftatbestände findet sich in § 1 Abs. 3 NetzDG. Siehe zu derartigen Regulierungsvor-

verbote von Beiträgen.[40] Eine Regulierung autonomer Systeme erfolgt hierdurch nicht. Autonome Systeme sind aber adressiert, soweit Vorgaben zu den Filterinhalten, dann also zum Lösungsalgorithmus, gemacht werden und neben die Personalisierung weitere Kriterien treten sollen, die auf eine Diversifikation des Informationsangebots abzielen.[41] Vorgeschlagen wird etwa die Ergänzung profilbasierter Filterungen um nicht profilbasierte Parameter[42] oder Randomisierungsverfahren.[43] Auch über substantielle Qualitätsanforderungen an das Informationsangebot wird nachgedacht.[44] Autonome Systeme werden auch unmittelbar reguliert, soweit Offenlegungsplichten hinsichtlich der Filterme-

schlägen *Nolte*, ZUM 21 (2017), 552–564; *Pille*, NJW 71 (2018), 3545–3550; *Oswald*, in: Grabenwarter/Holoubek/Leitl-Staudinger (Hrsg.), Regulierung von Kommunikationsplattformen, 2022, S. 67, 81–85; *Gärner*, in: Grabenwarter/Holoubek/Leitl-Staudinger (Hrsg.), Regulierung von Kommunikationsplattformen, 2022, S. 89, 98–101; *Martini*, Blackbox Algorithmus, 2019, S. 215–221. Siehe zur verfassungsgemäßen Gebotenheit etwa *Schimmele*, Staatliche Verantwortung für diskursive Integrität in öffentlichen Räumen, 2019.

[40] Vgl. *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, 297 f.; *Martini*, Blackbox Algorithmus, 2019, S. 222.

[41] Dies fordern etwa *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 208, so auch, wenngleich für Plattformen mit einem dominanten Marktanteil *Martini*, Blackbox Algorithmus, 2019, S. 224 („Mindestmaß an inhaltlicher Streubreite"). In diese Richtung auch *Dörr/Natt*, ZUM 58 (2014), 829, 845 f. Im Ansatz befürwortend *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 240. Siehe auch *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, 295 f.

[42] *Schwartmann/Hermann/Mühlenbeck*, MMR 22 (2019), 498, 501–503 „Zwei Säulen Modell"; *Schwartmann*, Zwei Säulen für die Demokratie, FAZ 26.05.2019, https://www.faz.net/aktuell/karriere-hochschule/forderung-fuer-demokratie-kontrolle-von-internet-und-algorithmen-16198048.html.; *Carson*, Journal of Science Policy and Governance 7 (2015), 1, 9 f.

[43] Vgl. *Martini*, Blackbox Algorithmus, 2019, S. 224. Umfassend zum politischen Verständnis und zu technischen Möglichkeiten der Mediendiversität *Helberger*, Journal of Information Policy 1 (2011), 441–469 Kritisch hinsichtlich der technischen Umsetzbarkeit und der grundrechtlichen Grenzen (unternehmerische Freiheiten der Plattformbetreiber und Informations- und Kommunikationsfreiheit der NutzerInnen) eines Diversitätsgebots *Ott*, MMR 2010, 301459.

[44] Für ein objektiviertes Punktesystem des Rankings treten ein *Danckert/Mayer*, MMR 13 (2010), 219, 221 f. In diese Richtung auch *Schulz/Dankert*, Die Macht der Informationsintermediäre, Friedrich-Ebert-Stiftung, S. 67 f. Kritisch hierzu *Ott*, MMR 2010, 301459; *Dörr/Natt*, ZUM 58 (2014), 829, 845. Insbesondere eine „Must Carry"-Pflicht, d.h. ein Gebot zur Anzeige als besonders meinungsrelevant erachteter Beiträge – dies meint dann regelmäßig durch öffentlich-rechtliche Rundfunkanstalten produzierte Beiträge – werden in der Literatur gemeinhin abgelehnt. Siehe nur *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 297 f.; *Martini*, Blackbox Algorithmus, 2019, S. 225; *Hartl*, Suchmaschinen, Algorithmen und Meinungsmacht, 2017, S. 219–221.

thodik, d.h. des Lösungsalgorithmus,[45] oder Mitbestimmungsoptionen der NutzerInnen hinsichtlich der Filterinhalte normiert werden sollen, etwa durch die Abwahloption profilbasierter Filterung (Opt-out-Option)[46] oder durch Einwirkungsrechte der NutzerInnen auf einzelne Filterkriterien.[47]

b) Digital Services Act als Instrument der Algorithmenregulierung

Mit dem Digital Services Package (Gesetz über digitale Dienste),[48] aufgespal-

[45] Gefordert wird vor allem, dass den NutzerInnen die (wesentlichen) Parameter der Filterung offengelegt werden. So etwa *Martini*, Blackbox Algorithmus, 2019, S. 222 f.; *Dörr/Schuster*, in: Stark/Dörr/Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, 2014, S. 262, 313 f.; *Schwartmann/Hermann/Mühlenbeck*, MMR 22 (2019), 498, 502; *Cornils*, AfP 49 (2018), 377, 386; *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 282 f. Die Beschränkung auf wesentliche Kriterien soll einen angemessenen Ausgleich mit den geschäftlichen Interessen der Plattformbetreiber herstellen. Statt der Transparenz fordern eine Beobachtbarkeit („observability") *Rieder/Hofmann*, Internet Policy Rev. 9 (2020), 1–28. Der MStV sieht bei Medienplattformen und Benutzeroberflächen eine Pflicht zur Offenlegung sämtlicher Kriterien vor (§ 85 S. 2 MStV), Medienintermediäre müssen zentrale Filterkriterien publik machen (§ 93 Abs. 1 Nr. 2 MStV) vor.

[46] Im Gegensatz zur staatlichen Vorgabe eines objektiviert-diversifizierten Informationsangebots in Ergänzung zur Personalisierung ist dies im Hinblick auf die Selbstbestimmung des Einzelnen und die unternehmerische Freiheit der Plattformbetreiber vorzugswürdig. Denn die betroffene Person hat es in der Hand, ob und inwieweit sie die Beschränkung des Informationsangebots durch die Personalisierung aufheben möchte. Den Plattformbetreibern wird auch nicht eine bestimmte Filtermethodik aufoktroyiert. Siehe zu diesen Erwägungen *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 293. Eine Opt-out-Option befürwortet auch *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019, S. 32.

[47] So etwa *Martini*, Blackbox Algorithmus, 2019, S. 223 f. Ebenso *Ignatidou*, AI-driven Personalization in Digital Media, The Royal Institute of International Affairs, International Security Department, Dezember 2019, S. 33 „right to modify their personalization".

[48] Ein Entwurf wurde im Dezember 2020 von der Europäischen Kommission vorgelegt. Der DMA ist am 01.11.2022 in Kraft getreten. Große Teile der Verpflichtungen aus der Verordnung treffen die Plattformbetreiber aber erst sechs Monate später, d.h. ab dem 2.5.2023. Der DSA ist am 16.11.2022 in Kraft getreten, der überwiegende Teil der Verordnung der Verordnung soll aber erst ab 24.2.2024 anwendbar sein. Zu Einschätzungen noch des Entwurfs aus der Literatur siehe etwa *Nettesheim*, Die unionsrechtliche Regulierung großer Internet-Plattformen, Bundestag, 11.2.2021; *Picht/Richter*, The proposed EU digital services regulation 2020: data desiderata, September 2021; *Badesow*, ZEuP 29 (2021), 217–226; *Wagner/Janssen*, A first impression of regulatory powers in the Digital Services Act, Verfassungsblog, 04.01.2021.

ten in den Digital Markets Act (DMA)[49] und den Digital Services Act (DSA)[50] hat die Europäische Union eine eigene Regelung von Online-Plattformen geschaffen. Der DMA beinhaltet allein markt- und kartellrechtliche Vorschriften,[51] von Interesse für die Regulierung ist daher allein der DSA, der ein gestuftes Regulierungssystem[52] für allgemeine Vermittlungsdienste, Hosting-Dienste, Online-Plattformen[53] und sehr große Online-Plattformen bzw. Suchdienste[54] vorsieht.[55] Relevant für die Regulierung autonomer Systeme[56] sind

[49] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG vom 27.10.2022 (ABl L 277/1).

[50] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 vom 12.10.2022 (ABl L 265/1).

[51] Siehe die Zielvorgabe in Art. 1 Abs. 1 DMA: Die Verordnung soll absichern, dass die Märkte im digitalen Sektor bestreitbar und fair bleiben. Vgl. eingehend zum DMA *Nettesheim*, Die unionsrechtliche Regulierung großer Internet-Plattformen, Bundestag, 11.2.2021, S. 4–6; *Badesow*, ZEuP 29 (2021), 217, 220 f. Gleichwohl wurde der DMA nicht auf die kartellrechtliche Kompetenz der Art. 103 AEUV, sondern auf die Binnenmarktkompetenz des Art. 114 AEUV gestützt; dies hatte politische Gründe, inhaltlich entspricht die Vorschrift typischen kartellrechtlichen Regulierungsmethodiken.

[52] Siehe nur *Mantelero*, Fundamental rights impact assessments in the DSA, Verfassungsblog, 01.11.2022; maßgeblich ist dabei vor allem die Größe des Vermittlungsdienstes, nicht ein einzelfallbezogenes, sachlich begründetes Risikoverständnis, kritisch hierzu *Laux/Wachter/Mittelstadt*, CLSR 43 (2021), 1, 7 sowie *Mantelero*, Fundamental rights impact assessments in the DSA, Verfassungsblog, 01.11.2022. Kritisch auch *Nettesheim*, Die unionsrechtliche Regulierung großer Internet-Plattformen, Bundestag, 11.2.2021, S. 16: „Der Betrieb einer sehr großen Online-Plattform wird als gefährliche Tätigkeit eingestuft, ohne dass allerdings ein hinreichend spezifisches Gefahrenkonzept entwickelt wird". Instruktive Übersicht über die Regulierungsabstufung bei *Schmid/Grewe*, MMR 24 (2021), 279. Siehe auch *Spindler*, Gewerblicher Rechtsschutz und Urheberrecht 123 (2021), 545 „Pyramidenmodell".

[53] Legaldefinition in Art. 3 lit. i) DSA: „Hostingdienst, der im Auftrag eines Nutzers Informationen speichert und öffentlich verbreitet".

[54] Legaldefiniert in Art. 3 Nr. 1 j) DSA: „Vermittlungsdienst, der es Nutzern ermöglicht, in Form eines Stichworts, einer Spracheingabe, einer Wortgruppe oder einer anderen Eingabe Anfragen einzugeben, um prinzipiell auf allen Websites oder auf allen Websites in einer bestimmten Sprache eine Suche zu einem beliebigen Thema vorzunehmen und Ergebnisse in einem beliebigen Format, in dem Informationen im Zusammenhang mit dem angeforderten Inhalt zu finden sind, angezeigt zu bekommen".

[55] Im Englischen „Very Large Online Platforms" (VLOPs). Hierzu zählen nach Art. 33 Abs. 1 DSA solche Online-Plattformen oder -Suchdienste, die monatlich durchschnittlich eine Zahl von mindestens 45 Millionen aktiven NutzerInnen innerhalb der Europäischen Union haben und von der Europäischen Kommission in einem förmlichen Beschluss (nach Art. 33 Abs. 4 DSA) als solche benannt wurden.

[56] Zu den Potentialen des DSA für die Regulierung von Systemen Künstlicher Intelligenz siehe auch eingehend, wenngleich noch zum Entwurf das DSA, *Kalbhenn*, ZUM 65 (2021), 663, 671–674.

dabei die Vorschriften zu manipulativen Maßnahmen, Werbemaßnahmen Empfehlungssystemen (aa)). sowie zu Einführung eines Risikomanagementsystems (bb)).[57]

aa) Regelungen zu Dark-Pattern-Verfahren, Empfehlungssystemen und Werbemaßnahmen

Der DSA etabliert ein Verbot von täuschenden, manipulativen oder auf sonstige Weise die freie Willensbildung beeinflussenden Praktiken (Dark-Pattern-Verfahren).[58] Besondere Vorschriften gelten für Werbemaßnahmen: Diese sind kenntlich zu machen,[59] überdies müssen aussagekräftige Informationen über die „wichtigsten" Parameter der Filterung bereitgestellt werden.[60] Werbemaßnahmen dürfen nicht auf Profile mit sensiblen Inhalten gestützt werden,[61] die personalisierte Werbung bleibt damit aber dem Grunde nach zulässig.[62] Für Empfehlungssysteme[63] sind Transparenzpflichten vorgesehen: Anbieter werden verpflichtet, die wichtigsten Parameter und die Gründe für die relative Bedeutung dieser Parameter darzulegen.[64] Kritisiert wird hieran, dass der DSA offen lässt, welche Parameter als die „wichtigsten" gelten sollen.[65] Auch sieht

[57] Der erste Teil des DSA beschäftigt sich mit Regelungen zum Umgang mit illegalen Inhalten und stellt keine Regulierung autonomer Systeme dar.

[58] Art. 25 DSA. Ergänzend Erwägungsgrund 67 des DSA. Siehe hierzu *Raue/Heesen*, NJW 75 (2022), 3537, 3541 f.

[59] Siehe Art. 26 Abs. 1 lit. a) DSA. Bei sehr großen Online-Plattformen – hierzu sogleich – ist zudem ein Archiv über erfolgte Werbemaßnahmen zu erstellen, Art. 39 DSA. Diese Pflicht bestand bereits nach alter Rechtslage, Art. 7 Abs. 2 UGP-RL; § 5 a IV UWG. Siehe hierzu auch *dies.*, NJW 75 (2022), 3537, 3542.

[60] Siehe Art. 26 Abs. 1 lit. d) DSA.

[61] Art. 26 Abs. 3 DSA.

[62] Im Gesetzgebungsverfahren war ein Verbot für personalisierte Werbemaßnahmen diskutiert worden, vgl. *Buiten*, JIPITEC 12 (2021), 361, 376. Ein solches Verbot befürworten *Laux/Wachter/Mittelstadt*, CLSR 43 (2021), 1, 11. sowie der *Europäischer Datenschutzausschuss*, Opinion 1/2021 on the Proposal for a Digital Services Act, 10.02.2021, S. 16. Ein solches Verbot ablehnend *Nettesheim*, Die unionsrechtliche Regulierung großer Internet-Plattformen, Bundestag, 11.2.2021, S. 17; *Helberger/van Drunen/Vrijenhoek u.a.*, Regulation of news recommenders in the Digital Services Act, 26.2.2021.

[63] Legaldefinition in Art. 3 lit. s) DSA: „Ein vollständig oder teilweise automatisiertes System, das von einer Online-Plattform verwendet wird, um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren, auch infolge einer vom Nutzer veranlassten Suche, oder das auf andere Weise die relative Reihenfolge oder Hervorhebung der angezeigten Informationen bestimmt".

[64] Siehe Art. 27 Abs. 1 und 2 DSA.

[65] So auch *Buri/van Hoboken*, The Digital Services Act (DSA) proposal, University of Amsterdam, 28.10.2021, S. 38 f.; *Helberger/van Drunen/Vrijenhoek u.a.*, Regulation of news recommenders in the Digital Services Act, 26.2.2021. Kritisch auch *Europäischer Datenschutzausschuss*, Opinion 1/2021 on the Proposal for a Digital Services Act, 10.02.2021, S. 15, demzufolge sämtliche, nicht nur die wesentlichen Parameter genannt und Einblicks-

der DSA verschiedene Einwirkungsoptionen für NutzerInnen vor. Sofern mehrere Filteroptionen zur Verfügung stehen, etwa nach Relevanz, Veröffentlichungszeitpunkt oder persönlicher Präferenz, so müssen Anbieter eine Funktion vorsehen, die den NutzerInnen eine Auswahl und Änderung der von ihnen bevorzugten Filteroption ermöglicht.[66] Werden den NutzerInnen Änderungs- und Einflussnahmeoptionen hinsichtlich der wichtigsten Parameter eingeräumt, ist auch hierüber zu informieren.[67] Eine Pflicht, verschiedene Filteroptionen oder Einflussnahmemöglichkeiten der NutzerInnen hinsichtlich der Filterparameter anzubieten, besteht aber nicht.[68]

Ein besonderes Regulierungsregime gilt für sehr große Plattformen bzw. sehr große Suchmaschinen.[69] Die Transparenzpflichten reichen hier weiter: Plattformbetreiber haben dem Koordinator digitaler Dienste[70] sowie der Europäischen Kommission umfassend Zugang zu ihren Diensten zu verschaffen,[71] sie müssen diesen die Gestaltung, Logik, Funktionsweise und Tests der algorithmischen Systeme einschließlich der Empfehlungssysteme erläutern.[72] Zudem ist bestimmten akkreditierten Forschern Zugang zu Daten zu gewähren, um diesen eine wissenschaftliche Erforschung systemische Risiken zu ermöglichen.[73] Für personalisierte Werbemaßnahmen ist ein öffentlich einsehbares

---

rechte in verwendete Profile normiert werden sollten. Die Europäische Kommission hat allerdings 2020 Leitlinien für die Transparenz bei Ranking-Diensten erstellt; diese können zumindest als Anhaltspunkte dienen, welche Parameter als „wichtigste" gelten können, siehe *Europäische Kommission*, Leitlinien zur Transparenz des Rankings gemäß der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates, 8.12.2020.

[66] Art. 27 Abs. 2 DSA. Für sehr große Online-Plattformen – siehe sogleich – ist in Art. 38 DSA darüber hinaus eine Pflicht zur Bereitstellung einer nicht-profilbasierten Filtermethode vorgesehen. Art. 27 Abs. 2 DSA geht damit nicht notwendig davon aus, dass die Filtermethode eine personalisierte ist.

[67] Art. 27 Abs. 1 DSA a.E.

[68] *Buri/van Hoboken*, The Digital Services Act (DSA) proposal, University of Amsterdam, 28.10.2021, S. 38; *Helberger/van Drunen/Vrijenhoek u.a.*, Regulation of news recommenders in the Digital Services Act, 26.2.2021. Kritisch hierzu *Helberger/van Drunen/Vrijenhoek u.a.*, Regulation of news recommenders in the Digital Services Act, 26.2.2021. Die Etablierung einer derartigen Pflicht fordert *Europäischer Datenschutzausschuss*, Opinion 1/2021 on the Proposal for a Digital Services Act, 10.02.2021, S. 16.

[69] Definition siehe oben Kapitel 3 B. I. 1. b) am Anfang. Diese haben, wie beschrieben, Gatekeeper und Intermediär-Funktion, die nachteiligen Effekte der automatisierten Filterung wirken hier besonders stark. Siehe Erwägungsgründe 75, 76, 79. Vgl. auch, wenngleich noch zum Entwurf, *Spindler*, Gewerblicher Rechtsschutz und Urheberrecht 123 (2021), 653, 658; *Laux/Wachter/Mittelstadt*, CLSR 43 (2021), 1, 6 f.

[70] Dabei handelt es sich um eine von den Mitgliedstaaten jeweils zu benennende Behörde, Art. 49 Abs. 2 DSA. Der Koordinator übernimmt Aufgaben der Überwachung, Durchsetzung und Beratung, siehe Art. 49 Abs. 2, Art. 51 DSA.

[71] Art. 40 Abs. 1 DSA.

[72] Art. 40 Abs. 3 DSA.

[73] Art. 40 Abs. 4–13 DSA.

Archiv anzulegen.[74] Schließlich gelten für Empfehlungssysteme ergänzende Vorschriften: Anbieter werden verpflichtet, eine Filtermethode, die nicht auf Profiling beruht, bereitzustellen.[75]

bb) Risikomanagementsystem

Kernstück der Regulierung sehr großer Plattformen ist ein Risikomanagementsystem.[76] Der DSA verpflichtet Betreiber, jährlich systemische Risiken zu ermitteln und effektive Minderungsmaßnahmen zu ergreifen.[77] Es geht damit nicht um Einzelfälle und auch nicht um Einzelpersonen, der Fokus liegt auf gesamtgesellschaftlichen, systemimmanenten Fehlentwicklungen.[78] Der technische Aufbau der Plattformen ist für die Risikobewertung ebenso relevant wie ihre praktische Nutzung und andere Aspekte.[79] Zur Spezifizierung systemischer Risiken werden vier Fallgruppen benannt: die Verbreitung rechtswidriger Inhalte, nachteilige Auswirkungen auf die Grundrechte, nachteilige Auswirkungen auf die gesellschaftliche Debatte und den Wahlprozess sowie nachteilige Folgen in Bezug auf die körperliche und geistige Integrität.[80] Die Gestaltung der eingesetzten algorithmischen Systeme ist als risikorelevantes Merkmal explizit benannt, das Risikomanagementtool lässt sich daher (auch) als algorithmenspezifisches begreifen.[81] Die Offenheit des Risikobegriffs soll Raum schaffen für den Einbezug sämtlicher, auch erst noch bekannt werdender sowie

---

[74] Art. 39 DSA.

[75] Art. 38 DSA.

[76] Es handelt sich um ein aus dem Finanzmarktsektor bekanntes Regulierungsinstrument, vgl. *Spindler*, Gewerblicher Rechtsschutz und Urheberrecht 123 (2021), 653, 658.

[77] Art. 34, 35 DSA. Vorgesehen ist darüber hinaus ein spezifischer Krisenreaktionsmechanismus, der bestimmte Anforderungen für das Risikomanagementsystem in akuten Krisensituationen aufstellt, Art. 36 DSA. Für diese Risikoprüfungen sind Berichte zu erstellen, die zu veröffentlichen sind, Art. 42 DSA. Die Einhaltung dieser und weiterer Pflichten wird durch eine jährliche unabhängige Prüfung kontrolliert, Art. 37 DSA. Vgl. zu diesem System der Auditierung des Risikomanagements eingehend *Laux/Wachter/Mittelstadt*, CLSR 43 (2021), 1, 7–9.

[78] Vgl. *Geese*, Why the DSA could save us from the rise of authoritarian regimes, Verfassungsblog, 08.11.2022.

[79] Siehe Art. 34 Abs. 2 DSA. Auf diese systematische Betrachtung der Plattformen siehe auch *Leerssen*, Algorithm Centrism in the DSA's Regulation of Recommender Systems, Verfassungsblog, 29.03.2022.

[80] Siehe Art. 23 Abs. 1 UAbs. 2 lit. a)-d) DSA.

[81] Art. 34 Abs. 2 lit. a) DSA. Siehe auch Erwägungsgrund 84. Nicht allein die Plattformen oder Filterdienste, sondern die Algorithmen selbst sind damit (auch) Gegenstand der Risikoprüfung. Vgl. zu dieser „Algorithmenzentriertheit" auch *Leerssen*, Algorithm Centrism in the DSA's Regulation of Recommender Systems, Verfassungsblog, 29.03.2022. Siehe auch *Flamme*, MMR 24 (2021), 770, 774, der im Rahmen der Risikoprüfung des DSA ebenso die Filteralgorithmen in den Vordergrund stellt.

neu entstehender Risiken.[82] Ähnliche Erwägungen gelten für die Risikominderungsmaßnahmen, die ebenfalls nur sehr vage benannt sind.[83] Die fehlende Spezifizierung von Risikokonzepten und Minderungsmaßnahmen wird in der Literatur vielfach kritisiert.[84]

2. *Verbraucherschutz und marktregulative Ansätze*

Das Verbraucherschutzrecht fokussiert zum einen auf personalisierte Werbemaßnahmen.[85] Problematisiert wird dabei vor allem, dass VerbraucherInnen weder die Werbemaßnahme noch ihre Personalisierung bekannt ist, auch die einzelnen Persönlichkeitsmerkmale nicht, auf die die Werbemaßnahme gestützt ist.[86] Kritisiert wird auch, dass sich personalisierte Werbemaßnahmen nicht abschalten lassen.[87]

Auch in der Automation der Vertragsverhandlung und -gestaltung[88] wird problematisiert, dass VerbraucherInnen im Einzelfall von der Automatisierung bzw. Personalisierung der Vertragsanbahnung und -gestaltung keine Kenntnis

---

[82] *Raue/Heesen*, NJW 75 (2022), 3537, 3543: „Der DSA enthält eine Reihe von neuen Regelungen, deren Trag- und Reichweite noch nicht ganz absehbar sind und die aufgrund von vielen unbestimmten Rechtsbegriffen von der Rechtsprechung, vor allem vom EuGH, näher ausgestaltet werden müssen. Das ermöglicht eine entwicklungsoffene, grundrechtsgeleitete Weiterentwicklung der Plattformregulierung".

[83] Der DSA benennt in Art. 35 Abs. 1 DSA eine anekdotische Auswahl möglicher Risikominderungsmaßnahmen, etwa die Beschränkung von Werbeanzeigen oder die Sicherstellung von Einzelinformationen (siehe hierzu Art. 35 Abs. 1 lit. e], lit. k] DSA). Siehe auch die Auflistung von Gegenmaßnahmen in Erwägungsgrund 87.

[84] Kritisch etwa *Mantelero*, Fundamental rights impact assessments in the DSA, Verfassungsblog, 01.11.2022. Siehe auch *Buri/van Hoboken*, The Digital Services Act (DSA) proposal, University of Amsterdam, 28.10.2021, S. 34–36; *Mantelero*, Fundamental rights impact assessments in the DSA, Verfassungsblog, 01.11.2022; *Nettesheim*, Die unionsrechtliche Regulierung großer Internet-Plattformen, Bundestag, 11.2.2021, S. 15 f. Spezifisch zur Offenheit der Minderungsmaßnahmen vgl. *Keller*, The EU's new Digital Services Act and the Rest of the World, Verfassungsblog, 07.11.2022; *Peukert*, Five Reasons to be Skeptical About the DSA, Verfassungsblog, 31.08.2021. Für eine Übertragung der im KI-Gesetz-E benannten Anforderungen, dort hinsichtlich Hochrisikosystemen, spricht sich *Kalbhenn*, ZUM 65 (2021), 663, 671 f. aus. Sehr kritisch auch *Laux/Wachter/Mittelstadt*, CLSR 43 (2021), 1, 5, 10, die die praktische Wirksamkeit des DSA umfassend in Zweifel ziehen.

[85] Siehe hierzu eingehend Kapitel 1 C. II.

[86] *Mik*, Law Innov. Technol. 8 (2016), 1, 12 spricht von einem „new type of information asymmetrie". Vgl. auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 239 f. Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 104 f.; *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 58 f.

[87] Vgl. *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, S. 239–240, 242–243.

[88] Siehe hierzu die Beispielsfälle der automatisierten Kreditentscheidung und der personalisierten Preisbildung unter Kapitel 1 C III. Zu Beeinträchtigungen der Privatautonomie durch Informationsasymmetrien siehe Kapitel 2 C. I. 1.

haben,[89] vor allem aber, dass die Entscheidungsgründe für die betroffene Person intransparent bleiben.[90] Befürchtet wird überdies, dass für den Markt unattraktive, d.h. vor allem wirtschaftlich schwach gestellte Konsumenten, umfassend aus dem Markt gedrängt werden könnten.[91]

Die Festlegung regulativer Gegenmaßnahmen ist anspruchsvoll, da die Privatautonomie gerade gestattet, Wissens-, Markt- oder Verhandlungsvorteile auszunutzen[92] und die Umstände und Motivationen einer Vertragsanbahnung oder eines Vertragsschlusses geheim zu halten.[93] Die ungleiche Verteilung von Wissen ist gerade typisches Risiko in einer liberalen Marktordnung.[94] Dass VerbraucherInnen fähig sind, manipulative Werbemaßnahmen abzuwehren, ist Prämisse einer auf Privatautonomie beruhenden Marktordnung. Der Einsatz subtil wirkender Werbestrategien ist nicht per se ablehnungswürdig.[95] Die Privatautonomie verschafft Unternehmen zudem gerade das Recht, nicht mit jeder Person kontrahieren zu müssen und – auch aus sozialethisch verwerflichen Gründen – zwischen VerbraucherInnen differenzieren zu können.[96] Es fällt daher schwer, in den beschriebenen Konstellationen klare Grenzen zu ziehen.[97]

---

[89] So *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 407 f.; *Dornis*, ZfPW 8 (2022), 310, 313. Vgl. auch *Tillmann/Vogt*, VuR 33 (2018), 447, 451–452, 454.

[90] Vgl. *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 406. Insbesondere wird die Intransparenz des verwendeten Profils angemahnt, so etwa *Dornis*, ZfPW 8 (2022), 310, 313.

[91] Eingehend hierzu Kapitel 2 C II. 2. Siehe auch *Schermer*, CLSR 27 (2011), 45, 47. Zu den Gefährdungen der Verbraucherwohlfahrt eingehend *Hofmann*, WiRO 62 (2016), 1074, 1080–1082; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 224–230.

[92] So auch *Mik*, Law Innov. Technol. 8 (2016), 1, 26 f. Werbemaßnahmen an sich stellen daher regelmäßig keine Beeinträchtigung der Privatautonomie dar, vgl. bereits die Untersuchung bei *Lerche*, Werbung und Verfassung, 1967.

[93] Vgl. *Hofmann*, WiRO 62 (2016), 1074, 1080.

[94] Vgl. *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1023: „plenty of border cases or de minimis infractions". In diese Richtung auch *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 58.

[95] *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 237. Ähnlich *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1032: „Not every impulse purchase, upsell, or emotional pitch threatens consumer autonomy in any deep sense". Die VerbraucherInnen könnten daher Resilienz- und Selbstschutzmechanismen entwickeln, so auch *Zarsky*, Theoretical Inquiries in Law 20 (2019), 157, 184.

[96] Statt vieler Dürig/Herzog/Scholz, GG/*Di Fabio*, Art. 2 Abs. 1 Rn. 101–102.

[97] So auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 232, 237; *Zarsky*, Theoretical Inquiries in Law 20 (2019), 157, 184. Explizit zur personalisierten Preisbildung *Hofmann*, WiRO 62 (2016), 1074, 1081. Zum Unterschied zwischen den bekannten Beeinträchtigungen der Privatautonomie der VerbraucherInnen und den neuartigen Gefährdungen durch autonome Systeme siehe ausführlich Kapitel 2 C. IV. e) sowie Kapitel 2 A. I. 2. Der Unterschied liegt vor allem in der Detailtiefe, Dynamik, Ubiquität, Subtilität, Intransparenz und beschränkten Einwirkungsmöglichkeit. Siehe hierzu auch *Mik*, Law Innov. Technol. 8 (2016), 1, 14-15, 24, 27; *Dornis*, ZfPW 8 (2022), 310, 312 f. sowie *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 238–240; *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 58 f.

Um die Grenzen des Zulässigen zu definieren, wird vielfach das Wettbewerbs- und Kartellrecht herangezogen. Personalisierte Werbung soll im Einzelfall unlauteres Verhalten im Sinne des § 3 Abs. 2 UWG darstellen und dann also unzulässig sein,[98] die personalisierte Preisbildung soll nach § 5a Abs. 2 UWG unzulässig sein, wenn sie verdeckt erfolgt.[99] Eine Ausnutzung marktbeherrschender Stellung soll vorliegen, wenn Unternehmen mit Marktmacht die Technologie desselben Anbieters nutzen, um personalisierte Preise zu bilden.[100] Vielfach wird über eine Anwendung und Ausweitung typischer verbraucherschützender Instrumente des Zivilrechts nachgedacht. Um VerbraucherInnen vor werbebezogenen manipulativen Einflussnahmen zu schützen, wird die Einführung spezifischer Widerrufsrechte vorgeschlagen.[101] Auch die Einführung von Opt-out-Rechten hinsichtlich personalisierter Anwendungen erscheint vielen als sinnvolles Schutzinstrument.[102] VerbraucherInnen sollen

[98] Herausfordernd gestaltet sich dabei das Bild vom „durchschnittlichen Verbraucher", der als Maßstab dafür gilt, welche Einflussnahmen VerbraucherInnen hinnehmen müssen und welche nicht. *Ebers*, MMR 21 (2018), 423, 424 f. plädiert für eine Abkehr von dieser Orientierung an DurchschnittsverbraucherInnen und tritt für eine an den individuellen VerbraucherInnen ausgerichtete Einzelfallprüfung ein. Ähnliche Erwägungen stellen *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 65–67; *Mik*, Law Innov. Technol. 8 (2016), 1, 32–36 für die Richtlinie 2005/29 / EG (UPG-Richtlinie) an. Vgl. allgemein zur Einordnung personalisierter Werbung als unlauteres Verhalten *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 59.

[99] So *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 407 f.; *Hofmann*, WiRO 62 (2016), 1074, 1080; *Tillmann/Vogt*, VuR 33 (2018), 447, 452. In diese Richtung auch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 228. Kritisch dagegen *Tietjen/Flöter*, GRUR-Prax 9 (2017), 546, 547 f. Teilweise wird auch für eine Pflicht zur Angabe des Durchschnittspreises, d.h. des Referenz- und Vergleichspreises plädiert, so etwa *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 408. Ablehnend *Tillmann/Vogt*, VuR 33 (2018), 447, 452 f.; *Tietjen/Flöter*, GRUR-Prax 9 (2017), 546, 548.

[100] Die Nutzung derselben Datensätze und Algorithmen kann dazu führen, dass VerbraucherInnen marktübergreifend ähnliche Preisen erhalten, was faktisch einer Preisabsprache entspricht. Eingehend *Tillmann/Vogt*, VuR 33 (2018), 447, 454. Siehe auch *Tietjen/Flöter*, GRUR-Prax 9 (2017), 546, 547. Siehe hierzu auch EuGH, Urteil v. 21.01.2016, Rs. C-74/14, CLI:EU:C:2016:42 – *Eturas*. zur Verwendung der Software eines Anbieters für die Berechnung von Rabattobergrenzen.

[101] Zu diesem Vorschlag *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 233 f. Kritisch hierzu *Ebers*, MMR 21 (2018), 423, 426; *Dornis*, ZfPW 8 (2022), 310, 340.

[102] *Gleixner*, VuR 35 (2020), 417, 420.

personalisierte Werbemaßnahmen[103] oder die Automatisierung von Vertragsgestaltungen abwählen können.[104]

Im Zentrum stehen Maßnahmen zur Überwindung der bestehenden Informationsasymmetrien. Vor allem wird eine Kennzeichnungspflicht gefordert.[105] Für die personalisierte Preisbildung ist eine solche, zumindest für Fernabsatzgeschäfte, in der Verbraucherrichtlinie 2011/83/EU[106] bereits vorgesehen.[107] Auch hinsichtlich der personalisierten Werbung ist eine solche allgemeine Offenlegungspflicht in der Diskussion.[108] Gefordert werden überdies Einblicksrechte der VerbraucherInnen in „ihre" Profile, die den personalisierten Maßnahmen zugrunde liegen.[109] Bei der Automatisierung von Vertragsanbahnung und -abschluss sollen wesentliche Entscheidungsparameter offengelegt werden, zumindest im Falle nachteiliger Entscheidungen.[110] Selbiges wird für personalisierte Werbemaßnahmen gefordert.[111] Vereinzelt wird auch für Verbote eingetreten; insbesondere bei personalisierten Werbemaßnahmen wird immer

---

[103] *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 242 f. *Calo*, Geo. Wash. L. Rev. 82 (2014), 995, 1047 schlägt eine Opt-out-Lösung für einen gänzlichen Ausstieg aus dem personalisierten „marketing ecosystem" vor. Statt eigene Daten müssten VerbraucherInnen für einzelne Dienste eine finanzielle Gegenleistung erbringen.

[104] Etwa bei der personalisierten Preisbildung *Paal*, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), 43, 49; *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 228–230; *Dornis*, ZfPW 8 (2022), 310, 341.

[105] Siehe nur – dies im Rahmen personalisierter Preisbildung – *Dornis*, ZfPW 8 (2022), 310, 340; *Tillmann/Vogt*, VuR 33 (2018), 447, 454; *Tietjen/Flöter*, GRUR-Prax 9 (2017), 546, 548; *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 408 f.

[106] Siehe Art. 6 Abs. 1 lit. e) der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, L 304/64.

[107] Diese wurde in § 312d Abs. 1 BGB iVm Art. 246a § 1 Ab. 1 Nr. 6 EGBGB in deutsches Recht umgesetzt. Zur Bewertung und Kritik dieser Vorschrift vgl. etwa *Gleixner*, VuR 35 (2020), 417–421. Sehr umstritten ist, ob auch auf Referenzpreise, d.h. den Preis ohne eine Personalisierung, hinzuweisen ist. Gemeinhin wird dies abgelehnt, so etwa *Tietjen/Flöter*, GRUR-Prax 9 (2017), 546, 548; aA *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 408.

[108] Siehe bereits für die Plattformregulierung unter Kapitel 3 B. I. 1. a).Vgl. auch *Kellner*, Die Regulierung der Meinungsmacht von Internetintermediären, 2019, S. 281.

[109] *Paal*, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), 43, 53. Sehr allgemein die Offenlegung der „zugrundeliegenden Parameter" fordert der *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 67.

[110] So für die personalisierte Preisbildung *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 408. Zumindest gegenüber staatlichen Akteuren *dies.*, VuR 2016, 403, 409. Kritisch *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 241 f.

[111] Im Grundsatz befürwortend, im Ergebnis aber kritisch aufgrund zu erwartender Informationsüberforderung *Mik*, Law Innov. Technol. 8 (2016), 1, 31 f.

wieder für Untersagungen geworben.[112] Bei automatisierten Vertragsgestaltungen sind Zulassungskontrollen in der Diskussion.[113] Teilweise wird auch generell für die Untersagung der Verwendung bestimmter Profilinhalte eingetreten, soweit diese sich im Hinblick auf die Autonomie, Diskriminierung oder allgemeine Wohlfahrt als besonders sensibel darstellen.[114]

3. Antidiskriminierungsrecht

Um den durch autonome Systeme ausgelösten Diskriminierungen zu begegnen,[115] kann schlicht das bestehende Antidiskriminierungsrecht auf autonome Systeme angewendet werden.[116] Um den Diskriminierungsschutz auszuweiten, muss zunächst definiert werden, welche Diskriminierungen überhaupt uner-

---

[112] Allgemein für die personalisierte Werbung *Wågström*, Why Behavioral Advertising Should Be Illegal, Forbes 05.05.2019, https://www.forbes.com/sites/forbestechcouncil/2019/03/05/why-behavioral-advertising-should-be-illegal. Spezifisch für ein Verbot der Dark-Pattern-Analyse, die die „kritische Schwelle der Ausnutzung privatautonomer Gestaltungsfreiheit" überschreitet, *Martini/Drews/Seeliger u.a.*, ZfDR 1 (2021), 72 f. Für Verbote, allerdings nur in Einzelfällen, statt Transparenzpflichten tritt auch *Mik*, Law Innov. Technol. 8 (2016), 1, 32 ein.

[113] In diese Richtung *Martini*, Blackbox Algorithmus, 2019, S. 229–230, 350, der allgemein für eine Zulassungsprüfung von autonomen Systemen eintritt, die ein hohes Risikopotential aufweisen oder die die Lebensführung, die gesellschaftliche Stellung und die wirtschaftliche Situation der betroffenen Person erheblich beeinträchtigen können. Für ein Zulassungsverfahren personalisierter Preisbildung ganz allgemein tritt die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 179 ein. Die Einführung eines „Algorihtmen-TÜVs" befürwortet auch *Dornis*, ZfPW 8 (2022), 310, 343.

[114] So etwa *Martini*, Blackbox Algorithmus, 2019, S. 239, der die Untersagung der Verwendung von Merkmalen bei der personalisierten Preisgestaltung vorschlägt, die nach allgemeiner Wertung sozialethisch verwerflich sind, etwa der Gesundheitszustand oder eine persönliche Notlage. So auch *Ernst*, JZ 72 (2017), 1026, 1035, der sich zudem für ein Verbot der Verwendung von besonders sensiblen Persönlichkeitsmerkmalen ausspricht. Sehr allgemein für ein Verbot von „Profilbildungen bei besonders sensiblen personenbezogenen Daten" bei „kritischen Einsatzzwecken" *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 100.

[115] Eingehend Kapitel 2 C II. 1. a).

[116] Zum komplexen Verhältnis von Diskriminierungsschutz und Datenschutz siehe etwa *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1171–1173; *Martini*, Blackbox Algorithmus, 2019, S. 77–82; vgl. auch *Schreurs/Hildebrandt/Kindt u.a.*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 241 Es gibt vielfache Überschneidungen, siehe etwa Art. 9 DSGVO; überwiegend wird von einer Idealkonkurrenz ausgegangen. Zum Konkurrenzverhältnis sowie den unterschiedlichen Schutzbererichen, Zielrichtungen und Steuerungsmechanismen siehe ausführlich *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1154–1170.

wünscht sind. Denn im Einzelfall können diese sogar erwünscht sein.[117] Es bedarf daher einer bereichsspezifischen Regulierung.[118] Verboten werden könnten dann Diskriminierungseffekte einzelner Anwendungen, aber auch die Verwendung von Diskriminierungsmerkmalen im Modell und Profil.[119] Herausfordernd ist dabei, dass es technisch, wie ausgeführt, äußerst anspruchsvoll ist, diese Diskriminierungsverbote umfassend umzusetzen.[120] Vor allem Diskriminierungen durch vermeintlich neutrale Parameter (sogenannte Proxies)[121] stel-

[117] Vgl. auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 436. Nach der Ethnie unterscheidende Werbung kann sogar wünschenswert sein, etwa bei Lebensmittelwerbung, die die unterschiedlichen Ernährungsgewohnheiten bestimmter Bevölkerungsgruppen berücksichtigen. Verpflichtet sich ein Arbeitgeber im Recruiting-Verfahren etwa für die Frauenförderung, ist dies eine diskriminierungsrelevante Entscheidung, die aber in einer gesamtgesellschaftlichen Perspektive diskriminierungshemmend wirkt.

[118] Vgl. den Ansatz bei *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 14–18, der mögliche Diskriminierungen durch (selbstlernende) Algorithmen in verschiedenen Anwendungsbereichen darstellt. Einer undifferenzierten Ausweitung des Diskriminierungsschutzes stünde überdies der Grundsatz der Privatautonomie entgegen, hierzu *Martini*, Blackbox Algorithmus, 2019, S. 236–239.

[119] Vgl. etwa *Corbett-Davies/Goel*, The Measure and Mismeasure of Fairness, Stanford University, 14.8.2018, S. 17–19; *Martini*, Blackbox Algorithmus, 2019, S. 243. Hierbei wird jeweils nicht klar zwischen Modell und Profil unterschieden, sondern allgemein von dem Verbot der Diskriminierung durch Algorithmen bzw. autonome Systeme gesprochen. Explizit ein Verbot von Diskriminierungen bei der Modellbildung fordern *Schreurs/Hildebrandt/Kindt u.a.*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 241, 259.

[120] Die Konstruktion diskriminierungsfreier Algorithmen, die dann zu diskriminierungsfreien Modellen, Profilen und automatisierten Entscheidungen bzw. Steuerungen führen, ist Gegenstand umfassender interdisziplinärer, insbesondere informationstechnischer Forschung. Aus der Fülle an Vorschlägen und Arbeiten siehe etwa *Bender/Gebru/McMillan-Major u.a.*, in: Coscia (Hrsg.), Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2021, S. 610; *Corbett-Davies/Goel*, The Measure and Mismeasure of Fairness, Stanford University, 14.8.2018, S. 17–20; *Dwork/Hardt/Pitassi u.a.*, Fairness Through Awareness, 20.04.2011, S. 24–44; *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1170–1183; *Mehrabi/Morstatter/Saxena u.a.*, A Survey on Bias and Fairness in Machine Learning, 23.08.2019, S. 13–24; *Martini*, Blackbox Algorithmus, 2019, S. 230–249; *Ntoutsi/Fafalios/Gadiraju u.a.*, Bias in Data-driven AI Systems, 14.01.2020, S. 7–12 jeweils mit zahlreichen weiteren Nachweisen.

[121] Eingehend Kapitel 2 C. II. 1. a). So kann etwa der Wohnort als Proxy für die Ethnie dienen, wenn an diesem Wohnort hauptsächlich Personen dieser Ethnie wohnen. Vgl. zu derartigen mittelbaren Diskriminierungen mit weiteren Beispielen *Ernst*, JZ 72 (2017), 1026, 1032; *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1152 f.; *Martini*, JZ 72 (2017), 1017, 1018; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 107–109.

len vor Herausforderungen.[122] Bei menschlich unverständlichen algorithmischen Strukturen wird man Ursachen der Diskriminierung überhaupt nicht mehr aufdecken können.[123] Diskutiert wird als Alternative die Pflicht zur diskriminierungsfreien Ausgestaltung des Trainingsdatenmaterials[124] oder die Einführung von Antidiskriminierungsaudits.[125] Im Übrigen bietet nach überwiegender Ansicht auch hier die Transparenz der Datensätze, der Profile und Algorithmen gute Lösungen: Dies erlaubt Betroffenen oder auch Experten, Diskriminierungen aufzudecken und auch technische Ursachen auszumachen. Gefordert wird etwa, die Herkunft der Daten zu markieren[126] oder ein Protokoll über die verwendeten Kriterien zu erstellen.[127] Auch Antidiskriminierungsstel-

[122] Die Diskriminierungsrelevanz dieser Parameter ist schon gar nicht erst erkennbar. Vgl. *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1149; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 108; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 20. Da letztlich ein jedes Merkmal ein Proxy darstellen kann, würde eine Pflicht zum Löschen sämtlicher Proxies auf eine Streichung sämtlicher Entscheidungsparameter hinauslaufen vgl. *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1149; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 8; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 107–109.

[123] Vgl. *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1153 f.; *Martini*, Blackbox Algorithmus, 2019, S. 74; *Martini*, JZ 72 (2017), 1017, 1019; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 108.

[124] Denkbar ist die Aufbereitung bzw. Überarbeitung bestehender Datensätze oder die Erzeugung synthetischer Datensätze, *Corbett-Davies/Goel*, The Measure and Mismeasure of Fairness, Stanford University, 14.8.2018, S. 19; vgl. *Martini*, Blackbox Algorithmus, 2019, S. 244 f.; *Ntoutsi/Fafalios/Gadiraju u.a.*, Bias in Data-driven AI Systems, 14.01.2020, S. 7 f. Hierdurch sollen „Standarddatensätze" („benchmark data sets") geschaffen werden. Dabei ist bereits schon unklar, was das Kriterium der Diversität ausmacht und wann demnach von einer hinreichenden Diversifizierung ausgegangen werden kann. Kontextspezifisch wird man möglicherweise zu unterschiedlichen Anforderungen kommen, vgl. *Ntoutsi/Fafalios/Gadiraju u.a.*, Bias in Data-driven AI Systems, 14.01.2020, S. 13. Problematisch ist darüber hinaus, dass die anhand dieser Daten trainierten Algorithmen fehlerhaft sein können, eben da die zugrundeliegenden Daten letztlich verfälscht sind, darauf weist auch *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 109 hin.

[125] Vgl. hierzu *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 28 f. In diese könnten dann auch unabhängige Kontroll- und Expertengremien, die etwaige Diskriminierungen aufdecken und als Aufsichtsbehörden dienen könnten, einbezogen werden, *ders.*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 30–32 „Equality Bodies".

[126] *Martini*, Blackbox Algorithmus, 2019, S. 245.

[127] *Ernst*, JZ 72 (2017), 1026, 1032 f.; *Martini*, JZ 72 (2017), 1017, 1022.

len, sollen umfassende Einblicks- und Prüfungsrechte zukommen.[128] Schließlich wird über Beweiserleichterungen für das Vorliegen einer Diskriminierung durch autonome Systeme nachgedacht.[129]

4. Regulierungsinitiativen zur Absicherung der Privatheit

Um anwendungs- und bereichsübergreifende Regulierungsansätze autonomer Systeme geht es, soweit auf Regulierungsbedarfe rekurriert wird, die aus dem Recht auf Privatheit folgen. Herausfordernd ist dabei vor allem die Abgrenzung zum Datenschutzrecht, mit dem es vielschichtig verwoben ist. Auf unionaler Ebene hat sich ein konsensfähiger Ansatz zur Abschichtung von Privatheit und Datenschutz bislang weder in der Rechtsprechung noch in der Literatur herausgebildet.[130] Regulierungsfragen autonomer Systeme, die sich mit

---

[128] Vgl. *Härtel*, Landes- und Kommunalverfassung 29 (2019), 49, 57; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 34 f. So auch *Ernst*, JZ 72 (2017), 1026, 1033. Eher unspezifisch *Steege*, MMR 22 (2019), 715, 720 f. Lediglich eine Offenlegung der maßgeblichen Kriterien bzw. einer Erklärung der Entscheidung gegenüber diesen Agenturen verlangt *Hacker*, Common Mark. Law Rev 55 (2018), 1143, 1170; *Ntoutsi/Fafalios/Gadiraju u.a.*, Bias in Data-driven AI Systems, 14.01.2020, S. 10 f. Problematisch sind dann Algorithmen höherer Komplexität, bei denen etwaige (menschlich verständliche) Parameter gerade nicht vorliegen, so auch *Martini*, JZ 72 (2017), 1017, 1019.

[129] Dies etwa in Form von Rechenschafts- und Erklärungspflichten für Anwender derartiger Systeme *Härtel*, Landes- und Kommunalverfassung 29 (2019), 49, 57 oder in Form gesetzlicher Vermutungen, so *Martini*, Blackbox Algorithmus, 2019, S. 247 f., der eine Erweiterung des § 22 AGG auf algorithmische Auswertungen sowie erhöhte Anforderungen an den Gegenbeweis für den Verwender eines solchen algorithmischen System vorschlägt. *Ernst*, JZ 72 (2017), 1026, 1033 geht dagegen bereits nach der aktuellen Rechtslage von einer Anwendbarkeit des § 22 AGG auf algorithmische Entscheidungsprozesse aus.

[130] Während in der deutschen Rechtsordnung das Datenschutzrecht – dort als Recht auf informationelle Selbstbestimmung – einen Teilbereich des Persönlichkeitsrechts darstellt, Datenschutz und Privatheit damit konzentrische Kreise darstellen, konstruiert die GRCh Datenschutz und Privatheit als eigenständige Rechte (Art. 8 und Art. 7 GRCh), was für eine Abspaltung des Datenschutzes von der Privatheit spricht. Datenschutz und Privatheit sind dann zwei unabhängige Kreise, die sich Venn-Diagramm-artig überlagern, (zu diesem Bild: *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 439.). In den Überschneidungsbereich fallen Konstellationen, in denen privatheitsspezifische Fragen, insbesondere solche der Privatsphäre, gerade durch die Datenverarbeitung aufgeworfen sind – so die herrschende Ansicht in der Literatur, siehe nur *Albers*, in: Albers/Hoffmann-Riem (Hrsg.), Grundlagen des Verwaltungsrechts, ^{2}2012, S. 107, Rn. 43, 46; *Forde*, Camb. L. Rev. 2016, 135, 146–147, 149; *Gellert/Gutwirth*, CLSR 29 (2013), 522, 526, 529; *Reinhardt*, AöR 142 (2017), 528, 539 f.; *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 69 f.; Sydow, DS-GVO/*Sydow*, Art. 1 Rn. 15; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 203–226, in diese Richtung auch der Ansatz Generalanwalt Villalón, Schlussanträge v. 12.12.2013, Rs. C-293/12, ECLI:EU:C:2013:845, Rn. 65 – *Digital Rights*. Der EuGH hat sich zu dieser Frage nicht eindeutig positioniert, vgl. die

Blick auf das Recht auf Privatheit stellen, werden daher vielfach auch aus der Warte des Datenschutzrechts behandelt und umgekehrt.[131] Problematisiert in der Perspektive des Rechts der Privatheit wird insbesondere, dass autonome Systeme tiefgehende Einblicke in die Persönlichkeit und das Privatleben des Einzelnen erlauben und also die Privatsphäre beeinträchtigen können.[132] Die Ableitung von als sensibel bewerteten Persönlichkeitsmerkmalen bzw. deren Verwendung soll dann untersagt sein.[133] Im Übrigen fokussiert das Recht der Privatheit auf die verschiedenen Einflussnahmen auf die Meinungs- und Entscheidungsfreiheit, wie dies in Kapitel 2 dargestellt wurde.[134] Als Gegenmaßnahme wird die Offenlegung der Profilbildung und die Profilverwendung, d.h. die Profilbasiertheit eines Dienstes, gefordert.[135] Darüber hinaus wird für ein

---

Analyse bei *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 59–60. Im Einzelnen ist hier vieles unklar. Siehe eingehend zu diesen Fragen etwa *Forde*, Camb. L. Rev. 2016, 135–149; *Kokott/Sobotta*, Int. Data Priv. Law 3 (2013), 222–228; *González Fuster*, The Emergence of Personal Data Protection As a Fundamental Right of the EU, 2014; *Fuster/Gellert*, Int. Rev. Law Comput. Technol. 26 (2012), 73–82; *Eichendorfer*, Der Staat 55 (2016), 41, 61 f.; *Michl*, DuD 41 (2017), 349–353; *Gellert/Gutwirth*, CLSR 29 (2013), 522–530; *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 52.

[131] Dass Profilbildungen überhaupt Privatheitsfragen aufwerfen, wird vielfach bezweifelt. Dem treten entgegen etwa *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 290, die ein Verbot von Profilbildungsmaßnahmen, wie dies die Privatheit nach ihrer Konzeption forderte, nicht für das richtige Regulierungsinstrument halten. Ablehnend auch *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 329 f., der die profilbasierten Problematiken im Gebot der Gleichbehandlung und Fairness und nicht der Privatheit verortet.

[132] Siehe hierzu Kapitel 2 C. III. 2. Vgl. auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 436; *van der Hof/Prins*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 111, 115 f.; *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 305 f.; *Hildebrandt*, Identity in the Information Society IDIS 1 (2008), 55, 62–64; *Martini*, Blackbox Algorithmus, 2019, S. 91 f.; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 57 f. sowie *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 45. Sehr allgemein *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 10.

[133] *Brownsword*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 345, 349–351 zieht hierfür eine Konstruktion der Privatheit heran, wie sie vom EGMR sowie im US-amerikanischen Raum unterstützt wird. Maßgeblich soll sein, ob die Inhalte der Profilbildung vernünftigerweise erwartbar („reasonable expectation of privacy") sind – dann sind sie zulässig – oder nicht – dann sind sie nicht zulässig.

[134] Kapitel 2 C. II. 2., IV. 2 a).

[135] *Martini*, Blackbox Algorithmus, 2019, S. 179, 341. Siehe auch bereits *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336. Eine Kennzeichnung des Stattfindens einer Profilbildung fordert auch *Lorentz*, Profiling, 2019, S. 341.

Einblicksrecht der betroffenen Person in ihr Profil[136] sowie in wesentliche Entscheidungsparameter, zumindest in belastenden Entscheidungssituationen,[137] eingetreten. Verlangt wird auch die Einführung von Begründungs- oder Erklärungspflichten oder einer Pflicht zur menschlich verständlichen Ausgestaltung von nicht nachvollziehbaren Entscheidungen autonomer Systeme.[138] Auch Widerspruchs- bzw. Abwahloptionen von einzelnen Anwendungen autonomer Systeme für Betroffene sollen Schutz bieten.[139] Als essentiell werden überdies Einwirkungs- oder Anfechtungsmöglichkeiten hinsichtlich der algorithmischen Entscheidungsfindung erachtet.[140] Diskutiert werden auch zentralisierte, durch staatliche oder private Expertengremien durchgeführte Kontrollverfahren von automatisierten Entscheidungen und Steuerungen,[141] auch von Profilbildungsmaßnahmen.[142] Abschließend werden auch im Rahmen der Privatheit Verbote von bestimmten Anwendungen autonomer Systeme erwogen, mittels derer Verwender auf besonders subtile Weise auf die Willensbildung betroffe-

---

[136] *Härting*, CR 4 (2014), 528, 532 f.; *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 448–450; *Schermer*, CLSR 27 (2011), 45, 51; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 10.

[137] Vgl. *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 70; *Martini*, DVBl 129 (2014), 1481, 1489; *Schermer*, CLSR 27 (2011), 45, 51. Vgl. auch das umfassende Transparenzkonzept bei *Martini*, Blackbox Algorithmus, 2019, S. 167–207, 339–347.

[138] Eingehend, wenngleich unspezifisch, welchem Rechtsgebiet (Verbraucher-, Daten- oder Privatheitsschutz) dies zuzuordnen ist *Wischmeyer*, AöR 143 (2018), 1, 42–65 Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 343–345 sowie *Selbst/Barocas*, Fordham L. Rev. 87 (2018), 1085, 1099–1109. Siehe zu einer derartigen Forderung mit ebenso unklarer rechtsdogmatischer Fundierung (dort im Rahmen der Diskussion um ein allgemeines Algorithmenrecht) *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 169 f. sowie bei (dort im Rahmen der Einführung eines KI-Gesetzes) *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 16.

[139] Zum Opt-in-Modell *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 68 f.; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 452. Zum Opt-out-Modell *Härting*, CR 4 (2014), 528, 533. Zu einer Möglichkeit der jederzeitigen Hinzuziehung eines menschlichen Entscheiders *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336.

[140] Zu Einwirkungsrechten hinsichtlich der Profilkonstruktion, wenngleich ohne klare Abgrenzung zum Datenschutzrecht, *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 325. Zu Anfechtungsmöglichkeiten der automatisierten Entscheidung *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 10.

[141] Etwa über Zertifizierung und Auditings für „persönlichkeitssensitive Verarbeitungsvorgänge", so *Martini*, DVBl 129 (2014), 1481, 1489; näher ausdifferenziert bei *Martini*, Blackbox Algorithmus, 2019, S. 348–354. Ein Auditing ex ante sowie ex post von automatisierten Entscheidungen fordert *Schermer*, CLSR 27 (2011), 45, 50 f.

[142] *Härting*, CR 4 (2014), 528, 535; siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 250–257, 268–272.

ner Personen einwirken können, etwa das Emotional Targeting oder die Dark-Pattern-Analyse.[143]

5. Regulierungsinitiativen zur Herstellung materieller Gerechtigkeit und Fairness

Um die materielle Gerechtigkeit und Fairness automatisierter Entscheidungen abzusichern, wird Transparenz als wesentliches Schutzinstrument angeführt, die eine Fehlerprüfung, Verfahrensbeteiligung sowie Anfechtung ermöglichen soll. Im Zentrum steht dabei Transparenz im Sinne menschlicher Nachvollziehbarkeit: Gefordert wird die menschlich verständliche Ausgestaltung der Entscheidungen insgesamt[144] oder einzelner als willkürlich bewerteter Merkmale.[145] Auch Begründungspflichten von automatisierten Entscheidungen werden gefordert.[146] Vereinzelt wird auch ein Verbot menschlich nicht verständlicher, rein korrelativer Merkmale erwogen.[147] Um Schutz vor Marginalisierung einzelner Personengruppen zu bieten, soll der Katalog der Diskriminierungsmerkmale erweitert werden.[148] Schutz vor fehlerhaften Zuordnungen sollen

---

[143] Zum Verbot personalisierter Werbung *Wågström*, Why Behavioral Advertising Should Be Illegal, Forbes 05.05.2019, https://www.forbes.com/sites/forbestechcouncil/2019/03/05/why-behavioral-advertising-should-be-illegal.; zum Verbot der Dark-Pattern-Analyse in spezifischen Konstellationen *Martini/Drews/Seeliger u.a.*, ZfDR 1 (2021), 72 f. bei Überschreiten der „kritische[n] Schwelle der Ausnutzung privatautonomer Gestaltungsfreiheit".

[144] Der Bereich der informationstechnischen Forschung, der sich mit der Umsetzung dieser Forderung beschäftigt, wird als „explainable AI" bezeichnet. Hierauf ist im Detail in Kapitel 5 B. III. 3. c) bb). zurückzukommen. Einen Ein- und Überblick über den aktuellen Stand dieses Forschungsbereichs bieten etwa *Islam/Eberle/Ghafoor u.a.*, Explainable Artificial Intelligence Approaches: A Survey, 23.01.2021; *Käde/Maltzan*, CR 36 (2020), 66–72; *Burkart/Huber*, Journal of Artificial Intelligence Research 70 (2021), 245–317 Dies ist bereits technisch äußerst anspruchsvoll, vgl. zu einzelnen technischen Schwierigkeiten im Einzelnen *Martini*, Blackbox Algorithmus, 2019, S. 193–195; *Käde/Maltzan*, CR 36 (2020), 66–72. In rechtlicher Hinsicht sind kollidierende unternehmerischen Freiheiten zu beachten, vgl. hierzu *Martini*, Blackbox Algorithmus, 2019, S. 195–197; *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 65.

[145] So *Wachter/Mittelstadt*, CBLR 2019, 494–620, die die Einführung eines Rechts auf angemessene Schlussfolgerungen vorschlagen. Kritisch hierzu *Martini*, Blackbox Algorithmus, 2019, S. 206 f.

[146] Ausführlich, obschon allein im Hinblick auf den Einsatz durch staatliche Akteure, *Wischmeyer*, AöR 143 (2018), 1, 54–61; *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 75, 93–97. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 189–207, 343–345.

[147] So etwa *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 67 f., der ein risikobasiertes Verbotsmodell vorschlägt.

[148] Hierzu etwa *Härtel*, Landes- und Kommunalverfassung 29 (2019), 49, 57. Für Konstellationen, in denen „die algorithmische Beurteilung von Personen genutzt wird, um die

Qualitätsstandards bezüglich der verwendeten Daten, Trainingsverfahren sowie der gebildeten Profile oder Algorithmen bieten.[149] Auch Kontrollverfahren durch private Experten,[150] Selbstprüfungsverfahren[151] sowie staatliche Kontrollen[152] werden diskutiert.

6. Definition absoluter Grenzlinien zum Schutz der Menschenwürde

Die Menschenwürde wird in der Regulierungsdiskussion herangezogen, um absolute Grenzlinien für autonome Systeme zu definieren. Eine konkrete Beschreibung dieser Grenzlinien fällt allerdings schwer, schon deshalb, da die allgemeine Konzeption der Menschenwürde äußerst diffus ist,[153] aber auch deshalb, da es (noch) nicht gelungen ist, in Anbetracht der technischen Entwicklung autonomer Systeme ein spezifisches (Gefährdungs-)Konzept der Menschenwürde zu entwickeln.[154] Überwiegend geht man deduktiv über das Aufstellen von Fallgruppen vor, die aber vielfach unspezifisch bleiben. Als Grenzlinien benannt werden etwa die umfassende „Verdatung" oder „Berechnung" des Menschen durch autonome Systeme[155] oder dessen Entindividualisierung,

---

Angewiesenheit einer Person auf die Leistung zu erzeugen, zu verstärken oder auszunutzen". Ebenso, wenn auch eher vorsichtig, *Martini*, Blackbox Algorithmus, 2019, S. 239, 349.

[149] *Martini*, JZ 72 (2017), 1017, 1019; *Martini*, Blackbox Algorithmus, 2019, S. 259. Siehe auch *Kroll/Huey/Barocas u.a.*, University of Pennsylvania Law Review 165 (2017), 633, 662–672.

[150] Wenn auch im Rahmen des Einsatzes derartige Algorithmen der Künstlichen Intelligenz im staatlichen Bereich und nicht spezifisch zur Profilbildung *Wischmeyer*, AöR 143 (2018), 1, 61 f.

[151] *Martini*, Blackbox Algorithmus, 2019, S. 266 f.

[152] *Ders.*, Blackbox Algorithmus, 2019, S. 253–256.

[153] Die Definition der Menschenwürde ist Gegenstand fortlaufender, kontroverser Debatte, vgl. zur umfassenden Literatur etwa *Bührer*, Das Menschenwürdekonzept der Europäischen Menschenrechtskonvention, 2020; *Nettesheim*, JZ 74 (2019), 1–11; *Wallau*, Die Menschenwürde in der Grundrechtsordnung der Europäischen Union, 2010. Vgl. auch *Bull*, Der Staat 58 (2019), 57, 70–72. Oftmals wird die Menschwürde auch in einem rechtspolitischen bzw. moralisierenden Verständnis angeführt, siehe etwa *Golla*, in: Donath/Brett-hauer/Dickel-Görig u.a. (Hrsg.), Verfassungen – ihre Rolle im Wandel der Zeit, 2019, S. 183, 190 „[D]ie Menschenwürde [ist] aufgrund ihrer Offenheit stets auch eine mögliche Projektionsfläche für Technikskepsis und sogar Fortschrittsfeindlichkeit". Eingehend zu verschiedenen Konzeptionen der Menschenwürde *Nettesheim*, JZ 74 (2019), 1–4.

[154] Dies stellen auch *Orwat/Folberth/Bareis u.a.*, Risikoregulierung der KI: normative Herausforderungen und politische Entscheidungen, Karlsruher Institut für Technologie (KIT); Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), 14.06.2020, S. 6 fest.

[155] So ist etwa die Rede von der Reduzierung des Menschen zum „Datenkonglomerat". Hier wird häufig das Bild vom „gläsernen Menschen" bemüht – eine Konstellation, die per se menschenwürdefeindlich ist, vgl. etwa, wenn auch im Hinblick auf die Profilbildung durch staatliche Akteure, *Härting*, Landes- und Kommunalverfassung 29 (2019), 49, 56; *Dreyer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, 140; *Golla*, in:

die dadurch entsteht, dass der Einzelne in seiner Standardisierbarkeit und Vergleichbarkeit in den Fokus rückt und das Profil, nicht mehr das Individuum, als Grundlage für die Interaktion und Kommunikation dient.[156] Eine Menschenwürdeverletzung soll auch dann vorliegen, wenn autonome Systeme die innere und äußere Verhaltensfreiheit des Menschen umfassend aufheben.[157] Gemeinhin geht man derzeit davon aus, dass die Grenzlinien der Menschenwürde noch nicht überschritten sind.[158]

II. Innovativ-technikspezifische Regulierungsansätze

Diskutiert werden auch Rechtsinstrumente, die spezifisch auf autonome Systeme ausgerichtet sind. Drei Ansätze sollen vorgestellt werden: das Recht auf menschliche Entscheidung (1.), die Einführung einer (Teil-)Rechtspersönlichkeit der Künstlichen Intelligenz (2.), schließlich ein Rechtsakt für Systeme der Künstlichen Intelligenz bzw. für Algorithmen (3.).

Donath/Bretthauer/Dickel-Görig u.a. (Hrsg.), Verfassungen – ihre Rolle im Wandel der Zeit, 2019, S. 183, 187 „total datafiziert" und „algorithmisiert". Auch die „Kommerzialisierung des menschlichen Daseins", die mit Techniken bzw. Anwendungen der Umgebungsintelligenz einhergeht, soll die Menschenwürde verletzten, vgl. *Dreyer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, 141. Schließlich sei es mit der Menschenwürde unvereinbar, menschliches Verhalten umfassend berechnen zu wollen, vgl. *ders.*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, 139.

[156] Kapitel 2 C. III. 1. Eingehend *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016; *Ernst*, JZ 72 (2017), 1026, 1028; *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 60 f.; ebenso *Leese*, Security Dialogue 45 (2014), 494, 506. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 97; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 10; *Tzanou*, The fundamental right to data protection, 2019, S. 31.

[157] Eingehend *Bull*, Der Staat 58 (2019), 57, 69. So sollen etwa subtil-manipulative Einwirkungen auf die Selbstbestimmung Menschenwürdeverletzungen darstellen, so *Dreyer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, 141. *Golla*, in: Donath/Bretthauer/Dickel-Görig u.a. (Hrsg.), Verfassungen – ihre Rolle im Wandel der Zeit, 2019, S. 183, 189 erkennt bereits in der Intransparenz algorithmischer Entscheidungsstrukturen, zumindest soweit es sich um Entscheidungen mit erheblicher Beeinträchtigung handelt, als mögliche Verletzungen der Menschenwürde. Schließlich wird auch in den durch Profilbildung ausgelösten Diskriminierungen oder Realdiskriminierungen eine Antastung der Menschenwürde gesehen, vgl. etwa *Dreyer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 135, 138 f. Zum Racial Profiling *Tischbirek/Wihl*, JZ 68 (2013), 219, S. 219–220, 222.

[158] Ebenso *Nettesheim*, JZ 74 (2019), 1, 10. So auch *Bull*, Der Staat 58 (2019), 57, 69 f., der nicht davon ausgeht, dass in nächster Zeit mit einer Menschenwürdeverletzung durch autonome Systeme zu rechnen ist.

1. Recht auf menschliche Entscheidung

Diskutiert wird die Einführung eines (Grund-)Rechts auf menschliche Entscheidungen[159] bzw. ein Abwehrrecht gegen maschinelle Entscheidungen.[160] Auch ein (grund-)rechtliches Verbot von Systemen der Künstlichen Intelligenz im Allgemeinen, oder aber deren Einsatz in spezifischen Anwendungsbereichen wird diskutiert.[161] Wenngleich es dort um Verbote der Verwendung autonomer Systeme durch den Staat geht,[162] wird auch eine Übertragung auf die Nutzung im Privatverhältnis erwogen. So soll es etwa ein Recht auf menschliche Kommunikation geben (Verbot von Chatbots).[163] Ein solches Recht ist

---

[159] *Mund*, in: Gwiasda/Greve/Kemper u.a. (Hrsg.), Der digitalisierte Staat, 2020, S. 177; *Mund*, Das Recht auf menschliche Entscheidung, 2021.

[160] Diskutiert wird etwa ein „right to be off", *Frischmann/Selinger*, Re-engineering humanity, 2018, d.h. ein Recht, ein Leben ohne algorithmische Systeme führen zu können, oder ein „right to attention", so *Danaher*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 98, 114, also ein Recht auf freie Entwicklung und Ausrichtung individueller Aufmerksamkeit.

[161] *Pfeil*, InTeR 8 (2020), 82, 88 f. Siehe auch Art. 12 der Landesverfassung Hessen, in dem es heißt: „Der Mensch steht höher als Technik und Maschine" sowie Art. 5 Abs. 6 Digitalcharta, wo normiert ist: „The use of artificial intelligence and robotics in areas related to fundamental rights violations must be subject to social debate and regulated by legislation".

[162] Zu den technischen Möglichkeiten und Ausgestaltungsformen siehe etwa *Eichel/Matt/Tovar Galván*, Wirtschaftsinformatik & Management 12 (2020), 392–403. Zur Anwendung von algorithmischer Automatisierung im Verwaltungsverfahren siehe aus der Fülle der Literatur etwa *Berger*, DVBl 132 (2017), 804–808; *Braun Binder*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 295; *Bull*, DVBl 132 (2017), 409; *Djeffal*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 277; *Guggenberger*, NVwZ 38 (2018), 844, S. 846, 849–850; *Hermstrüwer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 199 Teilweise liegen hierzu bereits einfach-gesetzliche Regulierungen vor, vgl. etwa §§ 35a, 23 Abs. 1 S. 3 VwVfG, § 155 Abs. 4 AO, § 31a SGB X. Zur umfassenden Literatur hinsichtlich der verfassungsrechtlichen Zulässigkeit der Automatisierung im Justizbereich siehe etwa *Buchholtz*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 175; *Enders*, JA 50 (2018), 721–727; *Marx*, DRiZ 96 (2018), 422; *Nink*, Justiz und Algorithmen, 2021, S. 261–355; *Quarch/Hähnle*, NJOZ 20 (2020), 1281–1286. Diese Betrachtungen und Vorschriften beschäftigen sich mit der algorithmischen Automatisierung; nicht notwendig geht es dann um Algorithmen der Künstlichen Intelligenz bzw. um Profilbildungen in dem hier verstandenen Sinne. Die grundlegenden Gedanken dürften jedoch übertragbar sein. Die aufgeworfenen Fragen sind voraussetzungsvoll; sie verlangen eine vertiefte Untersuchung dessen, was staatliche Akteure leisten sollen, vgl. etwa *Nink*, Justiz und Algorithmen, 2021, S. 95–130. Über die Sinnhaftigkeit bzw. den Mehrgewinn derartiger Grundrechtsinnovationen wird vielfach gestritten.

[163] Dieses Recht sieht vor, die betroffene Person über den Einsatz einer Maschine (Chat Bot) zu informieren und ihr gegebenenfalls ein Abwahlrecht (Opt-out) einzuräumen. Vgl. zur Regulierung von Social Bots etwa *Löber/Roßnagel*, MMR 22 (2019), 493–498; *Schröder*, DVBl 133 (2018), 464–494.

auch im Datenschutzrecht in Art. 22 DSGVO vorgesehen.[164] Darauf wird zurückzukommen sein. Auf das Recht auf menschliche Entscheidung werden weitere, vor allem prozessuale Schutzrechte wie Transparenz und Einwirkungs- und Anfechtungsoptionen gestützt.[165] Im Ergebnis geht es beim Recht auf menschliche Entscheidung um eine Zusammenführung punktueller Regulierungsansätze aus verschiedenen Anwendungsbereichen in einer Vorschrift. Dies ist von der Vorstellung getragen, dass diese punktuellen Regelungen nicht ausreichend sind. Als wesentlicher Gefährdungsmoment, der diese punktuellen Regulierungsbedarfe zusammenführt, wird nicht die technische Funktionsweise, sondern eine bestimmte Anwendung autonomer Systeme erkannt, nämlich die automatisierte Entscheidung.

2. (Teil)Rechtspersönlichkeit für Systeme Künstlicher Intelligenz

Zur regulativen Einfassung von Systemen Künstlicher Intelligenz wird auch vorgeschlagen, diesen selbst Rechtsfähigkeit zuzusprechen, dies in Gestalt einer Rechtssubjektivität,[166] eines spezifischen Rechtsstatus[167] oder einer partiellen Rechtssubjektivität[168] bis hin zu – so der überwiegende Ansatz –einer eigenständigen Form einer Rechtspersönlichkeit (sogenannte ePerson).[169] Die

---

[164] Auch Art. 9 Abs. 1 lit. a) Convention 108+ enthält ein solches Verbot.

[165] Siehe Art. 22 Abs. 3 DSGVO, Art. 9 Abs. 1 lit. a), c) Convention 108+. Siehe auch *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248; *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77. Vgl. auch *Mund*, Das Recht auf menschliche Entscheidung, 2021, S. 186–232.

[166] Vgl. aus der umfassenden Literatur etwa *Allen/Widdison*, Harv. J. Law Technol. 9 (1996), 26; *Beck*, AJP/PJA 2017, 183–191; *Solum*, N.C. L. Rev. 70 (1992), 1231–1288.

[167] So *Europäisches Parlament*, Zivilrechtliche Regelungen im Bereich Robotik, Europäisches Parlament, 16.02.2018.

[168] *Teubner*, AcP 218 (2018), 155, 177–196. Letztlich geht es um die Fortentwicklung bekannter rechtlicher Figuren aus dem Recht der Stellvertretung oder der Haftung für fremdes Verschulden bzw. Hilfspersonen.

[169] Aus der umfangreichen Literatur siehe etwa *Eidenmüller*, ZEuP 25 (2017), 765–777; *Schirmer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 123; umfassend und differenziert die Beiträge in *Gleß/Seelmann* (Hrsg.), Intelligente Agenten und das Recht, 2016; *Zech*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, 2020. Mit Darstellung des Diskussionsstands *Martini*, Blackbox Algorithmus, 2019, S. 290–294. Zur einer wirtschaftlichen Bewertung einer solchen Lösung vgl. *Scheufen*, Wirtschaftsdienst 99 (2019), 411–414. Diese soll der juristischen Person nachempfunden sein. Als solche soll sie wirksam eigene Willenserklärungen abgeben können, eigentumsfähig und insbesondere deliktsfähig sein. Die Eigenhaftung soll dann über anteilige Zahlung der verschiedenen Beteiligten (Hersteller, Verwender, Vertreiber) oder durch eine Pflichtversicherung abgedeckt werden, vgl. *Teubner*, AcP 218 (2018), 155, 161.

Diskussion seht erst am Anfang.[170] Mit diesem Regulierungsansatz werden vor allem die unklaren Verantwortlichkeits- und Haftungsverhältnisse bei der Anwendung von autonomen Systemen adressiert,[171] um inhaltlich-substantielle Regulierung geht es nicht.

3. Algorithmenrecht und Roboterrecht und Entwurf für ein KI-Gesetz

Bereits seit Längerem wird für eine eigenständige Regulierung autonomer Systeme eintreten, so etwa ein Rechtsakt für Algorithmen oder für Roboter (a)). Auf Unionsebene hat die Europäische Kommission bereits einen Entwurf für ein KI-Gesetz erarbeitet (b)).

a) Algorithmen- und Roboterrecht

Eine eigenständige Regulierung von Algorithmen erscheint vielen als gute Lösung, um sämtliche algorithmenbasierten Systeme, dann also auch autonome Systeme, einer effektiven Steuerung zuzuführen.[172] Anstelle der Regulierung einer konkreten Anwendung, etwa einer automatisierten Entscheidung, oder punktueller Regelungen einzelner Anwendungsbereiche, etwa der Informationsfilterung, verspricht man sich vom regulativen Zugriff auf die technische Funktionsweise algorithmischer Systeme erhebliche Steuerungsgewinne. Zugleich erkennt man in den Algorithmen die eigentliche Ursache der durch diese ausgelösten Gefährdungen und Spannungslagen wie Diskriminierungen, Feh-

---

[170] Es stellen sich rechtstechnische Probleme, etwa wenn ein autonomes System aus verschiedenen Einheiten physischer und algorithmischer Natur besteht, vgl. hierzu *Spindler*, CR 20 (2015), 766, 775. Dem Konzept kritisch gegenüber stehen *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 241 f., denen zufolge diese Lösung die eigentlichen Zurechnungsverteilungsfragen nicht beantwortet, so auch *Spindler*, CR 20 (2015), 766, 774, demzufolge die Verleihung der Rechtspersönlichkeit bloßer „Selbstzweck" ist. Auf einer metaphysischen Ebene wird befürchtet, die Zuerkennung von Rechtsfähigkeit könnte dazu führen, dass sich beteiligte menschliche Akteure ihrer Verantwortung entziehen könnten, vgl. *Schirmer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 123, 127; *Spindler*, CR 20 (2015), 766, 774 f.; *Teubner*, AcP 218 (2018), 155, 163.

[171] Diese haben ihre Ursache in der Intransparenz und fehlenden Nachvollziehbarkeit der Entscheidungsfindung autonomer Systeme, sind aber auch darauf zurückzuführen, dass bei der Erstellung und Anwendung der Lösungsalgorithmen, etwa der Sammlung des Trainingsdatenmaterials oder der Trainingsverfahren, eine Vielzahl unterschiedlicher Akteure beteiligt sind, vgl. zu den verschiedenen Ursachen der Verantwortungslücken *Schirmer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 123, 128. *Teubner*, AcP 218 (2018), 155, 156–159, 163–176, 196–203 kategorisiert diese in Autonomie-, Verbunds- und Vernetzungsrisiken.

[172] Grundlegend *Martini*, Blackbox Algorithmus, 2019, S. 157–331. So auch *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 67; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 159–224.

leranfälligkeiten oder manipulative Übergriffe. In eine ähnliche Richtung gehen Vorschläge zur Etablierung eines Roboterrechts,[173] die neben Algorithmen auch noch weitere Regulierungsfragen der Automatisierung der Mensch-Maschine-Interaktion abdecken könnten. Inhaltlich werden die bereits vorgestellten Mechanismen, insbesondere Transparenz und Verständlichkeit, Einwirkungs- und Abschaltrechte, Qualitätsanforderungen, Expertenprüfungen und Audits diskutiert.[174]

b) Entwurf für ein Gesetz der Künstlichen Intelligenz (KI-Gesetz-E)

Bereits seit Längerem wurde in Literatur und Rechtspolitik auf eine spezifische Regulierung der Künstlichen Intelligenz gedrungen.[175] Auch die von der Europäischen Kommission eingesetzte Hochrangige Expertengruppe für Künstliche Intelligenz forderte ein solches Gesetz.[176] Mit einem Vorschlag für ein Gesetz der Künstlichen Intelligenz vom 21.04.2021[177] hat die EU-Kommission hierauf reagiert (KI-Gesetz-E).[178] Das Gesetz soll sämtliche durch Künstliche Intelli-

---

[173] Siehe hierzu *Beck*, in: Japanisch-Deutsches Zentrum (Hrsg.), Mensch-Roboter-Interaktionen aus interkultureller Perspektive, 2012, S. 124, Vgl. etwa; *Lohmann*, ZRP 50 (2017), 168–171.

[174] Siehe beispielhaft den umfassenden Regulierungsvorschlag für Algorithmen bei *Martini*, Blackbox Algorithmus, 2019, S. 339–358.

[175] Siehe zu Forderungen von Seiten des Europäischen Parlaments und des Rates im Begründungsteil des Entwurfs, *Europäische Kommission*, Begründung Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 21.04.2021, S. 2 f. Zu Initiativen der Europäischen Kommission siehe *Europäische Kommission*, Künstliche Intelligenz für Europa, 25.04.2018; *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 10–12. Einen Überblick über die rechtspolitischen Vorläufe des Entwurfs bieten *Cooman*, Market and Competition Law Review 6 (2022), 49, 52–56; *Raposo*, Int. J. Law Inf. Technol. 30 (2022), 88, 89 f. Vgl. zu Forderungen von Seiten der Literatur siehe etwa *Lücke*, in: ders. (Hrsg.), Künstliche Intelligenz und Vorschläge zu einer EU-Regulierung, 2021, S. 10 sowie *Wischmeyer*, AöR 143 (2018), 1–66 Befürwortend zum KI-Gesetz-E etwa *Bomhard/Merkle*, RDi 1 (2021), 276, 283; *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 8.

[176] Siehe auch *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 14.

[177] *Europäische Kommission*, Begründung Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 21.04.2021.

[178] Der Vorschlag ist eingebettet in ein umfassendes Regulierungsprogramm der Europäischen Union, mit dem die Herausforderungen der aktuellen technischen Entwicklungen der

genz aufgeworfenen Regulierungsfragen übergreifend beantworten.[179] Im Folgenden sollen Kernelemente des Regulierungsentwurfs vorgestellt werden.
Der KI-Gesetz-E verfolgt einen risikobasierten Ansatz.[180] Es sieht Verbote für inakzeptable Risiken vor,[181] für solche mit mittlerem Risiko ist lediglich eine

---

Digital- und Kommunikationstechnik und der Künstlichen Intelligenz umfassend adressiert werden sollen. Dieses Programm umfasst die schon vorgestellten DMA und DSA, den Digital Governance Act (Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724, 30.5.2022, ABl. L 152, 1), eine noch zu schaffende Maschinenverordnung, die die Maschinenrichtlinie (Richtlinie 2006/42/EG des europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG vom 29.6.2006, ABl. L 157, 24) ersetzen soll, sowie einen Rechtsakt zur Haftung von Systemen der Künstlichen Intelligenz. Vgl. hierzu *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97; *Raposo*, Int. J. Law Inf. Technol. 30 (2022), 88, 106. Siehe auch bereits *Europäische Kommission*, Künstliche Intelligenz für Europa, 25.04.2018, S. 17.

[179] Vgl. zur Integration des KI-Gesetz-E in die Regulierungsstrategie der Europäischen Kommission *Europäische Kommission*, Begründung Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 21.04.2021, S. 6.

[180] In der Literatur wird dies gemeinhin begrüßt. Siehe nur *Ebers*, RDi 1 (2021), 588, 596; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 593, 601; *Cooman*, Market and Competition Law Review 6 (2022), 49, S. 61–62, 65; *Heiss*, EuCML 10 (2021), 252, 253; *Gellert*, Journal of Ethics and Legal Technologies 3 (2021), 15, 18; *Mahler*, in: Colonna/Greenstein (Hrsg.), Law in the era of artificial intelligence, 2022, S. 247, 250 f.; *Orwat/Folberth/Bareis u.a.*, Risikoregulierung der KI: normative Herausforderungen und politische Entscheidungen, Karlsruher Institut für Technologie (KIT); Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), 14.06.2020, S. 5. Befürwortend auch *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 8.

[181] Art. 5 KI-Gesetz-E. Verboten ist allerdings nur der Einsatz, die Inbetriebnahme und das Inverkehrbringen, nicht aber die Entwicklung derartiger Systeme, darauf weisen *Ebert/Spiecker gen. Döhmann*, NVwZ 40 (2021), 1188, 1189 hin. Der Unionsgesetzgeber hat drei derartiger Systeme benannt: Erstens Systeme zur Verhaltensmanipulation durch unterschwellige Techniken (Dark-Pattern-Analysen) oder zur Verhaltensmanipulation von Angehörigen besonders vulnerabler Gruppen, etwa Kinder, die der betroffenen Person oder Dritten einen physischen oder psychischen Schaden zufügen; zweitens behördliche Social-Scoring-Systeme; drittens automatisierte Gesichtserkennungssysteme in der Strafverfolgung und Gefahrenabwehr (biometrische Echtzeit-Fernidentifizierungssysteme). Kritisiert wird daran, dass die Auflistung unvollständig-anekdotisch ist. Siehe etwa *dies.*, NVwZ 40 (2021), 1188, 1193: „Die Liste […] entbehrt aber einer leitenden Systematik". Ähnlich *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97, 112: „The prohibitions range through the fantastical, the legitimising, and the ambiguous".

Kennzeichnungs- und Informationspflicht normiert,[182] für solche mit geringem Risiko ist allein die freiwillige Entwicklung von Verhaltensregeln vorgesehen.[183] Im Kern geht es um die Regulierung von Systemen mit einem hohen Risiko (sogenannte Hochrisikosysteme).[184] Für diese sind insbesondere Transparenzpflichten und Qualitätsanforderungen vorgesehen (aa)), im Übrigen sieht der Entwurf die Einführung eines Risikomanagementsystems vor (bb)). Der überwiegende Teil der derzeit zum Einsatz kommenden autonomen Systeme sind allerdings keine Hochrisikosysteme im Sinne des Vorschlags; die Regulierungswirkung fällt daher eher schwach aus.[185]

---

[182] Dies sind Systeme, die zur Interaktion mit dem Menschen oder zur Inhaltsgenerierung bestimmt sind, Emotionserkennungssysteme und Systeme zur biometrischen Kategorisierung sowie Deepfakes, Art. 52 KI-Gesetz-E. Diese Systeme stellen gleichsam eine vierte Risikoklasse dar, auch wenn dies im Entwurf nicht explizit so benannt ist. So auch *Geminn*, ZD 11 (2021), 354, 358; *Raposo*, Int. J. Law Inf. Technol. 30 (2022), 88, 92. Zu den Inhalten derartiger Kennzeichnungs- und Informationspflichten derartiger Systeme siehe eingehend *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97, 106–108; *Kalbhenn*, ZUM 65 (2021), 663, 669 f.

[182] Zu dieser Einordnung *Hoffmann*, K&R 20 (2021), 369, 371.

[183] Art. 69 KI-Gesetz-E.

[184] Diese sind in Art. 6 KI-Gesetz-E legaldefiniert. Unterschieden werden zwei Arten: erstens Systeme, die als Sicherheitskomponenten eines den in Anhang II genannten Harmonisierungsrechtsvorschriften unterfallenden Produkts verwendet werden oder selbst ein solches Produkt darstellen und für die nach diesen Harmonisierungsrechtsvorschriften eine Konformitätsbewertung durch Dritte bei Inverkehrbringen oder Inbetriebnahme des Produkts vorgeschrieben ist (Art. 6 Abs. 1 KI-Gesetz-E), zweitens Systeme, die zu den im Anhang III aufgeführten acht Fallgruppen zählen (Art. 6 Abs. 1 KI-Gesetz-E). Diese werden auch als „stand-alone AI systems" benannt, siehe etwa *Cooman*, Market and Competition Law Review 6 (2022), 49, 58. Aufgelistet werden in Anhang III: die biometrische Identifikation bzw. Kategorisierung natürlicher Personen, die Verwaltung und der Betrieb kritischer Infrastrukturen, die (Berufs-)Bildung, die Beschäftigung, das Personalmanagement und der Zugang zur beruflichen Selbstständigkeit, der Zugang zu und die Nutzung von elementaren privaten und öffentlichen Diensten und Leistungen (genannt werden hier behördliche Entscheidungen oder Entscheidungen über die Kreditvergabe sowie Entscheidungen über den Einsatz von Not- und Rettungsdiensten und medizinscher Nothilfe), die Strafverfolgung, Anwendungen im Bereich von Migration, Asyl und Grenzkontrollen sowie die Rechtspflege und demokratische Prozesse. Die Europäische Kommission wird ermächtigt, diese Liste dieser acht Fallgruppen durch delegierte Rechtsakte fortzuführen, Art. 13 Abs. 1 KI-Gesetz-E. Auch hier wird kritisiert, dass die Auflistung zu unbestimmt und unvollständig ist. Vgl. *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 532; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 593 f.; *Hoffmann*, K&R 20 (2021), 369, 371, die zahlreiche Beispiele aufführen, die nach dem KI-Gesetz-E keine Hochrisikosysteme darstellen, obschon sie mit einem hohen Schädigungspotential aufwarten. Sehr allgemein *Heiss*, EuCML 10 (2021), 252, 254.

[185] So auch *McCarthy Mark, Propp, Kenneth*, Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation, Lawfare, 28.04.2021. Sie benennen insbesondere Informationsfiltersysteme und Empfehlungssysteme, die in der Regel keine Hochrisikosys-

aa) Transparenzpflichten, Qualitätsanforderungen

Der Entwurf sieht eine Pflicht zur transparenten, d.h. für die NutzerInnen verständlichen Gestaltung der Systeme vor[186] sowie zur Bereitstellung bestimmter Informationen, darunter eine Gebrauchsanleitung.[187] Vorgesehen ist überdies eine Pflicht zur Gewährleistung menschlicher Aufsicht[188] – wohlgemerkt meint dies die Aufsicht irgendeines Menschen, nicht zwingend der NutzerInnen. Kritisiert wird dabei, dass weder bei der Transparenzpflicht[189] noch beim Aufsichtsgebot[190] näher spezifiziert wird, was damit gemeint ist. Im Übrigen stehen Schutzinstrumente im Fokus, die Anforderungen an die Systeme selbst stellen oder Anbieter der Systeme in die Pflicht nehmen. Vorgeschrieben werden Qualitätsstandards für die Trainingsdaten[191] und die Gewährleistung der Sicherheit und Robustheit der Systeme.[192] Auch Protokollierungs- und Aufzeichnungspflichten sind normiert.[193] Erst wenn die Systeme diese Anforderungen erfüllen, können sie rechtmäßigerweise auf den Markt gebracht werden.[194] Zur Durchsetzung der Vorschriften etabliert der KI-Gesetz-E zudem ein

---

teme darstellen. Vgl. auch *Chamberlain*, European Journal of Risk Regulation 13 (2022), 1, 7.

[186] Art. 13 Abs. 1 KI-Gesetz-E.

[187] Die Gebrauchsanweisung ist in Art. 13 Abs. 2 KI-Gesetz-E normiert. Weitere Informationspflichten sind in Art. 13 Abs. 3 KI-Gesetz-E aufgelistet, genannt sind etwa Name und Kontaktdaten des Anbieters, die Merkmale, Fähigkeiten sowie Leistungsgrenzen der Systeme sowie Maßnahmen zur Absicherung menschlicher Aufsicht und Interpretierbarkeit der Ergebnisse von KI-Systemen.

[188] Art. 14 KI-Gesetz-E.

[189] *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 533; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 596; *Varošanec*, Int. Rev. Law Comput. Technol. 36 (2022), 95, 103. Siehe auch *Ebers*, RDi 1 (2021), 588, 590. Kritisch auch im Hinblick auf die fehlende Berücksichtigung von unternehmerischen Interessen *Hoffmann*, K&R 20 (2021), 369, 372 f.

[190] So auch *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 533; *Geminn*, ZD 11 (2021), 354, 357; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 596 f. Kritisch auch *Hoffmann*, K&R 20 (2021), 369, 373 sowie *Orwat/Folberth/Bareis u.a.*, Risikoregulierung der KI: normative Herausforderungen und politische Entscheidungen, Karlsruher Institut für Technologie (KIT); Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), 14.06.2020, S. 19 f.

[191] Art. 10 KI-Gesetz-E.

[192] Art. 15 KI-Gesetz-E.

[193] Art. 11, 12 KI-Gesetz-E.

[194] Art. 19 KI-Gesetz-E. Prozessual wird dies über eine Konformitätsprüfung sichergestellt, die vor dem Inverkehrbringen von Hochrisikosystemen durchzuführen ist, Art. 19, Art. 43 KI-Gesetz-E. Je nach Risikograd kann diese intern durch den Anbieter oder muss extern durch eine in Anhang VII benannte Stelle durchgeführt werden. Bei Hochrisikosystemen nach Anhang II (Art. 6 Abs. 1 KI-Gesetz-E), bei denen externe Konformitätsprüfungen nach anderen Unionsvorschriften vorzunehmen sind, erfasst die dortige Konformitätsprüfung auch die Anforderung des KI-Gesetz-E, Art. 19 Abs. 2 KI-Gesetz-E. Das Konformitätsbe-

Qualitätskontrollsystem.[195]

bb) Risikomanagementsystem

Kern der Regulierung ist ein Risikomanagementsystem: Anbieter sind verpflichtet, die Systeme regelmäßig auf Risiken zu prüfen und gegebenenfalls Risikominderungsmaßnahmen zu ergreifen.[196] Um das Risikomanagementsystem dynamisch und entwicklungsoffen zu halten, ist der Risikobegriff bewusst offen formuliert.[197] Es wird sehr allgemein von den Risiken für die Gesundheit, die Sicherheit und die Grundrechte gesprochen.[198] Schließlich gibt es keine Präzisierungen hinsichtlich möglicher Risikominderungsmaßnahmen. Eine Konkretisierungskompetenz der Europäischen Kommission ist im KI-Gesetz-E nicht vorgesehen. An der Vagheit des Risikobegriffs[199] ebenso wie an der Unvollständigkeit der Liste[200] entzündet sich einige Kritik an dem Entwurf.

---

wertungsverfahren schließt mit dem Erwerb einer CE-Konformitätskennzeichnung ab. Das CE-Kennzeichen haben Anbieter verpflichtend am Produkt anzubringen, Art. 49 KI-Gesetz-E. Insbesondere die Effektivität eines internen Konformitätsprüfungsverfahrens wird vielfach in Zweifel gezogen, siehe nur *Ebert/Spiecker gen. Döhmann*, NVwZ 40 (2021), 1188, 1191, 1193; *McCarthy Mark, Propp, Kenneth*, Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation, Lawfare, 28.04.2021; *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 12 f.; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 595; *Raposo*, Int. J. Law Inf. Technol. 30 (2022), 88, 98 f. Siehe zum externen Prüfungsverfahren eingehend *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97, 106.

[195] Art. 17 KI-Gesetz-E. Siehe umfassend zum Durchsetzungssystem des KI-Gesetz-E *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97, 110.

[196] Art. 9 KI-Gesetz-E. Zur Einordnung dieses Risikomanagementsystems im Gesamtregulierungsmechanismus des Entwurfs *Hoffmann*, K&R 20 (2021), 369, 371.

[197] Siehe zu ähnlichen Erwägungen beim DSA Kapitel 3 B. I. 1. b) bb).

[198] Siehe etwa Erwägungsgrund 43 S. 1 KI-Gesetz-E.

[199] Sehr allgemein ist im KI-Gesetz-E von Risiken für die Gesundheit, Sicherheit und die Grundrechte die Rede. Siehe etwa Erwägungsgründe 1, 32, 38, 43, 50 und 58, siehe auch Art. 7 Abs. 1 lit. b), Art. 53 Abs. 2 KI-Gesetz-E. Kritisch hierzu *Cooman*, Market and Competition Law Review 6 (2022), 49, 56; *Hoffmann*, K&R 20 (2021), 369, 372.

[200] Kritisiert wird etwa, dass die Liste Emotionserkennungssysteme nicht enthält, so *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 531; *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 12. Bemängelt wird überdies, dass überindividuelle Schutzgüter wie etwa der Umweltschutz gänzlich ausgeblendet bleiben, so *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 537; *Kalbhenn*, ZUM 65 (2021), 663, 673. Kritisch auch *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Arti-

III. Ergebnis

Der Überblick hat gezeigt, wie unterschiedlich die Regulierungsfragen in einzelnen Anwendungsbereichen sind, aber auch wie verschieden die Vorstellungen über eine gelungene Regulierung autonomer Systeme sind. Es lassen sich aber auch übereinstimmende Merkmale erkennen. Die Intransparenz im Sinne fehlender menschlicher Verständlichkeit autonomer Systeme stellt die übergreifende und wesentliche Herausforderung autonomer Systeme dar. Eine gute Regulierung muss auf diese Herausforderung demnach eine Antwort finden. Überdies wird deutlich, dass die einzelnen Anwendungen autonomer Systeme unterschiedliche Regulierungsbedarfe aufwerfen. Teilweise sind diese auch noch nicht umfassend bekannt. Eine gute Regulierung muss auch dies aufgreifen; vielfach wird daher ein risikobasierter Regulierungsansatz befürwortet.[201]

C. Die DSGVO als Instrument zur Regulierung autonomer Systeme

Zur effektiven Regulierung autonomer Systeme bedarf es des Beitrags verschiedener Rechtsinstrumente. Es bedarf daher der Koordination der einzelnen Rechtsinstrumente (I.). Die DSGVO reguliert nach ihrem Entwurf einen ganz spezifischen Ausschnitt der Regulierungsfragen autonomer Systeme (II.).

I. Regulierungskoordination als Merkmal guter Regulierung

Die obige Darstellung lässt am Ende zwei grundlegende Regulierungsansätze erkennen: Während tradierte Regulierungsansätze punktuelle Steuerungsimpulse setzen, das technikspezifische aber ausblenden, ermöglichen innovative Regulierungsmethoden eine technikspezifische Steuerung, können aber Interessenskonflikte einzelner Anwendungen nicht auflösen. Innovative Regulierungsansätze verfolgen daher nicht das Ziel, die tradierten Methoden zu ver-

---

ficial Intelligence Act), 18.06.2021, S. 8, die herausstreichen, dass das Risikokonzept nachteilige Effekte für Personengruppen sowie die Gesellschaft insgesamt nicht aufnimmt.

[201] Einen risikobasierten Ansatz forderte bereits die *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 1, 20–21, 34 sowie die *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 20. Einen risikobasierten Regulierungsansatz befürwortet auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 173–182. In diese Richtung auch der *Reisch u.a.*, Verbraucherrecht 2.0, Dezember 2016, S. 65. Zu entsprechenden Forderungen aus der Literatur siehe etwa *Martini*, Blackbox Algorithmus, 2019, S. 338; *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528; *Spindler*, CR 37 (2021), 361, 373; *Unger*, ZRP 53 (2020), 234, 236; *Hacker*, NJW 73 (2020), 2124, 2143. Kritisch *Ingold*, MMR 23 (2020), 82, 84.

drängen, sondern diese zu ergänzen. Sie stellen sich vielmehr als generell-abstrakte Regulierungszugriff dar, eine Art „Allgemeiner Teil" einer Regulierung autonomer Systeme bzw. eine Rahmenordnung.[202] Eine gute Regulierung erfolgt dann in der Kombination von punktuellen und generellen Regelungen, d.h. über die gesamte Rechtsordnung. Die *eine* Antwort auf sämtliche Regulierungsfragen autonomer Systeme gibt es nicht.[203] Zwischen den einzelnen regulativen Ansätzen besteht dann ein hoher Abstimmungsbedarf. Andernfalls stehen Friktionen und Blockaden der Regulierungsinstrumenten zu befürchten, Synergie- und Verstärkungseffekte zwischen den Rechtsinstrumenten ungenutzt zu bleiben.[204] Hieraus ergibt sich ein Kriterium für eine gelungene Regulierung: Eine gute Regelung setzt ein Verständnis für das Zusammenspiel der verschiedenen Regelungen zu autonomen Systemen voraus.[205] Nur wenn klar ist, welchen Beitrag – gemeint ist der rechtsnormative Beitrag nach der legislativen Konzeption – die einzelne Regelung erbringen kann und soll und wo ihre Grenzen liegen, kann eine effektive Regulierung autonomer Systeme durch die verschiedenen Regelungen, d.h. die Rechtsordnung insgesamt erfolgen.

II. Normativer Regulierungsbeitrag der DSGVO

Die DSGVO ist nur eines von verschiedenen Instrumenten zur Regulierung autonomer Systeme. Für eine kritische Prüfung der DSGVO und für die Entwicklung von Reformvorschlägen bedarf es eines Verständnisses dafür, wie die DSGVO sich in die verschiedenen diskutierten Regelungsvorschläge autonomer Systeme einfügt, welche Steuerungsfragen datenschutzrechtliche sind

---

[202] Vgl. hierzu mit Gegenüberstellung einer allgemeinen und einer spezifischen – dort bezeichnet als horizontalen und vertikalen – Regulierung der Künstlichen Intelligenz *Unger*, ZRP 53 (2020), 234 f.

[203] So auch *Unger*, ZRP 53 (2020), 234 f.; *Smuha*, Law Innov. Technol. 13 (2021), 57, 66 f. Vgl. auch *Geminn*, ZD 11 (2021), 354, 359. Entsprechend hat auch die Europäische Kommission ihren Entwurf für ein KI-Gesetz – hierzu sogleich – in eine größere Regulierungsprogramm eingebettet, zu denen etwa auch Regulierungen im Bereich von Maschinenprodukten zählen. Sie hierzu unten Kapitel 3 B. II. 3. b). Da autonome Systeme in ein Konglomerat an Techniken und Anwendungen eingebunden sind, könnte eine derartige isolierte Regulierung sogar nachteilige Effekte haben. Risiken, die sich im Zusammenhang mit dem Einsatz autonomer Systeme realisieren, aber in dieser Technologie nicht oder nicht allein ihren Ursprung haben, blieben so außen vor. Vgl. hierzu *Smuha*, Law Innov. Technol. 13 (2021), 57, 63 f.

[204] So auch *Smuha*, Law Innov. Technol. 13 (2021), 57, 67. Spezifisch für eine Abstimmung des DSA und des KI-Gesetz-E zur effektiven Regulierung Künstlicher Intelligenz spricht sich *Kalbhenn*, ZUM 65 (2021), 663, 674 aus.

[205] Vgl. hierzu eingehend 5 *Hoffmann-Riem*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 1, 5 f. Siehe auch, dort explizit zum Datenschutzrecht, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 8.

und welche von anderen Rechtsinstrumenten (und welchen) beantwortet werden müssen.[206] Formal reguliert die DSGVO autonome Systeme, indem sie die durch diese durchgeführten Verarbeitungen personenbezogener Daten einer Regulierung unterwirft. Erst die einzelnen Rechtsinstrumente der DSGVO lassen aber erkennen, wie dieser normative Regulierungsbeitrag ganz konkret aussieht. In substantieller Hinsicht reguliert die DSGVO autonome Systeme hinsichtlich datenschutzspezifischen Regulierungsfragen und beantwortet diese mit datenschutzspezifischen Regulierungsmechanismen. Um dies zu ermessen, bedarf es daher einer Befassung mit den Zielen und Methoden sowie mit den Prämissen und Erwartungen der DSGVO, d.h. mit dem Dahinter bzw. Davor des Datenschutzrechts. All dies wird im nachfolgenden Kapitel zu beantworten sein.

D. Ergebnis und weiterer Gang der Untersuchung

Aus der Perspektive des Rechts eröffnet das technische Phänomen autonomer Systeme ganz unterschiedliche Untersuchungsprogramme. Diese Arbeit konzentriert sich auf die Frage, wie eine gute Regulierung autonomer Systeme aussehen könnte im Sinne einer normativen Angemessenheit. Sie fokussiert dabei auf die praktische Wirksamkeit und die Fähigkeit zur Herbeiführung eines Interessensausgleichs der Regelung. Betrachtet wird dabei die DSGVO, im Fokus stehen Interessenskonflikte aufgrund von Autonomiegefährdungen und Diskriminierungen. Eine „gute“ Regulierung ist dabei eine solche, die diese Vulnerabilitätsphänomene tatsächlich effektiv unterbindet bzw. auf ein akzeptables Niveau bringt und zugleich die technische Innovation ermöglicht.

Derzeit werden verschiedene Regulierungsansätze diskutiert, die sich über die gesamte Rechtsordnung erstrecken. Unterscheiden lassen sich tradiert-punktuelle und innovativ-technikspezifische Regulierungsansätze. Vor allem werden Regelungen im Bereich der Informations- und Meinungsfreiheit diskutiert, da dort die Auswirkungen autonomer Systeme als besonders schädlich wahrgenommen werden. Im Fokus steht hier die Plattformregulierung. Im DSA hat der Unionsgesetzgeber auch einige Regelungen, die autonome Systeme adressieren, aufgenommen. Im Verbraucherschutzrecht werden Maßnahmen gegen personalisierte Werbung sowie Methoden zum Schutz der Privatautonomie von VerbraucherInnen in automatisierten Vertragsgestaltungsverfahren vorgeschlagen. Im Antidiskriminierungsrecht werden in bestimmten Bereichen Verbote gefordert, vor allem aber konzentriert sich die Diskussion auf Maßnahmen, wie autonome Systeme diskriminierungsfrei gestaltet werden könnten. In

[206] Diesen Abgrenzungs- und Koordinierungsbedarf datenschutzrechtlicher Regulierungsaufträge und solche anderer Rechtsakte fordern auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 8.

der Perspektive der Privatheit geht es vor allem um Schutzmaßnahmen gegen Übergriffe in die Privatsphäre sowie gegen manipulative Beeinflussungen. Umfangreich sind die Regelungsvorschläge zur Herstellung materieller Gerechtigkeit und Fairness; hier soll sowohl die inhaltliche Angemessenheit automatisierter Entscheidungen als auch die Fairness des Entscheidungsverfahrens abgesichert werden. Der Schutz der Menschenwürde gebietet die Definition absoluter Grenzlinien, die über die Aufstellung von Fallgruppen angenähert werden. Technikspezifisch-übergreifende Regulierungsansätze sind solche, die ein Recht auf menschliche Entscheidung fordern oder für ein Algorithmen- oder Roboterrecht eintreten. Die Europäische Kommission hat mit dem KI-Gesetz-E ein spezifisches Instrument zur Regulierung autonomer Systeme vorgegeben. Eine gute Regulierung ergibt sich am Ende durch Kombination punktueller und technikspezifischer Regelungen. Wichtig ist daher, den konkreten Regulierungsbeitrag einer jeden Regelung zu bemessen. Die DSGVO erbringt ihren Beitrag formal, indem sie die Datenverarbeitungen autonomer Systeme reguliert. Substantiell-materiell ergibt sich dieser Beitrag aus den Zielen und Mechanismen des Datenschutzrechts.

Damit ist der weitere Gang der Untersuchung vorgegeben. Im nachfolgenden Kapitel soll analysiert werden, inwieweit über die Rechtsinstrumente der DSGVO ein Interessensausgleich mit Blick auf Autonomiegefährdungen und Diskriminierungen effektiv hergestellt werden kann. Soweit die Untersuchung zu dem Ergebnis gelangt, dass dies nicht gelingt, muss über Änderungen nachgedacht werden. Ob und inwieweit diese innerhalb oder außerhalb des Regulierungsbeitrags der DSGVO liegen und ob diese de lege lata oder de lege ferenda einzuordnen sind, ist Gegenstand des 5. Kapitels.

Kapitel 4

Regulierung autonomer Systeme durch die DSGVO

Die DSGVO bietet, so das Ergebnis des vorangegangenen Kapitels, eine von verschiedenen Möglichkeiten zur Regulierung autonomer Systeme. Gegenstand des folgenden Kapitels ist es, zu klären, wie dieser Regulierungsbeitrag der DSGVO rechtstatsächlich aussieht. Es soll dann kritisch geprüft werden, ob dieser Regulierungsbeitrag ausreichend ist. Maßgeblich ist dabei, wie in Kapitel 3 dargelegt, ein an der tatsächlichen Wirkung und dem Interessensausgleich orientierter Maßstab normativer Angemessenheit. Im Fokus stehen die in Kapitel 2 beschriebenen Autonomiegefährdungen und Diskriminierungen. Geprüft werden soll also, ob die DSGVO es tatsächlich leistet, diese Autonomiegefährdungen effektiv einzudämmen, ohne zugleich in unternehmerische Interessen unangemessen einzugreifen oder die Entwicklung autonomer Systeme unverhältnismäßig zu behindern. Die Erkenntnisse bilden die Grundlage für die in Kapitel 5 zu erörternden notwendigen Anpassungen der DSGVO.

Die Arbeit kann es nicht leisten, sämtliche Instrumente der DSGVO zu untersuchen. Die Darstellung beschränkt sich daher auf die Regulierungsinstrumente der Zweckfestlegung, der Rechtmäßigkeit und der Transparenz. Mit diesen Instrumenten eng verwoben ist der Anwendungsbereich und Regulierungszugriff der DSGVO, der über die Reichweite dieser Instrumente entscheidet.

Nach den Erkenntnissen des vorangegangenen Kapitels ist zudem entscheidend, welchen Beitrag die DSGVO nach der legislativen Vorstellung überhaupt zur Regulierung autonomer Systeme erbringen kann und soll. Nur so kann die DSGVO einer fairen und angemessenen kritischen Prüfung unterworfen werden – immerhin kann und soll die DSGVO nach der gesetzgeberischen Erwartung nicht sämtliche Regulierungsfragen autonomer Systeme beantworten. Es bedarf also eines Verständnisses vom normativen Regulierungsbeitrag der DSGVO in substantieller Hinsicht. Dieser ergibt sich aus dem Sinn und Zweck des Datenschutzrechts, ebenso dann aus dem Sinn und Zweck der einzelnen Rechtsinstrumente. Bevor die einzelnen Rechtsinstrumente analysiert werden, ist daher vorab eine Darstellung grundlegender Erwartungen und Prämissen des Datenschutzrechts geboten. Auf den normativen Beitrag der zu untersuchenden Rechtsinstrumente soll im Einzelnen bei deren jeweiliger Prüfung eingegangen werden.

Was der eigentliche Inhalt und Zweck des Datenschutzrechts ist, wird äußerst kontrovers diskutiert. Das Datenschutzrecht ist rechtliches Konstrukt der westlichen, präziser, zumindest in seinen Anfängen, der europäischen Welt.[1] Es lässt bis heute verschiedenste Zuschreibungen zu. Eine erschöpfende Diskussion ist für das Erkenntnisinteresse dieser Arbeit nicht förderlich. Die Darstellung erfolgt daher nur insoweit, als dies für die Anwendung und Bewertung der DSGVO geboten erscheint.

Zunächst sollen also die grundlegenden Ziele, Vorverständnisse und Prämissen der DSGVO vorgestellt werden (A.). Im Anschluss soll dann die DSGVO auf autonome Systeme angewendet und einer kritischen Prüfung unterzogen werden und also im Einzelnen Anwendungsbereich und grundlegende Regulierungszugriffe der DSGVO (B.), der Zweckfestlegungs- und Rechtmäßigkeitsgrundsatz (C.) sowie der Transparenzgrundsatz untersucht werden (D.).

A. Regulierungskonzept und Vorverständnisse der DSGVO

Was der Unionsgesetzgeber mit dem Datenschutz erreichen wollte, welchen Regulierungsauftrag er für die DSGVO definiert und auf welche Regulierungsziele und -schutzgüter das Datenschutzrecht verweist, lässt sich über zwei Ebenen annähern: über das grundlegende Regulierungskonzept und über die Vorverständnisse und Prämissen hinter dem Datenschutzrecht. Nach dem Zuschnitt dieser Arbeit ist auf dieser höheren Abstraktionsebene besonders von Interesse, was die DSGVO spezifisch zur Eindämmung der durch die Verarbeitung personenbezogener Daten ausgelösten Autonomiegefährdungen beitragen soll.

Nachfolgend soll daher zunächst die mittlere Abstraktionsebene, d.h. das allgemeine Regulierungskonzept der DSGVO vorgestellt werden (I.), sodann

---

[1] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Albrecht*, Einleitung Rn. 184 bezeichnet die Entwicklungen des Datenschutzes zutreffend als eine „lange, gewachsene europäische Rechtskultur". Am 26.10.1970 legte die USA den Fair Credit Reporting Act vor, der auch datenschutzrechtliche Aspekte enthielt, im Fokus aber Fragen der Fairness der Kreditvergabe betraft. Vornehmlich war es damit der deutsche Gesetzgeber, im Anschluss an die Entscheidung des BVerfGE 65, 1 (1958) – *Volkszählung* der maßgeblich das Konzept des Datenschutzes entwickelte und – im Anschluss daran und auf Grundlage dessen – der europäische Gesetzgeber, siehe eingehend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 1–69, zu sekundärrechtlichen Entwicklungen vor Erlass der DSGVO Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*dies.*, Einleitung Rn. 133–154. Auch der Europarat leistete mit der 1981 gefassten Konvention 108 wesentliche Beiträge, siehe hierzu sowie zu sonstigen internationalen datenschutzrechtlichen Bemühungen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*dies.*, Einleitung Rn. 70–132.

auf einer höheren Abstraktionsebene das datenschutzrechtliche Verständnis von digitaler Autonomie erläutert werden (II.).

I. Datenschutzrechtliches Regulierungskonzept: Ziele und Mechanismen des Datenschutzrechts

Der datenschutzrechtliche Regulierungsauftrag ergibt sich einerseits aus den Regulierungsziele und Schutzgütern hinter der DSGVO (1.), andererseits aus den Regulierungsmechanismen und -methoden der DSGVO (2.).

1. Regulierungsziele und Schutzgüter der DSGVO

Welchen Regulierungszielen und Schutzgütern die DSGVO dient, wird sehr unterschiedlich gesehen. Konsens besteht insoweit, als das Datenschutzrecht natürliche Personen schützen (a)) und datenverarbeitungsspezifische Risiken für diese abwehren soll (b)). Zugleich soll es Ausgleich schaffen mit dem Interesse an einem freien Datenfluss (c)).

a) Datenschutz als Betroffenenschutz und wesentliche Schutzgüter

Schutzgut der DSGVO sind nicht die Daten, sondern die von der Datenverarbeitung betroffene natürliche Person.[2] Dabei ist das Datenschutzrecht nicht Selbstzweck,[3] es soll vielmehr Schutz bieten vor den durch die Datenverarbeitung ausgelösten Gefährdungen für subjektive Rechte der betroffenen Person,[4]

---

[2] Siehe nur *Artikel 29 Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20.06.2007, S. 4. Die Artikel 29 Datenschutzgruppe ist Vorgängerin des Europäischen Datenschutzausschusses nach der DSRL. Mit Inkraftreten der DSGVO löste der Europäische Datenschutzausschuss die Artikel 29 Datenschutzgruppe ab. Aus der Literatur *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 4; *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 15; *Albers*, in: Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, 2017, S. 11, 23. *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 168 spricht von „Subjektivierung des Datenschutzes". Zu den historischen Hintergründen siehe *ders.*, Privates Datenschutzrecht, 2020, S. 167 f. Siehe auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 4.

[3] So auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 168; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 87. Siehe *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 32 sowie *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 4, 65. Die Gefahr der Misskonzeption eines solchen Selbstzwecks betonen *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 21; *Veil*, NVwZ 37 (2018), 686, 692.

[4] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 168; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 87. Siehe auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 4, 65. Vom Schutz der Rechte der natürlichen Personen spricht auch die *Artikel 29 Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20.06.2007, S. 4.

d.h. sowohl für Verhaltensfreiheitsrechte[5] als auch Persönlichkeitsrechte.[6] Die freie Entfaltung der Persönlichkeit, d.h. die menschliche Autonomie, ist dabei Kern und übergeordnetes Ziel des Datenschutzrechts.[7] Beeinträchtigungen der Verhaltensfreiheit sind typischerweise durch Hemmeffekte oder Manipulationen ausgelöst, sie wirken demnach auf der vor- und übergelagerten Ebene der inneren Entfaltungsfreiheit,[8] die rechtsdogmatisch dem Persönlichkeitsrecht zuzuordnen ist.[9] Das Persönlichkeitsrecht ist zudem angesprochen, soweit die betroffene Person Einblicke in ihr Privatleben nicht mehr abwehren kann,[10] und der Mensch vor einer umfassenden Verdatung („gläserner Bürger", „Menschen

[5] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 108 spricht hier von einer „freiheitsakzessorischen Ebene" des Datenschutzrechts. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 39; *Hoffmann-Riem*, AöR 123 (1998), 514, 520 f. Gefährdungen für die Meinungsfreiheit, Versammlungs- und Vereinigungsfreiheit oder den Diskriminierungsschutz benennen Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 1 Rn. 13–14; Wolff/Brink, BeckOK DatenschutzR/*Schantz*, Art. 1 Rn. 6; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 29–32, 36–40; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 4 Nr. 1 Rn. 3. Welche Grundrechte genau betroffen sind und wie diese jeweils konkret gefährdet werden, lässt der Unionsgesetzgeber offen. Hieran entzündet sich vielfach Kritik, siehe nur *Veil*, NVwZ 37 (2018), 686, 693–695.

[6] Art. 1 Abs. 2 DSGVO spricht von Grundrechten und Grundfreiheiten. Die *Artikel 29 Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20.06.2007, S. 4 führt als Zwecke des Datenschutzes den „Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre" an. Zur Differenzierung von Persönlichkeits- und Freiheitsrechten, die beide je für sich gefährdet sein können, siehe *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 91 f. Vgl. auch *Nettesheim*, in: Nettesheim/Diggelmann/Lege u.a. (Hrsg.), Der Schutzauftrag des Rechts, 2011, S. 7, 25–27. Allein auf Persönlichkeitsrecht stellt *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, [3]2019, 1, 12 ab.

[7] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 109. Siehe auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 81 „[B]eim Datenschutz [geht es] (nur) rechtstechnisch um den Schutz von (personenbezogenen) Daten, final aber um etwas Vorgelagertes, den Eigenwert des Menschen". Die menschliche Autonomie als übergeordnetes Schutzgut benennen auch *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 58–61; *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 51.

[8] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 41, 43.

[9] Eingehend *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 109–111. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 31 f. Ebenso *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 81 „[F]inal [geht es] um etwas Vorgelagertes, den Eigenwert des Menschen".

[10] Siehe auch ausführlich zu verschiedenen Gefährdungen einzelner Ausgestaltungen des Persönlichkeitsrechts *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 18–55.

als (Daten-)Objekt“) geschützt werden soll.[11] Der Unionsgesetzgeber löst sich demnach von einer Privatsphärenkonzeption des Datenschutzrechts[12] und nimmt sämtliche von Datenverarbeitungen ausgehende Gefährdungen für subjektive Rechte der betroffenen Person in den Blick.[13] Schutzziel des Datenschutzrechts ist auch die freiheitliche Demokratie: Die DSGVO soll staatliche oder private Informations- und Machtasymmetrien und den Missbrauch von (staatlicher) Informationsmacht verhindern,[14] überdies durch Absicherung der Freiheit der BürgerInnen auch die liberale Gesellschafts- und Staatsordnung insgesamt absichern.[15]

---

[11] Vgl. *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 19; *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 306–308; *Tzanou*, The fundamental right to data protection, 2019, S. 29–31.

[12] Vgl. Sydow, DS-GVO/*Sydow*, Art. 1 Rn. 10–11; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 29, 32, 36 sowie *Gellert/Gutwirth*, CLSR 29 (2013), 522, 530; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 85–87; *Reinhardt*, AöR 142 (2017), 528, 540; *Tzanou*, The fundamental right to data protection, 2019, S. 25. Es bedarf damit nicht des Nachweises, dass die Daten der Privatsphäre zugeordnet sind, um die Schutzwirkung des Datenschutz(grund)rechts auszulösen, der Personenbezug genügt, vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 38. Dies wird auch darin deutlich, dass Privatheit und Datenschutz als je eigenständige Grundrechte in Art. 7 bzw. Art. 8 GRCh normiert sind. Vgl. auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 217–219; *González Fuster/Gutwirth*, CLSR 29 (2013), 531, 535 f. Nur Datenverarbeitungen, die gerade die Privatheit gefährden, lassen eine Heranziehung des Art. 7 GRCh zu, siehe *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 209–217.

[13] So etwa Gefährdungen für die Meinungsfreiheit, Versammlungs- und Vereinigungsfreiheit oder den Diskriminierungsschutz, vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 1 Rn. 13–14; Wolff/Brink, BeckOK DatenschutzR/*Schantz*, Art. 1 Rn. 6; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 29–32, 36–40; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 4 Nr. 1 Rn. 3. Welche Grundrechte genau betroffen sind und wie diese jeweils konkret gefährdet werden, lässt der Unionsgesetzgeber offen. Auch hieran entzündet sich vielfach Kritik, siehe nur *Veil*, NVwZ 37 (2018), 686, 693–695. Vgl. zur Vielfalt der Schutzziele und -bedürfnisse auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 88.

[14] *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 55–62. Siehe hierzu auch Generalanwalt Pitruzzella, Schlussanträge v. 27.01.2022, Rs. C-817/19, ECLI:EU:C:2022:65, Einleitung Rn. 2 – *Ligue des droits humains*.

[15] Siehe hierzu schon BVerfGE 65, 1 (43) [1958] – *Volkszählung*: „Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist“. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 31–35; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 94; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 43; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Einleitung Rn. 16. Die Bedeutung der selbstbestimmten und ungehinderten Teilnahmefähigkeit an der öffentlichen Debatte beruht wesentlich auf Gedanken von *Habermas*. Ihm zufolge ist ein freiheitliches

b) Schutz vor datenverarbeitungsspezifischen Risiken

Die DSGVO schützt vor punktuellen Gefährdungen durch Datenverarbeitungen,[16] sie hat aber vor allem die Gefährdung durch eine intransparente und unregulierte Dateninfrastruktur insgesamt im Blick.[17] Diese Gefährdungen lassen

---

Gemeinwesen nur möglich, wenn eine unbeschränkte politische Debatte stattfinden kann; diese legitimiert und begrenzt staatliche wie private Macht. Wird der Einzelne durch unbegrenzte staatliche Beobachtungs- und Überwachungsmöglichkeiten in seiner kommunikativen Ungehemmtheit behindert, gibt es keine politische Öffentlichkeit mehr, die machtbegrenzend wirken könnte. Dies rechtfertigt und begründet datenschutzrechtliche Interventionen. Zur Kommunikationstheorie siehe eingehend *Habermas*, Faktizität und Geltung, [5]1997, S. 491–494, 503–505, zur Bedeutung der Erwägungen für den Datenschutz *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 188 f.

[16] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 108 spricht hier von einer freiheitsakzessorischen Dimension des Datenschutzes und meint damit solche Gefährdungen, die von einer einzelnen Datenverarbeitung für eine konkrete Verhaltensfreiheit ausgeht. Siehe zu dessen dreidimensionalen Modell vom Datenschutzrecht unter Kapitel 4 A. 1. b). Je nach Inhalt des Datums, den Verarbeitungsumständen oder dem Verwendungszweck kann die Datenverarbeitung eine Beeinträchtigung individueller Freiheit darstellen. Dies ist gemeint, wenn das BVerfGE 65, 1 (45) [1958] – *Volkszählung* davon spricht, dass kein Datum „belanglos" sein kann. Dem folgt man auch auf unionaler Ebene, siehe nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 242. Kritisch hierzu *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 28–32.

[17] Vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 38. Es ist vor allem der Umstand, dass sich die betroffene Person ubiquitär und unbegrenzt Datenverarbeitungen ausgesetzt sieht, die sie weder durchschauen, noch abwehren oder steuern kann, der Hemmeffekte auslöst, so prominent BVerfGE 65, 1 (42–43) [1958] – *Volkszählung.* So auch Generalanwalt Pitruzzella, Schlussanträge v. 27.01.2022, Rs. C-817/19, ECLI:EU:C:2022:65, Einleitung Rn. 2 – *Ligue des droits humains*. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 32; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 29. Erst durch diese Intransparenz und Unkontrolliertheit insgesamt werden Informationsasymmetrien begründet, betroffene Personen gegenüber manipulativen Übergriffen schutzlos gestellt oder auf lange Sicht eine umfassende „Verdatung" der betroffenen Person ermöglicht. Es geht einerseits um Dystopien einer unbegrenzten Überwachung („Big Brother"), so BVerfGE 65, 1 (42) [1958] – *Volkszählung:* „unkontrollierte Persönlichkeitserfassung"; Generalanwalt Pitruzzella, Schlussanträge v. 27.01.2022, Rs. C-817/19, ECLI:EU:C:2022:65, Einleitung Rn. 2 – *Ligue des droits humains* „digitales Panoptikum". Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 30. Andererseits geht es um Gefährdungen aufgrund der Undurchschaubarkeit von datenbasierten Entscheidungen oder sonstigen Folgen („kafkaeske Situation", Bezug nehmend auf das Schicksal der Romanfigur Josef K. in Kafkas Roman „Der Prozess"), vgl. auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 112. Eingehend auch *Lynskey*, ICLQ 63 (2014), 569, 592. Ebenso wird bei autonomen Systemen dieses dystopische Bild einer kafkaesken Situation herangezogen, dort ist es aber die Undurchschaubarkeit der algorithmischen Entscheidungsarchitektur, die Hemmeffekte begründe. Siehe Kapitel 2 C. IV. 2. d).

sich konkretisieren und so bestimmte datenverarbeitungstypische Risiken benennen.[18] Unterscheiden lassen sich technikspezifische Risiken (Informationspermanenz,[19] Informationsemergenz,[20] Entkontextualisierung,[21] Fehleranfälligkeit,[22] Klassifizierung und Diskriminierung,[23] Ubiquität, Sicherheit[24]), marktbezogene Risiken (Konstruktion neuer Machtasymmetrien[25]) sowie Risiken aufgrund fehlender Selbstschutzfähigkeit (technische Überforderung, Intransparenz, fehlende Einwirkungs- und Kontrollmöglichkeiten).[26] Diese Liste ist nicht erschöpfend.

c) Interessenausgleich zwischen Datenschutz und Datenfluss

Die DSGVO zielt darüber hinaus darauf ab, den freien Datenfluss zu garantieren,[27] der für eine freiheitliche Staats- und Gesellschaftsordnung und Wirtschaft unter modernen Bedingungen essentiell ist.[28] Sie soll einen Interessen-

---

[18] Eine Spezifizierung des Datenschutzrechts über die Gefährdungsebene befürwortet auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 87 f.

[19] Gemeint ist die dauerhafte Speicherung der gewonnenen Informationen, *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 299–301.

[20] Die Datenverarbeitung lässt Erkenntnisse jenseits des einzelnen verarbeiteten Datums zu, *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 304 f. Dies betrifft gerade den Fall der Profilbildung. Hierzu zählen auch unerwünschte Einblicke in die Persönlichkeit, siehe zu diesem Risiko *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 294 f.

[21] *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 301–304.

[22] *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 305 f.

[23] Dies kann zu Diskriminierungen und Stigmatisierungen führen, *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 295–299.

[24] Den Datenmissbrauch benennt *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 291–294.

[25] *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 280–282. Hierin erkennt *Lynskey*, ICLQ 63 (2014), 569, 592 f. die eigentliche vom Datenschutz adressierte Gefährdung. Siehe auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 55–56, 77–78.

[26] In ähnlicher Weise konstruiert *Lewinski* die Risiken von den Schutzgütern her und macht als solche den Eigenwert des Menschen, den Schutz physischer, logischer und sozialer Räume, die informationelle Selbstbeschränkung, die informationelle Gestaltung und Verfügung sowie das gesellschaftliche Informationsgleichgewicht aus. Eingehend *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 17–63.

[27] Zu diesem Doppelziel siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 235; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 5, 21, 27; *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 57.

[28] Eine allzu ausgreifende Datenregulierung kann demnach ebenso gemeinwohlschädlich sein wie eine unterbleibende. So bereits *Hoffmann-Riem*, AöR 123 (1998), 514, 519–521. Eingehend hierzu unter Heranziehung von kommunikationstheoretischen Erwägungen von *Habermas Bunnenberg*, Privates Datenschutzrecht, 2020, S. 188 f. In diese Richtung auch

ausgleich zwischen Datenschutz und Datenfluss ermöglichen.[29] Die DSGVO zielt daher nicht auf Unterbindung, sondern auf (strukturierende) Zulassung von Datenverarbeitungen ab.[30]

2. *Regulierungsmechanismen und -methoden der DSGVO*

Um betroffene Personen vor datenverarbeitungsspezifischen Risiken im Vorfeld zu schützen und dabei zugleich Datenverarbeitung zu ermöglichen, etabliert die DSGVO ein allgemeines Datenstrukturierungsmodell (a)), das substantiell maßgeblich durch die Datenschutzgrundsätze ausgestaltet wird (b)). Die DSGVO reguliert aber nicht die Datenverarbeitungstechnik (c)).

a) *Datenstrukturierung statt informationellem Selbstbestimmungsrecht*

Welches Schutzinstrumentarium das Datenschutzrecht auf unionaler Ebene bietet, ist nicht ganz klar. Gegenüber stehen sich Konzeptionen, die das Datenschutzrecht als individuelle Verfügungsmacht der betroffenen Person über „ihre" Daten begreifen,[31] und solche, die das Datenschutzrecht als objektivier-

---

Lewinski, Die Matrix des Datenschutzes, 2021, S. 83; *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 75 f. Auf die Notwendigkeit umfassender Datenverarbeitung durch den Staat für die Gewährleistung von Sicherheit und damit den Ausgleich von Gemeinwohl und Individualfreiheit weist Generalanwalt Pitruzzella, Schlussanträge v. 27.01.2022, Rs. C-817/19, ECLI:EU:C:2022:65, Einleitung Rn. 2 – *Ligue des droits humains* hin.

[29] Datenschutz soll also sowohl subjektive Rechte der betroffenen Person, gerade auch auf der Vorgelagerten Ebene deren Autonomie, sowie die Interessen am freien Datenfluss gewährleisten. Anschaulich spricht *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 51 vom Anspruch, „eine komplexe Vielzahl von Schutzanliegen lagenspezifisch in bestmöglicher Weise zum Ausgleich zu bringen". Vgl. hierzu auch, dort im Rahmen des Rechtmäßigkeitsgrundsatzes, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 35.

[30] Siehe nur *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 154, 157; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 4–5; Sydow, DS-GVO/*Sydow*, Einleitung Rn. 71; *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61, 76 f.; *González Fuster/Gutwirth*, CLSR 29 (2013), 531, 536 f.; *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 57. Vgl. auch *Hoffmann-Riem*, AöR 123 (1998), 514, 519–521. Siehe hierzu auch im Rahmen des Rechtsmäßigkeitsgrundsatzes unter Kapitel 4 C. I. 2. b) aa).

[31] So etwa *Lynskey*, ICLQ 63 (2014), 569, 591 f.; Gola, DS-GVO/*Gola/Heckmann*, Einleitung Rn. 1, 3; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 21; Kühling/Buchner, DS-GVO, BDSG/*Kühling/Raab*, Einführung Rn. 26; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Einleitung Rn. 1, 12a; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 3; Ehmann/Selmayr, DS-GVO/*Selmayr/Ehmann*, Einführung Rn. 9. Diese Konzeption hat ihre Wurzeln im Recht auf informationelle Selbstbestimmung wie es insbesondere im deutschen Rechtsraum im Staat-Bürger-Verhältnissen in den 1970er Jahren geprägt wurde. Zum deutschen Verfassungsrecht etwa Dürig/Herzog/Scholz, GG/*Di Fabio*,

tes Datenstrukturierungsregime verstehen.[32] Der Europäische Datenschutzausschuss,[33] teilweise auch die Generalanwälte am EuGH,[34] sprechen sich für ein Datenkontrollrecht aus, der EuGH positioniert sich bislang nicht eindeutig.[35] Maßgeblich hängt dies auch vom Vorverständnis des Datenschutzrechts und den Konzeptionen digitaler Autonomie ab, hierauf ist zurückzukommen.[36] Be-

---

Art. 2 Abs. 1 Rn. 175. Siehe aus US-amerikanischer Perspektive *Allen*, Connectivut Law Review 2000, 861–875.

[32] So etwa *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61, 93–96; *Eifert*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 365, 371 f.; Kuner/Bygrave/Docksey, GDPR/*Hijmans*, Article 1 Subject-matter and objectives Rn. 56; *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, Rn. 51, 56, 64. In diese Richtung auch *Tzanou*, The fundamental right to data protection, 2019, S. 13. Drei Ebenen des unionalen Datenschutzgrundrechts – abwehrrechtliche, instrumentelle und objektiv-rechtliche –, wobei der Kern in der objektivrechtlichen liegen soll, erkennt *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 107–124. Für das deutsche Verfassungsrecht *Hoffmann-Riem*, AöR 123 (1998), 514, 521–524; *Trute*, JZ 53 (1998), 822, 825 f. Siehe dort auch umfassend die Konzeptionen eines über zwei Ebenen – eine, die einen grundlegenden Schutz bietet, eine, die spezifische Schutzbedarfe einzelner Freiheitsrechte absichert – konstruierten Datenschutzes *Albers*, Informationelle Selbstbestimmung, 2005, S. 590–605; *Albers*, in: Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, 2017, S. 11, 30 f. Ablehnend gegenüber einem Recht auf informationelle Selbstbestimmung im Sinne eines eigentumsanalogen Verfügungsrechts äußern sich auch *Koops*, Int. Data Priv. Law 4 (2014), 250, 251–253; *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 51 f.; *Veil*, NVwZ 37 (2018), 686, 687 f.

[33] Zuletzt *Europäischer Datenschutzausschuss*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 05.12.2022, S. 36 f. Siehe überdies *ders.*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 17.

[34] Ausdrücklich Generalanwalt Villalón, Schlussanträge v. 12.12.2013, Rs. C-293/12, ECLI:EU:C:2013:845, Rn. 49 – *Digital Rights Ireland Ltd.*In diese Richtung etwa Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 53–64 – *Meta Platforms Inc. u.a./Bundeskartellamt*. AA Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 68–77 – *UI gegen Österreichische Post AG*; Generalanwalt Pitruzzella, Schlussanträge v. 27.01.2022, Rs. C-817/19, ECLI:EU:C:2022:65, Rn. 65 – *Ligue des droits humains*.

[35] Der EuGH spricht allgemein vom Schutz personenbezogener Daten, ohne zu spezifizieren, was damit gemeint ist. Zugleich weist er darauf hin, dass dieser Schutz nicht absolut gilt, sondern mit kollidierenden Interessen von Staat und Gesellschaft abzuwägen sind. So etwa EuGH, Urteil v. 16.07.2020, Rs. C-311/18, EU:C:2020:559, Rn. 172 – *Facebook Ireland und Schrems* m.w.N. Siehe auch die Analysen bei *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 105–107 unter Zitierung weiterer Entscheidungen. Der EGMR, auf dessen Rechtsprechung der EuGH sich maßgeblich vor Inkrafttreten der EU-Grundrechtecharta stützte, erkennt kein Recht auf informationelle Selbstbestimmung an, vgl. eingehend die Analyse bei *ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 8–14.

[36] Siehe unten Kapitel 4 A. II. 3.

reits die formale Ausgestaltung steht allerdings einem Verständnis der DSGVO als individuelles Datenkontrollrecht entgegen: Sie normiert nicht allein individuelle Verfügungs- und Betroffenenrechte, sondern sieht verschiedene Schutzinstrumente und -mechanismen vor.[37] Auch die Schutzziele der DSGVO widersprechen einem solchen Verständnis: Die DSGVO löst sich von einer Privatheitskonzeption des Datenschutzrechts; es geht also nicht (allein) um Datengeheimhaltung.[38] Zudem zielt die DSGVO auf Schutz und Ausgleich des Interesses an einem freien Datenfluss ab. Ein Datenkontrollrecht erlaubte demgegenüber willkürliche Zurückhaltung und priorisierte damit einseitig Datenschutz.[39] Da Datenschutz betroffene Personen vor den datenverarbeitungsspezifischen Gefährdungen ihrer subjektiven Rechte schützen soll, bedarf es individueller Datenkontrolle ohnehin nicht, um Datenschutz zu gewährleisten.

b) Konkretisierung des Strukturierungsauftrags durch Datenschutzgrundsätze

Inhaltlich wird dieser Datenschutzstrukturierungsauftrag durch die Datenschutzgrundsätze konkretisiert.[40] Vornehmlich sind diese in Art. 5 DSGVO

---

[37] So auch *Nettesheim*, Digitale Autonomie in Vertragsbeziehungen, Verfassungsblog, 12.10.2022; Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 73 – *UI gegen Österreichische Post AG*.

[38] So Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 82 – *UI gegen Österreichische Post AG*. *De Hert und Gutwirth* haben hierzu ein Modell zur Abgrenzung von Datenschutz und Privatheit entwickelt. Während das Recht auf Privatheit auf Abwehr unerwünschter Einblicke abzielt und also auf Datenzurückhaltung, geht es beim Datenschutzrecht im Kern um Zulassung, dabei aber um beschränkende Zulassung, um die Gemeinwohlverträglichkeit der Datenverarbeitung abzusichern. Für diese Unterscheidung prägen sie die Begriffe opacity (Unterbindung) und der transparency (Zulassung). Grundlegend *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61 Siehe auch *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271; *Gellert/Gutwirth*, CLSR 29 (2013), 522–530. Befürwortend *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 113, 154; *Gellert/Gutwirth*, CLSR 29 (2013), 522, 525, 529–530; *Lynskey*, ICLQ 63 (2014), 569, 595 f.; *Tzanou*, The fundamental right to data protection, 2019, S. 36 f.

[39] Siehe zu diesem Argument auch Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 78 – *UI gegen Österreichische Post AG*.

[40] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 139–142, demzufolge die in Art. 8 Abs. 2 GRCh normierten Datenschutzgrundsätze das Datenschutzgrundrecht näher definieren. Siehe auch *Tzanou*, The fundamental right to data protection, 2019, S. 42 f., derzufolge der Wesensgehalt des Datenschutzgrundrechts sich aus den Datenschutzgrundsätzen ergebe.

normiert, weitere kommen in der DSGVO implizit zum Ausdruck.[41] Im Kern lassen sich fünf Prinzipien ausmachen: Rechtmäßigkeit im Sinne präventiver Zulassungskontrolle,[42] Fairness,[43] Transparenz,[44] Erforderlichkeit sowie Angemessenheit[45] und Sicherheit bzw. Robustheit.[46] Im Rahmen dieser Arbeit werden Rechtmäßigkeit und Transparenz näher untersucht.

---

[41] Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 5 Rn. 8; *Roßnagel*, ZD 9 (2018), 339, 341 f.; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 29.

[42] Art. 5 Abs. 1 lit. a) DSGVO.

[43] Art. 5 Abs. 1 lit. a) DSGVO „nach Treu und Glauben". Als übergreifendes Prinzip lässt sich die Herstellung von Waffengleichheit zwischen betroffenen und verarbeitenden Personen ausmachen. Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 17. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 47, der fallgruppenartig den Missbrauch von Vertrauen oder die schädliche Ausnutzung eines Kräfteungleichgewichts benennt. Überwiegend wird der Grundsatz der Fairness als Auffangtatbestand bzw. als Korrektiv verstanden, der dort Schutz bieten soll, wo die übrigen Datenschutzgrundsätze nicht hinreichend effektiv oder präzise wirken. Vgl. eingehend Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Schwartmann/Hermann*, Art. 5 Rn. 31 f.; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 17; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 47; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Buchholtz/Stentzel*, Art. 5 Rn. 25; Paal/Pauly DS-GVO/*Frenzel*, Art. 5 Rn. 20.

[44] Art. 5 Abs. 1 lit. a) DSGVO.

[45] Der Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c) DSGVO, und der Speicherbegrenzung, Art. 5 Abs. 1 lit. e) DSGVO, sind in zeitlicher, räumlicher und sachlicher Hinsicht gefasste Korrektive gegen eine unbegrenzte Datenverarbeitung. Zudem sollen sie die Steuerungswirkung der übrigen Datenverarbeitungsgrundsätze, vor allem des Zweckfestlegungsgrundsatzes, verstärken. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 80, 82; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 56, 65.

[46] Normiert ist das Gebot der Datenrichtigkeit, Art. 5 Abs. 1 lit. d) DSGVO und der Grundsatz der Integrität und Vertraulichkeit der Technik, Art. 5 Abs. 1 lit. f) DSGVO. Das Gebot der Datenrichtigkeit hat fehlerhafte, unvollständige oder veraltete Daten, d.h. gegen datenverarbeitungsinterne und unbeabsichtigte Störungen im Blick hat, siehe ausführlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 136–141; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Schwartmann/Hermann*, Art. 5 Rn. 61 f.; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 60–62; Wolff/Brink, BeckOK DatenschutzR/*Schantz*, Art. 5 Rn. 27–32. Die Integrität und Vertraulichkeit zielt auf den Schutz vor datenverarbeitungsexternen, gezielten Schädigungen durch unbefugte Zugriffe Dritter ab, siehe Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Schwartmann/Hermann*, Art. 5 Rn. 75; Sydow, DS-GVO/*Reimer*, Art. 5 Rn. 48–50, sowie auf oder sonstiger unbeabsichtigte Schadensereignisse, Paal/Pauly DS-GVO/*Frenzel*, Art. 5 Rn. 47; Wolff/Brink, BeckOK DatenschutzR/*Schantz*, Art. 5 Rn. 35 f. Ausführlich Sydow, DS-GVO/*Reimer*, Art. 5 Rn. 47–52.

c) Grundsatz der Technikneutralität

Die DSGVO verfolgt einen technikneutralen Regulierungsansatz.[47] Sie stellt demnach keine spezifischen Anforderungen an die Verarbeitungstechniken oder Ergebnisse[48] und sie findet Anwendung in sämtlichen datenverarbeitenden Systemen unabhängig von der eingesetzten Technik oder anvisierten Verwendung.[49] Der Grundsatz der Technikneutralität soll die DSGVO vor allem dynamisch und zukunftssicher machen.[50] Der Unionsgesetzgeber verbindet damit die Erwartung, dass die DSGVO sämtliche datenschutzrechtliche Fragen, auch von erst noch zu entwickelnden datenverarbeitenden Systemen, umfassend adressieren kann. Rechtstechnisch wird dies umgesetzt, indem Verarbeitungs- und Verwendungstechniken nicht benannt werden,[51] indem prozedurale vor inhaltlich-substantiellen Rechtsinstrumenten bevorzugt werden,[52] vor allem aber, indem die DSGVO sehr abstrakt formuliert ist und so Konkretisierungen und Anpassungen an zukünftige Verarbeitungstechniken zulässt.[53] Dieser hohe Abstraktionsgrad ist zugleich Anlass für Kritik. So ist

---

[47] Siehe allgemein zum Grundsatz der Technikneutralität *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, S. 323, 324; *Hildebrandt/Tielemans*, CLSR 29 (2013), 509, 511. Genau genommen handelt es sich nicht um eine Technikneutralität, sondern eine Technikausgestaltungsneutralität. Denn mit Bezug auf die Digitaltechnik wird ja eine bestimmte Technik reguliert, allein Verfahren, Anwendung und Einsatzbereiche sind irrelevant. Siehe zu dieser Unterscheidung eingehend *Reed*, SCRIPed 4 (2007), 263, 269–273.

[48] Vgl. zu diesem Verständnis der Technikneutralität *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 72; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 6.

[49] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 241.

[50] In dieser Dynamisierung der DSGVO wird gemeinhin der eigentliche Wert des Grundsatzes der Technikneutralität gesehen, siehe nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*dies.*, Einleitung Rn. 241. Siehe auch *Reding*, ZD 2 (2012), 195, 198: „Der EU-Gesetzgeber hatte 1995 der Versuchung widerstanden, jede Einzelheit der seinerzeit aktuellen Erfahrungen im Gesetzestext detailliert regeln zu wollen. Diese richtige Grundentscheidung wurde in die vorgeschlagene DSGVO übernommen. […] Es sollte aber nicht versucht werden, jede Frage, die den Datenschutz in Europa in den nächsten 20 Jahren beschäftigen könnte, bereits heute im Detail regeln zu wollen".

[51] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 241.

[52] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*dies.*, Einleitung Rn. 214, 311.

[53] Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 241; *Martini*, Blackbox Algorithmus, 2019, S. 157; *Vatanparast*, ZaöRV 80 (2020), 819, 833. Siehe zur technikneutralen Ausgestaltung verschiedener Schutzinstrumente der DSGVO, insbesondere zu Betroffenenrechten, *Roßnagel/Richter/Nebel*, ZD 3 (2013), 103, 105–108. Anschaulich am Beispiel der Datenportabilität nach Art. 20 DSGVO *Wong/Henderson*, IDPL 9 (2019), 173–191. Siehe allgemein auch *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, S. 323, 325.

immer wieder bemängelt worden, dass der Unionsgesetzgeber in der DSGVO die Konfliktfälle nicht aufgelöst,[54] sondern dies den Rechtsanwendern überlassen hat.[55] Die DSGVO biete nur ein unzureichendes Rahmengesetz.[56] Kritisiert wird auch, dass aufgrund der fehlenden Technikspezifizierung die Regulierungsbedarfe digitaler Systeme nicht mehr adressiert werden können.[57] Ob diese These im Hinblick auf autonome Systeme zutreffend ist, ist Untersuchungsziel dieser Arbeit.

---

[54] Spezifisch zu hieraus folgenden Regulierungsdefiziten mit Blick auf aktuelle Entwicklungen digitaler Systeme Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 311. Allgemein *Sydow/Kring*, ZD 4 (2014), 271, 272; *Roßnagel*, DuD 40 (2016), 561, 565. Deutlich *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 361, 374: „Zu den geschilderten Herausforderungen und den Gefährdungen aller wichtige Bedingungen des Datenschutzes enthält die Datenschutz-Grundverordnung keine einzige Regelung. Keines der künftigen, aber klar absehbaren Risiken für die Grundrechte werden von der Verordnung adressiert". Ihm zufolge „bewirkt die die übertriebene Technikneutralität eine umfassende Risikoneutralität", siehe *ders.*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 361, 375. Kritisch auch *Hornung*, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, S. 315, 331.

[55] So ausdrücklich *Reding*, ZD 2 (2012), 195, 198: „Die Anwendung der Grundsätze der Datenschutzverordnung auf einzelne Dienste und Anwendungen muss den nationalen Datenschutzbehörden und den Gerichten überlassen bleiben". Ebenso, wenn auch kritisch *Hornung*, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, S. 315, 323: „Ganz offensichtlich hat sich der europäische Gesetzgeber insoweit entschieden, wesentliche Fragen der materiellen Rechtmäßigkeit der Datenverarbeitung nicht zu entscheiden und damit anderen zu überlassen". Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 241. Kritisiert wird daran, dass die wesentlichen Entscheidungen und Wertungen nicht vom Unionsgesetzgeber getroffen wurden, so *Roßnagel/Richter/Nebel*, ZD 3 (2013), 103, 104; *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, S. 323, 332. So auch *Hildebrandt/Tielemans*, CLSR 29 (2013), 509, 520. Einbußen hinsichtlich der Schutzeffektivität der DSGVO aufgrund des abstrakt gehaltenen Regulierungsansatzes betonen *Roßnagel*, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, 2009, S. 323, 334. *Hornung*, in: Roßnagel/Friedewald/Hansen (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, S. 315, 330 spricht von einem „Verlustgefühl" der Steuerung.

[56] Zum Begriff die Vizepräsidentin der Europäischen Kommission und Justizkommissarin *Reding*, ZD 2 (2012), 195, 198, die diese bewusst offene Redaktion der DSGVO gleichwohl positiv bewertet. Sehr kritisch hierzu *Roßnagel/Richter/Nebel*, ZD 3 (2013), 103, 106, die von einer bloßen „Ankündigungsgesetzgebung" sprechen.

[57] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 241, denen zufolge es eigenständiger Regulierungen neben der DSGVO bedarf, soweit technische Entwicklungen auf den Markt treten, die so disruptiv sind, dass die von ihnen ausgelösten Gefährdungen von der DSGVO nicht oder jedenfalls nicht sinnvoll adressiert werden können.

3. Ergebnis: Regulierungsbeitrag der DSGVO auf einer mittleren Abstraktionsebene

Die DSGVO schützt Rechte und Interessen betroffener Personen, vornehmlich ihre Persönlichkeitsrechte, vor Gefährdungen aufgrund unkontrollierter und intransparenter Datenverarbeitung und soll zugleich Ausgleich schaffen mit dem Interesse an einer freien Datennutzung. Darin liegt ihr normativer Beitrag zur Regulierung autonomer Systeme. Dies erfolgt durch ein umfassendes, objektiv-rechtliches Datenstrukturierungsprogramm. Die DSGVO etabliert kein Recht auf informationelle Selbstbestimmung. Inhaltliche Strukturierungsziele sind dabei Rechtmäßigkeit, Fairness, Transparenz, Erforderlichkeit und Angemessenheit sowie Sicherheit und Robustheit. Die DSGVO ist technikneutral ausgestaltet, reguliert also nicht eine bestimmte Technik oder Anwendung von Datenverarbeitungen und ist unabhängig dieser Techniken oder Verwendung anwendbar.

II. Datenschutzrechtliche Vorverständnisse: „Digitale Autonomie" durch Datenschutz

Auf einer vorgelagerten Ebene zielt die DSGVO auf Schutz und Gewährleistung digitaler Autonomie ab. Diese juridisch konzipierte digitale Autonomie grenzt sich von außerjuridischen, interdisziplinären Autonomieverständnissen ab (1.). In der Rechtswissenschaft werden verschiedene Annäherungen vorgeschlagen, um die digitale Autonomie mit Inhalt zu füllen (2.). Zur Gewährleistung digitaler Autonomie etabliert die DSGVO zwischen Privaten vornehmlich ein dezentrales Schutzregime. Sie begreift digitale Autonomie dabei nicht als individuelle Datenkontrolle (3.).

1. Abgrenzung: juridische und außerjuridische Autonomieverständnisse

Menschliche Autonomie ist ein schillerndes und diffuses Konzept.[58] Nach aktuellen neurowissenschaftlichen Erkenntnissen ist es durchaus zweifelhaft, ob

[58] Siehe beispielhaft zu Ansätzen aus philosophischer Sicht *Betzler* (Hrsg.), Autonomie der Person, 2013; *Seidel*, Selbst bestimmen, 2016; *Rössler*, Autonomie, 2017; *Heiden* (Hrsg.), Hat der Mensch einen freien Willen?, 2008, aus naturwissenschaftlicher, insbesondere neurowissenschaftlicher und psychologischer Sicht *Soon/Brass/Heinze u.a.*, Nature neuroscience 11 (2008), 543–545; *Völker*, Wie Menschen entscheiden, 2018; *Heinze/Fuchs/Reichies* (Hrsg.), Willensfreiheit – eine Illusion?, 2006. Siehe auch die interdisziplinären Bearbeitungen der Thematik bei *Kane* (Hrsg.), The Oxford handbook of free will, 2011; *Mele* (Hrsg.), Surrounding free will, 2015. Zur vielschichtigen und ambivalenten Aufladung des Begriffs und des Konzepts menschlicher Autonomie als wissenschaftlicher Gegenstand siehe nur *Bumke*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 3, 4–9. Er schlägt eine Definition vor, wonach der Mensch autonom ist, wenn er nach seinem freien Willen eine Entscheidung treffen (innere Autonomie) und diese realisieren kann (äußere Autonomie), vgl. *ders.*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 3, 9 f.

der Mensch überhaupt je tatsächlich autonom entscheiden kann.[59] In einer liberalen Rechtsordnung ist die menschliche Autonomie notwendige Bedingung.[60] Entsprechend wird in der juridischen Perspektive schlicht angenommen, man mag auch sagen fingiert, dass der Mensch autonom sein kann, und entwirft Voraussetzungen für die Existenz menschlicher Autonomie, um hieran rechtliche Instrumente zu knüpfen, vor allem Verantwortungszuschreibungen und Schutzkonzepte.[61] Dieses juridische Bild menschlicher Autonomie ist aus realwissenschaftlicher Sicht idealistisch und verkürzt.[62] Solange es aber durch realwissenschaftliche Erkenntnisse nicht gänzlich überholt ist, kommt es nicht zu Wertungswidersprüchen, denn das juridische Konzept erhebt allein für die Rechtsordnung und deren Funktionsfähigkeit den Anspruch der Gültigkeit. Gemeinhin besteht Konsens, dass das juridische Autonomieverständnis, zumindest derzeit, nicht realwissenschaftlich widerlegt ist.[63] Wenn im Weiteren von menschlicher Autonomie die Rede ist, so ist damit das rechtliche Konzept gemeint, wie es sich in einzelnen Rechtsinstrumenten, hier dann also der DSGVO darstellt. Aussagen über die tatsächliche Existenz und die Bedingungen menschlicher Autonomie in Anbetracht autonomer Systeme sind damit nicht

---

[59] Grundlegend *Libet*, Behavioral and Brain Sciences 8 (1985), 529–539 Siehe auch *Nahmias*, Wie frei ist der Mensch?, Spektrum 20.08.2015, https://www.spektrum.de/news/wie-frei-ist-der-mensch/1361221.; *Soon/Brass/Heinze u.a.*, Nature neuroscience 11 (2008), 543–545. Zur philosophischen Kritik hieran siehe etwa *Smith*, Nature 477 (2011), 23–25; *Walter*, Illusion freier Wille?, 2016.

[60] Autonomie ist Prämisse und eigentliches Ziel des Grundrechteschutzes, Autonomie bedarf es aber auch zur Zuordnung straf- und zivilrechtlicher Verantwortung sowie zur Ausübung staatsbürgerlicher Rechte. Die Autonomie ist darüber hinaus tragendes Prinzip für die rechtliche Ausgestaltung der Beziehungen zwischen Privaten – dann ist die Autonomie im Sinne der Privatautonomie gemeint, siehe hierzu *Bumke*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 3, 11–13. Auch der rechtliche Autonomiebegriff ist mehrdeutig, kann Rechtsprinzip, Tatbestandsmerkmal oder Zweck eines Rechtsakts sein, vgl. *ders.*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 3, 10 f.

[61] Vgl. eingehend zum rechtlichen Autonomiebegriff, seinen Inhalten und Funktionen *Bumke/Röthel* (Hrsg.), Autonomie im Recht, 2017.

[62] Zur Autonomie als juridisches Ideal siehe auch *Bumke*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 3, 36.

[63] In diese Richtung auch *ders.*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 3, 17 f. Anliegen der Rechtswissenschaft ist es vielmehr, Erkenntnisse der Neurowissenschaft über die Autonomie des Menschen in die Rechtsgestaltung und -auslegung zu integrieren. Die Schnittstelle wird als Neurojurisprudenz, im US-amerikanischen Raum als Neurolaw bezeichnet. Siehe hierzu etwa *Kruse*, NJW 73 (2020), 137–139; *D'Aloia/Errigo* (Hrsg.), Neuroscience and Law, 2020; *Ligthart/van Toor/Kooijmans u. a.* (Hrsg.), Neurolaw, 2021, zu Forschungsaufträgen im Völker- und Verfassungsrecht *Kruse*, NJW 75 (2022), 2091–2092.

verbunden. Dies verweist auf Forschungsbedarfe in anderen Wissenschaftsdisziplinen.[64]

2. *Annäherungen an die „digitale Autonomie"*

Dem Datenschutzrecht zugrunde liegt wesentlich die rechtshistorisch gewachsene und rechtskulturell bedingte Überzeugung, dass menschliche Autonomie durch eine unüberschaubare und unkontrollierbare Datenverarbeitungsumgebung beeinträchtigt werden kann.[65] Die menschliche Autonomie ist damit das eigentliche Ziel hinter bzw. über dem Datenschutzrecht.[66] In den Rechtswissenschaften werden verschiedene Annäherungen und Begründungen vorgeschlagen, weshalb und auf welche Weise unregulierte Datenverarbeitungen menschliche Autonomie gefährden können. Ziel ist es dabei, die impliziten Annahmen von Unionsgesetzgeber und (Verfassungs-)Gerichten zu explizieren, um so die richtige Auslegung und Anwendung der DSGVO auswählen zu können.[67] In diesem Raum „dahinter" bzw. „davor" sind verschiedene Zuschreibungen möglich, die eine richtige Vorstellung gibt es nicht.[68] Es ist nicht An-

---

[64] Siehe hierzu etwa *Lawless/Mittu/Sofge u. a.* (Hrsg.), Autonomy and Artificial Intelligence: A Threat or Savior?, 2017; *Formosa*, Minds & Machines 31 (2021), 595–616; *Laitinen/Sahlgren*, Frontiers in artificial intelligence 4 (2021), 1–14.

[65] Für das Datenschutzrecht bedeutend ist die Feststellung des Bundesverfassungsgerichts, dass der Mensch in seiner Freiheit beeinträchtigt ist, wenn er nicht mehr überblicken und kontrollieren kann, welche der ihm zugeordneten Daten von wem und auf welche Weise verarbeitet werden, siehe BVerfGE 65, 1 (42–43) [1958] – *Volkszählung*. Diese Grundannahme prägt auch wesentlich die DSGVO, wenngleich sich der Unionsgesetzgeber vom Konzept eines Rechts auf informationelle Selbstbestimmung gelöst hat, eingehend etwa *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 98–105. Siehe zur Bedeutung der Entscheidung des Bundesverfassungsgerichts für das unionale Datenschutzrecht auch *Tzanou*, The fundamental right to data protection, 2019, S. 29–31. Die Abstützung auf gewisse Intuitionen und nicht verifizierte Grundannahmen wird vielfach kritisiert. Siehe etwa *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 38: „[Ü]ber die *Wirkungen* der Informationstechnik auf die Rechtssphäre des Betroffenen herrschen vielfach irreale Vorstellungen" (Hevorhebung im Original). Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 44 f.

[66] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 109–111; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 32 f.; *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 45; *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 58–61. Siehe bereits oben Kapitel 4 A. I. 1. a) und b).

[67] Vgl. auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 186. Siehe etwa die Ansätze bei *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 186–197; *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 17–63; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 91–94, 205–217.

[68] Vielfach wird dabei kritisiert, dass die jeweiligen Entwürfe idealisiert erscheinen und sich vielfach auf Intuitionen und Plausibilitäten stützen, für die empirische Nachweise fehlen. Siehe nur *Nettesheim*, in: Nettesheim/Diggelmann/Lege u.a. (Hrsg.), Der Schutzauftrag des Rechts, 2011, S. 7, 28: „Das [Bundesverfassungsgericht] behilft sich damit, dass es in

spruch dieser Arbeit, sich in dieser Debatte zu positionieren oder gar ein eigenes, weiteres Konzept digitaler Autonomie einzuführen. Für das Erkenntnisinteresse der Arbeit ist allein entscheidend, was das Datenschutzrecht im Hinblick auf die Autonomiegefährdungen durch autonome Systeme leisten kann und was nicht. Hierfür ist es ausreichend, ein Grundverständnis dafür zu entwickeln, wie die menschliche Autonomie durch Datenverarbeitung gefährdet wird. Hierfür sollen nachfolgend vier Ansätze skizziert werden, die im rechtswissenschaftlichen Diskurs vorherrschend sind.[69] Ihnen zufolge sind die Autonomiegefährdungen darauf zurückzuführen, dass die unkontrollierte Datenverarbeitung Hemmwirkungen auslöst (a)), die Grundbedingungen menschlicher Persönlichkeitsentwicklung aufhebt (b)), eine hinreichende kommunikativer Teilhabe verhindert (c)) und die Subjektqualität des Menschen aufheben kann (d)).

a) Hemmwirkungen unkontrollierter Datenverarbeitung

Gemeinhin wird das Datenschutzrecht damit begründet, dass eine unregulierte Datenverarbeitung Hemm- und Einschüchterungseffekte freisetzt[70] und freiheitsnotwendige Unbefangenheit aufhebt.[71] Herangezogen wird das dystopi-

psychologisierender und suggestiver, allerdings empirisch nicht unterlegter Manier als Beeinträchtigungstatbestand, das ‚sich einstellende Gefühl des Überwachtwerdens' und ‚Einschüchterungseffekte' anführt". Ebenso *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 37: „Die gewählten Veranschaulichungen (zur Beschreibung der menschlichen Autonomie) sind symptomatisch für juristische Argumente, die zwar auf wohlgemeinten Intuitionen beruhen, die Wirkungen eines Verlusts an Kontrolle über persönliche Informationen aber nur bedingt plausibel erklären. Zugleich verdeutlichen sie, dass die Überzeugungskraft eines dogmatischen Konstrukts maßgeblich von der Plausibilität der ihm zugrundeliegenden Verhaltensannahmen abhängt".

[69] Zu systemtheoretischen Erwägungen siehe eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 189–197.

[70] Siehe nur *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 87 f.; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 186–188; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 91 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 40 f.; *Lynskey*, ICLQ 63 (2014), 569, 593. Vgl. auch *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 22. Diese stellt auch das BVerfGE 65, 1 (43) [1958] – *Volkszählung* ins Zentrum: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden".

[71] Das Datenschutzrecht ist damit „Vorbedingung" der Verhaltensfreiheit. Siehe *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 87. Vgl. hierzu auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 33 f.; *Lynskey*, ICLQ 63 (2014), 569, 593. Dieser Ansatz wird vielfach kritisiert, insbesondere das Fehlen empirischer Nachweise angemahnt. Eingehend *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 45–54.

sche Bild einer Totalüberwachung nach dem Benham´schen Panoptikum, wie dies insbesondere von *Foucault* aufgegriffen und macht- und autonomietheoretisch aufgearbeitet wurde.[72] Diese Dystopie wurde von *Solove* weiterentwickelt: Demnach ist es nicht die Totalüberwachung, sondern die undurchschaubare und unbeeinflussbare datenbasierte Entscheidungsumgebung, die die Hemmeffekte begründet.[73] Diese Phänomene sind auch im Verhältnis zwischen Privaten denkbar.[74] Dort sind es dann ökonomische oder soziale Sanktionen, die Einschüchterungseffekte herbeiführen können.[75]

b) Grundbedingungen freier Persönlichkeitskonstitution

Vor allem *Britz*[76] und *von Lewinksi*[77] haben die Zusammenhänge von Datenschutz und Persönlichkeitsrechten herausgearbeitet. Es geht dann einerseits um die Abwehr von unerwünschten Einblicken (Privatsphäre),[78] andererseits und

---

Kritisch auch *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 283–286; *Nettesheim*, in: Nettesheim/Diggelmann/Lege u.a. (Hrsg.), Der Schutzauftrag des Rechts, 2011, S. 7, 28.

[72] Eingehend *Foucault*, Überwachen und Strafen, 1977. Siehe hierzu auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 187 f.; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 91 f.

[73] Daher, so *Solove* passt das Bild des Benham'schen Panoptikums nicht, vielmehr entspreche diese Konstellation der Situation von Josef K. ins Kafkas Roman „Der Prozess". Ausführlich *Solove*, The digital person, 2004, S. 27–55. Befürwortend *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 112; *Lynskey*, ICLQ 63 (2014), 569, 593. Siehe hierzu bereits oben Kapitel 4 A. I. 1. b).

[74] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 265–268; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 64–65, 87; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 58–60. Eingehend auch *Hoffmann-Riem*, AöR 123 (1998), 514, 524 f. „Solche Gefahren [durch private Datenverarbeitungsakteure] können unter heutigen Rahmenbedingungen die von Trägern der Staatsgewalt verursachten Gefährdungen sogar übersteigen".

[75] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 186; *Hoffmann-Riem*, AöR 123 (1998), 514, 524 f. Siehe auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 87. Diese können im Einzelfall sogar belastender wirken als staatliche Sanktionen, so *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 58, der auf die besonderen Herausforderungen empirischer Nachweise hinweist. Ausführlich zu Gefährdungen durch Private *Bäcker*, Der Staat 51 (2012), 91, 101. Vgl. auch *Hoffmann-Riem*, in: ders. (Hrsg.), Big Data, 2018, S. 11, 38–40; *Hoffmann-Riem*, AöR 123 (1998), 514, 524 f.

[76] *Britz*, NVwZ 38 (2019), 672–677; *Britz*, in: Hoffmann-Riem/Brandt/Schuler-Harms (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561; *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007.

[77] *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 17–63.

[78] Wenn die betroffene Person keinen Rückzugsraum für Selbstdistanz und Selbstreflexion mehr hat, kann sie kein Verhältnis zu sich entwickeln und ihre Persönlichkeit formen. So *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 86; *Britz*, Freie Ent-

vor allem aber um die Möglichkeit der Mitgestaltung der Person an ihrer Darstellung in der Öffentlichkeit (Selbstdarstellung).[79] Diese besteht gerade nicht mehr, wenn die betroffene Person nicht überblicken kann, welche Informationen über sie im sozialen Umfeld kursieren und was das Gegenüber konkret von der betroffenen Person weiß.[80] In dieser Herleitung von Datenschutz steht die Datenverarbeitung gerade durch Private im Vordergrund.[81]

c) Absicherung kommunikativer Teilhabe

Andere stellen die Notwendigkeit einer freiheitlichen Kommunikations- und Interaktionsordnung in den Fokus.[82] Nach diesem Modell ist die menschliche Autonomie aufgehoben, wenn ein Beteiligter den Kommunikationsprozess einseitig dominiert und so Wissens- und Machtasymmetrien entstehen.[83] Sowohl

faltung durch Selbstdarstellung, 2007, S. 28–30. Vgl. auch *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 22.

[79] Eine freie Persönlichkeitsentwicklung kann nach dieser Konzeption nur gelingen, wenn das Selbstbild des Betroffenen nicht durch Fremdzuschreibungen im sozialen Umfeld dominiert und verdrängt wird. Eingehend *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 37–64. Ausführlich auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 40–50. In diese Richtung auch *Eifert*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 365, 372 f. Sehr allgemein auf die Persönlichkeitsentwicklung stellen *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 58–61 ab.

[80] *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 52 f. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 27; *Eifert*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, S. 365, S. 375–376, 379–380. Vgl. auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 86. Sie geht noch weiter und sieht Belastungen eines freien Persönlichkeitsentwurfs auch dann, wenn die betroffene Person die Bildung zutreffender Fremddarstellungen nicht verhindern kann. Sie verlangt dann ein effektives (Mit-)Bestimmungs- und (Mit-)Gestaltungsrecht am eigenen Fremdbild. Kritisch hierzu *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 36 f.

[81] So auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 27.

[82] Eingehend *Hoffmann-Riem*, AöR 123 (1998), 514–540. So auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 41, 43; *Lynskey*, ICLQ 63 (2014), 569, 592–597. Vgl. zur Integration der Kommunikationstheorie nach *Habermas* in das Datenschutzrecht eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 188 f. Unter Bezugnahme auf (Wissens-)Machtkonzeptionen nach *Foucault Vatanparast*, ZaöRV 80 (2020), 819, S. 823–825, 837.

[83] *Hoffmann-Riem*, AöR 123 (1998), 514, 521: „[Das Recht auf informationelle Selbstbestimmung] zielt darauf ab, dem einzelnen eine selbstbestimmte Teilhabe an Kommunikationsprozessen und dadurch die Entfaltung seiner Persönlichkeit zu ermöglichen“. Ebenso *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 62, 85–86; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 186–188, 198; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 112.

die Persönlichkeitsentwicklung[84] als auch die Privatautonomie[85] sind beeinträchtigt, wenn die betroffene Person nicht überschauen und dann auch nicht verhindern kann, was das Gegenüber von ihr weiß.[86] Dies begründet aber kein Recht der betroffenen Person auf einseitige Bestimmung des Kommunikationsprozesses – dies wäre freiheitsbeeinträchtigend für den Kommunikationspartner –, sondern nur auf eine gleichberechtigte Teilhabe.[87]

d) Schutzinstrument gegen die Aufhebung der Subjektqualität des Menschen

Schließlich wird das Datenschutzrecht in einer Art Dammbruchargumentation gerechtfertigt: Es soll verhindern, dass der Mensch in Situationen gerät, in denen er nicht mehr als autonom gelten kann. Das Datenschutzrecht soll Schutz dagegen bieten, dass der Mensch in seinem Verhalten und seiner Persönlichkeit umfassend registriert wird („gläserner Bürger"),[88] nurmehr als Datenkonglomerat wahrgenommen wird,[89] oder zum Objekt einer digitalen Maschine gemacht wird.[90]

3. Dezentrale Mechanismen zum Schutz digitaler Autonomie im Privatrechtsverhältnis

Um digitale Autonomie zu schützen und zu gewährleisten, hat der Unionsgesetzgeber sich vorwiegend, wenngleich nicht nur, für einen dezentralisierten Ansatz entschieden. Es obliegt maßgeblich den beteiligten Parteien, vornehmlich der betroffenen Person, substantielle Angemessenheitskriterien für Datenverarbeitungen zu entwickeln.[91] Im Verhältnis zwischen Privaten ist zum Schutz digitaler Autonomie vornehmlich die betroffene Person berufen (a)).

---

[84] *Hoffmann-Riem*, AöR 123 (1998), 514, 521 f.; *Lynskey*, ICLQ 63 (2014), 569, 593. Vgl. auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 86.

[85] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 87–89; *Lynskey*, ICLQ 63 (2014), 569, 593.

[86] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 41. Vgl. auch *Lynskey*, ICLQ 63 (2014), 569, 593.

[87] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 89: „Datenschutzrecht bezweckt […] gerade nicht die Freiheit der Kommunikation, sondern den Schutz des Einzelnen davor, dass andere unbegrenzt über ihn kommunizieren und Informationen austauschen".

[88] *Ders.*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 86. Vgl. auch *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 53.

[89] *Tzanou*, The fundamental right to data protection, 2019, S. 31. In diese Richtung auch *Rouvroy*, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, 11.01.2016, S. 36 f.

[90] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 93 f.

[91] So ausdrücklich *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 204–206, der dies als „datenschutzrechtliche Regelfindung ‚von unten'" bezeichnet.

Ein individuelles Datenkontrollrecht etabliert die DSGVO damit aber nicht (b)).

a) Dezentrales Regulierungsmodell durch Gewährleistung subjektiver Datenrechte

Anders als bei der staatlichen Datenverarbeitung gibt es im Verhältnis zwischen Privaten kaum apriorische Richtigkeitsvorstellungen zur Angemessenheit von Datenverarbeitungen.[92] Welche Datenverarbeitungen belastend wirken, werden Betroffene ganz unterschiedlich bewerten. Dies gilt besonders mit Blick auf die Autonomiegefährdungen, bei denen die jeweilige individuelle Sensibilität entscheidend ist.[93] Im Kern geht es um die Frage, wie ein gutes Leben in einer Welt ubiquitärer Datenverarbeitung aussehen soll. Die Befugnis zur Beantwortung dieser Frage steht im liberalen Verfassungsstaat allein der betroffenen Person zu.[94] Jede staatliche Vorgabe, sei es zu mehr Datenschutzsensibilität, sei es zu mehr Datenfreigiebigkeit, wäre bevormundend-paternalistisch.[95] Entscheidet sich die betroffene Person für die Freigabe ihrer Daten, ist dies staatlicherseits hinzunehmen.[96] Hinzu kommt: In einer Verfassungs-

---

[92] Etwa das Gebot der Gesetzmäßigkeit, wie es für die Verwaltung gilt, vgl. *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 62. Siehe auch eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 202–204, der von einem staatlichen Wissensdefizit hinsichtlich subsantieller Richtigkeitsvorstellungen spricht.

[93] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 202–204 spricht von epistemischen Wissensdefiziten des Staates. Vgl. auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 223 f.

[94] So auch explizit Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 32. Ebenso *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 66.

[95] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 62–66, 97, 102, 113 f., 202 f.: „Freiheit ist nur dann wirkliche Freiheit und nicht staatlich aufoktroyierte, wenn der Einzelne auch eine Wahl hat, seine Freiheit auszuüben oder auf diese zu verzichten". Ebenso *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 170, 200 f. Er spricht von der Gefahr einer „Schematisierung und Steuerung innergesellschaftlicher Kommunikationsbeziehungen", siehe *ders.*, Privates Datenschutzrecht, 2020, S. 184. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 68, 74; *Hoffmann-Riem*, AöR 123 (1998), 514, 528. Zur Anknüpfung des Datenschutzrechts an liberal-aufklärerische Grundgedanken *Yeung*, iCS 20 (2017), 118, 128 f.

[96] Dies folgt dem Grundsatz „volenti non fit iniuria" und dem Grundsatz, dass es keinen Grundrechtsschutz gegen sich selbst geben kann. So auch für das Datenschutzrecht *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 71 f.; *Krönke*, Der Staat 55 (2016), 319, 323–325, 330–337; *Nettesheim*, in: Nettesheim/Diggelmann/Lege u.a. (Hrsg.), Der Schutzauftrag des Rechts, 2011, S. 7, 41; *Reinhardt*, AöR 142 (2017), 528, 559. Zu den Grundsätzen im Allgemeinen einführend *Ohly*, „Volenti non fit iniuria", 2002, S. 81–107; *Littwin*, Grundrechtsschutz gegen sich selbst, 1993; *Möller*, Paternalismus und Persönlichkeitsrecht, 2005.

ordnung, die auf Selbstbestimmung und Selbstverantwortung beruht, trifft die Schutzzuständigkeit vor (digitalen) Gefahren zuvorderst die betroffene Person.[97] Kernaufgabe des Datenschutzrechts ist damit, diese Bestimmungsbefugnis der betroffenen Person zu gewährleisten und zu stärken.[98] Rechtstechnisch wird diese dezentrale Datenordnung durch subjektive Datenrechte, vornehmlich[99] durch den Zulassungsgrund der Einwilligung umgesetzt.[100] Zugleich ist Einwilligung selbst effektives Schutzinstrument:[101] Sie bietet Schutz gegen die Unkontrolliertheit und Intransparenz der Datenverarbeitungen, die Autonomiegefährdungen begründen. Um die Bestimmungsbefugnis der betroffenen Person abzusichern, bedarf es ergänzender, dann zentralisierter materialer und prozessualer Schutzstandards.[102] Im Verhältnis zwischen Privaten gebietet zu-

---

[97] *Hoffmann-Riem*, AöR 123 (1998), 514, 531 f. Neben einem liberalen Staatsverständnis sind auch hier praktische Erwägungen anleitend *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 66: „Selbstschutz ist die älteste und gleichsam natürlichste Form des Umgangs mit Beeinträchtigungen und Gefahren".

[98] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 207. Vgl. auch *Hoffmann-Riem*, AöR 123 (1998), 514, 534–537 So auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 198: „[Die] grundrechtliche Schutzpflichten [erfordern] daher eine gewisse Objektivierung und Materialisierung des privaten Datenschutzrechts durch die Etablierung soziotechnischer Schutzstandards", notwendig ist daher eine, so *ders.*, Privates Datenschutzrecht, 2020, S. 199, „objektiv-rechtliche Etablierung einer Vertraulichkeitsinfrastruktur". Er fordert eine „Einhegung" statt einer „Abschaffung" des Einwilligungsmodells, *ders.*, Privates Datenschutzrecht, 2020, S. 225 f. In diese Richtung auch Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 82 – *UI gegen Österreichische Post AG*.

[99] Zur Bedeutung des Art. 6 Abs. 1 lit. b) DSGVO im dezentralen Regulierungsregime siehe sogleich unter Kapitel 4 A. II. 3. b).

[100] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 113 f., 102, 207. Ebenso *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 170. Siehe auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 75. Die Vorschrift geht damit über tradierte Mechanismen des Schutzes von Rechtsgütern im Privatverhältnis deutlich hinaus, etwa den deliktischen Schutz, vgl. eingehend *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 72 f.

[101] Vgl. zu dieser Bedeutung der Einwilligung im Regulierungskonzept der DGSGVO Wolff/Brink, BeckOK DatenschutzR/*Stemmer*, Art. 7 Rn. 1; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 1. Siehe auch Gola, DS-GVO/*Schulz*, Art. 6 Rn. 21; Wolff/Brink, BeckOK DatenschutzR/*Albers/Veit*, Art. 6 Rn. 30. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 74.

[102] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 174, 207, 218; *Hoffmann-Riem*, AöR 123 (1998), 514, 534–536. Eingehend auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 68 f.; *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 77 f. Dies erfolgt maßgeblich durch die Datenschutzgrundsätze, etwa der Zweckfestlegung, der Transparenz oder der Speicherbegrenzung, eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 218–219, 246–256, 275. Um eine paternalistische Bevormundung zu verhindern, ist der Staat dabei allein gehalten, die Grundbedingungen herzustellen, die der betroffenen Person eine individuelle Bestimmung der Datenschutzbedingungen und des Selbstschutzes erlauben. So auch *ders.*, Privates Datenschutzrecht, 2020, S. 217 f. *Hoff-*

dem der Grundsatz der Privatautonomie staatliche Zurückhaltung.[103] Der Staat muss es demnach den beteiligten Personen – betroffener Person wie Verantwortlichem – überlassen, die Bedingungen der Datenverarbeitung festzulegen.[104]

b) Keine individuelle Datenkontrolle und Einbezug von Drittinteressen

Die DSGVO verschafft dem Einzelnen aber keine Verfügungsbefugnis im Sinne individueller Datenkontrolle.[105] Eine solch privatistische Kontrolle der betroffenen Person über „ihre" Daten widerspricht schon den Grundsätzen einer freiheitlichen Kommunikationsordnung[106] und wäre mit dem Interesse an einem freien Datenverkehr, vor allem den unternehmerischen Interessen der Verantwortlichen nicht vereinbar.[107] Vor allem aber verkennt ein solches Verständnis, dass in einer modernen Welt Interaktion und Kommunikation maßgeblich über Daten erfolgen. Ein Verständnis von Datenschutz als willkürlicher

---

mann-Riem, AöR 123 (1998), 514, 534, 537 fordert eine den Selbstschutz der betroffenen Person nur ergänzende und stärkende „Auffang- und Gewährleistungsverantwortung", nicht eine die betroffene Person verdrängende „Ergebnis- und Erfüllungsverantwortung".

[103] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 56; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 64-65, 87–88; *Reinhardt*, AöR 142 (2017), 528, 556 f.

[104] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 66–72. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 56, 64; *Reinhardt*, AöR 142 (2017), 528, 559.

[105] Der EuGH hat sich in dieser Frage (noch) nicht eindeutig positioniert, siehe bereits oben Kapitel 4 A. I. 2. a). Gegen ein Recht auf informationelle Selbstbestimmung spricht sich insbesondere Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 68–82 – *UI gegen Österreichische Post AG* aus.

[106] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 174; *Hoffmann-Riem*, AöR 123 (1998), 514, 520 f. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/*Roßnagel*, Art. 5 Rn. 37. Dies erkennt auch das BVerfGE 65, 1 (43–44) [1958] – *Volkszählung*: „[D]er Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit".

[107] Vgl. *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 87, 89. Siehe auch *ders.*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 86, 89: „Es ist von einer prinzipiellen Gleichwertigkeit beider Ausgangspositionen auszugehen". Siehe auch *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 14; *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 51; *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61, 77 sowie Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 78–81 – *UI gegen Österreichische Post AG*. Eingehend zu den betroffenen Grundrechten datenverarbeitender Akteure *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 58–62.

Rückzug bzw. Rückhalt von Daten würde dem nicht gerecht.[108] Datenverarbeitungen sind im Übrigen Teil der heutigen Wirtschaftsordnung, sie sind notwendig für die Abwicklung von Geschäften oder sind selbst Handelsware. Digitale Autonomie erhält damit auch eine ökonomische Dimension und gebietet Schutz auch aus der Perspektive der Privatautonomie.[109] Digitale Autonomie zielt im Ergebnis nicht auf Datenkontrolle ab, sondern soll die betroffene Person befähigen, ihre sozialen und wirtschaftlichen Beziehungen, die in einer modernen Welt auch durch Datenverarbeitungen realisiert werden, mitzubestimmen und mitzugestalten.[110]

Es bedarf daher Mechanismen, die dafür Sorge tragen, dass auch die Interessen der verarbeitenden Personen hinreichend Berücksichtigung finden.[111] Und es bedarf Mechanismen, die die betroffene Person befähigen und bestärken, auch die ökonomische Dimension digitaler Autonomie wahrzunehmen.[112] Die DSGVO sieht daher neben der Einwilligung weitere Zulässigkeitstatbestände vor,[113] dies dann in Gestalt der vertragsimmanenten Zulassung in Art. 6 Abs. 1 lit. b) DSGVO sowie der Zulassung durch Interessensabwägung in Art. 6 Abs. 1 lit. f) DSGVO. Was dies für das Verhältnis der Zulassungsgründe untereinander bedeutet, ist noch darzulegen. Schon hier kann vorweggenommen werden, dass bei vertragsakzessorischen Datenverarbeitungen Art. 6 Abs. 1 lit. b) DSGVO vorgehen muss, dies gilt auch gegenüber der Einwilligung, im Übrigen die Abgrenzung durch Abwägung im Einzelfall erfolgen muss.[114]

---

[108] Vgl. *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 6 f. sowie *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61, 77Siehe auch Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 81 – *UI gegen Österreichische Post AG*.

[109] Eingehend *Nettesheim*, Digitale Autonomie in Vertragsbeziehungen, Verfassungsblog, 12.10.2022; *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 14. Vgl. auch Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 81 – *UI gegen Österreichische Post AG*.

[110] *Nettesheim*, Digitale Autonomie in Vertragsbeziehungen, Verfassungsblog, 12.10.2022. Zum Verhältnis der Zulassungstatbestände siehe noch ausführlich unter Kapitel 4 C. II. 6.

[111] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 174.

[112] So *Nettesheim*, Digitale Autonomie in Vertragsbeziehungen, Verfassungsblog, 12.10.2022. Vgl. auch Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 82 – *UI gegen Österreichische Post AG*.

[113] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 208, 223–224.

[114] Eingehend unten Kapitel 4 C. II. 6.

4. Ergebnis: Regulierungsbeitrag der DSGVO auf einer höheren Abstraktionsebene

Die DSGVO soll digitale Autonomie gewährleisten bzw. schützen. Prägend ist dabei die rechtshistorisch und -kulturell begründete Vorstellung, dass menschliche Autonomie beeinträchtigt ist, wenn die betroffene Person nicht mehr überschauen und nicht mitbestimmen kann, welche Daten über sie verarbeitet werden. Dies gilt auch im Bereich zwischen Privaten. Zur Begründung dieser Annahme wird auf Hemm- und Einschüchterungseffekte verwiesen sowie auf Grundbedingungen der freien Persönlichkeitskonstitution, nämlich die Selbstbewahrung und Selbstdarstellung. Abgestellt wird aber auch darauf, dass ohne die Absicherung gleichberechtigter Teilhabe am Kommunikationsprozess eine freiheitliche Gesellschaftsordnung nicht denkbar ist. Schließlich soll das Datenschutzrecht der Gefahr einer Aufhebung der Subjektqualität des Menschen entgegenwirken. Im Verhältnis zwischen Privaten wird digitale Autonomie vorwiegend durch die betroffene Person wahrgenommen. Ein individuelles Datenkontrollrecht folgt hieraus nicht. Abgesichert wird dies insbesondere durch die Normierung weiterer Zulassungsgründe.

Ob die DSGVO mit diesem Autonomie(schutz)konzept den in Kapitel 2 vorgestellten Autonomiegefährdungen durch autonome Systeme sinnvoll begegnen kann, ist Untersuchungsauftrag dieser Arbeit. Dies ergibt sich nur auf einer konkreteren Untersuchungsebene, d.h. durch Analyse und Bewertung einzelner Rechtsinstrumente.

III. Ergebnis

Die DSGVO schützt natürliche Personen vor den Beeinträchtigungen ihrer subjektiven Rechte durch unkontrollierte und intransparente Datenverarbeitungen, zugleich stellt sie einen Ausgleich mit dem Interesse eines freien Datenflusses her. Hierzu etabliert sie eine umfassende, objektiv-rechtliche Datenstrukturierungsregelung, die inhaltlich durch die Datenschutzgrundsätze präzisiert ist. Nach dem Grundsatz der Technikneutralität reguliert sie bestimmte Techniken nicht und ist auf sämtliche digitale Systeme anwendbar. Der DSGVO liegt die Vorstellung zugrunde, dass menschliche Autonomie beeinträchtigt ist, wenn der Mensch einer unüberschaubaren Datenverarbeitungsarchitektur ausgesetzt ist. Um digitale Autonomie zu gewährleisten, gibt die DSGVO vornehmlich der betroffenen Person die Befugnis über die inhaltliche Angemessenheit von Datenverarbeitungen zu entscheiden. Ein Recht auf individuelle Datenkontrolle folgt hieraus nicht. Die DSGVO prägt nicht eine Vorstellung, wonach allein die willkürliche Datenzurückhaltung autonomieschützend ist. Vielmehr ist sie von der Auffassung getragen, dass in einer modernen Welt soziale und wirtschaftliche Beziehungen auch durch Datenverarbeitungen gestaltet werden. Um digitale Autonomie zu ermöglichen, muss dann der Einzelne befähigt und bestärkt werden, diese Beziehungen mitzugestalten und sich in diese ein-

bringen zu können. An diesem normativen Regulierungsauftrag ist dann im Weiteren die praktische Wirksamkeit der DSGVO und ihre Fähigkeit zur Eindämmung der in Kapitel 2 beschriebenen Autonomiegefährdungen und Diskriminierungen zu messen. Soweit dabei Regulierungslücken erkenntlich werden, lässt sich an diesem Regulierungsauftrag bestimmen, ob sie richtigerweise datenschutzrechtlich zu schließen sind. Dies ist dann Gegenstand des 5. Kapitels.

B. Datenschutzrechtliche Regulierungszugriffe auf autonome Systeme

Die DSGVO reguliert allein personenbezogene Daten.[1] Sie enthält drei regulative Anknüpfungspunkte: allgemeine Vorschriften für deren Verarbeitungen,[2] besondere Vorschriften zum Profiling[3] sowie zu automatisierten Entscheidungen.[4] Zunächst sollen die Grundsätze und Prämissen dieses regulativen Zugriffs der DSGVO dargelegt (I.) und der geltende Rechtsrahmen vorgestellt werden (II.). Im Anschluss sollen diese Regulierungszugriffe auf die einzelnen Verarbeitungsvorgänge autonomer Systeme angewandt werden (III.). Hiernach soll eine Bewertung dieses Regulierungszugriffs der DSGVO auf autonome Systeme anhand des Maßstabs normativer Angemessenheit erfolgen (IV.).

Komplexe Fragen des Regulierungszugriffs der DSGVO stellen sich auch hinsichtlich der territorialen Reichweite der DSGVO[5] sowie hinsichtlich der Verantwortlichkeit[6]. Um diese soll es nachfolgend nicht gehen.

---

[1] Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO.

[2] Art. 2 Abs. 1, Art. 4 Nr. 2 DSGVO.

[3] Art. 4 Nr. 4 DSGVO.

[4] Art. 22 DSGVO.

[5] In einer globalisierten Welt finden die Verarbeitungsvorgänge autonomer Systeme, etwa die Datenaggregation, nicht notwendig innerhalb der territorialen Grenzen statt. Dies setzt etwa voraus, dass die verwendeten Geräte oder Speicherserver innerhalb des Staatsgebiets der Mitgliedstaaten verbleiben oder die die Programmierungen betreibenden oder derartige Anwendungen vertreibenden Unternehmen ihren Sitz innerhalb der Europäischen Union haben. Das Unionsrecht ist jedoch auch in engen Grenzen extraterritorial anwendbar. Vgl. zu diesen Fragen eingehend etwa *Herrmann*, Völkerrechtliche Jurisdiktionsgrundlagen für den Datenschutz im Netz, 2020; *Klar*, DuD 41 (2017), 533–537.

[6] An der Entwicklung und Ausgestaltung von autonomen Systemen sind eine Vielzahl von Akteuren beteiligt, Entwickler ebenso wie Hersteller, Betreiber oder Verwender der Technik. Dies wirft komplexe Fragen der Verantwortungszuweisung auf, sowohl im Hinblick darauf, wer als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO gilt, als auch in welchem Verhältnis mehrere Verantwortliche zueinanderstehen. Siehe zu diesen Fragen Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 87–91; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Petri*, Art. 4 Nr. 7 Rn. 13–26. Zur gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO bei derartigen Kooperationen in der digital-vernetzten Wirtschaft siehe Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Petri*, Art. 26 Rn. 3; Paal/Pauly, DS-GVO/*Martini*, Art. 26 Rn. 8.

I. Regulierungsparadigmen des Steuerungszugriffs der DSGVO

Mit dem Konstrukt personenbezogener Daten stellt die DSGVO eine Verbindung zwischen Personen und Gefährdung her (1.). Die DSGVO fokussiert auf das Einzeldatum und dessen Verarbeitung (2.), sie schützt allein die Einzelperson und verpflichtet ausschließlich den Verantwortlichen (3.).

1. Konnektivistisches und absolutes Regulierungsregime: Personenbezug als Auslöser des Regulierungszugriffs

Über das Merkmal des Personenbezugs wird das Datenschutzrecht zu einem Betroffenenrecht modelliert.[7] Das Datenschutzrecht unterstellt, dass eine jede Datenverarbeitung nachteilig auf Interessen und Rechte betroffener Personen einwirken kann und zwar deshalb, da sich an die Datenverarbeitung nachteilige Folgen für die betroffene Person, etwa Entscheidungen, Manipulationen oder vertiefte Einblicke in die Persönlichkeit, anschließen.[8] In dieser Vorstellung bestehen zwischen Datum und nachteiligen Folgen direkte Verbindungslinien. Deshalb ist es richtig, die Datenverarbeitungen und nicht erst die Folgen zu regulieren. Diese Verbindungen werden durch die Rückverfolgbarkeit eines Datums auf eine Person geschaffen.[9] Es bedarf daher keines Nachweises der spezifischen Gefährlichkeit einer Datenverarbeitung, der Personenbezug genügt.[10] Anstelle eines sachlichen Risikos der Datenverarbeitung tritt dann ein

---

[7] Die von einer Datenverarbeitung betroffene Person sind schutzwürdig, nicht die Daten. Siehe hierzu bereits Kapitel A I. 1. a). Vgl. auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 4; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 87.

[8] Anschaulich *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 41: „Ausreichend ist, dass nachteilige Entscheidungen nicht ausgeschlossen werden können und der Grundrechtsträger angesichts der Unsicherheit über Wahrscheinlichkeit und Schwere des Nachteils psychischen Hemmungen unterliegt, unbefangen von seiner Verhaltensfreiheit Gebrauch zu machen". Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 4 Nr. 1 Rn. 22. Das Risiko hat seine Ursache damit nicht eigentlich in den Daten, sondern den hieraus abgeleiteten Informationen und den nachteiligen Reaktionen des Umfelds – sei es der Staat, seien es Privatpersonen – hierauf, so auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 40.

[9] Da eine Person über das Datum rückverfolgbar ist, sind vertiefte Einblicke in ihre Persönlichkeit oder Manipulationen möglich. Auch werden gerade deshalb Abschreckungseffekte begründet, denn aufgrund der Rückverfolgbarkeit muss sie nachteilige Entscheidungen im Anschluss an die Datenverarbeitung befürchten. Vgl. zu dieser Risikokonzeption auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 4 Nr. 1 Rn. 3; Ehmann/Selmayr, DS-GVO/*Klabunde*, Art. 4 Rn. 7; Kuner/Bygrave/Docksey, GDPR/*Bygrave/Tosoni*, Art. 4(1) Rn. 106. Siehe auch *Finck/Pallas*, Int. Data Priv. Law 10 (2020), 11, 35; *Dalla Corte*, European Journal of Law and Technology 10 (2019), 1, 9 f.

[10] Dieser Ansatz ist historisch gewachsen: Während zu Beginn der Digitaltechnik noch objektiv-rechtliche Technikfolgenregulierungsansätze vorherrschten, wandte sich der Gesetzgeber mit zunehmender Verbreitung der Digitaltechnik einem subjektiv-rechtlichen, an der einzelnen Person anknüpfenden Datenregulierung zu. Die Konzentrierung des Daten-

subjektiviertes Risiko, nämlich die Zuordenbarkeit des Datums zu einer bestimmten Person.[11]

2. *Atomistisches und partikularistisches Regulierungsregime: Datenverarbeitung als Regulierungsstimulus*

Der Steuerungsanspruch bezieht sich auf die Verarbeitungen von Einzeldaten.[12] Dies ist auf das konnektivistische Verständnis des Datenschutzrechts zurückzuführen, wonach nämlich sämtliche nachteilige Folgen mit dem Datum verbunden sind. Einer Regulierung von spezifischen Anwendungen, Folgen oder Systemen bedarf es daher nicht. Da das Risiko einer jeden Datenverarbeitung innewohnt, bedarf es auch der Regulierung einer jeden Datenverarbeitung. Dies ist mit der Erwartung verbunden, dass mit der Regulierung des Einzeldatums sämtliche nachteiligen Folgen eines datengetriebenen Systems eingedämmt werden können.[13] Die DSGVO etabliert so ein atomistisches,[14] d.h. auf die Verarbeitung des einzelnen Datums konzentrierendes, sowie partikularistisches, d.h. durch jede Datenverarbeitung neu ausgelöstes,[15] Regulierungsregime.

---

schutzes auf die betroffene Person erlaubte eine klare Zuordnung, die gegenüber einer objektiv-rechtlichen eine einfache und effektive Regulierungsalternative bot. Eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 164–171; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 205. Die konkrete Gefahren- und Beeinträchtigungsintensität der Datenverarbeitung wird dann aber auf der Rechtfertigungsebene relevant. Siehe hierzu auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 35. Kritisch zu diesem Konzept *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 28–32; *Nettesheim*, in: Nettesheim/Diggelmann/Lege u.a. (Hrsg.), Der Schutzauftrag des Rechts, 2011, S. 7, 29, 38.

[11] Der Personenbezug ist dabei ein absolutes Merkmal: Ein Datum ist personenbezogen oder nicht, es gibt keine Zwischenstufen. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 4 Nr. 1 Rn. 14. Entsprechend ist auch Frage nach der Anwendbarkeit der DSGVO binär – die DSGVO gilt ganz oder gar nicht. Vgl. insbesondere Begriff und Konzept der Binarität der DSGVO Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 4 Nr. 1 Rn. 14–15; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 148; *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 306 „dichotomy".

[12] Art. 4 Nr. 2 DSGVO.

[13] Dieser Ansatz wird besonders deutlich in der Regulierung der automatisierten Entscheidung nach Art. 22 DSGVO. Nur dort wird ausnahmsweise eine konkrete Anwendung bzw. ein spezifisches datenbasiertes System reguliert. Vgl. zu diesen Erwägungen – dies dann im Rahmen der Einordnung des Art. 22 DSGVO in das Regulierungskonzept der DSGVO – Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 11; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 10 f.

[14] Zum Begriff und zur Bedeutung eines atomistischen Datenschutzes siehe *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 92.

[15] Gemeint ist damit, dass jede Verarbeitung eines personenbezogenen Datums im Sinne der DSGVO das Regulierungsregime der DSGVO, insbesondere die Einhaltung der Datenschutzgrundsätze einfordert. Wird dasselbe Datum in verschiedenen Prozessen verarbeitet,

3. Individualistisches und relativistisches Regulierungsregime: Datenverarbeitungsverhältnis als Begrenzung des Regulierungsauftrags

Geschützt wird in der DSGVO allein die in den Daten repräsentierte Person und dies auch nur in Bezug auf „ihre" Daten.[16] Nachteilige Effekte für Dritte werden nicht, jedenfalls nur eingeschränkt, adressiert.[17] Die DSGVO etabliert also ein individualistisches Schutzsystem.[18] Die DSGVO konstruiert ein Datenschutzrechtsverhältnis allein zwischen betroffener Person und Verantwortlichem: Verpflichtet ist der personenbezogene Daten verarbeitende Akteur, soweit dieser Verantwortlicher[19] oder Auftragsverarbeiter[20] im Sinne der DSGVO ist, und auch nur dieser. Das Pflichtenprogramm bezieht sich allein auf die betroffene Person. Die DSGVO begreift Datenschutz als relativistisches Pflichtenverhältnis zwischen betroffener Person und Verantwortlichem.[21]

II. Darstellung des geltenden Rechtsrahmens für regulative Zugriffe auf autonome Systeme

Die datenschutzrechtliche Gestaltung der Steuerungszugriffe soll im Weiteren skizziert werden; die Ausführungen beschränken sich auf die für die Regulierung autonomer Systeme relevanten Aspekte. Komplexe Fragen wirft das Merkmal der Personenbezogenheit der von autonomen Systemen verarbeiteten

---

etwa durch ein aufeinanderfolgendes Erheben, Speichern, Analysieren und Auslesen, wird dieser Vorgang datenschutzrechtlich allerdings zu einer einheitlichen Datenverarbeitung verklammert; die verschiedenen Prozesse lösen die DSGVO also nur ein Mal aus. Vgl. hierzu Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 34; Paal/Pauly DS-GVO/*Ernst*, Art. 4 Rn. 21.

[16] Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 28: „Die betroffene Person ist diejenige, die davor zu schützen ist, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird". Siehe auch *Bull*, Der Staat 58 (2019), 57, 92. Auch das Verbot automatisierter Entscheidungen nach Art. 22 DSGVO normierten Rechte kommt nur der betroffenen Person zugute, d.h. der Person, gegenüber der die Entscheidung rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt, vgl. Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 43; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2.

[17] Vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 161; *Vatanparast*, ZaöRV 80 (2020), 819, 837–840. Hierauf ist unter Kapitel 4 C. IV. 2. a) bb) vertieft einzugehen.

[18] Ebenso *Bull*, Der Staat 58 (2019), 57, 92, der auch den Betriff eines „individualistischen Schutzes" nutzt. Von „individual privacy" spricht *Vatanparast*, ZaöRV 80 (2020), 819, 838–840.

[19] Art. 4 Nr. 7 DSGVO. Zur Definition siehe eingehend Paal/Pauly, DS-GVO/*Ernst*, Art. 4 Rn. 55.

[20] Art. 4 Nr. 8 DSGVO. Zu Definition siehe eingehend Paal/Pauly, DS-GVO/*ders.*, Art. 4 Rn. 56.

[21] *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 93 spricht von einem „Zweipersonenverhältnis".

Daten auf, vor allem im Hinblick auf Trainingsdaten, die für die Modellbildung oder die Erstellung des Lösungsalgorithmus verwendet werden. Die verarbeiteten Daten entstammen dabei aus den Aufzeichnungsprozessen, die im digitalen und analogen Bereich stattfinden.[22] Diese Daten sind vielfach anonymisiert,[23] auch können synthetische Daten[24] verwendet werden.[25] Es ist offen, inwieweit diese personenbezogene Daten darstellen können. Diese Fragen stehen jenseits des Untersuchungsauftrags dieser Arbeit, in der es maßgeblich um das „Wie", nicht das „Ob" des Regulierungszugriffs gehen soll. Im Weiteren wird daher unterstellt, dass die verarbeiteten Daten personenbezogen sind.

Soweit personenbezogene Daten verarbeitet werden, bietet die DSGVO verschiedene Anknüpfungspunkte zur Regulierung autonomer Systeme, entsprechend den einzelnen Stadien der technischen Prozesse. Die DSGVO benennt

---

[22] Die Verknüpfung von digitalen und analogen Welten erhöhen den Umfang verfügbarer Daten, siehe hierzu Kapitel 1 A. III. 1.

[23] Vielfach wird in der Praxis aber auf Anonymisierungen verzichtet, da diese mit einigem Aufwand einhergehen, vgl. *Hornung/Wagner*, CR 2019, 565, 573; *Lorentz*, Profiling, 2019, S. 299 f.; *Kaulartz*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 462, Rn. 21. Zudem kann sich die Anonymisierung der Trainingsdaten nachteilig auf das Maschinelle Lernverfahren auswirken, da die Anonymisierung zu Verfälschungen und Verzerrungen des Trainingsdatensets führen kann. Vgl. *Raji*, DuD 45 (2021), 303, 306; *Goldsteen/Ezov/Shmelkin u.a.*, Anonymizing Machine Learning Models, 26.7.2020, S. 2, siehe auch *Ohm*, University of California Law Review 57 (2010), 1701, 1751–1755.

[24] Hierbei werden Daten vollständig künstlich hergestellt. Vgl. ausführlich zu den eingesetzten Verfahren und deren datenschutzrechtliche Einordnung *Kaulartz*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 462, Rn. 22–25; *Meents*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 445, Rn. 47; *Raji*, DuD 45 (2021), 303, 304–306. Vgl. hierzu auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 132.

[25] Problematisch ist dabei insbesondere, dass parallel zu den Anonymisierungstechniken beständig De-Anonymisierungstechniken fortentwickelt werden. Vgl. zu verschiedenen Verfahren *Hacker*, ZGE 12 (2020), 239, 247. Siehe auch *Lorentz*, Profiling, 2019, S. 294 f. mit zahlreichen Beispielsfällen aus der Praxis, in denen trotz vermeintlich erfolgreicher Anonymisierung auf die hinter den Daten stehende Person geschlossen werden kann. Es ist daher unklar, welche Qualität diese Anonymisierungs- bzw. Synthetisierungsverfahren haben müssen, damit die Trainingsdaten auch im Sinne der DSGVO als nicht (mehr) personenbezogen gelten können, und wie damit umzugehen ist, wenn sich mit der technischen Fortentwicklung der (Re-)Identifikationstechniken diese Einordnung ändert. Siehe zu diesen Fragen etwa *Stalla-Bourdillon/Knight*, Wisconsin International Law Journal 34 (2017), 284, 318; *Wachter/Mittelstadt*, CBLR 2019, 494, 577. Teilweise sogar gänzlich in Zweifel gezogen, ob es überhaupt noch anonymisierte Daten im Sinne der DSGVO geben kann. Plakativ wird von einem „Ende der Anonymität" gesprochen, so ausdrücklich *Boehme-Neßler*, DuD 40 (2016), 419; *Sarunski*, DuD 40 (2016), 424, 427. Ähnlich *Rubinstein/Hartzog*, Washington Law Review 91 (2016), 703, 757: „Anonymization is dead".

drei Regulierungsmomente: die allgemeine Verarbeitung (1.), das Profiling (2.) und die automatisierte Entscheidung (3.).

1. Regulierung der Verarbeitung personenbezogener Daten

Datenverarbeitungen sind in Art. 4 Nr. 2 DSGVO als Vorgänge mittels teil- und vollständig automatisierter Verfahren im Zusammenhang mit personenbezogenen Daten definiert,[26] sie bieten, zumindest in dem hier interessierenden Rahmen, keine rechtlichen Unsicherheiten und bedürfen keiner weiteren Erörterung.

2. Regulierung des Profilings

Das Profiling ist in der DSGVO aufgeführt, wenn auch nur beschränkt: Es ist legaldefiniert (a)), seine Regulierungsbedarfe unterscheiden sich von denen der vor- und nachgehenden Datenverarbeitungen (b)), gleichwohl erfährt es in der DSGVO keiner, zumindest keiner eigenständigen Regelung (c)).

a) Definition des Profilings

Profiling wird in Art. 4 Nr. 4 DSGVO definiert.[27] Die dortige Definition enthält drei konstitutive Elemente: erstens die automatisierte Datenverarbeitung von personenbezogenen Daten[28], zweitens die Bewertung in Form einer Analyse oder Prognose und zwar – drittens – von persönlichen Aspekten.[29] Da auto-

---

[26] Siehe ausführlich zum Verarbeitungsbegriff *Ernst*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 53, 21–34; Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 29–57b; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 4 Nr. 2. Erfasst ist der gesamte Verarbeitungszyklus von der Erhebung der Daten bis zur Löschung der Daten, unabhängig von Art und Technik der Verarbeitung, Qualität der Daten oder Zwecksetzung der Verarbeitung.

[27] In der DSRL war noch keine Definition vorgesehen. Vgl. ausführlich zu den Merkmalen, auch zu den historischen Grundlagen des Profiling-Begriffs, *Lorentz*, Profiling, 2019, S. 79–118; mit systematischer Übersicht zu den Definitionen in verschiedenen unionalen Rechtstexten Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 54. Eine Darstellung zu nationalen und internationalen Rechtstexten zu Verständnis und Konzeption des Profilings bietet Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 4 (4) Rn. 129.

[28] Die Beschränkung auf personenbezogene Daten folgt aus dem Anwendungsbereich der DSGVO: Sollte die Profilbildung anhand anonymer oder anonymisierter Datenverarbeitungen stattfinden, ist die DSGVO schon gar nicht anwendbar, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 3. So auch Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 4 Nr. 4 Rn. 14.

[29] Damit folgt der Unionsgesetzgeber der Definition nach *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7. Diese Leitlinien gehen zurück auf die von der Artikel 29 Datenschutzgruppe erarbeiteten Leitlinien

nome Systeme die Profilbildung vollständig automatisiert durchführen, bereitet das erste Kriterium keine Schwierigkeiten.[30] Der Begriff der Bewertung meint nicht eine Beurteilung der Person, sondern eine Interpretation der verarbeiteten Daten.[31] Mittels der Datenverarbeitung sollen aus den analysierten Rohdaten[32] neue Erkenntnisse über die betroffene Person gewonnen werden.[33] Das bloße Zusammentragen von Informationen[34] ist dagegen ebenso wenig ausreichend wie die Gruppierung oder statistische Erfassung von Personen.[35] Die Bewertung erfolgt nach Art. 4 Nr. 4 DSGVO typischerweise in Form einer Analyse oder Prognose;[36] erst sie ermöglicht eine Interaktion, d.h. eine Entscheidung oder Steuerung in Bezug auf eine Person, die das eigentliche Ziel

---

vom 03.10.2017, überarbeitet und angenommen am 06.02.2018. Der Europäische Datenschutzausschuss übernahm diese ohne Änderungen mit Beschluss vom 25.05.2018.

[30] Umstritten ist, ob unter Art. 4 Nr. 4 DSGVO – anders als bei der automatisierten Entscheidung – auch teilautomatisierte Profilbildungsverfahren fallen. *ders.*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7 bejaht dies, gefolgt von der überwiegenden Ansicht in der Literatur. Siehe etwa Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 21. Siehe auch *Lorentz*, Profiling, 2019, S. 99.

[31] Paal/Pauly, DS-GVO/*Martini*, Art. 22 21a Vgl. auch *Lorentz*, Profiling, 2019, S. 103.

[32] Zum Begriff der Rohdaten siehe Kapitel 1 B. II. 1. a).

[33] So ausdrücklich *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7 f. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 6; *Linderkamp*, ZD 10 (2020), 506, 507; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 4 Nr. 4 Rn. 6.

[34] Es handelt sich dann allein um eine Datenaggregation, die Vorstufe, aber eben keine Bewertung ist, vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 6; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 4 Rn. 62. Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 8.

[35] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 6; *Linderkamp*, ZD 10 (2020), 506, 507; *Lorentz*, Profiling, 2019, S. 103. Ebenso *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 25 f. AA Ehmann/Selmayr, DS-GVO/*Klabunde*, Art. 4 Rn. 30, wonach auch bloße Klassifizierungen unter den Profilingbegriff fallen.

[36] So *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7 f. Diese Aspekte überschneiden sich vielfach in der Praxis, so auch *Lorentz*, Profiling, 2019, S. 103. Siehe mit Beispielen Sydow, DS-GVO/*Helfrich*, Art. 4 Rn. 84, 87–88; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 6; Ehmann/Selmayr, DS-GVO/*Hladjik*, Art. 22 Rn. 7.

des Profilings ist.[37] Bewertungsgegenstand sind persönliche Aspekte, von denen in Art. 4 Nr. 4 DSGVO einige beispielhaft genannt sind.[38] Der Begriff der persönlichen Aspekte ist breit gefasst und erstreckt sich auf sämtliche die Person beschreibende Umstände.[39] Auch hier ist das Merkmal der Bewertung entscheidend, es geht um Erkenntnisse jenseits der Rohdaten mit interaktionsleitendem Gehalt. Angaben wie Alter, Geschlecht oder Wohnort sind daher keine persönlichen Aspekte nach Art. 4 Nr. 4 DSGVO.[40] Art. 4 Nr. 4 DSGVO verlangt zudem den Personenbezug der persönlichen Aspekte, die bewertet werden, Bewertungsobjekt ist also die natürliche Person.

b) Profiling als eigenständiges Regulierungsmoment

Die DSGVO enthält keine eigenständigen Regelungen zum Profiling,[41] nur annexhaft zur automatisierten Entscheidung sind eigene Normen vorge-

---

[37] So Ehmann/Selmayr, DS-GVO/*Klabunde*, Art. 4 Rn. 28; ebenso Sydow, DS-GVO/*Helfrich*, Art. 4 Rn. 84. Dies muss nicht in Form einer automatisierten Entscheidung im Sinne des Art. 22 DSGVO erfolgen.

[38] Die Aufzählung ist nicht abschließend zu verstehen, siehe nur Paal/Pauly, DS-GVO/*Ernst*, Art. 4 Rn. 37; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 4.

[39] Vgl. mit Beispielen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 4 f.

[40] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 7 f. Ebenso *Lorentz*, Profiling, 2019, S. 104; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 11. Deutlich weiter Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 4: „beschreibende und charakterisierende Umstände, Merkmale, Eigenschaften, Verhältnisse und Beziehungen".

[41] So auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 9 f. Siehe auch Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 23; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 2, 23; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 2 sowie *Lorentz*, Profiling, 2019, S. 156–158. Plakativ Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 4 Nr. 4 Rn. 1 „lediglich politische Bedeutung". Dies war zwar vielerorts, insbesondere auch von der Artikel 29 Datenschutzgruppe, siehe *Artikel 29 Datenschutzgruppe*, Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, 23.03.2012, S. 14; *Artikel 29 Datenschutzgruppe*, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13.05.2013, S. 4, und dem Europäischen Parlament, vgl. *Europäisches Parlament*, Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI)), Europäisches Parlament, 6.7.2011, S. 107 Rz. 18, siehe auch Art. 4 Nr. 3a, Art. 20 Parlamentsentwurf zur DSGVO, gefordert worden, fand dagegen im Gesetzgebungsverfahren nicht die entscheidenden Mehrheiten. Siehe hierzu eingehend *Lorentz*, Profiling, 2019, S. 156 f.

sehen.[42] Ob diese auch für das Profiling isoliert gelten bzw. inwieweit diese sich auch auf das Profiling erstrecken, ist vielfach unklar. Darauf ist noch im Rahmen des Rechtmäßigkeits- und Transparenzgrundsatzes zurückzukommen. Eigenständige profilingspezifische Regulierungsansätze finden sich allein in den Erwägungsgründen.[43] Das Profiling unterfällt daher (jedenfalls) den allgemeinen Vorschriften der DSGVO.[44]

3. Regulierung automatisierter Entscheidungen

Mit Art. 22 DSGVO wird dieses Schutzregime der DSGVO erweitert auf Verfahren im Anschluss an eine Datenverarbeitung, es geht also um eine bestimmte Anwendungs- bzw. Verwendungsmodalität von Datenverarbeitungen bzw. Datenverarbeitungsergebnissen.[45] Art. 22 DSGVO gilt daher als atypisches Regulierungsinstrument.[46] Art. 22 Abs. 1 DSGVO definiert automatisierte Entscheidungen (a)); vorgesehen ist dann ein Verbot, für das gleichwohl einige Ausnahmen normiert sind, sowie weitere Schutzvorschriften (b)).

---

[42] Art. 22 DSGVO, in Art. 35 Abs. 3 lit. a) sowie in Art. 13 Abs. 2 lit. g), Art. 14 Abs. 2 lit. g) sowie Art. 15 Abs. 1 lit. h) DSGVO.

[43] Erwägungsgrund 60 S. 3 beinhaltet eine spezifische Hinweispflicht, in Erwägungsgrund 71 S. 6 werden qualitative Anforderungen an das Verfahren gestellt und Sicherungsmaßnahmen gegen unrichtige Daten, Fehler und weitere unerwünschte Phänomene gefordert. Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 21 bezeichnet diese Erwägungsgründe als „unsauber", da hier systemwidrig und gerade anders als im verfügenden Teil der DSGVO sowie in den Erwägungsgründen 63 S. 3 und 91 S. 2 isoliert auf das Profiling abgestellt wird.

[44] Dies stellt bereits Erwägungsgrund 72 S. 1 klar. Siehe ausführlich die Darstellung bei *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 10–20. Vgl. auch Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 26, 30; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 10–12.

[45] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 4; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 3 f.; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 1.

[46] *Edwards/Veale*, SSRN Journal 2017, 44 „rather odd provision"; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 1 „regelungstechnische Anomalie"; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 3; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 4 „flankierende Verfahrensvorschrift"; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 3„organisatorische (Verfahrens-)Vorschrift". *Ernst*, JZ 72 (2017), 1026, 1031 zufolge verfolgt Art. 22 DSGVO „streng genommen keine originären datenschutzrechtlichen Zwecke". *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 79 weisen darauf hin, „Art. 15 [als Vorgängervorschrift des Art. 22 DSGVO] is directed at a type of decision rather than data processing. It thereby resembles traditional administrative law rules on government decision making". Art. 22 DSGVO – bzw. die Vorgängerregelung Art. 15 DSRL – geht zurück auf ein französisches Gesetz aus dem Jahr 1978. Siehe ausführlich zur Geschichte der Norm *Djeffal*, ZaöRV 80 (2020), 847, 851–856.

a) Definition der automatisierten Entscheidung

Der automatisierten Entscheidung voran geht die Verarbeitung personenbezogener Daten.[47] Hinsichtlich der Entscheidung (aa)), dem ausschließlichen Beruhen (bb)), der Unterworfenheit (cc)) und der rechtlichen Wirkung und erheblichen Beeinträchtigungswirkung (dd)) bestehen einige Rechtsunsicherheiten.

aa) Entscheidung und Maßnahme

Art. 22 DSGVO verlangt eine Entscheidung, verstanden als ein bestimmtes zurechenbares[48] Ergebnis mit Außen- und Gestaltungswirkung im Einzelfall.[49] Dies grenzt die Entscheidung von der vorausgehenden automatisierten Datenverarbeitung ab.[50] Die Entscheidung meint dabei typischerweise eine Willensentäußerung mit rechtlicher Gestaltungswirkung.[51] Nach Erwgr. 71 S. 1 sind auch Maßnahmen („measures"), d.h. Realhandlungen, erfasst.[52] Der Be-

[47] Andernfalls ist die DSGVO ohnehin nicht anwendbar. Siehe nur Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 3. Dies schließt aber nicht aus, dass in dem technischen Verfahren daneben auch Daten verarbeitet werden, die nicht personenbezogen sind oder nicht von der betroffenen Person stammen, so auch Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 Rn. 533.

[48] Bloße Zufälle sind keine Entscheidungen, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 14. Zugleich muss diese einer Person oder Institution zuzuordnen sein, so Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 17.

[49] Siehe zu den hier genannten Anforderungen *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 305; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 15a; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 14 f. Auf das Erfordernis der Einzelfallbezogenheit – allgemeinabstrakte Entscheidungen oder Strategien reichen also nicht aus – weisen hin Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 15a; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 15.

[50] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 17.

[51] Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 37 – *SCHUFA Holding*: „[Die Entscheidung] muss auch ‚verbindlich' sein, um sie von einfachen ‚Empfehlungen' zu unterscheiden, die grundsätzlich keine rechtlichen oder tatsächlichen Folgen haben". Vgl. auch Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 15a.

[52] Vgl. Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 15a. Siehe auch Däubler/Wedde/wiechert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 25.

griff der Maßnahme ist unklar.[53] Jedenfalls muss dies mehr sein als ein bloßes technisches Internum.[54]

bb) Ausschließliches Beruhen

Die automatisierte Entscheidung muss ausschließlich auf einer automatisierten Datenverarbeitung[55] beruhen.[56] Ausweislich Erwgr. 71 S. 1 aE liegt dies vor, wenn die Entscheidung „ohne jegliches menschliche Eingreifen" erfolgt.[57] Unklar ist dann, ob Art. 22 DSGVO auch bei teilautomatisierten Entscheidungen greift, insbesondere bei reinen Entscheidungsassistenzsystemen. Ab welchem Umfang menschlicher Involvierung Art. 22 DSGVO ausgeschlossen ist, ist äu-

[53] Der *Europäische Datenschutzausschuss* hat hierzu in seinen Leitlinien (noch) keine Stellung bezogen. Vgl. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 21, in der das Tatbestandsmerkmal der Entscheidung nicht näher definiert wird. Dies ist auch Gegenstand des Vorlageverfahrens des VG Wiesbaden, siehe *Häuselmann*, The ECJ's First Landmark Case on Automated Decision-Making, 29.02.2023 (https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber).

[54] Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 15a; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 17. *Finck*, Int. Data Priv. Law 9 (2019), 78, 83 schlägt vor, den maschinellen an den menschlichen Entscheidungsbegriff anzupassen: Soweit eine maschinelle Ausgabe, sofern diese ein Mensch getroffen hätte, als Entscheidung zu werten ist, muss auch die maschinelle Ausgabe als Entscheidung gelten.

[55] Art. 22 DSGVO benennt als typischerweise vorangehende automatisierte Datenverarbeitung das Profiling, beschreibt aber nicht näher, welcher Qualität diese Datenverarbeitung sein muss und ob insbesondere einfache Wenn-Dann-Programme, wie etwa Geldautomatenausgaben, dem Art. 22 DSGVO unterfallen sollen. In der Literatur wird überwiegend dafür eingetreten, dass unterkomplexe Verarbeitungen, etwa die Ausgabe bei einem Bankautomaten, nicht unter Art. 22 DSGVO fallen. Da es vorliegend allein um Profiling-Verfahren, zudem um solche des Maschinellen Lernens geht, denen eine hinreichende Komplexität allgemein hin zugesprochen wird, kann diese Frage offenbleiben. Siehe eingehend zu diesen Fragen *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 305; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 8; *Buchner*, in: Tinnefeld/Buchner/Petri u.a. (Hrsg.), Einführung in das Datenschutzrecht, ^{6}2018, S. 220, Rn. 131; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 279.

[56] Die Vorschrift untersagt nicht die Nutzung automatisierter Verarbeitungsverfahren bei der (menschlichen) Entscheidungsfindung, sondern allein die unmittelbare Übersetzung dieses Verarbeitungsergebnisses in eine Einzelentscheidung, also allein rein technische Entscheidungsverfahren, vgl. zu dieser Differenzierung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 26; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 2, 17b, 20.

[57] In der englischen Fassung heißt es: „without any human intervention", in der französischen: „sans aucune intervention humaine".

ßerst umstritten.[58] Einigkeit besteht allein darin, dass die bloß formale menschliche Involvierung, etwa in Form einer ungeprüften Bestätigung des maschinellen Ergebnisses, nicht ausreichen soll.[59] In der Literatur wird verlangt, der Mensch müsse aktiv an der Entscheidung mitwirken,[60] die Letztentscheidungskompetenz innehaben,[61] auf das konkrete Entscheidungsergebnis tatsächlich Einfluss nehmen[62] oder sich selbst inhaltlich mit der Entscheidungsfrage auseinandersetzen.[63] Andernorts wird auf die typische Nutzung als Entscheidungshilfe oder als Entscheidungsautomat[64] oder auf einen Zurech-

---

[58] *Veale/Edwards*, CLSR 34 (2018), 398, 400 gestehen zu: „[D]ecisions [must be] made with *some* degree of human involvement, though the extent of that degree is hard to set" (mit Hervorhebung im Original). Siehe auch Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 25.1: „Mangels einschlägiger Rechtsprechung sind die Anforderungen an den Entscheidungsspielraum noch nicht geklärt".

[59] So die *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 22, ebenso die überwiegende Ansicht in der Literatur, siehe nur *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 101; *Walter*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 391, Rn. 7; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 252; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 92. So auch Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 25; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 17–17b; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 25. Insbesondere wäre so einer missbräuchlichen Zwischenschaltung einer menschlichen Abnickinstanz zur Ausschaltung des Art. 22 DSGVO Tür und Tor geöffnet, so *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 22; *Veale/Edwards*, CLSR 34 (2018), 398, 400.

[60] Vgl. Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 25; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 77; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 17b. Siehe auch *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 87.

[61] *Ernst*, JZ 72 (2017), 1026, 1031; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 13.

[62] So Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 15; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 251 f.

[63] *Hoeren/Niehoff*, RW 9 (2018), 47, 53. Ähnlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 26, der auf die bestimmenden Motive der Entscheidung abstellt.

[64] So *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 102; *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 253; *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 87. Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 14; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 24, 28 unterscheiden entsprechend algorithmendeterminierte und algorithmenbasierte bzw. -getriebene Entscheidungen. Die bloße Vorsortierung von Daten oder Anordnung von betroffenen Personen nach einem Bewertungssystem, etwa im Rahmen von Bewerber-Rankings, Kredit-Scorings, reicht daher nicht aus, solange hieraus nicht unmittelbar eine Entscheidung folgt, sondern dies dem Menschen allein zur Unterstützung in seiner Entscheidungsfindung dient, vgl. Paal/Pauly, DS-

nungs- und Kausalitätszusammenhang abgestellt.[65] Nach dem Europäischen Datenschutzausschuss, kommt es auf die Befugnis und fachliche Kompetenz zur Prüfung[66] und Abänderung[67] der involvierten Person im Einzelfall an.[68]

cc) Unterworfenheit unter die Entscheidung

Die betroffene Person ist der Entscheidung unterworfen, wenn der Verantwortliche einseitig das Entscheidungsprogramm vorgibt,[69] die betroffene Person also nicht unmittelbar an der Entscheidungsfindung beteiligt wird.[70] Wird dagegen lediglich ein vorab zwischen den Parteien vereinbartes Ergebnis automatisiert vollzogen, liegt kein Unterworfensein vor,[71] auch dann nicht, wenn die betroffene Person das System jederzeit kontrollieren, steuern oder auf dieses einwirken kann.[72]

GVO/*Martini*, Art. 22 Rn. 20, 24; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 16 f.

[65] Den Verantwortungsbegriff führen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 28; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 15. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 74 wendet von einer „conditio sine qua non"-Formel an: Die automatisierte Datenverarbeitung dürfe demnach nicht hinweggedacht werden, ohne dass die Entscheidung in ihrer konkreten Form entfiele.

[66] Die Prüfungskompetenz verlangt nicht nur fachliche Kenntnisse, sondern auch hinreichende Einblicke in das maschinelle Entscheidungsverfahren und die Entscheidungsinhalte. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 22. Siehe hierzu auch Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 24.

[67] Dies setzt die Existenz von Entscheidungsspielräumen voraus, so auch Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 59. Der Umfang des Entscheidungsspielraums bleibt allerdings unklar. So sollen etwa bloße Stichprobenkontrollen nicht genügen, vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 15; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 27, nach anderer Ansicht soll bereits das Herausfiltern unplausibler Einzelergebnisse ausreichend sein, so Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 25.1; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 15. Es besteht allerdings Konsens, dass der menschliche Entscheider nicht sämtliche Details des Programms oder Algorithmus kennen muss, so Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 27.

[68] Dies wird in der Literatur gemeinhin befürwortend, siehe etwa Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 18–19; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 27, 30; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 15. Ebenso *Lorentz*, Profiling, 2019, S. 262 f.

[69] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 18.

[70] Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 34.

[71] Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 24b.

[72] Vgl. Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 24c; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 18. Siehe auch zum Anwendungsbeispiel einer

dd) Rechtliche Wirkung oder in ähnlicher Weise erhebliche Beeinträchtigung

Die Entscheidung hat dann rechtliche Wirkung, wenn hierdurch unmittelbar die Rechtsposition der betroffenen Person verändert wird, etwa indem ein Rechtsverhältnis begründet oder aufgehoben oder indem in subjektive Rechte eingegriffen wird.[73] Unklar ist, ob diese rechtliche Wirkung nachteilig sein muss.[74] In den in Erwgr. 71[75] sowie in den Leitlinien des Europäischen Datenschutzausschusses[76] aufgeführten Beispielsfällen sind allein negative Rechtsfolgen benannt, auch in der Literatur fordern einige Stimmen eine Beschränkung auf nachteilige Rechtsfolgen.[77] Angeführt wird die regulierungsinterne Kohärenz der Vorschrift[78] sowie ein andernfalls fehlender Regulierungsbedarf.[79] In diese Richtung gehen auch die Erwägungen des Generalanwalts beim EuGH.[80] Andere wollen auch begünstigende rechtliche Wirkungen unter Art.

Suchmaschine sowie eines SmartHomes Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 19 f.

[73] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 24; *Veale/Edwards*, CLSR 34 (2018), 398, 401; *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 88. Dies kann sowohl Rechte aus dem Öffentlichen als auch dem Privatrecht betreffen.

[74] So die deutsche Vorgängervorschrift § 6a BDSG aF.

[75] Angeführt ist in Erwägungsgrund 71 S. 1 die Ablehnung eines Online-Kreditantrags oder das e-Recruiting, in Erwägungsgrund S. 6 wird auf potenzielle Bedrohungen für die Interessen und Rechte hingewiesen und auf diskriminierende Wirkungen abgestellt.

[76] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23. Dort sind unter anderem die Auflösung eines Vertrages oder die Ablehnung einer Einbürgerung benannt.

[77] So Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 25; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 21; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 71. Ebenso *Lorentz*, Profiling, 2019, S. 264. Bereits für Art. 15 DSRL *Zahariev*, 76. In diese Richtung wohl auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23, der allein rechtlich nachteilige Beispiele aufführt.

[78] So auch Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 25; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 21. Diese Koppelung der Alternativen ist wichtig, da eine solche in der Vorgängervorschrift des Art. 15 DSRL nicht vorgesehen war, vgl. zu diesem Argument Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 14b, 28; vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23. Die Definition setzt voraus, dass „erhebliche Beeinträchtigungen" nur negative Wirkungen darstellen können, hierzu sogleich.

[79] Gola, DS-GVO/*Schulz*, Art. 22 Rn. 21; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 71.

[80] Nach Ansicht von Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 34 – *SCHUFA Holding* sollen allein Entscheidungen, die

22 DSGVO fassen[81] und verweisen auf den offenen Wortlaut.[82] Die Verknüpfung der Alternativen („in ähnlicher Weise") verstehen sie in einer umgekehrten Zielrichtung: Die faktischen Beeinträchtigungen müssen den rechtlichen Wirkungen ähnlich sein, d.h. zu einer vergleichbaren Änderung des Status der Person führen.[83] Auch die erweiterte Schutzwirkung eines so verstandenen Art. 22 DSGVO wird angeführt.[84] Hingewiesen wird schließlich darauf, dass eine explizite Beschränkung auf nachteilige rechtliche Wirkungen im Gesetzgebungsverfahren gescheitert war.[85]

Die zweite Alternative umfasst rein faktische Wirkungen. Die Vorschrift erstreckt sich auf sämtliche Einwirkungen auf materielle und immaterielle Interessen und Rechtspositionen.[86] Auch hier ist offen, ob diese Beeinträchtigungen nachteilig sein müssen. Überwiegend wird dies in der Literatur bejaht, [87] auch der Europäische Datenschutzausschuss erläutert allein Beispiele mit nachteiliger Wirkung.[88] Hingewiesen wird hier auf den Wortlaut sowie den

---

(rechtlich oder tatsächlich) „schwerwiegende Auswirkungen" für die betroffene Person haben, dem Art. 22 DSGVCO unterfallen.

[81] So etwa Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 49; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 46; *Moos/Rothkegel*, ZD 6 (2016), 565. In diese Richtung auch *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 233; Ehmann/Selmayr, DS-GVO/*Hladjik*, Art. 22 Rn. 9.

[82] So Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 49; *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 89; Paal/Pauly. DS-GVO/*Martini*, Art. 22 Rn. 28. Vgl. auch Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 44, 46, der auch auf die englische („produces legal effects") und französische Sprachfassung („produisant des effets juridiques la concernant") hinweist, die – anders als die deutsche Begrifflichkeit „beeinträchtigen" – nicht auf eine nachteilige rechtliche Wirkung hindeuten.

[83] Vgl. *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 89; Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 Rn. 534.

[84] Vgl. Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 27; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 28; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 49.

[85] So war ursprünglich die Bezeichnung „significant adverse affects" im Ratsentwurf vorgesehen. Siehe hierzu Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 44; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 69.

[86] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 23; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 29. Die Beeinträchtigung erfasst also auch immaterielle Aspekte, vgl. Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 29; Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 Rn. 534 f.

[87] So etwa Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 38; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 23; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26. Ebenso *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 324.

[88] Vgl. nur *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23–25.

Schutzzweck der Norm.[89] Nur sehr vereinzelt wird dafür eingetreten, auch Entscheidungen mit faktischer begünstigender Wirkung dem Art. 22 DSGVO zuzuordnen,[90] dies dann mit Hinweis auf andere Sprachfassungen, die gegenüber der deutschen Übersetzung deutlich neutraler ausfallen,[91] sowie auf eine möglichst breite Schutzwirkung.[92]

Eine Einschränkung erfährt Art. 22 DSGVO durch das Kriterium der Erheblichkeit („meaningful"). Es handelt sich um ein einzelfallbezogenes Wertungselement.[93] Dem Europäischen Datenschutzausschuss zufolge muss die Beeinträchtigungswirkung „umfassend bzw. erwähnenswert" sein.[94] Die Literatur verlangt eine nachhaltige Störung des wirtschaftlichen oder persönlichen Status der betroffenen Person.[95]

---

[89] Vgl. Gola, DS-GVO/*Schulz*, Art. 22 Rn. 22; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 25; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 71.

[90] So etwa *Walter*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 391, Rn. 13; Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 28; *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 20.

[91] In der englischen und französischen Sprachfassung heißt es: „affect" bzw. „l'affectant".

[92] Vgl. zu diesen Argumenten *Walter*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 391, Rn. 13; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 46.

[93] So ausdrücklich *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 40; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27; *Finck*, Int. Data Priv. Law 9 (2019), 78, 84.

[94] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23. Im Weiteren führt er verschiedene Beispielsfälle aus, in denen seiner Ansicht nach die Erheblichkeit der Beeinträchtigung im Einzelfall vorliegen kann, vgl. *ders.*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 24. Ein eindeutiges Bild ergibt sich hieraus nicht.

[95] Siehe nur Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 55. Ähnlich Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 28: „in die Rechte und Freiheiten Betroffener nachhaltig hineinwirken"; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 29 „nicht nur kurzfristig und geringfügig"; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 64 „[nicht] bloße Unannehmlichkeiten oder im Rahmen des allgemeinen Lebensrisikos liegende Belästigungen". Siehe auch *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 88 „more than trivial for a person's welfare". Abzustellen ist auf eine durchschnittliche Person in der Situation des Betroffenen, so Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 38; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 66.

b) Regulierung automatisierter Entscheidungen

Art. 22 Abs. 1 DSGVO formuliert ein Verbot der automatisierten Entscheidung.[96] Wenngleich darin von einem Recht die Rede ist, wird gemeinhin davon ausgegangen, dass das Verbot allgemein gilt und nicht erst von der betroffenen Person geltend gemacht werden muss.[97] Art. 22 Abs. 2 DSGVO sieht verschiedene Ausnahmen vor. Hierauf ist noch im Rahmen der Rechtmäßigkeit zurückzukommen. Art. 22 DSGVO stellt im Übrigen keine inhaltlich-substantiellen Anforderungen, weder im Hinblick auf das Entscheidungsverfahren noch auf das Entscheidungsergebnis, auf.[98] Daneben sieht die DSGVO an weiteren Stellen Steuerungsinstrumente für automatisierte Entscheidungen vor, etwa Betroffenenrechte in Form von Einwirkung, Darlegung des Standpunkts und Anfechtung, Art. 22 Abs. 3 DSGVO, Transparenzvorschriften[99] sowie einer Datenschutzfolgeabschätzung.[100] Die Schutzinstrumente beziehen sich allein auf die Kontrolle der Automatisierung; einen Anspruch auf inhaltliche Richtigkeit der Entscheidung vermittelt Art. 22 DSGVO nicht.[101]

---

[96] So der überwiegende Teil der Literatur, siehe nur Gola, DS-GVO/*Schulz*, Art. 22 Rn. 5; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 12; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 29. So auch *Ernst*, JZ 72 (2017), 1026, 1029.

[97] So etwa Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 31 – *SCHUFA Holding* sowie *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 21. Aus der Literatur siehe etwa *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 97–99; *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 85–87; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 95. Aus der Kommentarliteratur Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 39; *Martini*, Rn. 29b.

[98] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 11. Insbesondere ein Zugriffsrecht auf den zugrundeliegenden Algorithmus verschafft die Vorschrift nicht, so Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 3.1.

[99] Art. 13 Abs. 2 lit. f), Art. 14 Abs. 2 lit. f), Art. 15 Abs. 1 lit h) DSGVO; Ausführungen hierzu erfolgen in Kapitel 4. D. II. 3.

[100] Art. 35 Abs. 3 lit. a) DSGVO. Diese liegen jenseits des Forschungsauftrags dieser Arbeit. Siehe hierzu *Artikel 29 Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.04.2017, zuletzt überarbeitet und angenommen am 04.10.2017; *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 32–34.

[101] Vgl. etwa *Martini*, Blackbox Algorithmus, 2019, S. 173.

III. Analyse der regulativen Zugriffe der DSGVO auf autonome Systeme

Bei autonomen Systemen finden eine Vielzahl von Datenverarbeitungsprozessen statt, die den Regulierungsmechanismus der DSGVO auslösen.[102] Unterscheiden lassen sich im Kern fünf Verarbeitungsprozesse: die Datenaggregation – dies sowohl für die Erstellung des Modells und des Lösungsalgorithmus als auch des Profils –, die Modellbildung, die Profilbildung und schließlich die Profilverwendung.[103] Auch die Erstellung des Lösungsalgorithmus in einem Maschinellen Lernverfahren auf Grundlage personenbezogener Daten stellt ein datenschutzrechtlich relevantes Verarbeitungsverfahren dar. Datenschutzrechtlich sind diese Prozesse zu differenzieren, da sich verarbeitete Daten, Methoden und Ziele unterscheiden.

Bei der Datensammlung und -speicherung kommen keine Verfahren des Maschinellen Lernens zum Einsatz, die Verarbeitungsverfahren der Datensammlung und -speicherung werfen daher keine neuartigen datenschutzrechtlichen Fragestellungen auf. Diese Verarbeitungsstufe bleibt daher im Weiteren außer Betracht.[104] In der Praxis sind vielfach die gebildeten Profile selbst Gegenstand von weiteren Datenverarbeitungen, etwa in Form der Speicherung, Löschung oder Weitergabe an Dritte.[105] Für die Funktionsfähigkeit autonomer Systeme ist dies allerdings nicht notwendig, zudem kommen hier keine Verfahren des Maschinellen Lernens zum Einsatz. Auch diese Datenverarbeitungen werden im Weiteren daher nicht untersucht.

Schließlich soll die Bildung des Lösungsalgorithmus im Nachfolgenden nicht vertieft untersucht werden. Vielfach lassen sich Wertungen hinsichtlich der Modellbildung auf die Erstellung des Lösungsalgorithmus übertragen. Hierauf wird an geeigneten Stellen der Untersuchung hingewiesen werden. Im Detail stellen sich die Risikolagen aber unterschiedlich dar. Bei der Modellbildung geht es um Erkenntnisse über NutzerInnen im Datensatz und um die Vorbereitung eines Erkenntnisgewinns über eine bestimmte Person, während die Erstellung des Lösungsalgorithmus im Maschinellen Lernverfahren auf die

---

[102] Treffend *Eckhardt*, DuD 45 (2021), 107, 113: „Die Definition [von Datenverarbeitungsprozessen nach der DSGVO] macht deutlich, dass auch im Kontext von IoT grundsätzlich keine Tätigkeit in Bezug auf personenbezogene Daten denkbar ist, welche nicht in den Anwendungsbereich der DSGVO fällt".

[103] Eingehend Kapitel 1 B. III. 3. Und Kapitel 1 B. IV.1. Diese Unterscheidung nimmt auch *Lorentz*, Profiling, 2019, S. 97–102, 120–122, 152–153, 254 vor. Ähnlich *Kamarinou/Millard/Singh*, Machine Learning with Personal Data, Queen Mary School of Law, 7.11.2016, S. 8 f., die aber Modell- und Profilbildung zusammenfassen und also drei wesentliche Verarbeitungsprozesse benennen.

[104] Siehe eingehend zu datenschutzrechtlichen Fragen der Rechtmäßigkeit der Datenaggregation bei der Profilbildung *Lorentz*, Profiling, 2019, S. 276–284.

[105] Siehe zu den Rechtmäßigkeitsanforderungen der Speicherung des Profils eingehend *dies.*, Profiling, 2019, S. 252 f.

Entwicklung einer Lösungsstrategie und Ermöglichung von automatisierten Anwendungen abzielt.

Für die weitere Untersuchung ist von Interesse, auf welche Weise die DSGVO regulative Zugriffe auf die Modellbildung (1.), die Profilbildung (2.) und die Profilverwendung[106] (3.) schafft.

1. Regulierungsmomente in der Modellbildung

Das Trainingsverfahren im Rahmen Maschinellen Lernens stellt eine Datenverarbeitung im Sinne der DSVO dar (a)). Die Modellbildung ist kein Profiling im Sinne der DSGVO (b)).

a) Datenverarbeitungen im Modellbildungsverfahren

Das Trainingsverfahren zur Erstellung des Modells ist ein Datenverarbeitungsverfahren im Sinne des Art. 4 Nr. 2 DSGVO. Auf die Verarbeitungsmethodik kommt es nach dem technikneutralen Ansatz der DSGVO[107] nicht an: Auch Maschinelle Lernverfahren stellen Datenverarbeitungen nach Art. 4 Nr. 2 DSGVO dar.[108] Die DSGVO hält für das Maschinelle Lernverfahren keine besonderen Vorschriften bereit, es gelten die allgemeinen Regeln.[109] Das Trainingsverfahren besteht aus einer Vielzahl von Verarbeitungsschritten,[110] datenschutzrechtlich werden diese verklammert.[111] Das Modellbildungsverfahren insgesamt muss den datenschutzrechtlichen Anforderungen genügen.

b) Modellbildung als Profiling

Die Modellbildung ist nicht als Profiling nach Art. 4 Nr. 4 DSGVO zu werten. Denn es werden nur Erkenntnisse über Zusammenhänge von Persönlichkeitsmerkmalen der Gesamtheit der Personen im Datensatz ermittelt, nicht aber Be-

---

[106] Die Profilanwendung bezeichnet in dieser Arbeit die Anwendung des Modells auf die Einzelperson und damit die eigentliche Profilerstellung (Inferenzbildung), während die Profilverwendung die Nutzung des Profils für die Auslösung einer spezifischen automatisierten Steuerung oder Entscheidung beschreibt. Siehe hierzu Kapitel 1 B. III. 3. C). 1 sowie Kapitel 4 B. IV. 1.

[107] Siehe hierzu Kapitel 4 A. I. 2. c).

[108] Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 32a.

[109] Siehe nur *Paal*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, 1, 3; *Schürmann*, ZD 12 (2022), 316, 317 f.

[110] Siehe Kapitel 1 B. III. 3. B) bb).

[111] Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 34; Paal/Pauly, DSGVO/*Ernst*, Art. 4 Rn. 21. Zur Einordnung des Trainingsverfahrens als eine einheitliche Datenverarbeitung im Sinne der DSGVO siehe auch *Lorentz*, Profiling, 2019, S. 97 f. Vgl. auch *Valkanova*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 336, Rn. 4, die ebenso das Trainingsverfahren insgesamt als datenschutzrechtlich relevanten Verarbeitungsprozess versteht.

wertungen von Persönlichkeitsmerkmalen einer Einzelperson vorgenommen. Es ist nur Vorverfahren zum Profiling.[112] In der individualistischen Perspektive löst das Modell auch keinen Regulierungsbedarf aus: Es enthält nur Aussagen über die Personengemeinschaft im Trainingsdatensatz, gefährdet die betroffene Person also noch nicht, erst das Profil begründet derartige Gefährdungen.[113] Zwar sind damit auf Stufe der Modellbildung spätere Gefährdungen von Einzelpersonen angelegt. Diese realisieren sich aber nicht notwendig. Denn nicht für jede Person, deren Daten im Modell verarbeitet wurden, wird ein Profil erstellt. Zudem werden bei der Modellbildung nicht allein Daten der betroffenen Person verarbeitet. Eine Anwendung des Art. 4 Nr. 4 DSGVO auf die Modellbildung bedeutete eine popularklagenartige Ausweitung des Datenschutzrechts auf Datenverarbeitungsprozesse Dritter.[114]

2. *Regulierungsmomente in der Profilbildung*

Die Profilbildung ist ein Datenverarbeitungsprozess im Sinne der DSGVO (a)), sie stellt überdies ein Profiling nach Art. 4 Nr. 4 DSGVO dar (b)).

a) Datenverarbeitungen im Rahmen der Profilbildung

Bei der Profilbildung werden Anwendungsdaten anhand des Modells verarbeitet. Dies stellt eine Datenverarbeitung nach Art. 4 Nr. 2 DSGVO dar. Wie auch

---

[112] Ebenso *Lorentz*, Profiling, 2019, S. 101, 105, 288. Sie unterscheidet das Profiling im engeren Sinne, das sich allein auf die Profilbildung, d.h. die Anwendung des Modells, erstreckt – allein dieses ist vom Profiling-Begriff des Art. 4 Nr. 4 DSGVO erfasst – und das Profiling im weiteren Sinne, das sämtliche vorgelagerten Prozesse wie die Datenaggregation oder die Modellbildung inkludiert – dies ist nicht von Art. 4 Nr. 4 DSGVO gedeckt, vgl. eingehend *dies.*, Profiling, 2019, S. 106–109. Siehe auch *Zahariev*, 75, der ebenso zwischen Individualprofilen oder Gruppenprofilen unterscheidet. Vgl. auch Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 4 Nr. 4 Rn. 14; *Schefzig*, K&R 14 (2014), 772, 777; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 540, 545–546. Vgl auch den Regulierungsentwurf des Europarats: Das Modell (dort missverständlich benannt als „Profile") beschreibt demnach allein die Zusammenstellung von Daten zu einer Mehrheit von Personen, wohingegen das Profiling die Anwendung des Modells auf das Individuum erfasst. Siehe: *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 9 Appendix 1. Definitions lit. d): „‚Profile' refers to a set of data characterizing a category of individuals that is intended to be applied to an individual" und lit. e) „‚Profiling' means an automatic data processing technique that consists of applying a ‚profile' to an individual".

[113] Vgl. auch *Lorentz*, Profiling, 2019, S. 107, die diese Überlegungen maßgeblich auf den Wortlaut des Art. 4 Nr. 4 DSGVO stützt. Ähnlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 6, wonach es um die Ableitungen in Bezug „auf eine bestimmte Person" gehe.

[114] In diese Richtung auch *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 308: „Data protection applies to this limited amount of personal data [of the individual], but […] the decision is not based on this limited amount of data, but on the ‚big' data of others".

bei der Modellbildung werden hierbei die verschiedenen einzelnen Verarbeitungsschritte datenschutzrechtlich zu einem Verarbeitungsvorgang zusammengefasst.[115] Dass bei dieser Datenverarbeitung selbstlernende Algorithmen zum Einsatz kommen, ist aufgrund des Grundsatzes der Technikneutralität irrelevant. Spezifische Vorschriften zu selbstlernenden Algorithmen enthält die DSGVO nicht, es finden daher die allgemeinen Grundsätze Anwendung.[116]

b) Profilbildung als Profiling

Die Bildung des Profils durch autonome Systeme stellt ein Profiling nach Art. 4 Nr. 4 DSGVO dar. Hier werden personenbezogene Daten automatisiert mittels des Modells ausgewertet, es erfolgt zudem eine Bewertung persönlicher Merkmale, d.h. eine Ableitung von Persönlichkeitsmerkmalen anhand und jenseits der verarbeiteten Rohdaten, und zwar in prognostisch-evaluativer Weise.[117] Die Profiling-Definition in Art. 4 Nr. 4 DSGVO benennt nicht klar, welche Verarbeitungsprozesse hierunter fallen sollen. Nach der überwiegenden Ansicht in der Literatur fällt allein die Inferenzbildung, d.h. die Verarbeitung eines Anwendungsdatums im Modell, unter den Profilingbegriff.[118] Nur vereinzelt wird für eine weite Auslegung eingetreten, wonach sämtliche, auch nur vorbereitende, Verarbeitungsverfahren im Rahmen der Profilbildung, also auch die Datenaggregation sowie die Modellerstellung, das datenschutzrecht-

---

[115] So auch *Härting*, CR 4 (2014), 528, 529; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 540; *Lorentz*, Profiling, 2019, S. 98.

[116] Vgl. *Paal*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, Rn. 3; *Niemann/Kevekordes*, CR 36 (2020), 17, 20. Siehe auch *Schürmann*, ZD 12 (2022), 316, 317 f. Vgl. allgemein zu algorithmischen Systemen *Klar*, BB 74 (2019), 2243, 2244. Siehe eingehend zur Anwendung allgemeiner Datenschutzvorschriften auf Systeme der Künstlichen Intelligenz *European Parliamentary Research Service*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Juni 2020, S. 35–72.

[117] *Lorentz*, Profiling, 2019, S. 101 f. „eindeutig". Ebenso *Kamarinou/Millard/Singh*, Machine Learning with Personal Data, Queen Mary School of Law, 7.11.2016, S. 9. Auch das Kredit-Scoring ist ein Profiling nach Art. 4 Nr. 4 DSGVO, so explizit Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 33 – *SCHUFA Holding*, siehe auch *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, [2]2022, S. 369, 277. Zur Profilbildung bei der personalisierten Werbung sowie beim Scoring siehe Sydow, DS-GVO/*Helfrich*, Art. 4 Rn. 86–87; Ehmann/Selmayr, DS-GVO/*Klabunde*, Art. 4 Rn. 29, bei Informationsfilterungen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 7; Sydow, DS-GVO/*Helfrich*, Art. 4 Rn. 86, bei personalisierten Preisen vgl. *Zuiderveen Borgesius/Poort*, J. Consum. Policy 40 (2017), 347, 361 f.

[118] So etwa *Lorentz*, Profiling, 2019, S. 106 f.; *Kamarinou/Millard/Singh*, Machine Learning with Personal Data, Queen Mary School of Law, 7.11.2016, S. 9. In diese Richtung auch *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, S. 540, 544 f.

liche Profilingverfahren umfassen.[119] Da die DSGVO, so zumindest die überwiegende Ansicht, keine eigenständigen Vorschriften zum Profiling enthält, folgt aus der Einordnung der Profilbildung bzw. der Inferenzbildung als Profiling allerdings kein eigener substantieller Regulierungszugriff. Erst im Rahmen der Profilverwendung, d.h. als Teil einer automatisierten Entscheidung nach Art. 22 DSGVO, ist das Profiling besonderen Vorschriften unterworfen.[120] Es gelten daher die allgemeinen datenschutzrechtlichen Bestimmungen. Aufgrund der Technikneutralität der DSGVO ist es irrelevant, dass die Daten dabei anhand des Modells, d.h. eines selbstlernenden Algorithmus verarbeitet werden.

3. Regulierungsmomente in der Profilverwendung

Bei der Profilverwendung kommen zum einen die allgemeinen Vorschriften zum Tragen (a)), zum anderen die besondere Vorschrift automatisierter Entscheidungen nach Art. 22 DSGVO (b)).

a) Datenverarbeitungen bei der Profilverwendung

Die automatisierte Entscheidung oder Steuerung wird durch Verarbeitung des Profils und gegebenenfalls weiterer Anwendungsdaten in einem Lösungsalgorithmus ausgelöst. Die vorliegende Untersuchung unterstellt, dass diese Anwendungsdaten personenbezogen sind. Auch das Profil und seine Einzelinhalte stellen in der Regel ein personenbezogenes Datum dar: Sie enthalten anhand des Modells abgeleitete Informationen über eine Person, die dieser zugeordnet werden können.[121] Die Profilverwendung erfolgt demnach technisch über eine

---

[119] So etwa *Rustici*, CRi 18 (2018), 34, 42 f. So auch *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 5 f.

[120] Die Profilbildung und automatisierte Entscheidung sind nach der Konzeption des Art. 22 DSGVO zu trennen. Vgl. nur *Kamarinou/Millard/Singh*, Machine Learning with Personal Data, Queen Mary School of Law, 7.11.2016, S. 11; *Lorentz*, Profiling, 2019, S. 156–158, 258. Vgl. auch Paal/Pauly, DS-GVO/*Martini*, Art. 22 20, 20a, 23; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 53. Vgl. auch *Edwards/Veale*, SSRN Journal 2017, 46: „[T]he output of an algorithmic system is merely something which is then used to make a decision". Sie weisen auch darauf hin, dass die bloße Zuordnung zu einer Gruppe im Modell noch keine Entscheidung im Sinne des Art. 22 DSGVO darstellt. Es fehlt bereits an der Auswirkung.

[121] So etwa *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 8, 19. Ausdrücklich auch *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 6 „Profiles […] generate new personal data". Zum selben Ergebnis kommen *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 301–303; Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 21c; *Custers*, in: Bayamlıoğlu/Baraliuc/Janssens u.a.

Verarbeitung personenbezogener Daten. Auf diese finden die allgemeinen Regeln der DSGVO Anwendung.[122] Ist der Lösungsalgorithmus selbst ein solcher aus Maschinellen Lernverfahren, ist dies aufgrund des technikneutralen Regulierungsansatzes der DSGVO irrelevant. Die DSGVO enthält hierfür keine besonderen datenschutzrechtlichen Vorschriften. Demgegenüber bezieht sich Art. 22 DSGVO nicht auf diese Datenverarbeitung, sondern auf die Verwendung des Datenverarbeitungsergebnisses, d.h. des Profils und seiner Einzelinhalte, für eine automatisierte Entscheidung. Die Vorschrift tritt neben diese allgemeinen datenschutzrechtlichen Anforderungen. Soweit eine Profilverwendung keine automatisierte Entscheidung im Sinne des Art. 22 DSGVO darstellt, erfolgt die Regulierung automatisierter Entscheidungen bzw. Steuerungen demnach allein über die allgemeinen datenschutzrechtlichen Bestimmungen.[123]

b) Profilverwendung als automatisierte Entscheidung

Damit das spezifische Regulierungsregime des Art. 22 DSGVO ausgelöst wird, muss eine Entscheidung vorliegen (aa)), der die betroffene Person unterworfen ist (bb)), die ausschließlich auf der automatisierten Datenverarbeitung beruht (cc)) und rechtliche Wirkungen oder sonstige erhebliche beeinträchtigende Folgen zeigt (dd)).

aa) Vorliegen einer Entscheidung

Der Output eines autonomen Systems ist dann eine Entscheidung im Sinne des Art. 22 DSGVO, wenn diesem Außenwirkung zukommt. Sind hieran rechtliche Folgen geknüpft, so etwa bei einer automatisierten Kreditentscheidung oder einer personalisierten Preisbildung, handelt es sich um eine automatisierte Ent-

---

(Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 112, 113 f.; *Lorentz*, Profiling, 2019, S. 113–116. Die Frage, ob und inwieweit ein Profil und seine Einzelinhalte, personenbezogene Daten darstellen können, ist im Einzelnen durchaus komplex. Umstritten ist insbesondere, ob die einzelnen Inferenzen, die letztlich Wahrscheinlichkeitsaussagen darstellen, personenbezogene Daten sein können. Siehe eingehend hierzu *Lorentz*, Profiling, 2019, S. 113–116. Diese Frage wird vor allem im Rahmen des Kredit-Scorings eingehend diskutiert, siehe hierzu Simitis, BDSG/*Ehmann*, § 28b Rn. 49–57; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 417–423; *Beckhusen*, BKR 5 (2005), 335, 337–339. Diese Fragen liegen jenseits des Forschungszugriffs dieser Arbeit. Im Weiteren wird daher unterstellt, dass es sich beim Profil sowie den einzelnen Profilinhalten um personenbezogene Daten handelt.

[122] Vgl. nur *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 9 f. Siehe auch *Kamarinou/Millard/Singh*, Machine Learning with Personal Data, Queen Mary School of Law, 7.11.2016, S. 11; *Lorentz*, Profiling, 2019, S. 156; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 10.

[123] Vgl. auch *Lorentz*, Profiling, 2019, S. 254–258.

scheidung.[124] Komplexer stellt sich die Situation bei Informationsfilterdiensten oder personalisierter Werbung dar. Nur wenn man anerkennt, dass auch Maßnahmen als Entscheidung nach Art. 22 DSGVO gelten können,[125] unterfallen sie der Vorschrift. Ob dann aber die bloße Anzeige des Outputs eine solche Maßnahme darstellt, ist unklar.[126]

bb) Unterworfenheit unter eine Entscheidung

Für die Bewertung, ob die betroffene Person den Einstellungen und Steuerungen durch autonome Systeme unterworfen ist, muss zwischen verschiedenen Anwendungsarten unterschieden werden. Hier können die Referenzbeispiele zur Differenzierung herangezogen werden, nämlich einerseits automatisierte Steuerung ((1)), andererseits automatisierte Entscheidungen[127] ((2)).

(1) Automatisierte Steuerungen

Für Unsicherheiten sorgt, worin bei personalisierten Diensten, etwa der Informationsfilterung oder der personalisierten Werbung, der Anknüpfungspunkt

---

[124] Zum Vertragsschluss *Finck*, Int. Data Priv. Law 9 (2019), 78, 82 f.; *Abel*, ZD 8 (2018), 304, 305. Bei personalisierten Preisen liegt die Entscheidung in der errechneten Preisvorgabe, so *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 101; *Tillmann/Vogt*, VuR 33 (2018), 447, 451. Zu dieser Einordnung auch *Veale/Edwards*, CLSR 34 (2018), 398, 401; *Golland*, CR 36 (2020), 186, 192; *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 250. AA *Hofmann/Freiling*, ZD 10 (2020), 331, 335, denenzufolge der berechnete Preis lediglich Angebot und daher keine Entscheidung ist.

[125] So Erwägungsgrund 71 S. 1. Siehe oben Kapitel 4 B. II. 3. a) aa).

[126] Befürwortend für die personalisierte Werbung Ebenso *Lorentz*, Profiling, 2019, S. 266. Ohne nähere Begründung bejaht der Europäische Datenschutzausschuss bei Online-Werbung das Vorliegen einer Entscheidung, siehe *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 24. Von einer Entscheidung bei der Online-Werbung gehen im Ergebnis auch aus, allerdings ohne Begründung, *Schleipfer*, ZD 7 (2017), 460, 462; *Kugelmann*, DuD 40 (2016), 566, 570; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 65; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 37. Ablehnend hinsichtlich Anzeigen von Suchdiensten Gola, DS-GVO/*Schulz*, Art. 22 Rn. 17; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 18. Ablehnend hinsichtlich der Anzeige von Werbeinhalten *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 235 f.; ablehnend bei Empfehlungssystemen *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 19. Allgemein zurückhaltend, ob ein bloßer Output eine Maßnahme darstellen kann, *Finck*, Int. Data Priv. Law 9 (2019), 78, 83.

[127] Hier sei nochmals darauf hingewiesen, dass die Bezeichnung automatisierter Entscheidung für die Beschreibung einer bestimmten Anwendung autonomer Systeme, nämlich solcher im Drittinteresse, gewählt wurde und nichts darüber aussagt, ob es sich dabei auch um eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO handelt. Siehe hierzu bereits oben Kapitel 1 A. III. 2.

der Unterworfenheit zu sehen ist. Liegt dieser in der Annahme des Vorschlags durch die betroffene Person, wird man ein Unterworfensein verneinen müssen. Denn es steht den NutzerInnen frei, die Suchvorschläge bzw. Empfehlungen zu übernehmen.[128] Personalisierte Werbeanzeige können sie ignorieren oder sich gegen die gefilterten Vorschläge entscheiden.[129] Liegt dieser in der Nutzung des Dienstes, ist eine Unterworfenheit ebenso ausgeschlossen, da die NutzerInnen das Informationsfilterungssystem jederzeit an- und abschalten können.[130] Fokussiert man dagegen auf die Auswahl des Informationsangebots bzw. der Werbeanzeige, so lässt sich eine Unterwerfung durchaus begründen, denn auf die Auswahl und Filterkriterien der Anzeige haben die NutzerInnen regelmäßig[131] keinen, jedenfalls keinen unmittelbaren Einfluss.[132]

(2) Automatisierte Entscheidungen

Bei personalisierten Entscheidungen, nach den Referenzbeispielen also bei automatisierten Kreditentscheidungen oder personalisierten Preisen, ist die betroffene Person regelmäßig einer Entscheidung unterworfen, zumindest in den hier behandelten Konstellationen, in denen die Vertragsinhalte, d.h. die Zu- oder Absage des Kreditvertrags oder der konkrete Preis, der betroffenen Person einseitig vorgegeben werden, diese also nicht mitverhandeln oder Vertragsinhalte selbst konfigurieren kann.[133]

---

[128] Vgl. Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 31a; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 18. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 19.

[129] Siehe zu diesem Argument *Veale/Edwards*, CLSR 34 (2018), 398, 401. Ähnlich *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 237: „[D]ie letzte Entscheidungsgewalt [verbleibt] beim Betroffenen". Vgl. auch *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 285.

[130] Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 19 f.; befürwortend Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 24c.

[131] In der Praxis gesteht der Verantwortliche den betroffenen Personen Abänderungsmöglichkeiten des Filtersystems und seiner Kriterien nur selten zu, insbesondere da dies mit einigem technischen Aufwand verbunden ist. Eine solche Einwirkungsoption entspricht ohnehin typischerweise nicht dem Interesse der NutzerInnen, für die der Mehrwert der Informationsfilterung gerade in der umfassenden Ab- bzw. Übernahme der Filterleistung durch die Dienste liegt.

[132] So für die Informationsfilterung Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 35. In diese Richtung wohl auch *Edwards/Veale*, SSRN Journal 2017, 47. So für die personalisierte Werbung *Lorentz*, Profiling, 2019, S. 266.

[133] Vgl. zu diesen Kriterien Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 16–17; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 24b.

cc) Ausschließlich automatisierte Entscheidung

Die Tatbestandsvoraussetzung des ausschließlichen Beruhens sorgt für einige Rechtsunsicherheiten. Unklar ist zum einen, auf welchen Zeitpunkt für den Einbezug des menschlichen Entscheiders abzustellen ist ((1)). Zudem ist nicht geklärt, wie damit umzugehen ist, wenn sich der menschliche Entscheider aus verhaltensökonomischen Gründen an die maschinelle Vorgabe gebunden fühlt (Automation Bias) ((2)).

(1) Zeitpunkt für die menschliche Involvierung

Die menschliche Supervision im Rahmen des Trainingsverfahrens ist unbeachtlich, denn dieses bezieht sich allein auf das vorangehende Algorithmentraining, nicht auf den eigentlichen Entscheidungsfindungsprozess.[134] Entscheidend ist demnach, inwieweit eine natürliche Person – dies kann die betroffene Person ebenso sein wie Entscheider auf Seiten des Verantwortlichen oder Dritter – auf den konkreten algorithmischen Entscheidungs- und Steuerungsprozess einwirken kann. Der Europäische Datenschutzausschuss stellt, wie beschrieben, maßgeblich auf die Befugnis und Fachkompetenz einer natürlichen Person zur Prüfung oder Abänderung der Entscheidung ab.[135] Wiederum ist dann, wie schon bei der Unterworfenheit, maßgeblich, auf welchen Moment – die Übernahme des Outputs, die Nutzung des Dienstes oder das algorithmische Verfahren der Ergebnisfindung – man abstellt. Bei personalisierten Steuerungen, d.h. bei der Informationsfilterung und personalisierter Werbung, wird überwiegend auf die Übernahme des Outputs abgestellt und daher ein Beruhen abgelehnt: Die betroffene Person hat die Kompetenz, den Vorschlag abzulehnen.[136] Nur teilweise wird auf das Verfahren der Ergebnisfindung fokussiert und ein Beruhen bejaht, da die betroffene Person regelmäßig auf die Ausgabe und die Auswahlkriterien keinen Einfluss hat.[137] Bei personalisierten Ent-

---

[134] *Hoeren/Niehoff*, RW 9 (2018), 47, 53; Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 19b; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 23.2. Anschaulich *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 279 „eher [eine] ‚Wartung' des Systems".

[135] Siehe unter II. 2. c) aa) (1).

[136] Für Suchmaschinen Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 19. Ähnlich für SmartHome-Anwendungen Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 24c.

[137] So für Suchmaschinen Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 35. So im Ergebnis auch die Stimmen, die die personalisierte Werbung dem Art. 22 DSGVO unterstellen – wenngleich jeweils ohne spezifische Befassung mit der Frage der Unterworfenheit –, so vor allem der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 24, bestätigt durch *ders.*, Guidelines 8/2020 on the targeting of social media users, Europäischer Datenschutzausschuss, 02.09.2020, S. 30 f. Aus der Literatur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 37. Ebenso zur Qualifizierung als ausschließlich automatisierte Entscheidung, wenngleich sie die Anwendung des Art. 22 DSGVO aufgrund des Fehlens einer erheblichen Be-

scheidungen, dann also der Kreditentscheidung oder personalisierten Preisbildung, soll es dagegen maßgeblich auf das algorithmische Verfahren *und* das Verfahren im Nachgang ankommen.[138] Kann ein menschlicher Entscheider rechtlich und tatsächlich in das algorithmische Verfahren zur Erstellung eines Outputs einwirken, liegt ein ausschließliches Beruhen nicht vor.[139] Auch wenn der menschliche Entscheider befugt und fähig ist, im Anschluss den Output des Systems zu prüfen oder hiervon abzuweichen, d.h. den Output nur, neben anderen Faktoren,[140] zur Grundlage einer eigenen Entscheidung macht, liegt ein ausschließliches Beruhen nicht vor.[141] Da eine den Art. 22 DSGVO ausschließende menschliche Beteiligung auch schon dann vorliegt, wenn eine natürliche Person den Output prüfen und vom ihm abweichen kann, ist es irrelevant, wenn sie nicht auch das algorithmische Entscheidungsverfahren prüfen kann. Dass selbstlernende Algorithmen nur beschränkt menschlich nachvollziehbar sind, führt daher nicht stets zu einem ausschließlichen Beruhen. Soweit die maschinelle Ausgabe unmittelbar in einen Vertrag mündet, liegt in jedem Fall eine automatisierte Entscheidung vor.[142] Soweit bei Kredit-Scoring-Verfahren das autonome System InteressentInnen unterhalb eines bestimmten Score-Wertes aussortiert (sogenannter Cut-Off-Score), liegt eine automatisierte Entschei-

---

einträchtigungswirkung ablehnen – *Lorentz*, Profiling, 2019, S. 265; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27b; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26. Zumindest für das Re-Targeting bejahend *Galetzka*, K&R 18 (2018), 675, 678.

[138] Vgl. nur Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 36 – *SCHUFA Holding*.

[139] Dies betrifft beim Kredit-Scoring den Fall, dass ein Mensch nicht in den algorithmischen Prozess zur Erstellung eines Kreditscores einwirkt bzw. einwirken kann. Siehe hierzu Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 36 – *SCHUFA Holding*.

[140] Stellt der Sachbearbeiter bei seiner Entscheidung neben dem maschinellen Vorschlag auch auf andere Umstände ab, ist dies kein Fall des Art. 22 DSGVO, vgl. Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 15.

[141] So liegt der Fall typischerweise beim Ranking, bei dem das System nur eine Vorauswahl trifft bzw. lediglich eine Vorstrukturierung vornimmt, es dann aber dem menschlichen Akteur überlassen bleibt, aus dieser Liste Vertragspartner auszuwählen. Siehe Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 16; ebenso Gola, DS-GVO/*Schulz*, Art. 22 Rn. 13 f.; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 14 f. Auch beim Kredit-Scoring ist ein ausschließliches Beruhen zu verneinen, wenn der Sachbearbeiter den errechneten Scorewert nochmals inhaltlich prüft und bewertet. Vgl. Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 15; Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 36 – *SCHUFA Holding*.

[142] Siehe auch Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 16c; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 13–14; *Lorentz*, Profiling, 2019, S. 263.

dung im Sinne des Art. 22 DSGVO vor,[143] ebenso, wenn im Rahmen personalisierter Preisbildung der Output den verbindlichen Preis darstellt.[144]

(2) Verhaltensökonomisch bedingte Entscheidungsautomation (Automation Bias)

Darüber hinaus ist unklar, wie der Umstand zu bewerten ist, dass Personen aus verhaltensökonomischen Gründen geneigt sind, algorithmische Ergebnisse ungeprüft zu übernehmen (Automation Bias auch quasi-automation).[145] In diesen Fällen bestehen formal Prüfungskompetenzen und -befugnisse, werden aber tatsächlich nicht wahrgenommen. Der EuGH hat sich hierzu bislang nicht geäußert.[146] Der Generalanwalt beim EuGH Pikamäe, tritt dafür ein, in Fällen faktischer Vorwegbestimmung im Einzelfall von einer automatisierten Entscheidung im Sinne des Art. 22 DSGVO auszugehen; ausdrücklich geht er aber nicht auf das Phänomen des Automation Bias ein.[147] Der Europäische Datenschutzausschuss bzw. die Artikel 29 Datenschutzgruppe als Vorgängerin hat sich zu dieser Frage noch nicht positioniert. In der Literatur wird teilweise die

[143] Siehe nur Erwägungsgrund 71 S. 1, der explizit die automatische Ablehnung eines Online-Kreditvertrages aufführt. So auch Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 24; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 16; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 15. Vgl. instruktiv *Kamp/Körffer/Meints*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 201, 210, die verschiedene Grade menschlicher Involvierung bei der automatisierten Kreditvergabe und die entsprechende Anwendbarkeit des Art. 22 DSGVO beleuchten.

[144] Vgl. wenn auch für die automatisierte Bestimmung der Zahlungsart *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 321, demzufolge regelmäßig von einem ausschließlichen Beruhen auszugehen ist, da es der zuständigen Person im Online-Handel regelmäßig schon aus Zeitgründen nicht möglich ist, eine eigenständige Auswahlentscheidung anzustellen.

[145] Eingehend Kapitel 2 C. IV. 2. a). Siehe zu diesem Phänomen auch *Skitka/Mosier/Burdick u.a.*, Int. J. Hum. Comput. 51 (1999), 991–1006; *Wagner*, Policy & Internet 11 (2019), 104–122, zur juristischen Rezeption siehe etwa *Edwards/Veale*, SSRN Journal 2017, 45; *Veale/Edwards*, CLSR 34 (2018), 398, 400. Vgl. auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 162.

[146] Allerdings hat das VG Wiesbaden am 15. Oktober 2021 eine Vorlagefrage zum externen Kredit-Scoring gestellt, geführt unter dem Aktenzeichen C-634/21. Die Entscheidung des EuGH stand im Zeitpunkt des Verfassens dieser Arbeit noch aus. Im Januar 2023 folgte hierzu eine mündliche Verhandlung, siehe hierzu *Häuselmann*, The ECJ's First Landmark Case on Automated Decision-Making, 29.02.2023, https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber. Angedeutet wird darin, dass bereits die Ausgabe des Kreditscores durch die Auskunftei, auf den dann eine natürliche Person auf Seiten des Kreditinstituts maßgeblich ihre Entscheidung stützt, als Entscheidung im Sinne des Art. 22 DSGVO gewertet wird. Da diese Ausgabe automatisiert erstellt ist, wäre Art. 22 DSGVO anwendbar.

[147] So im soeben genannten Vorlageverfahren Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 42, 47 – *SCHUFA Holding*.

Berücksichtigungsfähigkeit des Automation Bias gänzlich abgelehnt, da es sich um ein vages, kaum justiziables subjektives Phänomen handelt.[148] Vorgebracht wird auch, dass es sich nicht eigentlich um eine Problematik automatisierter Entscheidungsverfahren handle, sondern um Fragen der Unbefangenheit menschlicher Entscheidung und damit letztlich um Fragen der Entscheidungsrichtigkeit, die jenseits des Datenschutzrechts stehen.[149]

dd) Rechtliche Wirkung oder in ähnlicher Weise erheblich beeinträchtigend

Ob die automatisierte Entscheidung rechtliche Wirkung zeigt oder in ähnlicher Weise die betroffene Person erheblich beeinträchtigt, lässt sich nur mit Blick auf den Einzelfall feststellen. Umfassend diskutiert werden derzeit die Folgen von personalisierten Werbemaßnahmen, aus denen Wertungen für Informationsfilterdienste abgeleitet werden können; sie sollen daher vorab dargestellt werden ((1)), sodann soll auf die Informationsfilterung ((2)), die automatisierte Kreditvergabe ((3)) sowie personalisierte Preise ((4)) eingegangen werden.

(1) Personalisierte Werbung

Rechtliche Wirkungen erfolgen bei personalisierten Werbemaßnahmen nicht.[150] Die faktische Beeinträchtigungswirkung liegt hier in der der manipulativen Wirkung von Werbung, d.h. in der Einwirkung auf die menschliche Autonomie. Dem Europäischen Datenschutzausschuss zufolge kann personalisierter Werbung im Einzelfall eine erhebliche Beeinträchtigungswirkung zukommen. Er benennt dafür beispielhaft vier Kriterien: der eingreifende Charakter der Profiling-Prozesse, die Erwartungen und Wünsche der Person, die Art und Weise der Werbeanzeige sowie die Ausnutzung von Schwachstellen der betroffenen Person.[151] Dem schließen sich Teile der Literatur an.[152] Teilweise werden dort weitere Kriterien entwickelt, etwa die Schutzwürdigkeit der

---

[148] Vgl. *Ernst*, JZ 72 (2017), 1026, 1031 der zu bedenken gibt, dass sich im Einzelfall kaum wird feststellen lassen, welche Aspekte in die Entscheidung eingeflossen sind und inwieweit der menschliche Entscheider sich vom maschinellen Ergebnis hat leiten lassen.

[149] Vgl. *ders.*, JZ 72 (2017), 1026, 1031.

[150] So auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 22. Auf die Inhalte der potentiellen Vertragsschlüsse – ob diese also eine erhebliche beeinträchtigende Wirkung haben – kann es dagegen nicht ankommen: Dies setzte bereits einen Automatismus zwischen Marketingmaßnahme und Konsum voraus.

[151] *Ders.*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 24. Bestätigt durch *ders.*, Guidelines 8/2020 on the targeting of social media users, Europäischer Datenschutzausschuss, 02.09.2020, S. 30 f.

[152] Befürwortend etwa *Gausling*, ZD 9 (2019), 335, 340; Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 Rn. 535; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 37; *Galetzka*, K&R 18 (2018), 675, 679.

betroffenen Person,[153] eine bewusst-manipulative Ausnutzung von Vulnerabilitäten oder Notsituationen,[154] diskriminierende Effekte[155] der Werbung.[156] Auch eine Abstimmung mit dem wettbewerbsrechtlichen Maßstab des § 7 UWG wird vorgeschlagen.[157]

Überwiegend wird in der Literatur eine Anwendung des Art. 22 DSGVO auf personalisierte Werbemaßnahmen abgelehnt.[158] Gestützt wird dies vor allem

---

[153] So sind Kinder oder sonstige vulnerable Gruppen besonders schutzwürdig, vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 37. Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 24.

[154] So *Gausling*, ZD 9 (2019), 335, 340; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 253 f. mit dem Vorschlag der Übernahme von Gedanken der Wettbewerbsrichtlinie.

[155] Die personalisierte Werbung kann dazu führen, dass einzelnen Personen(gruppen) bestimmte Werbebotschaften übermittelt oder eben nicht übermittelt werden. So können etwa gegenüber einkommensstarken Personen(gruppen) Werbeanzeigen über Luxusgüter oder sonstige Produkte geschaltet werden, die einkommensschwache Personen(gruppen) nicht erhalten. Vgl. zu diesem Beispiel *Lorentz*, Profiling, 2019, S. 271; *Veale/Edwards*, CLSR 34 (2018), 398, 402.

[156] Sehr pauschal Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 31; zumindest bei wiederholter diskriminierender Werbung mit erheblichen wirtschaftlichen Folgen *Mendoza/Bygrave*, in: Synodinou/Jougleux/Markou u.a. (Hrsg.), EU Internet Law, 2017, S. 77, 89; Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 Rn. 534 f. Ähnlich *Veale/Edwards*, CLSR 34 (2018), 398, 401 f., die eine diskriminierende Wirkung im Einzelfall bejahen. In ähnliche Richtung *Galetzka*, K&R 18 (2018), 675, 679, demzufolge auch das Unterlassen von Werbemaßnahmen beeinträchtigende Wirkung zukommen kann. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 57, 59 differenziert nach der konkreten Werbemaßnahme: Geht es allein um Werbebotschaften, die in diskriminierender Weise (nicht) geschaltet werden, soll dies keine erhebliche Beeinträchtigung sein; das Zurückhalten von Prämien, Gutscheinen oder sonstigen Vergünstigungen für bestimmte Personen(gruppen) soll dagegen diskriminierungsrelevant sein.

[157] So etwa Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 65. Siehe auch *Galetzka*, K&R 18 (2018), 675, 679. Nach § 7 UWG ist eine Werbemaßnahme dann belästigend, wenn sie dem Empfänger gegen seinen erkennbaren oder doch mutmaßlichen Willen aufgedrängt wird und bereits wegen ihrer Art und Weise unabhängig Inhalt als störend empfunden wird. Sie muss zudem in unzumutbarer Weise erfolgen. Dies wird anhand verschiedener Kriterien wie etwa die Intensität des Eingriffs oder Ausweichmöglichkeit ermittelt.

[158] Ablehnend *Drewes*, CR 32 (2016), 721, 725 f.; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 235–237, wenn auch unter Anerkennung von Ausnahmen. Ablehnend zumindest für die einzelne geschaltete Werbemaßnahme *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 284 f. Aus der Kommentarliteratur äußern sich ablehnend Gola, DS-GVO/*Schulz*, Art. 22 Rn. 27; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 65; ebenso Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27b, der gleichwohl Ausnahmen anerkennt, sowie Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 34, 41; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26, die dies allerdings nur befürworten, solange sich die geschaltete Werbung innerhalb der wettbewerbsrechtlichen Grenzen des § 7 UWG hält.

auf den Schutzzweck des Art. 22 DSGVO: Betroffene Personen sollen vor undurchsichtigen, unanfechtbaren und unkontrollierbaren Entscheidungen geschützt werden, wohingegen es bei der personalisierten Werbung um Schutz vor manipulativen Einwirkungen gehe. Die Konstellationen sind nicht vergleichbar.[159] Im Übrigen haben diese manipulativen Übergriffe ihre Ursache in den besonders tiefgreifenden und manipulationssensiblen Kenntnissen über die betroffene Person und damit in der Profilbildung, nicht in der Automatisierung der Anwendung.[160] Schließlich werden systematische Argumente vorgebracht: Für die personalisierte Werbung hat der Unionsgesetzgeber mit Art. 21 DSGVO eine spezialisierte Norm geschaffen,[161] darüber hinaus in der ePrivacy-Richtlinie bestimmte Vorschriften – dann also jenseits des Datenschutzrechts – vorgesehen.[162] Letztlich wird das Manipulationspotential von Werbung als Problematik des Wettbewerbs- und des Verbraucherschutzrechts betrachtet, nicht als eine solche des Datenschutzrechts.[163]

(2) Informationsfilterdienste

Bei Informationsfilterdiensten ist allein denkbar, dass die verhaltensökonomisch bedingten Anreize als erhebliche Beeinträchtigungswirkungen einzuordnen sind. Auch diskriminierende Effekte der Informationsfilterung sind denkbar.[164] Der überwiegende Teil der Literatur lehnt eine Anwendung des

---

[159] Konsequent sind denn Werbemaßnahmen in Erwägungsgrund 71 nicht aufgeführt, im Übrigen mit den dort genannten Anwendungsfällen – Kreditvergabe und eRecruiting – nicht vergleichbar. Ebenso *Lorentz*, Profiling, 2019, S. 268, 270; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 236 f.; *Drewes*, CR 32 (2016), 721, 725 f.

[160] So auch *Lorentz*, Profiling, 2019, S. 268–270, 273, die darauf hinweist, dass auch die vom Europäischen Datenschutzausschuss benannten Kriterien – außer der Art und Weise der Werbeanzeige – ausschließlich auf die Phase der Profilbildung gerichtet sind. Art. 22 DSGVO stellt aber für die Frage, ob eine erhebliche Beeinträchtigung vorliegt, allein die Folgen der Verwendung des Profils im Anschluss ab. Ebenso *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 103. In diese Richtung auch *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 238–240.

[161] Siehe zu diesem Argument *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 306; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26; *Lorentz*, Profiling, 2019, S. 270 f. Ebenso Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27b, der aber zugesteht, dass im Einzelfall eine Beeinträchtigung im Sinne des Art. 22 DSGVO denkbar ist. Kritisch zu diesen Argumenten Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 38, demzufolge Art. 21 Abs. 2 DSGVO allein die Datenverarbeitung im Vorfeld der Direktwerbung, nicht die Schaltung der Werbebotschaft selbst betreffe.

[162] Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 67.

[163] So Wolff/Brink BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 41; *Veale/Edwards*, CLSR 34 (2018), 398, 401.

[164] Vgl. hierzu *Edwards/Veale*, SSRN Journal 2017, 56–58.

Art. 22 DSGVO auf Informationsfilterdienste jedoch ab.[165] Die Erwägungen hinsichtlich personalisierter Werbung lassen sich übertragen.

(3) Automatisierte Kreditvergabe

Hinsichtlich der Effekte auf automatisierte Vertragsgestaltungen ist zu differenzieren, ob ein Rechtsverhältnis nach den Vorstellungen der betroffenen Person zustande kommt. Ist dies der Fall, werden mit dem Rechtsverhältnis und den jeweiligen Bedingungen rechtliche Folgen gesetzt.[166] Verlangt man einschränkend, dass diese rechtliche Wirkungen nachteilig sein müssen, ist Art. 22 DSGVO bei automatisierten Vertragsgestaltungen allein dann von Relevanz, wenn es im Anschluss an den Vertragsschluss zu Aufhebungen oder Belastungen von Rechten kommt, etwa in Form automatisierter Kündigungen[167] oder wenn man auf die Begründung von Zahlungspflichten abstellt.[168]

Wird ein Rechtsverhältnis nicht begründet oder ein Rechtsverhältnis zwar eingegangen, aber nicht mit den von der jeweiligen Person erwünschten Inhalten, etwa bei der Nichtgewährung von Rabatten oder bei personalisierten Preisen,[169] bedingt dies zwar keine rechtlichen Folgen.[170] In Betracht kommt dann

---

[165] So etwa Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 31a; *Hennemann*, ZUM 61 (2017), 544, 547. Ähnlich Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 27b: „Personalisierte Werbung und sonstige vergleichbare Individualisierungen […] erfasst Abs. 1 grds. [nicht]". Vgl. auch *Edwards/Veale*, SSRN Journal 2017, 46–48.

[166] Vgl. zum Vertragsschluss anhand Kredit-Scorings, wenn auch zur deutschen Vorgängervorschrift § 6a BDSG a.F., *Moos/Rothkegel*, ZD 6 (2016), 565.

[167] So auch Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 28; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 34. Der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23 erwähnt die Auflösung eines Vertrags.

[168] *Finck*, Int. Data Priv. Law 9 (2019), 78, 84, die jedoch auch vorteilhafte rechtliche Wirkungen, etwa den Eigentumserwerb unter Art. 22 DSGVO fasst.

[169] Auch personalisierte Preise können als Verweigerung eines Vertragsschlusses gesehen werden, da der Vertrag eben nicht mit dem von der betroffenen Person erwünschten Preis zustande kommt. Dies entfaltet aber keine rechtlichen Folgen, vgl. zu dieser Einordnung Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 35; *Tillmann/Vogt*, VuR 33 (2018), 447, 450; *Golland*, CR 36 (2020), 186, 192. Andere weisen darauf hin, dass der personalisierte Preis immer nur Angebot des Verantwortlichen ist, das die betroffene Person nicht bindet, jedenfalls aber bloße Vorstufe zum Vertragsschluss ist und daher keine rechtlichen Folgen entfaltet, vgl. *Linderkamp*, ZD 10 (2020), 506, 507 f.; *Hofmann/Freiling*, ZD 10 (2020), 331, 335; *Ernst*, JZ 72 (2017), 1026, 1034. Vgl. auch *Hennemann*, AcP 219 (2019), 818, 836.

[170] Da es in einer privatautonomen Rechtsordnung keinen Anspruch auf Abschluss eines (bestimmten) Rechtsverhältnisses geben kann, löst die Ablehnung eines Vertrags keine Rechtsfolgen aus. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 34, 39a; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 24; Ehmann/Selmayr, DS-GVO/*Hladjik*, Art. 22 Rn. 9. AA Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 62 f.; Sydow,

allerdings eine erhebliche Beeinträchtigungswirkung. Einige verneinen eine solche mit Hinweis auf die Privatautonomie, wonach die Ablehnung eines erwünschten Vertragsschlusses rechtlich nicht schutzwürdig sei, alles andere zu einem Kontrahierungszwang durch die Hintertür führe.[171] Dem wird entgegengehalten, dass die Rechtsinstrumente des Art. 22 DSGVO gar nicht auf Abschluss eines Vertrags abzielten, sondern allein auf den Schutz vor einer maschinellen Vertragsablehnung.[172] Im Übrigen wird zwischen der Ablehnung eines Vertragsabschlusses und dem Scheitern eines Vertrages zu bestimmten Bedingungen unterschieden. Auf die zweite Konstellation ist sogleich im Rahmen personalisierter Preise vertieft einzugehen.

Hinsichtlich der Vertragsablehnung wird teilweise dafür eingetreten, dass eine jede automatisierte Ablehnung eines Vertragsschlusses eine beeinträchtigende Wirkung im Sinne des Art. 22 Abs. 1 DSGVO darstelle.[173] Der Europäische Datenschutzausschuss[174] wie auch der überwiegende Anteil der Literatur[175] stellen eine Einzelfallprüfung an. Maßgeblich soll etwa die Auswirkung

---

DS-GVO/*Helfrich*, Art. 22 Rn. 48; Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 35 – *SCHUFA Holding*, die die Ablehnung eines Vertrages als rechtliche Folge einordnen.

[171] Vgl. *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 306; *Golland*, CR 36 (2020), 186, 192; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 36. Es sei überdies nicht einleuchtend, warum für Online-Kreditverträge anderes gelten soll als für analog in der Bankfiliale geschlossene, vgl. zu all dem Gola, DS-GVO/*Schulz*, Art. 22 Rn. 26. Dem tritt Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26a entgegen: Nicht jede Ablehnung eines Vertragsschlusses, sondern allein eine solche durch ausschließlich automatisierte Verfahren sei durch Art. 22 DSGVO unterbunden. Eben diese weist gegenüber menschlicher Entscheidung eigene Gefährdungen auf. So auch Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 28. Ähnliche Gedanken im Rahmen des automatisierten Personalrecruitings äußert Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 56.

[172] Zutreffend Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 58; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26a.

[173] So etwa Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 S. 534; Ehmann/Selmayr, DS-GVO/*Hladjik*, Art. 22 Rn. 9. Überwiegend wird dies als zu weitgehend erachtet. Denn nicht jeder Verlust einer Vertragsabschlusschance zu einer nachhaltigen Belastung des wirtschaftlichen oder sonstigen Status. Vgl. etwa Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26a; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27.

[174] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 23 f.

[175] Vgl. nur Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27, 27a; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 38, 39a. Vgl. auch *Dammann*, ZD 6 (2016), 307, 313. Ähnlich Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26a, der zwar sämtliche Vertragsverweigerungen Art. 22 DSGVO unterstellen will, allerdings am Kriterium der Erheblichkeit scheitern lässt, wenn die Ablehnung des Vertrages nicht „von spürbarer Relevanz“ für die betroffene Person ist.

auf die finanzielle Lage der Person sein oder die Bedeutung des Vertrages für Lebensgestaltung, etwa wenn die Vertragsablehnung sich nachteilig auf den Zugang zu Gesundheitsleistungen, Arbeitsplätzen oder Bildung auswirkt.[176] Als Kriterium wird auch die Verfügbarkeit von Alternativen auf dem Markt herangezogen.[177] Auch auf diskriminierende Effekte wird abgestellt. Während die einen Art. 22 DSGVO bei jeglicher diskriminierender Vertragsablehnung anwenden wollen,[178] bejahen dies andere nur, falls Personen beim Zugang zu Gütern und Dienstleistungen diskriminiert werden,[179] die für den Lebensunterhalt essentiell sind, oder eine diskriminierte Minderheit marktübergreifend vom Zugang zu Gütern oder Dienstleistungen ausgeschlossen wird.[180]

(4) Personalisierte Preise

Ähnlich unklar ist, inwieweit das automatisierte Zustandekommen von Verträgen zu bestimmten Bedingungen eine erhebliche Beeinträchtigung darstellen kann. Als Referenzbeispiel sollen hierfür personalisierte Preisgestaltungen dienen. Manche sehen bereits in der Beschränkung der Verhandlungsfreiheit bzw. Privatautonomie die maßgebliche Beeinträchtigungswirkung.[181] Andere stellen

---

[176] *Artikel 29 Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10.04.2014, S. 23 f. Auch die Literatur stellt darauf ab, ob der Vertrag in einen für die Lebensführung wesentlichen Bereich, etwa den der Daseinsvorsorge, fällt. Vgl. Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 39a; *Abel*, ZD 8 (2018), 304, 307.

[177] Etwa, da sie die erwünschte Leistung überhaupt nicht oder jedenfalls nur zu deutlich ungünstigeren Bedingungen erlangen kann. Es geht dann um Versorgungsunternehmen oder Unternehmen mit monopolartiger Stellung, so Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 39a; *Moos/Rothkegel*, ZD 6 (2016), 566. Auch die Marktmacht des Anbieters ist dann von Relevanz, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 39a; *Golland*, CR 36 (2020), 186, 192. Teilweise werden diese Kriterien auch kombiniert. Es kommt dann also auf den Bedarf und die Verfügbarkeit an. Eine erhebliche Beeinträchtigung liegt etwa dann vor, wenn ein Vertragsschluss im Bereich der Daseinsvorsorge bei zugleich monopolartiger Struktur des Marktes verweigert wird, so etwa *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 306; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 24; *Abel*, ZD 8 (2018), 304, 306; *Golland*, CR 36 (2020), 186, 192.

[178] Kuner/Bygrave/Docksey, GDPR/*Bygrave*, Art. 22 Rn. 534; *Abel*, ZD 8 (2018), 304, 306.

[179] So Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27. In diese Richtung auch Gola, DS-GVO/*Schulz*, Art. 22 Rn. 23: „[…] wobei die Schwelle zur bloßen Belästigung überschritten sein muss".

[180] So etwa *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 306; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27; *Moos/Rothkegel*, ZD 6 (2016), 566. Kritisch *Golland*, CR 36 (2020), 186, 192 mit dem Hinweis darauf, dass bestimmte Personengruppen stets vom Zugang zu Gütern ausgeschlossen sind, etwa zu Luxuswaren oder zu verschreibungspflichtigen Medikamenten.

[181] So *Linderkamp*, ZD 10 (2020), 506, 507 f., der allerdings zusätzliche Defizite in der Entscheidungsfähigkeit der betroffenen Person verlangt. Dies soll der Fall sein bei diskrimi-

auf den Vertragsinhalt und dessen wirtschaftliche Belastungswirkung ab.[182] Es fällt dann allerdings schwer, eine Bemessungsgrundlage zu bestimmen, denn in einer freien Marktwirtschaft gibt es keine vorgegebenen Preislisten.[183] Die einen stellen auf den marktüblichen,[184] andere auf den von der betroffenen Person vorgeschlagenen[185] Preis ab. Klärungsbedürftig ist darüber hinaus, wie hoch die Preisdifferenz sein muss. Die einen betrachten bereits jede nachteilige Preisdifferenz als ausreichend,[186] andere stellen eine wertende Gesamtbeurteilung an und halten geringfügige Preisdifferenzen für unbeachtlich.[187] Andere lehnen es gänzlich ab, dass der automatisierten Vertragsgestaltung überhaupt eine Beeinträchtigungswirkung zukommen kann, da jeder Schutz vor einem bestimmten Vertragsinhalt mit den Grundannahmen einer freien Marktordnung unvereinbar sei.[188] Grenzen ergeben sich allein aus dem Verbraucher- und Wettbewerbsrecht.[189]

---

nierenden Preisdifferenzierungen oder bei der Ausnutzung von Notlagen der betroffenen Person. Auf das Ausnutzen einer Notlage, etwa das Höhertreiben des Preises im Falle besonderen Bedarfs, stellen ebenso ab *Tillmann/Vogt*, VuR 33 (2018), 447, 450. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 36.

[182] Etwa Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27a. So wohl auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 36.

[183] Vgl. *Tillmann/Vogt*, VuR 33 (2018), 447, 450; *Linderkamp*, ZD 10 (2020), 506, 508. So auch *Ernst*, JZ 72 (2017), 1026, 1034. Ähnlich ist die Konstellation, wenn das Scoring zu ungünstige(re)n Vertragsbedingungen führt, etwa einem höheren Kreditzins oder einer längeren Laufzeit, zu diesen Beispielen Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 40; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 25.

[184] So etwa *Golland*, CR 36 (2020), 186, 192; *Tillmann/Vogt*, VuR 33 (2018), 447, 450; *Linderkamp*, ZD 10 (2020), 506, 508. Ähnlich Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 62; *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 250.

[185] Noch weiter *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 250, der Art. 22 DSGVO bereits für einschlägig hält, wenn die personalisierte Preisbildung nicht nur zum Vorteil des Betroffenen erfolgt. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 36 benennt keine Bemessungsgrundlage und erkennt letztlich jede automatisierte Preisdifferenzierung als erhebliche Beeinträchtigung an.

[186] Vgl. etwa *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 250, wonach es bereits ausreichend sein soll, dass eine Person bestimmte Vergünstigungen nicht erhält, die anderen Personen zukommen.

[187] Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27a; *Martini*, Blackbox Algorithmus, 2019, S. 180 Fn. 75. So *Ernst*, JZ 72 (2017), 1026, 1035. Noch weiter *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 250, der Art. 22 DSGVO bereits für einschlägig hält, wenn die Personalisierte Preisbildung nicht nur zum Vorteil des Betroffenen erfolgt.

[188] Es gehöre zum typischen Risiko, Waren oder Dienstleistungen zu nachteiligeren Bedingungen einkaufen zu müssen als andere bzw. als gewollt. Vgl. zu diesen Überlegungen auch *Ernst*, JZ 72 (2017), 1026, 1034.

[189] So auch *ders.*, JZ 72 (2017), 1026, 1034.

Der Europäische Datenschutzausschuss, gefolgt von Teilen der Literatur,[190] stellen auch hier eine Einzelfallabwägung an. Eine erhebliche Beeinträchtigung soll vorliegen, wenn die Vertragsbedingung zu einem Ausschluss von bestimmten Waren oder Dienstleistungen führt.[191] Maßgeblich sind zudem Bedeutung und Bedarf der Ware oder Dienstleistung, die Verfügbarkeit von Alternativen und die Marktmacht des Anbieters.[192] Ebenso kann das Ausnutzen einer Notlage eine erhebliche Beeinträchtigung begründen.[193] Auch aus der Rechtsordnung bekannte Wertungen, etwa zu Wuchergeschäften, lassen sich übertragen.[194]

Eine diskriminierende Differenzierung der Vertragsbedingungen zwischen Personengruppen kann ebenso eine erhebliche Beeinträchtigung darstellen.[195] Während hier einige Stimmen jede gegenüber der Mehrheit striktere oder nachteilige Vertragsbedingung als relevant erachten,[196] fordern andere zusätzlich den Nachweis belastender Effekte, etwa das Herausdrängen aus dem Markt durch das Fehlen von Alternativen.[197]

Das automatisierte Zustandekommen eines Vertrags sowie der automatisierte Vertragsschluss zu erwünschten oder (nach wirtschaftlichen Kriterien zu bemessenden) günstigen Bedingungen fällt dagegen nach überwiegender Auffassung nicht unter Art. 22 DSGVO. Erhalten bei automatisierten Kreditvergaben Personen ein Vertragsangebot, das sie bei einer persönlichen Verhandlung nicht erhalten hätten,[198] ist Art. 22 DSGVO ebenso wenig anwendbar wie ein personalisierter Preis, der einen günstigeren Preis errechnet, als die betroffene

---

[190] Eine Einzelfallabwägung fordern auch Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 27a; *Tillmann/Vogt*, VuR 33 (2018), 447, 450; *Linderkamp*, ZD 10 (2020), 506, 508. So auch *Hofmann/Freiling*, ZD 10 (2020), 331, 335; *Dammann*, ZD 6 (2016), 307, 313.

[191] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 24.

[192] Vgl. *Linderkamp*, ZD 10 (2020), 506, 508; *Tillmann/Vogt*, VuR 33 (2018), 447, 450. Vgl. auch *Golland*, CR 36 (2020), 186, 192.

[193] So *Linderkamp*, ZD 10 (2020), 506, 508. Er führt als Beispiel den Kauf einer Flasche Wasser im Fall akuter Dehydrierung des Käufers.

[194] In diese Richtung *ders.*., ZD 10 (2020), 506, 508.

[195] Vgl. auch *Linderkamp*, ZD 10 (2020), 506, 508; *Abel*, ZD 8 (2018), 304, 306. Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 31. Kritisch *Golland*, CR 36 (2020), 186, 192.

[196] *Tillmann/Vogt*, VuR 33 (2018), 447, 450Vgl. *Abel*, ZD 8 (2018), 304, 306.

[197] So *Gausling*, ZD 9 (2019), 335, 340. In diese Richtung Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27a „rechtlich relevante Diskriminierung".

[198] AA Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 28, der auch den Vertragsschluss oder die Erteilung einer Leistung unter Art. 22 DSGVO fassen will.

Person dies selbst für sich verhandelt hätte oder als ihr nach der aktuellen Marktlage zukäme.

ee) Ergebnis: begrenzte Algorithmen- und Automatisierungsregulierung

Die Vorschrift des Art. 22 DSGVO führt zu einiger rechtlicher Unsicherheit. Allein Kreditentscheidungen in bedeutenden Lebensbereichen unterfallen zweifellos der Vorschrift, ob und unter welchen Umständen personalisierte Preisbildungen eine automatisierte Entscheidung darstellen, ist unklar. Umstritten ist insbesondere, ob die personalisierte Werbung in den Anwendungsbereich des Art. 22 DSGVO fällt. Überwiegend wird dies abgelehnt. Personalisierte Informationsfilterungen sind nach allgemeiner Ansicht keine automatisierten Entscheidungen. Soweit Art. 22 DSGVO anwendbar ist, gelten die besonderen für automatisierte Entscheidungen normierten Vorschriften. Annexhaft erfolgt dann auch ein regulativer Zugriff auf das der automatisierten Entscheidung vorausgehende Profiling.[199] Auf die konkreten Inhalte dieser Regelungen soll nachfolgend im Hinblick auf den Rechtmäßigkeits- und Transparenzgrundsatz eingegangen werden.

c) Ergebnis

Der überwiegende Teil der Profilverwendungen durch autonome Systeme unterfällt dem besonderen Regulierungsregime des Art. 22 DSGVO nach überwiegender Ansicht nicht. Autonome Systeme werden daher vornehmlich über die allgemeinen Datenschutzbestimmungen reguliert.

4. Ergebnis

Der regulative Zugriff auf autonome Systeme erfolgt über drei Ansatzpunkte: Die Modellbildung, die Profilbildung sowie die Profilverwendung. Auf allen Verarbeitungsstufen finden die allgemeinen Datenschutzregeln Anwendung. Die Profilbildung stellt zwar ein Profiling nach Art. 4 Nr. 4 DSGVO dar, die DSGVO sieht aber keine profilingspezifischen Regeln vor. Die Profilverwendung stellt nur in wenigen Fällen eine automatisierte Entscheidung nach Art. 22 DSGVO dar. Für die Referenzbeispiele lässt sich dabei feststellen: Automatisierte Entscheidungen sind nach überwiegender Ansicht nur automatisierte Kreditvergabeverfahren in besonderes bedeutenden Vertragsgestaltungen und unter bestimmten belastenden Umständen auch personalisierte Preisbildungen. Teilweise werden auch personalisierte Werbemaßnahmen hierunter gefasst. Informationsfilterdienste unterfallen dem Art. 22 DSGVO nicht. Liegt

[199] Siehe nur *Lorentz*, Profiling, 2019, S. 234 f., 244, 275; Paal/Pauly. DS-GVO/*Martini*, Art. 22 Rn. 23, 39d; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 5.

eine automatisierte Entscheidung vor, wird zugleich auch das Profiling über die Vorschriften zur automatisierten Entscheidung mitreguliert.

IV. Bewertung der regulativen Zugriffe der DSGVO auf autonome Systeme

Die DSGVO bietet über die allgemeinen Datenschutzvorschriften einen Regulierungszugriff über sämtliche Verarbeitungsstufen autonomer Systeme. Dies erlaubt eine umfassende Regulierung autonomer Systeme, zudem eine kooperative Koordination der Regelungen auf den jeweiligen Verarbeitungsstufen. Ob dabei Maschinelle Lernverfahren zum Einsatz kommen, ist ebenso wenig von Relevanz wie der Umstand, dass selbstlernende Algorithmen Anwendung finden. Auch ob Algorithmen erstellt oder Erkenntnisse oder Entscheidungen über betroffene Personen gebildet werden sollen, ist für die Anwendung der DSGVO irrelevant. Überdies erlaubt die DSGVO eine Differenzierung: Die Regulierungsintensität der DSGVO steigert sich entsprechend der Risiken der drei Verarbeitungsstufen für die einzelne betroffene Person. Mit der spezifischen Regulierung automatisierter Entscheidungen bietet die DSGVO einen Regulierungsmechanismus für eine besondere, dann zusätzlich im Algorithmus bzw. in der Automatisierung liegende Gefahr. Dabei wird auch berücksichtigt, dass diese Gefahr gesteigert ist, wenn der automatisierten Entscheidung ein Profiling voran geht. Im Hinblick auf die Steuerungseffektivität der DSGVO ist dies positiv zu bewerten.

Der Regulierungszugriff der DSGVO auf autonome Systeme ist dann aber dadurch abgeschwächt, dass eine Regelung zum Modell bzw. zum Lösungsalgorithmus sowie zu den Maschinellen Lernverfahren fehlt (1.) Zu kritisieren ist überdies, dass das Profil keine eigenständige Regulierung erfährt (2.). Schließlich ist die Regulierungswirkung des Art. 22 DSGVO gering, da nur ein sehr begrenzter Teil autonomer Systeme eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO darstellt (3.).

1. Fehlende Regulierung der Modellbildung und der Erstellung des Lösungsalgorithmus – defizitäre Regulierung des Maschinellen Lernens

Eine Regulierung der Modellbildung fehlt in der DSGVO, auch Vorschriften hinsichtlich der Erstellung des Lösungsalgorithmus enthält sie nicht (a)). Mit Blick auf die praktische Fähigkeit der DSGVO zur Regulierung autonomer Systeme ist dies problematisch. Denn gerade der algorithmische Erstellungsprozess sowie deren Ergebnis, d.h. das Modell und der Lösungsalgorithmus, begründen Regulierungsbedarfe, dies allgemein (b)), als auch im Hinblick auf den Datenschutz (c)).

a) Fehlen einer datenschutzrechtlichen Regulierung der Modellbildung und Erstellung des Lösungsalgorithmus

Die Untersuchung hat gezeigt: Die DSGVO vermittelt keinen spezifischen Zugriff auf das Modellerstellungsverfahren, d.h. auf das Maschinelle Lernverfahren, und auch nicht auf das erstellte Modell.[200] Selbiges gilt dann für die Erstellung und den Inhalt des Lösungsalgorithmus. Dies ist gerade Ausdruck des technikneutralen Regulierungsansatzes. Wie noch näher für den Rechtmäßigkeitsgrundsatz[201] sowie für den Transparenzgrundsatz[202] zu erläutern ist, gelingt es mit den allgemeinen Datenschutzvorschriften nicht, die Regulierungsfragen Maschineller Lernverfahren und seiner Ergebnisse hinreichend zu beantworten. Auch datenschutztypische Schutzinstrumente wie Anonymisierung oder Pseudonymisierung der (Trainings-)Daten bieten keinen Schutz, denn sie verhindern nicht, dass Modelle bzw. Lösungsalgorithmen gebildet werden, die dann belastende Profile bzw. automatisierte Entscheidungen auslösen können.[203] Nach Erwgr. 71 S. 6 sollen zwar bei der Profilbildung geeignete Verfahren verwendet werden,[204] was bestimmte Anforderungen an das Modell und damit auch an das Maschinelle Lernverfahren stellt.[205] Gleichwohl ist das Regulierungsprogramm sehr begrenzt: Gefordert sind allein inhaltlich-qualitative Mindestbedingungen, um fehlerhafte und diskriminierende Profilinhalte zu

---

[200] So auch ausdrücklich *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 308: „The material scope [of data protection law] does not include the model itself".

[201] Siehe Kapitel 4 C. IV. 2. a).

[202] Siehe Kapitel 4 D. IV. 2. a).

[203] Vgl., wenn auch allgemein für Big Data Analyseverfahren, *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 93; *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 307. Siehe auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 439 f.

[204] Nach Erwägungsgrund 72 S. 2 soll der Europäische Datenschutzausschuss konkretisierende Leitlinien erlassen; hiervon hat er bislang jedoch keinen Gebrauch gemacht. Siehe auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, in denen die Gruppe keine Regulierungsvorschläge entwirft, sondern allein die bestehende Rechtslage zusammenfasst.

[205] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 11, der eine Beobachtungs- und Überprüfungspflicht hinsichtlich selbstlernender Systeme verlangt. Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 39d zufolge muss das Modell sicherstellen, dass das Regelwerk im Algorithmus zu nachweisbar erheblichen Korrelationen führt. Ähnlich *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 31, der regelmäßige Algorithmenaudits zur Aufdeckung von Verzerrungen und Korrelationen (dort bezeichnet als „zu starkes Verlassen auf Zusammenhänge" bezeichnet) verlangt. Zudem verlangt er Prüfungen der Richtigkeit und Relevanz der Entscheidungen und des Profils, nicht aber des Algorithmus oder Algorithmenbildungsverfahrens selbst. Siehe auch *Lorentz*, Profiling, 2019, S. 290 f.

verhindern.[206] Die Soll-Vorschrift steht zudem im nicht-verfügenden Teil der DSGVO. Eine echte Regulierung des Modells und des Modellerstellungsverfahrens ist dies nicht.[207]

b) Allgemeine Regulierungsbedürftigkeit des Modells bzw. Lösungsalgorithmus

Im Modell bzw. im Lösungsalgorithmus haben die Autonomiegefährdungen bzw. Diskriminierungen durch autonome Systeme ihren Ursprung. Es ist das Modell, das die Generierung neuer Daten, d.h. die Erzeugung von Erkenntnissen jenseits des Rohdatums und damit effektvolle Personalisierungen erlaubt, die verhaltensökonomische und präemptive Effekte auslösen und Manipulationen ermöglicht.[208] Die Intransparenz des Modells führt dazu, dass diese neuen Erkenntnisse für die betroffene Person unvorhersehbar und nicht nachvollziehbar sind. Dies unterbindet Resilienzmechanismen der betroffenen Person gegen Selbstbestärkungs- und Präemptionseffekte sowie Manipulationen und kann Hemm- und Einschüchterungseffekte auslösen.[209] Das Modell ist es auch, das Klassifizierungen anhand von Diskriminierungsmerkmalen vornehmen und so Grundlage für spätere diskriminierende Anwendungen sein kann.[210] Die Intransparenz des Modells macht es betroffenen Personen unmöglich, diese Diskriminierungen aufzudecken und dagegen vorzugehen.[211] Auch im Lösungsalgorithmus, der die automatisierte Entscheidung bzw. Steuerung trägt, sind eigene Gefährdungen angelegt. Hier ist es die Verknüpfung von Persönlichkeitsmerkmalen mit bestimmten Vor- und Nachteilen, die Autonomiegefährdungen und Diskriminierungen hervorruft. Dass diese Verknüpfungen für

---

[206] Siehe nur *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 30 f., der allein auf Fehler und Verzerrungen abstellt. So auch *Lorentz*, Profiling, 2019, S. 339; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 36; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 11.

[207] So auch *Lorentz*, Profiling, 2019, S. 291, die deshalb die Bindungswirkung des Erwägungsgrundes 71 S. 6 verneint, da es an einem regulativen Anknüpfungspunkt in der DSGVO fehlt, als dessen Konkretisierung dieser Erwägungsgrund gelten könnte.

[208] In diese Richtung *Schermer*, CLSR 27 (2011), 45, 48, 50.

[209] Vgl. auch *Lorentz*, Profiling, 2019, S. 340 f. So auch, wenngleich allgemein hinsichtlich automatisierter Entscheidungsstrukturen, *Martini*, JZ 72 (2017), 1017, 1018 „[Die ‚Blackbox Algorithmus' kann den Menschen] zum Objekt sublimer Steuerung degradieren". Die Intransparenz der Modelle (dort bezeichnet als Gruppenprofile) kritisieren auch *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 448 f.

[210] Vgl. *Schermer*, CLSR 27 (2011), 45, S. 50, 52; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 434; *Lorentz*, Profiling, 2019, S. 207. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 50. Zur fehlenden Berücksichtigung von Gruppeninteressen in der DSGVO siehe sogleich unter B IV 2. a) cc).

[211] Vgl. *Schermer*, CLSR 27 (2011), 45, 50 f. Vgl. auch *Lorentz*, Profiling, 2019, S. 207.

die betroffene Person intransparent sind, kann Hemm- und Einschüchterungseffekte begründen.[212] Die fehlende menschliche Nachvollziehbarkeit verhindert, dass Diskriminierungen unterbunden werden können.[213] Allein mit Blick auf die Steuerungseffektivität erscheint es daher sinnvoll, bereits auf Stufe der Modellbildung bzw. der Erstellung des Lösungsalgorithmus regulativ einzugreifen. Ob dies gerade eine datenschutzrechtliche Regulierungsfrage ist, ist noch zu klären.[214]

c) Datenschutzspezifische Regulierungsbedürftigkeit des Modells bzw. Lösungsalgorithmus

Modell oder Lösungsalgorithmus lösen zudem Blockaden datenschutzrechtlicher Regulierungsinstrumente aus. Dies ergibt sich aus der Bedeutung des Modells bzw. Lösungsalgorithmus im Funktionssystem autonomer Systeme. Denn im Profil werden anhand des Modells Erkenntnisse über die Einzelperson gewonnen, die über den Informationsgehalt des Einzeldatums hinausgehen.[215] Das Profil enthält also ein „Mehr" gegenüber den verarbeiteten Rohdaten. Dabei ist es das Modell, das den Daten jenes „Mehr" hinzufügt. Wenn das Modell für die betroffene Person, im Übrigen auch für den Menschen insgesamt nicht verständlich und damit nicht steuerbar ist, kann es auch das Profil nicht sein. Ähnliches gilt dann für die Profilverwendung. Zwischen Datum und Verarbeitungsergebnis, d.h. das Profil bzw. die automatisierte Anwendung, schieben sich Modell bzw. Lösungsalgorithmus, die aufgrund ihrer fehlenden Nachvollziehbarkeit die in der DSGVO unterstellte[216] Verbindung zwischen Datum und Verarbeitungsergebnis bzw. Realfolgen und Gefährdungen der Datenverarbeitungen kappen.[217] Der fehlende regulative Zugriff auf Modell und Lösungsalgorithmus unterbindet daher auch die Regulierungseffektivität der DSGVO. Hierauf ist noch im Einzelnen im Rahmen des Rechtmäßigkeits- und Transparenzgrundsatzes zurückzukommen.

---

[212] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3; *Martini*, JZ 72 (2017), 1017; *Ernst*, JZ 72 (2017), 1026, 1030.

[213] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3; *Tischbirek*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 103, 110; *Martini*, Blackbox Algorithmus, 2019, S. 57. Siehe zu den Schwierigkeiten, Modell und Lösungsalgorithmus diskriminierungsfrei zu gestalten, bereits oben Kapitel 3 B. I. 3.

[214] Im Ergebnis ist dies zu verneinen, siehe Kapitel 5 B. I. 2. a) aa).

[215] So auch *Lorentz*, Profiling, 2019, S. 335.

[216] Siehe oben Kapitel 4 B I. 1.

[217] Ebenso *Leenes*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 293, 294 f. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 99.

2. Fehlende Regulierung des Profilings

Die Autonomiegefährdungen, wie sie in Kapitel 2 dargelegt wurden,[218] haben ihre Ursache maßgeblich in dem Profil, d.h. in dem über das Rohdatum hinausgehenden Wissen über die Einzelperson. Dieses kann verhaltensökonomische und präemptive Effekte, manipulative Übergriffe sowie Abschreckungs- und Hemmwirkungen auslösen. Zugleich stellt die Unkenntnis von den Profilinhalten die betroffene Person schutzlos vor diesen Autonomiegefährdungen und begründet Abschreckungs- und Hemmeffekte. Das Profil ist dabei nicht eine bloße Addition von Rohdaten und der darin repräsentierten Informationen, sondern Informationsgewinn durch evaluative oder prognostische Interpretation dieser Rohdaten. Das Profil enthält am Ende mehr als die Summe der einzelnen Daten.[219] Die Profilbildung ist damit eine Verarbeitungsart mit einem eigenständigen, d.h. über die allgemeine Verarbeitung von Rohdaten hinausgehenden Gefährdungspotential.[220]

Die Datenschutzinstrumente der DSGVO, die allein an den verarbeiteten Rohdaten anknüpfen, sind daher schon konzeptionell unzureichend.[221] Auch über die Regulierung automatisierter Entscheidungen lässt sich diese profilingspezifische Gefährdung nicht eindämmen,[222] denn Art. 22 DSGVO hat die Gefährdung im Anschluss an die Profilbildung, die durch eine intransparente, nicht beeinflussbare algorithmische Entscheidungsarchitektur ausgelöst ist, im Blick. Hierauf soll noch im Einzelnen eingegangen werden.[223] Für eine effek-

---

[218] Siehe Kapitel 2 C. IV. 2.

[219] Vgl. auch *Lorentz*, Profiling, 2019, S. 335–337. Ebenso spricht *Hildebrandt*, DuD 30 (2006), 548–552 von „knowledge" über die betroffene Person, das anhand der Profilerstellung gebildet wird. Ebenso *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 289: „All in all, profiling generates knowledge".

[220] Siehe bereits *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 28–32 Ebenso *Härting*, CR 4 (2014), 528, 531 f.; *Kugelmann*, DuD 40 (2016), 566, 570; *Lorentz*, Profiling, 2019, S. 334–342; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 10–11, sowie *Schermer*, CLSR 27 (2011), 45, 46–48. Ebenso *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 433–438.

[221] *Lorentz*, Profiling, 2019, S. 334 f. In diese Richtung auch *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 47 mit ihrer Aussage: „More often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern".

[222] Ebenso *Lorentz*, Profiling, 2019, S. 268–270, 273. Ähnlich *Wachter/Mittelstadt*, CBLR 2019, 494, 578: „[T]he problem does not lie so much with data collection, but rather with what can be read from the data and the decisions based on this knowledge".

[223] Siehe sogleich im Rahmen der Prüfung des Rechtmäßigkeits- sowie Transparenzgrundsatzes. Zu den Ergebnissen hinsichtlich des Rechtmäßigkeitsgrundsatzes siehe Kapitel 4 C. IV. 2. b), hinsichtlich des Transparenzgrundsatzes siehe Kapitel 4 D. IV. 2. b) aa).

tive Unterbindung von Autonomiegefährdungen bedarf es demnach einer eigenständigen Regulierung des Profilings.[224]

3. Limitierte Konzeption automatisierter Entscheidungen

Der Unionsgesetzgeber hat automatisierte Entscheidungen nach Art. 22 DSGVO zu eng gefasst; nur ganz bestimmte Ausgestaltungen bzw. Anwendungen autonomer Systeme unterfallen der Vorschrift. Art. 22 DSGVO erstreckt sich nur auf Entscheidungen, bloße Maßnahmen sind, zumindest ausdrücklich, nicht erfasst. Unklar ist insbesondere, ob bereits die Ausgabe eines autonomen Systems eine Entscheidung im Sinne des Art. 22 DSGVO darstellen kann.[225] Problematisch ist zudem, dass Entscheidungsunterstützungssysteme nicht reguliert sind.[226] Für die verhaltensökonomisch bedingte Vorwegbindung des menschlichen Entscheiders (Automation Bias) durch ein Entscheidungsunterstützungssystem bietet Art. 22 DSGVO keine Lösung.[227] Die Vorschrift ist schließlich nochmals beschränkt, da nur ausschließlich automatisierte Entscheidungen mit rechtlichen Folgen bzw. mit erheblichen faktischen Beein-

---

[224] Dies wird in der Literatur überwiegend gefordert siehe nur *Härting*, CR 4 (2014), 528, 531 f.; *Kugelmann*, DuD 40 (2016), 566, 570; *Lorentz*, Profiling, 2019, S. 334–342; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 10–11; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 26. Eine eigenständige Regulierung fordert auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 100. Eine Regulierung des Profilings ist in der ePrivacy-Richtlinie bzw. in der geplanten ePrivacy-Verordnung vorgesehen. Diese reguliert jedoch allein die dem Profiling vorgelagerte Ebene der Datensammlung in Form des Web-Trackings und dies (zumindest bislang) beschränkt auf solches in Endgeräten. Schutzlücken bestehen damit fort. Siehe ausführlich hierzu *Lorentz*, Profiling, 2019, S. 284–288; *Schleipfer*, ZD 7 (2017), 460, 463–466. Zumindest zum Kredit-Scoring ist in § 31 BDSG eine spezifische Vorschrift vorgesehen, diese erfasst aber nur einen ganz bestimmten Anwendungsbereich. Überdies wird diese Vorschrift gemeinhin als unionsrechtswidrig bewertet, vgl. nur *Moos/Rothkegel*, ZD 6 (2016), 567 f.; *Martini*, Blackbox Algorithmus, 2019, S. 175 f.; *Lorentz*, Profiling, 2019, S. 321–323 sowie aus der Kommentarliteratur *Buchner*, in: Tinnefeld/Buchner/Petri u.a. (Hrsg.), Einführung in das Datenschutzrecht, ^{6}2018, S. 220, Rn. 150, 153; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 88–89.

[225] Die hieraus entstehenden Rechtsunsicherheiten kritisieren *Finck*, Int. Data Priv. Law 9 (2019), 78, 83; *Edwards/Veale*, SSRN Journal 2017, 46.

[226] Dies wird in der Literatur vielfach kritisiert, siehe nur *Lorentz*, Profiling, 2019, S. 275; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 251 f.; *Martini*, JZ 72 (2017), 1017, 1020; *Martini*, Blackbox Algorithmus, 2019, S. 172 f.; *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 19.

[227] Defizite im Datenschutzrecht diesbezüglich erkennen auch *Edwards/Veale*, SSRN Journal 2017, 45; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 162; *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 133 f.; *Wagner*, Policy & Internet 11 (2019), 104, 114 f. Siehe auch *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 253.

trächtigungswirkungen reguliert werden.[228] Im Übrigen bestehen hier erhebliche Rechtsunsicherheiten. So ist nicht klar, ob diese rechtlichen oder tatsächlichen Folgen nachteilig sein müssen. Sofern man dies verlangt, ist weiterhin nicht eindeutig, wann eine solche Folge im Einzelfall als nachteilig bewertet werden kann.[229]

V. Ergebnis

Die DSGVO stellt für autonome Systeme einen Regulierungsrahmen zur Verfügung, soweit in den einzelnen Verarbeitungsstadien personenbezogene Daten verarbeitet werden. Dieser Regulierungsrahmen gilt dabei im Verhältnis zwischen betroffener Person und Verantwortlichem, er bezieht sich allein auf das einzelne Datum und seine Verarbeitung. Die DSGVO differenziert dabei nach den Risiken für die betroffene Person: Das Trainingsverfahren für die Modellbildung wird allein mittels der allgemeinen Datenschutzbestimmungen reguliert, spezifische Mechanismen im Hinblick auf das Maschinelle Lernverfahren sind nicht vorgesehen, ebenso wenig direkte Regulierungszugriffe auf das Modell. Dies gilt dann auch für den Lösungsalgorithmus, sofern dieser anhand personenbezogener Trainingsdaten gebildet wird. Die Profilbildung ist zwar als Profiling im Sinne des Art. 4 Nr. 4 DSGVO anerkannt, diese erfährt aber in der DSGVO keine eigenständige Regulierung. Die Profilverwendung unterfällt dem spezifischen Regulierungsregime des Art. 22 DSGVO, allerdings nur, soweit eine automatisierte Entscheidung in der engen Definition dieser Vorschrift vorliegt. Da der überwiegende Teil autonomer Systeme keine solche automatisierten Entscheidungen darstellen, wirken auf Stufe der Profilverwendung allein die allgemeinen Datenschutzinstrumente. Die DSGVO bietet regulative Zugriffe auf autonome Systeme in ihrer Gesamtheit und unabhängig vom Verarbeitungsverfahren und Zweck. Sie erlaubt zudem risikobezogene Differenzierungen. Mit Art. 22 DSGVO bietet sie zudem eine Regelung für eine besonders risikoreiche Verwendung von Datenverarbeitungsergebnissen. Zu kritisieren ist dagegen das Fehlen eigener profilingspezifischer Vorschriften und die äußerst enge Fassung des Art. 22 DSGVO. Modell bzw. Lösungsalgorithmus sowie Maschinelle Lernverfahren werden in der DSGVO nicht spezifisch reguliert. Dies ist problematisch: Autonomiegefährdungen und Diskriminierungen sind wesentlich im Modell bzw. Lösungsalgorithmus ange-

---

[228] Kritisch hierzu äußern sich auch *Lorentz*, Profiling, 2019, S. 275 f.; *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 19 f. In diese Richtung *Martini/Nink*, NVwZ 36 (2017), 1, 3. Zumindest rechtliche Unklarheiten kritisieren *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 134, 140 f.; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 279 f.

[229] Zu diesen Kritikpunkten siehe auch *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 19 f.

legt, sie begründen zudem datenschutzspezifische Regulierungsbedarfe, da Modell und Lösungsalgorithmus die Regulierungsmechanismen der DSGVO auf Stufe der Profilbildung und -verwendung behindern. Dies soll im Weiteren noch für den Rechtmäßigkeits- und Transparenzgrundsatz dargelegt werden. Der Regulierungszugriff der DSGVO auf autonome Systeme stellt sich im Ergebnis als umfassend dar, geht aber an den wesentlichen Regulierungsfragen – Maschinelles Lernverfahren und Profiling – vorbei.

C. Regulierung autonomer Systeme durch den Zweckfestlegungs- und Rechtmäßigkeitgrundsatz

Die menschliche Aufsicht bzw. Kontrolle prägt die Diskussion um die Regulierung autonomer Systeme. Es lohnt daher, das Verständnis von menschlicher Aufsicht hinsichtlich autonomer Systeme dem der DSGVO hinsichtlich Datenverarbeitungen und -verwendungen gegenüberzustellen. Dabei ist auch auf die Regulierungsprämissen, -ziele und -funktionen des Rechtmäßigkeits- und des Zweckfestlegungsgrundsatzes einzugehen (I.). Nach einer Darstellung des geltenden Rechtsrahmens (II.) erfolgt eine Analyse hinsichtlich der Datenverarbeitungen durch autonome Systeme (III.), die abschließend eine kritische Bewertung im Hinblick auf ihre Leistungskraft zur Eindämmung auf Autonomiegefährdungen und Diskriminierungen erlaubt (IV.).

I. Menschliche Aufsicht und Kontrolle als Regulierungsziele autonomer Systeme

Bei der Regulierung autonomer Systeme wird die menschliche Kontrolle bzw. Aufsicht zum tragenden Prinzip erklärt (1.). Das dortige Verständnis von Kontrolle grenzt sich jedoch vom datenschutzrechtlichen Kontrollkonzept ab (2.).

1. Allgemeine Konzepte menschlicher Aufsicht über autonome Systeme: Allgemeiner regulativer Steuerungsanspruch

Regulierung soll menschliche Kontrolle bzw. Aufsicht über autonome Systeme absichern; was damit konkret gemeint ist, bleibt aber überwiegend unklar.[1] So-

[1] Vgl. nur den Beitrag von *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, in dem der Begriff der Kontrolle vielfach fällt und sich auf ganz unterschiedliche Aspekte bezieht. Siehe auch *Hochrangige Expertengruppe für künstliche Intelligenz,* Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 19 f., die einen „Vorrang menschlichen Handelns“ und eine „menschliche Aufsicht“ fordert, dabei aber nicht deutlich macht, was dies konkret bedeutet. Vielfach geht es allein um eine allgemein-abstrakte Absicherung des Primats des Menschen gegenüber autonomen Systemen. Vgl. *Bau-*

weit spezifische Konzepte entwickelt werden, wird erkenntlich: Es geht ganz grundsätzlich bzw. allgemein um Regulierung bzw. Regulierbarkeit.[2] Die menschliche Kontrolle ist dann Gegenmodell zu einer deterministisch verstandenen Technik, die sich jenseits individueller oder gesellschaftlich konsentierter Gemeinwohlvorstellungen entwickelt.[3] Im Ergebnis meint dann menschliche Aufsicht und Kontrolle – zumindest im Bereich des Rechts – nichts anderes als die rechtliche Einfassung autonomer Systeme.

2. Konzepte menschlicher Aufsicht der DSGVO und Regulierungsparadigmen des Zweckfestlegungs- und Rechtmäßigkeitsgrundsatzes

Die DSGVO formuliert diesen Anspruch menschlicher Kontrolle bzw. Aufsicht spezifisch für die Technik der Datenverarbeitung (a)). Innerhalb der DSGVO bezieht sich Kontrolle auf ein konkretes Regulierungsinstrument, nämlich den Rechtmäßigkeitsgrundsatz, ergänzt und verstärkt um den Zweckfestlegungsgrundsatz (b)).

a) Datenschutzrechtliches Konzept menschlicher Aufsicht und Kontrolle: präventive Steuerung statt individueller Kontrolle

Der DSGVO liegt, wie beschrieben, die Vorstellung zugrunde, dass die Unkontrolliertheit und Unkontrollierbarkeit der Datenverarbeitungsvorgänge an

---

berger/Beck/Burchardt u.a., in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 907, 929 f.; *Scherer*, Harv. J. Law Technol. 29 (2016), 353, 366–369.

[2] So etwa zum Regulierungsentwurf für algorithmische Systeme *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 25, 177. Vgl. auch das Regulierungsregime für Algorithmen nach *Martini*, Blackbox Algorithmus, 2019, S. 157–332, in dem mehrfach der Begriff der Kontrolle fällt.

[3] Kontrolle meint dann vor allem die Unterbindung von Schäden und sonstigen unerwünschten Entwicklungen der Technik. So fordert etwa die *Hochrangige Expertengruppe für künstliche Intelligenz,* Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 12 f. die Wahrung des unional konsentierten Gemeinwohlbestands durch Systeme Künstlicher Intelligenz. Da die Systeme Künstlicher Intelligenz algorithmenbasiert sind, werden Fragen der Kontrolle von Systemen Künstlicher Intelligenz vielfach auch unter dem Begriff der Algorithmenkontrolle diskutiert. Siehe zu Forderungen der Wahrung des Gemeinwohlbestands durch Algorithmen etwa *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 163. Dies beinhaltet auch die Verteilung von Schadensverantwortung, siehe zu diesem Verständnis *Bauberger/Beck/Burchardt u.a.*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 907, 916–919; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 24.

sich gemeinwohlschädliche Potentiale in sich tragen.[4] Nach der Vorstellung des Unionsgesetzgebers kann den datenverarbeitungsspezifischen Gefährdungen am effektivsten dadurch begegnet werden, indem eine jede Datenverarbeitung eine Regulierung erfährt.[5] Der allgemeine Kontrollanspruch hinsichtlich der Digitaltechnik konkretisiert sich in der DSGVO zu einem Kontrollanspruch hinsichtlich des Einzeldatums und seiner Verarbeitung.[6] Die DSGVO insgesamt, d.h. die rechtliche Datenstrukturierung[7] ist damit Ausdruck dieses Aufsichts- und Kontrollkonzepts.

Ist im datenschutzrechtlichen Zusammenhang von Kontrolle die Rede, bezieht sich dies regelmäßig auf den Rechtmäßigkeitsgrundsatz nach Art. 5 Abs. 1 lit. a), Art. 6 DSGVO, ergänzt um den Zweckfestlegungsgrundsatz. Rechtmäßigkeits- und Zweckfestlegungsgrundsatz etablieren einen präventiven Regulierungsmechanismus. Menschliche Kontrolle meint in der DSGVO demnach ganz spezifisch: präventive Kontrolle. Von besonderer Bedeutung ist im Verhältnis zwischen Privaten der Zulassungsgrund der Einwilligung als wesentliches Instrument eines dezentralen Regulierungsregimes.[8] Die DSGVO verschafft dem Einzelnen aber keine individuelle Datenkontrolle.[9] Damit lässt sich noch weiter präzisieren: Kontrolle meint eine ange-

---

[4] Kapitel 4 A. I. 1. b). Siehe auch *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 68 f.; *Hahn*, EDPL 7 (2021), 31, 33; *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 91.

[5] Siehe oben Kapitel 4 A. I. 2. a) sowie Kapitel 4 B. I. 2.

[6] Eigentlicher Kontrollgegenstand ist gleichwohl nicht das Datum, sondern die darin verkörperte Information, d.h. die semantische Sinnaufladung des Datums. In dieser Information und hierauf gestützten nachteiligen Entscheidungen liegt das eigentliche Risiko der Datenverarbeitung, vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 42. Rechtstechnisch gewährleistet die DSGVO allein die Kontrolle der Daten, nicht der Information, siehe etwa *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 212–215. Diese Unterscheidung ist wichtig, da es eine Kontrolle über Informationen, d.h. Sinnzuschreibungen schon tatsächlich nicht geben kann, im Übrigen ein solcher Regelungsansatz sich in Widerspruch zu einer auf Sozialität des Einzelnen und kommunikativer Gemeinschaftlichkeit beruhenden Rechtsordnung stellte. Zur Definition und Unterscheidung von Information und Datum und der jeweiligen Kontrollansprüche (und der Sinnhaftigkeit dieser Kontrollansprüche) eingehend *Albers*, Informationelle Selbstbestimmung, 2005, S. 87–97, 109–113; *Poullet/Rouvroy*, in: Hert/Gutwirth/Poullet (Hrsg.), Reinventing Data Protection?, 2009, S. 45, 51; *Bäcker*, Der Staat 51 (2012), 91, 92; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 207–215; *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 9–14.

[7] Siehe hierzu Kapitel 4 A. I. 2. a).

[8] Siehe hierzu eingehend bereits oben Kapitel 4 A. II. 3. a).

[9] Siehe eingehend Kapitel 4 A. I. 2. a) sowie Kapitel 4 A. II. 3. b). Missverständlich heißt es dagegen in Erwägungsgrund 7 S. 2: „Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen“. So auch die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 14: „User control is only possible when the purpose of data processing is sufficiently clear and predictable“.

messene individuelle Mitbestimmungsmöglichkeit der betroffenen Person an der Verarbeitung der sie betreffenden Daten.

b) Regulierungsparadigmen des Zweckfestlegungs- und des Rechtmäßigkeitsgrundsatzes

Zweckfestlegungs- und Rechtmäßigkeitsgrundsatz erlauben Datenstrukturierung im Vorfeld (aa)). Der Zweckfestlegungsgrundsatz setzt hierfür den Prüfungsrahmen und sichert das Zulässigkeitsattestat über die Zeit ab (bb)). Der Rechtmäßigkeitsgrundsatz etabliert einen präventiven Kontrollmechanismus, innerhalb dessen dem Zulassungstatbestand der Einwilligung eine herausragende Rolle zukommt (cc)).

aa) Präventives Regulierungsregime

Der präventive Regulierungsmechanismus der DSGVO ist auf die Eigenart der Regulierungsmaterie zurückzuführen: Informationen können sinnvollerweise nur gesteuert werden, bevor sie in die Umwelt gelangen.[10] Hinzu kommt: Den faktischen ersten Zugriff auf Daten hat regelmäßig die verarbeitende Stelle.[11] Die Zulässigkeitsbedingung, insbesondere die der Einwilligung, sichert ab, dass nicht der Verantwortliche einseitig die Datenverarbeitungsbedingungen festlegt.[12] Weitere Wurzeln des präventiven Regulierungsansatzes liegen im Vorsorge- und Risikorecht:[13] Ist potentiell eine jede Datenverarbeitung auto-

---

[10] Vgl. *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 78; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Art. 1 Rn. 4. Vgl., wenngleich allein zur Einwilligung, *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 203; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 69 f.

[11] Betroffene Personen verfügen selten über die technische Ausstattung und Fähigkeiten, um Datenverarbeitungen unterbinden oder nachträglich Daten dauerhaft löschen zu können. So *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 203. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 37.

[12] Plakativ *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 203: Ohne eine derartige Zuordnung käme es zu „faktischen Zuordnungen von ‚Rechten' an diesen Informationen – im Zweifel zugunsten desjenigen, der mehr Macht, mehr Wissen und weniger Skrupel hat". So auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 69 f.; *Lynskey*, ICLQ 63 (2014), 569, 592 f.; *Buchner*, DuD 40 (2016), 155, 158. Eingehend, insbesondere durch Gegenüberstellung eines weitaus ineffektive(ren) nachträglichen Kontrollzugriffs der betroffenen Person, *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 75. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 37.

[13] Die Ungewissheit über Eintritt und Wirkungszusammenhänge datenverarbeitungsspezifischer Risiken sowie die potentielle Irreparabilität etwaiger Schäden verweisen auf das aus dem Risikorecht bekannte Vorsorgeprinzip, das auf die Schadensvermeidung durch frühzeitige Unterbindung der Risikoursachen abzielt. Diese Erwägungen gelten vor allem im Hinblick auf die beschriebenen Autonomiegefährdungen: Ob und aufgrund welcher spezifi-

nomiegefährdend, vor allem aber die unkontrollierte Datenverarbeitungsarchitektur an sich, so kann eine effektive Eindämmung nur in einer möglichst frühzeitigen, d.h. einer vorsorgenden Datenstrukturierung liegen.[14] Der Rechtmäßigkeitsgrundsatz zielt nicht auf Unterbindung der Datenverarbeitung, sondern auf Zulassung, wenngleich auf eine strukturierende, d.h. bestimmte Anforderungen einhaltende Zulassung ab.[15]

bb) Zweckfestlegungsgrundsatz: instrumentelle und funktionale Regulierungseffekte

Der Zweckfestlegungsgrundsatz unterteilt sich in die Grundsätze der Zweckbestimmung ((1)) und der Zweckbindung ((2)). Sie haben jeweils instrumentellen Charakter, stärken und ermöglichen also den Rechtmäßigkeitsgrundsatz sowie weitere Datenschutzgrundsätze,[16] als auch funktionalen Charakter, entwickeln Steuerungskräfte also aus sich heraus. Der Zweckfestlegungsgrundsatz gilt damit als grundlegendes Steuerungsinstrument der DSGVO.[17]

---

schen Umstände diese eintreten, ist unklar, ein nachträglicher Schutz ist kaum denkbar. Siehe hierzu *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 78–80. Vgl. auch *Bäcker*, Der Staat 51 (2012), 91, 96; *Grimm*, JZ 68 (2017), 585, 586. Siehe allgemein zur Einordnung der DSGVO als Risikoregulierungsinstrument *Gellert*, EDPL 2 (2016), 481.

[14] Hemmeffekte und Manipulationen werden maßgeblich durch die Unkontrolliertheit und Intransparenz der Datenverarbeitung ausgelöst, siehe hierzu Kapitel 4 A. I. 1. a), Kapitel 4 A. II. 2. a). Um diese effektiv zu unterbinden, bedarf es einer Regulierung von Datenverarbeitungen, noch bevor es überhaupt zu derartigen Einwirkungen auf die innere Autonomie kommt. Der Datenschutz greift also nicht erst bei Vorliegen einer – im rechtlichen Sinne – Gefahr für die menschliche Autonomie, sondern bereits auf der Vorstufe, d.h. bei einem bloßen Risiko für die menschliche Autonomie. Von einer „Vorfeldschutz-Kaskade" spricht daher *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 82 f. Siehe hierzu auch *Bäcker*, Der Staat 51 (2012), 91, 96; *Grimm*, JZ 68 (2017), 585, 586. Sehr kritisch zu diesem Schutzkonzept *Veil*, NVwZ 37 (2018), 686, 690 „Risikovorsorge".

[15] So auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 154, 157; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 3–4; Sydow, DS-GVO/*Sydow*, Einleitung Rn. 71. Nach der Konzeption von *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61 ist der Rechtmäßigkeitsgrundsatz ein „transparency tool", d.h. ein strukturierendes Zulassungsinstrumente, kein „opacity tool", d.h. Verbotsinstrument, so auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 154.

[16] So auch die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 4, 11: „Purpose specification is [...] a prerequisite for applying other data quality requirements". Ebenso Kuner/Bygrave/Docksey, GDPR/*Terwangne*, Art. 5 Rn. 315 „prerequisite for most other fundamental requirements".

[17] Paal/Pauly, DS-GVO/*Frenzel*, Art. 5 Rn. 23 „Dreh- und Angelpunkt"; Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 13 „Konstitutionsprinzip", „Fixpunkt"; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 64 „zentrale[s] Steuerungsinstrument im Datenschutzrecht".

(1) Konnektivierung und Vorstrukturierung durch die Zweckbestimmung

Die Zweckbestimmung verpflichtet zur Prädiktion der Zwecke, d.h. der Motive der Datenverarbeitung vor Stattfinden der Datenverarbeitung[18] und macht so die realen Auswirkungen und Folgen der Datenverarbeitung vorhersehbar.[19] Der konnektivistische Regulierungsansatz der DSGVO, dass nämlich durch die Regulierung des Datums die mit dessen Verarbeitung verbundenen Gefährdungen unterbunden werden können,[20] wird durch den Zweckbestimmungsgrundsatz abgesichert. Die Zweckbestimmung bildet dann die Grundlage für die Zulassungsprüfung im Rahmen der Rechtmäßigkeit.[21] Darüber hinaus entfaltet der Zweckbestimmungsgrundsatz aus sich heraus steuernde Wirkung, indem er die späteren Datenverarbeitungsprozesse vorstrukturiert. Diese müssen sich in die qualitativen und quantitativen Rahmenbedingungen des präskribierten Motivs fügen.[22] Auf diese Weise verhindert er Datensammlungen auf Vorrat oder ins Blaue hinein.[23] Schließlich hat der Zweckbestimmungsgrundsatz auch transparenzherstellende Funktion, indem er Realfolgen der Datenverarbeitungen vorhersehbar macht. Auf diese Weise trägt er zur Eindämmung von Autonomiegefährdungen bei.[24]

---

[18] Paal/Pauly, DS-GVO/*Frenzel*, Art. 5 Rn. 23 „Ziel, Grund und Wesen der Verarbeitung".

[19] Deutlich auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 64: „Durch die Zweckbindung werden informationsbedingt nachteilige Entscheidungen berechenbar gemacht". Siehe auch *Niemann/Kevekordes*, CR 36 (2020), 17, 21.

[20] Siehe hierzu oben Kapitel 4 B. I. 1. Siehe auch Kapitel 4 A. I. 1. und 2.

[21] Siehe zum Zusammenhang von Zweckbestimmungsgrundsatz und Rechtmäßigkeitsprinzip nur Erwägungsgrund 32 S. 1, 4 und 5, der diese Verbindung für die Einwilligung explizit beschreibt. Vgl. auch *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 15: „The purpose of the collection must be [...] detailed enough [...] to allow that compliance with the law can be assessed and data protection safeguards applied". Vgl. auch Wolff/Brink, BeckOK DatenschutzR/*Schantz*, Art. 5 Rn. 15 sowie *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61, 79 f.

[22] Zum eigenen Ziel der Strukturierung der Datenverarbeitungen siehe *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 159 f. Vgl. auch *Lynskey*, ICLQ 63 (2014), 569, 594. Ähnlich spricht die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 11 davon, dass der Zweckbestimmungsgrundsatz darauf abziele „to protect the data subject by setting limits on how controllers are able to use their data". Siehe auch *Finck/Biega*, Technology and Regulation 2021, 44, 55.

[23] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 72; *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 85.

[24] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 42: „Psychische Hemmungen werden damit in erster Linie aus Verstößen gegen das Zweckbindungsgebot hergeleitet". Siehe zum Steuerungsziel der Erwartbarkeit ausführlich, *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 4; explizit für Big-Data-Analysen, *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 22 f.

(2) Perpetuierung durch die Zweckbindung

Der Grundsatz der Zweckbindung sichert die Rechtmäßigkeit über die Zeit ab und aktualisiert die im Vorfeld festgelegten und durch die Rechtmäßigkeitsprüfung freigegebenen Verarbeitungszwecke während des gesamten Verarbeitungs- und Lebenszyklus eines Datums.[25] Dabei prägt die DSGVO ein gelockertes Verständnis von Zweckbindung:[26] Nicht jede Weiterverarbeitung liegt jenseits des Rahmens, den die Zweckbestimmung setzt, sondern nur eine solche, die mit dem ursprünglichen Zweck unvereinbar ist.[27] So wird ein Kompromiss geschaffen zwischen schützender Datenstrukturierung und Flexibilitätsbedarfen der Praxis hinsichtlich der Verarbeitungszwecke.[28]

cc) Rechtmäßigkeitsgrundsatz: prädiktiv-konnektionistische Steuerungseffekte und dezentrale Datenordnung

Der Rechtmäßigkeitsgrundsatz etabliert ein präventives Zulassungsregime mit dem Anspruch holistischer Steuerung ((1)). Dieser Ansatz lässt sich auch auf die Ausnahmezulassung automatisierter Entscheidungen übertragen ((2)). Im Verhältnis zwischen Privaten ist der Zulassungstatbestand der Einwilligung von besonderer Wichtigkeit, wird aber ergänzt (und potentiell verdrängt) durch weitere Zulassungsgründe ((3)).

---

[25] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 4: „[T]he principle of purpose limitation inhibits ‚mission creep'" und weiter *dies.*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 11: „[it] should [...] prevent the use of individuals' personal data in a way [...] that they might find unexpected, inappropriate or otherwise objectionalble". Vgl. auch *Norwegian Data Protection Authority*, Big Data, September 2013, S. 41. Siehe überdies Wolff/Brink, BeckOK DatenschutzR/*Albers/Veit*, Art. 6 Rn. 101: „Überspitzt formuliert bedeutet Zweckbindung ‚Zukunftsbindung'". *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 160 spricht von einer „phasenübergreifende[n] Wirkung".

[26] Dies steht im Gegensatz zum strikten deutschen Verständnis, wonach jede Zweckänderung, auch soweit eine Zweckkompatibilität vorliegt, unzulässig ist. Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 33–34; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 162.

[27] Siehe hierzu eingehend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 97. Auch dann sieht die DSGVO in Art. 6 Abs. 4 HS. 2 DSGVO Ausnahmen vor, hierzu sogleich. Siehe hierzu eingehend unten Kapitel 4 B. II. 1. b).

[28] Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 101.

(1) Konnektivistisches, partikularistisches und individualistisches Regulierungsregime

Der Rechtsmäßigkeitsgrundsatz macht eine jede Datenverarbeitung von der Existenz eines Zulassungsgrundes abhängig.[29] Auf diese Weise wird abgesichert, dass vorab die inhaltlichen Angemessenheitsbedingungen für eine jede Datenverarbeitung festgelegt werden und die jeweilige Datenverarbeitung diese auch tatsächlich einhält[30] – und dies während des gesamten (vom Zweck beschriebenen) Verarbeitungs- und Lebenszyklus des Datums.[31] Der Rechtmäßigkeitsgrundsatz gründet dabei wesentlich auf der Prämisse der Vorhersehbarkeit: Schon im Zeitpunkt der Freigabe eines Datums müssen der gesamte Verarbeitungsvorgang und etwaige Realfolgen erkennbar sein.[32] Der Rechtmäßigkeitsgrundsatz unterstellt damit direkte, antizipierbare Verbindungen zwischen dem Einzeldatum, der Einzelverarbeitung und den Folgen der Verarbei-

---

[29] Nach einem anderen Verständnis drückt der Rechtmäßigkeitsgrundsatzes das Gebot der Konformität der Datenverarbeitung mit der gesamten DSGVO aus, so etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 33; Sydow, DS-GVO/*Reimer*, Art. 5 Rn. 1, 13; Paal/Pauly, DS-GVO/*Frenzel*, Art. 5 Rn. 14–17; Kuner/Bygrave/Docksey, GDPR/*Terwangne*, Art. 5 Rn. 314; zumindest für „elementare" Datenschutzregelungen Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Schwartmann/Hermann*, Art. 5 Rn. 21. Dagegen spricht aber, dass die Vorschrift dann redundant wäre. Überdies verkennt diese Ansicht die rechtstechnische Notwendigkeit der Formulierung eines Zulassungs- (nicht eines Rechtmäßigkeits-)bedarfs, da – so im Verhältnis zwischen Privaten – jede Datenverarbeitung Ausdruck der Freiheitsrechte der verarbeitenden Stelle ist, die ohne besonderen Grund zulässig ist, hierauf weisen hin Gola, DS-GVO/*Schulz*, Art. 6 Rn. 2–4; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Albrecht*, Art. 6 Rn. 1 Fn. 1; *Karg*, DuD 37 (2013), 75, 78 f.; *Eckhardt/Kramer*, DuD 37 (2013), 287, 289 f. Dieses Verständnis prägt auch die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 19 f. Zur grundrechtlichen Dimension siehe eingehend *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 265–269, der in Art. 8 GRCh eine „eingriffsrechtfertigende Strukturermächtigung" erkennt, die zu einem Eingriff in die Datenverarbeitungsfreiheit der verarbeitenden Stellen ermächtigt, deren Ausgestaltung dann ins Ermessen des Gesetzgebers stellt ist.

[30] So auch Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 2: „Art. 6 [stellt] die grundlegenden Weichen". Ebenso *Buchner*, DuD 40 (2016), 155, 158. Siehe auch *Karg*, DuD 37 (2013), 75, 77 f., der von einem „Firewall-Effekt" spricht. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 32. Siehe auch, wenngleich allein zur Einwilligung, *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 69 f.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 203.

[31] Vgl., wenngleich allein für die Einwilligung, *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 72.

[32] So auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Simitis/Hornung/Spiecker gen. Döhmann*, Einleitung 36, 38. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 64.

tung für die Lebenswirklichkeit der konkret betroffenen Person.[33] Auch im Rechtsmäßigkeitsgrundsatz findet sich damit das bereits im Personenbezug dargelegte konnektivistische,[34] atomistische,[35] partikularistische[36] und individualistische[37] Regulierungsregime wieder.

(2) Sonderfall: Ausnahmezulassung automatisierter Entscheidungen

Demgegenüber ist Art. 22 DSGVO als echtes Verbot (Abs. 1) ausgestaltet, für das Ausnahmen formuliert sind (Abs. 2).[38] Die Inakzeptabilität einer derartigen Verwendung von Datenverarbeitungsergebnissen wird hier zentralisiert durch den Staat festgestellt.[39] Die Achtung vor der Autonomie des Einzelnen verlangt aber, dass die betroffene Person sich auch gegen diesen staatlichen Schutz entscheiden kann.[40] Die ausgeführten Erwägungen zum Rechtmäßigkeitsgrundsatz lassen sich übertragen:[41] Auch hier geht es um individuelle Angemessenheitsbedingungen – wenngleich dann der automatisierten Entscheidung, nicht der Datenverarbeitung[42] –, die im Vorfeld des Stattfindens einer automatisierten Entscheidung definiert sein müssen und deren Einhaltung durch die Ausnahmezulassung präventiv, dann aber mit holistischem Anspruch festgestellt wird. Der Zweckfestlegungsgrundsatz gilt hier nicht, da dieser sich nur auf Datenverarbeitungen bezieht. Die Vorhersehbarkeit möglicher nachteiliger Folgen wird daher allein über die Anforderungen der Informiertheit der Einwilligung, im Übrigen über die Transparenz abgesichert.[43]

---

[33] Siehe hierzu Wolff/Brink, BeckOK Datenschutzrecht/*Schild*, Art. 4 Rn. 28, vgl. überdies Gola, DS-GVO/*Gola*, Art. 4 Rn. 11. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 161.

[34] Siehe oben Kapitel 4 B. I. 1.

[35] Siehe oben Kapitel 4 B. I. 2.

[36] Siehe oben Kapitel 4 B. I. 2.

[37] Siehe oben Kapitel 4 B. I. 3.

[38] Eingehend unten Kapitel 4 B. II. 5.

[39] Siehe explizit, wenngleich noch zur Vorgängervorschrift des Art. 15 DSGRL, *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 290. Es handelt sich nach deren Konzeption des Datenschutzrechts also um ein „opacity tool". Siehe zur Konzeption von „opacity" vs. „transparency tools" eingehend unter Kapitel 4 A. 2. a). Das Europäische Parlament hatte ein Widerspruchsrecht vorgeschlagen; dies konnte sich aber nicht durchsetzen, siehe eingehend Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 9. Vgl. auch Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 1, 8.

[40] Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 38.

[41] Insbesondere zur Übertragbarkeit der Bedingungen der Einwilligung Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 41–42; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 38. Siehe auch sogleich unter Kapitel 4 C. II. 5.

[42] Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 41.

[43] Vgl. Gola, DS-GVO/*Schulz*, Art. 22 Rn. 31; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 38. Zu den Transparenzanforderungen automatisierter Entscheidungen nach Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO siehe eingehend unter Kapitel 4 D. II. 3.

(3) Dezentrales Zulassungsregime mit zentralisierten Ergänzungen

Im dezentralen Regulierungskonzept zwischen Privaten stützt sich das Zulassungsregime der DSGVO maßgeblich auf die Willensentscheidung der betroffenen Person. Die Zulassung erfolgt dann über die Einwilligung, im vertraglichen Verhältnis vorrangig über die Vereinbarung der Parteien.[44] Vertragsimmanente Zulassung und Interessensabwägung sichern ab, dass die Entscheidung nicht allein der betroffenen Person überlassen bleibt und auch der Verantwortliche seine Interessen einbringen kann.[45]

Im Verhältnis zwischen Privaten werden so die Angemessenheitsbedingungen einer Datenverarbeitung vornehmlich durch die Parteien definiert,[46] über die Inhalte dieser Angemessenheitsbedingungen sagt der Rechtmäßigkeitsgrundsatz dann nichts aus. Allein bei der Zulassung durch Interessensabwägung werden staatlicherseits Angemessenheitsbedingungen aufgestellt. Allerdings gibt die DSGVO keine bestimmten Ergebnisse vor und formuliert auch keine Abwägungskriterien. Erst im Einzelfall und auch nur für diesen werden Angemessenheitskriterien entwickelt; verbindlich erfolgt dies über Aufsichtsbehörden oder Gerichte.[47] Vielfach wird der Rechtfertigungsgrund des

[44] Zum Vorrang des Art. 6 Abs. 1 lit. b) DSGVO siehe sogleich Kapitel 4 C. II. 6.

[45] Siehe hierzu bereits Kapitel 4 A. I. 3. a), Kapitel 4 A. II. 3. b).

[46] Bei der Einwilligung erfolgt dies allein durch die betroffene Person. Siehe ausführlich Kapitel 4 A II. 2. a). Vgl. auch eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 168; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 102, 205. Ebenso *van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 94: „In order to be in control, a data subject should be able to make decisions that are in line with her existing attitudes and preferences". Ähnlich *Grimm*, JZ 68 (2017), 585, 588: „Aufgabe des Staates ist es hier, Voraussetzungen für eine freie, in Kenntnis der Risiken getroffene Willensentscheidung zu schaffen und zu stärken". Bei der vertragsimmanenten Zulassung werden die Angemessenheitsbedingungen durch betroffene Person und Verantwortlichem festgelegt, vgl. Kapitel 4 A. II. 3. b). Vgl. auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 47, 49.

[47] Andernfalls müsste der Unionsgesetzgeber für sämtliche Datenverarbeitungskonstellationen hinreichend präzise und justiziable materielle Angemessenheitskriterien aufstellen. Zudem müsste es beständig fortentwickelt werden, sodass auch neuartige Konfliktlagen der Datenverarbeitung abgebildet werden könnten. In einer umfassend digitalisierten Lebenswelt wird dies kaum gelingen. Ein entsprechendes Regelwerk wäre zudem aus quantitativen Gründen praktisch nicht handhabbar. Vgl. zu diesen Erwägungen *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 200. Eingehend *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 96–99, 102. Teilweise wird schon bezweifelt, dass der Staat diese sämtlich in Erfahrung bringen kann. So spricht *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 202–204 von epistemischen Wissensdefiziten des Staates. Ebenso *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 68 („fehlende[s] Entscheidungswissen[.]" des Staates). Die Gefahr einer „Verrechtlichung des Alltäglichen" eines solchen Vorhabens sieht *Hoffmann-Riem*, AöR 123 (1998), 514, 528.

Art. 6 Abs. 1 lit. f) DSGVO im rechtsgeschäftlichen Verhältnis auch als nachrangig erachtet.[48] Hierauf ist zurückzukommen.[49]

3. Ergebnis: präventiv-dezentrales Datensteuerungssystem zur menschlichen Kontrolle von Digitalsystemen

Aus dem allgemeinen Anspruch, autonome Systeme einer menschlichen und gerade rechtlichen Steuerung zu unterwerfen, formt die DSGVO mit dem Rechtmäßigkeits- und Zweckfestlegungsgrundsatz ein konkretes, nämlich ein präventiv ansetzendes Steuerungssystem. Während über den Rechtmäßigkeitsgrundsatz vorab bestimmte Angemessenheitsbedingungen für die Datenverarbeitung durchgesetzt werden können, sichert der Zweckfestlegungsgrundsatz deren Geltung über die Zeit ab. Das präventive Datenkontrollsystem basiert wesentlich auf der Vorstellung, dass Daten und Folgen unmittelbar verknüpft sind und sich so sämtliche Gefährdungen einer Datenverarbeitung prognostizieren lassen. Im Verhältnis zwischen Privaten erfolgt die Zulassung vorwiegend, wenngleich nicht ausschließlich, durch die betroffene Person. Die DSGVO schafft aber kein individuelles Datenkontrollrecht, sondern gewährt nur Mitbestimmungsoptionen hinsichtlich der Datenverarbeitungen einer Person. Die präventive Regulierung ist von der Auffassung getragen, dass sämtliche Gefährdungen im einzelnen Datum und seiner Verarbeitung angelegt sind und diese sich allein auf die betroffene Person beziehen. Über die Zulassungsfrage der Einzelverarbeitung kann dann effektiv sämtlichen Gefährdungen begegnet werden. Ob diese Annahme auch im Hinblick auf autonome Systeme zutreffend ist, soll die nachfolgende Untersuchung klären.

II. Darstellung des geltenden Rechts

Im Folgenden sollen die Kernpunkte des Zweckfestlegungs- und des Rechtmäßigkeitsgrundsatzes dargestellt werden, auf die im Weiteren die Analyse autonomer Systeme gestützt ist. Zunächst sollen die wesentlichen Inhalte der Zweckbestimmung und -bindung (1.), sodann die grundlegenden Bedingungen der Zulassungsgründe der Einwilligung (2.), der vertragsgemäßen Zulassung (3.) sowie der Interessensabwägung (4.) vorgestellt werden. Auch Ausführungen zur Ausnahmezulassung der automatisierten Entscheidung sollen erfolgen (5.). Abschließend ist auf das Verhältnis der Zulassungsgründe zueinander einzugehen (6.).

---

[48] Vgl. eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 65–68. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 69; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 13. In diese Richtung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 11.

[49] Siehe unter Kapitel 4 C. II. 6.

1. Zweckfestlegungsgrundsatz

Der Zweckfestlegungsgrundsatz gliedert sich in die Prinzipien der Zweckbestimmung (a)) und der Zweckbindung (b)).

a) Zweckbestimmung

Nach Art. 5 Abs. 1 lit. b) DSGVO müssen die Daten zu einem festgelegten, eindeutigen und legitimen Zweck verarbeitet werden.[50] Der Zweck ist vom unmittelbaren technischen Zweck der Datenverarbeitung zu unterscheiden. Er beschreibt das übergeordnete Ziel der Verarbeitung.[51] Die erste Bedingung erfordert, dass der Zweck hinreichend bestimmt („festgelegt") ist. Das Maß der Bestimmtheit wird in der DSGVO nicht ausdrücklich definiert,[52] gefordert wird aber gemeinhin ein strenger Maßstab.[53] Der Art. 29 Datenschutzgruppe zufolge sollen abstrakte und pauschale Zweckfestsetzungen wie „Verbesserung der Erfahrungen der NutzerInnen", „Werbung" oder „IT-Sicherheit" nicht ausreichen.[54] Die zweite und dritte Bedingung sind für die vorliegende Untersuchung nicht von Relevanz.[55]

---

[50] In der englischen Fassung: „for specified, explicit and legitimate purpose", in der französischen Fassung: „pour des finalités déterminées, explicites et légitimes".

[51] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 68: „Beschreibung des Zustands, der durch das Mittel der Datenverarbeitung erreicht werden soll. […] Der Zweck beantwortet die Frage des ‚Wozu'". Paal/Pauly DS-GVO/*Frenzel*, Art. 5 Rn. 23: „Ziel, Grund und Wesen der Verarbeitung". Siehe auch die Beispiele der Zweckbestimmung, die die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 16 benennt, etwa Marketingzwecke, IT-Sicherheit oder zukünftige Forschung.

[52] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 35–36; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 76–89. Siehe ausführlich zur Legitimität Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 90–91; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 37.

[53] Siehe nur Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 15. Dieser ergibt sich auch aus einem Umkehrschluss zu Erwägungsgrund 33. Für den besonderen Fall der Verarbeitung zu Forschungszwecken ist eine breite Beschreibung ausreichend, dann muss im Normalfall eine enge Beschreibung gefordert sein. Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 23; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 25.

[54] *Artikel 29 Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.04.2018, S. 13 unter Bezugnahme auf *dies.*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 16. Weitere Beispiele unzureichender Zweckbestimmungen aus der Rechtspraxis benennen *Finck/Biega*, Technology and Regulation 2021, 44, 48. Zu weiteren Beispielen siehe Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 9; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 88; Ehmann/ Selmayr, DS-GVO/*Heberlein*, Art. 5 Rn. 14.

[55] Die Eindeutigkeit spielt auf die Verständlichkeit für die betroffene Person an. Erwägungen, wie sie sogleich im Rahmen des Transparenzgrundsatzes angestellt werden, lassen sich insoweit übertragen. Die Legitimität meint Rechtskonformität des benannten Zwecks.

b) Zweckbindung: Umgang mit Zweckänderungen

Bewegt sich eine Datenverarbeitung außerhalb dieser Zweckbestimmung, liegt eine Zweckänderung vor. Hier differenziert die DSGVO: Ist der Zweck der Weiterverarbeitung nur schlicht ein anderer als derjenige, zu dem die Daten ursprünglich erhoben wurden, ist dies zulässig (Zweckänderung im weiteren Sinne).[56] Nur wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck unvereinbar ist – dies definiert Art. 6 Abs. 4 DSGVO –, sieht Art. 5 Abs. 1 lit. b) HS. 1 DSGVO ein Verbot der Weiterverarbeitung vor (Zweckänderung im engeren Sinne).[57]

aa) Vorliegen einer Zweckänderung im weiteren und im engeren Sinne

Um zu bestimmen, ob eine Zweckänderung im weiteren Sinne vorliegt, sind die Zwecke der originären und der Weiterverarbeitung zu vergleichen. Je nachdem, wie eng oder weit der Primärzweck gefasst ist, liegt dann eine solche Zweckänderung vor.[58] Die verarbeitende Stelle kann eine Anwendung des Art. 5 Abs. 1 lit. b) HS. 1 DSGVO bzw. Art. 6 Abs. 4 DSGVO also dadurch verhindern, dass sie den Primärzweck möglichst breit definiert oder sämtliche denkbare Zwecke bereits im Zeitpunkt der Erhebung auflistet.[59] Grenzen ergeben sich aus den bereits dargelegten Anforderungen des Zweckbestimmungsgrundsatzes, der Zweck darf daher nicht zu vage definiert sein.

Für die Frage, ob der Zweck der Weiterverarbeitung mit dem der originären Datenverarbeitung unvereinbar ist, stellt Art. 6 Abs. 4 DSGVO einen einzel-

---

Vgl. hierzu Sydow, DS-GVO/*Reimer*, Art. 5 Rn. 22; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 37. Verwiesen ist auf das gesamte Unionsrecht und – soweit Öffnungsklauseln dies zulassen – das nationale Recht, siehe Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 91.

[56] Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 32.

[57] Auf diese Weise öffnet und flexibilisiert sie den Zweckbindungsgrundsatz. So ausdrücklich *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 21. Siehe auch Wolff/Brink, BeckOK DatenschutzR/*Schantz*, Art. 5 Rn. 18. Dies unterscheidet die unionale Konzeption des Zweckbindungsgrundsatzes von der deutschen, die deutlich strikter jede Zweckänderung untersagte, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 33–34.

[58] Siehe hierzu ausführlich Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 217–221. Solange die Zweckbestimmung den Anforderungen des Art. 5 Abs. 1 lit. b) DSGVO genügt, vor allem also der Zweck hinreichend bestimmt ist, ist die verarbeitende Stelle frei, wie eng oder weit sie den konkreten Verarbeitungszweck fasst.

[59] Gola, DS-GVO/*Schulz*, Art. 6 Rn. 150. Vgl. auch *Finck/Biega*, Technology and Regulation 2021, 44, 48 f.

fallbezogenen Kompatibilitätstest auf.[60] Art. 6 Abs. 4 DSGVO benennt hierfür beispielhaft[61] fünf Kriterien.[62] Bei dem erstgenannten Kriterium[63] – die Verbindung zwischen den Zwecken – wird auf die inhaltliche Nähe von Primär- und Sekundärzweck abgestellt. Ist die Weiterverarbeitung ein „logischer nächster Schritt" der Erstverarbeitung, sind die Zwecke nicht unvereinbar.[64] Entscheidend ist die Sicht der betroffenen Person.[65] Das Merkmal des Verarbeitungskontextes[66] stellt maßgeblich auf das Verhältnis von betroffener Person und Verantwortlichem ab. Überraschende Weiterverarbeitungen führen demnach zu einer Unvereinbarkeit der Zwecke.[67] Ausschlaggebend sind die vernünftigen Erwartungen der betroffenen Person.[68] Bereits die Unvorhersehbarkeit der Weiterverarbeitung kann daher die Unvereinbarkeit der Zwecke be-

---

[60] Vgl. *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 21. Der Primärzweck ist damit der Bewertungsmaßstab, es findet keine allgemeine Interessensabwägung statt, vgl. Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 245; Paal/Pauly DS-GVO/*Frenzel*, Art. 5 Rn. 30. Siehe auch eingehend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 32–34.

[61] Die Liste ist nicht abschließend, siehe hierzu nur Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 49; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 35. Kritisiert werden vor allem die Vagheit und fehlende Präzision der Kriterien. Kritisch etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 35; Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 46; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 136.

[62] Im Ergebnis geht es um eine Abwägung der Interessen der betroffenen Person und der des Verantwortlichen. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 64; Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 169.

[63] Art. 6 Abs. 4 lit. a) DSGVO.

[64] So Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 36.

[65] So *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 23 f. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 36; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 187.

[66] Art. 6 Abs. 4 lit. b) DSGVO.

[67] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 24. So auch Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 248; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 188.

[68] Siehe Erwägungsgrund 50 S. 6. So auch bereits *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 24. Vgl. näher Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 43; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 237. Maßgeblich ist eine verobjektivierte Sicht, es wird also auf die Erwartungshaltung einer durchschnittlichen Person in der Situation des Betroffenen rekurriert. Vgl. eingehend Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 163–164.

gründen.[69] Durch entsprechende Hinweise seitens des Verantwortlichen kann aber die Kompatibilität herbeigeführt werden.[70] Die Art der verarbeiteten personenbezogenen Daten[71] spielt auf die Sensibilität der Daten an.[72] Das Kriterium der Folgen[73] bezieht sich auf sämtliche Konsequenzen der Weiterverarbeitung,[74] und zwar sowohl unmittelbare als auch mittelbare, wie sie etwa aus der Nutzung des Datenverarbeitungsergebnisses für Entscheidungen oder Maßnahmen entstehen.[75] Zum einen geht es um die Vorhersehbarkeit von Folgen: Sind diese für die betroffene Person nicht erkenntlich, ist in der Regel von einer Unvereinbarkeit der Zwecke auszugehen.[76] Auch hier kann sich die verarbeitende Stelle durch entsprechende Aufklärungen zu Beginn der Primärverarbeitung absichern.[77] Kann die verarbeitende Stelle die Folgen der Weiterverarbeitung selbst nicht absehen, führt dies daher typischerweise zur Unvereinbarkeit der Zwecke.[78] Zum anderen geht es um die Art der Folgen. Weist die Weiterverarbeitung gegenüber der ursprünglichen Verarbeitung ein höheres Risiko auf, steht dies einer Zweckvereinbarkeit regelmäßig entgegen.[79] Können Ge-

---

[69] Art. 13 Abs. 3 DSGVO verpflichtet zusätzlich ausdrücklich zur Information über Zweckänderungen. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 248. Vgl. auch Gola, DS-GVO/*Schulz*, Art. 6 Rn. 133.

[70] Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 163. Vgl. auch Gola, DS-GVO/*Schulz*, Art. 6 Rn. 145, 150.

[71] Art. 6 Abs. 4 lit. c) DSGVO.

[72] Vgl. etwa Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 Rn. 250.

[73] Art. 6 Abs. 4 lit. d) DSGVO.

[74] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 25. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 56; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 190.

[75] Vgl. *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 25. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 56; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 251.

[76] Je weniger die betroffene Person Chancen und Risiken der Weiterverarbeitung erkennen kann, desto eher liegt eine Unvereinbarkeit der Zwecke vor. Siehe Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 56, 59; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 190.

[77] Vgl. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 255.

[78] Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 252; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 56; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 140.

[79] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 25 f., die dieses Kriterium sehr weit versteht und auch emotionale Beeinträchtigungen, etwa Einschüchterungseffekte aufgrund von Kontrollverlusten über Daten, hierunter fassen will. Auf rechtliche, wirtschaftliche und sonstige Nachteile stellen auch ab Simitis/

fährdungen der Weiterverarbeitung durch technische Schutzmaßnahmen verhindert werden – so das letztgenannte Kriterium[80] –, liegt typischerweise keine Unvereinbarkeit der Zwecke vor.[81]

Bei bestimmten privilegierten Weiterverarbeitungen wird nach Art. 5 Abs. 1 lit. b HS. 2 DSGVO die Kompatibilität vermutet.[82] Relevant sind im Folgenden vor allem statistische Erhebungen, die in Erwgr. 162 S. 3 näher beschrieben sind. Auf Einzelheiten wird im Rahmen der Modellbildung zurückzukommen sein.

bb) Zulässigkeit der Zweckänderung im weiteren und im engeren Sinne

Die Zweckänderung im weiteren Sinne ist nicht untersagt. Die Zweckänderung im engeren Sinne ist zwar untersagt, Art. 6 Abs. 4 DSGVO sieht aber zwei Zulassungsgründe vor: die Zulassung durch Rechtsvorschrift[83] – was in der vorliegenden Untersuchung jedoch außer Acht bleiben soll – sowie diejenige durch Einwilligung. Für diese gelten die nämlichen Bedingungen wie für die der Einwilligung im Rahmen des Rechtmäßigkeitsgrundsatzes,[84] auf die sogleich einzugehen ist. Unklar ist sowohl bei der Zweckänderung im weiteren

Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 56; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 190.

[80] Art. 6 Abs. 4 lit. e) DSGVO.

[81] Siehe hierzu bereits *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 26 f. Vgl. eingehend zu diesem Merkmal Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 60; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 191; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 141; Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 168. Wie sich bereits aus der expliziten Benennung ergibt, ist dabei von besonderer Bedeutung die Schutzgarantie durch die Pseudonymisierung, vgl. hierzu auch *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 26 sowie Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 168; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 60; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 191; *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 17 (2016), 315, 328.

[82] Vgl. Erwägungsgrund 50 S. 4. Von einer Fikton bzw. widerleglichen Vermutung gehen aus Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 41, 109; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 223; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 292.

[83] Ausführlich hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 22–31.

[84] Siehe nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 20; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 179.

Sinne[85] als auch bei der Zweckänderung im engeren Sinne,[86] ob es für die Weiterverarbeitung zusätzlich eines eigenen Rechtfertigungsgrundes nach Art. 6 Abs. 1 DSGVO bedarf oder ob die Weiterverarbeitung von der Zulassung der ursprünglichen Verarbeitung profitiert.[87] Der EuGH hat in dieser Sache noch nicht entschieden. Die Art. 29 Datenschutzgruppe fordert zusätzlich das Vorliegen eines eigenen Rechtfertigungsgrundes.[88] Ist eine inkompatible Zweckänderung nicht nach Art. 6 Abs. 4 DSGVO ausnahmsweise zugelassen, ist de-

[85] Vielfach wird davon ausgegangen, dass die zweckkompatible Weiterverarbeitung keiner eigenständigen Rechtfertigung bedarf, da das Unionsrecht Zweckänderungen eben nur im Falle der Inkompatibilität anerkennt. Dann ist es konsequent, die kompatible Zweckänderung an der ursprünglichen Rechtfertigung teilhaben zu lassen, so Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 37.1; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 98–99; Paal/Pauly, DS-GVO/*Frenzel*, Art. 5 Rn. 31; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 142–143; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 5 Rn. 20.

[86] Zwar spricht Erwägungsgrund 50 S. 2 davon, dass im Fall der Zulassung der Zweckänderung keine andere gesonderte Rechtsgrundlage notwendig sei. Der Wortlaut lässt sich aber auch so verstehen, dass für die Primärverarbeitung, d.h. für die Erhebung der Daten, die herangezogene Rechtsgrundlage ausreichend bleibt und damit die Rechtmäßigkeit der ursprünglichen Erhebung von der später zweckgeänderten Datenverarbeitung unberührt bleibt, so Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 75. Im Übrigen wird in der Literatur vielfach von einem Redaktionsversehen ausgegangen, vgl. Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Wedde*, Art. 6 Rn. 125; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 182. Kritisch hierzu Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 215; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 12 Fn. 6.

[87] Dies hängt davon ab, ob man Art. 6 Abs. 4 DSGVO als zweck- und rechtmäßigkeitsspezifische Norm begreift, die Vorschrift also eine Privilegierung in Bezug auf Art. 5 Abs. 1 lit. b) HS. 1 DSGVO und Art. 6 Abs. 1 DSGVO darstellt. So Gola, DS-GVO/*Schulz*, Art. 6 Rn. 142; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 212–216; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 235; *Culik/Döpke*, ZD 7 (2017), 226, 230; Plath, DSGVO/BDSG/*Plath*, Art. 5 Rn. 9–10; Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 154, oder als allein zweckfestlegungsspezifische Norm, die allein als Privilegierung hinsichtlich des Art. 5 Abs. 1 lit. b) HS. 1 DSGVO zu begreifen ist, so Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 71–76; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Wedde*, Art. 6 Rn. 125–126; *Albrecht*, CR 32 (2016), 88, 92; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 183–184; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Albrecht*, Art. 6 Rn. 13; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 48.

[88] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 37: „[T]he prohibition of incompatible use and the requirement of a legal basis under Article 7 of the Directive [heute: Art. 6 DSGVO] are cumulative requirements. Therefore, for a change of purpose, one of the legal grounds (points a to f) needs to apply anyway".

ren Durchführung rechtswidrig.[89] Dem Verantwortlichen bleibt dann nur die Neuerhebung der Daten.[90]

2. Einwilligung

Die Einwilligung als wesentlicher Rechtfertigungsgrund im dezentralen Regulierungsregime zwischen Privaten ist in Art. 4 Nr. 11 DSGVO legaldefiniert, die Voraussetzungen ergeben sich aus Art. 6 Abs. 1 S. 1 lit. a), Art. 7, Art. 8 DSGVO.[91] Von besonderem Interesse im Hinblick auf die Einwilligung sind die Informiertheit (a)) und die Freiwilligkeit (b)).

a) Informiertheit der Einwilligung

Die Einwilligung „in informierter Weise" setzt voraus, dass die betroffene Person in Kenntnis der konkreten Sachlage entscheidet[92] und Tragweite und Bedeutung der erteilten Einwilligung abschätzen kann.[93] Es ergeben sich Überschneidungen mit den Informationspflichten nach Art. 12–15 DSGVO,[94] wenn-

---

[89] Die Weiterverarbeitung kann nicht durch Heranziehung eines Rechtfertigungsgrundes nach Art. 6 Abs. 1 DSGVO gerechtfertigt werden. Dies widerspricht nicht nur dem Wortlaut der Art. 5 Abs. 1 lit. b) HS. 1 DSGVO, vor allem würde der Zweckfestlegungsgrundsatz untergraben. Siehe nur *dies.*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 40. Ebenso Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 38; Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 23.

[90] Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Wedde*, Art. 6 Rn. 127; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 185; Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts 34, 38; Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 23.

[91] Zur Einwilligungsfähigkeit, für die insbesondere in Art. 8 DSGVO besondere Voraussetzungen normiert sind, siehe umfassend Wolff/Brink, BeckOK Datenschutzrecht/*Stemmer*, Art. 7 Rn. 33–36; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 49. Zur Rechtsnatur und Fragen von Willensmängeln, Nichtigkeitsgründen oder Stellvertretung siehe ausführlich Wolff/Brink, BeckOK Datenschutzrecht/*Stemmer*, Art. 7 Rn. 28–31.

[92] Siehe Erwägungsgrund 42 S. 4. Vgl. auch *Artikel 29 Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.04.2018, S. 15.

[93] Zu den Anforderungen siehe *dies.*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.04.2018, S. 15 sowie Wolff/Brink, BeckOK Datenschutzrecht/*Stemmer*, Art. 7 Rn. 52; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 59; Paal/Pauly. DS-GVO/*Ernst*, Art. 4 Rn. 79; *Andreotta/Kirkham/Rizzi*, 3, 6–7: „Such information allows them to perform a kind of risk assessment". Die Vorschrift ist von der Einwilligung in ärztliche Heileingriffe inspiriert, vgl. *Buchner*, in: Tinnefeld/Buchner/Petri u.a. (Hrsg.), Einführung in das Datenschutzrecht, [6]2018, S. 403, Rn. 56.

[94] Vgl. *Artikel 29 Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.04.2018, S. 14–15, 17, die einen „integrierten Ansatz" zwischen Einwilligung und Transparenzgrundsatz fordert. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Stemmer*, Art. 7 Rn. 52.

gleich hier eine spezifizierte, d.h. die Einwilligungsfähigkeit herstellende Transparenz gemeint ist.[95] Es ist auch über die Folgen der Datenverarbeitung zu unterrichten, soweit diese nicht ohne Weiteres für die betroffene Person erkennbar sind.[96]

b) Freiwilligkeit der Einwilligung

Die Freiwilligkeit erweist sich vielfach als neuralgischer Punkt der Einwilligung.[97] Dass die Freiwilligkeit der Einwilligung unter den Bedingungen einer modernen Datenwelt überhaupt je vorliegt, wird kontrovers diskutiert. Die Post-Privacy-Bewegung,[98] spiel- und verhaltensökonomische Erwägungen,[99] aber auch das Design der Digitalmärkte mit ihren wirtschaftlichen[100] oder in-

---

[95] Es gibt Überschneidungen mit den Informationspflichten aus Art. 13 und 14 DSGVO, die einwilligungsbezogene Transparenz unterscheiden sich jedoch von diesen, siehe hierzu etwa Gola, DS-GVO/*Schulz*, Art. 7 Rn. 37; *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 166; *Veil*, NJW 71 (2018), 3337, 3339. Zudem ergeben sich zeitliche Unterschiede: Die Information für die Einwilligung muss noch vor der Datenerhebung erfolgen, die Information nach Art. 13, 14 DSGVO erst bei Datenerhebung, bei Art. 15 DSGVO erst bei Anfrage, vgl. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 12 Rn. 16; Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 5. In der Praxis in der Datenschutzerklärung diffundieren die Unterschiede zusätzlich, da regelmäßig nur eine Datenschutzerläuterung erfolgt, die zugleich die Informationspflichten aus Art. 13 und Art. 14 DSGVO und die der Einwilligung bedient, so auch *Lorentz*, Profiling, 2019, S. 181 f. Siehe hierzu auch unter Kapitel 4 D. II. 2. b).

[96] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 13. Siehe auch Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Däubler*, Art. 7 Rn. 15, 17.

[97] Vgl. nur die Darstellungen bei Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 4; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 10–12, jeweils mit zahlreichen Literaturnachweisen.

[98] Vgl. hierzu etwa *Heller*, Post-privacy, 2011.

[99] Siehe hierzu umfassend die Untersuchung von *Hermstrüwer*, Informationelle Selbstgefährdung, 2015. Vgl. auch *Edwards/Veale*, SSRN Journal 2017, 66.

[100] Diese Machtstellung führt dazu, dass verarbeitende Akteure keine Alternative zu ihren Angeboten und deren Ausgestaltung, etwa in datenschutzfreundlicherer Form, zur Verfügung stellen. Den NutzerInnen bleibt dann nur, die Dienste in dieser Form anzunehmen oder sich gänzlich dem digitalen Angebot zu entziehen („Take it or leave it"). Vgl. hierzu Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 11; *Buchner*, in: Tinnefeld/Buchner/Petri u.a. (Hrsg.), Einführung in das Datenschutzrecht, ^{6}2018, S. 403, Rn. 39–43. Teilweise wird ein Marktversagen für datenschutzkonforme Angebote festgestellt, so etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 4–5. Vgl. für den Anwendungsbereich der Umgebungsintelligenz Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 42.

formationellen[101] Monopolstrukturen lassen hieran zweifeln. Auch empirische Befunde, prominent etwa das Privacy Paradox,[102] sprechen dagegen. Diese Fragen bedürfen, gerade auch im Hinblick auf autonome Systeme, vertiefter Untersuchung. Dies kann die vorliegende Arbeit nicht leisten, das Vorliegen der Freiwilligkeit wird daher im Folgenden unterstellt.[103]

3. *Vertragsimmanente Zulassung*

Die Zulassung der Datenverarbeitung nach Art. 6 Abs. 1 lit. b) DSGVO ist Bestandteil eines Vertrages oder einer vorvertraglichen Maßnahme.[104] Auch hier gelten gewisse Informationspflichten, wenngleich gegenüber der Einwilligung nur in eingeschränktem Maße.[105] Entscheidend ist, dass für die betroffene Person der Umfang der notwendigen Datenverarbeitungen erkennbar ist.[106] Im Übrigen unterscheiden sich die Bedingungen hinsichtlich der Ver-

---

[101] Siehe hierzu *Kamp/Rost*, DuD 37 (2013), 80 f.; *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 201 f.

[102] Das Privacy Paradox beschreibt die empirische Beobachtung, dass eine erhöhte datenschutzbezogene Sensibilität betroffener Personen nicht mit einer besonderen Zurückhaltung ihrer Daten korrespondiert, sondern betroffene Personen sogar besonders freigiebig ihre Daten teilen. Verschiedene Ansätze, vor allem aus der Verhaltensökonomie, werden bemüht, um dieses widersprüchliche Verhalten zu erklären. Aus der umfassenden Literatur siehe beispielhaft *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 100–116; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 232 f.; *Norberg/Horne/Horne*, Journal of Consumer Affairs 41 (2007), 100–126. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 4.

[103] Fragen der Freiwilligkeit im Rahmen der Profilbildung bearbeitet ausführlich *Lorentz*, Profiling, 2019, S. 168–176. Sie geht auch der Frage nach, ob die Einwilligung als Rechtfertigungsgrund im Rahmen der Profilbildung überhaupt geeignet ist. Im Ergebnis sieht sie dies kritisch, vgl. *dies.*, Profiling, 2019, S. 176–179.

[104] Die Vorschrift ist damit ganz wesentlich Ausdruck der Privatautonomie. Vgl. Wolff/Brink, BeckOK DatenschutzR/*Albers/Veit*, Art. 6 Rn. 29; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 15; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 26. Hinter der Vorschrift steckt auch der Gedanke des Schutzes des Vertragspartners vor treuwidrigem Verhalten der betroffenen Person: Stimmt diese einem Vertragsschluss bzw. einer vorvertraglichen Maßnahme zu, stellte es einen Verstoß gegen Treu und Glauben dar, wenn sie die dafür erforderlichen Datenverarbeitungen verweigerte, vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 15.

[105] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 15, 26. Sehr allgemein *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 6.

[106] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 25. Vgl. auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der

tragserfüllung (a)) und der vorvertraglichen Maßnahme (b)). Zum Verhältnis dieses Zulassungsgrundes zur Einwilligung soll im Anschluss eingegangen werden.[107]

a) Vertragserfüllung

Gemeinhin wird der Vertrag im Sinne dieser Vorschrift als vertragliches Schuldverhältnis, verstanden.[108] Die Vertragserfüllung meint die Erbringung der geschuldeten Leistung.[109] Erfasst sind sämtliche mit einem Vertragsverhältnis in Verbindung stehende Datenverarbeitungen.[110] Umfang und Inhalt der erfolgenden Datenverarbeitungen legen die Parteien im konkreten Vertragsverhältnis fest,[111] aufgrund der Privatautonomie sind sie dabei frei.[112] Das Merkmal der Erforderlichkeit meint nicht Verhältnismäßigkeit.[113] Der Generalanwalt beim EuGH,[114] die Artikel 29 Datenschutzgruppe[115] und der Europäische

Richtlinie 95/46/EG, 09.04.2014, S. 22. Maßgeblich ist die jeweilige Vertragsbeziehung; bei Dauerschuldverhältnissen kommt es daher auf den einzelnen Vertrag bzw. die einzelne geschuldete Leistung an, vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 29.

[107] Siehe Kapitel 4 C. II. 6.

[108] Vgl. Wolff/Brink, BeckOK DatenschutzR/*Albers/Veit*, Art. 6 Rn. 30; Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 13; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 27.

[109] Erfasst sind Haupt-, Neben(leistungs-)pflichten, ebenso das Gewährleistungsschuldverhältnis. Siehe eingehend Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 31; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 24; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 33.

[110] So auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 31; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 30. Ebenso *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 13 f.

[111] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 25; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 27, 39.

[112] Gola, DS-GVO/*Schulz*, Art. 6 Rn. 27, 39. Problematisch können aber Leistungsbeschreibungen in Form von AGB sein. Diese verlangen aufgrund der datenschutzrechtlichen Anforderungen eine besonderen Transparenz- und Inhaltskontrolle, siehe hierzu ausführlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 27–28; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 40.

[113] Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 14.

[114] Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 54 – *Meta Platforms Inc. u.a./Bundeskartellamt*.

[115] *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 21 f.

Datenschutzausschuss,[116] gefolgt von weiten Teilen der Literatur,[117] prägen ein striktes Verständnis: Die Datenverarbeitung ist nur dann erforderlich, wenn der geschuldete Leistungserfolg ohne die Datenverarbeitung nicht erbracht werden könnte. Dies meint anderes als bloße Nützlichkeit oder Zweckdienlichkeit.[118]

b) Vorvertragliche Maßnahme

Art. 6 Abs. 1 lit. b) Alt. 2 DSGVO setzt in der Phase vor dem Vertragsschluss an.[119] Es geht um Datenverarbeitungen für die Erstellung eines Vertragsangebots.[120] Bloße Ausforschungen oder generelle Anfragen genügen demnach nicht. Ausweislich des Wortlauts muss die Initiative dabei von der betroffenen Person ausgehen.[121] Da es hier noch keinen Vertrag gibt, definiert die Anfrage der betroffenen Person den Umfang der zulässigen Datenverarbeitungen.[122] Der Maßstab der Erforderlichkeit entspricht dem der ersten Alternative: Die Datenverarbeitung ist für die vorvertragliche Maßnahme demnach erforderlich, wenn der Vertragsschluss andernfalls nicht zustande kommen könnte.[123]

---

[116] *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 11.

[117] So etwa Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 14; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 32; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 38. So auch Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Klein*, Art. 6 Abs. 1 lit. b Rn. 63.

[118] Siehe Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 54 – *Meta Platforms Inc. u.a./Bundeskartellamt* sowie *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 22 f. Ebenso Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 42; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 13.

[119] Die DSGVO und auch das Unionsrecht im Übrigen definieren vorvertragliche Maßnahmen nicht, vgl. Gola, DS-GVO/*Schulz*, Art. 6 Rn. 32.

[120] Erfasst sind Vertragsverhandlungen und Vertragsanbahnungen, siehe hierzu ausführlich Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 35–36. Bloße unverbindliche Anfragen oder Ausforschungen genügen nicht, vgl. Paal/Pauly DS-GVO/*Frenzel*, Art. 6 Rn. 15; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 39.

[121] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 41; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 14. Vgl. auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 23.

[122] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 39.

[123] Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 15; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 43.

4. Interessensabwägung

Art. 6 Abs. 1 lit. f) DSGVO verlangt eine Interessensabwägung,[124] die in drei Schritten erfolgt: Darlegung eines berechtigten Interesses des Verantwortlichen (a)), Erforderlichkeit der Datenverarbeitung zur Wahrung des Interesses (b)) sowie kein Überwiegen berechtigter Interessen der betroffenen Person (c)).[125]

a) Berücksichtigungsrelevante Interessen

Auf Seiten des Verantwortlichen sind – anders als bei der betroffenen Person[126] – nur *berechtigte* Interessen berücksichtigungsrelevant, d.h. solche, die mit der Rechtsordnung im Einklang stehen.[127] Betroffene Personen können allein eigene Interessen vorbringen, solche Dritter sind unbeachtlich.[128] Vorgaben zum Inhalt und Qualität des Interesses erfolgen in der DSGVO nicht.[129] Erfasst sind rechtliche, wirtschaftliche, geschäftliche und ideelle Interessen.[130] Gemeint ist

---

[124] Der Rechtfertigungsgrund ist damit gegenüber den übrigen Zulassungsgründen strikter, da dort ein überwiegendes Interesse des Verantwortlichen nicht dargelegt werden muss. So auch *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 34.

[125] Gemeinhin wird dies als Dreistufenprüfung bezeichnet, siehe nur Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 146; Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 27.

[126] Für die betroffene Person können auch illegitime Interessen beachtlich sein. Die fehlende Anerkennung des Interesses durch die Rechtsordnung kann dann aber in der Interessensgewichtung Berücksichtigung finden, vgl. Gola, DS-GVO/*Schulz*, Art. 6 Rn. 62; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 28.

[127] Nicht nur Verstöße gegen die DSGVO – dort sind dann besondere andere Datenschutzgrundsätze aus Art. 5 DSGVO relevant –, sondern auch solche gegen sämtliche nationale und unionale Rechtsvorschriften sind zu berücksichtigen. Datenverarbeitungen zu strafrechtlich bewehrten Zwecken dienen demnach keinen berechtigten Interessen, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 68; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 98.

[128] Soweit eine Datenverarbeitung (auch) Interessen Dritter berührt, ist allein relevant, ob und in welchem Maße hierdurch Interessen der betroffenen Person berührt sind. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 102. Er tritt zwar für gewisse Öffnungen ein, löst sich aber nicht von der Bedingung, dass die Datenverarbeitung gerade die Interessen der einzelnen Person berühren muss.

[129] Eine ursprünglich vorgesehene Befugnis der Kommission zum Erlass delegierter Rechtsakte wurde ebenso gestrichen wie eine nähere Präzisierung, etwa durch einen Kriterienkatalog, vgl. Wolff/Brink, BeckOK DatenschutzR/*Albers/Veit*, Art. 6 Rn. 67; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 103.

[130] Siehe auch Erwägungsgrund 47 S. 2, 6, 7 und Erwägungsgrund 48. Vgl. überdies Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 28; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 146a. Ebenso sind auf Seiten der betroffenen Person rechtliche, wirtschaftliche, ideelle oder sonstige Interessen erfasst, siehe nur Kühling/Buchner, DS-GVO, BDSG/

nicht das Verarbeitungsinteresse, d.h. das bloße Interesse am technischen Prozess, sondern das übergeordnete Interesse,[131] wie es sich regelmäßig aus der Zweckbestimmung ergibt.[132]

b) Erforderlichkeit

Die Erforderlichkeit meint – anders als bei Art. 6 Abs. 1 lit. b) DSGVO – Angemessenheit. Maßgeblich ist, ob das berechtigte Interesse des Verantwortlichen ohne die Datenverarbeitung in angemessener Weise gewahrt werden könnte,[133] bzw. ob dem berechtigten Interesse des Verantwortlichen durch andere Methoden ebenso effektiv, aber für die betroffene Person beeinträchtigungsärmer Rechnung getragen werden kann.[134] Wie auch im Rahmen des Art. 6 Abs. 1 lit. b) DSGVO ist die Erforderlichkeit eng auszulegen, bloße Nützlichkeit oder Zweckdienlichkeit genügen nicht.[135]

c) Interessensabwägung im engeren Sinne

Bei der Abwägung verlangt Art. 6 Abs. 1 lit. f) DSGVO ein Überwiegen der Interessen der betroffenen Person; bei Gleichstand darf die Verarbeitung also stattfinden.[136] Der Vorschrift lässt sich vorab keine inhaltliche Ausrichtung

---

Buchner/Petri, Art. 6 Rn. 148a; *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 30 f. Diese Interessen können, müssen aber nicht grundrechtlicher Natur sein, vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 98. Die explizite Aufführung der Grundrechte und -freiheiten hat allein klarstellende Funktion, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 71.

[131] Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 68; Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 28.

[132] Gola, DS-GVO/*Schulz*, Art. 6 Rn. 61; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 149. Siehe auch Erwägungsgrund 47 S. 3.

[133] So Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 29; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Wedde*, Art. 6 Rn. 94.

[134] So Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 100; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 147a.

[135] Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 147a; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 100.

[136] Gola, DS-GVO/*Schulz*, Art. 6 Rn. 62; Sydow, DS-GVO/*Reimer*, Art. 6 Rn. 63. Siehe auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 11, wenn auch noch zur entsprechenden Vorschrift in der Datenschutzrichtlinie, wonach dieser Zulassungstatbestand weder als enge Ausnahmevorschrift noch als weite Auffangvorschrift zu verstehen ist.

entnehmen, weder zugunsten der betroffenen Person noch des Verantwortlichen.[137]

Nach Erwgr. 47 S. 1 HS. 2, S. 3 und S. 4 sind die vernünftigen Erwartungen der betroffenen Person von maßgeblicher Bedeutung. Von Relevanz ist dabei die Beziehung zwischen Verantwortlichem und betroffener Person (Erwgr. 47 S. 1 HS. 2, S. 3)[138] sowie der Kontext der Verarbeitung (Erwgr. 47 S. 4). Dabei gilt ein objektivierter Maßstab, es kommt also nicht auf den individuellen Erwartungshorizont an.[139]

Für die Interessensabwägung im engeren Sinne haben der Europäische Datenschutzausschuss[140] sowie die Literatur Abwägungskriterien vorgeschlagen. Im Wesentlichen gleichen diese den in Art. 6 Abs. 4 DSGVO benannten Kriterien. Maßgeblich sind also etwa Art und Inhalt[141] sowie Umfang[142] der verarbeiteten Daten, die, auch mittelbaren,[143] Folgen der Datenverarbeitung,[144] die individuelle Schutzwürdigkeit der betroffenen Person,[145] sowie technische Schutzmaßnahmen.[146]

---

[137] Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 27, 31; Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 13; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 86–87. Konsequent sehen Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 13 in der Vorschrift eine Form der regulierten Selbstregulierung.

[138] Ausführlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 109.

[139] Vgl. etwa Gola, DS-GVO/*Schulz*, Art. 6 Rn. 67, der einen „gemischt subjektiv-objektive[n]" Maßstab heranzieht, wonach auf die Erwartungen der betroffenen Person, objektiviert über die Sichtweise eines objektiven Dritten abzustellen ist. Siehe auch ausführlich *Lorentz*, Profiling, 2019, S. 199.

[140] Siehe für die Profilbildung etwa *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 15 f. Ausführlich hierzu unten Kapitel 4 C. III. 2. d) bb).

[141] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 105; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 63.

[142] Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 153.

[143] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 107.

[144] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 107; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 28. Darin wird ein risikobasierter Ansatz der DSGVO erkenntlich.

[145] Dieses Kriterium wird aus dem Hinweis auf die Personengruppe der Kinder in Art. 6 Abs 1 lit. f) DSGVO abgeleitet. Vgl. Gola, DS-GVO/*Schulz*, Art. 6 Rn. 63; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 112–113.

[146] Vgl. allgemein Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 114; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 63; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 143. Zu Einwirkungsrechten siehe Sydow, DS-GVO/*Reimer*, Art. 6 Rn. 61; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/

5. Automatisierte Entscheidung

Art. 22 Abs. 2 DSGVO sieht drei Ausnahmetatbestände für das Verbot automatisierter Entscheidungen vor: erstens die vertragsimmanente Zulassung (lit. a), dies allerdings anders als bei Art. 6 Abs. 1 lit. b) DSGVO exklusive vorvertraglicher Maßnahmen,[147] zweitens die Zulassung durch eine nationale oder unionale Rechtsvorschrift (lit. b) sowie drittens die Einwilligung (lit. c). Die Zulassung per Rechtsvorschrift soll nicht näher untersucht werden. Hinsichtlich der Einwilligung und der vertragsimmanenten Zulassung gelten dieselben Bedingungen wie für die der Datenverarbeitung,[148] allein der Anknüpfungspunkt ist ein anderer: Die automatisierte Entscheidung, nicht die Datenverarbeitung ist der Referenzpunkt.[149] Die Einwilligung darf nur ausdrücklich erteilt werden.

6. Verhältnis der Zulassungsgründe zueinander

Unklar ist, in welchem Verhältnis die Zulassungsgründe zueinander stehen.[150] Im Kern geht es dabei um die Frage, ob der Einwilligung gegenüber den ande-

---

Schwartmann/Klein, Art. 6 Abs. 1 lit. f) Rn. 162; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 152.

[147] In Abgrenzung zum Vertragsschluss mittels automatisierter Verfahren, die unter die Vorschrift fallen, sind mit vorvertraglichen Maßnahmen Methoden vor bzw. jenseits einer konkreten Vertragsanbahnung gemeint, etwa wenn geklärt werden soll, ob überhaupt ein Vertragsschluss in Betracht kommt oder personalisiertes Informationsmaterial zu einem Produkt erfragt wurde. Typische Anwendungen von automatisierten Vertragsgestaltungen, etwa das Kredit-Scoring oder personalisierte Preisbildung betreffen dagegen den Vertragsschluss. Siehe zu all dem Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 39.

[148] Zur vertragsimmanenten Zulassung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 41; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 31. Zur Einwilligung Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 41; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 38.

[149] Vgl. zur vertragsimmanenten Zulassung Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 21a sowie Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 41; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 30. Zur Einwilligung Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 41.

[150] Diese Frage stellt sich nur, wenn noch alle Zulassungsgründe offenstehen. Scheitert ein Zulassungsgrund ist das Heranziehen eines anderen Zulassungsgrundes untersagt. Vgl. für die Ersetzung der Einwilligung durch eine Interessensabwägung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 89. Aus rechtspraktischer Sicht stellt sich diese Frage, da die Zulassungsgründe für den Verantwortlichen unterschiedlich attraktiv sind. Während an die Einwilligung keine inhaltlichen Anforderungen gestellt sind, ist nicht sicher, dass die betroffene Person sie erteilt, zudem kann sie jederzeit widerrufen werden, Art. 7 Abs. 3 DSGVO, und geht mit einem umfassenden, potentiell ressourcenintensiven Informationspflichtenprogramm einher. Die vertragsimmanente Zulassung kann nicht zurückgenommen werden, zudem können Datenverarbeitungsbedingungen gemeinsam ausgehandelt werden, der Verantwortliche muss allerdings die Grenzen des all-

ren Zulassungstatbeständen eine vorrangige Stellung zukommt. Der EuGH und die Generalanwälte sind in dieser Frage uneindeutig,[151] der Europäischen Datenschutzausschuss tritt dagegen für einen Vorrang der Einwilligung ein.[152] Letztlich ist die Abgrenzungsproblematik auf Vorverständnisse des Datenschutzrechts zurückzuführen. Begreift man das Datenschutzrecht als Recht auf informationelle Selbstbestimmung, muss der Einwilligung notwendig eine übergeordnete Stellung zukommen.[153] Ein solches Verständnis überzeugt jedoch nicht.[154] Aufgrund des dezentralen Regulierungsmechanismus erscheint aber auch eine Gleichrangigkeit der Zulassungsgründe nicht sinnvoll.[155] Letztlich geht es um eine Abwägung der digitalen Autonomie der betroffenen Person mit dem Verarbeitungsinteresse des Verantwortlichen. Im vertraglichen Verhältnis geht es aber noch um anderes: Die digitale Autonomie hat unter modernen Marktbedingungen auch eine ökonomische Seite. Digitale Autonomie wird nicht beschränkt, sondern wahrgenommen, wenn die betroffene Person im Vertragsverhältnis ihre Daten teilt.[156] Im vertraglichen Verhältnis geht es also (zusätzlich) um den Schutz und die Anerkennung der Privatautonomie,

---

gemeinen Zivilrechts beachten. Auch hier bestehen Informationspflichten. Die Interessensabwägung ist ebenso unwiderruflich, hier ist der Verantwortliche auch nicht von der betroffenen Person abhängig und ihn trifft allenfalls ein eingeschränktes Informationspflichtenprogramm. Allerdings sind hier von Seiten des Staates inhaltliche Angemessenheitskriterien vorgegeben.

[151] Den Entscheidungen des EuGH lässt sich bislang keine klare Positionierung entnehmen. Für einen Vorrang der Einwilligung tritt etwa ein Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 53–64 – *Meta Platforms Inc. u.a./Bundeskartellamt*, für einen Vorrang des Art. 6 Abs. 1 lit. b) DSGVO vor der Einwilligung, Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 73–82 – *UI gegen Österreichische Post AG*.

[152] So etwa *Europäischer Datenschutzausschuss*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), 05.12.2022, S. 35 f. In anderen Texten geht die *Artikel 29 Datenschutzgruppe* von einer Gleichwertigkeit der Zulassungstatbestände aus, siehe etwa *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 13.

[153] Mit dieser Begründung etwa Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 53–64 – *Meta Platforms Inc. u.a./Bundeskartellamt*.

[154] Siehe oben Kapitel 4 A. I. 2. a), Kapitel A. II. 3. b).

[155] So aber *Veil*, NJW 71 (2018), 3337, 3337–3338, 3344; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 10; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 16. So wohl auch *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, [3]2019, 1, 448.

[156] Eingehend *Nettesheim*, Digitale Autonomie in Vertragsbeziehungen, Verfassungsblog, 12.10.2022; *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 14. Vgl. auch Generalanwalt Sánchez-Bordona, Schlussanträge v. 06.10.2022, Rs. C-300/21, ECLI:EU:C:2022:756, Rn. 81 – *UI gegen Österreichische Post AG*. Siehe auch bereits oben Kapitel 4 A. II. 2. b).

und zwar beider Seiten.[157] Daher muss dort die vertragsimmanente Zulassung den übrigen Zulassungsgründen, auch der Einwilligung vorgehen.[158] Es muss dann allerdings im Einzelfall geprüft werden, welche Datenverarbeitungen vertragsakzessorisch und -notwendig sind.[159] Was die Abgrenzung der Einwilligung von der Interessensabwägung anbelangt, so gilt: Solange die Datenverarbeitung über die Einwilligung interessensgerecht gerechtfertigt werden kann, ist vorrangig auf diese abzustellen.[160] Hat aber der Verantwortliche ein besonderes Interesse an der Zulassung, etwa im Falle der Missbrauchs- oder Betrugsprävention,[161] oder hat umgekehrt die betroffene Person kein oder nur ein geringes Interesse an der Erteilung der Einwilligung, da etwa die Datenverarbeitung nur ein geringes oder kein Risiko aufweist und sie auch nicht mit der Einholung der Einwilligung rechnet,[162] geht Art. 6 Abs. 1 lit. f) DSGVO vor.

---

[157] *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 14. Ausführlich auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 60–68, der die staatliche Zulassung im auf Privatautonomie beruhenden rechtsgeschäftlichen Verhältnis als „Fremdkörper" bezeichnet. Befürwortend Wolff/Brink, BeckOK DatenschutzR/*Albers/Veit*, Art. 6 Rn. 44, 69.

[158] Eingehend *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 54–60. Ebenso *Nettesheim*, Digitale Autonomie in Vertragsbeziehungen, Verfassungsblog, 12.10.2022; *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 14–16. In diese Richtung auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 44.

[159] So auch *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 14. Es geht dann also um das Tatbestandsmerkmal der Erforderlichkeit in Art. 6 Abs. 1 lit. b) DSGVO. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 44.

[160] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 65. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 11. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 69. Wohl auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 11. In diese Richtung gehen auch Argumentationen, wonach die missbräuchliche Abstützung auf Art. 6 Abs. 1 lit. f) DSGVO unzulässig ist. Siehe etwa Paal/Pauly, DS-GVO/*Frenzel*, Art. 7 Rn. 26, der von der Gefahr der „Flucht vor der Einwilligung" spricht. Siehe auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 63 f.

[161] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 66–57. Befürwortend Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 69.

[162] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 67. Ebenso auf die Erwartbarkeit der Einholung einer Einwilligung für die betroffene Person abstellend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 11, 89; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 13.

III. Analyse des Zweckfestlegungs- und Rechtmäßigkeitsgrundsatzes als Instrumente zur Regulierung autonomer Systeme

Im Folgenden sollen nun Zweckmäßigkeits- und Rechtmäßigkeitsgrundsatz auf die Modellbildung (1.), die Profilbildung (2.) und Profilverwendung (3.) angewendet werden.[163]

1. Modellbildung: Verarbeitung von Trainingsdaten im Maschinellen Lernverfahren

Die Auswertung der Trainingsdaten auf Stufe der Modellbildung ist letztlich nichts anderes als eine Big-Data-Analyse. Bei der Modellbildung kann es zu Irritationen mit dem Zweckfestlegungsgrundsatz kommen (a)). Im Einzelnen soll dann die Zulassung über die Einwilligung (b)), die Vertragsbeziehung (c)) oder Interessensabwägung (d)) untersucht werden.

a) Zweckfestlegungsgrundsatz bei der Modellbildung

Der Zweckfestlegungsgrundsatz verlangt zum einen, die übergeordneten Zwecke der Modellbildung über Maschinellen Lernverfahren vorab zu benennen (aa)), zum anderen die Trainingsdaten nicht aus anderen, dann inkompatiblen Zweckkontexten zu beziehen (bb)).

aa) Zweckbestimmung

Bei der Zweckbestimmung stehen nicht das technische Datenverarbeitungsverfahren, d.h. das Maschinelle Lernverfahren selbst,[164] sondern das eigentliche Motiv der Verarbeitung im Fokus. Inwieweit konkrete Modellinhalte anzugeben sind, ist daher eine Frage der Rechtmäßigkeit bzw. der Transparenz, auf die im nachfolgenden Kapitel einzugehen ist. Der übergeordnete Zweck der Modellbildung ist die Ermöglichung von Erkenntnissen über die betroffene Person. Diese Bestimmung ist allerdings viel zu pauschal, zudem handelt es sich allein um das Fernziel der Modellbildung.[165] Präziser lässt sich sagen: Der

---

[163] Siehe zu dieser Einteilung Kapitel 4 B. III. am Anfang. Die im Weiteren aufgeführten Problematiken stellen sich dann ebenso hinsichtlich des Maschinellen Lernverfahrens zur Erstellung des Lösungsalgorithmus. Mit der Frage der Nutzung von Daten für die Erstellung eines Lösungsalgorithmus war die italienische Datenschutzbehörde Garante im März/April 2023 befasst. Die folgenden Erwägungen über die Modellbildung lassen sich mit gewissen Anpassungen auf die datenschutzrechtlichen Fragen hinsichtlich ChatGPT übertragen.

[164] Die Modellbildung selbst, d.h. die Ableitung von Mustern und Regeln aus den Datensätzen, beschreibt nur das technische Verfahren, nicht aber den eigentlichen Zweck, so auch Lorentz S. 181, 159. Als Zweckbestimmung lassen dies aber ausreichen *Lohr/Winston/Watts*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 224, 239.

[165] So auch *Gausling*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 379, Rn. 9. Ähnlich Wolff/Brink, BeckOK Da-

höhere Zweck der Modellbildung ist die technische Realisierung autonomer Systeme. Allerdings ist die Modellbildung und damit das zweistufige Profilbildungsverfahren, wie ausgeführt,[166] nur eine und dabei nicht die einzig denkbare Methode für den Erkenntnisgewinn über die jeweilige Person, der für die technische Umsetzung autonomer Systeme notwendig ist. Richtig ist daher, dass die Modellbildung der Optimierung autonomer Systeme durch Effektivierung des Profilbildungsverfahrens dient.[167] Darüber hinaus muss der spezifische Anwendungskontext eines autonomen Systems, etwa die personalisierte Werbung oder die automatisierte Vertragsgestaltung, benannt werden.[168]

Die Zweckbestimmung im Rahmen der Modellbildung verlangt im Ergebnis erstens einen Hinweis auf das zweistufige Profilbildungsverfahren und die Bedeutung des Modells dabei – die Generierung von Wissen übrt die Personengemeinschaft im Trainingsdatensatz –, und zweitens einen Hinweis auf den konkreten Anwendungskontext, d.h. die technische Realisierung eines ganz bestimmten autonomen Systems.[169] Um der betroffenen Person diesen Zweck besonders zu veranschaulichen, bietet es sich an, bestimmte grobe Inhalte der Analyse zu benennen, also konkrete Persönlichkeitsmerkmale, die in der Modellbildung analysiert werden sollen. Ergibt sich dies nicht bereits aus dem Anwendungskontext, kann dies auch normativ geboten sein. Art. 4 Nr. 4 DSGVO bietet hierfür eine Orientierung. Anzugeben ist dann etwa, ob im Mo-

---

tenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 28, demzufolge die Angabe „Big-Data-Analyse" zu vage ist.

[166] Siehe oben Kapitel 1 B. III. 2.

[167] Vgl. eingehend zur Frage, inwieweit die Dienstoptimierung dem Zweckbestimmungsgrundsatz dienen kann *Finck/Biega*, Technology and Regulation 2021, 44, 50 f. Sie verlangen, dass klar dargelegt wird, dass die Datenverarbeitung, genauer: die Personalisierung bzw. das Profiling, der Optimierung des Dienstes dient und darüber hinaus, welche Aspekte durch die Profilbildung bzw. Personalisierung optimiert werden. Siehe hierzu auch, wenngleich im Rahmen der Rechtmäßigkeitsgrundsatzes, auch *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 15 f.

[168] Ebenso im Ergebnis *Lorentz*, Profiling, 2019, S. 302. Ähnlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 89. Auch *Finck/Biega*, Technology and Regulation 2021, 44, 50 f.; *Gausling*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 379, Rn. 10–11 stellen auf konkrete Dienste ab.

[169] Ebenso *Lorentz*, Profiling, 2019, S. 302, vgl. zur Herleitung, wenngleich für die Profilbildung, *dies.*, Profiling, 2019, S. 162 f. Dies entspricht vielfach der derzeitigen Praxis der Zweckbeschreibungen gängiger Such- und Informationsfilterdienste, vgl. *Finck/Biega*, Technology and Regulation 2021, 44, 50. Wird der Lösungsalgorithmus in einem Maschinellen Lernverfahren gebildet, muss sowohl auf das Trainingsverfahren als auch den Anwendungskontext, etwa ein Textgenerierungsprogramm, hingewiesen werden. Vgl. die Forderungen der italienischen Datenschutzbehörde hinsichtlich ChatGPT *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 8.

dell die Zuverlässigkeit oder aber die Interessen oder der Gesundheitszustand ermittelt werden sollen.

Unzulässig sind damit explorative Analysen, d.h. Modellbildungen, bei denen der Verantwortliche den Trainingsdatensatz nach brauchbaren Mustern analysiert, um dann im Nachhinein Anwendungsoptionen des Modells auszuloten.[170] Unzulässig ist es auch, die Zwecke des Maschinellen Lernverfahrens gezielt offenzulassen, um das Modell späterhin für verschiedene, hier dann im Vorfeld bereits bekannte Anwendungskonstellationen verwenden zu können.[171] Wenn allerdings der Verantwortliche vorab klar macht, dass der Trainingsdatensatz für verschiedene Modelle und Anwendungskontexte – etwa Informationsfilterung und Werbung – verwendet werden soll, ist dies zulässig.

bb) Zweckbindung: Vorliegen und Zulässigkeit von Zweckänderungen

Zu unterscheiden sind verschiedene Konstellationen der Zweckänderung. So kann der Verantwortliche Daten, die er innerhalb eines bestimmten Dienstes aufgezeichnet hat, als Trainingsdaten für diesen Dienst nutzen.[172] Die Daten verlassen dann den Anwendungskontext nicht, erhalten aber einen anderen Verwendungszweck: Sie werden zu Trainingsdaten umgewidmet. Zum anderen kann der Verantwortliche die Trainingsdatensätze durch Daten aus anderen

---

[170] *Valkanova*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 336, Rn. 10. Ebenso, wenngleich zu Big-Data-Auswertungen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 88: „Erst recht unzureichend bestimmt ist der Zweck […] [der] allgemeine Wissensmehrung oder [der] ‚zufälligen Identifikation von Korrelationen'". Vgl. auch, ebenso zu Big-Data-Auswertungen im Allgemeinen, *Weichert*, ZD 3 (2013), 251, 256; *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 85; *Forgó/Hänold/Schütze*, in: Corrales/Fenwick/Forgó (Hrsg.), New Technology, Big Data and the Law, 2017, S. 17, 31 f.

[171] Vgl. *Lorentz*, Profiling, 2019, S. 304. Vgl. auch *Forgó/Hänold/Schütze*, in: Corrales/Fenwick/Forgó (Hrsg.), New Technology, Big Data and the Law, 2017, S. 17, 27.

[172] Es handelt sich um Konstellationen, in denen der Verantwortliche auf ein zweistufiges Profilbildungsverfahren umstellt. In digitalisierten Diensten wie den autonomen Systemen fallen eine Vielzahl von Daten an. Für den Verantwortlichen ist es wirtschaftlich interessant, diese zu verwerten. Er kann diese nutzen, um im Sinne einer Marktanalyse allgemeine Erkenntnisse über die Personengemeinschaft insgesamt zu gewinnen, aber auch, um vertiefte Erkenntnisse über die einzelnen Personen, dann durch die zweistufige Profilbildung, zu gewinnen. Diese Erkenntnisse kann er nutzen, um seinen Dienst zu verbessern, aber auch, um personalisierte Werbung zu schalten. Dies wird aber erst ab einer bestimmten Datenmenge möglich sein, überdies nur, wenn die Daten überhaupt verwertbare Aussagen für eine Modellbildung enthalten. Ob sich die Daten also für die Modellbildung eigenen, ist im Zeitpunkt der Datenerhebung noch nicht klar. Daher können derartige Big-Data-Analysen bzw. Modellbildungen gerade nicht vorab in eine Zweckbestimmung aufgenommen werden. Vgl. auch *Lorentz*, Profiling, 2019, S. 304 f.

Anwendungskontexten anreichern.[173] Denkbar ist dabei, dass die ursprünglichen Daten als Trainingsdaten markiert waren, dann aber den Anwendungskontext wechseln – hier werden schlicht die Trainingsdaten eines autonomen Systems mehrfach verwendet.[174] Denkbar ist aber auch, dass die ursprünglichen Daten nicht als Trainingsdaten markiert waren, dann werden Daten aus einem anderen Anwendungskontext zu Trainingsdaten umgewidmet. In der Praxis kommt dies vor allem bei Werbemaßnahmen vor: Die etwa im Rahmen einer Vertragsbeziehung oder einer Online-Plattform erhobenen Daten werden dann für die Erstellung von Werbemodellen verwendet.[175] Diese Zweckänderungen sind typisch für das Geschäftsmodell „Dienst gegen Daten", wie es vielfach bei sozialen Netzwerken oder Suchdiensten verbreitet ist. Hier erfolgt die Finanzierung der Dienste regelmäßig, wenngleich nicht nur,[176] über diese werbebezogene Weiterverwendung der Daten: Die Dienste werden (vermeintlich) kostenlos zur Verfügung gestellt, die NutzerInnen erbringen ihre Gegenleistung in Form der Hingabe ihrer Daten. Diese Daten können dann als Trainingsdaten für die Erstellung detaillierter Werbeprofile dienen. Die Betreiber der Plattformen finanzieren sich, indem sie anhand dieser Werbeprofile personalisierte Werbeplätze verkaufen.[177] Andere Konstellationen derartiger Zweckän-

---

[173] Vgl. *dies.*, Profiling, 2019, S. 305. Vgl. allgemein im Rahmen der Big-Data-Analyse Gola, DS-GVO/*Schulz*, Art. 6 Rn. 155.

[174] Siehe zu diesem Fall *Lorentz*, Profiling, 2019, S. 305.

[175] War bereits die Vertragsbeziehung bzw. Online-Plattform durch ein autonomes System gestaltet, werden die Trainingsdaten mehrfach verwendet; war die Vertragsbeziehung bzw. Online-Plattform nicht automatisiert-personalisiert gestaltet, werden Trainingsdaten aus einem anderen Anwendungskontext umgewidmet. Werden die passenden Werbeangebote von den Verantwortlichen selbst bespielt, handelt es sich um sogenannte „Bestandskundenwerbung", siehe *Ehmann*, Rn. 39, 42–43.

[176] Eingehend zu verschiedenen datengetriebenen Geschäftsmodellen *Strahringer/Wiener*, HMD Praxis der Wirtschaftsinformatik 58 (2021), 457–476.

[177] Dieses Geschäftsmodell ist hier vereinfacht dargestellt. Der besondere wirtschaftliche Wert dieser Werbeplätze, aus deren Verkauf Plattformbetreiber Einnahmen generieren, liegt nicht allein im personalisierten Zuschnitt der Werbung, den die Plattformbetreiber bieten, sondern auch in der Nutzung von direkten und indirekten Netzwerkeffekten. Vgl. eingehend zum Geschäftsmodell von sozialen Netzwerken und Suchmaschinen („Plattformökonomie") *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 266 f. Vgl. *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 17 auch von „indirekter Finanzierung". Siehe auch die Auswertung bei *Strahringer/Wiener*, HMD Praxis der Wirtschaftsinformatik 58 (2021), 457, 459, wonach Google im Jahr 80–90 % seines Jahresumsatzes aus Werbung finanzierte. Siehe allgemein auch *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 5 sowie Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6 Rn. 47.

derung betreffen Fälle, bei denen Verantwortliche, um den hohen Datenbedarf autonomer Systeme zu decken, Trainingsdaten von Dritten, d.h. auf dem freien Datenmarkt erwerben. Diese Daten entstammen dann den unterschiedlichsten Quellen und Anwendungskontexten.[178] Weder die Nutzung als Trainingsdaten noch der konkrete Anwendungskontext entsprechen dann der ursprünglichen Zweckbestimmung.

In all diesen Konstellationen handelt es sich um Zweckänderungen im weiteren Sinne:[179] Die Weiterverarbeitung im Modell hat mit der ursprünglichen Erhebung nichts zu tun. Es stellt sich dann die Frage, ob es sich um Zweckänderungen im engeren Sinne nach Art. 6 Abs. 4 DSGVO handelt und ob, so dies der Fall ist, diese zulässig sind. Dabei ist zunächst festzustellen, dass die Modellbildung kein nach Art. 5 Abs. 1 lit. b) DSGVO privilegiertes statistisches Verfahren darstellt ((1)). Ob dann eine unzulässige Zweckänderung vorliegt, bestimmt sich danach, ob die Zwecke im Einzelfall kompatibel sind ((2)). Diese ist dann allein über die Einwilligung legitimierbar ((3)).

(1) Privilegierung nach Art. 5 Abs. 1 lit. b) HS. 2 DSGVO

Überwiegend geht man davon aus, dass die Modellbildung keine Verarbeitung zu statistischen Zwecken darstellt.[180] Teilweise wird bereits die Anwendbarkeit der Vorschrift auf private Big-Data-Analysen zu kommerziellen Zwecken ausgeschlossen.[181] Vorwiegend wird die Anwendung der Privilegierung aber auf-

---

[178] Explizit zu Maschinellen Lernverfahren *Finck/Biega*, Technology and Regulation 2021, 44, 45. Allgemein zu Big-Data-Auswertungen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 40. Unterscheiden lassen sich dabei Vorgänge, die bestehende Daten für denselben Zweck erneut auswerten (data recycling), solche, bei denen bestehende Daten für einen anderen Zweck (data repurposing), und solche, bei denen die Daten für einen anderen Verwendungskontext (data recontextualisation) analysiert werden, zu dieser Einordnung siehe *Custers/Uršič*, Int. Data Priv. Law 6 (2016), 1, 5–7. Eine Zweckänderung im Sinne des Art. 6 Abs. 4 DSGVO liegt nur in den beiden letztgenannten Fällen vor.

[179] Siehe hierzu oben Kapitel 4 C. II. 1. b) aa).

[180] Die Modellbildung dient auch nicht wissenschaftlichen Erkenntnissen. Über das Maschinelle Lernen sollen zwar neue Erkenntnisse aus den Daten gewonnen werden, Ziel der Modellbildung, wie auch der Profilbildung, ist aber nicht die Erweiterung des allgemeinen Wissensbestandes. Siehe eingehend hierzu *Norwegian Data Protection Authority*, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 17 f. Vgl. zur Einordnung Maschineller Lernverfahren als wissenschaftliche Verarbeitung auch *Finck/Biega*, Technology and Regulation 2021, 44, 51 f.

[181] Dagegen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 42; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 107; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 292; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Tinnefeld*, Art. 89 Rn. 15a; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Caspar*, Art. 89 Rn. 22–24; *Culik/Döpke*, ZD 7 (2017), 226, 230; *Richter*, DuD 39 (2015), 735, 739. Die Verarbeitung zu sta-

grund von Ziel und Zweck der Modellbildung abgelehnt.[182] Die Privilegierung ist darauf zurückzuführen, dass betroffenen Personen keine Risiken drohen, da das Erkenntnisinteresse auf statistische Aussagen, d.h. Aussagen über die abstrakten Datenstrukturen beschränkt ist.[183] Die Modellbildung ist demgegenüber technische Vorstufe für die spätere Profilbildung, sie zielt auf Erkenntnisse über und um Einwirkungen auf die Einzelperson ab.[184] An den generellen Aussagen über die Personengemeinschaft im Trainingsdatensatz hat die verantwortliche Stelle kein Interesse.[185] Ein derartiges striktes Verständnis prägt auch die Artikel 29 Datenschutzgruppe.[186]

---

tistischen Zwecken muss demnach im öffentlichen Interesse liegen, was bei der typischen Big-Data-Verarbeitung durch private Akteure gerade nicht der Fall ist. AA *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 29. Ebenso *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 17 (2016), 315, 322 f., 326 f.; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 288 sowie Gola, DS-GVO/*Schulz*, Art. 6 Rn. 149; *Lorentz*, Profiling, 2019, S. 306, die darauf hinweisen, dass Art. 5 Abs. 1 lit. b), Art. 89 Abs. 2 DSGVO – anders als Art. 89 Abs. 3 DSGVO – eine Beschränkung auf ein öffentliches Interesse nicht vorsehen.

[182] Das Auswertungsverfahren durch Maschinelle Lernverfahren erfolgt anhand statistischer Methoden. Eingehend *Finck/Biega*, Technology and Regulation 2021, 44, 52. So auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 122.

[183] So Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 104; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 52.

[184] Vgl. auch *Lorentz*, Profiling, 2019, S. 306 f.; *Finck/Biega*, Technology and Regulation 2021, 44, 52; *Forgó/Hänold/Schütze*, in: Corrales/Fenwick/Forgó (Hrsg.), New Technology, Big Data and the Law, 2017, S. 17, 40.

[185] Ebenso *Lorentz*, Profiling, 2019, S. 306 f. Zwischen genereller Marktanalyse – hier greift die Privilegierung – und Profiling-Maßnahmen – hier greift sie nicht – unterscheidet auch die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 28, 45, wenngleich ganz generell für Big-Data-Analysen. Dies befürwortet *Richter*, DuD 39 (2015), 735, 739. Explizit: *ders.*, DuD 40 (2016), 581, 584: „Die Privilegierung darf auch auf solche Verarbeitungen nicht angewendet werden, bei denen eine konkrete personenbezogene Anwendung zwar nicht geplant, aber das Ziel der statistischen Auswertungen ist". Zum selben Ergebnis hinsichtlich Big-Data-Analysen, die Grundlage für Profilbildungen sind, kommen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 104; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Tinnefeld*, Art. 89 Rn. 15a; *Zarsky*, Setton Hall Law Review 47 (2017), 995, 1008; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 288.

[186] Vgl. *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 28. Als Beispielsfall benennt sie Big-Data-Auswertungen zur allgemeinen Marktanalyse, die der Ausnahmebestimmung unterfallen. *dies.*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 29. In diese Richtung auch *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 32. Ebenso *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 17 (2016), 315, 323, die differenzieren zwischen Modellbildung für die Profilerstellung – hier gilt die Ausnahme nicht – und Modellbildung für Aussagen zum Kundenstamm insgesamt – hier gilt die Ausnahme.

(2) Vorliegen einer Zweckänderung im engeren Sinne

Für die Kompatibilitätsbewertung ist zwischen den einzelnen oben beschriebenen Konstellationen der Zweckänderung[187] zu unterscheiden.

Entscheidender Punkt für die Kompatibilität ist vor allem die Erwartbarkeit der zweckgeänderten Verarbeitung nach Art. 6 Abs. 4 lit. b) DSGVO.[188] Die Umwidmung von Daten zu Trainingsdaten ist typischerweise nicht vorhersehbar. Die NutzerInnen müssen nicht damit rechnen, dass der Verantwortliche die aufgezeichneten Daten zur Verbesserung seiner Dienste nutzt.[189] Auch die anwendungsübergreifende Nutzung der Daten stellt sich in der Regel als überraschend dar. Bereits die Mehrfachverwendung von Trainingsdatensätzen ist für die betroffenen Personen nicht erwartbar.[190] Erst recht müssen betroffene Personen nicht damit rechnen, dass ihre Daten aus anderen Anwendungskontexten, wo sie nicht als Trainingsdaten verwendet wurden, nunmehr als Trainingsdaten dienen.[191] Dies gilt auch bei der Weiterverwendung der Daten zur Personalisierung von Werbemaßnahmen, wie sie beim Geschäftsmodell „Dienst gegen Daten" erfolgt.[192] Wenngleich den NutzerInnen derartiger „kostenloser" Dienste in der Regel klar ist, dass sie den Dienst durch die Hingabe

---

[187] Siehe Kapitel 4 C. III. 1. a) bb) am Anfang.

[188] Siehe zu den einzelnen Kriterien des Kompatibilitätstests oben Kapitel 4 C. II. 1. b) aa).

[189] Denn mit der Verwendung der Daten zur bloßen Verbesserung eines Dienstes muss die betroffene Person nicht rechnen, erst recht nicht mit der Verwendung ihrer Daten für Maschinelle Lernverfahren im Interesse des Verantwortlichen. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 37, siehe explizit zur Optimierung von SmartHome-Anwendungen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 37; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 247 sowie von Shopping-Assistenten *Finck/Biega*, Technology and Regulation 2021, 44, 49 f. Ist von Anfang an bekannt, dass es sich um ein autonomes System im Sinne dieser Arbeit handelt, ist dies schon keine Zweckänderung, jedenfalls wäre aber die Weiterverarbeitung erwartbar im Sinne des Art. 6 Abs. 4 lit. d) DSGVO, so auch Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 Rn. 247. Einen ähnlichen Fall beschreibt Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 37 für selbstlernende Systeme: Den NutzerInnen dürfte bekannt sein, dass ihre Daten für die Funktionsweise der Systeme eingesetzt werden.

[190] Siehe hierzu eingehend *Lorentz*, Profiling, 2019, S. 313 f. Vgl. auch *Finck/Biega*, Technology and Regulation 2021, 44, 49 f.

[191] Vgl., wenngleich nicht klar zwischen den verschiedenen Arten der Zweckänderung differenzierend, *Lorentz*, Profiling, 2019, S. 314. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 51; *Kugelmann*, DuD 40 (2016), 566, 568; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 249, die allerdings nicht zwischen Modell- und Profilbildung unterscheiden und allgemein auf die Profilbildung aus Daten aus verschiedenen Anwendungskontexten abstellen.

[192] Siehe hierzu auch unter Kapitel 4 C. III. 2. c), Kapitel 4 C. III. 3 c).

ihrer Daten finanzieren, müssen die NutzerInnen aufgrund der Vielzahl der Kommerzialisierungsmöglichkeiten von Daten nicht damit rechnen, dass ihre Daten gerade für die Personalisierung von Werbung weiterverwendet werden.[193] Aber auch wenn bekannt ist, dass die Dienste werbefinanziert sind, kann sich die Weiterverwendung der Daten dennoch als überraschend darstellen, nämlich dann, wenn der Verantwortliche diese für die Bewerbung von Produkten oder Diensten nutzt, die mit den ursprünglich bereitgestellten nichts zu tun haben.[194] So kann ein Kosmetikproduktehersteller die Daten, bei entsprechendem Hinweis, für personalisierte Werbung hinsichtlich Kosmetika nutzen, nicht aber für personalisierte Werbung hinsichtlich Gartengeräten. Der Verantwortliche kann allerdings auf den Erwartungshorizont der betroffenen Personen durch entsprechende Hinweise einwirken.[195] Umgekehrt ist regelmäßig von einer Zweckinkompatibilität auszugehen, wenn der Verantwortliche besondere Vertraulichkeit zugesichert hat.[196] Eine solche Vertraulichkeit(szusicherung) wird die betroffene Person regelmäßig erwarten, wenn das autonome System im intimen Lebensbereich zum Einsatz kommt, etwa bei persönlichen Assistenten, oder wenn besonders sensible Daten verarbeitet werden, etwa bei Gesundheits-Apps.[197]

Wechseln die Daten durch Dateneinkäufe auf dem Markt von einem Verantwortlichen zu einem anderen und damit regelmäßig aus einem Verarbeitungskontext in einen anderen,[198] handelt es sich typischerweise um eine Zweckän-

---

[193] Siehe, wenn auch recht allgemein, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 38; *Finck/Biega*, Technology and Regulation 2021, 44, 49. Vgl., wenngleich ohne Differenzierung zwischen Modell- und Profilbildung, Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 55; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 77. AA Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Klein*, Art. 6 Abs. 1 lit. f) Rn. 170, die die Weiterverwendung der Daten für Werbemaßnahmen für erwartbar halten und daher keinen expliziten Hinweis auf die Weiterverwendung für personalisierte Werbemaßnahmen fordern.

[194] Vgl. *Lorentz*, Profiling, 2019, S. 314. In diese Richtung, wenn auch ohne klare Differenzierung zwischen Modell- und Profilbildung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 37; *Finck/Biega*, Technology and Regulation 2021, 44, 49 f.

[195] Siehe allgemein Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 Rn. 248; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 77. Vgl. für die eine Zweckkompatibilität herstellende Offenlegung der Weiterverwendung für personalisierte Werbemaßnahmen *Lorentz*, Profiling, 2019, S. 314; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 Rn. 246.

[196] So Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 187.

[197] Siehe zum Beispiel der Gesundheits-App Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 246, 248.

[198] Der Aspekt, dass der Verantwortliche wechselt, ist für die Zweckbindung irrelevant, da es beim Zweckfestlegungsgrundsatz allein um den übergeordneten Zweck der Verarbei-

derung im engeren Sinne: Die Weiterverwendung durch den (neuen) Verantwortlichen als Trainingsdaten, zudem in einem ganz anderen Verarbeitungskontext, ist für die betroffenen Personen nicht vorhersehbar.[199]

Ist die Weiterverwendung vorhersehbar, wird die Interessensabwägung im engeren Sinne in der Regel zur Kompatibilität der Zweckänderung führen, denn die Modellbildung bleibt in der Regel ohne Konsequenzen für die im Modelldatenset repräsentierten Personen.[200] Das Modell zeigt noch keine Außenwirkung, dies erfolgt erst durch die spätere Profilbildung und -verwendung. Im Übrigen werden Profile nicht für sämtliche Personen, deren Daten im Modell verwendet werden, gebildet, es sind also nicht sämtliche im Modell repräsentierten Personen gefährdet. Der Verantwortliche kann sich zusätzlich durch technische Maßnahmen, etwa durch Pseudonymisierung oder Anonymisierung, absichern.[201]

Im Ergebnis ist die Umwidmung von Daten bzw. Mehrfachverwendung von Trainingsdatensets bei entsprechendem Hinweis des Verantwortlichen in der Regel zulässig. Allein der Anreicherung des Trainingsdatensets durch Zukauf von Daten unterschiedlichster Herkunft setzt der Zweckbindungsgrundsatz Grenzen.

(3) Zulässigkeit der Zweckänderung

Sofern eine Zweckinkompatibilität vorliegt, kann diese durch Einwilligung der betroffenen Person gerechtfertigt werden. Die Anforderungen an die Wirksamkeit der Einwilligung entsprechen den allgemeinen Bedingungen.[202] Der Verantwortliche muss dann also sämtliche in einem Datensatz repräsentierten Per-

---

tung geht, der dann auch mehrere Verantwortliche einschließen kann. Siehe hierzu Gola, DS-GVO/*Schulz*, Art. 6 Rn. 135.

[199] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 190. Siehe auch *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 85. Spezifisch für die Weiterverwendung der Daten durch Dritte für Werbezwecke Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 Rn. 246.

[200] Vgl. auch *Lorentz*, Profiling, 2019, S. 303, 314. Vgl. auch Gola, DS-GVO/*Schulz*, Art. 6 Rn. 140, demzufolge die Weiterverwendung der Daten für Profilbildungen bei entsprechendem Hinweis mit der Primärverarbeitung vereinbar sein kann. E contrario und erst recht muss dann die Modellbildung mit dem Primärverarbeitung vereinbar sein.

[201] So auch, wenngleich allgemein zu Big-Data-Analysen Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 Rn. 290; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 63; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 289. Vgl., obschon im Rahmen des Art. 6 Abs. 1 lit. f) DSGVO hinsichtlich der Modellbildung, *Lorentz*, Profiling, 2019, S. 302 f.

[202] Siehe ausführlich zur Einwilligung im Rahmen der Zweckänderung bei Maschinellen Lernverfahren *Finck/Biega*, Technology and Regulation 2021, 44, 52–54, die darin eine „silver bullet" zur Umgehung des Zweckbindungsgrundsatzes erkennen. Ähnlich kritisch *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 254.

sonen identifizieren und kontaktieren und für jeden weiteren Verarbeitungsprozess eine eigenständige bzw. überarbeitete Datenschutzerklärung anbieten und Einwilligungen einholen.[203] Sieht man in Art. 6 Abs. 4 DSGVO lediglich eine zweckspezifische Vorschrift, bedarf es zusätzlich einer eigenen Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO für die kompatible bzw. inkompatible, dann aber zulässige zweckändernde Weiterverarbeitung.[204]

b) Einwilligung

Um die Datenverarbeitung über die Einwilligung rechtfertigen zu können, bedarf es hinreichender Informationen. Aufgrund des geringen Gefährdungspotentials auf Stufe der Modellbildung sind die Anforderungen abgesenkt. Für eine Einschätzung der Bedeutung und Folgen der Einwilligung ist es ausreichend, dass die betroffene Person über das zweistufige Profilbildungsverfahren und die Bedeutung des Modells darin informiert wird, im Übrigen auf den übergeordneten Verwendungszweck hingewiesen wird.[205] Eine derartige Information ist dann bereits im Rahmen der Zweckbestimmung erfolgt. Auch auf Stufe der Einwilligung ist es demnach irrelevant, wenn die betroffene Person die einzelnen Modellinhalte bei Maschinellen Lernverfahren nicht prognostizieren kann, da aus diesen keine Gefährdungen für die betroffene Person drohen.[206]

c) Vertragsimmanente Zulassung

Eine Rechtfertigung der Modellbildung im Rahmen des Art. 6 Abs. 1 lit. b) DSGVO kommt nur in Betracht, wenn die vorvertragliche Maßnahme, der Vertragsschluss oder der Vertragsgegenstand selbst die Modellerstellung, d.h. das zweistufige Profilbildungsverfahren, erfordert. Der strenge Maßstab der Erforderlichkeit lässt eine bloße Nützlichkeit nicht ausreichen. Ist allein die Automatisierung der vorvertraglichen Maßnahme des Vertragsgegenstands verein-

---

[203] Vgl. *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 285; *Culik/Döpke*, ZD 7 (2017), 226, 228.

[204] Siehe hierzu oben Kapitel 4 C. II. 1. b) bb).

[205] Ebenso *Lorentz*, Profiling, 2019, S. 302. Ähnlich *Gausling*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 379, Rn. 20–22.

[206] Vgl. *Tupay/Ebers/Juksaar u.a.*, Juridica International 30 (2021), 99, 102; *Zarsky*, Seton Hall Law Review 47 (2017), 995, 1006 f. Vgl., wenngleich allgemein zu Big-Data-Analysen, *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 51 f. Sehr viel weitergehend, wenngleich nicht explizit auf den Informationsbedarf im Rahmen der Einwilligung eingehend, die *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 6 für die Nutzung von personenbezogenen Daten für das Algorithmentraining durch ChatGPT, wonach den betroffenen Personen Informationen „on how the processing is carried out, the logic underlying the processing that is necessary for the operation of the service" bereitzustellen sind.

bart, ist dies noch nicht eine Erforderlichkeit im Sinne des Art. 6 Abs. 1 lit. b) DSGVO, da diese auch ohne Personalisierung möglich ist.[207] Aber auch eine vereinbarte Personalisierung macht die Modellbildung noch nicht erforderlich, da die Profilbildung auch einstufig erfolgen kann.[208] Die Modellbildung dient daher überwiegend allein der Optimierung und Effektivierung der Automatisierung bzw. der Personalisierung und ist damit nicht erforderlich im Sinne des Art. 6 Abs. 1 lit. b) DSGVO.[209] Nur wenn es gelingt, darzulegen, dass eine vorvertragliche Maßnahme, der Vertragsschluss oder der Vertragsgegenstand nur über die zweistufige Profilbildung möglich und die Verarbeitung der Daten für die Modellbildung auch notwendig ist, ist eine Rechtfertigung nach Art. 6 Abs. 1 lit. b) DSGVO denkbar.[210]

---

[207] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 17 f. In der Tendenz auch ablehnend Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 56 – *Meta Platforms Inc. u.a./Bundeskartellamt*. Siehe zu diesem Argument auch *Finck/Biega*, Technology and Regulation 2021, 44, 50, die dies – dort im Rahmen der Zweckbestimmung – am Beispiel von personalisierten Suchmaschinen erläutern. Auch über andere algorithmische Verfahren können die Systeme automatisiert werden und erzielen dabei gute Ergebnisse. Für die Zweckbestimmung bedeutet dies, dass Zweck der Datenverarbeitung der Profilbildung nur die Optimierung, nicht die Bereitstellung des Dienstes ist. Siehe hierzu bereits bei der Zweckbestimmung Kapitel 4 C. III. 1. a) aa).

[208] Vgl. allgemein für Big-Data-Auswertungen im vertraglichen Verhältnis *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 01.03.2017, S. 35; Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 37–38. Vgl. auch Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Wedde*, Art. 6 Rn. 67, demzufolge die abstrakte Analyse des Browsing-Verhaltens von NutzerInnen in keinem Zusammenhang mit konkreten Leistungspflichten steht.

[209] Spezifisch zur Modellbildung *Lorentz*, Profiling, 2019, S. 301. Allgemein zur Big-Data-Analyse *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 15. Vgl. auch allgemein zur Differenzierung von Optimierung und Erforderlichkeit Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 36; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 64. Die Erforderlichkeit ablehnend für Big-Data-Auswertungen im Rahmen des Kredit-Scorings Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 42.

[210] Angedeutet bei Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 38: „Solange beiden Vertragsparteien (und insbesondere freilich der betroffenen Person) transparent bewusst ist, welchen Vertrag sie schließen und welche Datenverarbeitungsvorgänge damit einhergehen, können auch die Vertragszwecke nach der hier vertretenen Auffassung grundsätzlich beliebig frei gewählt werden". In diese Richtung, wenngleich zu Big-Data-Analysen, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 41: „Rahmenverträge mit allgemeinen Zweckbestimmungen". Die Personalisierung allein macht noch nicht jede Datenverarbeitung erforderlich. Insbesondere die Verarbeitung auch dienstexterner Daten für die Bereitstellung eines personalisierten Dienstes ist in der Regel nicht erforderlich. Vgl.

Für personalisierte Werbemaßnahmen ist eine Rechtfertigung der Modellbildung über Art. 6 Abs. 1 lit. b) DSGVO ausgeschlossen.[211] Die Modellbildung lässt sich auch nicht mit dem Hinweis auf das datenbasierte Geschäftsmodell der verantwortlichen Stelle rechtfertigen. Dass ein Dienst ohne die Verwendung der Daten nicht wirtschaftlich sinnvoll erbracht werden kann, genügt für die Anwendung des Art. 6 Abs. 1 lit. b) DSGVO nicht.[212] Vor allem das Geschäftsmodell „Dienst gegen Daten"[213] lässt sich daher nach der überwiegenden Ansicht nicht nach Art. 6 Abs. 1 lit. b) DSGVO rechtfertigen.[214] Der Verantwortliche kann, so der Europäische Datenschutzausschuss[215] und die

---

auch Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 56–57 – *Meta Platforms Inc. u.a./Bundeskartellamt*.

[211] Dabei explizit auch zur Modellbildung *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 17.

[212] So ausdrücklich *ders.*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 16. Siehe auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 46. Im Übrigen bedient die Vorschrift allgemeine kommerzielle Interessen der verarbeitenden Stelle nicht, andernfalls könnte die verarbeitende Stelle den Rechtfertigungstatbestand des Art. 6 Abs. 1 lit. b) DSGVO missbräuchlich für die Durchsetzung eigener Interessen nutzen. In einer datenkapitalisierten Welt würde die Vorschrift letztlich ausgehöhlt. Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 40a. Dies gilt insbesondere für Datenauswertungen für personalisierte Werbung, die einen Dienst wirtschaftlich tragen soll, vgl. Kühling/Buchner, DS-GVO, BDSG/*dies.*, Art. 6 Rn. 64. Siehe hierzu auch *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 151–153.

[213] Siehe bereits oben Kapitel 4 C III. 1. a) bb) (2).

[214] Ablehnend etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 33; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 41; Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 46. Ablehnend auch *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 16 f. Dagegen auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 267–268, 303, der darauf verweist, dass die synallagmatischen Verhältnisse beim Geschäftsmodell „Dienst gegen Daten" nicht geradlinig sind. Der Verantwortliche finanziert seinen Dienst über den Verkauf von Werbeplätzen, die aufgrund der Personalisierung der Werbung und von direkten und indirekten Netzwerkeffekten besonders lukrativ sind. Die betroffenen Personen ermöglichen dieses Geschäftsmodell insgesamt, indem sie sich auf den sozialen Netzwerken registrieren und ihre Daten für die Personalisierung von Werbung hingeben. Ausgetauscht werden also nicht – im Sinne eines Synallagmas – Dienst gegen Daten, sondern Dienst gegen Aufrechterhaltung dieses gesamten Finanzierungssystems. Die Zulässigkeit des Datenhandels wirft vielfältige Problematiken auf, die allerdings jenseits des Forschungsauftrags dieser Arbeit liegen.

[215] *Europäischer Datenschutzausschuss*, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65

überwiegende Ansicht in der Literatur,[216] auch nicht durch entsprechende Vereinbarung sein datengetriebenes, in der Regel dann werbebasiertes Geschäftsmodell zum Vertragsgegenstand machen.

Aufgrund der synallagmatischen Verknüpfung des Art. 6 Abs. 1 lit. b) DSGVO könnten ohnehin nur die Verarbeitungen der Daten der betroffenen Person, für die die vorvertragliche Maßnahme, der Vertrag oder der Vertragsgegenstand bereitgestellt wird, gerechtfertigt werden, nicht aber die Verarbeitung der Daten Dritter.[217] Die Rechtfertigung ist also nur möglich, wenn für die Person, deren Daten bei der Modellbildung verarbeitet werden, auch ein Profil erstellt wird und eine Profilverwendungsmaßnahme erfolgt.

Im Ergebnis kommt der vertragsimmanenten Zulassung bei der Modellbildung geringe Bedeutung zu.

GDPR), 05.12.2022, Rn. 111–133, der das Argument von Meta zurückwies, die personalisierte Werbung sei Teil der vertragsgemäßen Leistung. Mit eingehender Kritik hierzu *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3–16 So auch bereits *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 22; *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 16 f.

[216] Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 40a; Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 46; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 289. Befürwortend dagegen *Nettesheim*, EU Law Live Februar Weekend Edition (2023), 3, 13–16, außer im Falle missbräuchlichen Verhaltens. Die Zulässigkeit dieser datengetriebenen Geschäftsmodelle ist Gegenstand kontroverser Debatte, die hier nicht im Einzelnen nachvollzogen werden kann. Im Kern geht es dabei auch um die Frage, ob der Einwilligung gegenüber anderen Zulassungsgründen ein Vorrang einzuräumen ist, siehe hierzu Kapitel 4 C. II. 6. Eine abschließende Entscheidung des EuGH steht noch aus. Zu einem anhängigen Vorlageverfahren betreffend das Verhältnis der Rechtmäßigkeitstatbestände bei werbebasierten Geschäftsmodellen siehe Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 46. Ablehnend hinsichtlich der Rechtfertigung einer vertraglichen Vereinbarung „Dienst gegen Daten" über Art. 6 Abs. 1 lit. b) DSGVO äußert sich Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 57, 63–64 – *Meta Platforms Inc. u.a./Bundeskartellamt*.

[217] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 91; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 40a. Diese synallagmatische Verknüpfung ist auch der Grund, weshalb die Verwendung von aus dem Internet bezogenen Daten für das Maschinelle Lernverfahren nicht auf den Rechtfertigungsgrund des Art. 6 Abs. 1 lit. b) DSGVO gestützt werden kann. So auch, wenngleich hinsichtlich des Trainingsverfahrens für einen Lösungsalgorithmus (dort für ChatGPT), *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 6; *Garante per la protezione dei dati personali*, Comunicato del 31 marzo 2023, 31.03.2023.

d) Berechtigte Interessen

Das Interesse des Verantwortlichen an der Modellbildung liegt in der Optimierung und Effektivierung der Methodik automatisierter Profilbildung und -verwendung.[218] Während bei personalisierten Anwendungen wie Informationsfilterungen die Erhöhung der Kundenzufriedenheit entscheidend ist,[219] dienen automatisierte Vertragsgestaltungen der Verbesserung der Verhandlungsposition,[220] die personalisierte Werbung einer besonders effektiven Ansprache neuer Kunden.[221] All dies sind ökonomische Erwägungen, die im Sinne des Art. 6 Abs. 1 lit. f) DSGVO berücksichtigungsfähig sind.[222]

Auf Seiten der betroffenen Personen gestaltet sich die Benennung konkreter Interessen schwierig, da das Modell keine Aussagen über Einzelpersonen trifft und auch keine Außenwirkung zeigt.[223] Gruppeninteressen sind in der individualistischen Perspektive der DSGVO nicht berücksichtigungsfähig.[224] Etwaige auf Stufe der Modellbildung angelegten Risiken, etwa Diskriminierungen, Verzerrungen oder sonstige Fehleranfälligkeiten, können erst bei der Profilbildung Berücksichtigung finden.[225] Allein privatheitsbezogene oder datenschutz-

---

[218] Eingehend *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 277 f. Ähnlich *Lorentz*, Profiling, 2019, S. 302.

[219] Kritisch dagegen Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 66 – *Meta Platforms Inc. u.a./Bundeskartellamt*, demzufolge die Produktverbesserung eher dem Interesse der betroffenen Person dient. Er verkennt dabei, dass ein verbessertes Produkt für den Kunden attraktiv(er) ist und damit einen erhöhten ökonomischen Wert hat. Insoweit kann die Produktverbesserung im Interesse des Verantwortlichen liegen.

[220] Vgl. zum Kredit-Scoring Gola, DS-GVO/*Schulz*, Art. 6 Rn. 103. Auch hier kann die Kundenzufriedenheit ein maßgeblicher Aspekt sein, wenn die Verträge an die Bedürfnisse der Kunden angepasst werden und Frustrationen vermieden werden, siehe eingehend Gola, DS-GVO/*ders.*, Art. 6 Rn. 104.

[221] Dieses Interesse ist in Erwägungsgrund 47 S. 7 explizit anerkannt. Siehe hierzu auch Paal/Pauly, DS-GVO/*Frenzel*, Art. 6 Rn. 28; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 53.

[222] Das Interesse an den Daten selbst bzw. der Datenverarbeitung genügt nicht, es bedarf stets eines über die technische Funktionsfähigkeit hinausgehenden Interesses. Geschützt ist daher das wirtschaftliche Interesse an der weiteren Vermarktung oder ökonomischen Verwertung der Daten. Vgl. Gola, DS-GVO/*Schulz*, Art. 6 61. Die Nutzung der Datenverarbeitung für Direktwerbung ist sogar in Erwägungsgrund 47 S. 7 als berechtigtes Interesse explizit aufgeführt. Das Interesse der Direktwerbung erfasst sämtliche hierfür notwendige Datenverarbeitungsphasen, sowohl die Erhebung als auch die Selektion von Kunden sowie die Ansprache, vgl. Gola, DS-GVO/*ders.*, Art. 6 Rn. 71, und ist damit sowohl für die Modell- als auch Profilbildung als auch Profilverwendung relevant.

[223] Vgl. eingehend *Lorentz*, Profiling, 2019, S. 303 f. So auch *Roßnagel*, ZD 3 (2013), 562, 564.

[224] Ausführlich hierzu *Lorentz*, Profiling, 2019, S. 303 f.; *Edwards/Veale*, SSRN Journal 2017, 35 f.

[225] So auch *Lorentz*, Profiling, 2019, S. 303.

rechtliche Interessen der betroffenen Personen sind daher relevant, d.h. deren Interesse am Schutz der im Rahmen der Modellbildung verarbeiteten personenbezogenen Daten.[226]

aa) Erforderlichkeit und Erwartbarkeit

Die Datenverarbeitungen sind für die Wahrung der Interessen des Verantwortlichen erforderlich, denn das Maschinelle Lernverfahren im Rahmen der Modellbildung bedarf einer Vielzahl von Daten, kann also auf andere Weise nicht erfolgen.[227] Ob die Verwendung der Daten für die Modellbildung vorhersehbar und erwartbar ist, bestimmt sich nach den Einzelfallumständen. Typischerweise wird man eine entsprechende Aufklärung der betroffenen Person verlangen müssen, da diese nicht damit rechnen muss, dass ihre im Rahmen eines Dienstes hingegebenen Daten für die generelle Verbesserung eines Systems und also für die Modellbildung verwendet werden.[228] Erst recht mit der Verarbeitung von Daten jenseits des Dienstes muss die betroffene Person nicht rechnen.[229] Fragen der Erwartbarkeit stellen sich vor allem im Hinblick auf personalisierte Werbemaßnahmen; Erwägungen im Hinblick auf die Zweck(in)kom-

---

[226] So ist insbesondere zu berücksichtigen, wenn Daten mit besonders sensiblem oder intimem Gehalt verarbeitet werden, vgl. allgemein für SmartHome-Anwendungen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 121–122. Siehe für das Werbe-Scoring Gola, DS-GVO/*Schulz*, Art. 6 Rn. 73, 77. Vgl. auch *Lorentz*, Profiling, 2019, S. 302 f.

[227] Ebenso *Lorentz*, Profiling, 2019, S. 302. Allgemein für die Big-Data-Auswertung Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 70. Dass Profilbildungen auch einstufig möglich sind, die Modellbildung also für die Profilbildung nur nützlich ist, ist dagegen irrelevant. Denn es geht gerade um das Interesse des Verantwortlichen an vertieften Erkenntnissen über die betroffenen Personen, die gerade nur über die Modellbildung möglich sind.

[228] Vgl. eingehend, dort allgemein zur Big-Data-Analyse, *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 279. Vgl. zum Anwendungsbeispiel des SmartHomes Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 121.

[229] Dies steht dann auch dem „Scraping" von personenbezogenen Internetdaten für das Trainingsverfahren entgegen. Betroffene Personen müssen nicht damit rechnen, dass ihre Daten, auch solche, die im Internet frei verfügbar sind, für Trainingsverfahren bestimmter Anwendungen eingesetzt werden. Siehe hierzu österreichischen Datenschutzbehörde hinsichtlich Clearview AI, *Österreichische Datenschutzbehörde*, Datenschutzbeschwerde Clearview AI, 9.5.2023, S. 25. Vgl. auch die Entscheidungen der italienischen Datenschutzbehörde hinsichtlich ChatGPT *Garante per la protezione dei dati personali*, Provvedimento del 30 marzo 2023, 30.03.2023; *Garante per la protezione dei dati personali*, Comunicato del 31 marzo 2023, 31.03.2023. Auch mit dem Abgreifen dienstexterner Daten für die Verbesserung eines Dienstes muss die betroffene Person nicht rechnen, selbst dann nicht, wenn der Dienst kostenfrei zur Verfügung gestellt wird, siehe Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 56 – *Meta Platforms Inc. u.a./Bundeskartellamt*.

patibilität der (Mehrfach-)Verwendung von Daten für Werbemaßnahmen[230] lassen sich vielfach übertragen.[231]

bb) Interessensabwägung im engeren Sinne

Auf Stufe der Modellbildung ist die Beeinträchtigungswirkung gering, da es hierbei gar nicht um das Einzeldatum und Erkenntnisse über die Einzelperson geht.[232] Interessen betroffener Personen sind allein dadurch gefährdet, dass überhaupt personenbezogene Daten verarbeitet werden und hierdurch datenverarbeitungstypische Risiken ausgelöst werden können. Relevant für die Interessensabwägung ist dann, dass für die Modellbildung große Datenmengen,[233] im Übrigen, wenn besonders sensible Daten[234] verarbeitet werden. Der Verantwortliche kann sich aber absichern, indem er die verarbeiteten Daten pseudonymisiert.[235] In der Regel wird sich die Datenverarbeitung im Rahmen der Modellbildung, sofern diese für die betroffene Person erwartbar ist, über Art. 6 Abs. 1 lit. f) DSGVO rechtfertigen lassen.

e) Verhältnis der Zulassungsgründe

Art. 6 Abs. 1 lit. b) DSGVO spielt in der Praxis, wie beschrieben, kaum eine Rolle. Die Einholung einzelner Einwilligungen für die Modellbildung kann für

---

[230] Siehe oben Kapitel 4 C. III. 1. a) bb) (2).

[231] Dort wie hier wird die betroffene Person ohne einen entsprechenden Hinweis nicht erwarten, dass die im Rahmen einer Vertragsgestaltung oder -erfüllung erhobenen Daten für die Modellbildung für personalisierte Werbung verwendet werden. Eingehend zu entsprechenden Informationspflichten bei der personalisierten Werbung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6 Rn. 31–33.

[232] So auch *Lorentz*, Profiling, 2019, S. 303 f. Siehe auch *Roßnagel*, ZD 3 (2013), 562, 565 („statistisches Auswerten von Big Data").

[233] Vgl., wenngleich nicht spezifisch zur Modellbildung, Gola, DS-GVO/*Schulz*, Art. 6 Rn. 63, sowie spezifisch zum Werbe-Scoring Gola, DS-GVO/*ders.*, Art. 6 Rn. 77. Siehe hierzu auch das Verfahren der italienischen Datenschutzbehörde gegen ChatGPT hinsichtlich der Nutzung sämtlicher verfügbar Daten von NutzerInnen und Nicht-NutzerInnen für das Algorithmentraining durch OpenAI *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 6; *Garante per la protezione dei dati personali*, Comunicato del 31 marzo 2023, 31.03.2023; *Garante per la protezione dei dati personali*, Provvedimento del 30 marzo 2023, 30.03.2023.

[234] Siehe zu den verschiedenen Kriterien, die im Rahmen von Big-Data-Analysen berücksichtigt werden können, *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 278 f.; *Weichert*, ZD 3 (2013), 251, 257.

[235] Vgl. allgemein Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 114–115; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 154, siehe auch für Tracking-Verfahren *Lorentz*, Profiling, 2019, S. 281, allgemein für die Big-Data-Verarbeitung Gola, DS-GVO/*Schulz*, Art. 6 Rn. 152, 155. Explizit für die Modellbildung *Lorentz*, Profiling, 2019, S. 302 f.

den Verantwortlichen technisch oder wirtschaftlich überfordernd[236] wirken und macht damit den Rechtfertigungsgrund des Art. 6 Abs. 1 lit. a) DSGVO unattraktiv.[237] Gerade für die Modellbildung für personalisierte Werbemaßnahmen rückt daher Art. 6 Abs. 1 lit. f) DSGVO in den Fokus.[238] Eine Berufung auf diesen Rechtfertigungsgrund erscheint angemessen. Denn die Risiken auf Stufe der Modellbildung sind für die betroffene Person gering, sie wird in der Tendenz auch nicht mit der Abfrage ihrer Einwilligung rechnen.[239] Demgegenüber hat der Verantwortliche ein besonderes Interesse an der Verbindlichkeit der Zulassung, da er bei Widerruf die Daten einer betroffenen Person aus dem Trainingsdatensatz löschen müsste, was in technischer und ökonomischer Sicht anspruchsvoll, mitunter sogar unmöglich ist.[240]

f) Ergebnis

Für die Modellbildung muss in der Zweckbeschreibung auf das zweistufige Profilbildungsverfahren hingewiesen werden und ein Bezug zum konkreten Anwendungskontext hergestellt werden. Zweckänderungen sind aufgrund des geringen Risikos für betroffene Personen in der Regel zulässig, es bedarf aber eines Hinweises der Verantwortlichen an die betroffene Person, dass die Daten den Verarbeitungskontext wechseln. Zudem empfiehlt sich die Pseudonymisierung der Trainingsdaten. Ein statistisches Verfahren im Sinne des Art. 5 Abs. 1 lit. b) HS. 2 DSGVO stellt die Modellbildung nicht dar.

Die Datenverarbeitungen im Rahmen der Modellbildung werden überwiegend durch die Einwilligung sowie die Interessensabwägung gerechtfertigt. Die vertragsgemäße Zulassung ist nur denkbar, wenn das zweistufige Profilbildungsverfahren funktionsnotwendig ist, zwischen den Parteien vereinbart wurde und zusätzlich für die Person, die ihre Daten für die Modellbildung hingibt, späterhin auch Profilbildungs- und Profilverwendungsmaßnahmen erfol-

---

[236] Siehe zur Überforderung im Hinblick auf die Einwilligung auch *Hackenberg*, in: Hoeren/Sieber/Holznagel u.a. (Hrsg.), Handbuch Multimedia-Recht, [58]2022, 42; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 40.

[237] So auch, wenngleich zur Big-Data-Anaylse, *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 275 f. Ebenso *Paal/Hennemann*, NJW 70 (2017), 1697, 1700; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 275 f.

[238] So auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6 Rn. 9.

[239] Siehe zu diesem Merkmal oben Kapitel 4 C. II. 6.

[240] Eingehend zu den nachteiligen Folgen eines Widerrufs für das Maschinelle Lernverfahren *Humerick*, Santa Clara High Technology Law Review 34 (2018), 393, 406 f. Auch der österreichischen und italienischen Datenschutzbehörde zufolge kann das Maschinelle Lernverfahren, hier dann zur Erstellung eines Lösungsalgorithmus, prinzipiell auf die Interessensabwägung gestützt werden, vgl. *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 7; *Österreichische Datenschutzbehörde*, Datenschutzbeschwerde Clearview AI, 09.05.2023, S. 24 f.

gen. Aufgrund des geringen Gefährdungspotentials der Modellbildung sind an die Rechtfertigung keine allzu hohen Anforderungen zu stellen. Für die Einwilligung ist eine vertiefte Erläuterung des technischen Prozesses nicht erforderlich, auch Prognosen zu möglichen Modellinhalten bedarf es nicht. Die Interessensabwägung führt in der Regel nicht zu einem Überwiegen der Interessen der betroffenen Person. Wichtig ist allerdings, dass der Verantwortliche durch entsprechende Hinweise sicherstellt, dass für die betroffene Person die Modellbildung nicht überraschend ist. Über Pseudonymisierung der Trainingsdaten können sich Verantwortliche zusätzlich absichern. Die Modellbildung wird daher in der Tendenz zulässig sein. Aufgrund des geringen Risikos und dem besonderen Interesse des Verantwortlichen an der Dauerhaftigkeit der Zulassung der Datenverarbeitung kann der Verantwortliche frei zwischen den Zulassungsgründen wählen.

2. Profilbildung: Verarbeitung von Anwendungsdaten durch selbstlernende Algorithmen

Bei der Profilbildung erfolgt eine Datenanalyse durch den zuvor im Modell erstellten selbstlernenden Algorithmus. Auch hier ergeben sich Schwierigkeiten hinsichtlich des Zweckfestlegungsgrundsatzes (a)), herausfordernd sind hier aber vor allem Fragen der Zulässigkeit über die Einwilligung (b)), die vertragsimmanente Zulassung (c)) und die Interessensabwägung (d)).

a) Zweckfestlegungsgrundsatz bei der Profilbildung

Komplex gestaltet sich bei der Profilbildung die präzise Bestimmung des Zwecks. Auch bei der Profilbildung kann es zu Zweckänderungen kommen. Typisch ist vor allem die Verwendung von Daten aus Vertragszusammenhängen zur Erstellung von Werbeprofilen.[241] Die hierdurch aufgeworfenen Fragen berühren nicht im Kern Regulierungsfragen autonomer Systeme,[242] sie sollen im Weiteren daher nicht erörtert werden.[243]

---

[241] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 10 f. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 38, 40.

[242] Anders als bei der Modellerstellung, bei der Maschinelle Lernverfahren zum Einsatz kommen, besteht bei der Profilbildung kein erhöhter Datenbedarf. Denn der besondere Wert des zweistufigen Profilbildungsverfahrens liegt ja gerade darin, dass auf Grundlage nur sehr eingeschränkter Informationen über eine betroffene Person vertiefte Erkenntnisse gewonnen werden können.

[243] Siehe zu Fragen der Zweckänderung bei der Profilbildung etwa *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 11 f. Siehe auch

Bei der Zweckbestimmung hinsichtlich der Profilbildung gilt, wie auch bei der Modellbildung, dass nicht der technische Prozess, sondern das übergeordnete Motiv für die Profilbildung benannt werden muss. Unklar ist, was dann der eigentliche übergeordnete Zweck ist. Dem Europäischen Datenschutzausschuss zufolge ist es die Erkenntnis über die betroffene Person selbst, also die Bewertung, Analyse oder Prognose. Das Profiling selbst beschreibt demnach den Zweck.[244] Er stützt sich dabei auf den Umstand, dass der Begriff des Profilings sowohl den technischen Prozess beschreibt als auch im allgemeinen Sprachgebrauch für das übergeordnete Motiv steht, nämlich den Erkenntnisgewinn anhand Bewertung, Prognose oder Analyse von Persönlichkeitsmerkmalen.[245] In der Literatur sieht man den übergeordneten Zweck vielfach allein im Anwendungskontext: Die Profilbildung ist „kein Selbstzweck",[246] sie soll die Personalisierung ermöglichen und zwar eines ganz bestimmten Dienstes, etwa einer Werbemaßnahme. Dieser Anwendungskontext ist in der Zweckbestimmung darzulegen.[247] Die Profilbildung selbst stellt hierzu nur einen technischen Verfahrensschritt dar und ist daher selbst nicht zu benennen. Entsprechend ist in die Zweckbestimmung nur der Anwendungskontext darzulegen, nicht aber aufzunehmen, dass überhaupt eine Profilbildung stattfindet.[248] Explorative Profilbildungsverfahren, bei denen konkrete Anwendungskontexte zunächst offengelassen werden, sind demnach unzulässig.[249] Eine Pflicht zur inhaltlichen Beschreibung der Profilinhalte – und damit Fragen der fehlenden Transparenz – betrifft dagegen Anforderungen der Rechtmäßigkeit bzw. der Transparenz.[250] Aber auch solche Profilbildungen sind unzulässig, die im Ergebnis so fern menschlicher Konsistenzbedingungen liegen, dass sie sich nicht mehr dem übergeordneten Anwendungszweck zuordnen lassen.

Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Abs. 4 246, 248.

[244] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 11. Befürwortend wohl Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 4 Nr. 4 Rn. 6; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 1, 4.

[245] Siehe hierzu *Lorentz*, Profiling, 2019, S. 161.

[246] *Dies.*, Profiling, 2019, S. 162.

[247] Mit ausführlicher Begründung *dies.*, Profiling, 2019, S. 161–163. In diese Richtung Paal/Pauly DS-GVO/*Ernst*, Art. 4 Rn. 36.

[248] *Lorentz*, Profiling, 2019, S. 163–165. Nach dieser Lesart ist dann erst im Rahmen der Rechtmäßigkeit über das Stattfinden einer Profilbildung zu informieren.

[249] Ebenso, wenngleich sehr allgemein, *Roßnagel*, ZD 3 (2013), 562, 564 „Bildung umfassender Profile".

[250] Ebenso *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 61, die die Problematik der Vorhersehbarkeit von Profilinhalten als Problem der Transparenz und der informierten Einwilligung begreift.

b) Einwilligung

Bei der Einwilligung in die Profilbildung ist, neben Fragen der Freiwilligkeit, die in dieser Arbeit nicht untersucht werden sollen,[251] fraglich, welche Anforderungen an die Informiertheit der Einwilligung zustellen sind (aa)). Insbesondere ist unklar, ob über den zu bildenden Profilinhalt vorab zu informieren ist (bb)).

aa) Informiertheit der Einwilligung

Für die Informiertheit der Einwilligung gilt, ebenso wie für die Zweckfestlegung, ein gegenüber der Modellbildung erhöhter Maßstab, da sich hier die Gefährdungslage intensiver darstellt.

Die Artikel 29 Datenschutzgruppe fordert, dass die betroffenen Personen Zugang zu ihren Profilen und der algorithmischen Logik der Profilbildung erhalten sollten.[252] Dies wird überwiegend als zu weitgehend erachtet.[253] Ist der Maßstab für die einwilligungsbezogene Informiertheit, dass die betroffene Person die Folgen ihrer Zulassungsentscheidung einschätzen kann,[254] ist eine Kenntnis der grundlegenden technischen Funktionsweise der Profilbildung ausreichend.[255] Dabei muss deutlich werden, dass ein Erkenntnisgewinn über das Rohdatum hinaus erfolgt und zwar durch den Abgleich mit Erkenntnissen zu Dritten.[256] Insbesondere bedarf es eines Hinweises, dass bereits aus wenigen Anwendungsdaten und auch solchen mit geringem Aussagewert (zB Wohnort) Rückschlüsse auf sensible Persönlichkeitsmerkmale, etwa intimen oder manipulationsaffinem Informationsgehalt (zB Vermögen, Familienstand, emotiona-

---

[251] Eingehend zu Fragen der Freiwilligkeit im Rahmen der Einwilligung in die Profilbildung *Lorentz*, Profiling, 2019, S. 168–176.

[252] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 47.

[253] Kritisch auch *Finck/Biega*, Technology and Regulation 2021, 44, 54, die zudem darauf hinweisen, dass die Artikel 29 Datenschutzgruppe damit sogar über die Anforderungen des Art. 22 DSGVO hinausgeht.

[254] Siehe *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 14.

[255] Eingehend *Lorentz*, Profiling, 2019, S. 182 f. Vgl. auch *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 66: „The DPA does not require the privacy notice to describe how the data is processed (ie, the technical details of how the algorithms work), but the purposes for which it is processed". Ähnlich, wenngleich im Rahmen der Einwilligung in die profilgetragene automatisierte Entscheidung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 54.

[256] So auch *Lorentz*, Profiling, 2019, S. 182. Ebenso *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 7.

ler oder physischer Zustand) möglich sind.[257] Risiken für die betroffene Person entstehen auch aus der Verwendung des Profils zur Aktivierung der automatisierten Entscheidungs- und Steuerungsarchitektur. Auch über die Bedeutung des Profils für die Automatisierungsinfrastruktur autonomer Systeme ist daher aufzuklären.[258] Bei diesen Darlegungen sind jeweils Informationen zu den Einzelheiten des technischen Auswertungsverfahrens nicht erforderlich.

bb) Offenlegung der Profilinhalte

Eine echte Risikoeinschätzung wird der betroffenen Person aber nur möglich sein, wenn ihr bewusst ist, mit welchen Ableitungen von Persönlichkeitsmerkmalen sie bei Freigabe eines Datums rechnen muss.[259] Denn andernfalls willigt sie in Folgen ein, die ihr nicht bekannt sind.[260] Welches Maß der Informiertheit dann aber gelten soll, ist äußerst unklar. Verlangt wird teilweise, dass eine jede Inferenz vorab präzise anzugeben ist.[261] Andere halten eine Angabe typischerweise zu erwartender Profilinhalte, wie sie in Art. 4 Nr. 4 DSGVO benannt sind, d.h. Inferenzgruppen wie Interessen, Vorlieben oder die Zuverlässigkeit, für ausreichend.[262] Darüber hinaus gibt es Ansätze, die diese Problematik nicht

---

[257] Ebenso *Lorentz*, Profiling, 2019, S. 182 f. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 54, demzufolge die betroffene Person abschätzen können muss, welche Bewertungen und Klassifizierungen über sie abgeleitet werden.

[258] So auch, hier spezifisch zum individuellen Kreditscore, Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 29.

[259] *Lorentz*, Profiling, 2019, S. 182 f. Ähnlich *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 7; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 54. Siehe auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 98 f.

[260] Anschaulich, wenngleich allgemein zur Big-Data-Analyse, *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 99: „Zum Zeitpunkt der Einwilligung besteht deshalb nicht allein Unwissenheit darüber, welche persönlichen Informationen der Informationsrezipient hat oder erlangen wird. Vielmehr besteht Unwissen darüber, welche persönlichen Informationen generiert und zu welchen präemptiven Zwecken sie eingesetzt werden". Er spricht von einer „Einwilligung in das Unbekannte".

[261] *Edwards/Veale*, SSRN Journal 2017, 55, wenngleich ohne Unterscheidung zwischen Modell- und Profilbildung und im Rahmen von Transparenz- nicht Rechtmäßigkeitserwägungen. Sie verlangen „summary statistics and qualitative descriptions of […] the output data or classifications being predicted in this model". Vgl. auch *Skistims*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 352, Rn. 28. Ähnlich wohl auch die *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 47, die einen umfassenden Zugang der betroffenen Person zu „ihrem" Profil – das ja letztlich eine Zusammenstellung der einzelnen Inferenzen darstellt – verlangt.

[262] Zu diesem Lösungsvorschlag siehe auch *Lorentz*, Profiling, 2019, S. 185. Sie schlägt die Benennung von veranschaulichenden Beispielen vor. Enthält das Profil am Ende auch andere Einzelerkenntnisse zur Person, die nicht in die Beschreibung aufgenommen wurden, erstreckt sich der Zulassungstatbestand nicht auf diese; diese Profilbildungen sind dann unzulässig. Ähnlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22

in der Rechtmäßigkeit, sondern in der Transparenz verorten. Ausreichend ist dann, dass nachträglich über Profilinhalte informiert wird und vorab die Grundzüge des technischen Verfahrens der Inferenzbildung – dass nämlich aus Rohdaten durch Anwendung des Modells neue Erkenntnisse gebildet werden – dargelegt werden.[263]

Diese Informationsanforderungen sind nicht unproblematisch, dies schon deshalb, da die Aufdeckung der Profilinhalte regelmäßig das unternehmerische Interesse der Verantwortlichen berührt.[264] Der Kern der Problematik liegt aber darin, dass im Zeitpunkt der Erhebung der Anwendungsdaten die späteren Inhalte des Profils, d.h. der Output der Modellanwendung, noch gar nicht – auch nicht dem Verantwortlichen – bekannt sind.[265] Denn Sinn und Zweck der Profilbildung ist es ja gerade, bislang unbekannte Erkenntnisse aus den Rohdaten abzuleiten. Vor allem aber hat sie ihre Ursache in der Verarbeitungsmethodik: Wer die Profilinhalte prognostizieren will, muss vorab benennen können, welchen Gruppen innerhalb des Modells eine Person zugeordnet werden wird. Die Informiertheit verlangt damit vertiefte Kenntnisse zum Modell. Ab einem bestimmten Komplexitätsgrad sind dessen Inhalte auch für technische ExpertInnen nicht mehr verständlich;[266] Modelle aus bestimmten Maschinellen Lernverfahren, etwa künstliche neuronale Netze, sind menschlich nicht nachvollziehbar.[267] In diesen Konstellationen können präzise Prognosen über mögliche Inferenzen nicht mehr erfolgen, aber auch vertypte Inferenzgruppen können nicht mehr – weder im Vor- noch im Nachhinein – angegeben werden. Die Intransparenz von Algorithmen aus Maschinellen Lernverfahren, das Blackbox-Phänomen, steht in diesen Fällen einer Rechtfertigung durch Einwilligung entgegen.

Rn. 54, demzufolge die betroffene Person die Vergleichsgruppen kennen muss, denen sie zugeordnet wird.

[263] In diese Richtung *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 367 f. Die Bedeutung des Transparenzgrundsatzes als Ergänzung zum Rechtmäßigkeitsgrundsatz erkennt auch *Lorentz*, Profiling, 2019, S. 185, derzufolge ein „Minus" bei der Profilinhaltsprognose durch ein „Plus" bei der Beschreibung des technischen Verfahrens der Profilbildung ausgeglichen werden kann.

[264] Vgl. auch *Lorentz*, Profiling, 2019, S. 341; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 368. Siehe hierzu allgemein auch unter Kapitel 4 D. IV. 1. a).

[265] So auch *Lorentz*, Profiling, 2019, S. 183 f.; *Andreotta/Kirkham/Rizzi*, AI and Society 36 (2021), 1, 6. Ebenso, wenngleich allgemein zur Big-Data-Analyse, *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 98–100.

[266] Vgl. zu dieser Problematik im Rahmen der Einwilligung *Lorentz*, Profiling, 2019, S. 185.

[267] Siehe eingehend hierzu unter Kapitel 4 D. IV. 1. d) und e).

c) Vertragsimmanente Zulassung

Die Profilbildung kann nur dann für eine vorvertragliche Maßnahme, den Vertragsabschluss oder die Erfüllung eines Vertrags erforderlich sein, wenn sie funktionsnotwendig, d.h. die Personalisierung explizit vereinbart ist. Denn andernfalls dient die Profilbildung lediglich der Optimierung oder Effektivierung des Dienstes.[268] Auch hier genügt die Vereinbarung einer bloßen Automatisierung eines Dienstes nicht, da eine solche auch ohne Personalisierung möglich ist.[269] Autonome Systeme, wie sie in dieser Arbeit untersucht werden, sind derartige personalisierte Dienste. Ist ihr Einsatz bei der Gestaltung von vorvertraglichen Maßnahmen oder von Verträgen vereinbart oder bilden autonome Systeme selbst den Vertragsgegenstand, ist die Profilerstellung von Art. 6 Abs. 1 lit. b) DSGVO gedeckt.[270] Bei vorvertraglichen Maßnahmen, dies betrifft vor allem das Kredit-Scoring, muss zusätzlich die Anfrage von der betroffenen Person ausgehen.[271] Setzen Verantwortliche aber autonome Systeme

---

[268] *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 15 f., 17 f. Ebenso *Skistims*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 352, Rn. 30; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 31, 36; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 39, 40a, 53; *Lorentz*, Profiling, 2019, S. 188. Plakativ *Ursic/Custers* EDPL 2 (2016), 209, 212: „[T]he data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services". Sehr allgemein zu persönlichen Assistenten Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 31. Das Beispiel persönlicher Shopping-Assistenten benennt *Gausling*, ZD 9 (2019), 335, 336.

[269] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 42; Wolff/Brink, BeckOK Datenschutzrecht/*Tinnefeld/Buchner*, System I. Datenschutz in Medien und Telekommunikation Rn. 86. Siehe auch *Finck/Biega*, Technology and Regulation 2021, 44, 50. Zu Suchdiensten Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 27; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 62. Kritisch zur Rechtfertigung der Personalisierung des Newsfeeds durch Facebook daher auch Generalanwalt Rantos, Schlußanträge v. 20.09.2022, Rs. C-252/21, ECLI:EU:C:2022:704, Rn. 56 – *Meta Platforms Inc. u.a./Bundeskartellamt*.

[270] So auch *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 16. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 31; *Skistims*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 352, Rn. 30; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 266 f. Siehe auch Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 44.

[271] Siehe nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 41. Das Kredit-Scoring kann auch auf die zweite Alternative gestützt werden. Das Kredit-Scoring ist dann erforderlich für die Begründung des vorvertraglichen Schuldverhältnisses. Siehe hierzu *Lorentz*, Profiling, 2019, S. 191.

eigenmächtig ein, fällt dies nicht unter Art. 6 Abs. 1 lit. b) DSGVO.[272] In der Praxis betrifft dies vor allem die Verwendung autonomer Systeme für die Klärung von Vertragsabschlüssen oder die Festsetzung von Vertragsgestaltungen, etwa automatisierte Kreditentscheidungen oder personalisierte Preise.[273] Zeitlich ist die Rechtfertigung auf die Erfüllung des Vertragszwecks beschränkt.[274] Sollen autonome Systeme über einen längeren Zeitraum zum Einsatz kommen, kann dies über die Vereinbarung eines Dauerschuldverhältnisses abgebildet werden.[275]

Weder für die Vertragserfüllung noch für eine vorvertragliche Maßnahme erforderlich sind personalisierte Werbemaßnahmen.[276] Anders kann dies sein,

---

[272] Vgl. zu internen Kredit-Scorings Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 42. Auch Bonitätsanfragen bei Dritten, etwa Auskunfteien, lassen sich nicht über diese Vorschrift rechtfertigen, denn mit jenen Stellen soll ein Vertragsschluss gar nicht zustande kommen und die Bonitätsabfrage ist von der betroffenen Person auch gar nicht angefragt, siehe hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 42; *Lorentz*, Profiling, 2019, S. 191. Die Bonitätsauskunft dient der Vertragserfüllung zwischen Auskunftei und Vertragspartner der betroffenen Person. Art. 6 Abs. 1 lit. b) DSGVO kann aber nicht Datenverarbeitungen in Drittverhältnissen rechtfertigen.

[273] Zu Bonitätsprüfungen siehe Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 42; Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 47. Zu personalisierten Preisen siehe Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 42; *Zuiderveen Borgesius/Poort*, J. Consum. Policy 40 (2017), 347, 360. Siehe auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 23.

[274] Ist etwa ein Kaufvertrag abgeschlossen, sind personalisierte Anwendungen, etwa Produktvorschläge, im Nachhinein nicht mehr erforderlich. Vgl. auch *Lorentz*, Profiling, 2019, S. 189.

[275] Vgl. hierzu Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 40.

[276] Plakativ *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 16 „Normalerweise kann kaum argumentiert werden, der Vertrag sei nicht erfüllt worden, weil es keine verhaltensbasierte Werbung gab“. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 31, 36; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 36, 39 f., 52 f.; *Lorentz*, Profiling, 2019, S. 189 f. Allgemein für die Datenverarbeitung zu Marketingzwecken Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 6 Rn. 13. Vgl. allgemein auch *Lorentz*, Profiling, 2019, S. 188–190; *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 151–153. Anders kann dies im Einzelfall sein, wenn eine Produktanfrage vom Kunden ausgeht, dieser etwa explizit personalisiertes Informationsmaterial anfordert, siehe *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, 08.10.2019, S. 15. Vgl. auch Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 52. Auch bei Bonuspunkte-Verträgen, bei denen

wenn werbebasierte Dienste Teil der vertraglichen Leistung sind, etwa personalisierte Rabatt- oder Bonuspunktesysteme.[277] Wie schon bei der Modellbildung sind auch hier Dienste problematisch, die über den Austausch von Daten finanziert werden („Dienst gegen Daten").[278] Auch hier gilt wie oben, dass nach überwiegender Ansicht der Datenhandel nicht auf Art. 6 Abs. 1 lit. b) DSGVO, allenfalls auf die Einwilligung gestützt werden kann.[279]

Da die Rechtfertigung in Art. 6 Abs. 1 lit. b) DSGVO letztlich auf der privatautonomen Entscheidung der betroffenen Person beruht, gelten im Übrigen dieselben Anforderungen wie bei der Einwilligung.[280] Entsprechend ist auch hier über das zweistufige Profilbildungsverfahren zu informieren, dass also anhand eines aus den Daten einer Vielzahl von NutzerInnen gebildeten Modells neue Erkenntnisse aus den Rohdaten abgeleitet werden.

Die im Rahmen der Einwilligung diskutierte Problematik, inwieweit die Generierung neuer Daten datenschutzrechtlich gerechtfertigt werden kann, stellt sich auch hier. Da Art. 6 Abs. 1 lit. b) DSGVO wesentlich auf der Privatautonomie der betroffenen Person beruht, gelten ähnliche Wertungen wie bei der Einwilligung: Die betroffene Person muss absehen können, welche Profilinhalte im Rahmen der Vertragsbeziehung gebildet werden, andernfalls liegen diese außerhalb der Vertragsvereinbarung.

d) Berechtigte Interessen

Das Interesse des Verantwortlichen an der Profilbildung ist in derartigen Fällen, wie schon bei der Modellbildung ausgeführt, ein wirtschaftliches: Der Verantwortliche hat ein Interesse an den Erkenntnissen über den Einzelnen, da ihm dies die Personalisierung des Dienstes erlaubt.[281] Bei personalisierten (Vor-)Vertragsgestaltungen ermöglicht dies die Effektivierung der Vertragsabwicklung und Stärkung der Verhandlungsposition, bei automatisierten Diensten die Erhöhung der Kundenzufriedenheit, bei personalisierter Werbung die

---

personalisierte Rabattaktionen gerade vertraglich vereinbart sind, ist eine Rechtfertigung über Art. 6 Abs. 1 lit. b) DSGVO denkbar, siehe *Lorentz*, Profiling, 2019, S. 190.

[277] Eingehend hierzu *Lorentz*, Profiling, 2019, S. 190 f.

[278] Siehe hierzu bereits oben unter Kapitel 4 C. III. 1. c). Eingehend zu diesen Fragen etwa *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 50–61.

[279] Vgl. nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 33; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 40a, 43; Wolff/Brink, BeckOK Datenschutzrecht/*Tinnefeld/Buchner*, System I. Datenschutz in Medien und Telekommunikation Rn. 86–87. Ebenso *Skistims*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 352, Rn. 29.

[280] Zum Informationsprogramm siehe eingehend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 25–27.

[281] Aus Art. 21 Abs. 1 S. 1 HS. 1, 2 DSGVO wird erkenntlich, dass der Unionsgesetzgeber Interessen am Profiling explizit anerkannt hat, vgl. auch *Lorentz*, Profiling, 2019, S. 195 f.

Steigerung der Werbewirkung.[282] Im Hinblick auf die berührten Interessen der betroffenen Person muss sauber zwischen den Folgen der Profilbildung und der Profilverwendung unterschieden werden.[283] Bei der Profilbildung geht es um Einblicke in die Persönlichkeit, also um Privatheitsinteressen,[284] sowie um datenschutzrechtliche Interessen.[285] Die nachteiligen Folgen einer Entscheidung oder Steuerung ergeben sich dagegen erst aus der nachfolgenden Profilverwendung.

aa) Erforderlichkeit und Erwartbarkeit

Für den umfassenden Erkenntnisgewinn über die Einzelperson ist in der Regel kein anderes Verfahren als die Profilbildung gleich geeignet, die Profilbildung ist daher erforderlich im Sinne der Vorschrift.[286] Vielfach wird die Profilbildung für die betroffene Person nicht erwartbar sein, da Personalisierungen von Diensten noch nicht derart verbreitet sind, dass betroffene Personen bei einem jeden digitalen Dienst mit einer solchen rechnen.[287] Besonders gilt dies bei Werbemaßnahmen: Die betroffene Person wird in der Regel nicht davon ausgehen, dass diese personalisiert erfolgen.[288] Es bedarf dann also expliziter Hinweise durch den Verantwortlichen.[289]

---

[282] Insbesondere die Werbung ist in Erwägungsgrund 47 S. 7 als Interesse anerkannt. Die Berücksichtigungsfähigkeit dieses Interesses folgt auch im Umkehrschluss aus Art. 21 Abs. 2 DSGVO, denn ein Widerspruchsrecht setzt denklogisch voraus, dass die Verarbeitung zunächst rechtmäßig war. Vgl. hierzu eingehend *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 154 f., siehe auch *Lorentz*, Profiling, 2019, S. 196 f.; *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 288.

[283] Eine ähnliche Forderung stellt *Lorentz*, Profiling, 2019, S. 199 f., 207 f. auf.

[284] So auch für personalisierte Werbemaßnahmen *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 291–293. AA *Lorentz*, Profiling, 2019, S. 206–209, derzufolge die wesentliche Beeinträchtigung in der Verletzung des Rechts auf informationelle Selbstbestimmung, d.h. auf die freie und selbstbestimmte Verfügung über eigene Daten, liegt.

[285] Ähnlich *Lorentz*, Profiling, 2019, S. 207–209.

[286] Ebenso *dies.*, Profiling, 2019, S. 198.

[287] Bei Risikogeschäften wird die betroffene Person zwar mit einer Prüfung ihrer Zahlungsfähigkeit und -bereitschaft rechnen, aber nicht notwendig mit einem profilbasierten Scoring. Vgl. Gola, DS-GVO/*Schulz*, Art. 6 Rn. 103, der selbst beim Bonitäts-Scoring im Rahmen eines so risikoreichen Geschäfts wie dem Online-Verkauf mit Vorleistung des Verantwortlichen einen entsprechenden Hinweis des Verantwortlichen fordert. Noch weniger erwartbar ist dies dann bei Alltagsgeschäften ohne besonderes wirtschaftliches Risiko.

[288] Vgl. Gola, DS-GVO/*Schulz*, Art. 6 Rn. 77; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 106. Explizit zur Datenverwertung bei vermeintlich kostenlosen Diensten *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 56.

[289] So *Lorentz*, Profiling, 2019, S. 211; Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 Rn. 91. Anders als bei der Einwilligung muss aber nicht über die technische Funktionsweise

bb) Interessensabwägung im engeren Sinne

Bei der Profilbildung besteht im Grundsatz keine Präponderanz der Interessensgewichtung zu einer Seite.[290] Da die Profilbildung in der DSGVO als besonders risikobehaftet anerkannt ist, bedarf es aber einer besonders strikten Einzelfallprüfung.[291] Für die Interessensabwägung hat der Europäische Datenschutzausschuss Abwägungskriterien entwickelt, die speziell auf die Profilbildung ausgerichtet sind.[292] Sie sollen der folgenden Untersuchung zugrunde gelegt werden.

(1) Inhalt und Umfang der Profile

Relevant sind zunächst die Profilinhalte, d.h. die anhand der Rohdaten erzeugten Erkenntnisse, und zwar deren Detailschärfe und Sensibilität[293] wie auch deren Umfang.[294] Hier kann auf tradierte Konzepte der Privatheit und auf be-

informiert werden, da es im Rahmen des Art. 6 Abs. 1 lit. f) DSGVO allein auf die Erwartbarkeit der Datenverarbeitung, nicht ihrer Einzelschritte ankommt. Diese Informationen können aber im Rahmen der Interessensabwägung im engeren Sinne maßgeblich sein.

[290] Dies ergibt sich schon aus der Wertung des Art. 21 Abs. 1 S. 1 HS. 2 DSGVO sowie aus Erwägungsgrund 47 S. 7, der das werbebasierte Profiling ohne Einschränkungen dem Art. 6 Abs. 1 lit. f) DSGVO unterstellt. So auch *Lorentz*, Profiling, 2019, S. 211; Plath, DSGVO/BDSG/*Plath/Struck*, Art. 6 92, 100. Ebenso nimmt der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 15 f. keine Vorabgewichtung vor.

[291] Dies ergibt sich aus der Wertung der Art. 4 Nr. 4, Art. 22, Art. 35 Abs. 3 lit. a) DSGVO sowie Erwägungsgrund 71 S. 1, 2, 6. Ebenso Gola, DS-GVO/*Schulz*, Art. 6 Rn. 63; *Lorentz*, Profiling, 2019, S. 210–212; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Pieper/Mühlenbeck*, Art. 6 Rn. 168. Siehe zum Kredit-Scoring eingehend *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, [2]2022, S. 369, 307.

[292] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 15 f. Es handelt sich um Weiterentwicklungen der in Art. 6 Abs. 4 DSGVO benannten Merkmale, mit denen sie teilweise übereinstimmen. Vielfach bilden sie ab, was bereits seit Längerem von der Literatur vorgeschlagen wird. Auch der EuGH stellt in seiner Entscheidung EuGH, Urteil v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 80 f. – *Google Spain* Kriterien auf, die mit denen des Europäischen Datenschutzausschusses übereinstimmen.

[293] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16. Ebenso *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 20.12.2021, S. 19. Auf den Detailgrad eines Profils stellt auch der EuGH, Urteil v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 80 – *Google Spain* ab.

[294] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018,

kannte Verständnisses von Intim- und Privatsphäre zurückgegriffen werden.[295] Auch auf die in Art. 9 DSGVO als sensibel bewerteten Inhalte kann abgestellt werden.[296] Entscheidend sind die Inhalte des Profils, nicht der verarbeiteten Anwendungsdaten,[297] wenngleich diesen Indizwirkung zukommt.[298] Bei Profilen, die den emotionalen oder gesundheitlichen Zustand einer Person abbilden, wird man in der Regel von einem Überwiegen der Interessen der betroffenen Person ausgehen müssen.[299] Auch bei diskriminierenden Profilinhalten[300] wird

---

S. 16. Diese Kriterien befürworten auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 106–107; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 153. Vgl. auch *Lorentz*, Profiling, 2019, S. 213–215. Dieses Merkmal benennt auch der EuGH, Urteil v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 80 – *Google Spain*.

[295] So ausdrücklich *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16: „in die Privatsphäre eingreifendes Profiling". Ebenso *Lorentz*, Profiling, 2019, S. 214 f. Vgl. auch Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Assion/Nolte/Veil*, Art. 6 Rn. 142; Sydow, DS-GVO/*Reimer*, Art. 6 Rn. 61.

[296] *Lorentz*, Profiling, 2019, S. 213 f. Siehe auch *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 20.12.2021, S. 20.

[297] Eine Trennung der Betrachtung von Anwendungsdaten und Profil(inhalten) und deren je eigenen Gefährdungsgrade mahnt auch *Lorentz*, Profiling, 2019, S. 199-200, 205-206 an.

[298] Ist das verarbeitete Datenset besonders umfangreich oder bildet dieses besonders private Inhalte ab, werden auch die Profilinhalte in der Tendenz von besonderer Detailschärfe sein. Wenn also Profile bei SmartHome-Anwendungen anhand von umfangreichen im Wohnraum aufgezeichneten Daten erstellt werden, spricht dies tendenziell für ein Überwiegen des Interesses der betroffenen Person. Vgl. *Lorentz*, Profiling, 2019, S. 218; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 106; *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 20.12.2021, S. 19. Profile für personalisierte Werbemaßnahmen, in deren Rahmen webseiten- und geräteübergreifend Daten gesammelt und ausgewertet werden, legen einen besonderen Umfang und einen hohen Detailgrad des Profils nahe und dürften in der Regel nicht nach Art. 6 Abs. 1 lit. f) DSGVO rechtfertigbar sein, so *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 301 f., vgl. auch Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 153. Auch der EuGH, Urteil v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 80 – *Google Spain* stellt maßgeblich auf den Umfang und die Herkunft der Anwendungsdaten ab.

[299] *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 50. So auch *Lorentz*, Profiling, 2019, S. 214; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 107.

[300] Siehe hierzu bereits Erwägungsgrund 75 S. 1, in dem die Diskriminierung explizit als Risikomerkmal der Profilbildung benannt ist. Bilden Profilinhalte diskriminierungssensible Merkmale ab, kann dies in den Anwendungsbereich des Art. 9 DSGVO fallen. Vgl. hierzu eingehend *Lorentz*, Profiling, 2019, S. 224–231.

die Abwägung typischerweise zugunsten der betroffenen Person ausfallen. Ein Profil, das ein umfassendes Persönlichkeitsbild der betroffenen Person zeichnet oder gesamte Lebensbereiche erfasst, ist ebenso in der Regel unzulässig.[301] Besonders geräte- oder systemübergreifende Profile sind daher problematisch.[302] Unzulässig sind dann erst recht Profile, die beide Aspekte verbinden, bei denen also eine Vielzahl von als sensibel bewerteten Persönlichkeitsmerkmalen abgebildet sind. Tendenziell unbedenklich sind dagegen Profile ohne bestimmte sensible Inhalte, die nur einen bestimmten Lebensbereich abdecken, etwa ein Werbeprofil zu Vorlieben in einer bestimmten Produktpalette, wenn dieses in Tiefe und Breite oberflächlich bleibt.

(2) Offenlegung der Profilinhalte

Über die Zulässigkeit der Generierung neuer Daten trifft Art. 6 Abs. 1 lit. f) DSGVO keine Aussage. Die Überlegungen, wie sie im Rahmen der Informiertheit der Einwilligung angestellt wurden, lassen sich übertragen: Um das Gefährdungspotential der Profilbildung einschätzen zu können, muss der betroffenen Person klar sein, welche Profilinhalte aus den Rohdaten generiert werden. Andernfalls stellt sich die Datenverarbeitung für sie als überraschend dar. Der Verantwortliche muss demnach offenlegen, dass eine Profilbildung stattfindet, zudem darüber informieren, dass durch Abgleich mit einem Modell Erkenntnisse jenseits der Rohdaten gewonnen werden.[303]

Unklar ist dann, inwieweit auch über die jeweilige einzelne Inferenz vorab zu informieren ist. Der Artikel 29 Datenschutzgruppe zufolge ist in der Interessensabwägung maßgeblich zu berücksichtigen, wenn die Verarbeitung zu überraschenden oder unerwarteten Voraussagen führt. Entscheidend soll dann die Art und Wirkung der Vorhersage sein.[304] Daraus folgt: Muss die betroffene

---

[301] Vgl. auch *Lorentz*, Profiling, 2019, S. 215–217; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 106 mit weiteren Beispielen. In diese Richtung auch EuGH, Urteil v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 80 – *Google Spain*. Siehe auch zum Behavioural Targeting *Zuiderveen Borgesius*, Improving Privacy Protection in the area of Behavioural Targeting, 2015, S. 158 f., der ein unzulässige Profilbildung anhand der Auswertung des gesamten Surfverhaltens einer Person über mehrere Webseiten hinweg einer zulässigen Profilbildung eines Online-Buchhändlers anhand der Analyse ausschließlich des Kaufverhaltens auf seiner Webseite gegenüberstellt.

[302] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 106. Vgl. auch *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, 20.12.2021, S. 19 f.

[303] So auch *Lorentz*, Profiling, 2019, S. 164–165, 211.

[304] *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 50 f. Befürwortend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 107. Allgemein für eine derartige an der Sensibilität der

Person nach einem objektivierten Maßstab nicht mit einer Einzelinferenz rechnen,[305] geht die Interessensabwägung in der Regel zu ihren Gunsten aus, allerdings nur, wenn das Profil sich für sie als belastend darstellt. Maßgeblich ist also das Risiko der Profilbildung, das sich wesentlich aus der Sensibilität der Profilinhalte, aber auch den Folgen der späteren Profilverwendung ergibt. Es kommt dann auf die Sensibilität der analysierten Rohdaten oder das Analyseziel, etwa Erkenntnisse zum emotionalen Zustand einer Person, an.[306] Auch Nachteile einer späteren Profilverwendung sind beachtlich. Bei Werbeprofilen, bei denen gezielt unterbewusste Anreize stimuliert werden sollen, wird die Ableitung überraschender Persönlichkeitsmerkmale in der Regel unzulässig sein.[307] Kommt es in diesen Konstellationen zu überraschenden Inferenzen oder ist dies jedenfalls nicht auszuschließen, kann sich der Verantwortliche nur absichern, indem er die betroffene Person vorab über die erwarteten Inferenzen informiert. Dies bedeutet aber nicht, dass der Verantwortliche sämtliche Inferenzen vorab aufdecken muss, sondern allein, dass er insoweit auf das Vorstellungsbild der betroffenen Person einwirken muss, dass sich die Einzelinferenzen für die betroffene Person nicht als überraschend darstellen.

Aus den Wertungen des Art. 6 Abs. 1 lit. f) DSGVO ergibt sich schließlich eine weitere Grenze: Kann generell, d.h. auch vom Verantwortlichen nicht vorhergesagt werden, welche Folgen eine Datenverarbeitung hat – hier also, welcher Art und welchen Inhalts ein Profil sein wird –, geht dies zulasten des Verantwortlichen.[308] Nach den Wertungen des Europäischen Datenschutzausschusses kommt es aber auf das Risiko im Einzelfall an. Damit können risikoreiche Profilbildungen anhand von nicht nachvollziehbaren Modellen nicht auf Art. 6 Abs. 1 lit. f) DSGVO gestützt werden, wenn sich Profilinhalte nicht mehr abschätzen lassen.[309] Dies bedeutet nicht, dass jede Einzelinferenz vorab prognostizierbar sein muss, wohl aber, dass Einzelinferenzen noch innerhalb des objektiven Erwartungshorizonts der betroffenen Person liegen müssen.

Daten ausgerichtete Differenzierung der Informationspflichten im Rahmen Art. 6 Abs. 1 lit. f) DSGVO tritt *Lorentz*, Profiling, 2019, S. 211 ein.

[305] Maßgeblich ist dabei vor allem der Kontext. Vgl. im Einzelnen zu erwartbaren bzw. nicht erwartbaren Inferenzen in verschiedenen Anwendungskonstellationen *Lorentz*, Profiling, 2019, S. 219–221.

[306] Vgl. zu diesen Aspekten im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO *dies.*, Profiling, 2019, S. 213.

[307] Vgl., auch hier allerdings im Rahmen des Art. 6 Abs. 1 lit. f) DSGVO, *dies.*, Profiling, 2019, S. 217 f.

[308] Dies entspricht den allgemeinen Wertungen der Interessensabwägung aus Art. 6 Abs. 4 lit. d) DSGVO, wonach bereits die Unvorhersehbarkeit der Folgen einer Datenverarbeitung zu einer Zweckinkompatibilität führt. Siehe hierzu etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 56.

[309] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*ders.*, Art. 6 Abs. 4 Rn. 58 zu Datenverarbeitungen durch Systeme der Künstlichen Intelligenz, wenngleich dort zur Frage der Zweckinkompatibilität, nicht der Interessensabwägung.

(3) Folgen der Profilbildung

Maßgeblich sind darüber hinaus die Folgen der Profilbildung. Hier ist klar zwischen denen der Profilbildung und -verwendung zu trennen, [310] die Folgen der Profilbildung ergeben sich allein aus den Profilinhalten.[311] Art. 9 DSGVO kann dabei als Schablone dienen. Je tiefgehender, diskriminierungs- oder fehleranfälliger ein Profilinhalt ist, desto eher wird die Interessensabwägung zugunsten der betroffenen Person ausfallen.[312] Darüber hinaus können bereits auf Stufe der Profilbildung Folgen der anschließenden Profilverwendung berücksichtigt werden, eben da das Profil für bestimmte automatisierte Entscheidungen und Steuerungen erstellt wurde.[313] Hier wird dann relevant, inwieweit in der konkreten Anwendung Autonomiegefährdungen und Diskriminierungen wirken. Hierauf ist sogleich zurückzukommen.[314]

(4) Schutzmaßnahmen

Von besonderer Bedeutung sind schließlich Schutzmaßnahmen.[315] Widerspruchs- und Abschaltoptionen[316] oder sonstige Einwirkungs- oder Modifika-

---

[310] Siehe auch unter Kapitel 4 C. III. 3. a) dd). Ebenso *Lorentz*, Profiling, 2019, S. 207–208, 217, die eine klare Differenzierung zwischen Profilbildung und -verwendung und der jeweils zugehörigen Risiken anmahnt.

[311] Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 151; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 107.

[312] Ausdrücklich *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 51: „Je negativer oder unsicherer die Folgen der Verarbeitung sein könnten, umso unwahrscheinlicher ist es alles in allem, dass die Verarbeitung als zulässig angesehen wird".

[313] Auf diese Folgen stellt auch die *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16 ab. Ebenso *Lorentz*, Profiling, 2019, S. 217 f. Siehe auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 47–49, die für ein weites Verständnis des Begriffs der Folgen eintritt.

[314] Siehe unten Kapitel 4 C. III. 3. d) (4).

[315] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16.

[316] Siehe hierzu Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 152; *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 54. Zu Abschaltoptionen bei Tracking-Verfahren Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 171b. Siehe auch *Lorentz*, Profiling, 2019, S. 219. Ein solches Widerspruchsrecht ist bereits gesetzlich normiert, Art. 21 Abs. 1 und 2 DSGVO, allerdings besteht es nur bei Direktwerbung vorbehaltlos, im Übrigen nur, wenn

tionsmöglichkeiten[317] können allerdings zu Verfälschungen des Profils und damit zu Funktionsstörungen der autonomen Systeme führen.[318] Die gängige Schutzmaßnahme der Pseudonymisierung der Rohdaten kann gegen die Gefährdungen der Profilbildung, d.h. der Inferenzbildungen anhand der Rohdaten, nichts ausrichten.[319] Vielversprechend sind dagegen technische Maßnahmen zur Verhinderung von Diskriminierungen.[320] Die informationstechnische Forschung ist hier allerdings noch am Anfang. Bislang hat man noch keine Lösung gefunden, mit denen sich Diskriminierungen effektiv und nachhaltig verhindern lassen.[321]

(5) Ergebnis

Profilbildungen durch autonome Systeme lassen sich zumindest dann über Art. 6 Abs. 1 lit. f) DSGVO rechtfertigen, wenn den betroffenen Personen diese bekannt sind und die Profile keine besonders tiefgehenden oder umfassenden Erkenntnisse über Persönlichkeitsmerkmale beinhalten. Auch wenn betroffenen Personen keine oder nur geringe Risiken durch die anschließende Profilverwendung drohen, kann der Verantwortliche eine Profilbildungsmaßnahme auf die Interessensabwägung stützen. Technische Schutzmaßnahmen sind hier kaum denkbar, für Diskriminierungen erscheinen sie sinnvoll, sind dort aber noch nicht in hinreichendem Maße entwickelt. Bei risikoreichen Profilbildungen ist die Erstellung überraschender Profilinhalte unzulässig. Dann

---

die betroffene Person eine besondere Situation nachweisen kann und die verantwortliche Stelle nicht dennoch zwingende schutzwürdige Gründe für eine Verarbeitung trotz Widerspruchs vorweisen kann, Art. 21 Abs. 1 S. 2 DSGVO. Vgl. eingehend zu Bedingungen und Bedeutung des gesetzlichen Widerspruchsrechts *Lorentz*, Profiling, 2019, S. 221 f.; *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 56–60.

[317] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 152. Allgemein ein Überwiegen des Interesses der betroffenen Person aufgrund fehlender Selbstschutzinstrumente bei der Profilbildung im Internet der Dinge konstatiert Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 121.

[318] Vor allem bei der (Vor-)Vertragsgestaltung wird sich der Einsatz autonomer Systeme dann vielfach erübrigen, etwa wenn die betroffene Person ihren Kreditscore willkürlich abändern oder die durch Zurückhaltung einzelner Daten oder Verhinderung einzelner Inferenzen wesentliche Erkenntnisse über ihre individuelle Zuverlässigkeit unterbinden kann.

[319] So auch *Lorentz*, Profiling, 2019, S. 219. Die Pseudonymisierung als Schutzmaßnahme betont *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 54.

[320] Siehe eingehend hierzu bereits oben unter Kapitel 3 B. I. 3. Siehe auch explizit zu derartigen technischen Maßnahmen zur Verhinderung diskriminierender oder fehlerhafter Profile Erwägungsgrund 71 S. 6. Vgl. auch *Lorentz*, Profiling, 2019, S. 218 f.

[321] Siehe oben unter Kapitel 3 B. I. 3.

ist es auch problematisch, wenn menschlich nicht verständliche Modelle zum Einsatz kommen, deren Ergebnisse sich nicht abschätzen lassen.

e) Verhältnis der Zulassungsgründe

Die vertragsimmanente Rechtfertigung der Profilbildung kommt nur für vertragsakzessorische Datenverarbeitungen in Betracht. Für diese ist der Rechtfertigungsgrund der Einwilligung gesperrt.[322] Der Zulassungsgrund der Interessensabwägung ist in der Regel durch die Einwilligung verdrängt, da das Risiko sich für die betroffene Person bei der Profilbildung als hoch darstellt.[323] Nur bei oberflächlichen Profilen, bei denen aufgrund des Anwendungskontextes Autonomiegefährdungen gering sein werden, ist Raum für Art. 6 Abs. 1 lit. f) DSGVO. Bei der Nutzung autonomer Systeme für die (Vor-)Vertragsgestaltung lässt sich ein vorrangiges Interesse des Verantwortlichen zumindest für das Kredit-Scoring begründen, sofern es der Betrugsprävention dient, nicht aber, wenn der Verantwortliche dies nur aus wirtschaftlichem Interesse betreibt.[324]

f) Ergebnis

Als Grundlage des Rechtmäßigkeitsgrundsatzes ist in der Zweckbestimmung anzugeben, dass die Datenverarbeitung der Profilbildung für eine bestimmte Anwendung dient, andere verlangen als Zweckbestimmung, dass die Verarbeitung der Personalisierung einer bestimmten Anwendung dient. Die Rechtfertigung der Profilbildung über Art. 6 Abs. 1 lit. b) DSGVO kommt in Betracht, soweit der Einsatz autonomer Systeme für die Vertragsgestaltung explizit vereinbart bzw. im Rahmen einer vorvertraglichen Maßnahme von der betroffenen Person angefragt wurde, oder das autonome System selbst Vertragsleistung ist. Dann sind die übrigen Zulassungsgründe gesperrt. Die Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO kann nur in bestimmten Fällen die Profilbildung rechtfertigen, nämlich dort, wo das Profil in Tiefe und Breite oberflächlich bleibt und der betroffenen Person aus der Profilverwendung keine Nachteile drohen. Jenseits rechtsgeschäftlicher Beziehungen kommt damit dem Zulassungsgrund der Einwilligung die größte Bedeutung für die Rechtfertigung von Profilbildungsmaßnahmen zu.

---

[322] So oben Kapitel 4 C. II. 6.

[323] Vgl. für personalisierte Werbemaßnahmen auf sozialen Netzwerken, gleichwohl ohne Differenzierung zwischen Profilbildung und -verwendung, *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 288 f. Zum besonderen Risiko der Verarbeitungsart der Profilbildung siehe bereits oben Kapitel 4 C III. 2. d) bb) am Anfang sowie *Lorentz*, Profiling, 2019, S. 211.

[324] Vgl. zum Kredit-Scoring, wenngleich ohne klare Differenzierung zwischen Profilbildung und -verwendung, *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 66 f.; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 96. Siehe auch Erwägungsgrund 47 S. 6.

Dreh- und Angelpunkt der datenschutzrechtlichen Rechtfertigung der Profilbildung ist die Vorhersehbarkeit der Einzelinferenzen. Im Einzelnen ist dann aber umstritten, wie weit diese Vorhersehbarkeit reichen muss. Während die einen nur eine Darlegung grober Profilinhalte nach Maßgabe der in Art. 4 Nr. 4 DSGVO benannten Gruppen verlangen, fordern andere eine präzise Vorabinformation über sämtliche erwarteten Profilinhalte. Auch gibt es Positionen, die die Problematik im Transparenzgrundsatz verorten. Diese Anforderungen stehen einer Verwendung hochkomplexer Profilbildungsmethoden entgegen, bei denen dem Verantwortlichen aus technischen oder wirtschaftlichen Gründen eine Vorhersage nicht sinnvollerweise möglich ist. Der Einsatz von menschlich nicht nachvollziehbaren Modellen ist damit von Rechts wegen ausgeschlossen. Die Rechtmäßigkeit der Profilbildung bestimmt sich damit am Ende maßgeblich an der Transparenz der Systeme.

3. Profilverwendung: Verarbeitung von Profilinhalten und Automatisierung von Entscheidungen durch selbstlernende Algorithmen

Für die Profilverwendung sieht die DSGVO zwei Rechtfertigungsstränge vor:[325] Einmal hinsichtlich der Verarbeitung des Profils bzw. der Einzelinhalte und des Anwendungsdatums – dies stellt eine Datenverarbeitung dar, die den Anforderungen des Art. 6 DSGVO genügen muss –, einmal hinsichtlich der Verwendung des Datenverarbeitungsergebnisses, regelmäßig des Profils, in einer automatisierten Entscheidung nach Art. 22 DSGVO. Die beiden Rechtfertigungsstränge ergänzen sich.[326] Zunächst soll auf die generellen Zulassungsbedingungen (a)), sodann auf die Anforderungen der Ausnahmezulassung eingegangen werden (b)).

a) Zulässigkeit der Profilverwendung nach den allgemeinen Grundsätzen

Die Profilverwendung als Datenverarbeitung muss dem Zweckfestlegungsgrundsatz genügen (aa)) und sich auf eine taugliche Rechtsgrundlage stützen, wobei die Einwilligung (bb)), die vertragsimmanente Zulassung (cc)) und die Zulassung durch Interessensabwägung (dd)) untersucht werden sollen.

aa) Zweckfestlegungsgrundsatz bei der Profilverwendung

Hinsichtlich des Zweckfestlegungsgrundsatzes ist zwischen Zweckbestimmung und Zweckbindung zu unterscheiden. Untersucht werden soll im Folgenden allein die Zweckbestimmung. Zweckänderungen kommen zwar in der Pra-

---

[325] Siehe oben Kapitel 4 B. III. 3.

[326] Ebenso *Lorentz*, Profiling, 2019, S. 254; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 12. Allgemein zur Parallelität von Art. 22 DSGVO und den generellen Datenschutzgrundsätzen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 4.

xis häufig vor. Da die Erstellung von Profilen ressourcenintensiv ist, ist es wirtschaftlich sinnvoll und gängige Praxis, erstellte Profile mehrfach zu verwenden.[327] Diese Zweckänderungen haben mit der Funktionsweise autonomer Systeme allerdings wenig zu tun und bleiben im Weiteren daher außer Betracht.

Die Zweckbestimmung stellt bei der Profilverwendung kaum vor Herausforderungen. Für die Zweckbestimmung ist der jeweilige Anwendungszweck, etwa die Informationsfilterung, anzugeben. Zur Konkretisierung bedarf es aber zusätzlich einer spezifischeren Beschreibung,[328] insbesondere ist daher der konkrete Anwendungskontext präzise darzulegen. Eine zulässige Zweckbestimmung wäre demnach: „Die Datenverarbeitung erfolgt zur automatisierten Erstellung von Medienangeboten des Dienstes anhand Interessen und Vorlieben". Anders als bei der Modell- und Profilbildung wird es dabei in der Praxis nicht zu völlig überraschenden Ergebnissen der Profilverwendung jenseits des Anwendungskontextes kommen. Denn der Lösungsalgorithmus wird darauf trainiert, eine ganz bestimmte Ausgabe zu generieren. Allerdings sind Algorithmen des Maschinellen Lernens so konzipiert, dass sie sich eigenständig fortentwickeln.[329] Es ist daher möglich, dass sich die Systeme von der Zielvorgabe im Trainingsverfahren entfernen. Dabei ist gleichwohl zu bedenken, dass an derartigen, d.h. sich völlig frei entwickelnden Systemen in der Praxis typischerweise schon wirtschaftlich kein Interesse besteht. Unternehmer und VerbraucherInnen sind nicht an Systemen interessiert, die ihr Anwendungsziel nicht mehr erreichen können oder gar unerwünschte Outputs generieren und Schäden anrichten.[330] Verantwortliche werden daher derartige wildwüchsige

---

[327] Insbesondere die Verwendung von Profilen aus einem Vertragskontext oder einer Geschäftsbeziehung für personalisierte Werbemaßnahmen durch den Anbieter (nicht notwendig für eigene Produkte) ist gängig. Vgl. zu derartigen Konstellationen *Finck/Biega*, Technology and Regulation 2021, 44, 49 f.; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 38. Auch ist es durchaus üblich, dass gebildete Profile an Dritte veräußert werden. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 40, der eine Zweckinkompatibilität für die Weitergabe der Daten für Profilbildungen durch Dritte feststellt.

[328] So auch *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 15 f.

[329] Siehe oben Kapitel 1 A. II.

[330] Siehe nur *Dukino*, Was ist Künstliche Intelligenz? Eine Definition jenseits von Mythen und Moden, Fraunhofer-Gesellschaft, 14.3.2019, https://blog.iao.fraunhofer.de/was-ist-kuenstliche-intelligenz-eine-definition-jenseits-von-mythen-und-moden. Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 61, 294. Ein bekanntes Beispiel hierfür ist der Chatbot Tay des Unternehmens Microsoft. Die (unüberwachte) Fortentwicklung des Bots anhand von Äußerungen der NutzerInnen führte dazu, dass der Bot rassistische, beleidigende und sexistische Äußerungen von sich gab. Microsoft entfernte daraufhin den Chatbot umgehend vom Markt. Siehe hierzu *Victor*, Microsoft Created a Twitter Bot to Learn From Users. It Quickly Became a Racist Jerk., The New York Times 24.05.2016, https://www.nytimes.com/2016/

Systeme schon gar nicht einsetzen oder jedenfalls Vorkehrungen treffen, damit diese sich nicht vom Trainingsziel entfernen. Dass sich selbstlernende Systeme dennoch gegen oder ohne den Willen des Verantwortlichen fortentwickeln, ist aber dennoch nicht auszuschließen.[331]

bb) Einwilligung

Die Profilverwendung wirft die Zulassungsfrage neu auf. Die betroffene Person verhält sich also nicht widersprüchlich, wenn sie zunächst die Verarbeitung ihrer Daten für die Profilbildung gestattet, dann aber die Zustimmung für die Verwendung des Profils versagt.[332] Die Einwilligung muss informiert erfolgen ((1)). Problematisch ist, wie damit umzugehen ist, wenn die Outputs bei der Profilverwendung nicht mehr vorhersehbar sind ((2)). Offen ist auch, wie damit umzugehen ist, dass bei der Profilverwendung die zuvor in der Profilbildung generierten, für die betroffene Person gegebenenfalls nicht bekannten Daten verarbeitet werden ((3)).

(1) Informiertheit der Einwilligung

Im Rahmen der Informiertheit ist über das grundlegende technische Verfahren zu informieren, dass also durch Eingabe des Profils und gegebenenfalls weiterer Anwendungsdaten in einen Lösungsalgorithmus eine automatisierte Entscheidung oder Steuerung ausgelöst wird.[333] Details zum algorithmischen Verarbeitungsverfahren bedarf es nicht. Dies folgt bereits e contrario aus den besonderen Informationspflichten der Art. 13–15 DSGVO, wo derartige Informationspflichten nur für automatisierte Entscheidungen vorgesehen sind.[334]

Über die mit einer jeden Profilverwendung einhergehenden Risiken, etwa Diskriminierungen, Fehleranfälligkeiten, Autonomiegefährdungen, ist dagegen nicht aufzuklären. Denn es handelt sich um typische Risiken autonomer Systeme, die mit der konkreten Datenverarbeitung nichts zu tun haben. Die

---

03/25/technology/microsoft-created-a-twitter-bot-to-learn-from-users-it-quickly-became-a-racist-jerk.html.

[331] Der ChatBot Tay ist ein prominentes Beispiel, bei dem Schutzmaßnahmen gegen ungewollte Weiterentwicklungen der selbstlernenden Algorithmen nicht ausreichten.

[332] Ähnlich, wenn auch im Rahmen des Widerspruchsrechts nach Art. 21 DSGVO, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Caspar*, Art. 21 Rn. 16.

[333] Sehr allgemein auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 14. Dies ist bereits im Rahmen der Zweckbestimmung erfolgt, siehe oben Kapitel 4 C. III. 3. a) aa).

[334] Art. 13-15 DSGVO als Orientierungsrahmen für die Informiertheit im Rahmen der Rechtmäßigkeit benennen auch Wolff/Brink, BeckOK DatenschutzR/*Stemmer*, Art. 7 Rn. 58; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 59. Siehe auch unter Kapitel 4 D. II. 2. sowie Kapitel 4 D. III. 3. a).

betroffene Person kann und muss mit diesen Risiken rechnen, sobald ein autonomes System erkennbar zum Einsatz kommt. Dies betrifft also eine Frage des allgemeinen Risikobewusstseins, die den allgemeinen Verbraucherschutz und einen medienspezifischen Bildungsauftrag adressiert, nicht aber eine datenverarbeitungsspezifische Informationspflicht.

(2) Einwilligung in nicht vorhersehbare Outputs

Bereits mit der Kenntnis von der Automatisierung einer bestimmten Anwendung, d.h. mit den Informationen im Rahmen der Zweckbestimmung, kann die betroffene Person in der Regel diese Folgen der Profilverwendung überblicken und damit die Trag- und Reichweite der Einwilligung überblicken. Aufgrund der Komplexität des Lösungsalgorithmus kann es im Einzelfall dennoch vorkommen, dass die betroffene Person die Folgen der Profilverwendung nicht einschätzen kann. Sie willigte dann in etwas Unerwartetes ein, die Einwilligung würde zur unzulässigen Blanko-Einwilligung.[335] Die Artikel 29 Datenschutzgruppe verlangt daher, dass bei komplexen Verarbeitungen auch über die Folgen der Verarbeitung aufzuklären ist.[336] Entstammt der Lösungsalgorithmus selbst Maschinellen Lernverfahren, stellt vor Herausforderungen, wenn dieser menschlich nicht verständlich sind. Dann kann auch der Verantwortliche mögliche Outputs des Systems nicht mehr vorhersagen und die betroffene Person nicht entsprechend aufklären. Dabei ist allerdings zu bedenken: Um eine informierte Entscheidung treffen zu können, muss die betroffene Person nicht sämtliche konkreten Outputs vorab kennen. Eine entsprechende Aufklärung wäre mit den Interessen des Verantwortlichen ohnehin nicht in Einklang zu bringen.[337] Sie muss allein die Folgen der Verarbeitung, hier also der Profilverwendung, überschauen können. Sind die einzelnen Outputs nicht vorhersehbar, wohl aber die Folgen, ist dies also unbedenklich. Problematisch sind allein solche Lösungsalgorithmen, die unerwartete Folgen produzieren. In der Praxis besteht allerdings an derartigen Lösungsalgorithmen, die völlig überraschende Outputs jenseits des definierten Anwendungskontextes und -ziels erzeugen, in der Regel kein Interesse.[338] Generieren selbstlernende Algorithmen

---

[335] Zur Unzulässigkeit von Blanketeinwilligungen siehe nur Wolff/Brink, BeckOK Datenschutzrecht/*Stemmer*, Art. 7 Rn. 79.

[336] So auch *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 8: „[D] die Verantwortlichen [sollten] bei komplexen, technischen oder unerwarteten Verarbeitungsvorgängen neben der Bereitstellung der nach den Artikeln 13 und 14 vorgeschriebenen Informationen […] gesondert und eindeutig formuliert die wichtigsten Folgen der Verarbeitung erklären".

[337] Ähnliche Gedanken, dort im Rahmen der Aufklärung über die Outputs der Profilbildung, *Lorentz*, Profiling, 2019, S. 185.

[338] An derartigen Algorithmen besteht in der Praxis kein Interesse, siehe bereits oben Kapitel 4 C. III. 3. a) aa).

allerdings derartige unerwartete Outputs, die dann zu unüberschaubaren (nachteiligen) Folgen führen, erstreckt sich die Einwilligung nicht mehr auf diese.[339] Derartige Outputs sind dann aber in der Regel schon nicht mehr von der Zweckbestimmung gedeckt.[340] Vorwiegend wird diese Problematik fehlender Nachvollziehbarkeit des Lösungsalgorithmus im Übrigen als Frage der Informationspflichten nach Art. 13–15 DSGVO, genauer: der Aufklärungspflichten hinsichtlich der involvierten Logik der Verarbeitung betrachtet.[341] Derartige Informationspflichten sind in der DSGVO gleichwohl nur für die automatisierte Entscheidung vorgesehen. Hierauf ist zurückzukommen.[342]

(3) Einwilligung in die Weiterverarbeitung neu generierter Daten

Da die betroffene Person in der Regel keinen Einblick in „ihr" Profil oder Teile hieraus erhält, willigt sie im Rahmen der Profilverwendung in die Verarbeitung von ihr unbekannten Daten[343] ein, erteilt also eine Blanko-Ermächtigung.[344] Es wird daher diskutiert, ob die Einwilligung in die Profilverwendung zunächst eine Information über einzelnen Profilinhalte voraussetzt. Teilweise wird eine solche umfassende Offenlegung gefordert.[345] Vorgeschlagen wird aber auch,

---

[339] Vgl., wenngleich im Rahmen des Art. 22 Abs. 2 lit. c) DSGVO, Gola, DS-GVO/*Schulz*, Art. 22 Rn. 31, demzufolge über die Information im Rahmen der Einwilligung auch deren Reichweite bestimmt wird.

[340] Siehe soeben Kapitel 4 C. I. 3. a) aa).

[341] Vgl. auch *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 41, die explizit auf die Transparenz hinsichtlich der Logik der Verarbeitung als notwendige Voraussetzung für die Einwilligung hinweist. Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 10, 14. Vgl. auch *Finck/Biega*, Technology and Regulation 2021, 44, 53. Die fehlende Vorhersehbarkeit von Outputs wird in der Literatur überwiegend im Rahmen des Art. 22 Abs. 2 lit. c) DSGVO diskutiert und dort dann für den Inhalt der Informiertheit der Einwilligung auf die Inhalte der Art. 13-15 DSGVO verwiesen, so etwa Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 42; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 53; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 31.

[342] Siehe Kapitel 4 D. II. 3.

[343] Die Profilinhalte stellen ihrerseits ein personenbezogenes Datum dar. Siehe hierzu eingehend oben Kapitel 4 B. III. 3. a).

[344] Siehe *Lorentz*, Profiling, 2019, S. 254. Eingehend auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 99 „[Zum Zeitpunkt der Einwilligung] […] besteht Unwissen darüber, welche persönlichen Informationen generiert und zu welchen präemptiven Zwecken sie eingesetzt werden". Siehe auch *Solove*, Harv. L. Rev. 126 (2013), 1880, 1889–1891. Diese Problematik deutet auch der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 13 an.

[345] So wohl Gola, DS-GVO/*Schulz*, Art. 7 Rn. 36, der für eine gestufte Einwilligung eintritt, bei der die betroffene Persno in einzelne Verarbeitungsphasen bzw. -ergebnisse ein-

die Informiertheit der Profilverwendung an die der Profilbildung zu koppeln: Die Darlegung der (erwarteten) Profilinhalte im Rahmen der Profilbildung wirkt dann auch für die Profilverwendung fort.[346] Problematisch ist es dann, wenn aufgrund der Komplexität oder fehlenden Nachvollziehbarkeit des Modells auch im Nachhinein an eine Profilbildungsmaßnahme Profilinhalte nicht ausgelesen werden können.

cc) Vertragserfüllung

Die Profilverwendung ist dann für die Vertragserfüllung oder vorvertragliche Maßnahme im Sinne des Art. 6 Abs. 1 lit. b) DSGVO erforderlich, wenn die personalisierte Automatisierung der Vertragsanbahnung beantragt, die Vertragsautomatisierung vereinbart oder ein autonomes System zum Vertragsgegenstand gemacht wurde. Ist also bereits die Profilbildung nach dieser Vorschrift gerechtfertigt, ist es auch die Profilverwendung, insoweit kann auf die Ausführungen oben verwiesen werden.[347] Ausgenommen sind personalisierte Werbemaßnahmen, denn diese ergehen weder auf Initiative der betroffenen Person, noch sind sie für einen Vertragsschluss oder die Vertragserfüllung erforderlich.[348] Problematiken der Vorhersehbarkeit, wie sie für die Einwilligung beschrieben wurden, stellen sich auch hier. Denn kommt es innerhalb der Vertragsbeziehung zu unvorhersehbaren Folgen, ist dies nicht mehr von der vertragsgemäßen Willenserklärung der betroffenen Person gedeckt. Die Erwägungen im Rahmen der Einwilligung lassen sich übertragen.

dd) Berechtigte Interessen

Auch für die Rechtfertigung der Profilverwendung anhand der Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO sind die im Rahmen der Profilbildung angestellten Überlegungen übertragbar. Die DSGVO erklärt die Profilverwendung nicht per se für unzulässig und nimmt auch keine Vorweggewichtung ei-

---

willigt, etwa zunächst in die Erhebung, dann in die Auswertung etc. Dies enstpräche vorliegend einer Einwilligung in die Verarbeitung (Profilbildung) sowie einer eigenständigen Einwilligung in die Nutzung des Analyseergebnisses (Verwendung der Profilinhalte).

[346] So *Lorentz*, Profiling, 2019, S. 254. So wohl auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 366 f., der für diese Konstellation allein nachträgliche Informationspflichten fordert.

[347] Siehe zu Datenverarbeitungen im Rahmen personalisierter Dienste Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 26, 40. Vgl. zur Datenverarbeitung bei einem Shopping-Assistenten *Gausling*, ZD 9 (2019), 335, 336.

[348] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 31. Zu missbräuchliche Vertragsinhaltsdefinitionen im Rahmen datenbasierter Geschäftsmodelle siehe *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 50 f.; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 rn. 40a.

ner Seite vor.[349] Die oben aufgelisteten wirtschaftlichen Interessen des Verantwortlichen stehen den Gefährdungen betroffener Personen gegenüber, hier dann aber derjenigen, die sich aus der Profilverwendung ergeben.[350] Dies sind andere als die der Profilverwendung: Es geht um die tatsächlich ausgelösten Autonomiegefährdungen und Diskriminierungen, wie sie in Kapitel 2 beschrieben wurden. Im Einzelnen sind dann Erforderlichkeit und Erwartbarkeit zu bewerten ((1)) sowie die Interessensabwägung anhand verschiedener Kriterien vorzunehmen ((2)–(6)).

(1) Erforderlichkeit und Erwartbarkeit

Ist die Personalisierung vereinbart, ist die Verarbeitung der Profilinhalte und Anwendungsdaten im Lösungsalgorithmus erforderlich; eine andere technische Methode zur Automatisierung besteht nicht. Da autonome Systeme derzeit noch nicht umfassend Verbreitung gefunden haben, bedarf es eines expliziten Hinweises von Seiten des Verantwortlichen. Andernfalls ist deren Einsatz nicht erwartbar. Vor allem gilt dies bei der personalisierten Werbung.[351]

(2) Inhalte des Profils

Der Gefährdungsgrad der Profilverwendung ergibt sich maßgeblich aus dem Inhalt des Profils. Vor allem Fragen der Privatheit sind dabei maßgeblich; detailreiche oder umfassende Profile verstärken die Gefahren von Autonomiebeeinträchtigungen.[352] Besonders die Aufdeckung emotionaler, unterbewusster Aspekte, wie sie beim Emotional Targeting erfolgt, ist dann problematisch.[353] Die Interessensabwägung fällt im Übrigen auch dann zugunsten der betroffenen Person aus, wenn das Profil in unzulässiger Weise gebildet wurde; die Rechtswidrigkeit der Profilbildung schlägt dann auf die Profilverwendung durch.[354] Auch die Transparenz des Profils kann von Bedeutung für die an-

[349] Dies ergibt sich aus verschiedenen Wertungen, etwa Art. 22, 21 Abs. 1, 2 DSGVO oder Erwägungsgrund 47 S. 7. Vgl. hierzu auch *Lorentz*, Profiling, 2019, S. 255.

[350] Vgl. auch *dies.*, Profiling, 2019, S. 257.

[351] *Dies.*, Profiling, 2019, S. 257.

[352] So auch am Beispiel personalisierter Werbung *dies.*, Profiling, 2019, S. 257. Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16, der vor einem „massiv in die Privatsphäre eingreifende[n] Profiling […] zu Marketing- oder Werbezwecken" warnt, dabei allerdings nicht zwischen Profilbildung und -verwendung unterscheidet.

[353] Ebenso *Lorentz*, Profiling, 2019, S. 257.

[354] Hierzu *dies.*, Profiling, 2019, S. 255 f.

schließende Profilverwendung sein.[355] Je weniger erkenntlich die Profilinhalte sind, die einer Entscheidung oder Steuerung zugrunde liegen, desto intransparenter ist auch die Profilverwendung.[356] Damit stellt sich die bereits bei der Einwilligung aufgeworfene Frage, inwieweit über Einzelinferenzen der Profile auf Stufe der Profilverwendung zu informieren ist. Die Erwägungen lassen sich übertragen. In der Interessensabwägung ist dann maßgeblich zugunsten der betroffenen Person zu berücksichtigen, wenn bei der Profilverwendung Profile zum Einsatz kommen, die sich aufgrund der fehlenden Verständlichkeit des Modells überhaupt nicht mehr vorhersagen lassen.[357]

(3) Folgen der Profilverwendung

Von besonderer Bedeutung sind darüber hinaus die Folgen der Profilverwendung. Zum einen geht es dann um Nachteile, wie sie oben für Art. 22 DSGVO vorgestellt wurden,[358] zum anderen um Autonomiegefährdungen und Diskriminierungen, wie sie Gegenstand dieser Arbeit sind. Dies gebietet eine Einzelfallbetrachtung einer jeden Anwendung.[359] Dabei lassen sich gewisse Kriterien synthetisieren.

Bei automatisierten Entscheidungen sind die Bedeutung des Guts bzw. der Dienstleistung für die betroffene Person sowie die Verfügbarkeit von Alternativen, im Übrigen die Folgen für die Lebensgestaltung maßgeblich. Personalisierte Preisbildungen haben dann geringere Schädigungspotentiale als automatisierte Kreditentscheidungen oder die automatisierte Bewerberauswahl.[360] Auch soweit die Entscheidung zu einer Diskriminierung der betroffenen Person führt, ist dies maßgeblich zu berücksichtigen.[361]

---

[355] Sind bereits so wenige Informationen erfolgt, dass die Profilbildung ihrerseits als rechtswidrig gelten muss, führt dies auch zur Rechtswidrigkeit der Profilverwendung. Siehe bereits oben unter Kapitel 4 A III. 3. d) (2).

[356] Vgl. *Lorentz*, Profiling, 2019, S. 255 f.

[357] Ähnliche Gedanken bei *dies.*, Profiling, 2019, S. 256 f., die von einem Überwiegen der Interessen der betroffenen Person ausgeht, wenn aufgrund der Profilbildung anhand von Daten aus anderen Kontexten der Profilinhalt für die betroffene Person nicht erwartbar ist.

[358] Siehe oben Kapitel 4 B. III. 3. b) dd).

[359] Einen Überblick über verschiedene Anwendungkonstellationen bietet etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 116–139; *Buchner/Petri*, Rn. 47–72a.

[360] Siehe auch *Lorentz*, Profiling, 2019, S. 217 f. Siehe zur Zulässigkeit nach Art. 6 Abs. 1 lit. f) DSGVO zum Kredit-Scoring Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 47–48; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 133–139 und zur Bewerberauswahl Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 49–51.

[361] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16, demzufolge Garantien zur Absicherung gegen diskriminierendes oder fehlerhaftes Profiling vorzusehen sind. Zur Bedeutung der Verwendung fehlerhafter Profil-

Bei automatisierten Steuerungen, dann also bei Informationsfilterungen oder personalisierten Werbemaßnahmen, ist die Intensität der Einwirkung auf die Autonomie der betroffenen Person von Bedeutung. Hier fehlt es vielfach noch an belastbaren Studien.[362] Bislang ist allein der Bereich personalisierter Werbung empirisch aufgearbeitet. Als maßgeblich wird dort bewertet, dass die Einwirkung auf die Willensbildung gerade Ziel der Anwendung ist. Relevante Kriterien sind die Erkennbarkeit der personalisierten Werbung, dann also sowohl der Werbung an sich, als auch deren Personalisierung,[363] überdies die Stimulation besonders manipulationsanfälliger Anreize und die Ausnutzung individueller Vulnerabilitäten der betroffenen Person sowie die Absicht dieser Art der Einflussnahme.[364] Darüber hinaus ist die Verbreitung des Systems relevant: Eine webseiten- oder geräteübergreifende Anwendung ist in der Tendenz risikoreicher.[365] Schließlich ist auch der Umstand relevant, ob die Werbemaßnahme einmalig oder über einen langen Zeitraum erfolgt. Auch der Anwendungsbereich ist relevant, sodass etwa bei politischer Werbung ein nochmals strengerer Maßstab gelten wird.[366]

(4) Nachvollziehbarkeit und Vorhersehbarkeit der Ergebnisse

Relevant für die Interessensabwägung kann auch die Verständlichkeit der algorithmischen Entscheidungs- und Steuerungsarchitektur für die betroffene Person sein. Führt eine fehlende Verständlichkeit dazu, dass die Folgen der Datenverarbeitung für die betroffene Person nicht mehr vorhersehbar sind, fällt die Interessensabwägung in der Regel zugunsten der betroffenen Person aus.[367]

---

inhalte für die Interessensabwägung siehe auch *Lorentz*, Profiling, 2019, S. 257 f. Unklarheiten hinsichtlich der Relevanz von Diskriminierungen in der Interessensabwägung bemängelt *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 66.

[362] Auf die fehlende rechtspraktische und rechtswissenschaftliche Diskussion hinsichtlich Manipulationen weist *Nettesheim*, in: Grabenwarter/Breuer/Bungenberg (Hrsg.), Europäischer Grundrechteschutz, [2]2022, 66 hin.

[363] *Lorentz*, Profiling, 2019, S. 257; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 52.

[364] Emotional Targeting oder Methoden zur gezielten Ausnutzung der Willensschwäche oder andere Verfahren, die gezielt auf unbewusster Ebene wirken, werden sich in der Regel nicht über Art. 6 Abs. 1 lit. f) DSGVO rechtfertigen lassen. Vgl. *Lorentz*, Profiling, 2019, S. 257. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 106.

[365] Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16.

[366] Vgl. zur besonderen Sensibilität politischer Werbung anhand profilbasierter Maßnahmen *Lorentz*, Profiling, 2019, S. 272 f. Siehe auch zum Mikrotargeting *Martini*, Blackbox Algorithmus, 2019, S. 101 f.

[367] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 56.

Bereits die fehlende Vorhersehbarkeit von Folgen führt zu diesem Ergebnis, die Folgen müssen nicht nachteilig sein. Nach den Wertungen der Artikel 29 Datenschutzgruppe ist dies aber nur der Fall, wenn es sich um eine risikoreiche Anwendung handelt.[368] Kann der Verantwortliche mögliche Folgen einer risikoreichen Profilverwendung aufgrund der fehlenden Nachvollziehbarkeit selbstlernender Systeme nicht vorhersagen, muss eine Rechtfertigung nach Art. 6 Abs. 1 lit. f) DSGVO ausscheiden.[369]

(5) Schutzmaßnahmen

Schließlich können Verantwortliche Schutzmaßnahmen vorsehen. Widerspruchsrechte oder Abschaltoptionen sowie Einwirkungsmöglichkeiten[370] sind zwar denkbar, können aber die Ergebnisse verfälschen und einem sinnvollen Einsatz der autonomen Systeme entgegenstehen. Als weiteres Schutzinstrument wird auch hier die Pseudonymisierung des Profils genannt,[371] die gleichwohl kein Mittel gegen die Autonomiegefährdungen und Diskriminierungen durch autonome Systeme darstellt. Im Übrigen werden auch hier technische Maßnahmen diskutiert, um Diskriminierungen auszuschließen, die derzeit aber noch unausgereift sind.[372]

(6) Ergebnis

Im Ergebnis kann die Profilverwendung nach Art. 6 Abs. 1 lit. f) DSGVO nur dann gerechtfertigt werden, wenn die Maßnahme wie auch die Personalisierung für die betroffene Person erwartbar ist. Entscheidend ist darüber hinaus der Inhalt des Profils: Sensible, umfangreiche und diskriminierende und vor allem auch menschlich nicht verständliche Profilinhalte führen in der Regel zu einem Überwiegen der Interessen der betroffenen Person. Im Übrigen sind die realen Folgen, dann also im Hinblick auf Autonomiegefährdungen und Diskri-

---

[368] *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 50 f. Siehe hierzu oben Kapitel 4 C. III. 2. d) bb) (2).

[369] Allgemein kritisch, ob eine Rechtfertigung von Verarbeitungsverfahren durch Systeme Künstlicher Intelligenz gelingen kann, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 121. Zweifelnd – dort dann allerdings im Rahmen der Zweckinkompatibilität – Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 58.

[370] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 121.

[371] Vgl. etwa für die personalisierte Werbung *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 300 f. Diese Maßnahme schützt dann allein das Privatheits- bzw. Datenschutzinteresse am Profil.

[372] Vgl. *Lorentz*, Profiling, 2019, S. 258. Siehe bereits oben Kapitel 4 C. III. 2. d) bb) (4) sowie Kapitel 3 B. I. 4.

minierungen von besonderem Gewicht. Relevante Faktoren bei automatisierten Entscheidungen sind etwa die Bedeutung der Entscheidung für Lebensführung des Einzelnen und die Verfügbarkeit von Alternativen. Bei automatisierten Steuerungen ist die Intensität der Autonomiegefährdung von Gewicht. Übergreifende Faktoren lassen sich derzeit vor allem für personalisierte Werbemaßnahmen aufstellen. Entscheidend sind etwa die Erkennbarkeit der Werbemaßnahme und ihrer Personalisierung, die Ausnutzung manipulationssensibler Umstände, die Manipulationsabsicht sowie der Umfang und Zeitraum. Politische Werbung erfordert eine besonders strikte Prüfung. Die fehlende Nachvollziehbarkeit des Lösungsalgorithmus steht einer Rechtfertigung nach Art. 6 Abs. 1 lit. f) DSGVO entgegen, wenn Prognosen über mögliche Ausgaben nicht mehr möglich sind, zumindest bei risikoreichen Anwendungen. Technische Schutzmaßnahmen versprechen vor allem bei Diskriminierungen gute Lösungen.

ee) Verhältnis der Zulassungsgründe

Ist der Einsatz autonomer Systeme durch die Parteien vereinbart, geht der Zulassungsgrund des Art. 6 Abs. 1 lit. b) DSGVO den übrigen Zulassungsgründen vor. Bei allen sonstigen Anwendungen wird es im Ergebnis zu einem Vorrang der Einwilligung kommen. Die Erwägung von oben zur Profilbildung lassen sich übertragen: Ein schutzwürdiges Interesse des Verantwortlichen, das sich gegen das der betroffenen Person durchsetzt und Raum für eine Abstützung der Profilverwendung auf Art. 6 Abs. 1 lit. f) DSGVO schafft, ist allein bei der automatisierten Kreditentscheidung zur Verhinderung von Betrugsfällen denkbar.[373] Im Übrigen besteht sowohl bei der personalisierten Werbung[374] als auch bei (Vor-)Vertragsmaßnahmen[375] ein erhöhtes Risiko für betroffene Personen. Sie dürfen daher erwarten, nach ihrer Zustimmung zu diesen automatisierten Anwendungen gefragt zu werden.

ff) Ergebnis

Die Zweckbestimmung erfolgt bei der Profilverwendung durch die Angabe des konkreten Anwendungsziels und wird in der Praxis wenig Probleme bereiten. Zwar ist es denkbar, dass sich selbstlernende Algorithmen von der Zielvorgabe entfernen; an derartigen Algorithmen besteht in der Praxis aber kein Interesse.

---

[373] Siehe auch Erwägungsgrund 47 S. 6. Vgl. zum Kredit-Scoring *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 66 f.; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 96.

[374] Vgl. für personalisierte Werbemaßnahmen auf sozialen Netzwerken *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 287 f.

[375] So zum Kredit-Scoring, das nicht allein der Betrugsprävention dient, *ders.*, Privates Datenschutzrecht, 2020, S. 66 f.

Bei der Zulassung der Profilverwendung ist zu unterscheiden, ob diese vertragsakzessorisch erfolgt oder nicht. Ist die automatisierte Vertragsgestaltung zwischen den Parteien vereinbart oder eine vorvertragliche Maßnahme, etwa ein Kredit-Scoring, von der betroffenen Person beantragt, kann dies über Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt sein. Auch dann, wenn der Einsatz eines autonomen Systems Vertragsinhalt ist, wenn etwa ein personalisierter Informationsfilterdienst Leistungsgegenstand ist, kommt Art. 6 Abs. 1 lit. b) DSGVO zum Tragen. Im Übrigen ist die Profilverwendung vornehmlich auf die Einwilligung zu stützen. Die Rechtfertigung durch Interessensabwägung kommt nur in Betracht, wenn das verwendete Profil oberflächlich bleibt und der betroffenen Person aus der automatisierten Entscheidung oder Steuerung keine Nachteile drohen. In jedem Fall muss der Einsatz eines autonomen Systems für die betroffene Person erkenntlich sein. In der Regel wird die Einwilligung den Zulassungsgrund der Interessensabwägung aber verdrängen, da sich die Profilverwendung als risikoreiche Datenverarbeitung darstellt, bei der die betroffene Person erwarten darf, um ihre Zustimmung gebeten zu werden. Insbesondere die personalisierte Werbung ist daher nur über die Einwilligung rechtfertigbar.

Dass die Profilinhalte, die die betroffene Person bei der Profilverwendung zur Verarbeitung frei gibt, der betroffenen Person nicht bekannt sind, ist nach überwiegender Ansicht irrelevant, solange im Rahmen der Profilbildung eine hinreichende Information erfolgte. Eine Rechtfertigung muss aber ausscheiden, wenn Ergebnis und Folgen der Profilverwendung aufgrund der Komplexität der Lösungsalgorithmus nicht mehr vorhersehbar sind.

b) Automatisierte Entscheidung

Stellt die Profilverwendung eine automatisierte Entscheidung dar, ist sie untersagt nach Art. 22 Abs. 1 DSGVO. Ausnahmsweise kann sie nach Art. 22 Abs. 2 lit. a) und lit. c) DSGVO zugelassen werden. Das soeben Ausgeführte lässt sich übertragen, da dort die nämlichen Bedingungen wie in Art. 6 Abs. 1 lit. b) bzw. Art. 6 Abs. 1 lit. a) DSGVO gelten.[376] Lediglich der Anknüpfungspunkt der Einwilligung bzw. der vertragsimmanenten Erforderlichkeit ist ein anderer: Es geht nicht um die Datenverarbeitung, sondern die automatisierte Entscheidung. Anders als bei Art. 6 Abs. 1 lit. a) DSGVO muss die Einwilligung nach Art. 22 Abs. 2 lit. c) DSGVO ausdrücklich erteilt werden.

Für den Vertragsabschluss nach Art. 22 Abs. 2 lit. a) DSGVO erforderlich ist die automatisierte Entscheidung nur, wenn die Parteien übereinstimmend

---

[376] Zur Vertragserfüllung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 41; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 31. Zur Einwilligung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 52; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 41; Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 38; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 83.

automatisierte Vertragsgestaltungen zur Anwendung bringen wollen.[377] Für den Vertragsabschluss ist sie erforderlich, wenn das Profil die maßgebliche Entscheidungs- und Kalkulationsgrundlage bilden soll.[378] Der Europäische Datenschutzausschuss prägt ein enges Verständnis: Nur wenn Vertragsabschluss oder -erfüllung allein durch die automatisierte Entscheidung, nicht aber durch eine natürliche Person möglich sind, ist die automatisierte Entscheidung erforderlich.[379] Dies ist nur bei Massengeschäften oder zeitkritischen Verträgen der Fall.[380] Die automatisierte Kreditentscheidung lässt sich damit auf Art. 22 Abs. 2 lit. a) DSGVO stützen.[381] Eine Ausnahmezulassung personalisierter Preisbildung ist zumindest bei Massengeschäften im Online-Handel denkbar.[382] Wie auch bei Art. 6 Abs. 1 DSGVO geht Art. 22 Abs. 2 lit. a) der Ausnahmezulassung der Einwilligung im vertraglichen Verhältnis vor.

Hinsichtlich der Informationspflichten im Rahmen des Art. 22 Abs. 2 lit. a) DSGVO ergeben sich zunächst keine Unterschiede zu oben.[383] Problematisch ist dann auch hier, wenn nicht nachvollziehbare selbstlernende Systeme zum Einsatz kommen, bei denen die Outputs und damit Folgen der automatisierten

---

[377] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 43.

[378] Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 30. Die Erforderlichkeit setzt voraus, dass die Bonitätsprüfung für den Vertragsschluss erforderlich ist, was nur bei einer entsprechenden vertraglichen Vereinbarung oder einer gesetzlichen Pflicht der Fall ist, so Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 43. Einschränkend Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Veil*, Art. 22 Rn. 78, der eine Erforderlichkeit nur dann anerkennen will, wenn die verantwortliche Stelle ein besonderes Risiko trägt.

[379] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 25. Er stellt darauf ab, dass die Einbeziehung einer natürlichen Person in die Entscheidung „aufgrund der reinen zu verarbeitenden Datenmenge mitunter unpraktisch oder schlicht unmöglich" ist. Ebenso Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 31a, wonach erforderlich „nicht gleichbedeutend mit ‚sinnvoll' bzw. ‚wünschenswert' [ist], sondern […] vielmehr ‚unvermeidlich' bzw. ‚unumgänglich' [meint]". Befürwortend auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 42. AA Plath, DSGVO/BDSG/*Kamlah*, Art. 22 Rn. 8, wonach auch wirtschaftliche Erwägungen eine Rolle spielen können.

[380] Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 43; *Golland*, CR 36 (2020), 186, 193.

[381] So auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 43; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 29.

[382] So *Golland*, CR 36 (2020), 186, 193.

[383] Siehe Kapitel 4 C. III. 3. a) bb) (1). Zu informieren ist über die Grundzüge des technischen Verfahrens der Profilverwendung, dass nämlich durch die Eingabe von Profil und gegebenenfalls weiteren Anwendungsdaten in einen Lösungsalgorithmus eine automatisierte Entscheidung erzeugt wird.

Entscheidung nicht mehr prognostiziert werden können.[384] Die Einwilligung kann sich dann auf diese nicht erstrecken. Wie ausgeführt, werden in der Praxis aber regelmäßig Vorkehrungen getroffen, damit Algorithmen sich nicht gänzlich frei und hinsichtlich ihrer Entscheidungsergebnisse und -folgen unvorhersehbar entwickeln.[385] Um die Tragweite der Einwilligung in die automatisierte Entscheidung richtig einschätzen zu können, wird vielfach auch im Rahmen der Ausnahmezulassung nach Art. 22 Abs. 2 lit. a) DSGVO eine Aufklärung über die „involvierte Logik", wie dies in Art. 13 Abs. 2 lit. f) DSGVO – hierzu im Anschluss genauer[386] – normiert ist, gefordert. Während die einen dann nicht zwischen den Inhalten der Informationspflicht nach Art. 22 Abs. 2 DSGVO und Art. 13 DSGVO unterscheiden, fordern andere im Rahmen des Art. 22 Abs. 2 DSGVO einen abgesenkten, nämlich die Einwilligungsfähigkeit herstellender Aufklärungsmaßstab, lassen dann aber offen, was dieser im Einzelnen enthalten soll.[387]

4. Ergebnis

Für die Steuerung der autonomen Systeme durch den Rechtmäßigkeitsgrundsatz ergibt sich zusammenfassend das folgende Bild:

Bei der Modellbildung verlangt die Zweckbestimmung, dass auf das zweistufige Profilbildungsverfahren und die Rolle der Modellbildung darin, im Übrigen auf den Anwendungskontext und gegebenenfalls erwartete generalisierbare Inhalte des Modells, etwa Interessen oder Vorlieben, hingewiesen wird. Der Zweckbindungsgrundsatz steht einer Umwidmung von Daten zu Trainingsdaten sowie einer Mehrfachverwendung von Trainingsdaten aufgrund des geringen Gefährdungspotentials der Modellbildung überwiegend nicht entgegen. Voraussetzung ist aber ein Hinweis an die betroffenen Personen, da diese in der Regel nicht mit einer derartigen Mehrfachverwendung ihrer Daten rechnen müssen. Werden Daten von Dritten zugekauft, handelt es sich in der Regel um eine Zweckänderung. Ihre Verwendung als Trainingsdaten setzt eine Einwilligung einer jeden im Datensatz repräsentierten betroffenen Person voraus.

Die Modellbildung stützt sich überwiegend auf den Zulassungsgrund der Einwilligung und der Interessensabwägung. Denn die Modellbildung ist nur Effektivierung, nicht Notwendigkeit eines automatisierten oder personalisier-

---

[384] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 52. Vgl. allgemein zur Begrenzung des Zulassungstatbestands aufgrund des Umfangs möglicher Informationen Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 35a.

[385] Siehe oben Kapitel 4 C. 3. a) aa).

[386] Siehe hierzu Kapitel 4 D. III. 3. b).

[387] In der Literatur wird im Rahmen des Art. 22 Abs. 2 lit. c) DSGVO dennoch häufig undifferenziert auf die Anforderungen des Art. 13–15 DSGVO verwiesen, vgl. etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 53; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 30, 32; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 42.

ten Dienstes. Aufgrund des geringen Risikos kann der Verantwortliche frei zwischen den Zulassungsgründen wählen. Sofern keine besonders sensiblen Daten verarbeitet werden, ist die Modellbildung in der Regel nach Art. 6 Abs. 1 lit. f) DSGVO zulässig, denn das Risiko für betroffene Personen ist typischerweise gering. Gruppenbezogene Interessen können zwar betroffen sein, sie sind aber nicht berücksichtigungsfähig. Wichtig ist, dass die Modellbildung für die betroffene Person nicht überraschend ist. Vertiefte Informationen über das technische Verfahren bedarf es weder im Rahmen der Einwilligung noch der Interessensabwägung.

Die Zweckbestimmung bei der Profilerstellung bedarf eines Hinweises auf die Individualisierung und den Anwendungskontext. Herausforderungen bezüglich des Zweckbindungsgrundsatzes wurden nicht näher untersucht. Der Zulassungsgrund der vertragsimmanenten Zulassung setzt voraus, dass gerade eine Personalisierung für die vorvertragliche Maßnahme, die Vertragsgestaltung oder für die Vertragserfüllung vereinbart wurde. Personalisierte Werbemaßnahmen können nicht nach Art. 6 Abs. 1 lit. b) DSGVO zugelassen werden. Die Einwilligung verlangt eine Aufklärung über das zweistufige Profilbildungsverfahren, insbesondere muss dabei klar sein, dass aus Rohdaten durch Abgleich mit Erkenntnissen über andere neue Daten gebildet werden. Ob die Profilbildung anhand der Interessensabwägung zu rechtfertigen ist, entscheidet sich vor allem anhand des Inhalts des Profils: Umfangreiche oder sensible Profile sind nicht über Art. 6 Abs. 1 lit. f) DSGVO rechtfertigbar. Auch soweit aus der späteren Profilverwendung der betroffenen Person Nachteile drohen, muss dieser Rechtfertigungsgrund ausscheiden. Schutzmaßnahmen sind hier kaum denkbar: Entweder bieten sie keinen Schutz gegen Autonomiegefährdungen oder sie führen zu Funktionsstörungen der Systeme. In der Regel ist der Zulassungsgrund des Art. 6 Abs. 1 lit. f) DSGVO von der Einwilligung verdrängt, da sich die Profilbildung als risikoreiche Datenverarbeitung darstellt. Bei all diesen Zulassungsgründen ist herausfordernd, dass durch die Profilbildung aus Rohdaten neue Erkenntnisse gebildet werden. Im Ergebnis ist dies eine Frage der Vorhersehbarkeit. Sind die Profilinhalte aufgrund fehlender Nachvollziehbarkeit des Modells nicht mehr vorhersagbar, steht dies der Zulassung entgegen, allerdings nur, wenn es sich um eine insgesamt risikoreiche Profilbildung handelt.

Für die Profilverwendung verlangt der Zweckfestlegungsgrundsatz eine konkrete Beschreibung des Anwendungszwecks. Die Mehrfachverwendung desselben Profils in verschiedenen Kontexten wurde nicht näher untersucht. Die Profilverwendung als Datenverarbeitung kann über Art. 6 Abs. 1 lit. b) DSGVO gerechtfertigt werden, wenn die Automatisierung der Vertragsgestaltung oder der vorvertraglichen Maßnahmen zwischen den Parteien vereinbart wurde, auch dann, wenn der Vertragsgegenstand selbst sich auf ein autonomes System bezieht. Die Rechtfertigung über die Einwilligung setzt eine Aufklärung über das Profilverwendungsverfahren voraus, Details zum technischen

Verfahren bedarf es nicht. Eine Rechtfertigung über die Interessensabwägung ist nur möglich, wenn das Profil keine sensiblen Inhalte aufweist und die Profilverwendung keine Nachteile, insbesondere keine erheblichen Autonomiegefährdungen erwarten lässt. Personalisierte Werbemaßnahmen anhand detailreicher Profile sind daher in der Regel nicht rechtfertigbar. Die Profilverwendung ist eine risikoreiche Datenverarbeitung, der Zulassungsgrund der Interessensabwägung ist daher in der Regel durch die Einwilligung verdrängt. Die bei der Profilbildung aufgeworfene Problematik, inwieweit über Profilinhalte zu informieren ist, stellt sich hier erneut, denn ohne Einblick in die Profilinhalte werden am Ende Daten freigegeben, die die betroffene Person nicht kennt. Vorwiegend wird die Information im Rahmen der Profilbildung für ausreichend erachtet. Die Intransparenz und fehlende Nachvollziehbarkeit des Lösungsalgorithmus stellt ihrerseits vor Herausforderungen. Kann die betroffene Person die Folgen der Profilverwendung nicht mehr vorhersehen, muss der Verantwortliche hierüber aufklären. Kann er dies nicht, wie dies bei Lösungsalgorithmen aus menschlich unverständlichen subsymbolischen Lernverfahren der Fall sein kann, so scheidet die Zulassung über die Einwilligung aus und geht, zumindest bei risikoreichen Anwendungskonstellationen, das Interesse der betroffenen Person im Rahmen der Interessensabwägung vor. Für die Zulassung automatisierter Entscheidungen nach Art. 22 DSGVO ergibt sich demgegenüber nichts Neues, wenngleich Bezugspunkt die automatisierte Entscheidung, nicht die Datenverarbeitung ist. Die vertragsimmanente Ausnahmezulassung ist nach der überwiegenden Ansicht nur bei Massengeschäften oder zeitkritischen Verträgen denkbar.

IV. Bewertung des Zweckfestlegungs- und des Rechtmäßigkeitsgrundsatzes als Instrumente zur Regulierung autonomer Systeme

Die Untersuchung lässt erkennen, wie die DSGVO den Regulierungszugriff auf sämtliche Verarbeitungsstufen und damit autonome Systeme insgesamt konkret ausgestaltet. Zweckfestlegungs- und Rechtmäßigkeitsgrundsatz stellen Anforderungen sowohl für die Modell- und Profilbildung als auch die Profilverwendung. Die Regulierungsintensität wird dabei entsprechend der Gefährdung für die betroffene Person von der Modellbildung über die Profilbildung bis hin zur Profilverwendung gesteigert. Die Untersuchung des Zweckfestlegungs- und Rechtmäßigkeitsgrundsatzes hat aber auch die im vorherigen Kapitel aufgestellte These bestätigt, dass die Regulierungsmechanismen nicht präzise die Gefährdung durch autonome Systeme erfassen können, die wesentlich im Modell und Lösungsalgorithmus ihre Ursache hat.[388] Inwieweit Zweckfestlegungs- und Rechtmäßigkeitsgrundsatz ganz spezifisch sinnvolle Steuerungsakzente setzen oder als unzureichend zu bewerten sind, verlangt eine dif-

[388] Siehe Kapitel 4 B. IV. 1. b) und c).

ferenzierte Bewertung, zunächst hinsichtlich des Zweckfestlegungsgrundsatzes (1.) und im Anschluss der Rechtmäßigkeitsgrundsatzes (2.).

1. Bewertung des Zweckfestlegungsgrundsatzes

Für die Bewertung ist zwischen Bildung des Modells (a)) sowie der Profilbildung und -verwendung (b)) zu differenzieren. Die Erwägungen hinsichtlich der Modellbildung lassen sich auch auf die Bildung des Lösungsalgorithmus übertragen. Um das Ergebnis vorwegzunehmen: Der Zweckfestlegungsgrundsatz ist insgesamt positiv zu bewerten. Insbesondere sorgt er für einen angemessenen Interessenausgleich hinsichtlich der Gefährdungen durch Maschinelle Lernverfahren.

a) Bewertung im Hinblick auf die Modellbildung im Maschinellen Lernverfahren

Da Zweckbestimmungsgrundsatz (aa)) und Zweckbindungsgrundsatz (bb)) unterschiedliche Steuerungseffekte freisetzen, ist zwischen diesen zu unterscheiden.

aa) Zweckbestimmung bei der Modellbildung

Dieser Steuerungsansatz der Zweckbestimmung steht im Gegensatz zur Zielausrichtung Maschineller Lernverfahren, bislang unerkannte Zusammenhänge in den Datenbeständen zu erkennen und hieraus neue Verwendungsszenarien zu erschließen.[389] Der Zweckbestimmungsgrundsatz wird daher vielfach als bedeutendes Innovationshemmnis des Maschinellen Lernens erkannt.[390] Die Untersuchung hat jedoch gezeigt, dass dies nur bedingt der Fall ist. Denn gesteckt wird nur ein sehr grober Rahmen: Bei der Modellbildung müssen allein der Anwendungskontext und mögliche grobe Inhaltsgruppen wie Vorlieben, Interessen oder Zuverlässigkeit festgelegt werden. Der Zweckbestimmungsgrundsatz zwingt aber nicht zu einer Vorabdefinition und -festlegung späterer Modellinhalte. Dies erlaubt Analysen der Zusammenhänge in den Daten in verschiedene inhaltliche Richtungen. Die Festlegung auf bestimmte An-

---

[389] So auch *Paal*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, Rn. 13. Vgl. auch *Norwegian Data Protection Authority*, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 18. Allgemein für die Big-Data-Analyse bzw. das Data Mining *Zarsky*, Yale J.L. & Tech. 5 (2003), 1, 4.

[390] Vgl. *Tupay/Ebers/Juksaar u.a.*, Juridica International 30 (2021), 99, 102. Mit anschaulichen Beispielen *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 140 f. Vgl. auch, wenngleich allgemein zur Big-Data-Analyse, *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 99, ebenso *Zarsky*, Setton Hall Law Review 47 (2017), 995, 1005 f.

wendungskontexte und Grobinhalte erscheint nicht unangemessen, da der Verantwortliche regelmäßig eine bestimmte Anwendung – etwa die Informationsfilterung oder ein Kredit-Scoring – vor Augen haben wird.[391] Der Zweckbestimmungsgrundsatz stellt sich auch nicht nachvollziehbaren Modellbildungen nicht entgegen, solange sich die Modellinhalte innerhalb der geforderten Grobbeschreibung der Zweckbestimmung halten. Zugleich grenzt dieser grobe Rahmen das Maschinelle Lernverfahren in sinnvoller Weise ein. Er verhindert, dass Verantwortliche ohne Erkenntnisziele oder Anwendungskontexte vor Augen Daten nach potentiell brauchbarem Wissen durchforsten. Der Zweckbestimmungsgrundsatz unterbindet zudem die Entstehung von Algorithmen, die sich gänzlich von der menschlichen Vorgabe entfernen und sich überhaupt nicht mehr in menschliche Sinnmuster – Anwendungskontext einerseits, inhaltliche Themen andererseits – einordnen lassen und damit jenseits der Beschreibung des Anwendungskontextes und der Grobinhalte liegen.[392] Dies ist nach den Prämissen des Datenschutzrechts sinnvoll und richtig. Sowohl wenn der Verantwortliche Analyseziele des Maschinellen Lernverfahrens bewusst offen lässt, als auch wenn er diese aufgrund der fehlenden Nachvollziehbarkeit vorab nicht benennen kann, entstehen intransparente und unkontrollierbare Datenverarbeitungsstrukturen, die das Datenschutzrecht als autonomiegefährdend erkennt und verhindern will. Diese Annahme erscheint auch im Hinblick auf die Bedeutung des Modells im zweistufigen Profilbildungsverfahren schlüssig. Denn dann können im Anschluss Profile gebildet werden, deren Inhalte sich nicht mehr prognostizieren oder nachvollziehen lassen und so Autonomiegefährdungen oder Diskriminierungen begründen können. Der Zweckbestimmtheitsgrundsatz erweist sich daher im Hinblick auf die Modellbildung als angemessen.

bb) Zweckbindung bei der Modellbildung

Der Zweckbindungsgrundsatz verhindert die Mehrfachverwendung von Daten und stellt sich damit als Hemmnis für das datenintensive Maschinelle Lernverfahren dar.[393] Nach der Erkenntnis der Arbeit belässt die DSGVO aber einigen

---

[391] Die ergebnis- und anwendungsoffene Analyse von Datensätzen entspricht eher der Tätigkeit von Data Scientists, siehe hierzu oben Kapitel 1 A. II. 1.

[392] Diese Konstellation sprechen *Paal*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, Rn. 13; *Norwegian Data Protection Authority*, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 18 an, denen zufolge die Offenheit und Unvorhersehbarkeit der erlernten Regeln im Maschinellen Lernverfahren dem Zweckbestimmungsgrundsatzes entgegenstehen können.

[393] Die DSGVO öffnet sich der Mehrfachverwendung von Daten gerade durch den Mechanismus der Zweckinkompatibilität. So auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 6 Abs. 4 Rn. 58. Siehe überdies *Norwegian Data Protection Au-*

Raum für multiple Datennutzungen. Solange betroffene Personen auf die Umwidmung oder Mehrfachverwendung hingewiesen werden, ist die Zweckänderung typischerweise zulässig, zudem kann der Verantwortliche durch Pseudonymisierungen eine Zweckkompatibilität herbeiführen.[394] Allein die Mehrfachverwendung sensibler Daten sowie der Zukauf von Daten stellt in der Regel eine Zweckänderung im engeren Sinne dar. Eine Zulassung derartiger Zweckänderungen über die Einholung einer Einwilligung ist zwar möglich. Da dies aber (allzu) ressourcenintensiv ist, wird dies in der Praxis kaum sinnvoll realisiert werden können,[395] die Zweckänderung demnach unzulässig bleiben. Im Ergebnis erscheint dies aber richtig. Die Verarbeitung von sensiblen Daten ist stets risikoreich. Auch die Verarbeitung zugekaufter vielschichtig zusammengesetzter Trainingsdatensätze unterschiedlichsten Inhalts und verschiedener oder gar unbekannter Herkunft weist ein hohes Gefährdungspotential auf, sind doch Folgen und Risiken der ursprünglichen Datenfreigabe für die betroffenen Personen überhaupt nicht mehr überschaubar. Am Ende führt der Zweckbindungsgrundsatz zu einem angemessenen Ausgleich zwischen den Interessen betroffener Personen und Verantwortlichem, er verhindert die praktische Umsetzbarkeit Maschineller Lernverfahren nicht.

b) Bewertung im Hinblick auf die Profilbildung und -verwendung

Der Zweckbestimmungsgrundsatz hinsichtlich der Profilbildung und -verwendung setzt sinnvolle Steuerungsakzente, ohne allzu beschränkend zu wirken.

---

thority, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 17.

394 Zu diesem Ergebnis, allerdings allgemein hinsichtlich Big-Data-Analysen, kommt auch *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 291. Diese Öffnung hin zur Mehrfachverwendung von Daten entspricht gerade dem Sinn und Zweck der Konzeption der Zweckänderung in der DSGVO, die ein enges Verständnis prägt und nur bei Unvereinbarkeit der Verarbeitungszwecke eine Mehrfachverwendung von Daten unterbinden soll. Siehe ausdrücklich *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 4: „The prohibition of ‚incompatibility' [...] does not altogether rule out new, different uses of data" und weiter *dies.*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 21: „[T]he legislators intended to give some flexibility with regard to further use. [...] The fact that the further processing is for a different purpose does not necessarily mean that it is automatically incompatible: this needs to be assessed on a case-by-case basis".

395 Denn die Einwilligung verlangt, dass Verantwortliche jede im Datensatz repräsentierte Person herausfiltern, um ihre Einwilligung ersuchen und mit entsprechenden Informationen versorgen. Ab einer bestimmten Quantität und Komplexität des Datensatzes wird dies aus technischen oder wirtschaftlichen Gründen nicht mehr möglich sein. Vgl. *Valkanova*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 336, Rn. 5; *Culik/Döpke*, ZD 7 (2017), 226, 228; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 285. Für Big-Data-Analysen *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 99.

Bei der Profilbildung zwingt der Zweckbestimmungsgrundsatz zur Vorfestlegung auf die Individualisierung, nach anderer Ansicht: auf einen bestimmten Anwendungskontext. Einzelinferenzen müssen dagegen nicht detailreich offengelegt werden. Auch hier ist innovationshindernde Wirkung gering, da der Analyserahmen sehr weit gesteckt ist: Innerhalb des benannten Anwendungskontextes und der Grobinhalte sind Inferenzen unterschiedlichsten Inhalts möglich. Diese müssen auch nicht nachvollziehbar bzw. prognostizierbar sein, solange sie sich innerhalb dieses Rahmens halten. Ohnehin wird der Verantwortliche Profile in der Regel mit Blick auf einen bestimmten Anwendungskontext bilden, die Anforderung ist daher in der Praxis kaum belastend. Die Begrenzungswirkungen des gesetzten Rahmens sind sinnvoll: Unterbunden werden ergebnisoffene, kontextlose und anwendungsunspezifische Profilbildungen, ebenso solche, die so fern von menschlichen Sinnzusammenhängen liegen, dass sie sich nicht mehr in die Beschreibung des Anwendungskontextes fügen. Dies ist sinnvoll, da Autonomiegefährdungen gerade darin ihre Ursache haben, dass betroffene Personen nicht mehr überschauen können, welche Erkenntnisse über sie gewonnen und welche Folgen aus der Datenverarbeitung sie befürchten müssen. Die Zweckbestimmung macht diese Erkenntnisse zumindest in groben Zügen vorhersehbar, ohne den Erkenntnismöglichkeiten autonomer Systeme allzu strenge Grenzen zu setzen.

Die nämlichen Erwägungen lassen sich auf die Profilverwendung übertragen, bei der ebenso zwar der spezifische Anwendungskontext benannt, nicht aber konkrete Inhalte der Entscheidung oder Steuerung prognostiziert werden müssen. Die Begrenzungswirkung ist bei der Profilverwendung noch ungleich geringer: Dem Verantwortlichen wird stets eine bestimmte Anwendung vor Augen stehen. Dass das autonome System eigenmächtig ganz neue Anwendungskontexte erschließt, liegt nicht in seinem Interesse. Wäre dies der Fall, wäre es dagegen richtig, dass über den Zweckbestimmungsgrundsatz abgesichert wird, dass es nicht zu völlig unerwarteten und unerwartbaren Ausgaben des Systems kommt.

Der Zweckbestimmungsgrundsatz definiert im Ergebnis die äußersten Grenzen der fehlenden Nachvollziehbarkeit des Modells bzw. des Lösungsalgorithmus und deren Outputs: Er verhindert, dass die Ergebnisse so wenig menschlich verständlich sind, dass sie sich menschlich vorab überhaupt nicht mehr beschreiben, also auch nicht in einen übergeordneten Zweckrahmen einordnen lassen. Für die Erstellung selbstlernender Algorithmen setzt er damit einen sinnvollen, zugleich nicht allzu weit reichenden Steuerungsrahmen.

2. Bewertung des Rechtmäßigkeitsgrundsatzes

Der Rechtmäßigkeitsgrundsatz erlaubt, inhaltliche Angemessenheitskriterien für alle Verarbeitungsstufen aufzustellen. Bei der Profilbildung und -verwendung ist dabei die Annahme zutreffend, dass gewisse Folgen und Gefährdun-

gen der Verarbeitung bereits im zu verarbeiteten Rohdatum angelegt sind und so über die Zulassung des Rohdatums auch über die Angemessenheit der Folgen entschieden werden kann. Auch erlaubt der Rechtmäßigkeitsgrundsatz Nuancierungen hinsichtlich der Gefährdungspotentiale der einzelnen Verarbeitungsstufen. Zugleich können Risikomerkmale der jeweils vorangehenden oder nachfolgenden Verarbeitungsstufe bei Angemessenheitsbewertung der spezifischen Verarbeitungsstufe berücksichtigt werden, so also etwa, wenn die Folgen der Profilverwendung auch bereits für die Rechtmäßigkeit der Profilbildung maßgeblich sind. Die DSGVO erlaubt damit eine koordinative Regulierung. Überwiegend ist aber, so die Erkenntnis der Untersuchung, der Rechtmäßigkeitsgrundsatz im Hinblick auf autonome Systeme an Grenzen geführt. Dies liegt schon daran, dass eine echte Zulassungsfrage hinsichtlich der Modellbildung gar nicht gestellt werden kann. Aus der Blickrichtung der praktischen Schutzwirkung der DSGVO ist dies unproblematisch, solange die allgemeinen Regeln, wie sie für sämtliche Datenverarbeitungen gelten, ausreichen, um die betroffenen Personen vor Gefährdungen, dann also der Profilbildung und -verwendung zu schützen. Die vorstehende Untersuchung hat jedoch gezeigt, dass dies nicht der Fall ist. Denn die fehlende Nachvollziehbarkeit und damit auch Vorhersehbarkeit führt dazu, dass der Rechtmäßigkeitsgrundsatz bei der Profilbildung und -verwendung versagt.[396] Die fehlende Nachvollziehbarkeit sowie quantitative und qualitative Überlastungen führen zu Schwächungen des Rechtmäßigkeitsgrundsatzes.

Dies soll im Einzelnen ausgeführt werden, und zwar für die Ebenen der Modellbildung (a)), der Profilbildung (b)) und der Profilverwendung (c)). Darüber hinaus stellt der Rechtmäßigkeitsgrundsatz vor Herausforderungen, die übergreifend für alle Verarbeitungsstufen gelten (dI). Die im Rahmen der Bewertung des Rechtmäßigkeitsgrundsatzes für das Modell angestellten Überlegungen lassen sich dabei auf den Lösungsalgorithmus übertragen.

a) Bewertung im Hinblick auf die Modellbildung im Maschinellen Lernverfahren

Nach der vorgestellten Untersuchung ist die Modellbildung regelmäßig zulässig, zumindest solange betroffenen Personen die Verarbeitung ihrer Daten im Maschinellen Lernverfahren bekannt sind. Dabei fällt aber auf, dass die eigentlichen Gefährdungsmomente gar nicht adressiert werden. Hieraus wird erkenntlich, dass die gesamte Regulierungssystematik nicht auf die Regulierungsbedarfe des Maschinellen Lernverfahrens eingerichtet ist. Dies liegt schon daran, dass die DSGVO auf das Einzeldatum und die Einzelverarbeitung (aa)) und die Einzelperson fokussiert (bb)), vor allem aber daran, dass das Algorithmische in der DSGVO ausgeblendet bleibt (cc)). Die Erwägungen lassen

[396] Siehe hierzu bereits oben Kapitel 4 B. IV. c).

sich, soweit der Lösungsalgorithmus anhand personenbezogener Daten trainiert wird, übertragen.

aa) Datenkollektiv und Verarbeitungskollektiv als Quelle Maschineller Wissensextraktion

Die maßgebliche Erkenntnisquelle Maschineller Lernverfahren ist das Datenkollektiv: Die gefundene Regel stellt sich als stochastisches Muster der Datenstrukturen dar. Das Einzeldatum ist dabei nicht von Interesse.[397] Die DSGVO fokussiert in ihrer Regulierungssystematik dagegen auf das Einzeldatum.[398] Die Einordnung eines Einzeldatums in einen größeren Verarbeitungs- und Erkenntniszusammenhang wird datenschutzrechtlich nicht abgebildet.[399] Der Algorithmus wird zudem in einem iterativen Trainingsverfahren gebildet. Das Regelwerk stellt sich als Gesamtkonstrukt dieser Einzelverarbeitungen dar. Die Verarbeitung des einzelnen Datums geht in dieser Trainingsarchitektur auf, ohne dass sich vorhersehen oder nachträglich feststellen ließe, wie die einzelne Datenverarbeitung im algorithmischen Regelwerk aufgeht und welche Bedeutung sie für dieses hat. Es ist damit das Verarbeitungskollektiv, nicht die Einzelverarbeitung, in der die wesentliche Gefährdung ihren Ursprung hat.[400] Zwischen Einzeltrainingsdatum bzw. Einzelverarbeitung und Modell bestehen keine direkten Verbindungslinien.[401]

bb) Steuerungsverkürzungen individualistischer Steuerungsperspektiven

Der Unionsgesetzgeber unterstellt, dass Gefährdungen von der Datenverarbeitung allein für die betroffene Person ausgehen können. Dies erweist sich in einer Welt autonomer Systeme als unzutreffend. Sowohl fremdschädigende Effekte ((1)) als auch die Repräsentation von Gruppeninteressen ((2)) sind im Rechtmäßigkeitskonzept nicht aufgenommen.

---

[397] *Floridi*, in: Taylor/Floridi/van der Sloot (Hrsg.), Group Privacy, 2017, S. 83, 98 vergleicht dies anschaulich mit einem Sardinenschwarm: Nicht auf den einzelnen Fisch, sondern auf den Schwarm ist der Fokus gerichtet; dieser, nicht der einzelne Fisch bedarf des Schutzes.

[398] Siehe auch oben Kapitel 4 B. I. 2.

[399] Einen „atomistischen Ansatz" kritisiert auch *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 92. Er bezieht dies aber auf sozioökonomische Wirkungen der Wissensvorsprünge von Big-Data-Unternehmen insgesamt, für die die DSGVO „blind" ist.

[400] Siehe auch bereits *Roßnagel*, MMR 8 (2005), 71, 75: „Gegenstand der Kontrolle müssen Systeme mit ihren Funktionen und Strukturen sein, nicht so sehr die individuellen Daten".

[401] Siehe hierzu bereits oben Kapitel 4 B. IV. 3. c).

(1) Fehlende Integration fremdschädigender Datenverarbeitungen

In der DSGVO ist nicht die Konstellation abgebildet, wie sie für das zweistufige Profilbildungsverfahren typisch ist, dass nämlich die Verarbeitung eigener Daten einen Dritten gefährden.[402] Die Modellbildung erlaubt Erkenntnisse über Persönlichkeitsmerkmale einer bestimmten Person, ohne dass diese derartige Einblicke freiwillig zugestanden, d.h. entsprechende Daten, geteilt hat.[403] Die Datenfreigabe durch eine Person in der Modellbildung bedingt damit immer auch eine Informationspreisgabe für Dritte, nämlich diejenigen, für die anhand des Modells ein Profil gebildet wird.[404] Für die Person, die ihre Daten für ein Modell freigibt, muss im Übrigen nicht notwendig ein Profil gebildet werden.[405] Es ist also denkbar, dass sie durch die Datenfreigabe allein andere gefährdet.

(2) Unzureichende Repräsentation von Gruppeninteressen

Die Erkenntnisse in der Modellbildung werden nicht über Einzelpersonen, sondern über die Personengemeinschaft im Trainingsdatensatz gebildet. Dies kann eigene Gefährdungen auslösen, nämlich Diskriminierungen, Stigmatisierungen und andere unerwünschte Effekte der Klassifizierung. Diese Interessen von Minderheiten bzw. der Gemeinschaft insgesamt finden im Rechtmäßigkeitsgrundsatz keine Berücksichtigung.[406] Die Zulassung- und Angemessenheitsfrage wird immer nur der betroffenen Person und im Hinblick auf die betroffene Person gestellt.[407] Nachteilige Effekte einer Maßnahme für (Minderheiten-)Gruppen oder einzelne Angehörige einer Gruppe bleiben ausgeblen-

---

[402] Siehe hierzu eingehend *Hornung*, in: Hoffmann-Riem (Hrsg.), 94 f.; *Hermstrüwer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 99, S. 105–107, 163-165; *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 56; *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 307 f. Vgl. auch *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 9; *Vatanparast*, ZaöRV 80 (2020), 819, 837. Siehe auch *Roßnagel*, ZD 3 (2013), 562, 566.

[403] *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 5; *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 94; *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 56; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 163 f.

[404] Dabei gilt: Je mehr Personen ihre Daten für die Modellbildung freigeben, desto umfassender, detailgenauer und präziser fallen die Modellinhalte aus und desto tiefgehender sind die Profile, die mittels dieses Modells erzeugt werden können. So auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 164.

[405] Noch allgemeiner *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 307: „If this model is applied to individuals, these individuals are not necessarily the people whose data have been processed in the first two phases".

[406] In der DSGVO sind allerdings in Art. 9, Art. 22 Abs. 4 DSGVO Verbote für Diskriminierungen normiert.

[407] Selbiges gilt dann für die Ausnahmezulassung der automatisierten Entscheidung, siehe hierzu *Lorentz*, Profiling, 2019, S. 271 f.

det.[408] Im Rechtmäßigkeitsgrundsatz können zwar im Rahmen der Interessensabwägung diskriminierende Wirkungen Berücksichtigung finden. Dies setzt aber voraus, dass die betroffene Person selbst Angehörige der diskriminierten Gruppe ist.[409] Sonstige inakzeptable Ungleichbehandlungen sind nicht berücksichtigungsfähig. Bei der automatisierten Entscheidung, die keine Interessensabwägung kennt, bleiben gruppenspezifische Aspekte völlig außen vor.[410] In der individualistischen Perspektive werden zudem gesamtgesellschaftliche Fehlentwicklungen durch autonome Systeme nicht offenbar und können durch das Datenschutzrecht nicht adressiert werden.[411]

cc) Gefährdungsmoment in algorithmischer Regelfindung

Die maschinelle Erkenntnis ist eine algorithmische Interpretation des Trainingsdatensatzes. Der selbstlernende Algorithmus addiert demnach nicht die natürlich-semantischen Aussagegehalte der einzelnen Daten, sondern formt nach stochastischen Grundsätzen eine algorithmische Regel aus dem Datenkollektiv. Das Modell enthält am Ende ein analytisch-interpretatives „Mehr" gegenüber dem Datenkollektiv. Auch beim Maschinellen Lernverfahren wird letztlich, wie auch beim Profil, Wissen gebildet, das über den Informationsgehalt der Daten hinausreicht.[412] Dieses algorithmische Regelwerk ermöglicht Erkenntnisse über die Einzelperson jenseits des Rohdatums. Es ist also jenes über das Rohdatum hinausgehende Wissen, jenes „Mehr", das im Rahmen der Profilbildung dem Rohdatum hinzugefügt wird und den eigentlichen Informationsgewinn ermöglicht.[413] Zugleich ist dieses „Mehr" nur beschränkt menschlich verständlich und steuerbar. Die Intransparenz und Unkontrollierbarkeit

---

[408] *Hoffmann-Riem*, in: ders. (Hrsg.), Big Data, 2018, S. 11, 59; *Lorentz*, Profiling, 2019, S. 271 f. Vgl. ausführlich zu Fragen der Group Privacy und Class Actions *Edwards/Veale*, SSRN Journal 2017, 35–36, 74-75.

[409] Denn die Interessensabwägung erfolgt stets mit Blick auf die betroffene Person. Berührt die Datenverarbeitung allein Interessen Dritter, ist dies im Rahmen des Art. 6 Abs. 1 lit. f) DSGVO unbeachtlich. Vgl. hierzu Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/*Schantz*, Art. 6 Abs. 1 Rn. 102. Allein auf die Diskriminierung der betroffenen Person stellt auch *Lorentz*, Profiling, 2019, S. 258 ab. Offen lässt dies zwar der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 16, der ganz allgemein Schutzmaßnahmen gegen diskriminierende Profilinhalte fordert. Die *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 38 stellt aber allein auf Interessen der betroffenen Person ab.

[410] Eingehend *Lorentz*, Profiling, 2019, S. 271 f.

[411] Siehe hierzu *Vatanparast*, ZaöRV 80 (2020), 819, 839.

[412] Vgl. hierzu *Lorentz*, Profiling, 2019, S. 335.

[413] Siehe hierzu oben Kapitel 4 B. IV. 2.

von Datenverarbeitungen werden so noch gesteigert.[414] Das Modell stellt damit ein eigenständiges, neues Gefährdungsmoment dar. Dieser haftet aber nicht dem Datum bzw. dem Datenkollektiv, sondern der stochastisch-algorithmische Interpretation der aggregierten Daten, d.h. dem Modell als algorithmisches Regelwerk an. Demgegenüber konzentriert die Zulassungsprüfung des Rechtmäßigkeitsgrundsatzes allein auf die Daten und lässt jenes „Mehr", den Algorithmus, außer Betracht.[415] Dies blockiert die Steuerungswirkung des Rechtmäßigkeitsgrundsatzes: Wer über die Zulassung der Verarbeitung des Einzeldatums bei der Modellbildung entscheidet, sagt damit nichts über die Zulässigkeit des algorithmischen Konstrukts aus.

b) Bewertung im Hinblick auf die Profilbildung

Im Hinblick auf die Profilbildung hat die Rechtsanalyse gezeigt, dass über die Zulassung des Rohdatums für die Profilbildung zugleich über die Zulassung der Outputs, d.h. der generierten Profilinhalte entschieden werden kann.[416] Dies ist aber nur dann möglich, wenn zwischen Rohdatum und Profilinhalten prognostizierbare Verbindungslinien bestehen, was bei autonomen Systemen nur bedingt der Fall ist (aa)). Problematisch ist zudem, dass die DSGVO für die Generierung neuer Daten keine eigene Zulassungsfrage stellt (bb)).

aa) Intransparenzbedingte Aufhebung linear-prognostischer Verbindungen zwischen Rohdatum und Profil

Die wesentliche Gefährdung bei der Profilbildung ist die Ermöglichung von Erkenntnissen jenseits des Rohdatums. Die Entscheidung über die Datenfreigabe nach Art. 6 Abs. 1 DSGVO richtet sich demnach maßgeblich danach, ob diese Erkenntnisse, die aus dem Rohdatum gebildet werden können, als akzeptabel bewertet werden können. Diese Erkenntnisse sind also die Folge der Datenverarbeitung, über deren Angemessenheit nach Art. 6 Abs. 1 DSGVO zu entscheiden ist. Dies setzt voraus, dass die betroffene Person diese Profilinhalte abschätzen kann.[417] Dies bedeutet nicht, dass sie jede einzelne Ableitung vorab kennen muss, wohl aber, dass ihr bekannt ist, mit welchen Profilinhalten sie allgemein zu rechnen hat. Vor Herausforderungen stellt es dann, wenn ein Sys-

---

[414] Siehe hierzu oben Kapitel 4 B. IV. 1. c).

[415] So auch, wenngleich allgemein für Big-Data-Auswertungen, *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 93: „Die Bändigung der […] durch Big-Data-Wissen generierten Macht liegt damit jedenfalls überwiegend außerhalb des Datenschutzrechts". Ähnlich, dort dann allgemein zu automatisierter Profilbildung und Data Mining Verfahren, *Schermer*, CLSR 27 (2011), 45, 52.

[416] Siehe hierzu auch nochmals ausführlich unter Kapitel 5 B. II. 3. a).

[417] Eingehend problematisiert dies auch *Schermer*, CLSR 27 (2011), 45, 50; *Roßnagel*, DuD 40 (2016), 561, 563; *Lorentz*, Profiling, 2019, S. 183 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 98 f.

tem Profilinhalte erzeugt, die sich für die betroffene Person als überraschend darstellen. Problematisch ist es vor allem, wenn menschlich nicht verständliche selbstlernende Algorithmen zum Einsatz kommen. Kann nicht ausgeschlossen werden, dass diese überraschende Profilinhalte generieren, sind die Folgen der Profilbildung menschlich überhaupt nicht mehr vorhersehbar. Eine Einwilligung bzw. vertragsgemäße Zulassung kann dann nicht mehr stattfinden, auch für die Interessensabwägung fehlt es an einer sinnvollen Bewertungsgrundlage. Der Rechtmäßigkeitsgrundsatz bietet für diese Konfliktlage keine Lösungen an. Er attestiert allein die Unzulässigkeit der Verarbeitung, knüpft also eine rechtliche Folge an die fehlende Vorhersehbarkeit, trägt aber zur Überwindung dieser Intransparenz und also zur Verknüpfung der unterbrochenen Verbindungslinien nichts bei.

bb) Fehlende Regulierung der Generierung neuer Daten

Während es bei der Vorhersehbarkeit allein um die Prognose möglicher Profilinhalte geht – dies kann dann auch bloße Grobbeschreibungen, wie Interessen oder Vorlieben – beinhalten, stellt sich mit Blick auf die Rechtmäßigkeit noch eine weitere Problematik. Die inferierten Daten stellen ihrerseits personenbezogene Daten dar.[418] Diese begründen gerade Autonomiegefährdungen, da sie potentiell tiefgreifend, diskriminierend oder fehlerhaft, in jedem Fall intransparent sind.[419] Es ist fraglich, inwieweit dieses besondere Verarbeitungsverfahren, nämlich die originäre Erzeugung neuer Daten, über Art. 6 Abs. 1 DSGVO gerechtfertigt werden kann. Die Kontrollfrage ist nämlich neu aufgeworfen: Die betroffene Person mag mit der Freigabe eines Anwendungsdatums einverstanden sein, etwa dem Wohnort, womöglich aber nicht mit der Freigabe weiterer, daraus abgeleiteter Informationen, etwa dem Vermögensstand.[420] Die Einwilligung in die Verwendung der Output-Daten,[421] wie dies spezifisch Art. 22 DSGVO vorsieht, betrifft eine andere Frage, nämlich die Zulässigkeit im

---

[418] Vgl. statt vieler *Lorentz*, Profiling, 2019, S. 183. Eingehend zu dieser Frage bereits oben Kapitel 4 B. III. 3. a).

[419] Vgl. auch *dies.*, Profiling, 2019, S. 184 f.

[420] *Andreotta/Kirkham/Rizzi*, AI and Society 36 (2021), 1, 6: „[M]any people are concerned, or anxious, about their data being used in ways that go beyond what they originally thought would occur when they first consented". Siehe auch *Edwards/Veale*, SSRN Journal 2017, 36–38. Eingehend zu dieser Frage *Lorentz*, Profiling, 2019, S. 183–187. Siehe auch *Solove*, Harv. L. Rev. 126 (2013), 1880, 1889–1891.

[421] Zu diesem Vorschlag siehe Gola, DS-GVO/*Schulz*, Art. 7 Rn. 36; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 155. Er fordert, dass die Einwilligung gestuft erteilt wird, d.h. für jede Verarbeitungsphase. Nach Abschluss eines Auswertungsverfahrens zur Generierung neuer Daten, für das eine Einwilligung erteilt wurde, müsste dann also eine weitere Einwilligung in die Verarbeitung der neu generierten Daten erteilt werden. In diese Richtung auch *Andreotta/Kirkham/Rizzi*, AI and Society 36 (2021), 1, 6, wonach die Datengenerierung eine Zweckänderung (re-purposed data) darstellt.

Anschluss an die Profilbildung. Es entsteht so eine Schutzlücke, da die betroffene Person in die Verwendung der Input-Daten für die Profilbildung und der Output-Daten für die Profilverwendung einwilligen kann, nicht aber in die Erzeugung der Output-Daten. Zulässigkeitstatbestände für die Generierung neuer Daten sieht die DSGVO nicht vor.[422]

c) Bewertung im Hinblick auf die Profilverwendung

Bei der Profilverwendung wirkt die fehlende Transparenz der Profilinhalte fort. Problematisch ist vor allem die beschränkte menschliche Nachvollziehbarkeit des Lösungsalgorithmus (aa)). Zu Regulierungsschwächen der DSGVO kommt es überdies dadurch, dass schädliche Wirkungen, die aus der Ubiquität und Dauerhaftigkeit automatisierter Entscheidungen und Steuerungen entstehen, im Rechtmäßigkeitsgrundsatz nicht abgebildet werden können (bb)).

aa) Intransparenzbedinge Aufhebung linear-prognostischer Verbindungen zwischen Rohdatum und Profilverwendung

Kommt es bei der Profilbildung zu unerwarteten Einzelinferenzen, führt dies auf Ebene der Profilverwendung zur Verarbeitung von Daten, die der betroffenen Person nicht bekannt sind. Die Steuerungswirkung des Rechtmäßigkeitsgrundsatzes ist damit erheblich gemindert. Ist bereits bei der Profilverwendung das Modell nicht nachvollziehbar, wirkt dies also auch abträglich auf die Zulässigkeit der Profilverwendung. Auch der Lösungsalgorithmus kann Outputs generieren, die zu unüberschaubaren Folgen führen, wenngleich an derartigen Lösungsalgorithmen in der Praxis nur ein geringes Interesse besteht. Kann auch der Verantwortliche bei Einsatz nicht nachvollziehbarer selbstlernender Algorithmen diese Folgen nicht vorab benennen und die betroffene Person entsprechend informieren, so fehlt es, wie schon bei der Profilbildung, an einer hinreichenden Grundlage, um die Angemessenheit der Datenverarbeitung bzw. der automatisierten Entscheidung bemessen zu können. Nach den Wertungen des Rechtmäßigkeitsgrundsatzes ist dann die Datenverarbeitung bzw. automatisierte Entscheidung unzulässig. Wie schon bei der Profilbildung festgestellt, sieht der Rechtmäßigkeitsgrundsatz also keine Lösung für die fehlende Nachvollziehbarkeit des Lösungsalgorithmus vor, sondern knüpft nur eine rechtliche Folge daran.

---

[422] Vgl. auch eingehend *Lorentz*, Profiling, 2019, S. 335–338; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 10. Strenge(re) Anforderungen für das Profiling im Hinblick auf den Rechtmäßigkeitsgrundsatz fordert auch Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 4 Nr. 4 Rn. 8. *Lorentz*, Profiling, 2019, S. 184 erkennt darin einen unauflöslichen Widerspruch: Die betroffene Person kann in die Nutzung von Rohdaten einwilligen, aber nicht in die Erzeugung neuer Daten. Die Einwilligung in die Verwendung der Rohdaten reicht aber nicht so weit, dass die Erzeugung von neuen Daten abgedeckt ist.

bb) Fehlende Abbildung inkrementell-ubiquitärer Gefährdungsdimensionen

Die beschriebenen Autonomiegefährdungen der maschineller Wissensapplikation entstehen häufig nicht aus einer einzelnen Entscheidung oder Steuerung, sondern aus einer ubiquitär-systematischen Verbreitung autonomer Systeme, in der betroffene Personen permanent und umfassend mit Anwendungen autonomer Systeme, etwa Informationsvorschlägen oder Werbemaßnahmen konfrontiert werden.[423] Auch Diskriminierungen schlagen vielfach erst durch, wenn verschiedene Vergleichsgruppen systematisch vorteilhaften bzw. nachteiligen Entscheidungen oder Steuerungen unterworfen sind.[424] Demgegenüber konzentriert die DSGVO auf die einzelne Datenverarbeitung bzw. die einzelne automatisierte Entscheidung. Der Blick für das große Ganze, das Anwendungskollektiv und die gesamtgesellschaftliche Gefährdungsdimension fehlt.

d) Übergreifende Defizite des Rechtmäßigkeitsgrundsatzes

Der Rechtmäßigkeitsgrundsatz kommt sowohl hinsichtlich der Modell- und Profilbildung als auch der Profilverwendung an seine Grenzen, da die Verarbeitungsverfahren sich als äußerst komplex darstellen, zudem die Anzahl der notwendigen Kontrollleistungen in einer Welt autonomer Systeme ins Übermäßige steigt (aa)). Die Notwendigkeit der Zulassung einer jeden Datenverarbeitung bzw. einer jeden automatisierten Entscheidung wirken innovationshinderlich (bb)).

aa) Kontrolllähmungseffekte durch qualitative und quantitative Überforderung

Die Steuerungskonzeption des Rechtmäßigkeitsgrundsatzes verlangt der betroffenen Person einiges ab: Sie muss individuelle Angemessenheitskriterien aufstellen und die jeweilige Datenverarbeitung daran prüfen und dies für sämtliche im Rahmen autonomer Systeme stattfindenden Datenverarbeitungsprozesse. Aber auch Verantwortliche und staatliche Akteure, die über die Zulassung einer jeden Datenverarbeitung nach der Interessensabwägung entscheiden, sind herausgefordert. Aufgrund der Komplexität ((1)), ebenso wie der Anzahl ((2)) der freizugebenden Datenverarbeitungen wird es den jeweiligen Akteuren nicht mehr gelingen, ihre Steuerungsleistung effektiv zu erbringen.

---

[423] Hierauf weist auch hin *Leerssen*, Algorithm Centrism in the DSA's Regulation of Recommender Systems, Verfassungsblog, 29.03.2022. Siehe auch *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 20.

[424] Siehe hierzu eingehend bereits unter Kapitel 2 II. Vgl. auch *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 93, 96–97; *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 19, 31; *Casey/Farhangi/Vogl*, BTLJ 34 (2019), 143, 180 f.

(1) Lähmungseffekte durch Komplexitätsüberlastung

Mit steigender Komplexität von Datenverarbeitungen steigen auch die Anforderungen an die Bewertung der Akzeptabilität einer Datenverarbeitung. Es ist vielfach festgestellt worden, dass der Mensch ab einem gewissen Komplexitätsgrad einer Entscheidung zu Entscheidungsmüdigkeit bis -apathie neigt. In derartigen Konstellationen verlässt sich der Mensch auf Heuristiken, stützt sich also auf irrationale Erwägungen und nimmt vielfach das Risiko verzerrt wahr.[425] Nicht nur die betroffene Person bei der Einwilligung bzw. vertragsimmanenten Zulassung, auch Verantwortliche und staatliche Akteure werden ab einer gewissen Komplexität der Verarbeitung daher an Grenzen kommen. Aufgrund ihrer fachlichen Expertise und ressourcenmäßigen Ausstattung werden Verantwortliche und staatliche Akteure vielfach die anspruchsvolle Abwägungsleistung noch erbringen können, wo die betroffene Person bereits überfordert ist, doch ist auch hier denkbar, dass ab einem bestimmten Komplexitätsniveau ihre Entscheidungsfähigkeit beeinträchtigt ist.

(2) Lähmungseffekte durch Kontrollüberforderung

Der Rechtmäßigkeitsgrundsatz zwingt zur Zulassungsprüfung einer jeden Datenverarbeitung, die durch autonome Systeme vorgenommen werden. Schon im Trainingsverfahren der Modellbildung findet eine Vielzahl einzelner Datenverarbeitungsprozesse statt. Auch bei der Profilbildung werden in der Praxis mehrere Anwendungsdaten ausgewertet, um das Profil besonders detailreich zu gestalten. Vor allem aber wird, sobald autonome Systeme umfassend in den Alltag des Einzelnen Eingang finden sollen, eine Fülle an Zulassungsentscheidungen bezüglich verschiedenster autonomer Systeme auf die betroffene Person zukommen. Am Ende werden betroffene Personen in einer Welt autonomer Systeme mit einer nicht mehr überschaubare Anzahl von Datenverarbeitungsprozessen konfrontiert sein.[426] Dass betroffene Personen dann ihre Zulassungsentscheidung noch effektiv wahrnehmen können und werden, ist praktisch aus-

---

[425] Beobachtbar ist dabei eine Tendenz zur Risikounterschätzung.Vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 238. Er untersucht umfassend die verhaltensökonomischen Irrationalitäten hinsichtlich der Einwilligung im Datenschutzrecht. Siehe etwa zu enthemmenden Effekten bei Unsicherheiten der Folgen einer Datenfreigabe *ders.*, Informationelle Selbstgefährdung, 2015, S. 277–279. Siehe dagegen zu Hemmwirkungen, also einer Risikoüberschätzung, bei ambivalenten Folgen der Datenfreigabe *ders.*, Informationelle Selbstgefährdung, 2015, S. 276 f. Siehe auch *Ausloos/Dewitte*, Int. Data Priv. Law 8 (2018), 4, 22 f.

[426] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 73 spricht zutreffend von einer „Entscheidungshypertrophie". Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 41.

geschlossen.[427] Schon aktuell nehmen betroffene Personen, wie einschlägige Studien belegen, ihre Prüfungskompetenz überwiegend nicht wahr (Click and Consent).[428] Dies folgt Erkenntnissen, vor allem der Verhaltensökonomie, wonach ab einer bestimmten Anzahl von Entscheidungsangeboten Kontrolllähmungs- und -blockadeeffekte freigesetzt werden (Control Overload).[429] Ähnliche Überlegungen lassen sich auch für die Interessensabwägung anstellen, denn auch hier entscheidet ein menschlicher Akteur, der mit der Masse an Datenverarbeitungen überfordert sein kann.[430]

bb) Innovationsbehinderungen durch partikularistische Rechtmäßigkeitserfordernisse sowie fehlende Vorhersehbarkeit

Verantwortliche sind gezwungen, jede einzelne Datenverarbeitung auf einen Rechtfertigungsgrund zu stützen. Bei der Einwilligung ist dies verbunden mit einer Identifizierung der betroffenen Person sowie mit Informationspflichten und Anfrage.[431] Zudem ist der Verantwortliche von der Erteilung der Einwilligung und deren Verbindlichkeit (Art. 7 Abs. 3 DSGVO) abhängig.[432] Doch

---

[427] *Bäcker*, Der Staat 51 (2012), 91, 112: „Unter solchen Bedingungen [eines informierten Alltags] erscheint das hergebrachte datenschutzrechtliche Leitbild des aufmerksamen Betroffenen, der die Chancen und Risiken eines bestimmten Datenverarbeitungsvorgangs abwägt, dann eine informierte Einwilligung erteilt und den weiteren Datenfluss beobachtet, um gegebenenfalls gegenüber einer klar bestimmten verantwortlichen Stelle seine Rechte geltend zu machen, weitgehend illusorisch". Ebenso *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 136 f.

[428] Vgl. *Norwegian Data Protection Authority*, Big Data, September 2013, S. 40, die von einer „consent apathy" spricht.

[429] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 369. Ebenso *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 320. Ähnlich *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2019, S. 137 f. Allgemein zu diesem Phänomen *Scheibehenne/Greifeneder/Todd*, Journal of Consumer Research 37 (2010), 409–425.

[430] Ebenso, explizit zu lernenden Systemen, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 41.

[431] Vgl., wenngleich allgemein zur Big-Data-Analyse und bezogen allein auf die Einwilligung *Hackenberg*, in: Hoeren/Sieber/Holznagel u.a. (Hrsg.), Handbuch Multimedia-Recht, [58]2022, 42; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 40. Siehe auch *Veil*, NJW 71 (2018), 3337, 3339. Auch bei der Interessensabwägung kann es gleichwohl notwendig sein, die betroffenen Personen zu identifizieren und, um überraschende Datenverarbeitungen auszuschließen, Informationsmaterial bereitgestellt werden. Zu entsprechenden Schwierigkeiten bei der Einwilligung in die Zweckänderung siehe *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 285; *Culik/Döpke*, ZD 7 (2017), 226, 228.

[432] Widerruf die betroffene Person ihre Einwilligung, darf der Verantwortliche die Daten nicht weiter nutzen (die Verarbeitung in der Vergangenheit bleibt aber zulässig). Die einzelnen Daten, für die die Einwilligung zurückgezogen wurde, aus dem Trainingsdatensatz herauszufiltern, kann aber technisch sehr herausfordernd bis unmöglich sein. Jeder Widerruf verkleinert zudem den Umfang des Trainingsdatensatzes, damit auch die Effektivität des

auch der Zulassungsgrund der Interessensabwägung verlangt dem Verantwortlichen einiges ab, kann er doch zur umfassenden Informationsbereitstellung verpflichten, zudem die Durchführung der Abwägung einige Ressourcen binden.[433] Auch hier müssen betroffene Personen herausgefiltert werden.[434] Soweit der Verantwortliche diesen Ressourceneinsatz nicht wirtschaftlich sinnvoll erbringen kann oder will, wird er autonome Systeme nicht zum Einsatz bringen können. Oder aber er muss auf Techniken zurückgreifen, die datensparsam funktionieren – und damit erhebliche Einbußen hinsichtlich der Qualität Maschineller Lernverfahren hinnehmen. Doch auch bei der Profilbildung und -verwendung kann das Erfordernis des Rechtmäßigkeitsattestats einer jeden Datenverarbeitung innovationshinderlich wirken, da auch dort eine Vielzahl von Datenverarbeitungen stattfinden können. Bei Profilbildung und -verwendung wirkt der Rechtmäßigkeitsgrundsatz insoweit technikhinderlich, als er der Verwendung selbstlernender Algorithmen entgegensteht, bei denen die Ergebnisse und Folgen der Verarbeitung nicht vorhersehbar sind.

V. Ergebnis

Der datenschutzrechtliche Rechtmäßigkeitsgrundsatz, ermöglicht und verstärkt durch den Zweckfestlegungsgrundsatz, etabliert ein Regulierungsregime, das von einer unmittelbaren und prognostizierbaren Verknüpfung zwischen Datum und Gefahr ausgeht, auf die Einzelperson fokussiert und über die Steuerung des Einzeldatums sämtliche Gefährdungen der Datenverarbeitung eindämmen soll. Im Verhältnis zwischen Privaten wird ein dezentrales Steuerungssystem geschaffen, in dem die Steuerungs- und Kontrollleistung maßgeblich der betroffenen Person überantwortet wird. Ein individuelles Datenkontrollrecht schafft die DSGVO aber nicht.

Der Zweckfestlegungsgrundsatz als zentrales Kontrollinstrument der DSGVO erweist sich im Hinblick auf autonome Systeme als effektiver, zugleich die Interessen der verarbeitenden Stelle hinreichend berücksichtigender Regulierungsmechanismus. Er verlangt nur sehr allgemeine Vorfestlegungen im Rahmen der Modell- und Profilbildung und Profilverwendung und erlaubt so Analysen bzw. Automatisierungen in verschiedener Richtung. Damit stellt er sich allein der Erstellung von Modellen entgegen, die sich gänzlich jenseits

---

Lernverfahrens. Unklar ist im Übrigen, ob der Widerruf eines Trainingsdatums auch die Verwendung des hieraus gebildeten Algorithmus unzulässig macht; denn immerhin ist der Algorithmus auf dieses Trainingsdatum gestützt. Siehe zu diesen Fragen eingehend *Humerick*, Santa Clara High Technology Law Review 34 (2018), 393, 406 f.; *Finck/Biega*, Technology and Regulation 2021, 44, 54.

[433] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 41.

[434] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*ders.*, Art. 5 Rn. 41. Siehe auch, wenngleich zur Einwilligung bei der Zweckänderung, *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 285.

menschlicher Sinnzusammenhänge und damit jenseits der Zweckbeschreibungen durch den Verantwortlichen einordnen. Der Zweckbindungsgrundsatz lässt Raum für die multiple Verwendung von (Trainings-)Daten und verhindert allein die Mehrfachverwendung besonders schutzwürdiger Datensätze, insbesondere solcher, die sensible Daten enthalten, und solcher, die – insbesondere durch Datenzukauf – patchworkartig zusammengesetzt und unstrukturiert sind. Die Modellbildung stellt kein statistisches Verfahren nach Art. 5 Abs. 1 lit. b) HS. 2 DSGVO dar. Damit setzt der Zweckfestlegungsgrundsatz sinnvolle Steuerungsakzente für autonome Systeme, ohne diese zu sehr einzuschränken.

Der Rechtmäßigkeitsgrundsatz erweist sich im Hinblick auf autonome Systeme als schwaches bzw. durch diese Technologie geschwächtes Steuerungsinstrument. Er führt bei der Modellbildung regelmäßig zur Zulässigkeit, da die Gefährdungslage für den Einzelnen hier gering ist. Es gelingt ihm aber nicht, die eigentlichen Gefährdungsmomente des Maschinellen Lernens zu adressieren, die im Daten- und Verarbeitungskollektiv, der Gefährdung von (Teil-)Gruppen und der algorithmischen Interpretation der Daten liegen. Bei der Profilbildung untergräbt die fehlende Nachvollziehbarkeit des Modells die auf Prädiktion setzenden Regulierungseffekte des Rechtmäßigkeitsgrundsatzes, zudem sieht die DSGVO keine Schutzinstrumente für die Generierung neuer Daten vor. Auf der Profilverwendungsebene wirkt die fehlende Kenntnis von den Profilinhalten fort. Herausfordernd ist zudem, wenn beim Einsatz selbstlernender Algorithmen Folgen der Profilverwendung nicht vorhersehbar sind. Dass Autonomiegefährdungen hier vor allem durch die dauerhafte Konfrontation mit autonomen Systemen ausgelöst werden, findet in der Regulierungsstruktur der DSGVO keinen Widerhall. Problematisch ist aber vor allem, dass in einer Welt autonomer Systeme eine solche Vielzahl an Datenverarbeitungen, zudem solche von hoher Komplexität, stattfinden, dass eine Rechtmäßigkeitsprüfung kaum mehr sinnvoll stattfinden kann. Sowohl auf Seiten betroffener Personen als auch auf Seiten menschlicher Entscheider (Verantwortlicher oder Aufsichtsbehörden) kann es zu Blockaden und Kontrolllähmungseffekten kommen. Die Erforderlichkeit der nachweisbaren Zulassung einer jeden Datenverarbeitung erweist sich als besonders innovationshemmend, insbesondere auf Stufe der Modellbildung, d.h. bei Maschinellen Lernverfahren.

Am Ende ist wesentliche Ursache der Steuerungsdefizite des Rechtmäßigkeitsgrundsatzes die fehlende Vorhersehbarkeit von Profilinhalten und Ergebnissen automatisierter Entscheidungen und Steuerung. Dies verweist auf ein anderes Rechtsinstrument der DSGVO: den Transparenzgrundsatz.

D. Regulierung autonomer Systeme durch den Transparenzgrundsatz

Transparenz ist das zentrale Steuerungsinstrument autonomer Systeme, dies nicht nur im Rahmen der DSGVO. In der allgemeinen Diskussion über die Regulierung autonomer Systeme wird deren Transparenz übereinstimmend und vorrangig gefordert, sie fehlt in keinem Regulierungsentwurf. Im Zentrum dieser Arbeit steht das Transparenzkonzept der DSGVO, das vornehmlich in den Art. 12–15 DSGVO ausgeformt ist. Die DSGVO prägt damit ein ganz bestimmtes Verständnis von Transparenz, nämlich eine Betroffenentransparenz, die durch ein ausdifferenziertes Informationspflichtenprogramm hergestellt werden soll. Zur Schärfung des Transparenzkonzepts der DSGVO und zum Verständnis von dessen Leistungsfähigkeit erscheint es sinnvoll, zunächst die diskutierten Transparenzkonzepte zu skizzieren. Hieraus wird dann das Steuerungsziel der Transparenz in der DSGVO erkenntlich (I.). Es folgt eine Darstellung des relevanten Rechtsrahmens (II.) sowie eine Analyse der Einhaltung der Transparenzvorschriften in den einzelnen Datenverarbeitungsschritten autonomer Systeme (III.). Hieraus lässt sich die Leistungskraft des Transparenzkonzepts der DSGVO bemessen (IV.). Am Ende sollen für aufgedeckte Transparenzdefizite rechtsinnovative Lösungen vorgestellt werden (V.).

I. Transparenz als Regulierungsziel autonomer Systeme

Dass autonome Systeme transparent zu gestalten sind, ist eine Forderung, die interdisziplinär erhoben wird. Dabei bleibt im Vagen, was mit Transparenz überhaupt gemeint ist – geht es um Einblicksmöglichkeiten in die Technik, um laiengerechte Verständlichkeit oder um eine menschliche Nachvollziehbarkeit? Transparenz ist ein interdisziplinär aufgeladenes, mehrdeutiges Konstrukt.[435] Entsprechend werden an autonome Systeme verschiedene Transparenzerwartungen und -anforderungen herangetragen, denen ganz unterschiedliche Prämissen und Grundüberzeugungen zugrunde liegen. Die allgemeine Diskussion leidet darunter, dass diese Transparenzkonzepte oftmals nicht expliziert und häufig nicht trennscharf differenziert werden.[436] Es ist nicht Aufgabe und Ziel dieser Untersuchung, dieses Diskussionsfeld aufzuarbeiten. Für das Verständnis des Transparenzkonzepts der DSGVO und insbesondere seine spätere Bewertung ist es aber essentiell, sich die außerrechtlichen und außerdatenschutzrechtlichen Transparenzvorstellungen in ihren Grundzügen zu vergegenwärtigen (1.). Mit der Gegenüberstellung des Transparenzentwurfs der

[435] Eingehend zum Begriff der Transparenz siehe etwa *Bröhmer*, Transparenz als Verfassungsprinzip, 2004, S. 18–23.

[436] So auch *Yeung/Weller*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 36.

DSGVO lässt sich dann das Steuerungsziel der Transparenz im Allgemeinen umso präziser erkennen (2.).

1. Allgemeine Transparenzkonzepte in Bezug auf autonome Systeme: Vielschichtige Transparenzerwartungen

Neben der Forderung nach menschlicher Aufsicht ist es vor allem die Transparenz autonomer Systeme, die die Debatte um die Regulierung autonomer Systeme wesentlich prägt. Diese Forderung ist im Technikrecht etwas Altbekanntes: Seit jeher wird verlangt, dass Technik vor allem transparent sein möge.[437] Was im Technikrecht allgemein unter Transparenz der Technik verstanden wird, lässt sich dann auch auf autonome Systeme übertragen. Im Kern lassen sich zwei Ausgestaltungen der Techniktransparenz unterscheiden. Transparenz meint zum einen die menschliche Verständlichkeit der technischen Funktionsweise. Dies erlaubt etwa Herstellern und Entwicklern, Fehler und Mängel aufzudecken und die Techniken fortlaufend zu verbessern,[438] während staatliche Akteure Regulierungswissen sammeln und eine Grundlage zur Durchsetzung rechtlicher Vorgaben erhalten.[439] Zum anderen meint Transparenz die laienbezogene Verständlichkeit, dass also VerbraucherInnen und NutzerInnen der Technik die technische Funktionsweise verstehen können. Dies zielt vor allem auf die sichere und sinnvolle Bedienung der Technik ab.[440] Es geht aber auch um Vertrauens- und Akzeptanzsicherung: Nur wenn Technik verständlich ist, können VerbraucherInnen von der Gemeinwohlverträglichkeit der Technik ausgehen und werden bereit sein, die Technik tatsächlich zu nutzen.[441] Der In-

---

[437] So auch *Wischmeyer*, AöR 143 (2018), 1, 44. Deutlich *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 6: „[T]ransparency is often naively treated as a panacea for ethical issues arising from new technologies".

[438] *Yeung/Weller*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 36; *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, 571 f.

[439] Siehe allgemein zur Funktion der Transparenz, Selbstprüfungen oder Kontrollen durch staatliche Institutionen zu ermöglichen *Hoffmann-Riem*, in: ders. (Hrsg.), Big Data, 2018, S. 11, 47; *Wischmeyer*, AöR 143 (2018), 1, 56–58. Diesen Aspekt der Transparenz, wenn auch im Rahmen der Algorithmentransparenz, unterstreicht auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 169, 171.

[440] Vgl. *Burrell*, Big Data and Society 3 (2016), 4.

[441] Prominent zu dieser Verknüpfung, die explizit die Vertrauenswürdigkeit der Systeme Künstlicher Intelligenz zum Ziel bestimmt, für deren Herstellung die Transparenz wesentliches Instrument ist, siehe *Hochrangige Expertengruppe für künstliche Intelligenz,* Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 16, 22, 36–37. So auch *Europäische Kommission*, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, 19.2.2020, S. 23 f. Vgl. ausführlich zum Zusammenhang von Transparenz und Vertrauen bzw. Vertrauenswürdigkeit *Felzmann/Villaronga/Lutz u.a.*, Big Data and Society 6 (2019), 1, 9. Siehe auch *Da-*

halt der Transparenz bestimmt sich dann anhand des vorhandenen Vor- und Fachwissens: Liegt dieses vor, kann ein bloßer Einblick genügen – Transparenz meint dann Offenlegung –, oder vertiefte Erläuterungen verlangen – Transparenz meint dann Erklärung.

Im Anwendungsfeld autonomer Systeme und Künstlicher Intelligenz erhält die Forderung nach Transparenz darüber hinaus eine eigene Bedeutung. Sie bezieht sich dann auf das Merkmal fehlender menschlicher Verständlichkeit, wie sie für subsymbolische Maschinelle Lernverfahren typisch ist.[442] Diese fehlende menschliche Verständlichkeit ist neuartig, sie war bislang in der Digital- und Informationstechnik so nicht bekannt. Sie ist wesentlicher Grund, weshalb eine Unbeherrschbarkeit dieser Technik und eine Vorherrschaft der autonomen Systeme befürchtet werden. Transparenz in Bezug auf Systeme der Künstlichen Intelligenz meint dann eine Methode zur Überwindung bzw. zum Umgang mit dieser fehlenden menschlichen Nachvollziehbarkeit,[443] es geht um die Herstellung einer originär menschlichen Verständlichkeit.[444] Ziel ist nicht die Offenlegung von Daten, Algorithmen oder Hardware, sondern die Einordnung des algorithmischen Verarbeitungswegs und der Ausgabe in menschliche Sinnzusammenhänge.[445] Werden autonome Systeme durch den Staat einge-

---

tenethikkommission, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 185; *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 7.

[442] Siehe eingehend hierzu bereits unter Kapitel 2 A. II. 2. c).

[443] Zwar ist häufig recht unspezifisch von der Transparenz „der KI", „der Systeme" oder „der Algorithmen" die Rede, Transparenzbezugsobjekt ist jedoch stets die individuell produzierte Ausgabe und die dieser zugrundeliegende algorithmische Entscheidungs- und Steuerungsarchitektur eines autonomen Systems.

[444] Ebenso *Hochrangige Expertengruppe für künstliche Intelligenz,* Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 22, die Transparenz explizit als Erklärbarkeit versteht. Auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 169 f. differenziert zwischen Transparenz (Offenlegung) sowie Erklärbarkeit und Nachvollziehbarkeit. Differenzierend auch *Mittelstadt/Allo/Taddeo u.a.*, Big Data and Society 3 (2016), 1, 6; *Burrell*, Big Data and Society 3 (2016), 3–5.

[445] Vgl. eingehend zum Begriff der Erklärung, auch in Zusammenhang mit Künstlicher Intelligenz *Miller*, Explanation in Artificial Intelligence: Insights from the Social Sciences, 22.06.2017, S. 11–14, 20-23. Die Offenlegung der algorithmischen Entscheidungsstruktur kann Teil davon sein, ist aber nicht ausreichend. So auch *Kroll/Huey/Barocas u.a.*, University of Pennsylvania Law Review 165 (2017), 633, 657–660; *Selbst/Barocas*, Fordham L. Rev. 87 (2018), 1085, 1137. Eine „Traceability" der verarbeiteten Daten und Verfahren neben bzw. als Grundlage der „explainability" fordert etwa die *High-Level Expert Group on Artificial Intelligence*, Ethics Guidelines for Trustworthy AI, Europäische Kommission, 8.4.2019, S. 18, im deutschen dann eine „Rückverfolgbarkeit" sowie eine „Nachprüfbarkeit", siehe *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, 10. April 2019, S. 16.

setzt, erweitert sich das Transparenzprogramm;[446] derartige Anwendungen liegen aber jenseits des Untersuchungsprogramms dieser Arbeit.

Transparenz im Hinblick auf autonome Systeme weist damit drei Bedeutungsebenen auf: erstens die menschliche Verständlichkeit autonomer Systeme bzw. solcher der Künstlicher Intelligenz (Verständlichkeit bzw. Nachvollziehbarkeit), d.h. die menschlich-semantische Aufbereitung von Ergebnissen und Entscheidungsverfahren dieser Systeme, zweitens die Verständlichkeit technischer Systeme für VerbraucherInnen, d.h. die laiengerechte Erläuterung der technischen Funktionsweise und Ergebnisse (Erklärbarkeit), sowie drittens Offenlegung (meist gegenüber staatlichen oder privaten ExpertInnen) von technischen Verfahren und Ergebnissen (Offenlegung bzw. Transparenz im engeren Sinne).[447] Die Intransparenzen haben jeweils unterschiedliche Ursachen, nämlich technische, adressatenbezogene und wirtschaftliche. Für die Konkretisierung dieser Transparenzinhalte ist die jeweilige Funktion der Transparenz maßgeblich,[448] von denen bereits einige beispielhaft benannt wurden, nämlich Fehlersuche, Haftung und Zurechnung, Regulierbarkeit, Überprüfung und Durchsetzung regulativer Anforderungen, Akzeptanz und Vertrauen. Entsprechend unterscheiden sich auch die Adressaten der Transparenz, etwa Hersteller und Entwickler, staatliche Akteure, VerbraucherInnen. Am Ende ist die Transparenz autonomer Systeme ein multifunktionales Konstrukt, dessen konkreter Inhalt sich erst dem Gesamtgefüge eines Regulierungsentwurfs entnehmen lässt.

2. Transparenzkonzept der DSGVO und Regulierungsparadigmen des Transparenzgrundsatzes

Demgegenüber prägt die DSGVO ein eigenes Verständnis von Transparenz (a)). Aus dem Gesamtregulierungssystem lassen sich die verschiedenen Dimensionen und Inhalte dieser datenschutzspezifischen Transparenz ableiten (b)). Am Ende erweist sich der Transparenzgrundsatz vorwiegend als Instrument des dezentralen Regulierungsregimes der DSGVO (c)).

---

[446] So etwa *Wischmeyer*, AöR 143 (2018), 1, 44.

[447] Diese Unterscheidung von Transparenz und Nachvollziehbarkeit nehmen auch *Wischmeyer*, AöR 143 (2018), 1, 47; *Yeung/Weller*, in: Bayamlıoğlu/Baraliuc/Janssens u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 36, 38 f. vor. Auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 72 f. unterscheidet zwischen Nachvollziehbarkeit, d.h. allgemein menschlicher Verständlichkeit – dann also für ExpertInnen –, und Erklärbarkeit, d.h. die laienhafte Verständlichkeit. Soweit es auf die Herstellung originär menschlicher Verständlichkeit, werden unterschiedliche Begriffe genutzt, etwa „Erklärbarkeit", so *Hochrangige Expertengruppe für künstliche Intelligenz,* Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz*,* 10. April 2019, S. 22; *Käde/Maltzan*, CR 36 (2020), 66–72 oder „Interpretierbarkeit" *Selbst/Barocas*, Fordham L. Rev. 87 (2018), 1085, 1109; *Adadi/Berrada*, IEEE Access 6 (2018), 52138, 52141.

[448] Hierauf weist auch *Beck*, Künstliche Intelligenz und Diskriminierung, 2019, S. 98 hin.

a) Datenschutzrechtliches Transparenzkonzept: datenschutzbezogene Information statt Verarbeitungs- und Algorithmentransparenz

Der Transparenzbegriff in der DSGVO grenzt sich teilweise gegenüber diesen allgemeinen Techniktransparenzvorstellungen ab,[449] weist aber auch einige Überschneidungen auf. Der Transparenzgrundsatz wird primärrechtlich aus dem Gebot der Verarbeitung nach Treu und Glauben Art. 8 Abs. 2 GRCh abgeleitet,[450] sekundärrechtlich ist er ausdrücklich in Art. 5 Abs. 1 lit. a) Var. 3 DSGVO normiert. Die DSGVO enthält keine Definition der Transparenz.[451] Die Informationspflichten nach Art. 12–15 DSGVO ebenso wie die Anforderungen der Einwilligung,[452] spezifizieren das Transparenzverständnis der DSGVO.[453] In inhaltlicher (aa)), sachlicher (bb)) und persönlicher (cc)) Hinsicht wird das Transparenzkonzept der DSGVO im Verhältnis zu dem oben vorgestellten Techniktransparenzkonzept eng geführt.

aa) Datenschutzbezogenes, nicht verarbeitungsbezogenes Transparenzverständnis

Hinsichtlich des Transparenzgegenstands unterscheidet der Unionsgesetzgeber zwischen Datenverarbeitungen und automatisierten Entscheidungen: Bei Datenverarbeitungen ist der Betroffene allein über datenschutzrelevante Aspekte, d.h. die formalen Umstände der Datenverarbeitung zu informieren, nicht aber über technische Aspekte der Datenverarbeitung oder ihrer Ergebnisse.[454] Zu

---

[449] Auch mit dem verfassungstheoretischen Transparenzverständnis hat das Transparenzgebot der DSGVO wenig gemein, vgl. Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 12.

[450] Siehe nur Gola, DS-GVO/*Franck*, Art. 13 Rn. 2; Gola, DS-GVO/*Pötters*, Art. 5 Rn. 12; Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 10.

[451] So ausdrücklich auch *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 6.

[452] Auch für den Zulassungsgrund der vertragsimmanenten Zulassung sowie der Interessensabwägung bedarf es, wie ausgeführt, gewisser Informationen, die inhaltlich aber nicht über das Informationsprogramm der Einwilligung hinausgehen. Sie bleiben in der weiteren Untersuchung daher außer Betracht.

[453] Dies kommt auch in den Erwägungsgründen 39 und 58 zum Ausdruck. Ebenso Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 1. Die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 16 beschränkt ihre Darstellungen zum Transparenzgebot dagegen auf Art. 12–14 DSGVO.

[454] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 55; Sydow, DS-GVO/*Greve*, Art. 12 Rn. 2. Ausdrücklich auch *Norwegian Data Protection Authority*, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 19: „Transparency is achieved by providing data subjects with process details". Siehe

diesen Umständen zählen etwa das Stattfinden der Verarbeitung, die Person des Verantwortlichen sowie Zwecke der Verarbeitung.[455] Eine Informationspflicht hinsichtlich der Datenverarbeitungstechnik, etwa über Methoden, Algorithmen, Verfahrensschritte oder Ergebnisse, ist nicht vorgesehen. Anders ist dies bei automatisierten Entscheidungen: Hier müssen der betroffenen Person „aussagekräftige Informationen über die involvierte Logik" bereitgestellt werden.[456] Datenschutzrechtliche Transparenz grenzt sich damit deutlich vom oben beschriebenen Konzept der Techniktransparenz ab: Um eine Verständlichkeit der technischen Funktionsweise der Digitaltechnik geht es nicht. Nur bei automatisierten Entscheidungen entsprechen sich das Transparenzkonzept der DSGVO und das des allgemeinen Technikrechts. Die Problematik fehlender Nachvollziehbarkeit wird in der DSGVO nicht adressiert. Hierauf ist zurückzukommen.

bb) Atomistisch-partikularistisches Transparenzkonzept

Die Informationspflichten der DSGVO beziehen sich dabei stets nur auf die einzelne Datenverarbeitungssituation.[457] Ziel der Betroffenentransparenz ist es daher nicht, ein grundlegendes Verständnis betroffener Personen von der Funktionsweise der digitalen Systeme, der Datenverarbeitungstechnik bzw. der automatisierten Entscheidung herzustellen.

cc) Betroffenenbezogenes, individualistisches und relativistisches Transparenzkonzept

Wenngleich die DSGVO an verschiedenen Stellen weitere Vorschriften vorsieht, die sich als Ausgestaltungen von Transparenz verstehen lassen,[458] konkretisiert der Unionsgesetzgeber den Transparenzgrundsatz wesentlich in Art. 12–15 DSGVO, in denen Informationspflichten des Verantwortlichen gegen-

---

auch *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 16.

[455] Art. 13 Abs. 1 lit a), c), Art. 14 Abs. 1 lit a), c), Art. 15 Abs. 1 lit a) DSGVO.

[456] Art. 13 Abs. 1 lit. f), Art. 14 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO.

[457] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 60; Sydow, DS-GVO/*Greve*, Art. 12 Rn. 7.

[458] Sydow, DS-GVO/*Greve*, Art. 12 5 Rn. 16 führt zusätzlich Art. 7 Abs. 2, Art. 18 Abs. 3, Art. 19, Art. 21 Abs. 4 und Art. 34 DSGVO an. Weitere Auflistungen transparenzbezogener Normen der DSGVO bei *Schulte*, PinG 5 (2017), 227, 226 Fn. 2. Vorgesehen sind überdies Einblicks- und Informationsrechte des Datenschutzbeauftragten, Art. 38 Abs. 1 DSGVO sowie der Aufsichtsbehörden, so in Art. 30 Abs. 4, Art. 31, Art. 57 Abs. 1 lit. a), Art. 58 Abs. 1 lit. a), lit. b) und lit. e) DSGVO. Auch Dokumentations- und Protokollierungspflichten der Verantwortlichen, die in Art. 30 DSGVO, im Übrigen auf die Rechenschaftspflichten nach Art. 5 Abs. 2, Art. 24 DSGVO gestützt wird, zielen maßgeblich auf Einsichtnahme durch staatliche Akteure ab. Vgl. hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 181; Paal/Pauly, DS-GVO/*Frenzel*, Art. 5 Rn. 52.

über der betroffenen Person normiert sind.[459] Transparenz im Sinne der DSGVO ist eine Betroffenentransparenz.[460] Die Transparenzpflichten adressieren allein die betroffene Person. Die DSGVO kennt keine Pflicht des Verantwortlichen, der allgemeinen Öffentlichkeit Informationen bereitzustellen.[461] Durch die Informationen an die betroffenen Personen ist freilich mittelbar auch die Betroffenenöffentlichkeit angesprochen.[462] Demgegenüber sieht die DSGVO für staatliche Institutionen gerade Informationspflichten gegenüber die Betroffenenöffentlichkeit vor, wenngleich allein im Rahmen allgemeiner Aufklärung.[463] Das Transparenzprogramm ist, wie sich dann auch besonders aus Art. 12 DSGVO ergibt, an der menschlichen, genauer: der laienbezogenen Verständlichkeit ausgerichtet.[464] Die Transparenz ist damit wesentlicher Be-

---

[459] Auch die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 6 f. stellt allein auf die Art. 12–15 DSGVO ab, um den Transparenzgrundsatz zu beschreiben. Ebenso die überwiegende Literatur, vgl. beispielsweise Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 19; *Strassemeyer*, K&R 16 (2016), 176, 178–181. Gemeinhin wird von einer Konkretisierung des Transparenzgrundsatzes durch die Art. 12–15 DSGVO gesprochen, siehe nur Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 5 Rn. 12; Paal/Pauly, DS-GVO/*Frenzel*, Art. 5 Rn. 22. Teilweise werden Transparenzgrundsatz und die Informations- und Mitteilungspflichten sogar gleichgesetzt, vgl. etwa Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 11. Ähnlich, wenn auch noch zur DSRL, *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 170–172.

[460] Dies wird bereits in Art. 5 Abs. 1 lit. a) DSGVO deutlich, in dem auf die Nachvollziehbarkeit „für die betroffene Person" abgestellt wird. Auch Erwägungsgrund 60 S. 1 stellt allein auf die Unterrichtung der betroffenen Person ab. Dies folgt auch aus der primärrechtlichen Wertung: In Art. 8 Abs. 2 S. 2 GRCh ist ein Auskunftsrecht allein für die betroffene Person vorgesehen. Explizit auch *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 6: „Das Transparenzkonzept laut der DSGVO ist eher im Sinne einer Fokussierung auf den Nutzer als in rechtlicher Dimension zu verstehen". Ebenso Sydow, DS-GVO/*Reimer*, Art. 5 Rn. 15; *Schulte*, PinG 5 (2017), 227, 227, 229.

[461] So ist denn auch bei der Datenschutzfolgenabschätzung nach Art. 35 DSGVO eine Pflicht zu Veröffentlichung des abschließenden Berichts nicht vorgesehen. Siehe hierzu Paal/Pauly, DS-GVO/*Martini*, Art. 35 Rn. 55.

[462] Ebenso *Schulte*, PinG 5 (2017), 227; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 5 Rn. 26. Siehe auch Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 5 Rn. 11–12; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Schwartmann/Hermann*, Art. 5 Rn. 38, die sowohl auf die betroffene Person als auch die allgemeine Öffentlichkeit als Adressat der Informationspflichten abstellen.

[463] So etwa bei der Berichterstattung durch den Europäischen Datenschutzausschuss, Art. 71 DSGVO, oder allgemeine Risikoaufklärungen der Aufsichtsbehörden an die Öffentlichkeit, Art. 57 Abs. 1 lit. b) DSGVO.

[464] Vgl. auch *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 8, die die Unterscheidung zwischen verschiedenen Adressatengruppen und deren technischen Wissensstand anregt.

standteil des dezentralen Regulierungsregimes der DSGVO. Verpflichtet ist der Verantwortliche,[465] nur ergänzend treten Aufsichtsbehörden und Europäischer Datenausschuss hinzu.[466] Dies entspricht dem bereits im Anwendungsbereich aufgedeckten Befund, wonach das Datenverarbeitungsverhältnis relativistisch verstanden wird.[467]

b) Regulierungsparadigmen des Transparenzgrundsatzes

Aus diesem datenschutzrechtlichen Transparenzkonzept lassen sich drei wesentliche Funktionen ableiten, anhand derer im Weiteren eine Konkretisierung der Transparenzinhalte im Hinblick auf autonome Systeme und eine Bewertung dieser Informationsangebote der DSGVO erfolgen soll. Dem Transparenzgrundsatz der DSGVO liegen freilich eine Vielzahl an Prämissen und Konzepte zugrunde,[468] die auf ganz unterschiedliche Funktionen verweisen. Weitere Funktionen – und damit auch inhaltliche Ausgestaltungen der datenschutzrechtlichen Transparenz – sind daher denkbar.[469] Unterscheiden lassen sich eine instrumentelle (aa)), ein funktionale (bb)) sowie ein gemischt instrumentell-funktionale Dimension (cc)) des Transparenzgrundsatzes der DSGVO. Dies gilt auch für die Regulierungsmechanismen, die die DSGVO im Hinblick auf automatisierte Entscheidungen bietet (dd)).

---

[465] Siehe hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 52; *Strassemeyer*, K&R 16 (2016), 176, 177.

[466] So etwa in Art. 57 Abs. 1 lit. b) DSGVO (Aufsichtsbehörden) oder Art. 71 DSGVO (Europäischer Datenschutzausschuss). Ebenso auch auf die Aufsichtsbehörden abstellend Paal/Pauly DS-GVO/*Frenzel*, Art. 5 Rn. 22; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 5 Rn. 23. In der DSRL war deren Beitrag zur Transparenz noch deutlicher hervorgehoben. So hieß es in Erwägungsgrund 63 der DSRL: „Die Kontrollstellen haben zur Transparenz der Verarbeitungen in dem Mitgliedstaat beizutragen, dem sie unterstehen".

[467] Siehe oben Kapitel 4 B. I. 3.

[468] *Schulte*, PinG 5 (2017), 227.

[469] Ausgeblendet bleibt insbesondere die Funktion der Herstellung von Akzeptanz und Vertrauen, da sich aus dieser nicht präzise auf Inhalte der Transparenz schließen lässt. Vgl. zu diesem Ziel bereits *Europäische Kommission*, Vorschlag für Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, 25.01.2012, S. 1-2, 118. Siehe auch *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 27 f. Ebenso Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 1; Sydow, DS-GVO/*Greve*, Art. 12 Rn. 1; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Schwartmann/Hermann*, Art. 5 Rn. 34; Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 4.

aa) Instrumentelle Dimension: Transparenz als Grundlage für datenschutzrechtliche Selbstschutzinstrumente

Die DSGVO gibt der betroffenen Person im Wesentlichen drei Steuerungsinstrumente zur Hand: Die Einwilligung bzw. auch die vertragsimmanente Zulassung im Rahmen der Rechtmäßigkeit, die Betroffenenrechte in Art. 16–21 DSGVO sowie Rechtsschutzoptionen in Form des Beschwerderechts in Art. 77 DSGVO sowie begleitende gerichtliche Durchsetzungsmechanismen, wie sie in Art. 78, 79 DSGVO garantiert werden. Die Informationspflichten dienen als Grundlage für diese Betroffenenrechte. Die Einwilligung verweist auf eine eigene Dimension des Transparenzgrundsatzes, auf diese ist sogleich einzugehen. Die Betroffenenrechte können nur dann sinnvollerweise ausgeübt werden, wenn die betroffene Person um die Datenverarbeitung, die verarbeiteten Daten und Zwecke weiß.[470] Nur dann kann sie die Konformität der Datenverarbeitung mit den datenschutzrechtlichen Vorgaben sowie individuellen Datenschutzpräferenzen prüfen und Berichtigungs-, Löschungs- oder Widerspruchsrechte geltend machen. Auch eine Beschwerde wie auch gerichtliche Verfahren sind nur denkbar, wenn die betroffene Person eine hinreichende Informationsbasis hat, anhand derer sie Verstöße gegen die DSGVO prüfen kann.[471] Die Transparenz in der DSGVO hat damit vornehmlich instrumentelle Funktion: Sie bereitet die Basis, auf der die einzelnen Steuerungsinstrumente effektiv wahrgenommen werden können.[472]

Ziel der Transparenz ist hier die Herstellung von einem Verständnis, das die Überprüfung der Datenverarbeitung durch die betroffene Person ermöglicht, und zwar anhand datenschutzrechtlicher Vorgaben sowie individueller Daten-

---

[470] So explizit die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 6, 33 „zweckdienliche Ausgangsposition". Siehe aus der Literatur etwa *Strassemeyer*, K&R 16 (2016), 176, 177; *Kamps/Schneider*, K&R 19 (2020), 24, 25; Gola, DS-GVO/*Franck*, Art. 12 Rn. 1–4.

[471] Auch die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 6, 33 hebt die Bedeutung der Transparenz für den Rechtsschutz hervor. Vgl. zu dieser Funktion des Transparenzgrundsatzes Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 1; *Albers*, in: Gutwirth/Leenes/Hert (Hrsg.), Reloading data protection, 2014, S. 213, 231 f. Siehe etwa *Reinhardt*, AöR 142 (2017), 528, 560.

[472] In dieser instrumentellen Funktion wird überwiegend die Steuerungsfunktion der Transparenz erkannt, siehe nur *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 6 sowie Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 50; Kuner/Bygrave/Docksey, GDPR/*Zanfir-Fortuna*, Art. 13 Rn. 415 f.; Plath, DSGVO/BDSG/*Plath*, Art. 5 Rn. 6. Siehe auch Erwägungsgrund 63 S. 1, demzufolge die Auskunft die betroffene Person befähigen soll, die Rechtmäßigkeit der Datenverarbeitung prüfen zu können.

schutzpräferenzen. In der instrumentellen Dimension der Transparenz geht es also um Auditabilität hinsichtlich datenschutzrechtlicher und außerrechtlicher, d.h. individueller Richtigkeitskriterien.

bb) Funktionale Dimension: Transparenz als Grundlage für außerrechtliche Selbstschutzmechanismen

Die Transparenz entfaltet aber auch aus sich heraus Steuerungskräfte.[473] Dabei stützt sich der Unionsgesetzgeber auf bestimmte Grundannahmen von Wirkungseffekten der Transparenz jenseits verknüpfter rechtlicher Schutzinstrumente. Es geht um die Aktivierung außerrechtlicher Schutzmechanismen, da es um eine Betroffenentransparenz geht also um Selbstschutzmechanismen. Wie konkret dies erfolgt, wird sehr unterschiedlich gesehen. Da diese Schutzdimension der Transparenz auf der vorgelagerten Ebene, nämlich derjenigen der menschlichen Autonomie, wirkt, sind ganz verschiedene Annäherungen denkbar.[474] Im Wesentlichen geht es darum, die durch Intransparenz ausgelösten Autonomiegefährdungen aufzuheben. Mittels Transparenz sollen betroffene Personen befähigt werden, Hemm- und Einschüchterungseffekten entgegenzutreten,[475] Manipulationen abzuwehren[476] Informationsasymmetrien zu

[473] Dass den Informationspflichten neben den Betroffenenrechten und der Einwilligung eine eigenständige Schutzfunktion zukommt betonen, ist Konsens. Siehe nur Wolff/Brink, BeckOK Datenschutzrecht/*Wolff*, Grundlagen und bereichsspezifischer Datenschutz; System A. Prinzipien des Datenschutzrechts Rn. 69; Kühling/Buchner, DS-GVO, BDSG/*Herbst*, Art. 5 Rn. 18; Kuner/Bygrave/Docksey, GDPR/*Polčák/Radim*, Art. 12 Rn. 401 f.; Sydow, DS-GVO/*Greve*, Art. 12 2, 5. Vgl. auch *Nettesheim*, in: Nettesheim/Diggelmann/Lege u.a. (Hrsg.), Der Schutzauftrag des Rechts, 2011, S. 7, 40 f.: „Transparenzpflichten können die freiheitsbelastende Wirkung von Datenerhebungen reduzieren".

[474] Siehe zu Annäherungen an die datenverarbeitungsspezifische Autonomie(gefährdung) Kapitel 4 A. II. 2.

[475] *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233, 236. Ähnlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 1: „[Die Transparenzregeln sollen] diffuse[.] Bedrohlichkeit […] kompensieren". Ähnlich die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 8: „Bei dem […] Transparenzgrundsatz stellt die Tatsache einen zentralen Erwägungsfaktor dar, dass die betroffene Person den Umfang und die Folgen der Verarbeitung im Vorfeld ermitteln kann und nicht später von der Art und Weise überrascht werden sollte, in der ihre personenbezogenen Daten verwendet worden sind". Siehe auch Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 10; Sydow, DS-GVO/*Greve*, Art. 12 Rn. 2.

[476] Vgl. für personalisierte Werbung *Mik*, Law Innov. Technol. 8 (2016), 1, 14–16, für Suchmaschinen *dies.*, Law Innov. Technol. 8 (2016), 1, 16–18.

überwinden,[477] und insgesamt ihre Subjektqualität zurückgewinnen.[478] In dieser Dimension zielt die Transparenz auf Auditabilität im Hinblick auf außer(datenschutz)rechtliche Richtigkeitskriterien ab und also auf eine Kenntnis betroffener Personen von den Datenverarbeitungsumständen, die ihnen eine Prüfung der Datenverarbeitung anhand individuell definierter Angemessenheitsvorstellungen erlaubt.

cc) Instrumentell-funktionale Dimension: Ermöglichung der Einwilligung als Wahlmöglichkeit zwischen Datenschutzrecht und Selbstschutz

Im dezentralen Regulierungsregime der DSGVO ist digitale Autonomie, dies ist bereits gesagt worden, vornehmlich durch die betroffene Person zu schützen und wird dadurch überhaupt erst wahrgenommen.[479] Im vertraglichen Verhältnis erfolgt dies über die Aushandlung der Vertragsbedingungen, in allen anderen Konstellationen über die Einwilligung.[480] Dabei kommt der Transparenz maßgebliche Bedeutung für die Wahrnehmung digitaler Autonomie zu: Erst, wenn die betroffene Person die Folgen einer Datenverarbeitung überblicken, d.h. vorhersehen kann, kann sie sinnvoll ihre Zustimmung erteilen.[481] Deshalb muss die Einwilligung in „informierter Weise" erfolgen.[482] Diese Erwägungen lassen sich mit gewissen Einschränkungen auch auf die vertragsimmanente Zulassung übertragen, bei der ebenso Transparenzgebote, wenngleich in geringe-

---

[477] So auch Sydow, DS-GVO/*Greve*, Art. 12 Rn. 2; *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 289. *Hoffmann-Riem*, AöR 123 (1998), 514, 532 spricht von „Mindestvoraussetzungen informationeller Chancengleichheit". Ähnlich *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 367 f. Für automatisierte Entscheidungen Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 35a. Siehe auch *Norwegian Data Protection Authority*, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 19: „Data protection is largeley about safeguarding the rights of individuals to decide how information about themselves is used. This requires that controllers are open about the use of personal data, that such use is transparent".

[478] Vgl. allgemein *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233, 236. Siehe auch Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3, 10; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 1.

[479] Siehe oben Kapitel 4 A. II. 3.

[480] Zum Verhältnis der Zulassungsgründe zueinander und zur Bedeutung des Rechtfertigungsgrunds der Interessensabwägung siehe oben Kapitel 4 C. II. 6.

[481] Diese Funktion der Transparenz bezogen auf die Einwilligung betonen *Schulte*, PinG 5 (2017), 227, 229; Paal/Pauly DS-GVO/*Frenzel*, Art. 5 Rn. 21; *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 89. Vgl. auch Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 4: „Sinn und Zweck der Regelung ist es, der betroffenen Person den informierten Umgang der Preisgabe ihrer personenbezogenen Daten zu ermöglichen". Siehe bereits Kapitel 4 C. II. 2. a).

[482] Vgl. Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 5 Rn. 11; Wolff/Brink, BeckOK Datenschutzrecht/*Schantz*, Art. 5 Rn. 11.

rem Umfang, bestehen.[483] Die Transparenz hat insoweit – wie oben beschrieben – instrumentelle Funktion.

Transparenz hat hier aber zusätzlich eine funktionale Dimension, verweist also auf Schutzinstrumente jenseits des (Datenschutz-)Rechts. Die Einwilligung zielt nicht allein darauf ab, sicherzustellen, dass Datenverarbeitungen den Datenschutzpräferenzen der betroffenen Person entsprechen. In der Wahlmöglichkeit zwischen der Zulassung und der Nichtzulassung fungiert sie zugleich als Schalter für individuelle, dann außerrechtliche Selbstschutz- und Resilienzinstrumente: Wer sich auf eine Datenverarbeitung (unter bestimmten Bedingungen) einlässt, wird dies nur tun, wenn er diese für akzeptierfähig und also nicht autonomiegefährdend erachtet. Die Zulassungsentscheidung wird daher nur erfolgen, wenn die betroffene Person sich für fähig hält, sich etwaiger Autonomiegefährdungen mittels eigener Resilienz- und Schutzmechanismen zu erwehren. Mit der Einwilligung trifft die betroffene Person also immer auch eine Abwägungsentscheidung zwischen eigener Schutzfähigkeit – dann Zulassung der Datenverarbeitung – und Schutzbedarf durch das Datenschutzrecht – dann keine Zulassung der Datenverarbeitung, und damit eine Wahl zwischen Selbstschutz und Datenschutz.[484] Diese Abwägungsentscheidung ist aber nur möglich, wenn die betroffene Person die Folgen der Datenverarbeitung absehen kann. Und sie ist nur möglich, wenn sie ihre außerrechtlichen Resilienz- und Schutzmechanismen überhaupt sinnvoll aktivieren kann, wofür sie ebenso Informationen über die Datenverarbeitung und ihrer Folgen bedarf. Die Transparenz entfaltet somit ohne Verknüpfung mit einem datenschutzrechtlichen Instrument, d.h. aus sich heraus eine Schutzwirkung.

Die Transparenz zielt hier auf Auditabilität im Hinblick auf individuelle, d.h. außerdatenschutzrechtlicher Richtigkeitskriterien, ab.

dd) Insbesondere: Regulierungsparadigmen der Transparenz bei automatisierten Entscheidungen

Diese Erwägungen lassen sich auf die Transparenzdimensionen der automatisierten Entscheidungen übertragen. Der Unionsgesetzgeber sieht hier verschiedene Betroffenenrechte in Art. 22 Abs. 3 DSGVO vor, für deren Wahrnehmung ein hinreichendes Maß an Transparenz hinsichtlich Verfahren und Ergebnis der automatisierten Entscheidung notwendig ist.[485] Hierauf ist noch zurückzukom-

---

[483] Siehe oben Kapitel 4 C. II. 3. am Anfang. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 15.

[484] Sie entscheidet sich dann nämlich gegen die Datenzurückhaltung, im Sinne von *Hert/Gutwirth*, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, 2006, S. 61 also gegen die „privacy" und für die „transparency". Siehe hierzu oben Kapitel 4 A. I. 2. a). Vgl. auch *Lewinski*, Die Matrix des Datenschutzes, 2021, S. 66 f.

[485] Vgl. *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284 f. Siehe auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 183.

men. Die Transparenz entfaltet hier also instrumentelle Funktion. Zugleich ist auch die funktionale Dimension der Transparenz angesprochen, denn gerade die Intransparenz der Entscheidungsarchitektur ist nach der Vorstellung des Unionsgesetzgebers autonomiegefährdend und droht, menschliche Subjektqualität aufzuheben.[486] Schließlich ist auch die verknüpfte instrumentell-funktionale Ebene abgebildet, denn Art. 22 DSGVO sieht als Ausnahmezulassungsgründe sowohl die Einwilligung als auch die vertragsimmanente Zulassung vor. Wenngleich hier zentral normiert ist, dass die automatisierte Entscheidung unzulässig und damit inakzeptabel ist, lässt der Unionsgesetzgeber über die Ausnahmezulassung Raum für abweichende individuelle Bewertungen und damit für eine Abwägungsentscheidung zwischen Datenschutz – dann Verbot – und Selbstschutz – dann Ausnahmezulassung. Die außerrechtlichen Resilienzmechanismen beziehen sich hier dann gleichwohl nicht auf die Datenverarbeitung, sondern auf die automatisierte Entscheidung.

3. Ergebnis: Transparenz als grundlegendes Instrument des dezentralen Regulierungsregimes der DSGVO

Während Transparenzforderungen hinsichtlich autonomer Systeme auf Einblicksoptionen in die technischen Abläufe und deren laiengerechte Aufbereitung sowie auf die Überwindung der systemimmanenten fehlenden Nachvollziehbarkeit abzielen, geht es beim datenschutzrechtlichen Transparenzkonzept allein um eine an die betroffene Person adressierte Transparenz, zudem um eine Transparenz, die sich nur auf äußere Umstände der Datenverarbeitung bezieht. Allein bei automatisierten Entscheidungen sind auch Transparenzanforderungen hinsichtlich des technischen Verfahrens vorgesehen. Die datenschutzrechtliche Transparenz soll die Wahrnehmung der Betroffenenrechte der DSGVO ermöglichen, zugleich aus sich heraus Steuerungseffekte freisetzen, indem sie eine wesentliche Ursache der Autonomiegefährdungen durch Datenverarbeitung, nämlich deren Intransparenz, überwindet. Schließlich soll Transparenz die Grundlage dafür schaffen, dass die betroffene Person zwischen rechtlichem Datenschutz und außerdatenschutzrechtlichem Selbstschutz wählen kann. Die datenschutzrechtliche Transparenz zielt jeweils darauf ab, die betroffene Person zu befähigen, die Datenverarbeitung auf ihre Vereinbarkeit mit datenschutzrechtlichen Bestimmungen und individuellen Angemessenheitskriterien zu prüfen. Am Ende erweist sich die Transparenz als Ausdruck und Bedingung des dezentralen Regulierungssystems der DSGVO.[487]

---

[486] Siehe nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 10; *Martini*, JZ 72 (2017), 1017, 1018; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2.

[487] Vgl. auch Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Buchholtz/Stentzel*, Art. 5 Rn. 27. Vgl. auch *Schulte*, PinG 5 (2017), 227, 229. Alternative Datenschutzmodelle gehen sogar so weit, das Datenschutzrecht ausschließlich als Transparenzrecht zu konzipieren, so

Der Inhalt der datenschutzrechtlichen Transparenz ist eng mit den Vorstellungen der DSGVO von digitaler Autonomie und ihrer Gefährdung sowie dem Regulierungsregime der DSGVO insgesamt verknüpft. Inwieweit diese Transparenzkonzeption im Angesicht der neuen Technologie autonomer Systeme weiterhin tragfähig ist, ist Ziel der nachfolgenden Untersuchung.

II. Darstellung des geltenden Rechts

Die DSGVO normiert einen allgemeinen Teil zur Ausgestaltung der Informationsangebote und zu den Grenzen der Informationspflicht (1.). Hinsichtlich der Inhalte des Transparenzprogramms unterscheidet sie zwischen Datenverarbeitungen (2.) und automatisierten Entscheidungen (3.).

1. Formale Anforderungen des Transparenzgebots

Die DSGVO sieht in Art. 12 DSGVO übergreifende Pflichten[488] zur Ausgestaltung des Informationsprogramms vor (a)) und formuliert bestimmte Grenzen (b)).

a) Ausgestaltung und Aufbereitung der Informationen

Der Unionsgesetzgeber überlässt die Form der Informationspräsentation überwiegend dem Verantwortlichen,[489] sie kann in schriftlicher, elektronischer anderer Form erfolgen.[490] Die Verwendung von Bildsymbolen ist nach Art. 12 Abs. 7 DSGVO allerdings nur als Ergänzung zulässig.[491] Beschränkungen ergeben sich allein aus Art. 12 Abs. 1 S. 1 DSGVO. Danach sind die In-

---

etwa das kanadische Datenschutzrecht. Siehe hierzu sowie entsprechenden Reformbewegungen im deutschen Datenschutzrecht Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 4.

[488] Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 12 1, 20 sprechen von einem „allgemeinen Teil" der Informations- und Mitteilungspflichten; Wolff/Brink, BeckOK Datenschutzrecht/*Quaas*, Art. 12 Rn. 5 von „Rahmenbedingungen für das Wie der Information".

[489] *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 17.

[490] Art. 12 Abs. 1 S. 2 DSGVO. Siehe auch *dies.*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 13 f.

[491] Siehe mit konkreten Musterbeispielen aus dem Parlamentsentwurf Gola, DS-GVO/*Franck*, Art. 12 Rn. 48. Art. 12 Abs. 8 DSGVO sieht eine Ermächtigung der Europäischen Kommission zum Erlass von Delegationsrechtsakten, die hiervon jedoch bislang keinen Gebraucht gemacht hat.

formationen in präziser, transparenter[492], verständlicher und leicht zugänglicher Form bereitgestellt werden müssen.[493]

Die Anforderung der Präzision begrenzt die Informationen in drei Richtungen: Sie muss vollständig sein, darf zugleich nichts Überflüssiges enthalten und muss inhaltlich zutreffend sein.[494] Transparent ist die Information dann, wenn die Information als solche erkennbar und erfassbar ist.[495] Dies bereitet in der Praxis wenig Probleme. Verständlich ist die Information, wenn der Adressat diese inhaltlich erfassen und zur Grundlage seiner Entscheidungen machen kann.[496] Dies hat eine inhaltliche und eine formale Zielrichtung: Die Information muss inhaltlich so aufbereitet sein, dass sie für die durchschnittlichen NutzerInnen verständlich ist.[497] Und sie muss äußerlich so gestaltet sein, dass sie ohne größeren zeitlichen oder kognitiven Aufwand erfasst werden kann.[498] Abzustellen ist auf durchschnittliche NutzerInnen in der konkreten Verarbeitungssituation.[499] In der DSGVO ist ein Zielkonflikt zwischen Präzision und Verständlichkeit bzw. innerhalb der Verständlichkeit angelegt: Das Gebot der Präzision bzw. der Verständlichkeit kann umfassendere Erläuterungen notwendig machen, die dann aber in quantitativer Hinsicht den Rahmen der Verständlich-

---

[492] Gemeinhin wird die Anforderung von Transparenz in Art. 12 DSGVO als Hinweis darauf verstanden, dass die bereitgestellten Informationen (gemeint ist dann: die Transparenz der Datenverarbeitung) in einer für die betroffenen Personen verständlichen und nicht verschleiernden Weise (gemein ist dann: die Transparenz der Information) darzustellen sind. Dadurch werden die übrigen Anforderungen – verständlich und leicht zugänglich – nochmals betont. Vgl. hierzu Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 29; Wolff/Brink, BeckOK Datenschutzrecht/*Quaas*, Art. 12 Rn. 14.

[493] Diese Anforderungen überschneiden sich vielfach. Sie werden daher nicht im Sinne einzelner Tatbestandsvoraussetzungen verstanden. Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12.

[494] Vgl. Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 28; Wolff/Brink, BeckOK Datenschutzrecht/*Quaas*, Art. 12 Rn. 13. Es geht um eine „kurze und bündige" Darstellung, so *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 35 f.

[495] So die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 7 f. Siehe auch Wolff/Brink, BeckOK Datenschutzrecht/*Quaas*, Art. 12 Rn. 14; Gola, DS-GVO/*Franck*, Art. 12 Rn. 19. Die Information muss dann etwa abgetrennt von anderen Erläuterungen oder ohne sonstige nebulöse Einkleidung erfolgen. Insbesondere bei Datenschutzerläuterungen in Form von AGBs kommt diese Anforderung zum Tragen.

[496] Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 30; *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 8.

[497] Vgl. Plath, DSGVO/BDSG/*Kamlah*, Art. 12 Rn. 2.

[498] Vgl. Gola, DS-GVO/*Franck*, Art. 12 Rn. 20; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 12 Rn. 11.

[499] Es gilt damit ein objektivierter Maßstab, vgl. Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 25–26; Wolff/Brink, BeckOK Datenschutzrecht/*Quaas*, Art. 12 Rn. 12.

keit sprengen.[500] Der Verantwortliche muss dann einen Ausgleich finden. Die Anforderung der leichten Zugänglichkeit spielt auf die faktische, niedrigschwellige Erreichbarkeit des Informationsmaterials an.[501] Auch dies ist in der Praxis regelmäßig unproblematisch. Das Gebot klarer und präziser Sprache wiederholt und bestärkt die im Rahmen der Form gestellten Anforderungen der Präzision und Verständlichkeit.[502] Diese Anforderung kann sich in Widerspruch zu Vorgaben der Form, dort dann der Präzision stellen, wenn es mit einer (allzu) einfachen Sprache nicht mehr gelingt, den Sachverhalt umfassend und zutreffend abzubilden.[503]

Die verantwortliche Stelle schuldet allein die Erbringung der Information, nicht deren Erfolg. Das konkrete Abrufen und die Wahrnehmung der Information fällt in die Verantwortungssphäre der betroffenen Person.[504]

b) Grenzen der Informations- und Auskunftspflicht

Die DSGVO erkennt drei Ausnahmegründe für die Informationspflichten an: Die Pflicht zur Information entfällt erstens, wenn die betroffene Person bereits über diese verfügt, Art. 13 Abs. 2 DSGVO. Zweitens entfällt die Pflicht bei Unmöglichkeit oder Unverhältnismäßigkeit. In Art. 14 Abs. 5 DSGVO ist dies ausdrücklich normiert, in Art. 13 und Art. 15 DSGVO fehlt dagegen derartige Ausnahmebestimmungen.[505] Gemeinhin werden diese Ausnahmetatbestände

---

[500] *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 22 „grundsätzliches Spannungsfeld". Ebenso *Wischmeyer*, AöR 143 (2018), 1, 53; *Kamps/Schneider*, K&R 19 (2020), 24, 25. Von einer „Pattsituation" spricht *Strassemeyer*, K&R 16 (2016), 176, 178, da sich der Verantwortliche bei komplexen Verarbeitungsformen entweder für eine vereinfachte oder eine detailgenaue Darstellung entscheiden muss.

[501] Die betroffene Person muss die Informationen mit den üblichen, ihr zur Verfügung stehenden Mitteln ohne besondere Hürden, Hinweise oder Mitwirkungspflichten erreichen und ohne Aufwand visualisieren können. Siehe eingehend Gola, DS-GVO/*Franck*, Art. 12 Rn. 21; *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 9.

[502] Bei schriftlicher Sprache muss diese klar und deutlich gehalten sein, ohne Verwendung komplexer Sprachgestaltungen, abstrakter oder missverständlicher Begrifflichkeiten und auch ohne Fachvokabular. Siehe im Einzelnen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 14; *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 9–11.

[503] Zu diesem Zielkonflikt Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 34; Gola, DS-GVO/*Franck*, Art. 12 Rn. 23.

[504] Dass die betroffene Person die zur Verfügung gestellten Informationen nicht liest, ist demnach ihr Risiko. Ein „Aufzwingen" von Informationen kennt die DSGVO nicht, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Quaas*, Art. 12 Rn. 25–26.

[505] Es ist daher auch von der „Absolutheit" der Informationspflicht die Rede, vgl. Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 34a.

aber auch für Art. 13 und 15 DSGVO anerkannt,[506] rechtsdogmatisch dann auf die allgemeinen Rechtsgrundsätze gestützt.[507] Drittens können rechtliche Gründe den Informations- und Auskunftspflichten entgegenstehen.[508] Insbesondere geht es dabei um Grundrechte und Grundfreiheiten der verarbeitenden Stellen, etwa in Form von Geschäfts- und Betriebsgeheimnissen oder Eigentumsrechten an den Datenverarbeitungstechniken oder -ergebnissen.[509] Rechtsdogmatisch geht man den Weg entweder über eine grundrechtskonforme Lesart der Art. 13–15 DSGVO[510] oder aber – so die überwiegende Ansicht – über eine nationale Beschränkungsgesetzgebung nach Art. 23 DSGVO.[511]

2. *Informationsprogramm für Datenverarbeitungen*

Das Informationsprogramm wird inhaltlich durch Art. 13–15 DSGVO (a)) sowie die Anforderungen der informierten Einwilligung (b)) definiert. Jenseits dessen sieht die DSGVO gewisse ergänzende Informations- und Aufklärungspflichten vor (c)). Art. 14 DSGVO hat die Situation vor Augen, dass die Daten

---

[506] So für die Unmöglichkeit Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Däubler*, Art. 13 Rn. 32; Gola, DS-GVO/*Franck*, Art. 15 Rn. 51. Ähnlich Sydow, DS-GVO/*Ingold*, Art. 13 Rn. 11; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 67. Bei der Unverhältnismäßigkeit muss das Missverhältnis allerdings so hoch sein, dass die Unverhältnismäßigkeit der Unmöglichkeit faktisch nahe kommt. Vgl. Gola, DS-GVO/*Franck*, Art. 15 Rn. 51. Der Europäische Datenschutzausschuss bzw. die Artikel 29 Datenschutzgruppe hat sich zu dieser Frage noch nicht explizit geäußert. Insbesondere den Leitlinien der *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 33–41 lässt sich keine klare Aussage entnehmen.

[507] Eine analoge Anwendung des Art. 14 Abs. 5 DSGVO auf Art. 13 und Art. 15 DSGVO wird allgemein abgelehnt. Es fehlt an einer planwidrigen Regelungslücke und der Vergleichbarkeit Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 22; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 13 Rn. 95; Sydow, DS-GVO/*Ingold*, Art. 13 Rn. 11.

[508] Vgl. Paal/Pauly, DS-GVO/*Paal*, Art. 23 Rn. 40. Siehe hierzu auch Erwägungsgrund 63 S. 5.

[509] In Erwägungsgrund 63 S. 5 wird hierauf Bezug genommen. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 23 Rn. 35; Paal/Pauly, DS-GVO/*Paal*, Art. 23 Rn. 42.

[510] Vgl. etwa Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 67.

[511] So die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 41 f. sowie die überwiegende Auffassung in der Literatur. Im deutschen Recht wurde eine entsprechende Ausnahme in § 32 Abs. 1 Nr. 4 BDSG normiert. Für Art. 13 DSGVO siehe etwa Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 68; Ehmann/Selmayr, DS-GVO/*Knyrim*, Art. 14 Rn. 48. Für Art. 15 DSGVO Sydow, DS-GVO/*Specht*, Art. 15 Rn. 32. AA Gola, DS-GVO/*Franck*, Art. 15 Rn. 51, der die dogmatische Grundlage für die Interessensabwägung im allgemeinen Rechtsgrundsatz von Gebot von Treu und Glauben sieht.

nicht bei der betroffenen Person erhoben wurden. Eine derartige Situation steht nicht im Fokus der Arbeit, sie soll in der Bearbeitung außer Betracht bleiben. Die folgenden Erwägungen lassen sich gleichwohl auf diese Konstellationen übertragen.

a) Informationspflichten nach Art. 13, 15 DSGVO

Art. 13 DSGVO normiert eine aktive Informationspflicht, denn hier muss der Verantwortliche von sich aus der betroffenen Person Informationen zur Verfügung stellen,[512] wohingegen Art. 15 DSGVO eine passive Auskunftspflicht darstellt, die eine Anfrage der betroffenen Person voraussetzt.[513] Die Transparenzpflichten setzen an unterschiedlichen Zeitpunkten des Verarbeitungszyklus an: Während die Informationspflicht nach Art. 13 DSGVO im Moment der Datenerhebung greift,[514] ist die Auskunft nach Art. 15 DSGVO im Moment des Antrages zu erteilen, was zeitlich vor, während oder nach der Datenverarbeitung sein kann.[515] Während Art. 13 DSGVO prognostischer Natur ist, kann der Präzisionsgrad bei Art. 15 DSGVO höher ausfallen, da hier die Datenverarbeitung bereits vorliegt; [516] das inhaltliche Programm ist jedoch grundsätzlich identisch.[517] Art. 13 Abs. 2 DSGVO erhält einen Zusatz, wonach dort gelistete Informationen nur bereitzustellen sind, soweit sie für die Gewährleistung einer fairen und transparenten Verarbeitung notwendig sind. Gemeinhin wird dies nicht als Einschränkung verstanden; die in Abs. 2 genannten Informationen sind stets und nicht nur fakultativ mitzuteilen.[518]

---

[512] *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 22: „[D]er Verantwortliche selbst [muss] aktiv werden". Ebenso Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 1. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 23 Rn. 1 „Bringschuld".

[513] Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 1.

[514] Die Information muss also noch vor Durchführung der Datenverarbeitung ergehen, ausführlich hierzu *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 17–19. Vgl. auch Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 12; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 56. Siehe auch *Kamps/Schneider*, K&R 19 (2020), 24, 28.

[515] Vgl. hierzu auch *Hoeren/Niehoff*, RW 9 (2018), 47, 54.

[516] Vgl. hierzu Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 27; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16.

[517] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Ehmann*, Anhang 2 Art. 6. Siehe zur Frage nach der zeitlichen Differenzierung und hieraus folgender Unterschiede des Informationsprogramms unter Kapitel 4 D. 3. a) cc).

[518] Siehe nur *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 16. Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 13; Küh-

Der Katalog der in Art. 13, 15 DSGVO genannten Informations- bzw. Auskunftspflichten[519] beinhaltet erstens die äußeren Umstände der Verarbeitung, etwa Name und Kontaktdaten des Verantwortlichen[520] und Verarbeitungszweck,[521] zweitens die rechtlichen Bedingungen der Verarbeitung, etwa die Rechtsgrundlage,[522] sowie drittens Betroffenenrechte, etwa Hinweise auf die in Art. 15–22 DSGVO vorgesehenen Rechte[523]. In Art. 15 Abs. 1 DSGVO hat die betroffene Person überdies Anspruch auf Auskunft darüber, welche der auf sie bezogenen Daten verarbeitet wurden.[524] Darüber hinaus fordert die Artikel 29 Datenschutzgruppe auch eine Aufklärung über Folgen und Risiken der Datenverarbeitung.[525] Informationspflichten technischer Art, etwa zu gewählten Verfahren und Methoden der Auswertung, sind nicht vorgesehen.

b) Informationspflichten nach dem Rechtmäßigkeitsgrundsatz

Informationspflichten ergeben sich, dies ist bereits ausgeführt worden, auch aus dem Rechtmäßigkeitsgrundsatz:[526] Die Einwilligung muss „in informierter Weise" erfolgen. Hier sind, wie bereits dargelegt, solche Informationen erforderlich, die es der betroffenen Person erlauben, Bedeutung und Tragweite der Einwilligungsentscheidung zu überblicken. Auch die vertragsgemäße Zulassung[527] sowie die Zulassung durch Interessensabwägung[528] setzen gewisse Informationen voraus. Diese Informationspflichten können inhaltlich über das

---

ling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 20. AA Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 16; Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 21–23.

[519] Die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 43–52 hat hierzu eine Tabelle erstellt.

[520] Art. 13 Abs. 1 lit. a) DSGVO.

[521] Art. 13 Abs. 1 lit. c) Art. 15 Abs. 1 lit. a) DSGVO.

[522] Art. Art. 13 Abs. 1 lit. c) DSGVO.

[523] Art. 13 Abs. 2 lit. b), Art. 15 Abs. 1 lit. e) DSGVO.

[524] Art. 15 Abs. 1 HS. 1 DSGVO. Vgl. hierzu Gola, DS-GVO/*Franck*, Art. 15 Rn. 5, sogenannte „Negativauskunft". Siehe auch Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 8.

[525] *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 8 f. Dies findet sich auch in Erwägungsgrund 39 S. 5, demzufolge auch über die Risiken und Folgen der Verarbeitung aufzuklären ist.

[526] Vgl. zur Anknüpfung und Ausgestaltung des Transparenzgebots im Rechtmäßigkeitsgrundsatz siehe auch *Schulte*, PinG 5 (2017), 227, 229. Zur Verbindung von Einwilligung und Transparenzgrundsatz siehe auch *Artikel 29 Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.04.2018, S. 14–15, 17.

[527] Siehe hierzu in Kapitel 4 B II. 3. am Anfang.

[528] Siehe hierzu eingehend Kapitel 4 B II. 4. c).

Programm der Art. 13, 15 DSGVO hinausreichen, aber auch dahinter zurückbleiben.[529]

c) Beschränkte Informationspflichten jenseits des Datenverarbeitungsrechtsverhältnisses: allgemeine Stärkung der Medienkompetenz und des Risikobewusstseins

In die Transparenzpflichten treten auch Akteure jenseits des Datenschutzrechtsverhältnisses ein, wenngleich mit einem inhaltlich zurückgefahrenen Informationsauftrag. Nach Art. 57 Abs. 1 lit. b) DSGVO hat die Aufsichtsbehörde einen proaktiven Bildungs-, Aufklärungs- und Sensibilisierungsauftrag.[530] Ziel ist die Stärkung der Medienkompetenz[531] und des Risikobewusstseins.[532] Diesen Zielen dient auch der Tätigkeitsbericht der Aufsichtsbehörde in Art. 59 Abs. 1 DSGVO.[533] Üblicherweise enthält er eine Darstellung auffälliger Entwicklungen, Risiken oder Schutzgarantien.[534] Auch der Europäische Datenschutzausschuss nimmt an die Allgemeinheit gerichtete, dann aber allein allgemeine Aufklärungspflichten wahr, dies dann in Form des Jahresberichts nach Art. 71 DSGVO.[535] Datenschutzbeauftragte treffen dagegen keine eigen-

---

[529] Siehe bereits oben Kapitel 4 C. II. 2. a).

[530] Dieser verpflichtet zur proaktiven Öffentlichkeitsarbeit. Siehe hierzu eingehend Paal/Pauly, DS-GVO/*Körffer*, Art. 57 Rn. 6; Kühling/Buchner, DS-GVO, BDSG/*Boehm*, Art. 58 Rn. 33; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Polenz*, Art. 58 Rn. 52. Vgl. zu möglichen Inhalten des Aufklärungsauftrags Paal/Pauly DS-GVO/*Körffer*, Art. 57 Rn. 3; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Polenz*, Art. 58 Rn. 51.

[531] Siehe auch Erwägungsgrund 132. Vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Eichler*, Art. 57 Rn. 7–8; Paal/Pauly, DS-GVO/*Körffer*, Art. 57 Rn. 3.

[532] Siehe hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Polenz*, Art. 57 Rn. 13–17.

[533] Dieser soll ein grundlegendes Bild von der Anwendung und Umsetzung der DSGVO und datenschutzrechtlichen Fragestellungen bieten, vgl. zu den Zielen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Polenz*, Art. 59 Rn. 2; Wolff/Brink, BeckOK Datenschutzrecht/*Moos*, Art. 39 Rn. 19. Zum Zusammenhang mit dem Aufklärungsauftrags nach Art. 57 Abs. 1 lit. b) DSGVO siehe Ehmann/Selmayr, DS-GVO/*Selmayr*, Art. 57 Rn. 13.

[534] Mit beispielhafter Aufführung von möglichen Inhalten der Tätigkeitsberichte Ehmann/Selmayr, DS-GVO/*Selmayr*, Art. 59 Rn. 7; Paal/Pauly DS-GVO/*Eichler*, Art. 59 Rn. 4; Plath, DSGVO/BDSG/*Hullen*, Art. 59 Rn. 2; Paal/Pauly DS-GVO/*Körffer*, Art. 59 Rn. 4; Gola, DS-GVO/*Nguyen*, Art. 59 Rn. 3. Zum Zusammenhang mit Art. 57 Abs. 1 lit. b) DSGVO siehe etwa Gola, DS-GVO/*Nguyen*, Art. 59 Rn. 1, 3.

[535] Die Inhalte werden sich dabei an den Berichten der Aufsichtsbehörden orientieren und die generalisierbaren und unionsweit als berichtenswert erachteten Datenschutzverstöße und Gegenmaßnahmen, technischen Entwicklungen und Risiken der Digitaltechnik zusammenfassen. Siehe eingehend zu Funktionen und Inhalten des Jahresberichts Paal/Pauly DS-GVO/*Körffer*, Art. 71 Rn. 3.

ständigen Informationspflichten.[536] An den umfassenden Einblicksrechten in die Verarbeitungstechniken und -ergebnisse, die den Aufsichtsbehörden und Datenschutzbeauftragten zustehen, haben die betroffenen Personen damit keinen Anteil. Diese Einblicksrechte dienen allein als Grundlage von Kontrollen, Sanktionen oder Beratungen. Damit wird einmal mehr deutlich, dass das Transparenzpflichtenverhältnis dem Datenverarbeitungsrechtsverhältnis entspricht: Es ist zwischen Verantwortlichen und betroffener Person konstruiert.

3. Informationsprogramm für automatisierte Entscheidungen einschließlich Profiling

Die DSGVO sieht ein besonders Transparenzkonzept für automatisierte Entscheidungen einschließlich Profiling vor. In Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO sind spezifische Informationspflichten für automatisierte Entscheidungen vorgesehen (a)), im Übrigen bedarf auch die Ausnahmezulassung nach Art. 22 Abs. 2 DSGVO besonderer Informationen (b)). Schließlich werden besondere Informationspflichten auch als unbenannte Schutzmaßnahme in Art. 22 Abs. 3 DSGVO diskutiert (c)).

a) Informationspflichten Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO

Hinsichtlich der besonderen Informationspflichten der Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO ist schon der Anwendungsbereich unklar (aa)), doch auch die konkreten Inhalte sorgen für Rechtsunsicherheiten (bb)). Offen ist schließlich, ob diese Informationsvorschriften unterschiedliche Informationsprogramme enthalten (cc)).

aa) Anwendungsbereich: Profiling und automatisierte Entscheidungen

Die maßgeblichen Vorschriften ordnen spezifische Informationspflichten für „automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Absätze 1 und 4“ an. Unzweifelhaft erfasst sind automatisierte Entscheidungen

---

[536] Art. 38 Abs. 4 DSGVO sieht zwar eine Beratungspflicht vor, hier fungiert der Datenschutzbeauftragte aber allein als Bindeglied, Mediator bzw. Ombudsstelle zwischen betroffener Person und Verantwortlichem, vgl. zu dieser Funktion Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 37 Rn. 9; Ehmann/Selmayr, DS-GVO/*Heberlein*, Art. 38 Rn. 18; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Däubler*, Art. 38 Rn. 15. Die Informationspflichten, die den Verantwortlichen treffen, kann er nicht selbst erfüllen, vielmehr soll er gerade die ordnungsgemäße Erfüllung dieser Pflichten überprüfen bzw. hierzu anregen. Siehe hierzu eingehend Kühling/Buchner, DS-GVO, BDSG/*Bergt*, Art. 38 Rn. 37; Wolff/Brink, BeckOK Datenschutzrecht/*Moos*, Art. 38 Rn. 28; Paal/Pauly, DS-GVO/*Paal*, Art. 38 Rn. 12; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Jaspers/Reif*, Art. 38 Rn. 25. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Drewes*, Art. 38 Rn. 44–45.

im Sinne des Art. 22 DSGVO.[537] Im Übrigen bestehen aber einige rechtliche Unklarheiten, von denen nachfolgend nur ein Ausschnitt präsentiert werden soll.[538] Umstritten ist etwa, ob die Vorschrift auch dann gelten soll, wenn der automatisierten Entscheidung kein Profiling zugrunde liegt ((1)), oder ob das Profiling unabhängig von einer automatisierten Entscheidung erfasst ist ((2)). Unklar ist auch, ob die Vorschrift für automatisierte Entscheidungen jenseits des Art. 22 DSGVO gilt ((3)).

(1) Automatisierte Entscheidungen nur in Verknüpfung mit Profilingmaßnahmen

Die Frage, ob die besonderen Informationspflichten auch isoliert automatisierte Entscheidungen, d.h. solche ohne eine Profilbildung, erfassen, hat ihren Ursprung in der Parenthese „zumindest in diesen Fällen", deren Auslegung für Schwierigkeiten sorgt.[539] Allein der Zusatz „zumindest" ist eindeutig: Dem Verantwortlichen steht es frei, jenseits der gesetzlichen Pflicht freiwillig entsprechende Informationen bereitzustellen.[540] Offen ist aber der Bezugspunkt des Einschubs „in diesen Fällen". Je nach Lesart ergibt sich daraus, dass die besonderen Informationspflichten nur für eine automatisierte Entscheidung auf Grundlage einer Profilbildung oder für die automatisierte Entscheidung unabhängig von einer Profilbildung gelten. Sie lässt sich aber auch so lesen, dass die Vorschrift sowohl für die automatisierte Entscheidung als auch die Profilbildung gilt. Der EuGH hat sich in diesen Fragen noch nicht positioniert.

In einer Lesart der Parenthese wird das Profiling als konstitutives Merkmal der automatisierten Entscheidung verstanden.[541] Die besonderen Informations-

---

[537] Siehe nur Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 52; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 57; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28; *Sesing*, MMR 24 (2021), 288 f.

[538] Aufgrund des Wortlauts „gemäß Art. 22 Absätze 1 und 4" wird etwa auch diskutiert, ob die Informationspflichten auch dann gelten, wenn die automatisierte Entscheidung ausnahmsweise nach Art. 22 Abs. 2 DSGVO zugelassen wurde. Gemeinhin wird dies befürwortet. Siehe zu dieser Problematik etwa Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31.

[539] Zutreffend bezeichnet *Martini*, Blackbox Algorithmus, 2019, S. 184 diese als „sibyllinisch". *Sesing*, MMR 24 (2021), 288, 290 bezeichnet sie als „wenig geglückt". Auch andere Sprachfassungen, insbesondere die englische und französische, bringen keine Klarheit („the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved"; „l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente").

[540] Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 13 Rn. 77; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 27.

[541] Dabei muss das Profiling die automatisierte Entscheidung aber nicht ausschließlich tragen. So präzisierend Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 52.

pflichten greifen demnach nur „in den Fällen“ einer automatisierten Entscheidung, der ein Profiling zugrunde liegt und gelten damit weder isoliert für die automatisierte Entscheidung noch isoliert für das Profiling.[542] In einer zweiten Lesart des Einschubs wird allein die automatisierte Entscheidung unabhängig von einem Profiling gedacht. Die besonderen Transparenzpflichten seien vorgesehen „in den Fällen“ einer automatisierten Entscheidung.[543] Das Profiling ist demnach nur erfasst, wenn und soweit es in der automatisierten Entscheidung aufgeht, die automatisierte Entscheidung ist dagegen abgedeckt unabhängig vom Profiling.

(2) Besondere Informationspflichten beim Profiling

Nur sehr vereinzelt wird dafür eingetreten, die besonderen Transparenzvorschriften isoliert auf das Profiling anzuwenden, d.h. auch ohne dass dieses in eine automatisierte Entscheidung Eingang findet.[544] Teilweise werden solche Transparenzpflichten nur für risikoreiche Profilbildungen gefordert.[545] Hier

---

[542] So Ehmann/Selmayr, DS-GVO/*Knyrim*, Art. 13 Rn. 63–64. Wohl auch Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31. Dieser Ansicht wird mit dem Argument entgegengetreten, die DSGVO kenne eine solche Verknüpfung nicht, weder in Art. 22 DSGVO noch in Art. 35 Abs. 3 lit. a) DSGVO, siehe *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 148. Angeführt wird auch, dass auch die Vorgängervorschrift des Art. 15 DSRL eine solche Einschränkung nicht enthielt, so *Dammann*, ZD 6 (2016), 307, 312: „Der Tatbestand wurde generalisiert“ sowie Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 14b. Auch der Entwurf der DSGVO der Europäischen Kommission und vom Europäischen Parlament enthielt eine derartige Einschränkung, die dann aber nach den Anregungen des Europäischen Rates in die Endfassung des Art. 22 DSGVO nicht übernommen wurde, vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 10; Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 12.

[543] So *Martini*, Blackbox Algorithmus, 2019, S. 178; *Sesing*, MMR 24 (2021), 288, 290. So auch Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 27, der Informationen zu automatisierten Entscheidungen ohne Profiling in das Ermessen des Verantwortlichen stellt. Im Ergebnis ebenso ohne nähere Begründung Kuner/Bygrave/Docksey, GDPR/*Zanfir-Fortuna*, Art. 13 Rn. 429. So wohl auch Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Däubler*, Art. 13 Rn. 23 sowie *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 148. Angeführt wird vor allem auch der Gleichlauf mit Art. 22 DSGVO, vgl. Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 77.

[544] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16. So auch Kuner/Bygrave/Docksey, GDPR/*Zanfir-Fortuna*, Art. 13 Rn. 429. So wohl auch *Strassemeyer*, K&R 16 (2016), 176, 179. Befürwortend auch *Norwegian Data Protection Authority*, Big Data, September 2013, S. 51 f. Nicht ganz eindeutig Gola, DS-GVO/*Franck*, Art. 13 Rn. 30 f.; Sydow, DS-GVO/*Ingold*, Art. 13 Rn. 20; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 57. Für die Zulässigkeit freiwilliger Informationen über das Profiling unabhängig von einer automatisierten Entscheidung plädieren Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 32; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 77.

[545] Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53.

wird eine dritte Lesart der Parenthese eingeführt, bei der Bezugspunkt das Profiling *oder* die automatisierte Entscheidung ist. Die besondere Transparenzvorschriften gelten also „in den Fällen" des Profilings *oder* der automatisierten Entscheidung.[546] Diese Lesart befürwortet vor allem der Europäische Datenschutzausschuss.[547] Begründet wird dies mit dem Wortlaut der Art. 13 Abs. 2 lit. f) DSGVO bzw. Art. 15 Abs. 1 lit. h) DSGVO – siehe hierzu oben – sowie mit der besonderen Gefährlichkeit dieser Art der Datenverarbeitung.[548] Die überwiegende Ansicht in der Literatur tritt dem entgegen.[549] Angeführt wird neben dem Wortlaut, siehe hierzu oben,[550] vor allem, dass es andernfalls zu Wertungswidersprüchen mit Art. 22 DSGVO käme,[551] zudem die DSGVO keine profilingspezifische Regulierung kenne.[552] Über das Profiling ist nach überwiegender Ansicht nur zu informieren, soweit es in der automatisierten Entscheidung aufgeht.

(3) Erstreckung auf automatisierte Entscheidungen jenseits des Art. 22 DSGVO

Teilweise wird vorgeschlagen, die besonderen Transparenzvorschriften auch auf automatisierte Entscheidungen jenseits des Art. 22 DSGVO zu erstrecken, etwa solche, die nicht ausschließlich auf einer automatisierten Datenverarbei-

---

[546] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 16, 18. Aus der Parenthese liest Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 27 einen Ermessensspielraum für den Verantwortlichen ab, ob er beim Profiling besondere Informationen bereitstellt.

[547] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 18; *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 47; *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 27.

[548] So Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53; *Strassemeyer*, K&R 16 (2016), 176, 179. Ohne nähere Begründung Kuner/Bygrave/Docksey, GDPR/*Zanfir-Fortuna*, Art. 13 Rn. 429.

[549] Siehe nur Gola, DS-GVO/*Franck*, Art. 13 Rn. 30; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 25–26; *Martini*, Blackbox Algorithmus, 2019, S. 178; *Lorentz*, Profiling, 2019, S. 236 f. So auch *Sesing*, MMR 24 (2021), 288, 289 mwN.

[550] Auf den Wortlaut und damit eine andere Lesart der Parenthese „in den Fällen" beziehen sich insbesondere *Lorentz*, Profiling, 2019, S. 236; Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31; *Sesing*, MMR 24 (2021), 288, 290.

[551] Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 77.

[552] Vgl. etwa *Martini*, Blackbox Algorithmus, 2019, S. 178; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 148. Hingewiesen wird überdies auf das Gesetzgebungsverfahren: Im Vorschlag des Europäischen Parlaments war zunächst eine Informationspflicht allein für das Profiling vorgesehen, der Entwurf des Rates formulierte diese aber auf automatisierte Entscheidungen inklusive Profiling um. Siehe hierzu eingehend *Lorentz*, Profiling, 2019, S. 236, 238; *Bräutigam/Schmidt-Wudy*, CR 31 (2015), 56, 61 f.

tung beruhen oder keine rechtlichen oder erheblichen Beeinträchtigungswirkungen aufweisen.[553] Dabei wird auf den Wortlaut verwiesen, der anders als Art. 22 DSGVO keine Einschränkungen der automatisierten Entscheidung vornimmt.[554] Überwiegend wird dies jedoch abgelehnt[555] und hierfür vor allem die Kohärenz der Vorschriften in der DSGVO zu automatisierte Entscheidungen hingewiesen.[556]

bb) Inhalt der Informationspflichten

Die Informationspflicht in Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO enthält drei Aspekte: Erstens die Aufklärung über das Bestehen einer automatisierten Entscheidung,[557] zweitens aussagekräftige Informationen über die involvierte Logik sowie drittens die Tragweite und angestrebten Auswirkungen

---

[553] So etwa Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 52; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 57; *Strassemeyer*, K&R 16 (2016), 176, 179. Ebenso *Edwards/Veale*, SSRN Journal 2017, 53, die die Vorschrift auf sämtliche automatisierte Entscheidungen, unabhängig vom Verfahren, anwenden wollen. Nicht ganz klar, ob de lege lata oder de lege ferenda *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 265. Zumindest für die Zulässigkeit einer freiwilligen Informationspflicht für derartige automatisierte Entscheidungen treten ein Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 23; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 77. Dagegen geht die *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 27 von einem strengeren Verständnis aus, betont aber, dass die Übertragung der Informationspflichten auf sonstige automatisierte Entscheidungen „einer guten Praxis" entsprächen. Allein Entscheidungen im Sinne des Art. 22 DSGVO erfasst sehen *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 24; *Martini*, Blackbox Algorithmus, 2019, S. 178; Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 282. Eine entsprechende Normierung durch Mitgliedstaaten für zulässig hält Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 16, 18.

[554] Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 52; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 57.

[555] Ebenso *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 18. Ablehnend auch Gola, DS-GVO/*Franck*, Art. 13 Rn. 29; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 77; Kuner/Bygrave/Docksey, GDPR/*Zanfir-Fortuna*, Art. 13 Rn. 429 f.; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 282.

[556] Vgl. Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 24–25; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 77.

[557] Dies ist auch in Erwägungsgrund 71 S. 4 aufgeführt. Vgl. zu dieser Pflicht auch *Martini*, Blackbox Algorithmus, 2019, S. 177; *Walter*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 391, Rn. 21; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 32; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 34; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 145 f.

der automatisierten Entscheidung.[558] Tragweite und angestrebte Auswirkungen spielen auf die beabsichtigten und unbeabsichtigten Folgen der automatisierten Entscheidung an.[559] Dagegen ist unklar, was mit „aussagekräftigen Informationen über die involvierte Logik" gemeint ist. Hierauf ist zurückzukommen.[560]

cc) Zeitlich differenzierte Informationspflichten

Unklar ist darüber hinaus, ob Art. 13 Abs. 2 lit. f) und Art. 15 Abs. 1 lit. f) DSGVO unterschiedliche Informationspflichten begründen, da diese an unterschiedlichen Zeitpunkten anknüpfen.[561] Da im Vorhinein eine konkrete Entscheidung noch nicht vorliegt, kann nur über die grundlegende, allgemeine Systemfunktionalität der algorithmischen Entscheidungsarchitektur und der darin integrierten, womöglich unterschiedlichen Algorithmen informiert werden. Demgegenüber kann im Nachhinein über den konkret verwendeten Algorithmus, dessen Auswertung und die Inhalte der konkreten algorithmischen Entscheidung informiert werden.[562] Diese Pflicht zur nachträglichen Erläuterung der Entscheidung(sgründe) wird unter dem Begriff des Rechts auf Erklärung (Right to Explanation) diskutiert, auf das noch vertieft einzugehen ist.[563] Vielfach wird aber, gestützt auf die identische Wortwahl der Vorschriften[564]

---

[558] Nach überwiegender Ansicht ist auch über das Bestehen der Betroffenenrechte in Art. 22 Abs. 3 DSGVO zu informieren. Dies wird aus der in Erwägungsgrund 71 S. 4 benannten Pflicht zur „spezifischen Unterrichtung" herausgelesen. So etwa Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 32; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 41d–41e.

[559] Abzustellen ist damit auf die automatisierte Entscheidung, für die das Profiling die Grundlage bietet, nicht auf das Profiling selbst, siehe hierzu Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 55; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 29. Ebenso *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 28 f.

[560] Siehe unter Kapitel 4 D. III. 3. b) aa).

[561] Vgl. allgemein zu den potentiell unterschiedlichen Informationsgehalten der Vorschriften *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 78 f.

[562] Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25.

[563] Siehe Kapitel 5 B. III. 2. b) sowie Kapitel 5 B. III. 3 a) bb).

[564] Zu diesem Argument *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 84, 97; *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 870 f.; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 283; *Martini*, Blackbox Algorithmus, 2019, S. 192. Vgl. auch Plath, DSGVO/BDSG/*Kamlah*, Art. 15 Rn. 14. AA *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233, 241; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 195 f.; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 256, die den Fokus auf die Unterschiedlichkeit der Formulierungen legen. Hingewiesen wird auch auf die prognostische Ausgestaltung des Art. 15 DSGVO („angestrebte Auswirkungen"), so *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 283; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 83; *Martini*, Blackbox Algorithmus, 2019, S. 192. AA *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 256;

und den systematischen Gleichlauf der Vorschriften,[565] für einen inhaltlichen Gleichlauf der Informationspflichten der Art. 13 und Art. 15 DSGVO eingetreten.[566] Der Europäische Datenschutzausschuss hat sich noch nicht klar zu dieser Frage positioniert.[567]

b) Informationspflichten nach der Ausnahmezulassung gem. Art. 22 Abs. 2 DSGVO

Die ausnahmsweise Zulassung der automatisierten Entscheidung nach Art. 22 Abs. 2 lit. a) und c) DSGVO löst, dies ist bereits im Rahmen der Rechtmäßigkeit dargelegt worden,[568] eigene Informationspflichten aus. Dies gilt vor allem für die Einwilligung, die in informierter Weise ergehen muss. Informationen sind insoweit notwendig, als sie die betroffene Person befähigen, die Bedeutung und Tragweite ihrer Entscheidung, hier also der Ausnahmezulassung der automatisierten Entscheidung, abzuschätzen.[569] Dies setzt voraus, dass die betroffene Person die Folgen und Risiken der Zulassung der automatisierten Entscheidung vorhersehen kann. Über diese ist also vorab zu informieren, soweit sie für die betroffene Person nicht ohne Weiteres erkennbar

---

Vogel, Künstliche Intelligenz und Datenschutz, 2021, S. 195 f., die auf die übrigen Formulierungen des Art. 15 DSGVO abstellen, in der derart prognostische Ansätze nicht erkennbar sind, und darauf hinweisen, dass mit „angestrebten Auswirkungen" auch Spätfolgen der Entscheidung gemeint sein können.

[565] Auf die Systematik weist *Wischmeyer*, AöR 143 (2018), 1, 51 hin. Vgl. auch die Kommentarliteratur zu Art. 13 und Art. 15 DSGVO, die vielfach von einer Inhaltsgleichheit der Vorschriften ausgehen, so etwa Plath, DSGVO/BDSG/*Kamlah*, Art. 15 Rn. 14; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 13 Rn. 77; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 27; Gola, DS-GVO/*Franck*, Art. 15 Rn. 17.

[566] So etwa *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 283; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 83; *Martini*, Blackbox Algorithmus, 2019, S. 192; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 27; Gola, DS-GVO/*Franck*, Art. 15 Rn. 17; Plath, DSGVO/BDSG/*Kamlah*, Art. 15 Rn. 14.

[567] Zu dieser Frage findet sich in den Ausführungen der *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 29 f. zu Art. 15 DSGVO keine klare Aussage.

[568] Siehe Kapitel 4 C. II. 5.

[569] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 14, 26 mit Verweis auf *Artikel 29 Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, 10.04.2018, S. 15–18. Siehe auch *Kaminski*, BTLJ 34 (2019), 189, 203, 211-212; *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 26–27, 36.

sind. Teilweise wird auch hier eine Information im Sinne des Art. 13 Abs. 2 lit. f) DSGVO, dann also über die involvierte Logik verlangt.[570]

c) Informationspflichten nach Art. 22 Abs. 3 DSGVO

Art. 22 Abs. 3 DSGVO enthält keine expliziten Transparenzvorschriften. Da die darin normierten Betroffenenrechte aber nicht abschließend sind, wird die Vorschrift herangezogen, um Transparenzlücken zu schließen, die nach Anwendung der übrigen, oben vorgestellten Informationspflichten verbleiben. Inhaltlich ist hier nichts vorgegeben, entsprechend unklar sind Inhalte und Grenzen. Das bereits erwähnte Recht auf Erklärung (Right to Explanation)[571] wird vielfach auch in Art. 22 Abs. 3 DSGVO verortet.[572]

4. Ergebnis

Informationspflichten hinsichtlich der Datenverarbeitung beziehen sich allein auf den nicht-technischen Bereich. Sie ergeben sich aus den Informationspflichten nach Art. 13–15 DSGVO sowie den Anforderungen des Rechtmäßigkeitsgrundsatzes. Ergänzt wird dies durch allgemeine Aufklärungspflichten verschiedener Datenschutzinstitutionen. Einblicke in die technischen Umstände der Datenverarbeitung kennt die DSGVO nicht, allein für automatisierte Entscheidungen ist derartiges vorgesehen. Dort ist aber rechtlich vieles unklar. Zum einen ist offen, welche Verfahren – automatisierte Entscheidung im Sinne oder auch jenseits des Art. 22 DSGVO, Profiling oder nur kumulativ automatisierte Entscheidung auf Grundlage des Profilings – von der Informationspflicht erfasst sind, zum anderen, was der Inhalt der Pflicht zur Bereitstellung „aussagekräftige(r) Informationen zur involvierten Logik“ erfasst und ob Art. 13 und Art. 15 DSGVO ein identisches Informationsprogramm aufstellen. Auch Art. 22 Abs. 3 DSGVO kann eigene Informationspflichten enthalten, für die es aber inhaltlich noch gänzlich an Konturen fehlt. Der EuGH war mit all diesen Fragen bislang noch nicht befasst.

III. Analyse des Transparenzgrundsatzes als Instrument zur Regulierung autonomer Systeme

Bei der Anwendung des Transparenzmodells der DSGVO auf autonome Systeme ist zwischen den einzelnen Verarbeitungsstufen zu differenzieren. Inhalt

---

[570] In der Literatur werden die einwilligungs- und die transparenzbezogenen Informationspflichten daher vielfach gleichgesetzt. Siehe etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 53; Paal/Pauly, DS-GVO/*Martini*, Art. 25 Rn. 38; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 42.

[571] Hierzu genauer unter Kapitel 5 B. III. 2. b) sowie Kapitel 5 B. III. 3 a) bb).

[572] So etwa *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 254.

und Reichweite der Informationspflichten unterscheiden sich beim Modellbildungsverfahren (1.), bei der Profilerstellung (2.) und bei der Profilverwendung (3.) erheblich.

1. Modellbildung: Transparenz Maschineller Lernverfahren

Im Rahmen der Modellbildung bestehen nur eingeschränkte Informationspflichten. Da diese kein Profiling im Sinne des Art. 4 Nr. 4 DSGVO, erst recht nicht eine automatisierte Entscheidung nach Art. 22 DSGVO darstellt, stellen sich Fragen der Offenlegung von technischen Verfahren erst gar nicht.[573] Es bleibt bei den ganz basalen Transparenzgeboten der Art. 13 Abs. 1, 2 und Art. 15 DSGVO. Im Rahmen der Zweckbestimmung ist, wie ausgeführt,[574] dann auf das zweistufige Profilbildungsverfahren und die Bedeutung des Modells als Grundlage der Profilbildung und als Maßnahme zum Erkenntnisgewinn über die Personengesamtheit im Datensatz hinzuweisen, im Übrigen darauf, dass die Modellbildung der Realisierung autonomer Systeme dient. Auch die Transparenzanforderungen der Einwilligung, erst recht dann der anderen Zulassungsbedingungen, gehen über dieses Programm nicht hinaus. Um die Bedeutung und Tragweite der Datenfreigabe für die Modellbildung einzuschätzen, genügt das Wissen, dass die Modellbildung der Musterbildung zu generalisierenden Persönlichkeitseigenschaften und Verhaltensweisen für einen bestimmten Dienst dient. Welchen Inhalts diese im Einzelnen sind, muss die betroffene Person nicht wissen, um ihre Entscheidung sinnvollerweise treffen zu können. Dass diese Maschinellen Lernverfahren und die Ergebnisse hieraus menschlich nurmehr begrenzt verständlich sind, ist auf Stufe der Modellbildung datenschutzrechtlich nicht von Bedeutung.

2. Profilbildung: Transparenz bei Einsatz selbstlernender Algorithmen

Komplexe Fragen der Transparenz stellen sich auf der Stufe der Profilbildung. Unterscheiden lassen sich Informationspflichten ex ante (a)) sowie ex post (b)) einer Profilbildungsmaßnahme. Die Informationen sind laienverständlich an-

---

[573] So auch im Ergebnis *Leenes*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 293, 300. Dies gilt dann auch für das Maschinelle Lernverfahren für die Erstellung eines Lösungsalgorithmus. Anders aber die italienische Datenschutzbehörde, die hinsichtlich des Maschinellen Lernverfahrens für die Erstellung des Lösungsalgorithmus bei ChatGPT eine Offenlegung der Methode, Logik und Funktionsweise der Verarbeitung fordert („le modalità del trattamento, la logica alla base del trattamento necessario al funzionamento del servizio" – in englischer Übersetzung: „information on how the processing is carried out, the logic underlying the processing that is necessary for the operation of the service"), siehe *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 2, 6.

[574] Siehe Kapitel 4 C III. 1. a).

zubieten (c)). Dieses Informationspflichtenprogramm ist durch die Profilbildung anhand autonomer Systeme besonders herausgefordert (d)).

a) Informationspflichten im Vorhinein einer Profilbildung

Im Vorfeld einer Profilbildung ergeben sich Transparenzgebote aus den Informationspflichten der Art. 13, 15 DSGVO (aa)) sowie aus der Rechtmäßigkeit, insbesondere der Einwilligung (bb)).

aa) Informationspflichten nach Art. 13 DSGVO

Die generellen Informationspflichten der Art. 13 DSGVO gelten für die Profilbildung ohne weiteres. Für die Zweckbestimmung ist, wie ausgeführt,[575] auf das Ziel des Erkenntnisgewinns jenseits des Rohdatums durch das zweistufige Profilbildungsverfahren hinzuweisen sowie auf das Erkenntnisinteresse, etwa die Prognose oder Bewertung, die Persönlichkeitsmerkmalsgruppen und den Anwendungskontext.

Informationspflichten zum Profilbildungsverfahren bestehen nur, wenn man eine Anwendung des Art. 13 Abs. 2 lit. f) DSGVO auch auf das Profiling befürwortet. Der überwiegende Teil der Literatur tritt dem, wie beschrieben, entgegen.[576] Soweit aber eine automatisierte Entscheidung auf ein Profiling folgt, erstreckt die Literatur mehrheitlich die auf die automatisierte Entscheidung bezogene Informationspflicht auch auf das in dieser aufgehende Profiling.[577]

Soweit man eine (annexhafte) Anwendung des Art. 13 Abs. 2 lit. f) DSGVO befürwortet, ist unklar, welchen Inhalt diese Informationspflicht hat. Gemeinhin wird verlangt, dass auf das Stattfinden der Profilbildung hingewiesen wird.[578] Gefordert wird im Weiteren teilweise eine Offenlegung des Algorithmus, der der Profilbildung zugrunde liegt,[579] überwiegend wird aber nur eine Erläuterung der grundlegenden Funktionsweise der Profilbildung verlangt.[580]

---

[575] Siehe Kapitel 4 C III. 2. a).

[576] Siehe oben Kapitel 4 D. 3. a) aa) (2).

[577] Siehe oben Kapitel 4 D. 3. a) aa) (2).

[578] Siehe auch Erwägungsgrund 60 S. 3. Befürwortend auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 18. Ebenso Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 52; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16. AA *Lorentz*, Profiling, 2019, S. 247.

[579] So die *Norwegian Data Protection Authority*, Big Data, September 2013, S. 51: „[A]ccess should also be granted to the decision-making criteria (algorithms) the development of the profile is based upon".

[580] So Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28a. Ähnlich Ehmann/Selmayr, DS-GVO/*Ehmann*, Art. 15 Rn. 19: „das Prinzip [ist] darzustellen, auf dem die Berechnung basiert". So auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 28: „Der

Noch enger sind Lesarten des Art. 13 Abs. 3 lit. f) DSGVO, die über das Profiling nur insoweit informieren wollen, als dieses die automatisierte Entscheidung trägt. Stellen also die Profilinhalte die wesentlichen Entscheidungsparameter dar, so sind dieser Lesart zufolge diese profilbasierten Entscheidungskriterien – etwa das Alter, der Wohnungsort oder das Interesse an einem bestimmten Produkt – zu nennen; auf das Profilbildungsverfahren ist aber nicht einzugehen.[581]

Aufzuklären ist darüber hinaus über die Tragweite und angestrebten Wirkungen der Profilbildung. Dies erfasst zum einen das Stattfinden der Profilbildung und die Erzeugung von Erkenntnissen jenseits des Rohdatums sowie die Bedeutung des Profils für autonome Systeme, d.h. deren Relevanz für die Automatisierung einer Anwendung, schließlich auch den Anwendungskontext, aus dem sich dann die Folgen der Profilbildung ableiten lassen.[582] Dies ist bereits Teil der Informationspflichten im Rahmen der Zweckbestimmung sowie der Rechtmäßigkeit.

bb) Informationspflichten aufgrund des Rechtmäßigkeitsgrundsatzes

Das Informationsprogramm im Rahmen der Rechtmäßigkeit,[583] wie es für die Einwilligung,[584] die vertragsimmanente Zulassung[585] und die Interessensabwägung[586] gilt, ist bereits eingehend dargestellt worden: Hinzuweisen ist auf das Stattfinden der Profilbildung sowie auf das zweistufige Profilbildungsverfahren, anhand dessen durch Abgleich mit dem Modell, d.h. mit Erkenntnissen über Dritte, aus Rohdaten weitreichende, auch intime Persönlichkeitsmerkmale und Verhaltensweisen ermittelt werden können. Was den Detailgrad der Informationspflichten hinsichtlich der neu generierten Daten anbelangt, herrscht, auch dies ist bereits eingehend dargestellt worden,[587] Uneinigkeit: Während die einen eine umfassende Prognose sämtlicher Profilinhalte verlangen, lassen andere Grobbeschreibungen im Sinne des Art. 4 Nr. 4 DSGVO genügen, während wiederum andere Informationen auf die Informationspflichten des Transparenzgebots nach Art. 13–15 DSGVO, d.h. auf vorherige und nachträgliche Informationen zum Profilbildungsverfahren verweisen.

Verantwortliche [sollte] […] über die der Entscheidungsfindung zugrundeliegenden Überlegungen bzw. Kriterien […] informieren".

[581] In diese Richtung wohl Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 10; Gola, DS-GVO/*Franck*, Art. 13 Rn. 30.

[582] Ebenso Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 19, dort spezifisch zum Kredit-Scoring. Siehe hierzu auch Kapitel 4 C III. 2. a) sowie Kapitel 4 C. III. 2. b) aa).

[583] Siehe zur Bedeutung der Transparenz im Rahmen des Transparenzgrundsatzes allgemein Kapitel 4 D. I. 2. b).

[584] Siehe Kapitel 4 C. III. 2. b) aa).

[585] Siehe Kapitel 4 C. III. 2. c).

[586] Siehe Kapitel 4 C. III. 2. d) aa) sowie Kapitel 4 C. III. 2. d) bb) (2).

[587] Siehe Kapitel 4 C. III. 2. b) bb) und Kapitel 4 C. III. 2. d) bb) (2).

b) Informationspflichten im Nachhinein einer Profilbildung

Im Nachgang einer Profilbildung ist nach Art. 15 DSGVO insbesondere darüber zu informieren, dass und welche Daten in das Profil eingeflossen sind.[588] Erkennt man darüber hinaus an, dass Art. 15 Abs. 1 lit. h) DSGVO sich auch (annexhaft) auf die Profilbildung erstreckt, stellen sich hinsichtlich nachträglicher Informationspflichten zwei Fragen: erstens, in welchem Umfang im Nachhinein das Profilbildungsverfahren aufzudecken ist (aa)), zweitens, ob über die einzelnen Profilinhalte zu informieren ist (bb)).

aa) Informationspflichten hinsichtlich des Profilbildungsverfahrens

Dass auch im Nachgang Auskunft über eine erfolgte Profilbildung erteilt werden muss, wird teilweise befürwortet.[589] Nur soweit man das inhaltliche Informationsprogramm von Art. 13 Abs. 2 lit. f) und Art. 15 Abs. 1 lit. h) DSGVO nicht für identisch hält, ergeben sich überhaupt Fragen zu nachträglichen Informationspflichten. In diesem Fall ist in Art. 15 Abs. 1 lit. h) DSGVO über das spezifische Profilbildungsverfahren zu informieren, während im Vorhinein nur Darlegungen der allgemein-abstrakten Funktionslogik eines Profilbildungssystems erfolgen müssen.[590] Vor allem beim Kredit-Scoring[591] sind der-

---

[588] Vgl. eingehend zu den Inhalten der nachträglichen Informationspflicht *Lorentz*, Profiling, 2019, S. 246 f.

[589] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 27. Nicht ganz klar *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 18. AA *Lorentz*, Profiling, 2019, S. 247.

[590] Vgl. zu dieser grundlegenden Unterscheidung vorheriger und nachträglicher Informationspflichten *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 78 f. Explizit zwischen Informationspflichten im Vor- und im Nachhinein unterscheiden Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 15; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17, dort im Hinblick auf das Kredit-Scoring. Sie verweisen darauf, dass nur im Nachhinein über die konkrete Scoreformel unterrichtet werden kann, da diese vorab noch gar nicht vorliegt.

[591] Problematisch ist dabei, dass dort Profilbildung und Profilverwendung zusammenfallen: Im Kredit-Score ist sowohl eine Profilbildung enthalten, da die betroffene Person Vergleichsgruppen zugeordnet wird, als auch schon die Profilverwendung, da diese Zuordnung zugleich mit der Bewertung der Zahlungsfähigkeit und -bereitschaft und also der Kreditwürdigkeit verknüpft ist. Das Modell enthält hier also Anteile der Profilbildung als auch der automatisierten Entscheidung. Es wird nicht klar differenziert, ob die Offenlegungspflichten dann Fragen der Profilbildung oder der automatisierten Entscheidung betreffen. Zur Einordnung des Scoring-Verfahrens als Profilbildungsverfahren siehe Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10. Vgl. auch *Lorentz*, Profiling, 2019, S. 240 f.

artige Informationspflichten diskutiert worden.[592] Einen Anhaltspunkt bietet die Entscheidung des BGH aus dem Jahr 2014 zum Kredit-Scoring, die allerdings vor Inkrafttreten der DSGVO, dann zu § 34 Abs. 2 BDSG aF erging.[593] In der Entscheidung hat der BGH festgestellt, dass die Scoreformel – dies entspricht dem Modell im Rahmen dieser Arbeit –, vor allem darin enthaltende Vergleichsgruppen, sowie der individuelle Scorewert – dies entspricht dem Profil im Rahmen dieser Arbeit – nicht offengelegt werden müssen und begründet dies mit den schutzwürdigen Interessen der Kreditinstitute.[594] Der BGH fordert allein, dass die basale Methodik der Bildung des individuellen Scorewerts (also: des Profils) zu erläutern ist.[595] In der Literatur wird dieses Informationsprogramm vielfach als zu eng, die Entscheidung des BGH daher als unvereinbar mit der DSGVO erachtet.[596] Gefordert wird dort, dass zumindest über die maßgeblichen Faktoren – d.h. wesentlichen Vergleichsgruppen und deren Zuordnungskriterien – und deren grundlegende Gewichtung der Scoreformel (also: des Modells) zu unterrichten ist, die den individuellen Scorewert (also: das Profil) tragen.[597] Von derartigen Offenlegungspflichten geht auch der Berliner Datenschutzbeauftragte aus.[598] Demgegenüber fordert der Generalanwalt beim EuGH Pikamäe beim Kredit-Scoring hinreichend detaillierte Erläuterungen der Berechnungsmethode des Scorewerts und der Gründe für ein bestimmtes Ergebnis, sofern dabei keine schutzwürdigen widerstreitenden Interessen bestehen. Der notwendige Ausgleich der konfligierenden Interessen könnte ihm zu folge durch Verwendung geeigneter Kommu-

---

[592] Das LVwG Wien hat in diesem Zusammenhang am 23.03.2022 ein Vorabentscheidungsverfahren eingeleitet, EuGH, Vorabentscheidungsverfahren v. 23.03.2022, Rs. C-203/22, anhängiges Verfahren – *Dun & Bradstreet Austria*, das jedoch zum Zeitpunkt des Abschlusses der vorliegenden Arbeit noch nicht entschieden ist. Siehe hierzu auch Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 78.3.

[593] BGH, Urteil v. 28.01.2014, Rs. VI ZR 156/13, = BGHZ 200, 38 – *Scoring*.

[594] BGH, Urteil v. 28.01.2014, Rs. VI ZR 156/13, = BGHZ 200, 38, Rn. 26–32 – *Scoring*.

[595] BGH, Urteil v. 28.01.2014, Rs. VI ZR 156/13, = BGHZ 200, 38, Rn. 29 – *Scoring*.

[596] So etwa Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 78.3; *Lorentz*, Profiling, 2019, S. 241; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54. Kritisch auch Gola, DS-GVO/*Franck*, Art. 13 Rn. 31. AA Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28a.

[597] So *Hoffmann*, Profilbildung unter der DSGVO, 2020, S. 153; Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10; *Schönmann*, in: Schläger/Thode (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, [2]2022, S. 369, 340. Ebenso *Lorentz*, Profiling, 2019, S. 241; *Martini*, Blackbox Algorithmus, 2019, S. 190. Ähnlich Ehmann/Selmayr, DS-GVO/*Ehmann*, Art. 15 Rn. 19 „das Prinzip […], auf dem die Rechnung basiert"; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54 „Grundzüge seines Verarbeitungsverfahrens".

[598] Er verhängte entsprechend einen Bußgeldbescheid gegen eine nationale Bank, die der betroffenen Person keine entsprechenden Informationen über das Kredit-Scoringverfahren zur Verfügung stellte, siehe *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Computer sagt Nein Kreditkartenantrags, 31.5.2023.

nikationsmittel erreicht werden.[599] Eine umfassende Aufdeckung der Scoreformel wird dagegen überwiegend abgelehnt.[600] Eine Stellungnahme des EuGH in der Sache steht noch aus. Wenn man von einer Kongruenz der Informationspflichten von Art. 15 Abs. 1 lit. h) und Art. 13 Abs. 2 lit. f) DSGVO ausgeht, lassen sich diese Erwägungen auf die Informationspflichten ex ante übertragen.

bb) Informationspflichten hinsichtlich der Profilinhalte

Ob die betroffene Person ein Recht hat, die Einzelinhalte des über sie erstellten Profils einzusehen, wird sehr kontrovers diskutiert. Die Artikel 29 Datenschutzgruppe tritt für eine umfassende Offenlegung der Profilinhalte – dies dann auch im Nachhinein – ein.[601] Diesem Ansatz schließen sich Stimmen in der Literatur an.[602] Teilweise wird dies auf Art. 15 Abs. 1 lit. h) DSGVO gestützt,[603] andernorts Art. 15 Abs. 1 HS. 1 DSGVO herangezogen mit dem Hinweis, dass die neu generierten Daten ihrerseits personenbezogene Daten darstellten.[604] Andere lehnen dies mit Verweis auf den Wortlaut der Art. 15 Abs. 1 lit. h) DSGVO[605] bzw. Art. 15 Abs. 1 HS. 1 DSGVO[606] und auf kollidierende

---

[599] Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 54–58 – *SCHUFA Holding*.

[600] Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28a; Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10; Ehmann/Selmayr, DS-GVO/*Ehmann*, Art. 15 Rn. 19. So auch Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 57 – *SCHUFA Holding*. AA Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17, der eine Offenlegung der Scoreformel fordert, wenn sich andernfalls Fehler nicht aufdecken oder vermeiden lassen. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 78.3.

[601] *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 47. Ebenso *Norwegian Data Protection Authority*, Big Data, September 2013, S. 51.

[602] Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 27; Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10. Vor allem in Rahmen des Kredit-Scorings wird gefordert, dass die betroffene Person Einblick in ihren individuellen Scorewert erhalten soll. So etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; ebenso Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 78.3 „in bestimmten Fällen".

[603] So etwa Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 9a, 27; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17.

[604] Werden diese weiterverarbeitet – was bei autonomen Systemen stets der Fall ist – kann die betroffene Person nach Art. 15 Abs. 1 HS. 1 DSGVO Auskunft über diese Daten verlangen. So etwa *Wachter/Mittelstadt*, CBLR 2019, 494, 545 f.; *Lorentz*, Profiling, 2019, S. 249.

[605] Dieser spricht nur von involvierter Logik, nicht von einer Offenlegung von Profilingergebnissen, so *Martini*, Blackbox Algorithmus, 2019, S. 201 f.

[606] Die Vorschrift des Art. 15 Abs. 1 HS. 1 DSGVO meint nur eine Bestätigung im Sinne einer Positiv- bzw. Negativauskunft, nicht aber eine Offenlegung, so Gola, DS-GVO/*Franck*, Art. 15 Rn. 5.

unternehmerische Interessen ab.[607] Auch der BGH vertrat in seiner Entscheidung zum Kredit-Scoring die Auffassung, dass die Vergleichsgruppen in der Scoreformel und damit die konkreten Zuordnungen zu den Vergleichsgruppen im individuellen Scorewert nicht offenzulegen sind.[608] Nach dieser Ansicht ist dann nur im Rahmen der Informationen über die automatisierte Entscheidung über wesentliche Profilinhalte zu unterrichten, also über solche, die die automatisierte Entscheidung maßgeblich tragen.[609]

c) Aufbereitung der Informationen

Art. 12 DSGVO verlangt vom Verantwortlichen eine präzise, zugleich laienmäßig verständliche Aufbereitung der Informationen. Das jeweils geforderte Informationsangebot – Offenlegung der Algorithmen, Darlegung der grundlegenden Funktionsweise der Profilbildung, Darstellung der maßgeblichen Vergleichsgruppen und ihrer Parameter, Aufdeckung der Profilinhalte – ist demnach so darzustellen, dass dieses umfassend und präzise, vor allem aber für den Laien verständlich dargestellt wird. Dies kann – und in der Regel: wird – zusätzliche Erläuterungen notwendig machen.[610] Die technisch anspruchsvollen Informationsangebote können zudem für den Laien herausfordernd sein und abschreckend wirken.[611]

d) Grenzen der Informationspflichten: Unverhältnismäßigkeit und Unmöglichkeit der Information

Die Informationspflichten hinsichtlich des Profilbildungsverfahrens können mit einem unverhältnismäßigen Aufwand des Verantwortlichen einhergehen (aa)), sowie aufgrund fehlender menschlicher Verständlichkeit an Grenzen stoßen (bb)).

---

[607] So auch *Martini*, Blackbox Algorithmus, 2019, S. 200. Hinsichtlich der Scorecard beim Kredit-Scoring Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28a. Siehe auch Paal/Pauly, DS-GVO/*Paal*, Art. 15 Rn. 31b.

[608] BGH, Urteil v. 28.01.2014, Rs. VI ZR 156/13, = BGHZ 200, 38 – *Scoring*. Siehe hierzu genauer unter Kapitel 4 C. 2. b) aa).

[609] Vgl. Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31b; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 12, die dies ganz grundsätzlich für das Informationsprogramm hinsichtlich automatisierter Entscheidungen feststellen und nicht zwischen profilbasierten und nicht-profilbasierten Entscheidungsparametern unterscheiden. Daraus lässt sich ablesen, dass allein über solche Profilinhalte aufzuklären ist, die die Entscheidung maßgeblich tragen.

[610] Gola, DS-GVO/*Franck*, Art. 13 Rn. 29 „um erklärende Bestandteile angereichert".

[611] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12. Siehe bereits oben Kapitel 4 D. II. 1. a).

aa) Unverhältnismäßiger Aufwand der Informationsbeschaffung und -aufbereitung

Die Einzelheiten des teilweise hochkomplexen Verarbeitungsverfahrens sowie die Ergebnisse der Profilbildung in ihrem gesamten Umfang auszulesen, ist anspruchsvoll. Der zeitliche, personelle, soft- und hardwarebezogene Aufwand kann für den Verantwortlichen im Einzelfall sehr hoch ausfallen.[612] Ab einer bestimmten Komplexitätsstufe der algorithmischen Strukturen ist es dann nur noch theoretisch denkbar, dass ExpertInnen(gruppen) diese entschlüsseln: Allein der zeitliche Aufwand wäre so hoch, dass eine Entschlüsselung praktisch nicht denkbar ist.[613] Hinzu kommt, dass in der Praxis an der Entwicklung des Modells oder der Profilerstellung eine Vielzahl spezialisierter Unternehmen oder Organisationseinheiten beteiligt ist.[614] Um Einblicke in das Profilbildungsverfahren bzw. Profilinhalte gewähren zu können, müssten Verantwortliche zunächst das notwendige Wissen bei verschiedenen Stellen erfragen. Dies kann faktisch und rechtlich – hier sind Geschäfts- und Berufsgeheimnisse der beteiligten Einheiten relevant – an Grenzen führen. In einer Interessensabwägung zwischen Informationsinteresse der betroffenen Person und unternehmerischen Freiheiten der Verantwortlichen kann dies zu einer Unverhältnismäßigkeit des Transparenzgebots führen.

bb) Unüberwindliche Zielkonflikte bei hochkomplexen Verarbeitungen

Um das bereitzustellende Informationsmaterial im Rahmen der Profilbildung verstehen zu können, bedarf es ausführlicher Informationen, die dann die betroffene Person aber aufgrund ihres Umfangs nicht erreichen.[615] Das Gebot der

---

[612] Vgl. *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 845; *Paal*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, Rn. 11. Vgl. auch *Beck*, Künstliche Intelligenz und Diskriminierung, 2019, S. 98 f.

[613] Vgl. *Gausling*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 379, Rn. 43; *Paal*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, Rn. 8. Anders als bei Algorithmen aus subsymbolischen Lernverfahren – hierzu sogleich – betrifft dies Konstellationen symbolischer Lernverfahren, bei denen das Modell bzw. der Lösungsalgorithmus Klassifizierungen, Parameter und deren Verbindungen zueinander in menschlich verständlicher Form abbildet, die Verschachtelungen aber so komplex sind, dass sie das menschlich Fassbare bei Weitem übersteigen.

[614] Vgl. hierzu auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 71 f.; *Wischmeyer*, AöR 143 (2018), 1, 46. Von einem „komplexe[n] sozioinformatische[n] Ökosystem" spricht die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 169.

[615] Siehe zu all dem eingehend *Edwards/Veale*, SSRN Journal 2017, 59, 64; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 194. Siehe auch *Paal*, in: Kaulartz/Braegelmann (Hrsg.),

Präzision und der Verständlichkeit treten in einen Zielkonflikt, da die Informationsaufbereitung notwendig so umfassend ausfallen muss, dass sie das Maß der zumutbaren Informationsmasse übersteigt,[616] oder der Verantwortliche zu Reduktionen des Informationsmaterials gezwungen ist, was zu Verzerrungen und Unvollständigkeiten führen kann.[617] Für diesen Zielkonflikt sieht die DSGVO keine Lösung vor. Am Ende muss dann die Informationspflicht aufgrund Unmöglichkeit entfallen.

cc) Menschliche Kognitionsgrenzen und fehlende Nachvollziehbarkeit Maschineller Lernverfahren

Schließlich stellt der Transparenzgrundsatz aufgrund menschlicher Kognitionsgrenzen vor Herausforderungen.[618] Problematisch ist schon, wenn die Verfahren ohne fachliche Grundkenntnisse nicht nachvollzogen werden können (technische Illiteralität). Doch auch die Komplexität des Verfahrens kann an Grenzen stoßen: Die hohe Menge an Variablen, Parametern sowie deren anspruchsvolle stochastisch-mathematische Verbindungen und Verschachtelungen können das menschlich-kognitiv Fassbare überschreiten.[619]

Herausfordernd ist aber vor allem die fehlende Nachvollziehbarkeit von Algorithmen aus subsymbolischen Maschinellen Lernverfahren (Deep Learning).[620] Problematisch sind zum einen Verfahren, bei denen Vergleichsgruppen und Parameter datenbasiert-korrelativ gebildet werden, die sich menschlich-rationalen Konsistenzzusammenhängen entziehen.[621] Diese können zwar offengelegt, d.h. der Algorithmus in seinen Einzelteilen veröffentlicht werden, eine Einordnung in menschliche Konsistenzzusammenhänge ist dann aber nicht mehr möglich.[622] Die im Modell repräsentierten Gruppen und Zuordnungsfaktoren ergäben für die menschlichen NutzerInnen nach rational-logischen Konsistenzkriterien keinen Sinn. Zum anderen betrifft dies Fälle subsymbolischer Lernverfahren, bei denen das Modell sich als künstliches neuronales Netz, d.h. als komplexe algorithmische Struktur darstellt. Vergleichsgruppen oder Zuordnungsparameter gibt es hier gar nicht. In beiden Konstellationen kann das Profilbildungsverfahren nicht konkret beschrieben werden,

---

Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 427, Rn. 8; Gola, DS-GVO/*Franck*, Art. 12 Rn. 23.

[616] Vgl. *Martini*, Blackbox Algorithmus, 2019, S. 188; Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Buchholtz/Stentzel*, Art. 5 Rn. 27, 30.

[617] Ebenso kritisch im Hinblick auf Intelligente Systeme *Wischmeyer*, AöR 143 (2018), 1, 53.

[618] Siehe hierzu bereits Kapitel 2 A. II. 2. b).

[619] *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 860 f.

[620] Siehe hierzu bereits Kapitel 1 A. II. 2. c), Kapitel 2 A. II. 2. b).

[621] *Edwards/Veale*, SSRN Journal 2017, 59 f.: „[Some ML models] lack any convenient or clear human interpretation in the first place".

[622] *Dies.*, SSRN Journal 2017, 60.

dies weder im Vor- noch im Nachhinein.[623] Auch ist es ausgeschlossen, menschlich verständliche Profilinhalte aufzudecken: Sie enthielten keine nach menschlichen Verständniszusammenhängen sinnvolle Merkmale oder stellten sich als unverständliche Datenmatrixen als Ausgabe eines künstlichen neuronalen Netzes dar.

e) Ergebnis: Rechtlich unklare und technisch begrenzte Transparenzgebote für die Profilbildung

Im Rahmen des Profilbildungsverfahrens ist über die allgemeinen Umstände der Datenverarbeitung zu unterrichten. Im Rahmen der Einwilligung sind darüber hinaus Informationen zum zweistufigen Profilbildungsverfahren und zu wesentlichen Inhalten des Profils bereitzustellen. Ob dann aber auch über das Stattfinden der Profilbildung, das Profilbildungsverfahren und die Profilinhalte als neu generierte Daten zu informieren ist, wird unterschiedlich gesehen. Das besondere Informationspflichtenprogramm nach Art. 13 Abs. 2 lit. f) und Art. 15 Abs. 1 lit. h) DSGVO gilt nur, wenn man diese Vorschriften auch isoliert auf die Profilbildung anwenden will. Dies wird in der Literatur überwiegend abgelehnt. Soweit man dies befürwortet, ist unklar, ob auf das Stattfinden der Profilbildung hinzuweisen ist, im Übrigen, wie detailgenau über das Verfahren sowie die Profilinhalte zu informieren ist. Während die einen sowohl im Vor- als auch im Nachhinein eine Aufdeckung des Modells verlangen, fordern andere nur eine Darlegung der wesentlichen Vergleichsgruppen, Zuordnungskriterien und Gewichtungen. Wiederum andere differenzieren nach Informationspflichten im Vor- und im Nachhinein: Während im Vorhinein nur die Systemfunktionalität des Modells zu erläutern ist, muss im Nachhinein das konkret verwendete Modell in seinen Grundzügen dargestellt werden. Kontrovers wird schließlich diskutiert, ob betroffene Personen im Nachhinein ein Recht auf Einsicht in ihr Profil haben. Insbesondere die Artikel 29 Datenschutzgruppe befürwortet dies, während der BGH wie auch Stimmen in der Literatur ein solches Einblicksrecht ablehnen.

Die Informationspflichten kommen an Grenzen, soweit deren Erfüllung wirtschaftlich unverhältnismäßig oder aufgrund menschlicher Kognitionsgrenzen unmöglich ist. Vor allem die fehlende menschliche Nachvollziehbarkeit von Algorithmen aus Maschinellen Lernverfahren ist hierbei problematisch. Wie mit derartigen Konstellationen umzugehen ist, ist unklar.

---

[623] Ohne Spezifizierung der Gründe der fehlenden Nachvollziehbarkeit allgemein zu Algorithmen des Maschinellen Lernens, nicht spezifisch zu Profilbildungsmaßnahmen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12; Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31e.

3. Profilverwendungsverfahren: Transparenz bei selbstlernenden Algorithmen und automatisierten Entscheidungen

Für die Profilverwendung unterscheiden sich die Informationspflichten, je nachdem, ob es sich um eine automatisierte Entscheidung nach Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h), Art. 22 DSGVO handelt oder nicht. Ist dies nicht der Fall, bestehen besondere Informationspflichten allein aufgrund des Rechtmäßigkeitsgrundsatzes (a)). Soweit es sich um eine automatisierte Entscheidung handelt, bestehen besondere Informationspflichten im Vorhinein (b)) sowie im Nachhinein (c)). Dabei stellt sich besonders die Frage, inwieweit im Rahmen der Informationen über die automatisierte Entscheidung auch Erläuterungen hinsichtlich des Profilingverfahrens und seiner Ergebnisse zu erfolgen haben (d)). Die Informationen sind laiengerecht verständlich aufzubereiten (e)). Bei autonomen Systemen stößt man mit diesem Informationspflichtenprogramm allerdings an Grenzen (f)).

a) Informationspflichten bei der Profilverwendung

Für sämtliche Profilverwendungen gelten die generellen Informationspflichten der Art. 13, 15 DSGVO. Insbesondere ist dann über den Zweck, hier also die Verwendung des Profils für eine bestimmte Anwendung, etwa eine personalisierte Preisbildung oder eine personalisierte Werbemaßnahme, aufzuklären.

Hinsichtlich der Datenverarbeitungen im Rahmen der Profilverwendung jenseits automatisierter Entscheidungen sind im Rahmen der Rechtmäßigkeit, genauer der Einwilligung, basale Informationen zum technischen Verfahren bereitzustellen. Zu informieren ist darüber, dass das Profil in einen Lösungsalgorithmus Eingang findet und dann eine automatisierte Entscheidung auslöst.[624] Über die involvierte Logik der Verarbeitung ist dagegen nicht zu unterrichten.[625] Darüber hinaus ist über die Folgen der Profilverwendung aufzuklären, soweit diese der betroffenen Person nicht ohne weiteres erkenntlich sind.[626] Umstritten ist, ob darüber hinaus über die zuvor gebildeten Profilinhalte im Detail informiert werden muss. Vereinzelt wird dies befürwortet, insbesondere vom Europäischen Datenschutzausschuss, während der überwiegende Teil der Literatur die Informationen im Rahmen der Profilbildung für ausreichend erachtet.[627]

---

[624] Siehe oben Kapitel 4 C. III. 3. a) bb) (1) zur Einwilligung sowie Kapitel 4 C. 3. c) dd) (4) zur Interessensabwägung.

[625] Siehe oben Kapitel 4 C. III. 3. a) bb) (1).

[626] Siehe oben Kapitel 4 C. III. 3. a) bb) (1).

[627] Siehe hierzu Kapitel 4 C. III. 3. a) bb) (3).

b) Informationspflichten im Vorhinein der automatisierten Entscheidung

Transparenzgebote hinsichtlich der Profilverwendung, die eine automatisierte Entscheidung darstellen, lassen sich auf die Informationspflichten stützen (aa)) sowie auf die Ausnahmezulassung (bb)).

aa) Informationspflichten nach Art. 13 DSGVO

In welchen Fällen die besondere Informationspflicht des Art. 13 Abs. 2 lit. f) DSGVO greift, hängt davon ab, wie eng man die Vorschrift versteht: Wie ausgeführt[628] gibt es hier Ansichten, die automatisierte Entscheidungen nur dann den besonderen Informationspflichten unterwerfen wollen, wenn sie auf eine Profilingmaßnahme gestützt sind.[629] Bei autonomen Systemen ist dies stets der Fall. Offen ist darüber hinaus, ob auch teilautomatisierte Entscheidungen der Vorschrift unterfallen sollen sowie solche, von denen keine rechtlichen Wirkungen oder erheblichen faktischen Beeinträchtigungswirkungen ausgehen.[630] Dies ist bei autonomen Systemen durchaus denkbar.[631] Den besonderen Informationspflichten unterfallen jedenfalls nicht sonstige Profilverwendungen, insbesondere automatisierte Steuerungen wie Informationsfilterdienste oder personalisierte Werbemaßnahmen.

Soweit Art. 13 Abs. 2 lit. f) DSGVO zur Anwendung kommt ist sehr unklar, was genau mit „aussagekräftige(n) Informationen über die involvierte Logik" gemeint ist. Im Grundsatz stehen sich zwei Ansichten gegenüber: Solche, die eine Algorithmentransparenz fordern ((1)) und solche die nur basale Informationen über diesen Algorithmus fordern ((2)).

(1) Offenlegung der verwendeten Algorithmen

Nur sehr vereinzelt werden die Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO so verstanden, dass der Quellcode einer automatisierten Entscheidung umfassend aufgedeckt werden muss.[632] Nach dieser Ansicht müsste also der

---

[628] Siehe oben Kapitel 4 D II. 3. a) aa).

[629] Siehe oben Kapitel 4 D. II. 3. a) aa) (1).

[630] Siehe oben Kapitel 4 D. II. 3. a) aa) (3).

[631] Die Frage stellt sich nicht nur bei teilautomatisierten Entscheidungssystemen, sondern auch bei vollautomatisierten Systemen, bei denen es jedoch an Merkmal rechtlicher Folgen oder erheblicher Beeinträchtigungswirkung fehlt, so etwa bei der personalisierten Werbung. Siehe eingehend Kapitel 4 B. III. 3. b) dd).

[632] *Iphofen/Kritikos*, Contemporary Social Science 2019, 1, 6. In diese Richtung auch Gola, DS-GVO/*Franck*, Art. 13 Rn. 29: „Darstellung von Algorithmen (angereichert) um erklärende Bestandteile". Sehr weit auch *Norwegian Data Protection Authority*, Big Data, September 2013, S. 52 „[A]ccess should also be granted to the decision-making criteria (algorithms)".

Lösungsalgorithmus aufgedeckt werden. Die Mehrheit in der Literatur[633] ebenso wie der Europäische Datenschutzausschuss folgt dem nicht.[634] Schon der Wortlaut lege dies nicht nahe,[635] auch sei dies mit Blick auf schutzwürdige unternehmerische Interessen der Verantwortlichen nicht zu rechtfertigen.[636] Hingewiesen wird auch darauf, dass der technische Laie mit dem Quellcode ohnehin nichts anfangen könnte.[637]

(2) Offenlegung der grundlegenden Funktionsweise

Der Europäische Datenschutzausschuss verlangt die Information über „zugrunde liegende[.] Überlegungen bzw. Kriterien", sodass „die betroffene Person die Gründe der Entscheidung nachvollziehen kann".[638] Dies entspricht der vorherrschenden Auffassung in der Literatur, wonach nur die grundlegende technische Funktionsweise der automatisierten Entscheidung darzulegen ist und zwar in einer für die betroffene Person verständlichen Weise.[639] Diese Auf-

---

[633] Siehe nur Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 32b; Gola, DS-GVO/*Franck*, Art. 13 Rn. 29; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28a; *Martini*, Blackbox Algorithmus, 2019, S. 181. Ebenso *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 90; *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 872; *Strassemeyer*, K&R 16 (2016), 176, 179.

[634] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 28: „Die DSGVO verpflichtet den Verantwortlichen […] nicht unbedingt […] zur Offenlegung des gesamten Algorithmus".

[635] Dieser spricht eben nur von „involvierter Logik", zusätzlich einschränkend von „aussagekräftige[n] Informationen". Siehe zu diesem Argument *Lewinski/Pohl*, ZD 9 (2018), 17, 22; *Hoeren/Niehoff*, RW 9 (2018), 47, 56. Auch Erwägungsgrund 63 S. 3 – hier allerdings ist die französische Sprachfassung deutlicher – differenziert zwischen der Logik, die nicht offenzulegen ist, und deren Grundlage, über die informiert werden muss („la logique qui sous-tend leur eventuel traitement automatisé"). Vgl. hierzu *Hoeren/Niehoff*, RW 9 (2018), 47, 56.

[636] Insbesondere deren Unternehmens- und Berufsfreiheit sowie deren Eigentumsfreiheit ist betroffen, eingehend *Martini*, Blackbox Algorithmus, 2019, S. 182; *Hoffmann-Riem*, in: ders. (Hrsg.), Big Data, 2018, S. 11, 59; *Wischmeyer*, AöR 143 (2018), 1, 51 f.; *Strassemeyer*, K&R 16 (2016), 176, 179. Auch Privatheits- oder Datenschutzinteressen Dritter können betroffen sein, deren Daten notwendig mitaufgedeckt werden, hierauf weist *Wischmeyer*, AöR 143 (2018), 1, 52 hin.

[637] *Edwards/Veale*, SSRN Journal 2017, 67; *Wischmeyer*, AöR 143 (2018), 1, 53; *Martini*, Blackbox Algorithmus, 2019, S. 181. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 54.

[638] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 28.

[639] Siehe nur Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54; Plath, DSGVO/BDSG/*Kamlah*, Art. 13 Rn. 28a; *Martini/Nink*, NVwZ 36 (2017), 1, 10 f.; *Hoeren /Niehoff*, RW 9 (2018), 47, 65 f.; *Kaminski*, BTLJ 34 (2019), 189, 213 f.; *Strassemeyer*, K&R

fassung teilt auch der Generalanwalt beim EuGH.[640] Zu nennen sind die basale Methodik des technischen Verfahrens und die entscheidungserheblichen Faktoren, d.h. wesentliche Klassifizierungen und Parameter, sowie deren Gewicht und Bedeutung für die anschließende Entscheidung.[641] Auch über die der Entscheidung zugrundeliegenden Daten ist – zumindest überblicksartig – aufzuklären.[642] Entscheidend soll zudem der Transparenzbedarf im Einzelfall sein: Je mehr die betroffene Person der Kenntnisse hinsichtlich der Algorithmenlogik bedarf, um die algorithmische Entscheidung verstehen, diese prüfen und Fehler erkennen zu können, desto detailgenauer müssen auch die Informationen zu den verwendeten Algorithmen ausfallen.[643] Vielfach wird auch auf eine Einzelfallprüfung abgestellt. Der Detailgrad der Informationspflichten soll sich anhand eines Ausgleichs von Transparenzbedarf der betroffenen Person und Geheimhaltungsinteressen des Verantwortlichen bestimmten.[644] Nach diesem Verständnis müsste dargelegt werden, welche maßgeblichen Profilinhalte (zB Interessen, Vorlieben, wirtschaftliche Leistungsfähigkeit) bzw. anderen Aspekte (zB umweltbezogene Informationen wie Wetter, Tageszeit oder Zu-

16 (2016), 176, 179 f.; *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 864–866. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 181 „Informationen über die Entscheidungsmechanismen" (Hervorhebung im Original). Gerade zum zweiten Aspekt Gola, DS-GVO/*Franck*, Art. 13 Rn. 29 „um erklärende Bestandteile angereichert".

[640] Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, 54, 58 – *SCHUFA Holding*: „Generell sollte der Verantwortliche der betroffenen Person allgemeine Informationen übermitteln, vor allem zu bei der Entscheidungsfindung berücksichtigten Faktoren und deren Gewichtung auf aggregierter Ebene".

[641] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54: „Methoden und Kriterien der Datenverarbeitung"; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16–17: „Aufbau, [...] Struktur und [...] Ablauf der Datenverarbeitung"; konkret für das Scoring: „Informationen darüber, welche erhobenen Daten [...] mit welcher Gewichtung in die Berechnung des Wahrscheinlichkeitswerts (Scoringwerts) einfließen und wie sich die Scoringwerte gegenseitig beeinflussen"; Paal/Pauly. DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31c: „Grundannahmen der Algorithmus-Logik. [...] [Hierzu zählen] die Datenbasis (im Überblick), der Einsatz best. Faktoren bzw. Parameter sowie die Grundstruktur des dem Algorithmus inhärenten Entscheidungsprozesses"; *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 25: „Beschreibung der Datenverarbeitung, [...] Darlegung der Funktionsweise der Bewertung auf Grundlage der Datenverarbeitung und der dafür verwandten Konzepte und Berechnungsmodelle".

[642] Paal/Pauly DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31c. Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 198.

[643] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 78.3; *Sesing*, MMR 24 (2021), 288, 291.

[644] *Sesing*, MMR 24 (2021), 288, 291. In diese Richtung auch Gola, DS-GVO/*Franck*, Art. 15 Rn. 18. Unter Heranziehung der Öffnungsklausel des Art. 23 DSGVO Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54.

gangsort) auf welche Weise (zB vorrangig, gleichmäßig, untergeordnet) in die Entscheidung einfließen; je risikoreicher eine Anwendung, desto umfassender müssten diese Informationen ausfallen.

bb) Informationspflichten aufgrund der Ausnahmezulassung nach Art. 22 Abs. 2 DSGVO

Ist die Profilverwendung eine automatisierte Entscheidung, fordert die ausnahmsweise Zulassung nach Art. 22 Abs. 2 DSGVO eigenständige Informationsangebote. Teilweise wird hier das nämliche Informationsprogramm wie für sonstige Profilverwendungen gefordert, andernorts dasjenige des Art. 13 Abs. 2 lit. f) DSGVO, teilweise auch nur mit beschränktem Inhalt, herangezogen.[645]

c) Informationspflichten im Nachhinein der automatisierten Entscheidung

Erkennt man an, dass das Informationsprogramm des Art. 15 DSGVO über Art. 13 DSGVO hinausreicht,[646] kommt man zu einem spezifischen Informationsprogramm ex post. Die Informationspflicht erstreckt sich dann auf die konkret getroffene Entscheidung, eine Beschreibung der allgemeinen Systemfunktionalität genügt nicht. Dies kann im Einzelnen über die bereits erfolgten Offenlegungen hinausgehen. Wer die Aufdeckung des Quellcodes verlangt, müsste dann also den konkret verwendeten Lösungsalgorithmus und die tatsächlich durchgeführten einzelnen Berechnungsschritte offenlegen. Verlangt man dagegen allein eine Erläuterung der grundlegenden Funktionsweise, ist anzugeben, welche spezifischen Parameter die Entscheidung in welchem Umfang geprägt haben.[647] Bei einem Kredit-Scoring müsste also dargelegt werden, dass die Faktoren Alter, Vermögenslage und Wohnort eingeflossen sind und dabei auf die Vermögenslage das meiste Gewicht gelegt wurde.

d) Annexhafte Informationspflichten hinsichtlich der Profilbildung und der Profilinhalte

Überwiegend wird ein Bestehen profilingbezogener Informationspflichten allein im Rahmen der automatisierten Entscheidung anerkannt. Dann aber ist unklar, wie weit die profilingbezogenen Informationen reichen, wie umfassend also auf Stufe der Profilverwendung über Aspekte der Profilbildung und der Profilinhalte zu unterrichten ist. Vielfach wird in der Literatur das oben beschriebene Programm für die Profilbildung umfassend in das Informationspro-

---

[645] Siehe oben Kapitel 4 C. III. 3. a) bb) (2), Kapitel 4 C. III. 3. b).

[646] Zu dieser Frage siehe oben unter Kapitel 4 D. II. 3. a) cc).

[647] Vgl., insbesondere anhand des Beispiels des Kredit-Scorings, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10.

gramm der automatisierten Entscheidung integriert.[648] Die Pflicht zur Bereitstellung aussagekräftiger Informationen zur involvierten Logik beziehen sich dann also auch auf das Profilbildungsverfahren. Diesem Verständnis folgt auch der Europäische Datenschutzausschuss.[649] Folgt man dem, sind also im Rahmen der Informationen über die Profilverwendung zugleich Informationen über die Profilbildung bereitzustellen. In einer strenge(re)n Lesart muss nur dann über das Profilingverfahren informiert werden, wenn es in das Profilverwendungsverfahren integriert ist, Profilbildung- und verwendungsverfahren also zusammenfallen. Dies betrifft den Fall des Kredit-Scorings. Hier lässt sich beobachten, dass Informationspflichten zur Profilbildung als solche der Transparenz automatisierter Entscheidung (und nicht des Profilings) diskutiert werden.[650] Teilweise wird keine Offenlegung des Profilbildungsverfahrens, sondern allein eine Offenlegung von Profilinhalten gefordert, wenn diese zugleich Teil des Quellcodes sind oder wesentliche Parameter der algorithmischen Entscheidungsarchitektur darstellen.[651]

Ob Profilinhalte, sobald diese vorliegen, umfassend aufzudecken sind, wird auch und vorwiegend im Rahmen der Transparenzpflichten zu automatisierten Entscheidungen diskutiert.[652] Da dabei die Profilinhalte verarbeitet werden, greift nach Ansicht mancher das Recht auf Datenauskunft nach Art. 15 Abs. 1 HS. 1 DSGVO.[653] Im Übrigen wird die Pflicht zur Offenlegung der Profilinhalte als Teil nachträglicher Auskunftspflichten der automatisierten Entscheidung diskutiert, dann also gestützt auf Art. 15 Abs. 1 lit. h) DSGVO, soweit die Profilinhalte die automatisierte Entscheidung stützten.[654] Welche Ansätze

---

[648] So etwa Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53 f. sowie Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17–18. Explizit eine Darlegung der involvierten Logik hinsichtlich des Profilings fordern Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 13 Rn. 58.

[649] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 27: „Funktionsweise einer automatisierten Entscheidungsfindung oder Profiling".

[650] Siehe etwa Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10; Ehmann/Selmayr, DS-GVO/*Ehmann*, Art. 15 Rn. 19; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 15 Rn. 78.3.

[651] In der Literatur äußert sich dies darin, dass auf profilingbezogene Informationspflichten gar nicht erst eingegangen wird, sondern auch, soweit das Profiling in der automatisierten Entscheidung aufgeht, allein auf die involvierte Logik der automatisierten Entscheidung insgesamt abgestellt wird. So etwa Gola, DS-GVO/*Franck*, Art. 13 Rn. 30; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 4 Nr. 4 Rn. 12; Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31a.

[652] Siehe hierzu bereits oben Kapitel 4 D. III. 2. b) bb).

[653] *Lorentz*, Profiling, 2019, S. 249; *Wachter/Mittelstadt*, CBLR 2019, 494, 545 f.

[654] So etwa Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 15 Rn. 27; Sydow, DS-GVO/*Specht*, Art. 15 Rn. 10.

zwischen umfassender Offenlegungspflicht und Versagung jeglichen Einblicks dabei vertreten werden, ist bereits oben ausgeführt worden.

e) Aufbereitung der Informationen

Wie auch bei der Profilbildung müssen die Informationsangebote auf die betroffenen Personen, d.h. technische Laien, ausgerichtet sowie leicht erkennbar und umfassend sein. Die notwendigen Informationen, die der betroffenen Person im Vor- und Nachhinein ein Verständnis der automatisierten Entscheidung und der Profilbildung ermöglichen, sind komplex und verlangen vom Verantwortlichen eine laiengerechte Aufbereitung. Die Umschreibung der technischen Verfahren wird umso umfassender und für den Verantwortlichen anspruchsvoller und ressourcenbindender ausfallen, je diffiziler sich diese darstellen.

f) Grenzen der Informationspflichten: Unverhältnismäßigkeit und Unmöglichkeit

Die wirtschaftlichen und faktischen Grenzen der Informationspflichten, wie sie bereits im Rahmen der Profilbildung erläutert wurden, gelten auch für die Profilverwendung. Hier ist es dann der Lösungsalgorithmus, der aufgrund seiner Komplexität die Offenlegung bzw. Erläuterung für den Verantwortlichen unverhältnismäßig macht oder einer laiengerechten, zugleich präzise Erläuterung faktisch entgegensteht.[655] Schließlich sind auch menschliche Kognitionsgrenzen problematisch, wenn die Anzahl der Entscheidungsparameter und die einzelnen Rechenschritte im Lösungsalgorithmus das menschliche Erkenntnisvermögen übersteigen. Kommen für die Bildung des Lösungsalgorithmus Maschinelle Lernverfahren zum Einsatz, setzt auch die fehlende menschliche Nachvollziehbarkeit faktische Grenzen.[656] Anders als im Rahmen der Informiertheit aufgrund des Rechtmäßigkeitsgrundsatzes stellt dies im Rahmen der Informationspflichten nach Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h DSGVO vor Probleme:[657] Zwar mögen erwünschte Outputs vorhersehbar bleiben, der konkrete algorithmische Entscheidungsweg bzw. einzelne Entscheidungskriterien und deren Gewicht können dem Laien aber nicht verständlich vermittelt werden.

---

[655] Siehe etwa zur Problematik der Inakkuratesse der laiengerecht aufbereiteten, dann notwendig simplifizierten Informationen, Gola, DS-GVO/*Franck*, Art. 12 Rn. 23; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12.

[656] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25.

[657] Siehe zu den Informationspflichten im Rahmen des Rechtmäßigkeitsgrundsatzes bei der Profilverwendung oben Kapitel 4 C. III. 3. a) bb) (2) hinsichtlich der Einwilligung und Kapitel 4 C. III. 3. d) (5) hinsichtlich der Interessensabwägung. Hinsichtlich automatisierter Entscheidungen siehe Kapitel 4 C. III. 3. b).

g) Ergebnis: Beschränkte Informationspflichten hinsichtlich automatisierter Entscheidungen

Informationspflichten zur technischen Funktionsweise sämtlicher Profilverwendungen bestehen nur im Rahmen der Zweckbestimmung sowie der Informationspflichten des Rechtmäßigkeitsgrundsatzes, insbesondere der Einwilligung. Im Nachhinein bestehen keinerlei Informationsansprüche. Vertieftere Einblicke in das technische Verfahren sind nur für automatisierte Entscheidungen vorgesehen. Hier ist im Einzelnen aber vieles umstritten. Schon der Anwendungsbereich der Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO sorgt für Rechtsunsicherheit. Offen ist, ob diese Informationspflichten nur für profilgestützte oder auch für sämtliche, dann auch teilautomatisierte Entscheidungen oder solche ohne rechtlich bzw. faktische Beeinträchtigungswirkung gelten. Soweit die Informationspflichten greifen, ist deren konkreter Inhalt unklar. Während die einen eine umfassende Algorithmentransparenz, dann also eine Offenlegung des Lösungsalgorithmus fordern, verlangen andere nur eine Darlegung der grundlegenden Funktionsweise, dann also der wesentlichen Parameter der algorithmischen Entscheidung sowie deren Gewicht. Teilweise wird dafür eingetreten, das Informationsprogramm zeitlich zu differenzieren: Im Vorfeld ist dann nur die abstrakte Systemfunktion, im Nachhinein die konkrete algorithmische Entscheidungsfindung darzulegen. Soweit die automatisierte Entscheidung eine profilbasierte ist, wie dies bei autonomen Systemen der Fall ist, lassen die Vorschriften offen, inwieweit auch über das zugrundeliegende Profilbildungsverfahren zu informieren ist. Schließlich besteht keine Einigkeit darüber, ob die betroffene Person im Nachhinein einen Anspruch auf Einblick in sämtliche Profilinhalte hat. Wie schon bei der Profilbildung ergeben sich auch bei der Profilverwendung Grenzen dieser Informationspflichten aufgrund Unverhältnismäßigkeit und Unmöglichkeit, die einmal in der hohen Komplexität der Algorithmenstruktur, einmal in der fehlenden Nachvollziehbarkeit von Algorithmen aus Maschinellen Lernverfahren ihren Ursprung haben.

4. Ergebnis

Das datenschutzrechtsspezifische Transparenzprogramm erstreckt sich überwiegend nicht auf technische Details der Modell- und Profilbildung sowie die Profilverwendung. Nach den allgemeinen Vorschriften ist nur über äußere Umstände der Verarbeitung aufzuklären. Allein der Zweckbestimmungs- und Rechtmäßigkeitsgrundsatz verlangt gewisse abstrakte Darstellungen der technischen Funktionsweise. Vertieftere Einblicke sind allein für automatisierte Entscheidungen einschließlich Profiling vorgesehen.

Die DSGVO verschafft daher keine Einblicksrechte in das Modellbildungsverfahren und auch nicht in einzelne Modellinhalte. Technische Informationen zum Maschinellen Lernverfahren gibt es daher nicht.

Das Transparenzprogramm hinsichtlich der Profilbildung ist allein im Hinblick auf Zweckbestimmungs- und Rechtmäßigkeitsgrundsatz rechtssicher umrissen. Demnach ist vorab über die Profilbildung, das zweistufige Profilbildungsverfahren, Anwendungskontexte und erwartete Profilinhaltsgruppen zu unterrichten. Nur wenn man Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO auch allein auf die Profilbildung anwendet oder jedenfalls im Rahmen von Informationen über die automatisierte Entscheidung das diesbezügliche Informationsprogramm umfassend auch auf die Profilbildung erstreckt, ergeben sich weitere, vertieftere Informationspflichten. Es ist dann aber unklar, ob auf das Stattfinden der Profilbildung hinzuweisen ist. Vor allem aber wird sehr unterschiedlich gesehen, ob die Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO eine Aufdeckung des Algorithmus, d.h. des Modells, verlangen oder ob nur die grundlegende Methodik, dann also wesentliche Vergleichsgruppen, Zuordnungsparameter und Gewichtungen im Modell darzulegen ist. Unklar ist auch, ob zwischen vorherigen und nachträglichen Informationspflichten zu differenzieren ist, im Vorhinein also nur die Systemfunktionalität, im Nachhinein das konkret gewählte Modell Informationsgegenstand ist. Eine Aufdeckung der einzelnen Profilinhalte wird von der Artikel 29 Datenschutzgruppe sowie von einigen Teilen der Literatur gefordert, während andere nur eine Offenlegung der grundlegenden, die anschließende automatisierte Entscheidung tragenden Profilinhalte fordern.

Bei der Profilverwendung ist im Vorhinein aufgrund des Zweckbestimmungs- sowie des Rechtmäßigkeitsgrundsatzes über die Verwendung des Profils zum Auslösen einer automatisierten Anwendung zu informieren. Ob dann die besonderen Informationspflichten nach Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO nur bei profilbasierten oder sämtlichen automatisierten Entscheidungen gelten, ist offen, ebenso, ob die Vorschriften auch teilautomatisierte Entscheidungen und solche ohne rechtliche Wirkung oder faktische Beeinträchtigung erfassen. Die Informationen über die „involvierte Logik" begreifen die einen als Pflicht zur umfassenden Aufdeckung des Lösungsalgorithmus, während nach überwiegender Ansicht die Darlegung der grundlegenden Funktionsweise, d.h. der wesentlichen Parameter und deren Gewicht, ausreichend ist. Auch hier ist unklar, ob sich das vorherige – hier nur allgemein Systemtransparenz – und das nachträgliche Informationsprogramm – hier der konkret gewählte Lösungsalgorithmus in seiner spezfischen Anwendung – unterscheiden. Inwieweit das Informationsprogramm hinsichtlich der automatisierten Entscheidung auch das Profilbildungsverfahren und die Profil-inhalte einbezieht, ist umstritten.

Soweit Einblicksrechte in die technischen Aspekte der Profilbildung und -verwendung gewährt werden, stoßen diese in Anbetracht der Technologie autonomer Systeme an Grenzen: Die hohe Komplexität kann zur Unverhältnismäßigkeit der Offenlegungspflichten für den Verantwortlichen führen, im Übrigen stellt das Gebot einer laienverständlichen Darlegung vor Herausforde-

rungen. Problematisch ist aber vor allem die fehlende menschliche Nachvollziehbarkeit von Algorithmen aus Maschinellen Lernverfahren, die einer Erfüllung der Informationspflichten entgegensteht.

IV. Bewertung des Transparenzgrundsatzes als Instrument zur Regulierung autonomer Systeme

Den hohen Erwartungen, die an den Transparenzgrundsatz der DSGVO gestellt werden, um autonome Systeme effektiv steuern zu können, wird dieser zumindest teilweise gerecht. Die DSGVO erlaubt auch Einblicke in die Verarbeitungstechnik, wenngleich allein bei automatisierten Entscheidungen einschließlich einem Profiling, sowie, in begrenztem Rahmen, innerhalb des Rechtmäßigkeitsgrundsatzes. Zudem erkennt die DSGVO an, dass es einer laiengerechten Aufbereitung bedarf, damit die Information die betroffene Person auch tatsächlich erreicht. Am Ende verschaffen diese besonderen Informationspflichten der betroffenen Person überwiegend aber nicht eine solche Grundlage, die es ihr erlaubte, Datenverarbeitungen durch autonome Systeme effektiv steuern und Autonomiegefährdungen abwehren zu können. In das maschinelle Wissen, wie es im Modell und Lösungsalgorithmus repräsentiert ist, erhält die betroffene Person nur bedingt Einblicke. Soweit diese gewährt werden, stößt der Transparenzgrundsatz aber aufgrund der hohen Komplexität der Maschinellen Lernverfahren und ihrer fehlenden menschlichen Nachvollziehbarkeit an Grenzen. Dies führt zu erheblichen Schwächungen des Regulierungsapparats der DSGVO. Das Transparenzkonzept der DSGVO kann diese Intransparenzen nicht auffangen, teilweise verstärkt es diese sogar.

Bevor auf diese Defizite des Transparenzgrundsatzes eingegangen wird, ist es wichtig, sich nochmals die verschiedenen Formen der Intransparenz autonomer Systeme zu vergegenwärtigen. Diese sollen vorab dargestellt werden (1.). Im Weiteren soll dann näher auf die Folgen eines unzureichenden Transparenzangebots für die Steuerungseffektivität der DSGVO im Hinblick auf die Modell- und Profilbildung sowie die Profilverwendung eingegangen werden (2.). Abschließend soll dargelegt werden, dass das Transparenzkonzept der DSGVO in seiner aktuellen Ausgestaltung ungeeignet ist, diese Intransparenzen – und damit auch den ausgelösten Regulierungsdefiziten – zu begegnen (3.).

1. Vorüberlegungen: maschinelles Wissen als Herausforderung für Transparenzgebote

Es ist bereits ausgeführt worden, dass das maschinelle Wissen, wie es sich im Modell bzw. Lösungsalgorithmus darstellt, erhebliche Gefährdungspotentiale für die betroffene Person bereithält. Im Rahmen der Profilbildung erlaubt das Modell die Generierung neuer Daten, deren Informationsinhalte weit über die Informationsinhalte der hierfür verarbeiteten Daten hinausgehen, im Rahmen der Profilverwendung erlaubt der Lösungsalgorithmus die Automatisierung

von Anwendungen mit potentiell nachteiligen Effekten für die betroffene Person.

Jene Form des Wissens verspricht im Gegensatz zu menschlichem Wissen sogar ein erhöhtes Maß an Transparenz – verwendete Daten und Auswertungsverfahren sind vorab und abschließend festgelegt, Inhalte in Form algorithmischer Ergebnisse bzw. Konstrukte liegen statisch, dauerhaft gespeichert und jederzeit ablesbar vor.[658] Dies ist aber nur bedingt richtig. Tatsächlich ist das maschinelle Wissen dem technischen Laien, in weiten Teilen auch dem Menschen generell nicht mehr zugänglich. Auch rechtlich sind Grenzen aufgezeigt.

Unterscheiden lassen sich fünf verschiedene Formen der Intransparenz:[659] rechtlich bedingte Intransparenz (a)), Intransparenz aufgrund fehlender technischer Expertise (b)), Intransparenz aufgrund der kontinuierlichen Fortentwicklung der Systeme (c)), Intransparenz aufgrund menschlicher Kognitionsgrenzen (d)) und Intransparenz aufgrund menschlich unverständlicher Epistemik autonomer Systeme (e)).

Im Einzelfall greifen dann je eigene Formen der Intransparenz, auch können mehrere zugleich zutreffen. Die Intransparenz hat zwei zeitliche Richtungen: Sie führt zu Unvorhersehbarkeit und zu fehlender nachträglicher Verständlichkeit. Es ist dann nicht prognostizierbar, welches Profil aus einem Datum gebildet wird oder welche automatisierte Entscheidung oder Steuerung mit der Freigabe eines Datums bzw. mit der Zulassung einer Anwendung erfolgt. Auch im Nachhinein kann nicht nachvollzogen werden, auf welche Regeln die algorithmischen Ergebnisse, sei es das Profil, sei es die automatisierte Entscheidung, gestützt wurden.[660]

a) Intransparenz aufgrund rechtlicher Umstände: Unangemessenheit von Aufdeckungspflichten

Erstens stehen rechtlich geschützte unternehmerische Interessen einer Aufdeckung von Analyseverfahren und -ergebnissen sowie eingesetzter Algorithmen entgegen. Die Intransparenz hat hier rechtliche Gründe.[661] Sowohl das Modell bzw. der Lösungsalgorithmus als auch das Profil selbst sind Kern des Ge-

---

[658] So auch *Wischmeyer*, AöR 143 (2018), 1, 45.

[659] Siehe hierzu bereits Kapitel 2 A. II. 2. c). Eine Differenzierung der verschiedenen Ausgestaltung der Intransparenz autonomer Systeme nehmen auch vor *Mittelstadt*, Int. J. Commun. 10 (2016), 4996 f.; *Martini*, Blackbox Algorithmus, 2019, S. 33–47.

[660] Vgl. auch Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 13 Rn. 31e; *Martini*, Blackbox Algorithmus, 2019, S. 43 f.

[661] Siehe hierzu eingehend *Martini*, Blackbox Algorithmus, 2019, S. 33–41. Siehe auch Gola, DS-GVO/*Franck*, Art. 13 Rn. 31; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16. Siehe hierzu auch Erwägungsgrund 63 S. 5.

schäftsmodells des Verantwortlichen.[662] Diese preiszugeben bedeutete, die autonomen Systeme nicht mehr wirtschaftlich verwerten zu können. Auch bestünde die Gefahr, dass Dritte schadhaft Einfluss auf die Systeme nehmen.[663] Zudem könnte die betroffene Person bei Aufdeckung der Funktionsweise Funktionsstörungen herbeiführen;[664] dies ist besonders bei autonomen Systemen im Bereich der Vertragsgestaltung der Fall. So könnte etwa bei der automatisierten Kreditvergabe ein Kredit trotz tatsächlich bestehendem hohem Zahlungsausfallrisiko erteilt werden, da die betroffene Person Entscheidungskriterien manipuliert hat. Schließlich zählt auch zur rechtlichen Intransparenz im weiteren Sinne, wenn die Herstellung von laienmäßigem Verständnis mit einem unangemessen hohen finanziellen, technischen, personellen oder zeitlichen Aufwand verbunden ist.[665]

b) Intransparenz aufgrund fehlender technischer Expertise: technische Illiteralität

Zweitens ist die technische Methode der Wissensbildung, d.h. die stochastisch-mathematische Auswertung, besonders dann die vielschichtigen algorithmischen Schachtelungen, ohne eine gewisse technische Grundausbildung oder auch spezifische Fachkenntnis für den technischen Laien unverständlich.[666] In eine ähnliche Richtung geht es, wenn es für ein Nachrechnen der Analyseverfahren spezifischer Soft- oder Hardwareausstattung bedürfte.

c) Intransparenz aufgrund Fortentwicklung: dynamische Intransparenz

Problematisch ist drittens, dass das Maschinelle Lernverfahren nicht statisch ist, sondern sich beständig fortentwickelt. Ein Auslesen zu einem bestimmten Zeitpunkt hilft dann wenig, da dies dann weder präzise den algorithmischen

---

[662] Vgl. *Hoffmann-Riem*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, S. 1, 17; *Martini*, Blackbox Algorithmus, 2019, S. 33–38; *Wischmeyer*, AöR 143 (2018), 1, 48; *Burrell*, Big Data and Society 3 (2016), 3 f.

[663] *Burrell*, Big Data and Society 3 (2016), 3 f. hin.

[664] *Miller*, J. Law Technol. Policy 2014, 41, 51: „Proponents of such secret practices typically argue that the confidentiality of algorithms is necessary in order to prevent people from ‚gaming' the system and foster innovation and competition". Siehe hierzu auch *Burrell*, Big Data and Society 3 (2016), 4.

[665] Siehe zur rechtlichen Einordnung der Unverhältnismäßigkeit oben Kapitel 4 D. II. 1. b), siehe zu konkreten Konstellationen der Unverhältnismäßigkeit bei der Profilbildung Kapitel 4 D. III. 2. d) aa) sowie Kapitel 4 D. III. 3. f).

[666] Vgl. *Martini*, Blackbox Algorithmus, 2019, S. 41 f.; *Burrell*, Big Data and Society 3 (2016), 4; *Mittelstadt*, Int. J. Commun. 10 (2016), 4996.

Aufbau für eine bereits erfolgte Auswertung wiedergibt noch sich hieraus spezifische Aussagen für zukünftige Datenanalysen ableiten lassen.[667]

d) Intransparenz aufgrund menschlicher Kognitionsgrenzen: ressourcenbedingte Intransparenz

Viertens übersteigt die maschinelle Wissensschöpfungsmethode regelmäßig quantitativ und qualitativ das kognitive Leistungsvermögen des Menschen: Autonome Systeme können umfassende und komplexe Datensätze analysieren, eine Vielzahl an komplexen Regeln verarbeiten und multivariable, hochanspruchsvolle stochastische Berechnungen in kurzer Zeit vornehmen.[668]

e) Intransparenz aufgrund epistemisch-semantischer Sinnaufladung: Blackbox-Phänomen

Fünftens sind Verarbeitungen anhand von Algorithmen bestimmter Maschineller Lernverfahren für den Menschen im Allgemeinen, d.h. sowohl für die betroffene Person als auch für ExpertInnen, nicht verständlich. Es geht um Konstellationen, in denen autonome Systeme aus Daten Muster ableiten, die jenseits menschlicher Verständniszusammenhänge liegen, in denen die Systeme also aus den Daten ein eigenes epistemisches Wissen ableiten, das für den Menschen unverständlich ist. Diese Intransparenz ist darauf zurückzuführen, dass autonome Systeme „anders denken" als der Mensch.[669] Dies wird als Blackbox-Phänomen bezeichnet.[670] Zwei Formen sind dabei denkbar: Erstens treten datenbasiert-korrelative Sinnaufladungen anstelle menschlich-rationaler, kausalbedingter Hypothesenbildung. Diese maschinell-epistemische Sinnaufladung liegt jenseits menschlich-rationaler Konsistenzbedingungen und stellt sich für den Menschen als irrational-willkürlich dar (inhaltlich-substantielle Intransparenz).[671] Zweitens stellen sich die vielschichtigen, hochkomplexen algorithmischen Strukturen künstlicher neuronaler Netze als für den Menschen unverständlich dar. Auf welche Weise die unzähligen einzelnen Funktionen und Schichten im künstlichen neuronalen Netz geordnet sind, lässt sich am Ende

---

[667] *Martini*, Blackbox Algorithmus, 2019, S. 42. Siehe hierzu auch *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 40; *Mittelstadt*, Int. J. Commun. 10 (2016), 4997.

[668] Vgl. *Wischmeyer*, AöR 143 (2018), 1, 48; *Martini*, Blackbox Algorithmus, 2019, S. 41 f.; *Mittelstadt*, Int. J. Commun. 10 (2016), 4996. Vgl. auch *Beck*, Künstliche Intelligenz und Diskriminierung, 2019, S. 98 f.

[669] So explizit *Burrell*, Big Data and Society 3 (2016).

[670] Siehe eingehend hierzu bereits Kapitel 2 A. II. 2. c).

[671] *Mann/Matzner*, Big Data and Society 6 (2019), 1, 4; *Schneider/Ulbricht*, in: Kolany-Raiser/Heil/Orwat u.a. (Hrsg.), Big Data und Gesellschaft, 2018, S. 198, 204; *Martini*, Blackbox Algorithmus, 2019, S. 60. Eingehend auch *Wachter/Mittelstadt*, CBLR 2019, 494, 505–514.

eines Lernverfahrens kaum bestimmen. In jedem Fall ist in der Einzelanwendung nicht möglich, konkret zu beschreiben, auf welche Weise ein Input einen bestimmten Output erzeugt hat, da das algorithmische Regelwerk menschlich unverständlich ist. Weder im Vor- noch im Nachhinein einer Verarbeitung lassen sich die algorithmischen Verarbeitungsarchitekturen auslesen oder bestimmte mathematisch-stochastische Regeln erkennen.[672]

2. *Bewertung des Transparenzgrundsatzes*

Diese verschiedenen Formen der Intransparenz liegen auf den verschiedenen Verarbeitungsstufen autonomer Systeme in unterschiedlicher Weise vor, bei der Modellbildung (a)) anders als auch bei der Profilerstellung (b)) und nochmals anders bei der Profilverwendung (c)). Die übergreifenden faktisch bedingten Intransparenzen und deren Folgen für das Regulierungsregime der DSGVO insgesamt sollen im Anschluss allgemein vorgestellt werden (d)).

a) Bewertung im Hinblick auf die Modellbildung

Schon von Rechts wegen gibt es Einblicke in die Modellbildung, d.h. das Maschinelle Lernverfahren nicht. Weder sind Trainingsdatensets aufzudecken noch die verwendete Lernmethode – überwacht, unüberwacht oder verstärkend –, auch sind die eingesetzten Lernverfahren oder einzelne Trainingsverarbeitungsschritte nicht offenzulegen. Ebenso wenig besteht ein Anspruch auf Einblick in das algorithmische Konstrukt am Ende des Trainingsverfahrens, hier also in das Modell und seine einzelnen Inhalte. Selbige Erwägungen gelten dann, soweit ein Lösungsalgorithmus anhand personenbezogener Daten in einem Maschinellen Lernverfahren entwickelt wurde. Damit bestätigt sich die Erkenntnis der vorherigen Teilkapitel: Das Maschinelle Lernen wird in der DSGVO nicht eigentlich reguliert: Weder gewährt sie Einblicke in das Trainingsverfahren noch in das Ergebnis, d.h. die gebildeten selbstlernenden Algorithmen.

b) Bewertung im Hinblick auf die Profilbildung

Das Profil hat, anders als das Modell, Auswirkung auf die Einzelperson. Steuerungsdefizite bestehen zum einen aufgrund fehlender profilspezifischer Informationspflichten (aa)), zum anderen aufgrund der faktischen Grenzen der Transparenz (bb)).

---

[672] *Burrell*, Big Data and Society 3 (2016), 9; *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 573; *Purtova*, Law Innov. Technol. 10 (2018), 40, 53. Explizit *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 759: „[D]eep networks may form internal layers whose meaning is opaque to humans, even though the input is still correct". Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 43 f.; *Mittelstadt*, Int. J. Commun. 10 (2016), 4997.

aa) Regulierungsdefizite aufgrund rechtlicher Grenzen: fehlende Normierung profilingspezifischer Informationspflichten

Autonomiegefährdungen durch autonome Systeme haben ihre Ursache gerade in den vertieften Erkenntnissen über die betroffene Person, wie sie die Profilbildung ermöglicht. Aber nicht allein in der Informationsemergenz, sondern auch in deren Intransparenz sind die Autonomiegefährdungen und Diskriminierungen angelegt: Mit der Grundannahme des Datenschutzrechts ist es bereits autonomiegefährdend, dass die betroffene Person nicht weiß, was das Gegenüber von ihr weiß.[673] Nach den Erkenntnissen dieser Arbeit können aufgrund der intransparenten Informationsemergenz verhaltensökonomische Effekte wirken und sind manipulative Nutzungen dieses Wissens möglich.[674] Im Ergebnis bestehen so besondere Bedarfe die Profilbildung gerade durch das Instrument der Transparenz einzugrenzen: Mögliche Profilinhalte müssen möglichst umfassend vorhersehbar und nachträglich auslesbar sein, das Profilverfahren insgesamt muss in das Transparenzprogramm einbezogen werden.[675]

Damit ist die funktionale Dimension der Transparenz von besonderer Bedeutung: Die Kenntnis allein von der Profilbildung und von möglichen Erkenntnissen des Verantwortlichen über Persönlichkeitsmerkmale und individuelle Lebensumstände kann hemm- und verhaltensökonomische Effekte sowie Manipulationen abschwächen oder aufheben. Gleichwohl sieht die DSGVO kein besonderes Informationsprogramm im Sinne des Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO für die Profilbildung vor.

bb) Regulierungsdefizite aufgrund faktischer Grenzen der Transparenz

Zum Problem werden dann auch die faktischen Grenzen der Transparenz im Profilbildungsverfahren.[676] Mit dem soeben Gesagten lässt sich dann feststellen: Die faktische Intransparenz der maschinellen Erkenntnis über den Einzelnen begründet Autonomiegefährdungen. Sie schaltet dann die datenschutzrechtlichen Schutzinstrumente aus. Wie dargelegt, untergräbt die fehlende Vorhersehbarkeit von Profilinhalten etwa die Steuerungswirkungen des Rechtmäßigkeitsgrundsatz auf Stufe der Profilbildung.[677] Allein laienhaft Unverständliches steht der Rechtmäßigkeitsprüfung durch die betroffene Person entgegen, während menschlich Unverständliches die Steuerungswirkungen der Rechtmä-

---

[673] Siehe oben Kapitel 4 A. I. 1. a), Kapitel 4 A. II. 2.

[674] Siehe Kapitel 2 C. IV. 2.

[675] Das Fehlen von Vorschriften zur Transparenz hinsichtlich der Profilbildung kritisiert auch *Lorentz*, Profiling, 2019, S. 340 f. Sehr allgemein eine Erstreckung des Transparenzgrundsatz auf die Verarbeitungsverfahren (Processing) und das Ergebnis (Output) sämtlicher Datenverarbeitungsverfahren fordern *Wachter/Mittelstadt*, CBLR 2019, 494, 514.

[676] Siehe hierzu oben Kapitel 4 D. IV. 1. b)-e). Zur Informationsüberforderung siehe sogleich genauer unter Kapitel 4 D. IV. 2. d) aa).

[677] Siehe Kapitel 4 C. IV. 2. b) aa).

ßigkeit insgesamt aufhebt, denn hier können auch staatliche Akteure sowie Verantwortliche nicht mehr sinnvoll substanzielle Richtigkeitskriterien aufstellen oder überprüfen. Auch die Schutzeffekte der funktionalen Dimension des Transparenzgrundsatzes wirken nicht, denn ohne Vorhersehbarkeit und Kenntnis möglicher Profilinhalte kann die betroffene Person Einwirkungen auf ihre Autonomie keine Resilienz- und Widerstandsmechanismen entgegensetzen. Ist der betroffenen Person etwa nicht bewusst, dass sie eine personalisierte Werbemaßnahme deshalb erhält, da das System sie als psychisch labil erkannt und eine besondere Neigung für ein bestimmtes Produkt errechnet hat, wird sie keine Widerstandskräfte mobilisieren können. Schließlich wirkt die instrumentell-funktionale Dimension der Transparenz nicht mehr: Die betroffene Person kann im Falle ihr unverständlicher Profilbildungen keine sinnvolle Abwägung zwischen Datenschutz, also Ablehnung ihrer Zustimmung, und Selbstschutz, also Erteilung ihrer Zustimmung unter Aktivierung individueller Resilienzmechanismen, treffen.

c) Bewertung im Hinblick auf die Profilverwendung

Auf Stufe der Profilverwendung werden besondere Informationspflichten nur für automatisierte Entscheidungen angeboten. Diese sind aber unzureichend ausgestaltet, und dies im Hinblick auf den Anwendungsbereich wie auch der inhaltlichen Vorgaben (aa)). Zudem stellen faktische Grenzen der Transparenz vor Herausforderungen (bb)). Auch hier droht das dezentrale Regulierungsregime unterwandert zu werden (cc)).

aa) Regulierungsdefizite aufgrund rechtlicher Grenzen: defizitäre Ausgestaltung des Anwendungsbereichs und des Inhalts des besonderen Informationsprogramms

Sowohl im Hinblick auf die Anwendung der besonderen Informationspflichten ((1)) als auch im Hinblick auf deren Inhalte ((2)) erweist sich das auf automatisierte Entscheidungen ausgerichtete Transparenzprogramm als defizitär.

(1) Eingeschränkter Anwendungsbereich des besonderen Informationsprogramms

Bereits der rechtlich zu strikt bemessene Anwendungsbereich der Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO führt zu Steuerungsverlusten des Transparenzgrundsatzes. Vorgeschlagen wird insbesondere, automatisierte Entscheidungen jenseits des Art. 22 DSGVO auszuschließen und zudem allein profilbasierte automatisierte Entscheidungen den besonderen Informationspflichten zu unterwerfen. Dass auch teilautomatisierten Entscheidungen Risiken innewohnen, ist bereits ausgeführt worden. Zudem erscheint die Verknüpfung von Profilbildung und automatisierter Entscheidung nicht sinnvoll. Denn

automatisierte Entscheidungen warten mit einem eigenen Gefährdungsmoment auf, der in der Intransparenz und Unkontrollierbarkeit der algorithmischen Entscheidungsarchitektur liegt. Sicherlich erhöht der Einbezug eines Profils und also die Abstützung der Entscheidung auf weitreichenden, dabei intransparenten Erkenntnissen über die betroffene Person die Gefährdungslage. Doch auch automatisierte Entscheidungen ohne Profilbildung können im Einzelfall autonomiegefährdend sein.

(2) Defizitäre Ausgestaltung des Inhalts des besonderen Informationsprogramms

Soweit die besonderen Informationspflichten für automatisierte Entscheidungen greifen, erweist sich die konkrete Ausgestaltung des Informationsprogramms als unzureichend. Gefordert wird zum einen eine Offenlegung der Algorithmen. Schon aufgrund entgegenstehender unternehmerischer Interessen ist dies nicht überzeugend; da der Laie mit derartigen Einblicksrechten ohnehin nichts anfangen könnte, ist dies auch im Hinblick auf die Steuerungseffektivität nicht sinnvoll. Richtig ist es daher, allein die Darlegung der grundlegenden Funktionsweise, d.h. wesentliche entscheidungstragende Parameter und deren Gewichtung in der algorithmischen Entscheidungsarchitektur, zu verlangen. Es ist dann aber unklar, in welchem Detailgrad dies erfolgen soll. Was im Einzelnen „wesentliche Parameter" sind, bleibt offen. Auch bieten Art. 13 Abs. 2 lit. f), Art. 15 Abs. 2 lit. h) DSGVO keine rechtsklare Grundlage hinsichtlich Einblicksrechten in das Profilbildungsverfahren. Soweit dieses in die automatisierte Entscheidung aufgeht, trägt die Intransparenz des Profils bzw. Profilbildungsverfahrens auch zur Intransparenz der algorithmischen Entscheidungsarchitektur bei.

bb) Regulierungsdefizite aufgrund faktischer Grenzen der Transparenz

Soweit Informationen hinsichtlich der automatisierten Entscheidung bzw. dem Profiling bereitzustellen sind, ist problematisch, wenn aufgrund Unverhältnismäßigkeit bzw. Unmöglichkeit – hierzu im Anschluss genauer – eine Verständlichkeit der algorithmischen Entscheidung für die betroffene Person nicht hergestellt werden kann. Die betroffene Person kann sich dann der Autonomiegefährdungen der automatisierten Entscheidung nicht erwehren, die Betroffenenrechte nach Art. 22 Abs. 3 DSGVO nicht sinnvoll ausüben. Schließlich kann die betroffene Person, soweit die Folgen der automatisierten Entscheidung nicht mehr vorhersehbar sind, die Abwägungsentscheidungen zwischen zentralisiertem datenschutzrechtlichem Verbot und dezentraler, Selbstschutz aktivierender Ausnahmezulassung nach Art. 22 Abs. 2 DSGVO nicht sinnvoll treffen. Zwar muss sie, dies ist bereits ausgeführt worden,[678] nicht die konkreten Out-

[678] Siehe hierzu oben Kapitel 4 C. III. 3. b) aa) (2).

puts vorhersehen können, wohl aber die Folgen der automatisierten Entscheidung überblicken können. Der Einsatz solcher selbstlernenden Algorithmen, die nicht vorhersehbare Folgen auslösen, steht dem entgegen.[679] In diesen beschriebenen Konstellationen der Intransparenz autonomer Systeme versagt der auf Transparenz gestützte Regulierungsmechanismus der DSGVO im Hinblick auf automatisierte Entscheidungen.

d) Übergreifende Defizite des Transparenzgrundsatzes

Soweit die DSGVO Einblicke in die algorithmische Auswertungsmethodik und deren Ergebnisse bietet oder zumindest eine Aufklärung über Folgen der Verarbeitung fordert, ist das Transparenzregime der DSGVO durch autonome Systeme zusätzlich herausgefordert. Die DSGVO adressiert die Problematik nicht, dass mehr Information auch zu weniger Verständnis führen kann (aa)) und die relativistische Beschränkung des Transparenzgebots auf Verantwortlichen und betroffene Person mit weiteren Transparenzverlusten einhergeht (bb)). Zudem sieht die DSGVO keine Mechanismen vor, wie im Falle menschlich nicht nachvollziehbarer und also unüberwindlicher Intransparenzen vorzugehen ist (cc)). Soweit Verfahren und Ergebnisse ExpertInnen, nicht aber betroffenen Personen verständlich sind, wird das dezentrale Regulierungsregime der DSGVO ausgehöhlt (dd)). Schließlich kann das Transparenzgebot innovationshinderlich wirken (ee)).

aa) Intransparenz durch Informationsüberangebot (Informationsüberforderung)

Die DSGVO wartet im Hinblick auf den Umfang ((1)) und den Inhalt ((2)) der Informationen mit einem überlastenden Informationsprogramm auf.

(1) Quantitative Überforderung (Informationsflut)

Das Informationsangebot droht in einer datenverarbeitungsintensiven Welt autonomer Systeme zu quantitativen Überforderungen zu führen. Die DSGVO verlangt begleitende Informationen für jeden einzelnen Verarbeitungsprozess, dies schon akzessorisch für die Rechtmäßigkeit, insbesondere die Einwilligung, und dann zusätzlich aufgrund der Informationspflichten in Art. 13–15 DSGVO. Die Informationen nach Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO fallen notwendig umfassender aus, sie erhöhen den Informationsumfang dann zusätzlich. In einer Welt autonomer Systeme, in der eine Vielzahl von Modell- und Profilbildungen und -verwendungen mit ihrer hohen Menge

[679] An derartigen, sich völlig frei entwickelnden selbstlernenden Algorithmen besteht gleichwohl in der Praxis in der Regel kein Interesse, siehe hierzu oben Kapitel 4 C. III. 3. a). aa).

an einzelnen Datenverarbeitungen Alltag sein wird, wird die Informationsmenge ins Unermessliche steigen.[680]

Es hat sich gezeigt, dass Informationen ab einem bestimmten Umfang von der betroffenen Person nicht mehr verarbeitet werden können (Informationsflut, Information Overload).[681] Häufig äußert sich dies sogar in der Verweigerung der Informationsaufnahme: Datenschutzerklärungen werden überwiegend als belästigend empfunden und ungelesen weggeklickt.[682] Schon aktuell ist das Informationsangebot so umfangreich, dass es von den durchschnittlichen NutzerInnen kaum wahrgenommen werden kann und auch gar nicht wahrgenommen wird,[683] ja sogar für unwichtig gehalten

---

[680] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 61; *Bäcker*, Der Staat 51 (2012), 91, 112; *Yeung*, iCS 20 (2017), 118, 125 f. Ebenso *van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 94; *Jarovsky*, EDPL 4 (2018), 447, 449 f. Vgl. auch schon *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 133–136. Plakativ *Hildebrandt*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 303, 324: „Beyond that, if we had both the legal and the technological tools to access all the profiles that may impact our lives, we would be swamped by the sheer volume of it".

[681] *Van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 95; *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 7. Unter Zitierung einer repräsentativen Umfrage *Jarovsky*, EDPL 4 (2018), 447, 455.

[682] *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 7. Schon bei Einführung der DSGVO legten einschlägige Studien nahe, dass die Datenschutzerklärungen nicht oder nur teilweise gelesen werden, vgl. die zitierten Untersuchungen bei *Strassemeyer*, K&R 16 (2016), 176; *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 63. Eine Studie im Auftrag der Europäischen Kommission aus dem Jahr 2019 kommt zu dem Ergebnis, dass 37 % der Befragten die Datenschutzerklärungen wahrnehmen, 47 % nur teilweise; gegenüber den Zahlen von 2015 lässt sich eine sinkende Tendenz der Lektüre von Datenschutzerklärungen feststellen, siehe *Eurobarometer*, Special Eurobarometer 487a – March 2019, Directorate-General for Justice and Consumers; Europäische Kommission, März 2019, S. 47–49. Einer Studie des Eurobarometers von 2011 – dann also unter dem Regime der DSRL – zufolge liest der überwiegende Anteil der NutzerInnen eines sozialen Netzwerks dessen Datenschutzerklärungen überhaupt nicht (27 %), selten (27 %) oder nur manchmal (23 %); 73 % gaben an, ihre Einwilligung zur Datenverarbeitung auf Webseiten zu erteilen, vorab die Bedingungen der Datenverarbeitung aber nie, selten oder nur manchmal zu lesen, siehe *Custers/van der Hof/Schermer u.a.*, SCRIPed 10 (2013), 435, 440.

[683] *Kamps/Schneider*, K&R 19 (2020), 24, 26; *Bäcker*, Der Staat 51 (2012), 91, 111; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 82 f.; *Robrecht*, EU-Datenschutzgrundverordnung: Transparenzgewinn oder Information-Overkill, 2015, S. 64 f. Vgl. *Strassemeyer*, K&R 16 (2016), 176, 177, demzufolge der durchschnittliche Zeitaufwand bei gängigen Online-Diensten im Mittel bei über 37 Minuten liegt. Der ausführlichen Studie bei *McDonald/Lorrie Faith Cranor*, J. Law. Soc. 4 (2008-2009), 543, 554 f. zufolge benötigt bereits im Jahr 2008 ein durchschnittlicher InternetnutzerInnen etwa 10 Minuten Lesezeit für die Datenschutzerklärungen auf einer Webseite. Bei der durchschnittlichen Anzahl be-

wird.[684] All dies lässt erwarten, dass das Informationsprogramm für autonome Systeme die betroffene Person nicht mehr erreichen wird.

(2) Qualitative Überforderung (Komplexitätsüberlastung)

Auch die Komplexität eines Sachverhalts kann informationsblockierende Effekte freisetzen. Insbesondere in der Verhaltensökonomie hat man aufgedeckt, dass Betroffene ab einem gewissen Komplexitätsschwellenwert die Informationsaufnahme vollständig verweigern, um ihre Entscheidung dann auf irrationale Beweggründe zu stützen.[685] Bereits aktuell legen Studien nahe, dass das bereitgestellte Informationsmaterial nicht gelesen wird und im Falle der Lektüre auch nicht zu einem echten Verständnis für die technischen Funktionsweisen führt.[686] Da Techniken autonomer Systeme weitaus diffiziler sind, sind der-

---

suchter Webseiten pro Jahr bedeutete dies einen durchschnittlichen Zeitaufwand von 244 Stunden pro Jahr, die NutzerInnen aufwenden müssten, um sämtlicher Datenschutzerklärungen der aufgesuchten Webseiten umfassend zu lesen, siehe *dies.*, J. Law. Soc. 4 (2008-2009), 543, 562 f. Der Zeitaufwand dürfte heutzutage deutlich höher sein. In der Entscheidung gegen die Lektüre der Datenschutzerklärungen steckt also eine durchaus kluge Strategie: Die Befassung mit den quantitativ und qualitativ herausfordernden Informationsangeboten stehen in keinem Verhältnis zur tendenziell kurzen Nutzungszeit eines Dienstes oder Produktes, vgl. zu derartigen Rationalitätserwägungen *Strassemeyer*, K&R 16 (2016), 176; *McDonald/Lorrie Faith Cranor*, J. Law. Soc. 4 (2008-2009), 543, 549; *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 8. Ausführlich *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 83. Dies eröffnet auch Missbrauchsmöglichkeiten: Durch quantitativ oder qualitativ anspruchsvoll gestaltete Datenschutzerklärungen kann die Durchführung unerwünschter Datenverarbeitungen verschleiert werden, hierauf weist *Jarovsky*, EDPL 4 (2018), 447, 449 hin.

[684] Vgl. zu derartigen Abstumpfungseffekten *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 16, ebenso Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 310. Dies bestätigt die Studie des *Eurobarometer*, Special Eurobarometer 487a – March 2019, Directorate-General for Justice and Consumers; Europäische Kommission, März 2019, S. 51, wonach 11 % der Befragten als Grund für die fehlende Lektüre angaben, dass sie diese nicht für wichtig erachteten.

[685] Vgl. *van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 95; *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 7. Unter Zitierung einer repräsentativen Umfrage *Jarovsky*, EDPL 4 (2018), 447, 455. Eingehend zu diesen Effekten auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 368 f.

[686] Bereits in der Studie von 2011 gaben nur 21 % der Befragten an, dass sie die Datenschutzerklärungen tatsächlich vollständig, 42 % dass sie diese nur teilweise verstünden; als Grund wurde unter anderem die komplizierte Sprachgestaltung genannt, siehe *Custers/van der Hof/Schermer u.a.*, SCRIPed 10 (2013), 435, 440, 443. Die Umfrage des *Eurobarometer*, Special Eurobarometer 487a – March 2019, Directorate-General for Justice and Consumers;

artige Transparenzblockaden erst recht zu erwarten. Ohne gewisse technische Vorkenntnisse wird sich ein echtes Verständnis von der Wirkungsweise und den Risiken autonomer Systeme nicht herstellen lassen,[687] betroffene Personen mit geringem technischen Verständnis oder Interesse wird man womöglich ganz verlieren.[688]

Der Zielkonflikt zwischen Präzision und Verständlichkeit verstärkt sich immer mehr, je komplexer sich die Automatisierungsmethodiken darstellen. Zur Darlegung der involvierten Logik wird es immer umfassenderer Informationen bedürfen, die abschreckend auf die betroffenen Personen wirken[689] und aufgrund ihres quantitativen Umfangs überfordernd sind.[690] Oder aber der Verantwortliche ist zu Simplifizierungen gezwungen, die den Sachverhalt nicht korrekt wiedergeben.[691] Bei einer gewissen Komplexitätsschwelle wird es zudem gar nicht mehr gelingen, eine technische Funktionsweise laiengerecht darzustellen.[692]

bb) Transparenzverluste durch individualistische und relativistische Beschränkung des Transparenzkonzepts

Die Informationspflichten in der DSGVO adressieren allein die betroffene Person, zudem bestehen sie allein im Verhältnis zwischen Verantwortlichen und

---

Europäische Kommission, März 2019, S. 51 f. deckt auf, dass 31 % der Befragten die Datenschutzerklärungen für unklar oder schwer verständlich halten.

[687] So auch *Strassemeyer*, K&R 16 (2016), 176 f. Vgl. allgemein für Digitalprozesse *Martini*, Blackbox Algorithmus, 2019, S. 188 f.; für Maschinelle Lernverfahren *Edwards/Veale*, SSRN Journal 2017, 65–67, die auch von „transparency fallacy" sprechen. Dazu trägt sicherlich auch der Umstand bei, dass autonome Systeme den Alltag des Einzelnen erleichtern sollen, ohne dass sich die betroffene Person über diese Gedanken macht. Vgl. zu dieser Überlegung Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Roßnagel*, Art. 5 Rn. 61.

[688] Der Bildungsstand der betroffenen Person ist bereits auch für das Verständnis einer nicht-technischen Datenschutzerklärung bedeutend, siehe die zitierte Studie bei *van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 96.

[689] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 12 Rn. 12; *van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 95. In der Studie des *Eurobarometer*, Special Eurobarometer 487a – March 2019, Directorate-General for Justice and Consumers; Europäische Kommission, März 2019, S. 51 f. wird als maßgeblicher Grund, weshalb Datenschutzerklärungen nicht gelesen werden, deren Länge angegeben, ebenso in der Studie des Eurobarometer von 2011, zitiert nach *Custers/van der Hof/Schermer u.a.*, SCRIPed 10 (2013), 435, 443.

[690] Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 12 Rn. 12.

[691] Vgl., wenngleich sehr allgemein, Gola, DS-GVO/*Franck*, Art. 12 Rn. 23; Paal/Pauly, DS-GVO/*Paal/Hennemann*, Art. 12 Rn. 28.

[692] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12; Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 12. Zu diesem Zielkonflikt Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 12; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 12 Rn. 12.

betroffener Person. Auf Seiten der betroffenen Person werden dann Ausgleichsmechanismen nicht genutzt, die dadurch entstehen könnten, dass anstelle der betroffenen Person die gesellschaftliche Öffentlichkeit insgesamt oder Interessensverbände bzw. ExpertInnengruppen treten. Auch die Fachöffentlichkeit bleibt – anders als etwa im DSA[693] – im Transparenzmodell der DSGVO völlig außen vor.[694] Dass die Fachöffentlichkeit nicht eigens adressiert wird, ist schon problematisch vor dem Hintergrund, dass den betroffenen Personen vielfach die notwendige technische Expertise fehlt, um die Verarbeitungsverfahren überhaupt verstehen zu können. Vor allem aber besteht ein besonderer Bedarf an Einbindung der Fachöffentlichkeit, da für eine zutreffende Einordnung der technikbedingten Autonomiegefährdungen und Diskriminierungen der technische Blick allein nicht reicht, sondern auch interdisziplinäre Kenntnisse, etwa aus dem Bereich der Psychologie, Soziologie oder Ökonomie notwendig sind.[695] Auf Seiten des Verantwortlichen bleiben Transparenzgewinne, wie sie durch Vermittlung Dritter entstehen könnten, etwa durch Aufsichtsbehörden, Interessensverbände oder sonstige Dritte, ungenutzt.[696]

cc) Fehlende Lösung für unüberwindliche Grenzen der Transparenzherstellung, insbesondere Blackbox-Phänomen

Für sämtliche der eingangs beschriebenen Formen der Intransparenz sieht die DSGVO im Ergebnis keine Lösungen vor. Dies gilt schon für den Fall, dass die Offenlegung aufgrund der einzusetzenden Ressourcen unverhältnismäßig wäre (rechtliche Intransparenz). Auch in Konstellationen, in denen die technischen Verfahren nicht mehr laiengerecht, d.h. ohne technisches Vorverständnis erläutert werden können (technische Illiteralität), werden nicht aufgelöst, ebenso solche, in denen sich Erläuterungsanspruch und verständlichkeitsbegrenzender Umfang widersprechen (ressourcenmäßige Intransparenz), die Bedingungen der Präzision und Verständlichkeit also unüberwindlich kollidierend aufeinandertreffen. Auch für menschliche Kognitionsgrenzen sieht die DSGVO keine Lösungen vor (ressourcenmäßige Intransparenz). Problematisch ist schließlich die fehlende Nachvollziehbarkeit bei Algorithmen aus Maschi-

---

[693] Vgl. Art. 40 Abs. 4–12 DSA, Erwägungsgründe 96–98 des DSA.

[694] Der Einbezug von FachexpertInnen kann auch die öffentliche Diskussion bestärken und damit Effekte der Selbstregulierung anregen, vgl. hierzu *Hoffmann-Riem*, in: Schulte/Di Fabio (Hrsg.), Technische Innovation und Recht, 1997, S. 3, 28.

[695] Vgl. auch *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 28, der deshalb Audits der algorithmischen Systeme durch (verschiedene) ExpertInnen fordert.

[696] Vgl. zu den Potentialen der Aufklärungspflichten der Aufsichtsbehörden *Temme*, EDPL 3 (2017), 473, 476. Zum expertenbezogenen Audit mit Veröffentlichungspflichten statt betroffenenbezogener Informationspflichte siehe auch *Casey/Farhangi/Vogl*, BTLJ 34 (2019), 143, 179–183.

nellen Lernverfahren (Blackbox-Phänomen sowie dynamische Intransparenz). Hier bleiben auch dem Verantwortlichen selbst die Auswertungsverfahren unverständlich, ihm bleibt also nichts, was er an die betroffenen Personen weitergeben könnte.[697] Lässt man in diesen Fällen der Unverhältnismäßigkeit bzw. der Unmöglichkeit die Transparenzpflicht entfallen,[698] diktierte das Faktische das Normative.[699] Hält man am Transparenzgrundsatz fest, verpflichtet man den Verantwortlichen im Falle der Unverhältnismäßigkeit zu etwas jenseits des rechtlich als für angemessen definiertem, im Falle der Unmöglichkeit verstieße man gegen den Grundsatz *ultra posse nemo obligatur.* Mittelbar etablierte man ein Technikverbot, da mit (angemessenen Maßnahmen) nicht verständlich aufbereitbare Datenverarbeitungstechniken nicht mehr zulässigerweise genutzt werden könnten.[700] Der Unionsgesetzgeber geht offenbar davon aus, dass allein der fehlende Wille des Verantwortlichen sowie die unzureichende technische Expertise der betroffenen Personen zu Intransparenzen führt, die Auswertungsverfahren automatisierter Entscheidungen (und der Profilbildung) aber stets menschlich verständlich gemacht werden können. Unüberwindliche Intransparenzen hat er nicht mitbedacht.[701]

dd) Aushöhlung des dezentralen Regulierungsregimes aufgrund technischer Illiteralität

Soweit das Profilbildungs- und Profilverwendungsverfahren und deren Ergebnisse noch menschlich verständlich, nicht aber für den technischen Laien verständlich sind, droht das dezentrale Regulierungsregime der DSGVO zu zerfallen. Denn dann kann allein der Verantwortliche, der um die technische Funktionsweise und deren Folgen der Profilbildung weiß, inhaltliche Angemessenheitsbedingungen festlegen. Der Mechanismus der Regelbildung „von unten", der beide am Datenverarbeitungsverfahren Beteiligte einbezieht, funktioniert dann nicht mehr. Schon aus Gründen des Interessenskonflikts wird man an der Schutzeffektivität eines auf den Verantwortlichen verlagerten Steuerungssys-

---

[697] *Van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91, 96.

[698] So zur Unmöglichkeit der Transparenz *Gausling*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, S. 379, Rn. 43.

[699] Ebenso *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 285.

[700] So auch *Hoeren/Niehoff*, RW 9 (2018), 47, 60; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 343.

[701] So auch *Goodman/Flaxman*, AI Magazine 38 (2017), 50, 55, die darauf hinweisen, dass der Unionsgesetzgeber bei der Normierung des Transparenzgrundsatzes allein die Konstellationen vor Augen hatte, dass die betroffene Person aufgrund technischer Illiteralität das automatisierte Entscheidungsverfahren nicht verstehen kann sowie dass der Verantwortliche aus geschäftlichen Gründen entsprechende Informationen nicht herausgeben will, nicht aber, dass auch der Verantwortliche selbst das automatisierte Entscheidungsverfahren nicht nachvollziehen kann. Ebenso *Temme*, EDPL 3 (2017), 473, 483.

tems zweifeln müssen.[702] Alternativ könnten nur staatliche Institutionen, insbesondere die Aufsichtsbehörden, in die Schutzlücke treten und etwa über die Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO für angemessenen Ausgleich sorgen. Dies führte aber zu einer zentralistisch-paternalistischen Verschiebung des Regulierungsregimes der DSGVO.[703]

ee) Innovationsbehinderung durch Informationspflichten

Transparenzgebote können schließlich innovationshemmende Wirkungen freisetzen. Bereits der Umstand, dass hierdurch unternehmerische Interessen in empfindlichem Maße berührt sein können, kann es wirtschaftlich unattraktiv machen, in diese Technik und ihre Weiterentwicklung zu investieren. Zudem besteht die Gefahr, dass Dritte wie auch betroffene Personen befähigt werden, funktionsbeeinträchtigend auf das System einzuwirken. Bei automatisierten Vertragsgestaltungen könnten etwa technisch versierte NutzerInnen bei entsprechender Kenntnis von den Entscheidungsparametern und deren Gewicht, so auf das automatisierte Entscheidungssystem einwirken, dass dieses begünstigende, tatsächlich aber fehlerhafte Risikoeinschätzungen und Entscheidungen ausgibt, etwa einen Kredit erteilt, obwohl ein hohes Ausfallrisiko besteht (sogenanntes System Gaming).[704]

Problematisch erweist sich die Forderung nach Transparenz im Sinne menschlicher Verständlichkeit vor allem im Hinblick auf hochkomplexe Auswertungsverfahren bzw. menschlich nicht verständliche Algorithmen aus Maschinellen Lernverfahren. Transparenz und Leistungsstärke von Datenauswertungs- und Lernverfahren erweisen sich dort als nicht vereinbare Größen: Hochkomplexe, vor allem subsymbolische Lernmethoden liefern besonders gute Ergebnisse, sind aber nicht erklärbar, während einfach gelagerte Lernmethoden menschlich verständliche Ergebnisse liefern, dies aber nur für Konstel-

---

[702] Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Hornung/Spiecker gen. Döhmann*, Einleitung Rn. 247.

[703] Vgl. auch *Krönke*, Der Staat 55 (2016), 319, 339 f., demzufolge datenpaternalistische Maßnahmen gerechtfertigt sein können, wenn die Fähigkeit der betroffenen Person zu selbstbestimmtem Handeln ausgeschlossen ist. Er benennt insbesondere Konstellationen kognitiver (Wissens-)Dezifite.

[704] Siehe hierzu etwa *Hacker*, NJW 73 (2020), 2124, 2144; *Kroll/Huey/Barocas u.a.*, University of Pennsylvania Law Review 165 (2017), 633, 639. Eingehend hierzu *Bambauer/Zarsky*, Notre Dame Law Review 94 (2018), 1–48 Dies kann sogar soziale Spannungen begründen, da sich Ungleichheiten ergeben zwischen technisch Begabten und Interessierten bzw. solchen, die eine entsprechende Dienstleistung einkaufen können, und anderen, die über derartige technische Fachkompetenz oder entsprechende finanzielle Mittel nicht verfügen. Diese Gefahr erkennen auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 386. Siehe auch bereits *Hoffmann-Riem*, AöR 123 (1998), 514, 536, der von einer „neuen sozialen Frage" zwischen Schutzfähigen und Schutzlosen spricht. Ebenso *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 226.

lationen geringer Komplexität und mit einem geringeren Maß an Präzision und Effektivität.[705] Man muss sich also zwischen erklärbaren, aber leistungsschwachen und nicht erklärbaren, aber leistungsstarken Auswertungs- bzw. Lösungsmechanismen entscheiden.[706]

V. Ergebnis

Der datenschutzrechtliche Transparenzgrundsatz fordert Offenlegung der äußeren Umstände der Datenverarbeitung, um technische Details der Datenverarbeitung geht es nicht. Allein bei automatisierten Entscheidungen sind derartige Informationspflichten vorgesehen. Damit unterscheidet sich die datenschutzspezifische Transparenz wesentlich von Transparenzforderungen im Hinblick auf Systeme der Künstlichen Intelligenz, bei der es vorwiegend um eine Herstellung menschlicher Verständlichkeit der Verarbeitung geht.

Seine Steuerungskraft entfaltet der Transparenzgrundsatz über drei Dimensionen: eine instrumentelle Dimension, indem die Transparenz die Grundlage für die Wahrnehmung von Betroffenenrechten schafft, eine funktionale, indem die Transparenz aus sich heraus Schutzwirkung entfaltet, und eine instrumentell-funktionale, indem die Transparenz die Zustimmung oder Ablehnung der Einwilligung und damit die Wahl zwischen Daten- und Selbstschutz ermöglicht.

Die Leistungskraft des Transparenzgrundsatzes, wie er in der DSGVO konzipiert ist, wird im Hinblick auf autonome Systeme von zwei Seiten abgeschwächt: erstens aus einer rechtlichen Perspektive, zweitens aus einer faktischen Perspektive. Eine echte Steuerungswirkung entfaltet der Transparenzgrundsatz für diese autonomen Systeme nur, wenn Einblicke in Verfahren und Ergebnisse der Auswertungen gewährt werden. Derartige Informationspflichten sind in der DSGVO aber nur bedingt vorgesehen, nämlich nur für automatisierte Entscheidungen, nach dem Verständnis bestimmter Ansichten in der Literatur sogar nur für ganz spezifische, nämlich profilbasierte automatisierte Entscheidungen. Nur insoweit kann der Transparenzgrundsatz der DSGVO als effektiv bewertet werden. Einblicke in das Maschinelle Lernverfahren selbst, d.h. die Modellbildung und Modellinhalte gewährt die DSGVO dagegen nicht, auch nicht in das Maschinelle Lernverfahren des Lösungsalgorithmus. Zudem sind auch besondere Informationspflichten zum Profilbildungsverfahren sowie zu Profilinhalten nicht normiert. Dies führt zu erheblichen Steuerungsdefiziten

---

[705] *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 575. Dies erkennt auch die *Hochrangige Expertengruppe für künstliche Intelligenz, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz,* 10. April 2019, S. 22 an, die eine einzelfallbezogene Abwägung zwischen Leistungskraft des Systems und Erklärbarkeit vorschlägt.

[706] So auch *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 343 f. Vgl. auch *Casey/Farhangi/Vogl*, BTLJ 34 (2019), 143, 182.

der DSGVO, sind doch wesentliche Autonomiegefährdungen autonomer Systeme gerade in der Intransparenz des Profils angelegt. Soweit derartige Einblicke für (profilbasierte) automatisierte Entscheidungen gewährt werden, stoßen sie vor allem an faktische Grenzen aufgrund der Komplexität und der fehlenden Nachvollziehbarkeit der Auswertungsmethodik durch Algorithmen aus Maschinellen Lernverfahren. Problematisch mit Blick auf das dezentrale Regulierungsregime ist es vor allem, wenn ExpertInnen die Funktionsweise noch verstehen können, betroffene Personen aber nicht: Dann drohen Verantwortliche oder staatliche Stellen, die Regelfindung im Rahmen des Rechtmäßigkeitsgrundsatz an sich zu ziehen; das dezentrale Regulierungsregime der DSGVO wäre unterwandert.

Der Transparenzgrundsatz sieht für diese faktischen Grenzen keine Lösungen vor, ja er verstärkt die Intransparenzen sogar noch. Der Unionsgesetzgeber hat keine Mechanismen in die DSGVO integriert, die einen Ausgleich schaffen, wenn die bereitgestellten Informationen aufgrund ihres Umfangs oder Komplexität die betroffenen Personen überfordern. Die relativistische Ausgestaltung des Transparenzverhältnisses lässt Steuerungsgewinne, wie sie durch Einblicksrechte für ExpertInnen, Informationspflichten an die Gesamtöffentlichkeit sowie durch Informationsvermittlung durch Dritte entstehen könnten, außen vor. An Methoden zum Umgang mit unüberwindlichen Intransparenzen – sei es aufgrund rechtlicher Unangemessenheit, fehlender technischer Expertise, menschlicher Kognitionsgrenzen, fehlender Nachvollziehbarkeit oder dynamischer Fortentwicklung der autonomen Systeme – fehlt es in der DSGVO. Die DSGVO beruht damit auf der Vorstellung, dass technische Verfahren stets transparent, d.h. menschlich und laienhaft verständlich dargelegt werden können, allein die fehlende Bereitschaft der Verantwortlichen zu Aufdeckung bzw. Erläuterung der Transparenz entgegensteht. Für die verschiedenen Formen unüberwindlicher Intransparenz ist die DSGVO dagegen nicht vorbereitet. Schließlich ist nicht hinreichend berücksichtigt, dass ein zu weites bzw. undifferenziertes Informationsprogramm in besonderem Maße innovationshemmend wirken kann.

E. Ergebnis

Die Untersuchung hat gezeigt: Die DSGVO bietet auf allen Verarbeitungsstufen autonomer Systeme – Modellbildung, Profilbildung und Profilverwendung – Regulierungszugriffe und passt die Regulierungsintensität entsprechend dem Risiko der Verarbeitung für die betroffene Person an. Der Regulierungszugriff erfolgt mit Blick auf das Datum, dem eine unmittelbare, prognostizierbare Verbindung mit den aus der Datenverarbeitung nachteiligen Folgen unterstellt wird. Die DSGVO fokussiert zudem auf das Einzeldatum und die einzelne Verarbeitung, hat allein die betroffene Person im Blick und gestaltet das Daten-

schutzverhältnis relativistisch zwischen betroffener Person und Verantwortlichem aus. Die DSGVO ist datenbezogen, gewisse Öffnungen hinsichtlich automatisierungs- und algorithmenspezifischer Regulierungszugänge sind allein für automatisierte Entscheidung vorgesehen.

Für Maschinelle Lernverfahren sieht die DSGVO keine eigenen Vorschriften vor, obschon hierin Autonomiegefährdungen und Diskriminierungen ihre Ursache haben, zudem die dabei erzeugten Algorithmen – Modell und Lösungsalgorithmus – aufgrund ihrer fehlenden Nachvollziehbarkeit datenschutzrechtliche Rechtsinstrumente beeinträchtigen. Die Profilbildung stellt eine besondere Gefährdungslage dar, da hier Erkenntnisse jenseits des Rohdatums gebildet werden, die für die betroffene Person in der Regel nicht vorhersehbar und kontrollierbar sind und gerade deshalb Autonomiegefährdungen auslösen. Die DSGVO definiert zwar das Profiling, es sind aber keine weiteren inhaltlichen Vorschriften allein für die Profilbildung normiert. Mit den Vorschriften zu automatisierten Entscheidungen lassen sich die spezifischen Gefahren der Profilverwendung, die in der Intransparenz des Lösungsalgorithmus ihre Ursache haben, adressieren. Allerdings fällt nur ein kleiner Teil von Anwendungen autonomer Systeme unter diese Vorschrift, insbesondere teilautomatisierte Entscheidungssysteme bzw. Entscheidungsassistenzsysteme nicht, obschon von diesen die nämlichen Autonomiegefährdungen und Diskriminierungsanfälligkeiten angelegt sind.

Der Zweckfestlegungsgrundsatz stellt sich als angemessenes Instrument zur Regulierung Maschineller Lernverfahren dar. Der Zweckbestimmungsgrundsatz verlangt auf Stufe der Modellbildung keine präzise Prognose von Auswertungsergebnissen, unterbindet aber anwendungs- und ergebnisoffene Maschinelle Lernverfahren, zudem solche, die sich so weit von menschlichen Konsistenzzusammenhängen bewegen, dass sich auch Anwendungskontext und Grobinhalte nicht mehr bestimmen ließen. Einer Mehrfachverwendung von Trainingsdaten stellt sich der Zweckbindungsgrundsatz nicht entgegen, solange betroffene Personen auf die Weiterverwendung ihrer Daten hingewiesen werden und keine sensiblen Daten oder Daten aus unbekannten und unstrukturierten Kontexten, wie dies häufig bei Datenzukauf der Fall ist, verarbeitet werden. Auch die Profilbildung und Profilverwendung, d.h. der Einsatz selbstlernender Algorithmen, ist zulässig, solange sich Analyseergebnisse noch in die angegebenen Anwendungskontexte ordnen lassen.

Der Rechtmäßigkeitsgrundsatz erlaubt eine auf das jeweilige Risiko der Verarbeitung abgestimmte Angemessenheitsprüfung einer jeden Datenverarbeitung autonomer Systeme, setzt aber voraus, dass die Folgen unmittelbar mit dem für diese Verarbeitung freigegeben Datum verknüpft sind. Die Untersuchung hat vor Augen geführt, dass das Maschinelle Lernverfahren datenschutzrechtlich nicht reguliert werden kann: Die atomistische, partikularistische, individualistische und datenbezogene Perspektive der DSGVO geht an den eigentlichen Regulierungsfragen Maschineller Lernverfahren vorbei, bei denen

der Wissensgewinn und damit die Ursache für spätere Autonomiegefährdungen und Diskriminierungen im (Trainings-)Datenkollektiv, (Trainings-)Verarbeitungskollektiv, in der Gefährdung von Dritten bzw. Gruppen und algorithmische Erkenntnis liegt. Führt der Einsatz selbstlernender Algorithmen dazu, dass Folgen und Ergebnisse der Profilbildung oder der Profilverwendung nicht mehr vorhersehbar sind, versagt der konnektivistisch-prädiktive Mechanismus des Rechtmäßigkeitsgrundsatzes. Für die Generierung neuer Daten, wie sie in der Profilbildung erfolgt, sieht die DSGVO keine Lösung vor. Dass bei der Profilverwendung die Gefährdung durch Ubiquität und Permanenz der Einwirkung autonomer Systeme entsteht, kann die DSGVO nicht abbilden. Die hohe Anzahl und Komplexität der Datenverarbeitungen durch autonome Systeme bewirkt Kontrollblockaden bei der betroffenen Person, aber auch bei sonstigen menschlichen Prüfern auf Seiten des Verantwortlichen oder staatlicher Institutionen. Das Erfordernis der Einzelrechtfertigung einer jeden Datenverarbeitung autonomer Systeme und die Gefahr der Rücknahme der Rechtmäßigkeit bei der Einwilligung (Art. 7 Abs. 3 DSGVO) wirken innovationshinderlich. Innovationshinderlich wirkt ebenso die Anforderung, dass Folgen der Datenverarbeitung für die Rechtmäßigkeitsprüfung vorhersehbar sein müssen. Dies steht der Verwendung selbstlernender Algorithmen entgegen, bei denen sich Outputs und Folgen nicht prognostizieren lassen.

Der Transparenzgrundsatz vermag die Regulierungsschwächen des Rechtmäßigkeitsgrundsatzes, namentlich die fehlende Vorhersehbarkeit der Folgen der Datenverarbeitungen durch selbstlernende Algorithmen teilweise auszugleichen, zudem dämmt er die Ursache von Autonomiegefährdungen und Diskriminierungen ein, die gerade in der Intransparenz der Folgen und Ergebnisse der Datenverarbeitungen der Profilbildung und -verwendung ihre Ursache hat. Dies gilt jedoch nur, soweit der Transparenzgrundsatz ins Algorithmische hineinreicht und also zur Offenlegung technischer Funktionsweise oder Ergebnisse verpflichtet. Dies ist allein bei der automatisierten Entscheidung vorgesehen. Dabei bleibt aber der Inhalt der Informationspflichten unklar. Ob die besonderen Transparenzpflichten auch für die Profilbildung gelten, ist äußerst umstritten, wird aber überwiegend abgelehnt. Der Grundsatz kommt an Grenzen, wo sich Verarbeitungsverfahren und Ergebnisse der automatisierten Entscheidung nicht mehr für die betroffene Person in angemessener Weise verständlich darstellen lassen. Problematisch ist, dass das Informationsangebot vielfach überfordernd ist, zudem allein der Verantwortliche zur Herstellung von Transparenz gefordert und auch nur die betroffene Perosn als Informationsempfänger adressiert ist. Vor allem aber ist problematisch, dass die DSGVO keinen Ausgleichsmechanismus vorsieht, soweit sich Ergebnisse und Verfahren autonomer Systeme menschlich nicht verständlich darlegen lassen. Soweit noch der Verantwortliche, nicht aber die betroffene Person Ergebnisse und Verfahren verstehen kann, droht das dezentrale Regulierungsregime der DSGVO zu kippen. Der Transparenzgrundsatz verlangt vom Verantwortlichen

einigen Ressourceneinsatz und kann einen Missbrauch der autonomen Systeme ermöglichen. Dies kann innovationsfeindlich wirken. Auch ein Verständnis des Transparenzgrundsatzes als Gebot der Ausgestaltung menschlicher Verständlichkeit der eingesetzten selbstlernenden Algorithmen kann innovationshinderliche Effekte freisetzen.

Kapitel 5

Reformvorschläge und Grenzen der DSGVO als Instrument zur Regulierung autonomer Systeme

Die voranstehende Untersuchung hat gezeigt: Regulierungszugriffe auf autonome Systeme bietet die DSGVO nur beschränkt, nämlich nur auf Profilbildung und -verwendung, nicht auf Modell und Lösungsalgorithmus und das Maschinelle Lernverfahren. Die Regulierungsinstrumente des Zweckfestlegungs-, des Rechtmäßigkeits- und des Transparenzgrundsatzes kommen zudem vielfach an Grenzen. Die neue Technologie autonomer Systeme macht damit Fortentwicklungen des Datenschutzrechts erforderlich.

Eine Vielzahl derartiger Anpassungen der DSGVO im Hinblick auf Maschinelle Lernverfahren und autonome Systeme wird derzeit diskutiert. Ziel des folgenden Kapitels ist es, einen Ausschnitt dieser Diskussion darzustellen, um so ein Verständnis dafür zu entwickeln, an welchen Punkten und mit welchen Methoden man sinnvollerweise für eine Reform der DSGVO ansetzt. Die Darstellung erhebt nicht den Anspruch auf Vollständigkeit. Insbesondere werden nicht für jedes der in Kapitel 4 aufgedeckten Defizite Lösungsmechanismen vorgestellt.

Nicht sämtliche der aufgezeigten Regulierungsdefizite der DSGVO im Hinblick auf autonome Systeme sind richtigerweise datenschutzrechtlich zu beantworten. Der normative Regulierungsbeitrag der DSGVO definiert die Grenzen. Damit ist auch eine Zuordnung möglich, welche der in Kapitel 4 aufgedeckten Regulierungslücken der DSGVO diesseits, welche jenseits der DSGVO liegen. Am Ende lässt sich so feststellen, welchen Beitrag die DSGVO zur Regulierung autonomer Systeme erbringen kann.

Dieser Innovationsrahmen soll zunächst vorgestellt werden (A), bevor dann verschiedene Ansätze zu Innovationen des Anwendungsbereichs, des Zweckfestlegungs- und des Rechtmäßigkeitsgrundsatzes und des Transparenzgrundsatzes vorgestellt und bewertet werden (B.). Anleitend ist dabei, wie schon bei der Bewertung der Rechtsinstrumente der DSGVO, der Maßstab normativer Angemessenheit, wie er in Kapitel 3 vorgestellt wurde.[1] Als Ergebnis lässt sich vorwegnehmen: Das Maschinelle Lernverfahren und die hierbei gebildeten Al-

[1] Siehe Kapitel 3 C II. Siehe zum normativen Regulierungsauftrag der DSGVO überdies Kapitel 4. A.

gorithmen können nicht zum Gegenstand des Datenschutzrechts gemacht werden, ihre Regulierung erscheint aber im Einzelfall geboten. Das Kapitel soll mit einem Ausblick enden, wie eine solche Regulierung aussehen könnte (C.).

A. Innovationsrahmen der DSGVO: datenschutzrechtliche Regulierungsfragen und Schutzinstrumente

Der Gesetzgeber ist – innerhalb der verfassungsgemäßen Grenzen – frei, die DSGVO nach seinen Vorstellungen fortzuentwickeln. Denkbar ist dabei auch, dass er den Regulierungsauftrag erweitert und das Schutzinstrumentarium ausbaut. Im Hinblick auf die Steuerungseffektivität ist dies wenig sinnvoll. Für eine effektive Regulierung autonomer Systeme ist, wie bereits ausgeführt,[2] die Abgrenzung zu und Abstimmung mit Rechtsinstrumenten jenseits der DSGVO wichtig. Eine Zurückhaltung der DSGVO führt dann nicht zu weniger, sondern zu mehr Schutz durch die Rechtsordnung insgesamt.[3]

Die Abgrenzung von Regulierungsaufträgen diesseits und jenseits der DSGVO erfolgt anhand des Regulierungsauftrags der DSGVO, der sich aus dem Regulierungsauftrag (I.) sowie aus dem dezentralen Regulierungsmechanismus zur Gewährleistung digitaler Autonomie ergibt (II.).

---

[2] Kapitel 3 C. I.

[3] Ebenso *Oostveen*, Int. Data Priv. Law 6 (2016), 229, 309: „[To] prevent all the negative effects of big data […] we need to look beyond data protection". Vgl. auch Gola, DS-GVO/*Schulz*, Art. 22 Rn. 2: „Zu den eigentlich dringend regelungsbedürftigen, in den zum Einsatz kommenden Algorithmen liegenden (manipulativen) Gefahren für die Grundrechte und -freiheiten des Einzelnen […] sagt die DSGVO nichts, wobei systematisch richtig solche Regelungen ohnehin im Antidiskriminierungrecht bzw. Produkthaftungsrecht zu verorten wären". Siehe auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192: „Soweit die neue Regulierungsschicht algorithmische Systeme miterfasst, die auch in den – gegebenenfalls im Lichte der hiesigen Empfehlungen modifizierten – Anwendungsbereich des Art. 22 DSGVO fallen, ist auf eine präzise Synchronisierung der Regelungssysteme zu achten". Vgl. zu ähnlichen Erwägungen *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 261 sowie *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 553 f. Vgl. auch *Ernst*, JZ 72 (2017), 1026, 1031, der darauf hinweist, dass die automatisierungs- und algorithmenspezifische Rechtsnorm des Art. 22 DSGVO nur deshalb in die DSGVO Eingang fand, da es an einem anderen Regelwerk fehlte, in das die Vorschrift hätte integriert werden können. Die Situation stellt sich heute anders dar. Mit dem KI-Gesetz-E oder dem DSA sind Regelungen entworfen worden, die gerade algorithmenspezifisch sind.

I. Normativer Regulierungsauftrag: Datenschutzrecht vs. Algorithmen- und Automatisierungsrecht

Die DSGVO reguliert die Verarbeitung personenbezogener Daten, auf Algorithmen und automatisierte Anwendungen erstreckt sie sich nicht.[4] Soweit Reformbestrebungen der DSGVO darauf abzielen, das Datenschutzrecht zu einem Algorithmen- oder Automatisierungsrecht auszuweiten, liegt dies jenseits des normativen Regulierungsbeitrags der DSGVO. Im Übrigen lässt sich auch ein politischer Wille hierzu nicht erkennen.[5]

Gleichwohl öffnet sich die DSGVO an verschiedenen Stellen algorithmen- bzw. automatisierungsbezogenen Regulierungsfragen, vor allem durch die Vorschriften zur automatisierten Entscheidung. Zur Steigerung der Steuerungseffektivität der DSGVO bietet es sich an, diese datenschutzübergreifenden Regulierungsmechanismen zu nutzen. Umso wichtiger ist dann aber eine friktionsfreie Abstimmung mit algorithmen- und automatisierungsspezifischen Regulierungsinstrumenten. Dies bedeutet: Nur im Überschneidungsbereich von datenschutzspezifischen und algorithmen- und automatisierungsbezogenen Regulierungsfragen kann die DSGVO wirken.[6]

Datenschutzspezifische Gefährdungen sind solche, die ihre Ursache in der Intransparenz und Unkontrollierbarkeit von Verarbeitungen personenbezogener Daten haben.[7] Demgegenüber sind algorithmen- und automatisierungsbezogene Gefährdungen solche, die ihre Ursache in der Intransparenz und Unkontrollierbarkeit sowie in der Fehlerhaftigkeit oder Manipulation der algorithmischen Entscheidungsarchitektur haben.[8] Datenschutzspezifische Regulie-

---

[4] Siehe hierzu bereits Kapitel 3 C. II. sowie zum technikneutralen Regulierungsansatz Kapitel 4 A. I. 3. c).

[5] Soweit der Unionsgesetzgeber im Hinblick auf autonome Systeme regulativ tätig wird, tut er dies in eigenen Rechtsakten, etwa dem DSA oder KI-Gesetz-E. Siehe zu diesen Regulierungsentwürfen Kapitel 3 B I. 1. b) sowie Kapitel 3 B. II. b). Zu einer analytischen Kritik des Entwurfs siehe unten Kapitel 5 C. II.

[6] Diese Abschichtung lässt sich bildlich als zwei sich überschneidende Kreise darstellen: Die DSGVO gilt im datenschutzrechtlichen Kreis, der durch datenschutzrechtliche Risiken und Schutzinstrumente definiert ist, nicht dagegen im algorithmen- bzw. automatisierungsbezogenen Kreis, der durch algorithmen- bzw. automatisierungsbezogene Risiken und Schutzinstrumente bestimmt wird. Sie gilt auch im Überschneidungsbereich zwischen datenschutzrechtlichem und algorithmen- bzw. automatisierungsbezogenem Kreis. Dies deutet Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 11 an: Art. 22 DSGVO spreche „das Konzept der informationellen Selbstbestimmung nur am Rande an". Dieser Randbereich meint demnach den Überschneidungsbereich von Datenschutzrecht und Algorithmen- bzw. Automatisierungsrecht. Ähnlich Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 4, demzufolge Art. 22 DSGVO eine „flankierende zu den eigentlichen datenschutzrechtlichen Erlaubnistatbeständen" darstellt.

[7] Siehe hierzu Kapitel 4 A. I. 1. a) und b).

[8] Eingehend Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 1. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3; Däubler/Wedde/Wei-

rungsmechanismen fokussieren auf die Daten, die vorgelagerte Ebene der Soft- und Hardware ist ebenso wenig von Relevanz wie die nachgelagerte Ebene der Anwendung. Darin äußert sich der Grundsatz der Technikneutralität.[9] Vor allem die inhaltliche Angemessenheit des Ergebnisses einer Datenverarbeitung oder der auf die Datenverarbeitung folgenden Entscheidung oder Maßnahme liegt jenseits des Regulierungszugriffs der DSGVO.[10]

Algorithmen- und Automatisierungsregulierung kann damit über die DSGVO erfolgen, soweit hierbei Verarbeitungen personenbezogener Daten stattfinden.[11] Die DSGVO greift, wenn algorithmen- und automatisierungsbezogenen Risiken zugleich datenschutzspezifische sind und die datenschutzrechtlichen Schutzinstrumente passen. Dies bedarf einer Untersuchung einzelner Gefährdungssituationen und korrespondierender Schutzinstrumente. Sie soll nachfolgend im Einzelnen für die Modellbildung, Profilbildung und -verwendung durchgeführt werden.[12]

II. Normativer Regulierungsmechanismus: dezentrale Regulierung vs. zentralisierte Regulierungsmechanismen

Digitale Autonomie im Verhältnis zwischen Privaten wird in der DSGVO durch eine dezentrale Regulierungsmethodik gewährleistet und geschützt.[13] Maßgebliche Mechanismen, etwa Rechtmäßigkeitsgrundsatz, Einwilligung und Transparenzgebot, sind dabei auch primärrechtlich in Art. 8 GRCh verankert. Diese Regulierungsmethodik zu ändern, bedeutete, die datenschutzrechtlichen Vorverständnisse über digitale Autonomie umzuschreiben und also den Regulierungsbeitrag der DSGVO auf höherer Abstraktionsebene neu zu defi-

---

chert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 17. Siehe überdies *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 30 f.

[9] Eingehend Kapitel 4 A. I. 2 c).

[10] *Martini*, Blackbox Algorithmus, 2019, S. 206. Vgl. auch Generalanwältin Kokott, Schlussanträge v. 20.07.2017, Rs. C-434/16, ECLI:EU:C:2017:582, Rn. 35–41 – *Nowak*; EuGH, Vorabentscheidung v. 17.07.2014, Rs. C-141/12 und C-372/12, ECLI:EU:C:2014:2081, Rn. 43–47 – *YS und andere*.

[11] Vgl. nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 4; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 11.

[12] Auch die Normierung weiterer Schutzinstrumente ist denkbar. Diskutiert wird etwa, ob auch inhaltlich-substantielle Anforderungen an das Modell im Datenschutzrecht formuliert werden könnten. Eine Grundlage hierfür böte Erwägungsgrund 71 S. 6. Vgl. zu derartigen Forderungen hinsichtlich des Modells *Lorentz*, Profiling, 2019, S. 339 f.; *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 30 f. Ob dies dann aber noch im datenschutzrechtlichen Regulierungsauftrag der DSGVO gedeckt ist, bedarf vertiefter Erörterung, die aber jenseits des Untersuchungsauftrags dieser Arbeit liegt.

[13] Eingehend Kapitel 4 A. II. 3.

nieren. Der Unionsgesetzgeber könnte dies freilich jederzeit tun. Es bedürfte dann allerdings einer schlüssigen Neukonzeption des Datenschutzes. Dies kann die vorliegende Arbeit nicht leisten. Rechtstechnisch wäre überdies eine Vertragsänderung nach Art. 47 EUV erforderlich, rechtspolitisch erscheint dies unwahrscheinlich. Soweit Innovationsansätze auf eine Zentralisierung des Regulierungssystems setzen, liegt dies jenseits des Innovationsrahmens im Sinne dieser Arbeit.

B. Gebotene Fortentwicklungen der DSGVO

Im Weiteren sollen verschiedene Vorschläge für Weiterentwicklungen der untersuchten Rechtsinstrumente der DSGVO de lege lata und de lege ferenda vorgestellt und aus diesen diejenigen Rechtsänderungen ausgewählt werden, die in optimaler Weise praktische Wirksamkeit und Ausgleich zwischen Innovationsförderung und -behinderung im Sinne normativer Angemessenheit realisieren. Dies erfolgt für den Regulierungszugriff der DSGVO (I.), den Rechtmäßigkeitsgrundsatz (II.) sowie den Transparenzgrundsatz (III.). Der Zweckfestlegungsgrundsatz weist, wie ausgeführt, keine Regulierungsdefizite auf, es bedarf daher diesbezüglich auch keiner Diskussion von Innovationspotentialen.[14]

I. Reformoptionen für den Anwendungsbereich der DSGVO

Im Hinblick auf Reformoptionen der Regulierungszugriffe der DSGVO sind zunächst solche Vorschläge abzuschichten, die jenseits des oben für diese Arbeit definierten Innovationsrahmens der DSGVO liegen (1.). Innovationspotentiale der DSGVO de lege lata ergeben sich allein mit Blick auf automatisierte Entscheidungen nach Art. 22 DSGVO (2.). Besonderes Innovationspotential liegt in der eigenständigen Normierung des Profilings sowie in legislativen Erweiterungen des Art. 22 DSGVO (3.).

1. Innovationsräume im Hinblick auf den Anwendungsbereich der DSGVO

Nach dem oben vorgestellten Innovationsrahmen ist eine Einordnung der drei wesentlichen Verarbeitungsverfahren – Modellbildung bzw. Bildung des Lösungsalgorithmus, Profilbildung und Profilverwendung – in den Regulierungsapparat der DSGVO möglich. Regulierungsfragen der Modellbildung – ebenso der Bildung des Lösungsalgorithmus – unterfallen der DSGVO nicht, wohl aber die Profilbildung sowie die automatisierte Entscheidung (a)). Profilbildung und automatisierte Entscheidung werfen je eigene Regulierungsbedarfe auf. Dies erlaubt, die in Kapitel 2 beschriebenen Autonomiegefährdungen spe-

[14] Siehe oben Kapitel 4 C. IV. 1.

zifischen Regulierungsaufträgen zuzuordnen. Sie stellen sich überwiegend als Problematik des Profilings dar (b)).

a) Interregulative Abgrenzung: Keine datenschutzspezifische Regulierung des Modells

Die DSGVO ist sinnvollerweise nicht auf die Regulierung der Modellbildung sowie die Regulierung des Lösungsalgorithmus zu erstrecken (aa)), wohl aber auf die Profilbildung (bb)) und die automatisierte Entscheidung (cc)).

aa) Keine datenschutzrechtliche Regulierung der Modellbildung und der Erstellung des Lösungsalgorithmus

Regulierungsbedarfe im Hinblick auf die Modelbildung, d.h. die Datenauswertung hinsichtlich einer Personenmehrheit[15] ebenso wie das Maschinelle Lernverfahren, d.h. die Gestaltung von Algorithmen,[16] dies schon deshalb, da hier algorithmenspezifische Gefährdungen angesprochen sind: Die Gefährdungen liegen im abgeleiteten Wissen zur Personengemeinschaft aus den Trainingsdaten, also in der algorithmischen Struktur: Diese ist intransparent und potentiell fehlerhaft und diskriminierungsanfällig.[17] Zur Regulierung bedürfte es eines Zugriffs auf das Daten- und Verarbeitungskollektiv, Trainingsverfahren und -methoden sowie den trainierten Algorithmus selbst. Dies liegt jenseits der datenbezogenen, individualistischen, atomistischen und partikularistischen Perspektive des Datenschutzes[18] und stellt sich in Widerspruch zum technikneutralen Regulierungsansatz der DSGVO.[19] Die Erwägungen gelten auch für die datenschutzrechtliche Regulierung des Lösungsalgorithmus, sofern dieser in einem anhand personenbezogener Daten durchgeführten Maschinellen Lernverfahren gebildet wird. Eine Öffnung des individualistischen Regulierungsregimes der DSGVO hin zum Schutz von Dritt- bzw. Gruppeninteressen erscheint mit dem normativen Regulierungsauftrag der DSGVO dagegen durchaus vereinbar und für eine Schutzverstärkung sinnvoll. Diese Weiterentwicklungen der DSGVO, die unter dem Begriff der Group Privacy diskutiert werden,[20] bedürfen jedoch eingehender Untersuchung, die die vorliegende Arbeit nicht leisten kann.

---

[15] So explizit zur Modellbildung im Rahmen zweistufiger Profilbildungsverfahren *Oostveen*, Int. Data Priv. Law 6 (2016), 229, S. 307, 309. Vgl. auch allgemein zur Big-Data-Analyse *Roßnagel*, ZD 3 (2013), 562, 566.

[16] Allgemein zur Ausgestaltung von Algorithmen, allerdings mit kritischer Wertung, Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 4, 11.

[17] Siehe hierzu bereits oben Kapitel 4 B. IV. 1. b) sowie Kapitel 4 C. IV. 2. a) cc).

[18] Siehe hierzu bereits oben Kapitel 4 C. IV. 2. a).

[19] Siehe oben Kapitel 4 A. I. 2. c).

[20] Siehe aus der umfassenden Literatur einführend *Taylor/Floridi/van der Sloot* (Hrsg.), Group Privacy, 2017; *Mantelero*, in: Taylor/Floridi/van der Sloot (Hrsg.), Group Privacy,

bb) Datenschutzrechtliche Regulierung der Profilbildung

Demgegenüber ist die Profilbildung nicht ausschließlich dem Bereich des Algorithmen- und Automatisierungsrechts zuzuordnen, sie unterfällt dem Überschneidungsbereich. Bei der Profilbildung werden umfassende Erkenntnisse aus der Verarbeitung von (Roh-)Daten gewonnen, die typischerweise weder für die betroffene Person vorhersehbar noch durch sie kontrollierbar sind, dies aufgrund eines seinerseits intransparenten und bedingt kontrollierbaren Algorithmus, d.h. dem Modell. Das Profil enthält am Ende mehr und anderes, als in den einzelnen Daten abgebildet ist.[21] Diese Informationsemergenzen sind potentiell autonomiegefährdend, dabei haben sie ihre Ursache gerade in einer Datenverarbeitung. Es handelt sich damit um ein Gefährdungsmoment, vor dem das Datenschutzrecht gerade schützen soll.[22] Der Schutzmechanismus der DSGVO der an der Einzelperson, dem Einzeldatum und der Einzelverarbeitung anknüpft, ist hier, anders als bei der Modellbildung, passend, da gerade eine ganz spezifische Person betroffen ist und die Gefährdung durch die konkrete Verarbeitung ganz bestimmter Daten ausgelöst wird. Welche Schutzvorschriften für die Profilbildung sinnvoll sind, soll nachfolgend für die Rechtmäßigkeit und die Transparenz geklärt werden. Welche weiteren Vorschriften geboten sind, bedarf genauer Analyse und kann im Rahmen dieser Arbeit daher nicht geklärt werden.

cc) Eingeschränkte datenschutzrechtliche Regulierung automatisierter Entscheidungen

Auch automatisierte Entscheidungen können dem Überschneidungsbereich zugordnet werden; hier bedarf es aber einer besonders präzisen Abgrenzung der Regulierungsaufträge diesseits und jenseits der DSGVO. Denn die Risiken erwachsen der intransparenten, potentiell fehlerhaften und bedingt kontrollierbaren algorithmischen Entscheidungsarchitektur,[23] nicht (allein) der Datenverarbeitung. Es bestehen aber Verknüpfungen zum Datenschutzrecht, da für die Auslösung der Entscheidung ein Datum bzw. Datenverarbeitungsergebnis ver-

---

2017, S. 139; *Puri*, Cornell Journal of Law and Public Policy 30 (2021), 477–538 Spezifisch zu Potentialen für die Regulierung von Systemen der Künstlichen Intelligenz *Majeed/Khan/Hwang*, Electronics 11 (2022), 1–34.

[21] So auch *Lorentz*, Profiling, 2019, S. 335–337. Siehe bereits oben Kapitel 4 B. IV. 2.

[22] Zur Einordnung der Informationsemergenz als datenverarbeitungsspezifisches Risiko *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 304 f. Zur Einordnung der Profilbildung als gerade typisches datenverarbeitungsspezifisches Risiko *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 309. Siehe auch *Roßnagel*, DuD 40 (2016), 561, 563; *Lorentz*, Profiling, 2019, S. 336; *Kugelmann*, DuD 40 (2016), 566, 570.

[23] Siehe zu diesen Risiken Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2.

wendet bzw. weiterverarbeitet wird. Es sind dann nicht wie bei der Profilbildung Erkenntnisse, wohl aber nachteilige Ergebnisse und Folgen, die mit dem verarbeiteten Datum bzw. dem verarbeiteten Datenverarbeitungsergebnis verknüpft werden. Diese Ergebnisse und Folgen kann die betroffene Person in der Regel aus dem verarbeiteten Datum bzw. Datenverarbeitungsergebnis nicht vorhersehen oder nachvollziehen und damit auch nicht steuern. Dies kann dann zu Diskriminierungen[24] oder Autonomiegefährdungen, insbesondere Hemmeffekte, [25] durch die automatisierte Entscheidung führen. Die Risiken der automatisierten Entscheidung sind damit zugleich datenverarbeitungsspezifische Risiken.[26]

Nicht sämtliche automatisierte Entscheidungen begründen allerdings Regulierungsbedarfe.[27] Die Notwendigkeit der Regulierung muss demnach eigens begründet werden. Die DSGVO definiert diesen Regulierungsbedarf im Ergebnis nicht, vielmehr schafft sie mit dem Tatbestandsmerkmal der rechtlichen Folgen und nachteiligen faktischen Wirkungen einen Raum, um diese Regulierungsbedarfe anhand Wertungen jenseits des Datenschutzrechts zu bestimmen. Dies ist richtig, da die Gefährdungsmomente bei der automatisierten Entschei-

---

[24] Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3.

[25] Vgl. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3; *Ernst*, JZ 72 (2017), 1026, 1030. Art. 22 DSGVO soll insbesondere verhindern, dass der Mensch seine Subjektqualität verliert, da er zum „Objekt der Maschine" gemacht wird. Siehe hierzu *Sesing*, MMR 24 (2021), 288, 290; Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 2.

[26] Eine derartige Überschneidung datenverarbeitungs- und algorithmenspezifischer Risiken stellen auch *Ernst*, JZ 72 (2017), 1026, 1030; *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 306 fest. Siehe zu datenverarbeitungsspezifischen Risiken Kapitel 4 A. I. 1. b), spezifisch zu Autonomiegefährdungen Kapitel 4 A. II. 2.

[27] Vgl. Gola, DS-GVO/*Schulz*, Art. 22 Rn. 21; Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 28. In diese Richtung auch *Martini*, Blackbox Algorithmus, 2019, S. 343, der eine Anwendung des Art. 22 DSGVO, dort dann hinsichtlich der Informationspflichten, nur für „grundrechtssensitive[.] Algorithmenanwendungen" vorschlägt. Anders ist dies bei der Profilbildung: Hier ist es gerade die Unüberschaubarkeit und Unkontrollierbarkeit der Einzelinferenzen, die an sich Autonomiegefährdungen auslöst. Es bedarf daher keines (zusätzlichen) Nachweises des Regulierungsbedarfs. Auf den Punkt gebracht von *Rustici*, CRi 18 (2018), 34, 35 f.: „Profiling is a type of processing to be kept under constant scrutiny, not because it will always infringe rights and freedoms, but because it will always have the potential of doing so. […] It is because of the risks inherent in any form or stage of profiling that the GDPR imposes all of its constraints on all forms and stages of profiling" (mit Hervorherbung im Original). Ähnlich *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 239: „[D]ie Gefahr resultiert schon aus der Bildung eines Nutzerprofils (Generierung der Datenbasis), nicht erst aus hierauf folgenden Entscheidungen (Verknüpfung aus Analyse der Daten)". Diese befürwortet am Ende aber eine Regulierung nur von risikoreichen Profilbildungen und fordert damit eine zusätzliche Rechtfertigung der Regulierung, siehe *dies.*, Nutzerprofilbildung durch Webtracking, 2018, S. 266 f.

dung maßgeblich in der Algorithmisierung und Automatisierung und damit jenseits des Datenschutzes liegen. Über diese Gefährdungen und deren Regulierungsbedürftigkeit kann die DSGVO nichts aussagen.[28] Die Einschränkung der Regulierung in Art. 22 Abs. 1 DSGVO auf solche automatisierten Entscheidungen mit rechtlicher Wirkung oder faktischer Beeinträchtigungswirkung ist daher sinnvoll: Sie beschränkt den Anwendungsbereich auf im Einzelfall steuerungsbedürftige automatisierte Entscheidungen und ermöglicht zugleich die Definition von Steuerungsbedarfen anhand außerdatenschutzrechtlicher Wertungen. Darüber hinaus schafft diese Einschränkung einen angemessenen Ausgleich zwischen den Interessen der betroffenen Person und des Verantwortlichen sowie zwischen Innovationsbehinderung und -ermöglichung.[29] Dies entspricht letztlich einem risikobasierten Regulierungsansatz.[30]

Ebenso wie bei der Profilbildung erscheint der auf die Einzelperson, die einzelne automatisierte Entscheidung und die hierbei erfolgende Verarbeitung eines einzelnen Datums fokussierende Regulierungsmechanismus der DSGVO richtig, denn zur Auslösung der automatisierten Entscheidung wird gerade ein ganz konkretes Datum verarbeitet, eine bestimmte Person gefährdet.[31] Regulierungsmechanismen müssen allerdings datenschutzrechtliche bleiben, d.h. Schutzinstrumente, die spezifisch den Lösungsalgorithmus und das für dessen Erstellung erfolgende Maschinelle Lernverfahren adressieren, liegen jenseits des Datenschutzrechts.[32] Hierauf ist noch zurückzukommen.

---

[28] Ähnliche Gedanken bei Gola, DS-GVO/*Schulz*, Art. 22 Rn. 2; *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2 (2016), 535, 553 f., die die maßgebliche Regulierungsfragen des Art. 22 DSGVO jenseits der DSGVO, vor allem im Antidiskriminierungs- oder Verbraucherrecht verorten.

[29] Auf den Ausgleich im Hinblick auf unternehmerische Interessen des Verantwortlichen und dessen Privatautonomie weist Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 6 hin. Zum Ausgleich im Hinblick auf die Innovationsförderung siehe Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 8.

[30] Für eine risikobasierte Regulierung (teil-)automatisierter Entscheidungen tritt auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192. Einen risikobasierten Ansatz zumindest hinsichtlich der besonderen Informationspflichten für automatisierte Entscheidungen schlagen *Sesing*, MMR 24 (2021), 288, 290 f.; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53.

[31] Zu einer Erweiterung des Datenschutzes auf Dritt- und Gruppeninteressen (Group Privacy) siehe oben Kapitel 5 B. I. 1. a) aa).

[32] So aber der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 31, wonach auch ein Algorithmenaudit Teil der DSGVO sein sollte, das sich sowohl auf die Planungs- als auch die Anwendungsphase der Profilbildung erstreckt. Die Erkenntnisse sollen dann in den „Systemaufbau" der Profilbildung einfließen. Siehe auch *Wachter/Mittelstadt*, CBLR 2019, 494, 614: „[T]he ECJ should re-define the law's remit to include the assessment of the accuracy of decision-making processes". Ebenso *Hermstrüwer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 99, 113, der für sektorale Algorithmengenehmigungen bzw. -kontrollmechanismen oder Algorithmenverbandsklagen eintritt. Einge-

b) Einordnung der Autonomiegefährdungen durch autonome Systeme

Die Differenzierung von Regulierungsbedarfen hinsichtlich des Profilings von solchen automatisierten Entscheidungen erfolgt danach, ob die Gefährdung im maschinellen Wissensgewinn über eine Person, d.h. in der Verknüpfung von Rohdaten mit Erkenntnissen vergleichbarer Personen,[33] oder im maschinellen Wissen hinsichtlich einer Lösungsstrategie, d.h. in der Verknüpfung dieser Erkenntnisse mit Realfolgen, begründet liegt.[34] Damit lassen sich die in Kapitel 2 erläuterten Autonomiegefährdungen zuordnen.

Der überwiegende Teil der im Rahmen dieser Arbeit untersuchten Autonomiegefährdungen haben damit ihre Ursache allein im Profiling, d.h. in den für die betroffene Person intransparenten Erkenntnissen jenseits der verarbeiteten Rohdaten. Diese ermöglichen passgenaue Automatisierungen, die dann verhaltensökonomische Effekte hervorrufen, erlauben wirkungsstarke Manipulationen oder lösen Hemmeffekte aus. Dies betrifft vor allem die Anwendungsfälle der Informationsfilterung und personalisierten Werbung. Die dort beobachtbaren Autonomiegefährdungen sind auf verhaltensökonomische bzw. psychosoziale Wirkmechanismen zurückzuführen, die umso stärker sind, je detailgenauer und tiefgehender die Erkenntnisse über die Einzelperson ausfallen. Der (intransparente) Lösungsalgorithmus ist hier nicht das Problem.[35] Entsprechend wären die Steuerungsinstrumente des Art. 22 Abs. 3 DSGVO – die Anfechtung der Entscheidung bzw. Steuerung oder eine Übergabe an einen

---

hend überdies *Martini*, Blackbox Algorithmus, 2019, S. 157–331, der regulative Änderungen vornehmlich in der DSGVO verortet und die Entwicklungen des Datenschutzrechts zur Regulierung der Analysemittel befürwortet, *ders.*, Blackbox Algorithmus, 2019, S. 162.

[33] Vgl. *Lorentz*, Profiling, 2019, S. 268–270, 273; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 9–10. Veranschaulichen lässt sich diese inter- und intraregulative Abgrenzung am Beispiel des Kredit-Scorings: Die Verarbeitung der Daten „Wohnort" und „Alter" lassen nicht erkennen, ob hieraus auch auf die Vermögenslage oder den Beruf geschlossen werden kann bzw. auf welcher Stufe des Rankings zwischen „kreditwürdig" und „nicht kreditwürdig" sie eingeordnet werden. Notwendig sind daher auch regulative Zugriffe auf das Profling. Die Einblicke in sowie die Kontrolle über das Profiling nützen der betroffenen Person aber wenig, wenn sie mit einer ablehnenden automatisierten Entscheidung konfrontiert ist, da als eigenständiges Gefährdungsmoment die maschinelle Entscheidungsarchitektur hinzutritt, die Profil und gegebenenfalls weitere Anwendungsdaten mit dem Output, dann also die Zu- oder Absage einer Kreditanfrage verknüpft. Für einen effektiven Schutz bedarf die betroffene Person sowohl der Einblicke sowie der Abänderungs- oder Anfechtungsmöglichkeit hinsichtlich der Entscheidungsparameter.

[34] Gola, DS-GVO/*Schulz*, Art. 22 Rn. 2; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 1.

[35] So auch *Lorentz*, Profiling, 2019, S. 268-270, 273 sowie *Brkan*, Int. J. Law Inf. Technol. 27 (2019), 91, 103. In diese Richtung auch *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 238–240; *Kugelmann*, DuD 40 (2016), 566, 570.

menschlichen Entscheider – nicht schutzförderlich.[36] Eine Regulierung des Profilings erscheint dann ausreichend, diesen Autonomiegefährdungen zu begegnen. Im Übrigen bieten hier Opt-out-Rechte effektiven Schutz. Ein solches ist bereits in Art. 21 Abs. 1 DSGVO, dort bei Vorliegen eines besonderen Interesses, für die personalisierte Werbung voraussetzungslos in Art. 21 Abs. 2 DSGVO vorgesehen.[37]

Demgegenüber erfasst die Regulierung automatisierter Entscheidungen solche Konstellationen, in denen gerade die automatisierte Entscheidungsarchitektur Autonomiegefährdungen auslöst, da diese potentiell diskriminierungsanfällig und nicht durchschaubar ist. Dies betrifft dann Konstellationen der Kreditvergabe oder der personalisierten Preisbildung. Hier ist eine Regulierung der automatisierten Entscheidung geboten. Im Ergebnis bedarf es sowohl der Regulierung des Profilings als auch der automatisierten Entscheidung, um den Autonomiegefährdungen durch autonome Systeme effektiv zu begegnen.

2. Innovationspotentiale de lege lata: automatisierte Entscheidungen

Im geltenden Recht sind Rechtsänderungen allein im Hinblick auf Art. 22 DSGVO möglich. Die Vorschrift ist auch auf Maßnahmen zu erstrecken (a)), zudem ist eine Lösung für den Automation Bias vorzusehen (b)). Hinsichtlich des Merkmals der rechtlichen Wirkungen und erheblichen Beeinträchtigungen ist klarzustellen, dass die Norm allein nachteilige Folgen erfasst; eine grundrechtsspezifische Lesart ist nicht überzeugend (c)). Dass eine Erstreckung des Art. 22 DSGVO auf sämtliche Profilverwendungen nicht sinnvoll ist, wurde soeben bereits erörtert.[38]

a) Erstreckung auf Maßnahmen

Um sämtliche Phänomene der Einwirkungen autonomer Systeme abzudecken, bietet sich ein weites Verständnis der Entscheidung und damit auch der Maß-

---

[36] Ähnliche Erwägungen stellt die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192 an: „So wäre für algorithmische Systeme, bei denen keine ‚Entscheidung' des Systems im Sinne der bisherigen Fassung des Art. 22 Abs. 1 DSGVO vorliegt, auch ein Recht auf menschliche Letztentscheidung regelmäßig wenig praktikabel und zudem oft auch nicht wünschenswert". Vgl. auch *Lorentz*, Profiling, 2019, S. 271; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27b, die darauf hinweisen, dass es – zumindest für die personalisierte Werbung – bereits ein eigenes Schutzrecht gibt, nämlich Art. 21 Abs. 2 DSGVO.

[37] Daher eine Erstreckung des Art. 22 DSGVO auf die personalisierte Werbung ablehnend Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 26; *Lorentz*, Profiling, 2019, S. 270.

[38] Siehe Kapitel 5 B. I. 1.

nahme an.[39] Erfasst ist damit jede Ausgabe eines autonomen Systems, die Außenwirkung zeigt, d.h. den algorithmischen Auswertungsbereich verlässt und auf sonstige Weise die (analoge oder digitale) Lebenswirklichkeit der betroffenen Person faktisch oder rechtlich verändert. Auch der Generalanwalt beim EuGH tritt für eine derartige Lösung ein.[40] Da dies bislang nur im nicht verfügenden Teil aufgenommen ist,[41] sollte der Unionsgesetzgeber hier klarstellend tätig werden. Damit ist die bloße Anzeige eines Ergebnisses, etwa bei der automatisierten Kreditvergabe die Anzeige der Zu- oder Absage, bei der personalisierten Preisgestaltung die Anzeige des Preises, eine Entscheidung im Sinne des Art. 22 DSGVO.

b) Lösungen für den Automation Bias

Um das Phänomen des Automation Bias[42] in Art. 22 DSGVO zu integrieren, bietet sich ein materielles Verständnis des Merkmals der Ausschließlichkeit an. Ein derartiges materielles Verständnis des Art. 22 DSGVO befürwortet auch der Generalanwalt beim EuGH.[43] Es ist dann nicht auf formale Aspekte abzustellen, ob etwa eine Prüfung durch einen Menschen vorgesehen ist und dieser fachkompetent ist,[44] sondern eine substantielle Abwägungsentscheidung vorzunehmen. In dieser ist zu ermessen, ob im Einzelfall der Automation Bias so hoch liegt, dass er wertungsmäßig der formalen Ausschließlichkeit gleichkommt. Hierzu sind objektive und subjektive Kriterien heranzuziehen.[45] Als

---

[39] Ebenso *Lorentz*, Profiling, 2019, S. 261; Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 15a; *Finck*, Int. Data Priv. Law 9 (2019), 78, 83.

[40] Mit der Frage befasst, ob die Erstellung eines Kreditscores durch eine Auskunftei eine Entscheidung nach Art. 22 DSGVO darstellt, befürwortet er ein weites Verständnis des Begriffs der Entscheidung, Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 38–39 – *SCHUFA Holding*. Maßgeblich sei, welche (tatsächlichen und rechtlichen) Folgen der algorithmische Output für die betroffene Person zeitigt. Ob eine Entscheidung vorliegt, lasse sich daher nicht allgemein feststellen, sondern sei mittels Einzelfallprüfung zu ermitteln. Siehe eingehend Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 38–40 – *SCHUFA Holding*.

[41] Erwägungsgrund 71 S. 1.

[42] Siehe Kapitel 4 B. III. 4. B) cc) (2) sowie Kapitel 4 B. IV. 3.

[43] Konkret war der Generalanwalt mit der Frage befasst, ob bei Einsatz von Auskunfteien bereits die Erstellung des Kreditscores durch die Auskunftei eine ausschließlich automatisierte Entscheidung darstellt oder erst die Entscheidung durch das Kreditinstitut anhand des durch die Auskunftei übermittelten Kreditscores. Hierfür stellt der Generalanwalt eine wertende Gesamtbetrachtung an und bejaht im Ergebnis diese Frage. Denn in der Praxis gibt der Kreditscore wesentlich die Entscheidung vor. Vgl. ausführlich Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 44–46 – *SCHUFA Holding*.

[44] Siehe hierzu Kapitel 4 B. II. 3. a) bb) und Kapitel 4 B. III. 4. B) cc) (2).

[45] Für einen multikriterialen Ansatz sprechen sich auch *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 125–134; *Wagner*, Policy & Internet 11 (2019), 104,

Kriterien können – neben der Kompetenz zur Prüfung und Abänderung der Entscheidung[46] – etwa die intendiert, typische und individuelle Nutzung eines Dienstes,[47] die Komplexität der Entscheidung,[48] die Entscheidungsstrukturen, etwa die verfügbare Zeit und die zugänglichen Ressourcen,[49] die fachliche Kompetenz der beteiligten Person,[50] Haftungsverteilungen und Begründungspflichten,[51] das Bewusstsein von der Problematik des Automation Bias,[52] der Zugang zu den Daten, die durch das autonome System für die Entscheidung herangezogen wurden,[53] sowie die Transparenz der Systeme[54] dienen. Liegt nach dieser Einzelfallbewertung ein rechtlich relevanter Automation Bias vor, ist eine ausschließlich automatisierte Entscheidung anzunehmen, selbst wenn formal Prüfungs-, Einwirkungs- und Abänderungsbefugnisse bestehen.

---

115 f. aus. Ähnlich der Vorschlag von *Veale/Edwards*, CLSR 34 (2018), 398, 401, die für die Frage des ausschließlichen Beruhens die Vornahme einer Datenschutzfolgenabschätzung vorschlagen.

[46] So die allgemeinen Kriterien zur Einschätzung des ausschließlichen Beruhens, siehe oben unter Kapitel 4 B. II. 3. a) bb) und Kapitel 4 B. III. 4. B) cc) (2).

[47] Es geht dann nicht um die Unterscheidung anhand der originären Ausgestaltung als Entscheidungsunterstützungs- und -automatisierungssysteme, sondern um die empirisch belegte tatsächliche Nutzung der Dienste zur bloßen Entscheidungsunterstützung, falls eine Übernahme des Ergebnisses nicht stets erfolgt, oder zur Entscheidungsübernahme, falls von der Mehrheit der NutzerInnen im überwiegenden Teil der Nutzung die Vorschläge übernommen werden. Dies macht umfassende Studien notwendig. Vgl. zu diesen Überlegungen auch eingehend *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 128–132. Auf die tatsächlichen „internen Regeln und Praktiken" stellt auch der Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 44 – *SCHUFA Holding* ab.

[48] Nach Erkenntnissen der Verhaltensökonomie werden irrationale Motivationen, hier dann das blinde Vertrauen auf die algorithmische Vorgabe, vor allem bedient, wenn die Entscheidung einen hohen kognitiven Aufwand erfordert. Die Komplexität kann damit als Hinweis für das Bestehen eines automation bias dienen. Vgl. auch *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 131.

[49] *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 131; *Wagner*, Policy & Internet 11 (2019), 104, 115.

[50] *Wagner*, Policy & Internet 11 (2019), 104, 115.

[51] Der Umstand, dass der menschliche Entscheider seine Entscheidung nach außen hin begründen muss oder für seine Entscheidung haftbar gemacht werden kann, steht einer „blinden" Übernahme der maschinellen Vorgabe in der Regeln entgegen, *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 131 f.; *Wagner*, Policy & Internet 11 (2019), 104, 115.

[52] *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 132 f.

[53] *Wagner*, Policy & Internet 11 (2019), 104, 115.

[54] Je transparenter sich die maschinelle Entscheidungsfindung darstellt, desto leichter fällt die Distanzierung von der und eine Abwahl der maschinellen Vorgabe. Siehe zu diesem Kriterium auch *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 125–127.

c) Auslegung des Merkmals rechtlicher Wirkungen und sonstiger erheblicher Beeinträchtigungen

Art. 22 DSGVO sollte allein rechtlich oder faktisch nachteilige Entscheidungen erfassen.[55] Der Regulierungsbedarf wird aber nicht erst dann ausgelöst, wenn Grundrechtsgefährdungen drohen (aa)). Sinnvoll erscheint dagegen eine schärfere Konturierung des Tatbestandsmerkmals durch das Aufstellen von Abwägungskriterien (bb)).

aa) Eingrenzung auf grundrechtsgefährdende Beeinträchtigungen

Eine Interpretation des Art. 22 DSGVO, wonach allein grundrechtsrelevante Beeinträchtigungen erfasst sein sollen,[56] überzeugt nicht. Die Schwelle der Anwendung des Art. 22 DSGVO würde so erheblich hochgesetzt. Dies eröffnete zwar mehr Raum für technische Innovation, in einer derart strikten Lesart wäre dann aber eine Vielzahl tatsächlich autonomiegefährdender und damit regulierungsbedürftiger automatisierter Entscheidungen nicht abgedeckt. Im Blick auf die Steuerungseffektivität der DSGVO ist dies wenig wünschenswert.

bb) Konkretisierung nachteiliger Wirkungen durch Aufstellen von Abwägungskriterien

Das Rechtsinnovationspotential für Art. 22 DSGVO liegt dann darin, das Tatbestandsmerkmal der – nachteiligen – rechtlichen Folgen und erheblichen Beeinträchtigungswirkungen näher zu spezifizieren. Im Einzelfall kann die Abgrenzung schwerfallen, insbesondere bei nur teilweise vorteilhaften Entscheidungen, etwa bei einem nur teilweise gewährten Kredit, oder bei Entscheidungen mit unklarer Wirkung, so bei personalisierten Preisen, bei denen es an einem klaren Bewertungsmaßstab fehlt.

Zur Präzisierung bietet es sich an, Kriterien für eine Einzelfallabwägung aufzustellen (deduktiver Ansatz) oder bestimmte Referenzkonstellationen exemplarisch vorzuführen (induktiver Ansatz).[57] Hier ist vor allem der Europäische Datenschutzausschuss gefragt.[58] Auch selbstregulative Maßnahmen,

---

[55] Siehe oben Kapitel 5 B. I. 1. a) cc).

[56] Zu diesem Vorschlag etwa *Geminn/Roßnagel*, Datenschutz-Grundverordnung verbessern, 2020, S. 85; *Glatzner*, DuD 44 (2020), 312, 314.

[57] Diesen kombinativen Ansatz verfolgt der Europäische Datenschutzausschuss bzw. als Vorgängerin die Artikel 29 Datenschutzgruppe auch andernorts, so etwa bei der Zweckbestimmung, vgl. *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013.

[58] Der Europäische Datenschutzausschuss hat zu automatisierten Entscheidungen bereits Leitlinien aufgestellt, siehe *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018. Diese sind aber recht unpräzise, zudem nicht spezifisch an Regulierungsbedarfe autonomer Systeme angepasst.

etwa in Gestalt von Verhaltensregeln nach Art. 40, 41 DSGVO erscheinen sinnvoll.

Als derartige Kriterien sind unter anderem denkbar der Inhalt und die Bedeutung der erstrebten Ware oder Dienstleistung (zB Daseinsvorsorge, Relevanz für die individuelle Lebensgestaltung), der Inhalt der getroffenen Entscheidung im Vergleich zur erwünschten Entscheidung (zB vollständige Verweigerung, teilweise Zusage oder Zusage nur unter belastenden Umständen, Zusage unter Umständen, die die betroffene Person faktisch von einem Vertragsschluss ausschließen, etwa durch überhöhte Preise), die Verfügbarkeit und Zugänglichkeit von Alternativen, individuelle Umstände (zB Notlage, finanzielle Engpässe), subjektive Merkmale und die Motivationslage des Verantwortlichen (zB gezieltes Ausnutzen einer Notlage), diskriminierungsrelevante Merkmale sowie technikbezogene Umstände (Fehleranfälligkeit, Maß und Umfang der Transparenz und Einwirkungsmöglichkeit).[59] Die Versagung eines Kredits für einen Hausbau oder für die Ausbildungsfinanzierung aufgrund der Zugehörigkeit zu einer geschützten Minderheit ist dann als automatisierte Entscheidung mit erheblicher Beeinträchtigungswirkung zu werten. Dagegen erscheint eine personalisierte Preisbildung für eine Zeitschrift, bei der die betroffene Person aufgrund ihres Zugangsgeräts einen höheren Preis zahlen muss als im analogen Handel, in der Regel nicht belastend und unterfällt daher dem Art. 22 DSGVO nicht.

3. De lege ferenda

Zur effektiven Einfassung autonomer Systeme bedarf es einer eigenständigen Regulierung des Profilings (a)). Hinsichtlich Art. 22 DSGVO sollte der Unionsgesetzgeber klarstellen, dass nur nachteilige Entscheidungen erfasst sind. Im Übrigen sollte die Vorschrift auf teilautomatisierte Entscheidungen erstreckt werden (b)). Die Modellbildung ist, wie ausgeführt, nicht eingeständig zu regulieren.[60]

a) Regulierung des Profilings

Eine Regulierung des Profilings ist bislang nur annexhaft zu automatisierten Entscheidungen entworfen und damit unzureichend. Die DSGVO sollte daher eigenständige Vorschriften zur Profilbildung vorsehen.[61] Welche Schutzinstru-

---

[59] Vgl. zu ähnlichen Merkmalen im Rahmen personalisierter Preisbildung Paal/Pauly, DS-GVO/*Martini*, Art. 22 Rn. 27a sowie allgemein Wolff/Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 38–40.

[60] Siehe oben Kapitel 5 B. I. 1. a) aa).

[61] Dies wird in der Literatur gemeinhin befürwortet, siehe nur *Lorentz*, Profiling, 2019, S. 335; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 280 f.; *Moos/Rothkegel*, ZD 6 (2016), 567. Vgl. auch *Martini*, Blackbox Algorithmus, 2019, S. 340; *Kugelmann*, DuD 40 (2016), 566, 569 f.

mente dabei sinnvoll sind, bedarf vertiefter Untersuchung. Im Rahmen dieser Untersuchung soll eine profilspezifische Ausgestaltung des Rechtmäßigkeits- sowie des Transparenzgrundsatzes untersucht werden.

b) Regulierung teilautomatisierter Entscheidungen: Aufnahme auch teilautomatisierter Entscheidungen

Eine Aufhebung der einschränkenden Tatbestandsmerkmale der rechtlichen Wirkung und erheblichen Beeinträchtigung ist nicht geboten (aa)). Innovationspotentiale liegen vor allem in der Erfassung teilautomatisierter Entscheidungen (bb)).

aa) Keine Aufhebung des Merkmals rechtlicher Wirkungen und erheblicher Beeinträchtigungen

Wie ausgeführt, ist eine Streichung des Merkmals der rechtlichen Wirkungen und erheblichen Beeinträchtigungen in Art. 22 DSGVO sinnvoll. Auch eine Erstreckung auf vorteilhafte automatisierte Entscheidungen ist nicht geboten, dies sollte der Unionsgesetzgeber klarstellen.

bb) Ersetzung der Ausschließlichkeit durch Kausalität

Die Beschränkung des Art. 22 DSGVO auf Entscheidungen, die ausschließlich auf automatisierten Datenverarbeitungen beruhen, entspricht nicht mehr den Regulierungsbedarfen der technischen Wirklichkeit. Denn autonome Systeme werden vielfach als bloße Entscheidungsunterstützungssysteme eingesetzt.[62] Dennoch wirken gerade auch in diesen Fällen die Gefahren automatisierter Entscheidungen, nämlich Fehleranfälligkeiten, Diskriminierungen, Intransparenz und fehlende Anfechtungsmöglichkeit.[63] Vor allem kann in dieser Fassung des Art. 22 DSGVO das Phänomen des Automation Bias nicht reguliert werden. Der oben dargestellte Vorschlag eines materiellen Verständnisses der

[62] So auch *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 133; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192. So dient etwa in der Praxis vielfach ein errechneter Kreditscore nur als eines von mehreren Kriterien in der menschlichen Entscheidungsfindung über eine Kreditvergabe.

[63] Ebenso *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192: „Das Schädigungspotential algorithmendeterminierter Entscheidungssysteme, die ursprünglich das Leitbild des Art. 22 DSGVO gebildet hatten, unterscheidet sich insbesondere nicht kategorial von demjenigen vieler algorithmengetriebener Entscheidungssysteme. Dafür ist auch die Neigung menschlicher Akteure, Empfehlungen algorithmischer Systeme schlicht zu übernehmen und bestehendes Ermessen nicht auszuüben, mitverantwortlich". Vgl. auch *Geminn/Roßnagel*, Datenschutz-Grundverordnung verbessern, 2020, S. 84; *Glatzner*, DuD 44 (2020), 312, 313; *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 133 f.

Ausschließlichkeit bietet zwar einen gewissen Ansatz; eine Erweiterung des Art. 22 DSGVO auf teilautomatisierte Entscheidungen bietet allerdings ein höheres Maß an Rechtssicherheit.

Das Kriterium der Ausschließlichkeit ist daher zu streichen.[64] Ein Regulierungsbedarf für teilautomatisierte Entscheidungen besteht allerdings nur, wenn sich deren Risiko in der konkreten Entscheidung auch tatsächlich realisiert. Um dies abzusichern, kann ein Kausalitätskriterium eingeführt werden: Immer dann, wenn die Entscheidung im Sinne einer conditio sine-qua-non ohne den maschinellen Beitrag anders ausgefallen wäre, liegt eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO vor.[65] Dies macht eine kontextuelle Einzelfallprüfung notwendig, bei der die Kriterien, wie sie oben für den Automation Bias entwickelt wurden, herangezogen werden können. Diese Lösung geht zwar mit einer gewissen Rechtsunsicherheit einher, berücksichtigt aber, dass die Automatisierung je nach Anwendungskontext das Entscheidungsergebnis ganz unterschiedlich beeinflussen kann. Zugleich erlaubt dies einen angemessenen Ausgleich zwischen den kollidierenden Interessen der betroffenen Person und des Verantwortlichen sowie zwischen Innovationsermöglichung und -eingrenzung.

Demgegenüber ist es nicht überzeugend, Konstellationen, in denen die automatisierte Datenverarbeitung auf irgendeine, auch nur eine marginale Weise in die Entscheidung eingeflossen ist, zu erfassen.[66] Denn dann wird die automatisierungsspezifische Gefahr regelmäßig nicht durchschlagen, der Eingriff in unternehmerische Interessen und die Innovationsbeeinträchtigungswirkung wären nicht zu rechtfertigen. Eine ersatzlose Streichung des Begriffs „ausschließlich“ ist daher nicht überzeugend.

---

[64] Dies wird in der Literatur seit Längerem gefordert, siehe nur *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 98; *Geminn/Roßnagel*, Datenschutz-Grundverordnung verbessern, 2020, S. 84; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 279. So auch *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 134. Ähnlich bereits *Artikel 29 Datenschutzgruppe*, Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, 23.03.2012, S. 16.

[65] In ähnliche Richtung *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 134, die anhand einer Einzelfallbewertung verschiedene Grade der Einflussnahme des maschinellen Ergebnisses und korrespondierend ein abgestuftes Schutzkonzept vorschlägt. Eine Konkretisierung des Art. 22 DSGVO, die auch den Einbezug des automation bias und damit teilautomatisierte Entscheidungen erlaubt, fordert die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192. Sie entwickelt aber keinen präzisen Vorschlag.

[66] So aber wohl *Glatzner*, DuD 44 (2020), 312, 313; *Geminn/Roßnagel*, Datenschutz-Grundverordnung verbessern, 2020, S. 83 f.

4. Ergebnis

Jenseits des Regulierungszugriffs der DSGVO liegen das Modell und der Lösungsalgorithmus, inklusive der jeweiligen Maschinellen Lernverfahren. Denn die DSGVO adressiert allein datenverarbeitungsspezifische Risiken für subjektive Rechte der einzelnen betroffenen Person aus der Verarbeitung eines Einzeldatums, wohingegen Modell und Lösungsalgorithmus sowie Maschinelle Lernverfahren algorithmen- bzw. automatisierungsbezogene Risiken aufweisen. Es ist daher nicht überzeugend, die DSGVO auf diese zu erstrecken. Vielmehr bedarf es hierfür eigener Regulierungsinitiativen.

Demgegenüber stellt das Profiling eine datenschutzspezifische Gefahr dar: Diese liegt in der Informationsemergenz. Eine eigenständige datenschutzrechtliche Normierung des Profilings erweist sich als wesentliches Element einer Anpassung der DSGVO auf die Technologie autonomer Systeme.

Auch die Regulierung automatisierter Entscheidungen lässt sich sinnvoll in das datenschutzrechtliche Regulierungsregime integrieren, da die Intransparenz und fehlende Steuerbarkeit der algorithmischen Entscheidungsarchitektur auch zu Intransparenz und Kontrolllosigkeit der hierbei verarbeiteten Daten führt. Eine Einschränkung der Regulierung auf solche Entscheidungen, die nachteilige Effekte für die betroffene Person zeitigen, ist allerdings geboten. Denn nicht jede automatisierte Entscheidung begründet Regulierungsbedarfe. Die DSGVO kann es aber nicht leisten, diese Regulierungsbedarfe zu definieren, da diese algorithmen- und automatisierungsspezifischer Natur sind. Mit dem inhaltlich unspezifischen Merkmal der rechtlichen Wirkungen und faktischen Beeinträchtigungswirkungen ermöglicht sie eine Definition von Regulierungsbedarfen anhand außerdatenschutzrechtlicher Kriterien.

Art. 22 DSGVO ist sinnvollerweise auch auf Maßnahmen, d.h. sämtliche Outputs von autonomen Systemen mit Außenwirkung zu erstrecken. Um die verhaltensökonomische Vorwegbindung des Menschen an die maschinelle Ausgabe (Automation Bias) aufzunehmen, bietet sich im geltenden Recht an, das ausschließliche Beruhen in Art. 22 DSGVO materiell zu verstehen und anhand einer multikriterialen Abwägungsentscheidung zu bestimmen. Innovationspotentiale im geltenden Recht liegen dann vor allem in einer präziseren Umschreibung des einschränkenden Merkmals der rechtlichen Wirkungen und erheblichen Beeinträchtigungswirkungen durch das Aufstellen von Kriterien oder Erarbeiten von Referenzanwendungsfällen. Eine Einschränkung auf grundrechtsgefährdende Entscheidungen überzeugt nicht. Schließlich ist anstelle des Merkmals der Ausschließlichkeit das einer Kausalität des Beruhens der Entscheidung auf der automatisierten Datenverarbeitung einzuführen, um auch Gefährdungen durch teilautomatisierte Entscheidungen zu fassen. Auch für das Phänomen des Automation Bias böte dies eine gegenüber der Abwägungslösung elegantere und rechtsichere Lösung.

II. Reformoptionen für den Rechtmäßigkeitsgrundsatz

Die Untersuchung hat wesentliche Defizite des Rechtmäßigkeitsgrundsatzes aufgezeigt. Problematisch ist zum einen die beschränkte Ausgestaltung der Zulassungskontrolle, die sich nicht auf das Maschinelle Lernverfahren erstreckt. Zum anderen ist herausfordernd das atomistisch-partikularistische Zulassungssystem, das aufgrund der Anzahl und Komplexität der Zulassungsfragen in einer Welt autonomer Systeme erhebliche Steuerungsblockaden auslöst. Reformvorschläge liegen dabei vielfach jenseits des in dieser Arbeit definierten Innovationsrahmens (1.). Es gibt allerdings auch Innovationsvorschläge, die sich in das bestehende Datenschutzrechtssystem fügen, dabei sowohl solche diesseits (2.) und jenseits (3.) des geltenden Rechts.

1. Innovationsräume im Hinblick auf den Rechtmäßigkeitsgrundsatz

Reformbestrebungen, die auf eine Erstreckung des Rechtmäßigkeitsgrundsatzes auf das Maschinelle Lernverfahren oder Algorithmen abzielen, liegen ebenso wenig innerhalb des definierten Innovationsrahmens wie solche, die den dezentralen Steuerungsmechanismus aufheben wollen (a)). Weiterentwicklungen sind sinnvollerweise auf die Stärkung des dezentralen Zulassungsregimes auszurichten, was nicht allein Reformen des Rechtmäßigkeitsgrundsatzes notwendig macht: Vor allem die Stärkung der Transparenz ist von maßgeblicher Bedeutung (b)).

a) Inter- und intraregulative Abgrenzung: keine Einführung einer Algorithmenkontrolle und keine Umstellung auf ein zentralisiertes Zulassungsregime

Mit den Erkenntnissen zum beschränkten Regulierungsauftrag der DSGVO[67] ist eine Erstreckung des Rechtmäßigkeitsgrundsatzes und damit die Einführung einer Zulassungskontrolle von Maschinellen Lernverfahren bzw. darin gebildeter Algorithmen in der DSGVO nicht angemessen. Wohl aber ist es sinnvoll, die Profilbildung und – dort in Gestalt der Ausnahmezulassung – die automatisierte Entscheidung einer Zulassungskontrolle der DSGVO zu unterwerfen, da beide im Überschneidungsbereich algorithmen- bzw. automatisierungsspezifischer und datenschutzbezogener Regulierungsfragen liegen.

Doch auch solche Reformbestrebungen liegen jenseits des Innovationsrahmens der DSGVO, die den Regulierungsmechanismus des Rechtmäßigkeitsgrundsatzes grundlegend in Zweifel ziehen. Derartige Reformbestrebungen beziehen sich vornehmlich auf den Zulassungstatbestand der Einwilligung. In der Erkenntnis, dass der Einzelne seine Steuerungsleistung aufgrund qualitativer

[67] Siehe oben Kapitel 5 A.

und quantitativer Überforderung[68] nicht oder nurmehr bedingt erbringen kann, erscheint vielen – dies übrigens bereits vor der Etablierung autonomer Systeme – das dezentrale Regulierungsregime der DSGVO, wie es insbesondere im Rechtmäßigkeitsgrundsatz und dort der Einwilligung umgesetzt ist, als überholt.[69] Als Alternative wird ein zentralisiertes Regulierungssystem befürwortet, in dem staatlicherseits zulässige und nicht zulässige Datenverarbeitungen vorgegeben werden[70] oder eine behördliche Zulassung von Datenverarbeitungen anhand vordefinierter Kriterien erfolgt.[71] Auch Elemente regulierter Selbstregulierung, bei denen also Verantwortliche inhaltliche Richtigkeitskriterien entwickeln und die autonomen Systeme auf deren Einhaltung hin prüfen, werden diskutiert.[72] Mit dem dezentralen Regulierungskonzept der DSGVO zwischen Privaten, wonach digitale Autonomie vornehmlich durch die betroffene Person wahrzunehmen und zu schützen ist, ist dies nicht zu machen.[73]

---

[68] Die Steuerungseffektivität der Einwilligung wird aus verschiedenen Gründen, nicht allein aufgrund der quantitativen und qualitativen Überforderung der betroffenen Person, in Zweifel gezogen. Problematisch erscheint vor allem auch – siehe hierzu Kapitel 4 C. II. 2. b) – die Freiwilligkeit der Einwilligung. Die Vielschichtigkeit und Multikausalität der Steuerungsschwächen der Einwilligung bedingt aber eine Fülle an Innovationsinitiativen, die sich auf die verschiedenen Ursachen konzentrieren und mit unterschiedlichen Ansätzen aufwarten. Aus der Fülle der Literatur etwa zu verhaltensökonomischen Erwägungen *Hermstrüwer*, Informationelle Selbstgefährdung, 2015. Siehe auch *Bietti*, Pace Law Review 40 (2020), 310–398; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2021; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2012; *Sandfuchs*, Privatheit wider Willen?, 2015. Um eine umfassende Kritik der Einwilligung soll es in der vorliegenden Arbeit aber nicht gehen, entsprechend wird nachfolgend auch nur ein Ausschnitt möglicher Reformen für den Zulassungsgrund der Einwilligung vorgestellt.

[69] Aus der umfassenden Literatur siehe beispielhaft allgemein zum Einwilligungsgrundsatz *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 81–83; *Solove*, Harv. L. Rev. 126 (2013), 1880–1903; *Cate/Mayer-Schonberger*, Int. Data Priv. Law 3 (2013), 67–73; *Koops*, Int. Data Priv. Law 4 (2014), 250, 251–253; *Bietti*, Pace Law Review 40 (2020), 310–398; *Hornung*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 81, 96; siehe speziell zum Einwilligungsgrundsatz bei autonomen Systemen *Yeung*, iCS 20 (2017), 118, 125; *Bull*, Der Staat 58 (2019), 57, 94.

[70] *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 17 (2016), 315, 332, die Parallelen zum Lebensmittelrecht sowie der Regulierung von Fahrzeugen ziehen. Ebenso *Solove*, Harv. L. Rev. 126 (2013), 1880, 1902 f. Vgl. auch *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 86 f.

[71] *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 17 (2016), 315, 332. *Zarsky*, Setton Hall Law Review 47 (2017), 995, 1007 schlägt etwa ein Monitoring-System vor. Vgl. auch *Hoffmann-Riem* (Hrsg.), Big Data, 2018, S. 63.

[72] Vgl. *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 17 (2016), 315, 332.

[73] Siehe hierzu bereits eingehend Kapitel 4 A. II. 3. Vgl. auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 200 f.; *Masing*, NJW 65 (2012), 2305, 2308; *Bäcker*, Der Staat 51 (2012), 91, 105. Kritisch auch *Dornis*, ZfPW 8 (2022), 310, 322 f.

Im Verhältnis zwischen Privaten steht einem solchen Konzept zudem der Grundsatz der Privatautonomie entgegen.[74]

b) Datenschutzrechtlich konsistente Methoden zum Umgang mit fehlender Vorhersehbarkeit und individueller Steuerungsüberforderung

Innovationen des Rechtmäßigkeitsgrundsatzes, die intraregulativ konsistent sind, müssen daher auf die Stärkung des dezentralen Regulierungsregimes setzen. Wesentliche Steuerungsschwächen des Rechtmäßigkeitsgrundsatzes liegen darin begründet, dass die Verbindung von Datum und Folgen gekappt sind, da Ergebnisse und Folgen der Datenverarbeitung, sei es bei der Profilbildung, sei es bei der automatisierten Entscheidung, nicht mehr vorhersehbar sind.[75] Um diese Verbindung wiederherzustellen, ist die Transparenz hinsichtlich Verarbeitungsverfahren, Ergebnissen und Folgen ein effektives Instrument.[76] Im Übrigen liegen Steuerungsschwächen maßgeblich in der Komplexität und Anzahl der notwendigen Zulassungsentscheidungen. Es bedarf daher Mechanismen, um die Anzahl der Kontrollen zu reduzieren sowie den inhaltlichen Prüfungsanspruch herabzusenken.[77] Dies ist auf verschiedene Weise denkbar: Durch Reduktion der Kontrollhandlungen, durch Unterstützung bei oder Auslagerung der Entscheidung durch ExpertInnen, vor allem durch technische Lösungen. Dies soll sogleich im Einzelnen ausgeführt werden.

---

[74] Ebenso *Masing*, NJW 65 (2012), 2305, 2307. So auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 170. Die Freiheit der Gestaltung rechtsgeschäftlicher Verhältnisse ist zudem Garant des Binnenmarktes und Ausdruck einer auf Grundfreiheiten basierenden Marktordnung. Ein dezentrales Datenordnungssystem zwischen Privaten lässt sich daher auch als binnenmarktrechtliches Gebot verstehen. Siehe zu diesem Ansatz eingehend *ders.*, Privates Datenschutzrecht, 2020, S. 140–143.

[75] Siehe Kapitel 4 C. IV. 2. b) aa) zur Profilbildung, Kapitel 4 C. IV. 2. c) aa) zur Profilverwendung.

[76] Die Reduktion von Intransparenz, hier spezifisch die Intransparenz hinsichtlich der aus den Daten abgeleiteten Erkenntnissen über eine Person, benennt auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 366 f. als eines von vier Zielfunktionen zur Überwindung der verhaltensökonomisch bedingten Schwächen des Rechtmäßigkeits- und Einwilligungsmodells der DSGVO (Reduktion von Unwisssen, Komplexität, Trägheit und Zeithorizonten).

[77] Das Ziel der Quantitäts- und Komplexitätsreduktion der Zulassungskontrolle ist die zweite von *ders.*, Informationelle Selbstgefährdung, 2015, S. 368–370 aufgeführte Zielfunktion. Hinzu kommen noch die Zielfunktionen der Reduktion von Trägheit sowie die Reduktion von Zeithorizonten, siehe *ders.*, Informationelle Selbstgefährdung, 2015, S. 370–375. Auf die Zielfunktion der Trägheit ist unter Kapitel 5 II. 2. a) dd) und Kapitel 5 II. 3. b), auf die der Zeitreduktion ist sogleich unter Kapitel 5 II. a) bb) einzugehen.

2. *Innovationspotentiale de lege lata: Kontrollreduktion bei der Zulassungskontrolle*

Im dezentralen Regulierungsregime der DSGVO zwischen Privaten kommt der Einwilligung eine zentrale Rolle zu. Entsprechend fokussiert die Diskussion zu Reformen des Rechtmäßigkeitsgrundsatzes im Anblick der neuen Technologie der autonomen Systeme vor allem auf diesen Zulassungsgrund. Die nachfolgende Untersuchung folgt dieser Schwerpunktsetzung (a)). Weiterentwicklungsmöglichkeiten des Zulassungsgrunds der vertragsimmanenten Zulassung sowie der Interessensabwägung sollen nur knapp dargestellt werden (b)).

a) Innovationspotentiale hinsichtlich der Einwilligung

Zur quantitativen Reduktion des Steuerungsanspruchs werden sogenannte broad consent-Modelle sowie Verfahren der Einwilligungsbündelung (aa)) vorgeschlagen, die im Ergebnis allerdings nicht überzeugen. Eine risikobasierte Staffelung der Einwilligungsentscheidungen verspricht dagegen gute Lösungen (bb)). Treuhänderische Auslagerungen der Zulassungsentscheidung erscheinen nicht sinnvoll (cc)). Am Ende sind vor allem technische Lösungsansätze vielversprechend (dd)).

aa) Ansätze zur Reduktion der Einwilligungserklärungen

Zur Absenkung der Anzahl der Datenverarbeitungen werden zum einen Ansätze diskutiert, die den Umfang der Einwilligung erweitern ((1)), und solche, die eine Übertragung einer Einwilligung auf verschiedene Verarbeitungskonstellationen erlauben ((2)).

(1) Broad-Consent-Modelle

Vorgeschlagen wird, die normierte Konzeption einer breiten Einwilligung (Broad Consent), wie sie in der DSGVO für die wissenschaftliche Forschung vorgesehen ist,[78] auf sämtliche Big-Data-Analysen, dann also auch auf Maschinelle Lernverfahren, auszuweiten.[79] Die betroffene Person definiert vorab einen bestimmten Forschungsbereich oder Teile hiervon und erteilt dann ihre Einwilligung für sämtliche Datenverarbeitungen innerhalb dieses zuvor festgelegten Bereichs. Im Ergebnis überzeugt dies jedoch nicht. Der Unionsgesetzgeber rechtfertigt die Sonderregelung vor allem mit einem geringen Gefährdungspotential forschungsbasierter Datenverarbeitung: Es gelten besondere

[78] Siehe Erwägungsgrund 33.

[79] Vgl. etwa Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Gierschmann*, Art. 7 Rn. 75, die zusätzliche Schutzvorkehrungen, etwa in Form von Verhaltensregeln, fordert.

Schutzstandards,[80] zudem steht ein abstraktes, d.h. von den Einzeldaten und -personen losgelöstes Erkenntnisinteresse im Fokus.[81] Das Maschinelle Lernverfahren stellt sich ganz anders dar. Zudem ist fraglich, ob es bei Maschinellen Lernverfahren überhaupt gelingt, hinreichend präzise Bereiche für einen broad consent zu definieren. Am Ende führt dieser Ansatz zu einer Absenkung, nicht aber zu einer Reduktion des Steuerungszugriffs.

(2) Generalisierte Einwilligungen

Als weitere Methoden zur Verringerung der Anzahl der Einwilligungsentscheidungen sind „generalisierte Einwilligungen"[82] bzw. Einwilligungsbündelungen[83] in der Diskussion. Eine für eine bestimmten Verarbeitung erteilte Einwilligung wird dabei auf sämtliche vergleichbare Datenverarbeitungen übertragen.[84] Dabei geht es um zweckübergreifende, regelmäßig dann dienste- und webseitenübergreifende Einwilligungsbündelungen.[85] Dies scheitert aber daran, dass sich eine derartige Vergleichbarkeit kaum wird bestimmen lassen: Die Risiken einer Datenverarbeitung sind regelmäßig an einen bestimmten Zweck gebunden,[86] und hängen von den spezifisch verarbeiteten Daten, der

[80] Diese sind nicht allein datenschutzrechtlicher Natur. Hierauf weist auch Erwägungsgrund 33 S. 2 explizit hin.

[81] Sie entspricht damit der statistischen Auswertung, die nach Art. 5 Abs. 1 lit. b) HS. 2 DSGVO privilegiert ist. Dass und weshalb das Modell kein statistisches Verfahren darstellen kann, ist umfassend dargelegt worden, siehe hierzu Kapitel 4 C. IV. 1. a) bb) (1). Die Argumente lassen sich entsprechend übertragen.

[82] *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 138.

[83] So etwa *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 7. Kritisch dagegen *Solove*, Harv. L. Rev. 126 (2013), 1880, 1901 f., der auf die Unterschiedlichkeit der Einwilligungsentscheidungen hinweist, die einer generalisierend-vereinheitlichen Aufbereitung entgegensteht.

[84] In Art. 35 Abs. 1 S. 2 DSGVO ist ein derartiger Ansatz bereits in die DSGVO anerkannt: Eine Datenschutzfolgenabschätzung für bestimmte Verarbeitungsvorgänge gilt auch für andere mit ähnlich hohen Risiken; für diese muss dann eine eigenständige Datenschutzfolgenabschätzung nicht mehr vorgenommen werden. Siehe auch Erwägungsgrund 92. Notwendig ist ein übergreifender geteilter Zweck, der die einzelnen Datenverarbeitungen bündelt. *Artikel 29 Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.04.2017, zuletzt überarbeitet und angenommen am 04.10.2017, S. 8. Vgl. hierzu Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/*Karg*, Art. 35 Rn. 18.

[85] So wird etwa darüber nachgedacht, dass die betroffene Person webseiten- bzw. dienstübergreifende Tracking-Maßnahmen durch denselben Tracking-Provider durch eine einzige Einwilligungserklärung zulassen können sollte. Vgl., dort im Rahmen der Überlegungen zur Automatisierung der Einwilligungserklärung, *Jakobi/Stevens/Seufert u.a.*, i-com 19 (2020), 31, 40.

[86] Vgl. bereits für die Risikoähnlichkeit nach Art. 35 Abs. 1 S. 2 DSGVO, wonach Voraussetzung für die Ähnlichkeit der identische Zweck ist, vgl. Simitis/Hornung/Spiecker gen.

verwendeten Verarbeitungstechnologie und -methodik oder den Verwendungs- und Nutzungsoptionen eines ganz bestimmten Dienstes ab.[87] Schon das Risiko der Datenverarbeitung einer Informationsplattform wird kaum mit dem einer anderen vergleichbar sein. Auch die Person des Verantwortlichen wird für die Risikobestimmung entscheidend sein. Echte Bündelungseffekte jenseits der Zweckbestimmung sind im Ergebnis kaum denkbar.

bb) Staffelung der Einwilligung

Anstelle einer zahlenmäßigen Reduktion wird vorgeschlagen, die notwendigen Einwilligungen zeitlich zu staffeln (graduated consent) ((1)). Begreift man dieses Einwilligungsmodell risikobasiert, erscheint dies als sinnvolles Instrument zur Effektivierung der Einwilligungssteuerung ((2)).

(1) Zeitliche Einwilligungsstaffelung (Graduated Consent)

Das Information Commissioner's Office führt das Modell einer Einwilligungsstaffelung (Graduated Consent) ein.[88] Hierbei wird die Einwilligung nicht bei Einrichtung des Systems für alle Datenverarbeitungen während seines gesamten Lebens- und Verarbeitungszyklus erteilt, vielmehr wird die Einwilligung immer nur dann angefordert, wenn sich eine konkrete Verarbeitung eines Da-

---

Döhmann, DS-GVO/*Karg*, Art. 35 Rn. 18–19; Paal/Pauly DS-GVO/*Martini*, Art. 35 Rn. 21; *Artikel 29 Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.04.2017, zuletzt überarbeitet und angenommen am 04.10.2017, S. 8.

[87] Vgl. für Art. 35 Abs. 1 S. 2 DSGVO Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 35 Rn. 18–19; *Artikel 29 Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.04.2017, zuletzt überarbeitet und angenommen am 04.10.2017, S. 8.

[88] *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 30.

Eine Zeitaktualisierung der Einwilligung – wie dann auch der Datenschutzinformation – befürworten auch *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 6, 8; *Solove*, Harv. L. Rev. 126 (2013), 1880, 1902. In eine ähnliche Richtung geht der Vorschlag von *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 369 hinsichtlich der Einwilligung in Zweckänderungen. Er schlägt eine zahlenmäßige Begrenzung für Sekundärverwendungen und Weitergabe von Daten vor: So sollen derartige Sekundärnutzungen nur bis zu einer bestimmten Anzahl in die primäre Zweckbestimmung und Einwilligungsentscheidung aufgenommen werden. Ab Überschreiten einer bestimmten zahlenmäßigen Schwelle soll die Primäreinwilligung nicht mehr gelten und für diese Sekundärnutzungen eine eigenständige Einwilligung erteilt werden. Auch hier geht es letztlich um eine Aufteilung der Zulassung von Datenverarbeitungen – hier dann der Weiterverarbeitungen – in überschaubare(re) Einzelpakete.

tums herauskristallisiert und konkret beschreiben lässt.[89] Das Rechtmäßigkeitsprinzip wird als kontinuierliche Pflicht konzipiert, die immer dann und immer wieder neu ausgelöst wird, sobald sich (neue) Verarbeitungsfragen konkretisieren.[90] Dies verringert den kognitiven Anspruch hinsichtlich der Erteilung einer jeden Einwilligung:[91] Die einzelnen Datenverarbeitungen werden in kleinere, dann überschaubare Verarbeitungspakete unterteilt. Zudem wird die Prädiktionsspanne zwischen Datenfreigabe und Folgen der Datenverarbeitung verkürzt, schließlich die Zulassungsfragen immer erst dann gestellt, wenn sie für die betroffene Person virulent werden. Was zunächst wie eine Erhöhung der Anzahl der notwendigen Zulassungsentscheidungen erscheint, ist tatsächlich nur eine zeitliche Streckung.

Die Idee einer Staffelung der Einwilligungserklärungen erscheint vielversprechend, es bleibt jedoch offen, nach welchen Kriterien die Staffelung erfolgen soll. Das Informations Comissioner's Office unterteilt die Datenverarbeitungspakete nach der Art der Verwendung der Daten („use of data").[92] Dies ist allerdings kein in der DSGVO bekanntes Kriterium.

(2) Risikobasierte zeitliche Einwilligungsstaffelung

Sinnvoll erscheint die Einführung eines risikobasierten Separierungsmerkmals.[93] Jedes Verarbeitungspaket wird dann danach definiert, ob die Datenverarbeitung ein eigenständiges relevantes Risiko aufwirft. Dieser Risikotest kann anhand der Kriterien, wie sie für den Inkompatibilitätstest in Art. 6 Abs. 4

---

[89] *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 30. Einher geht dies mit aktualisierten Zweckbestimmungen und Datenschutzerklärungen („just in time notifications").

[90] *Dass.*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 30: „[P]eople can give consent or not to different uses of their data throughout their relationship with a service provider, rather than having a simple binary choice at the start".

[91] Es handelt sich also um eine Methode, mit der sowohl die Komplexität als auch die Zeithorizonten der Einwilligung einer Datenverarbeitung reduziert werden können. Zu diesen Zielfunktionen eines rationalitätsfördernden Datenschutzrechts *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 368–370, 373–375.

[92] *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 30 („different use of their data"). Als Beispiel wird die Datenweitergabe an Dritte angeführt. Plant der Verantwortliche die Weitergabe der Daten, muss er die Einwilligung hierfür nicht zu Beginn der Datenverarbeitung bei der betroffenen Person erfragen, sondern erst, sobald er tatsächlich die Daten mit Dritten teilt.

[93] Siehe allgemein zur Integration eines risikobasierten Ansatzes in den Rechtmäßigkeitsgrundsatz Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 14. Zu den Potentialen des risikobasierten Ansatzes der DSGVO allgemein *Veil*, ZD 5 (2015), 347–353; *Gellert*, EDPL 2 (2016), 481.

DSGVO[94] sowie für die Datenschutzfolgenabschätzung nach Art. 35 DSGVO[95] entworfen wurden, erfolgen.

Bei der Modell- sowie Profilbildung liegt das maßgebliche Risiko, wie ausgeführt, in deren Inhalt sowie in der geplanten Verwendung. Sollen hierbei neue Erkenntnisse analysiert werden, etwa zunächst nur Erkenntnisse demographischer Natur, dann auch Erkenntnisse zum emotionalen Zustand,[96] muss hierfür zeitaktuell eine eigenständige Einwilligung eingeholt werden. Auch wenn das Profil zunächst nur für die Informationsfilterung vorgesehen ist, dann aber auch für die personalisierte Werbung verwendet werden soll,[97] bedarf es einer eigenständigen Einwilligung. Bei der Profilverwendung ergeben sich neuartige Risiken, wenn das Profil für verschiedene Dienste oder innerhalb desselben Dienstes für verschieden Applikationen verwendet werden soll. Wird etwa der personalisierten Werbung für bestimmte Produkte zugestimmt, bedarf es einer neuen Einwilligung, wenn diese Werbung später auch auf Produkte jenseits der ursprünglichen Produktpalette erstrecken soll.

Das Komplexitätsreduktionspotential dieser risikobasierten zeitlichen Staffelung zeigt sich vor allem, wenn – wie dies in der Praxis üblich sein wird – betroffene Personen ihre Einwilligung in das autonome System insgesamt erteilen sollen, dann also zugleich in die Modell- und Profilbildung sowie Profilverwendung. Anstelle von Globaleinwilligungen der betroffenen Person in das autonome System in seiner Gesamtheit, erteilt die betroffene Person dann eine eigene Einwilligung in die Modellbildung und in verschiedene Modellinhalte, anschließend in Profilbildung und dort in verschiedene Profilinhalte, schließlich in die Profilverwendung und in verschiedene Verwendungsszenarien – und dies instantan, d.h. in dem Zeitpunkt, in dem die jeweilige Verarbeitungsstufe erreicht wird.

---

[94] Siehe hierzu oben Kapitel 4 C. II. 1. b) aa).

[95] Eingehend Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Karg*, Art. 35 Rn. 33–55; Paal/Pauly, DS-GVO/*Martini*, Art. 35 Rn. 15–20. Siehe hierzu auch Erwägungsgrund 91, in dem einige Risikokonstellationen benannt sind.

[96] Dies muss in der Zweckbestimmung zuvor angegeben sein, andernfalls handelt es sich um eine Zweckänderung. Bei der zeitlichen Staffelung sind also sämtliche Zweckbestimmungen von Anfang an in die Zweckbestimmung aufgenommen; allein die Zulassungsanfrage bei der betroffenen Person erfolgt erst zu dem Zeitpunkt, in dem die jeweilige (zweckgeänderte) Datenverarbeitung tatsächlich erfolgt. Zweckbestimmung und Einwilligungsanfrage fallen so auseinander: Die Zweckbestimmung erfolgt zu Beginn der Datenverarbeitung, dann für den gesamten Verarbeitungszyklus, die Einwilligung – dann nochmals mit eigener Information gerade über diesen Zweck – erst unmittelbar vor der jeweiligen Datenverarbeitung.

[97] Auch dies muss in der ursprünglichen Zweckbestimmung benannt sein, andernfalls handelt es sich um eine Zweckänderung.

cc) Auslagerung der Einwilligungsentscheidung durch treuhänderische Datenverwaltung

Eine Entlastung bei der Einwilligungsentscheidung kann auch durch Auslagerung auf Dritte erreicht werden, so ein weiterer Reformansatz. Diese Dritten, typischerweise Interessensverbände oder ExpertInnengruppen, verwalten die Daten[98] dann treuhänderisch und erteilen anstelle der betroffenen Person die Einwilligung oder nehmen andere Betroffenenrechte wahr.[99] Rechtstechnisch erfolgt dies durch eine Bevollmächtigung durch die betroffene Person.[100]

Derartige Treuhandmodelle sehen sich allerdings mit einigen rechtlichen und praktischen Herausforderungen konfrontiert. An die Bevollmächtigung sind dieselben Anforderungen hinsichtlich Bestimmtheit und Informiertheit zu stellen wie an die Einwilligung, andernfalls kann die von den Treuhändern erteilte Einwilligung nicht als bestimmt und in informierter Weise gelten.[101] Ob sich ein solches Maß an Bestimmtheit und Informiertheit für sämtliche Anwendungsfälle erreichen lässt, ist fraglich.[102] Zudem besteht die Gefahr, dass sich Wertungen des Treuhänders schrittweise anstelle der Datenschutzpräferenzen der betroffenen Person setzen oder diese sogar durch Drittinteressen unterwandert werden.[103] Im Übrigen ist noch völlig offen, inwieweit betroffene Perso-

---

[98] Diese treuhänderische Verwaltung von Daten kann nur für bestimmte Dienstleistungen, aber auch für den gesamten Datenstamm einer Person eingerichtet werden. Vgl. *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133.

[99] Vgl. hierzu *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 8; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133.

[100] In Art. 6–8 DSGVO ist dies nicht ausdrücklich vorgesehen. Gleichwohl wird eine derartige Bevollmächtigung vielfach befürwortet. So etwa Wolff/Brink, BeckOK Datenschutzrecht/*Stemmer*, Art. 7 Rn. 33; Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 31; Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Däubler*, Art. 7 Rn. 13. Ablehnend *Ernst*, ZD 7 (2017), 110, 111; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 37. In der Tendenz auch Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 7 Rn. 34, die nur eine „botenähnliche Überbringung der Einwilligungserklärung" für zulässig halten.

[101] Vgl. Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 31. Zu den Anforderungen der Bestimmtheit und Informiertheit siehe auch Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 7 Rn. 34.

[102] Kühling/Buchner, DS-GVO, BDSG/*Buchner/Kühling*, Art. 7 Rn. 31.

[103] *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133. Ganz grundlegend wird auch kritisiert, dass sich die betroffenen Personen durch die Kontrollauslagerung ihrer Entscheidungsverantwortung entziehen könnten. Vgl. zu paternalistischen Tendenzen der Auslagerung von Betroffenenrechten an Dritte, dort hinsichtlich der Verbandsklage ohne den Willen der betroffenen Person, Kühling/Buchner, DS-GVO, BDSG/*Bergt*, Art. 80 Rn. 15.

nen überhaupt bereit wären, Datenschutzfragen auszulagern, und Märkte für diese ressourcenintensive Datentreuhand bestünden.

dd) Automatisierte Einwilligungsassistenten

Diskutiert werden schließlich technische Methoden, die betroffene Person bei der Einwilligungserteilung unterstützen.[104] Assistenzsysteme, auch bezeichnet als Personal Information Manager,[105] Einwilligungsassistenten,[106] Agentensysteme,[107] Smart Defaults,[108] oder Consent Intermediaires,[109] sollen die Einwilligung automatisiert entsprechend den Datenschutzvorgaben der betroffenen Person erteilen.[110] Es handelt sich um Softwareprogramme, etwa Apps oder Plug-ins, die Datenschutzbedingungen eines Dienstes maschinell auslesen und mit den Datenschutzpräferenzen der betroffenen Person abgleichen.[111] Kommt

---

[104] Dieses Modell befürworten etwa *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 8; *Jakobi/Stevens/Seufert u.a.*, i-com 19 (2020), 31, 40; *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 21. Sehr allgemein *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 46; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133. Angedeutet wird dies schließlich auch vom *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 04.05.2020, S. 23, der die Entwicklung von Einwilligungserklärungen via Browsereinstellung anregt. Siehe überdies *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 30 f.; *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 46. Im Rahmen von PIMS *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 8 f. Vorgeschlagen wird auch, die Einwilligungsassistenz nur für bestimmte, risikoarme Teilbereiche zuzulassen. Vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 371 f. In diese Richtung auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 71.

[105] *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133.

[106] Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 38.

[107] *Jakobi/Stevens/Seufert u.a.*, i-com 19 (2020), 31, 40; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133.

[108] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 372 f.

[109] So *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 5.

[110] Zur Frage, ob ein automatisiertes Einwilligungssystem seinerseits eine zulassungsbedürftige automatisierte Entscheidung nach Art. 22 DSGVO darstellt, siehe *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 46; *Riechert*, Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, Dezember 2016, S. 67 f. In diesem Falle bedürfte es eines Vertrags zwischen dem Anbieter eines automatisierten Entscheidungsassistenten und der betroffenen Personen, ihrer Einwilligung oder einer unionalen oder nationalen gesetzlichen Zulassung.

[111] Rechtstechnisch handelt es sich nicht um eine Bevollmächtigung, vielmehr fungiert der Einwilligungsassistent als bloßes Erklärungsmedium. Die Einwilligungserklärung bleibt

es zu Diskrepanzen zwischen den vorgegebenen Datenschutzpräferenzen der betroffenen Person und den Datenverarbeitungsbedingungen des Verantwortlichen kann entweder Zugang zu diesem Dienst gesperrt,[112] eine Warnung ausgesprochen oder eine explizite Einwilligung bei der betroffenen Person erfragt werden.[113]

Die Vorgaben für die Einwilligungserteilung, d.h. die individuellen Datenschutzpräferenzen kann die betroffene Person manuell, etwa durch Schnittstellen oder Dashboards, eingeben.[114] Möglich ist aber auch, dass das System die Bedingungen einer anderweitig bereits erteilten Einwilligung abspeichert und übernimmt.[115] Noch weiter gehen Automatisierungsmethoden unter Einsatz Maschineller Lernverfahren, in denen das System eigenständig durch Analyse des Verhaltens der betroffenen Person, etwa ihres Browsingverhaltens, die Datenschutzpräferenzen ermittelt.[116] Denkbar ist schließlich die Integration von datenschutzrechtlichen Einschätzungen Dritter, etwa von Interessensverbänden oder sonstigen ExpertInnen.[117] Diese Systeme versprechen neben der bloßen Unterstützung bei der Einwilligungserteilung eine Stärkung der Datenschutzkompetenz betroffener Personen: Noch vor der Verwendung digitalisierter Dienste werden sie zur Reflexion über eigene Datenschutzpräferenzen angeregt,[118] zudem ermöglicht der Überblick über abgespeicherte Datenschutzpräferenzen deren kritische Prüfung.[119]

---

der betroffenen Person zurechenbar. Siehe nur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 38.

[112] Diese Lösung befürwortend *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 30 f. Zu diesem Modell siehe auch *Hermstrüwer*, in: Hoffmann-Riem (Hrsg.), Big Data, 2018, S. 99, 114; *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 5.

[113] Einen umfassenden Überblick über verschiedene Verfahren bieten *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 10.

[114] *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41 f.

[115] Vgl. *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 372 f.

[116] Siehe eingehend *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 6. Ein derartiges Modell zur datenschutzbezogenen Personalisierung und Automatisierung, ergänzt um ein Vorschlagssystem, präsentieren etwa *Stach/Steimle*, in: Association for Computing Machinery (Hrsg.), The 34th Annual ACM Symposium on Applied Computing, April 8–12, 2019, 2019, S. 1500. Zur technischen Methodik datenschutzbezogener Profilbildung siehe ausführlich *Wisniewski/Knijnenburg/Lipford*, Int. J. Hum. Comput. 98 (2017), 95–108 Siehe zur datenschutzrechtlichen Personalisierung auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 372 f.

[117] Vgl. *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 6.

[118] Hierauf weisen auch *Jakobi/Stevens/Seufert u.a.*, i-com 19 (2020), 31, 40 hin.

[119] *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 7.

Gleichwohl stellen diese Assistenzsysteme auch vor einige rechtliche und tatsächliche Herausforderungen. Diesen kann im Ergebnis aber durch technische Verfahren sowie rechtliche Vorgaben begegnet werden. Herausfordernd ist vor allem die Bestimmtheit der Einwilligung. Die von der betroffenen Person vordefinierten Datenschutzpräferenzen, vor allem hinsichtlich des Zwecks, müssen so präzise sein, dass die auf diesen basierenden automatisiert erteilten Einwilligungen ihrerseits als hinreichend bestimmt gelten können.[120] Hier bietet es sich an, Assistenzsysteme nur für bestimmte Bereiche, etwa für einzelne soziale Netzwerke oder personalisierte Werbemaßnahmen eines bestimmten Unternehmens,[121] zuzulassen. Problematisch ist überdies, wenn im Einzelfall atypische Datenverarbeitungskonstellationen auftreten. Dem könnte über Ausnahmebestimmungen oder Beschränkungen der Assistenzsysteme auf standardmäßige Datenverarbeitungen begegnet werden.[122] Soweit die Systeme eigenständig die Datenschutzpräferenzen der betroffenen Personen ermitteln, muss abgesichert sein, dass diese dem tatsächlichen und aktuellen Willen der betroffenen Person entsprechen. Dies kann durch Mechanismen der Gegenprüfung[123] sowie der Aktualisierungssicherung erfolgen.[124] Zudem müssten Schutzmechanismen vorgesehen werden, die den Missbrauch der Einwilligungsassistenten durch Dritte, auch durch den Verantwortlichen selbst, verhindern.[125]

Im Ergebnis bieten Einwilligungsassistenten gute Lösungen für die Kontrollüberforderung der betroffenen Person. Hinsichtlich der technischen Umsetzung und einer sinnvollen rechtlichen Einkleidung bestehen allerdings noch einige Forschungsbedarfe. Für eine rechtssichere Integration von Einwilli-

---

[120] Vgl. *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133; *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 12; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 38, 71. Siehe auch *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 45. Aus Gründen der Bestimmtheit lehnt die Einführung eines Einwilligungsassistenten generell ab Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 38, 71.

[121] So *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 134.

[122] *Jakobi/Stevens/Seufert u.a.*, i-com 19 (2020), 31, 40.

[123] So auch *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 9. Vgl. auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 373.

[124] Die Notwendigkeit der Absicherung der Aktualität der Datenschutzpräferenz betonen auch *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 37, 40; *Riechert*, Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, Dezember 2016, S. 60, 71; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 373.

[125] Vgl. *Lehtiniemi/Kortesniemi*, Big Data and Society 4 (2017), 1, 10. Siehe auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133 f.

gungsassistenten in die DSGVO wäre ein Tätigwerden des Europäischen Datenschutzausschusses wünschenswert, Verantwortliche könnten aber auch selbst über die selbstregulativen Instrumente der DSGVO für ein höheres Maß an Rechtsklarheit sorgen.[126]

b) Innovationspotentiale hinsichtlich der vertragsimmanenten Zulassung und der Interessensabwägung

Hinsichtlich der übrigen Zulassungsgründe erscheint vor allem eine Automatisierung der vertragsimmanenten Zulassung (aa)) sowie eine Konkretisierung der Interessensabwägung für Datenverarbeitungen durch autonome Systeme (bb)) sinnvoll.

aa) Automatisierung der Zulassung: Smart Contracts, aber keine Automatisierung der Interessensabwägung

Auch in der Vertragsbeziehung sowie bei der Interessensabwägung ist der Einsatz von Assistensystemen denkbar. In der Vertragsbeziehung versprechen vor allem Smart-Contract-Systeme gute Lösungen.[127]

Eine Automatisierung der Interessensabwägung muss dagegen aus technischen Gründen ausscheiden. Denn mit den aktuellen Techniken ist es (noch) nicht möglich, einzelfallbezogene Wertungsfragen mit guten Ergebnissen in ein algorithmisches, d.h. metrisierbar-stochastisches Berechnungssystem zu übertragen. Schon ganz grundsätzlich stehen sich die algorithmische Verarbeitungsmethodik, die auf Standardisierung und Metrisierung ausgerichtet ist, und die an der Einzelfallgerechtigkeit orientierte Interessensabwägung, die durch die Merkmale der Atypik, Flexibilität und Dynamisierung geprägt ist, entgegen.[128] Allenfalls für Standardentscheidungen, bei denen tatsächlich einige wenige Parameter mit klaren Gewichtungen maßgeblich sind, ist dies denkbar. Dort besteht dann aber kein Bedarf für Entlastung der Verantwortlichen bzw. Behörden.

bb) Inhaltliche Präzisierungen der Interessensabwägung

Um die Interessensabwägung zu erleichtern, bietet es sich dagegen an, die Bewertungskriterien und Abwägungstendenzen hinsichtlich autonomer Systeme

---

[126] Eine legislative Aufnahme von Assistenzsystemen in die DSGVO fordern dagegen Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Klement*, Art. 7 Rn. 71.

[127] Vgl. eingehend *Merlec/Lee/Hong u.a.*, Sensors 21 (2021).

[128] Siehe hierzu bereits unter Kapitel 2 A. II. 2. b), Kapitel 2 C. II. 3. Siehe allgemein zu den Grenzen automatisierter Systeme bei komplexen Abwägungsentscheidungen, dort dann im Rahmen staatlicher Entscheidungen, *Martini/Nink*, NVwZ 36 (2017), 1, 2; *Ernst*, JZ 72 (2017), 1026, 1028.

präzise(r) zu fassen.[129] Überdies erhöht sich so die Rechtssicherheit. Hier kann man entweder deduktiv durch das Aufstellen von Kriterien oder induktiv durch Auswertung typisierter Anwendungskonstellationen vorgehen.[130] Dies sollte risikobasiert erfolgen.[131] Hinsichtlich der aufzunehmenden Kriterien kann man sich auf die vom Europäischen Datenschutzausschuss und der Literatur für die Interessensabwägung entwickelten Merkmale stützen, wie sie auch in Kapitel 4 C. aufgeführt wurden.[132] Es geht dann vor allem darum, diese präzise zu benennen und zu gewichten und spezifisch auf autonome Systeme in bestimmten Anwendungskontexten auszuformen. Hinsichtlich der Profilbildung sind relevante Kriterien etwa die Sensibilität der Profilinhalte, deren Diskriminierungs- und Fehleranfälligkeit sowie die Vorhersehbarkeit von Einzelinferenzen sowie schließlich der Anwendungskontext, aus dem sich ergibt, inwieweit sich die in den Informationsemergenzen der Profilbildung angelegten Autonomiegefährdungen und Diskriminierungen realisieren. Bei der Profilverwendung spielen neben den auch hier relevanten profilbildungsbezogenen Kriterien vor allem die Transparenz und Vorhersehbarkeit der automatisierten Entscheidung oder Steuerungen und die nachteilige Wirkung für den Einzelnen, insbesondere Diskriminierungen und Fehleranfälligkeiten eine Rolle.

Zur Darstellung typisierter Fallgestaltungen bedarf es einer Auswahl geeigneter Anwendungen autonomer Systeme, die sowohl standardmäßig zur Anwendung kommen als auch typisierende Betrachtungen zulassen. Die Referenzbeispiele, wie sie dieser Arbeit zugrunde liegen, können ein Ansatzpunkt sein.

3. Innovationspotentiale de lege ferenda

Weiterentwicklungen des Rechtmäßigkeitsgrundsatzes, die sich an den Unionsgesetzgeber richten, sind insbesondere solche, die das Profiling betreffen (a)). Vor allem geht es dann um Rechtsinnovationen, die den Zulassungsgrund der Einwilligung betreffen. Diskutiert werden hier vor allem technische Ver-

---

[129] Allgemein eine klarere Konkretisierung fordern Kühling/Buchner, DS-GVO, BDSG/*Buchner/Petri*, Art. 6 Rn. 143. So auch Wolff/Brink, BeckOK Datenschutzrecht/*Albers/Veit*, Art. 6 Rn. 67. Vgl. auch *Lorentz*, Profiling, 2019, S. 336–338, die fehlende Konkretisierungen des Europäischen Datenschutzausschusses sowohl für die Profilbildung als auch die Profilverwendung bemängelt.

[130] Für die Interessensabwägung hinsichtlich der Profilbildung befürwortet dies auch *Lorentz*, Profiling, 2019, S. 337 f. vor. Dieser Ansatz entspricht dem Vorgehen der Artikel 29 Datenschutzgruppe bzw. des Europäischen Datenschutzausschusses in anderen Bereichen. Siehe etwa die Darstellung der Fallbeispiele bei *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 51–70.

[131] Vgl. hierzu Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Schantz*, Art. 6 Abs. 1 Rn. 107.

[132] Siehe oben Kapitel 4 C. III. 2. d) bb) sowie Kapitel 4 C. III. 3. a) dd).

fahren, die betroffenen Personen eine zentrale Verwaltung ihrer Daten erlauben (b)).

a) Eigenständige Zulassungsentscheidung für das Profiling

Zur Integration der Profilbildung in den Rechtmäßigkeitsgrundsatz bieten sich verschiedene Wege an. Diskutiert wird ein Verbot (aa)), die Einführung einer eigenständigen Zulassung des Profilings (bb)), eine Zulassung einzelner Profilinhalte (cc)) sowie die Einführung eigenständiger Zulassungstatbestände (dd)). Am Ende erweist sich das bestehende System, nämlich eine am Rohdatum orientiertes Zulassungskontrolle, als ausreichend. Die Problematik der Zulassung der Profilbildung stellt sich als Frage der Vorhersehbarkeit dar (ee)).

aa) Verbot des Profilings

Diskutiert wird ein generelles Verbot des Profilings,[133] vorgeschlagen werden aber auch bereichsspezifische Verbote von Profilbildungsmaßnahmen, etwa mit sensiblen Inhalten, so zB Emotional Profiling,[134] oder mit bestimmten Anwendungszielen, etwa in Gestalt eines Verbots der Verwendung von Werbeprofilen.[135] Dies überzeugt im Ergebnis aber nicht.[136] Dies verkennt schon, dass die Profilbildung ein natürlicher Prozess ist, der überhaupt erst die Kommunikation ermöglicht sowie für die Persönlichkeitsentwicklung konstitutiv ist.[137] Dass ein jedes Profiling (autonomie-)gefährdend ist, ist zudem unzutreffend. Wie die Untersuchung aufgezeigt hat, ist dies nur in bestimmten Verwendungs-

---

[133] Sydow, DS-GVO/*Sydow*, Einleitung Rn. 82–83 geht davon aus, dass die DSGVO bereits in ihrer geltenden Fassung ein Verbot des Profilings enthält, da Art. 22 DSGVO auch auf das Profiling anwendbar ist.

[134] So etwa, wenn auch im Rahmen eines Gesetzes für Künstliche Intelligenz, *Access Now*, Prohibit emotion recognition in the Artificial Intelligence Act, November 2021.

[135] *Wågström*, Why Behavioral Advertising Should Be Illegal, Forbes 05.05.2019, https://www.forbes.com/sites/forbestechcouncil/2019/03/05/why-behavioral-advertising-should-be-illegal.; *Edelman*, Why Don't We Just Ban Targeted Advertising, Wired 22.3. 2020, https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising.

[136] So im Ergebnis auch *Lorentz*, Profiling, 2019, S. 335–338; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 268 f. Siehe auch *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, S. 284, 290. Auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192 spricht sich gegen ein Verbot aus. Befürwortend Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Hermann*, Art. 4 Nr. 4 Rn. 74. Ebenso sieht der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018 in seinen Erwägungen kein Verbot des Profilings vor.

[137] Siehe hierzu Kapitel 2 A. I. 1. sowie Kapitel 4 A. II 2. Dieses Argument gegen ein Verbot führen auch *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 290.

konstellationen der Fall[138] und nur aufgrund bestimmter Umstände, insbesondere aufgrund der Intransparenz der Profilbildung und deren Inhalte.[139] Einem generellen Verbot steht aber vor allem entgegen, dass die Frage der Akzeptabilität automatisierter Profilbildungen zwischen Privaten in besonderem Maße von individuellen Wertungen und Befindlichkeiten abhängig ist und grundlegende Fragen des individuellen Lebensentwurfs anspricht.[140] Das staatlicherseits erteilte Inakzeptabilitätsattestat von (bestimmten) Profilbildungen ist damit bevormundend-paternalistisch. Ziel eines autonomiestärkenden Datenschutzes muss es damit sein, die betroffene Person zu befähigen, ihre Vorstellungen zumutbarer und nicht zumutbarer Profilbildung zu entwickeln und zu realisieren. Dies verweist auf ein dezentrales Zulassungsregime.[141]

bb) Eigenes Zulassungsregime für die Profilbildung

Eine eigene Zulassungsprüfung der Profilbildung ist nicht sinnvoll. Denn bereits mit der Zulassung eines Datums für die Profilbildung ist eine solche Entscheidung über die Profilbildung an sich getroffen.[142] Es entstehen also keine Schutzlücken. Im Übrigen liegen die wesentlichen Gefährdungen, die eine

---

[138] Siehe oben Kapitel 2 C. IV. 2. Siehe auch zum Unterschied der Profilbildung der analogen Welt und derjenigen durch autonome Systeme, aufgrund dessen Profilbildungen durch autonome Systeme sich anders darstellen und Regulierungsbedarfe begründen, Kapitel 2 A. I. 2. sowie Kapitel 2 C. IV. 2. e).

[139] Ähnlich *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 334 f. sowie *Hildebrandt/Gutwirth*, in: dies. (Hrsg.), Profiling the European Citizen, 2008, S. 365, 368.

[140] Siehe hierzu bereits Kapitel 4 A. II. 3. a).

[141] Vgl. auch *Lorentz*, Profiling, 2019, S. 184: „[E]s [wäre] bevormundend […], dem Betroffenen die Möglichkeit der Einwilligung [in die Profilbildung] zu versagen". Siehe auch *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 10, der eine dem dezentralen Regulierungsregime der DSGVO entsprechendes Rechtmäßigkeitsprinzip vorschlägt. Auf Informationsansprüche und Widerspruchsrechte der betroffenen Person stellen auch *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336; *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 290 ab. Informationspflichten hinsichtlich der Profilbildung gegenüber betroffenen Person fordert auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192.

[142] So auch *Lorentz*, Profiling, 2019, S. 184, 332. Ebenso etabliert der Europarat in seinem Entwurf kein Zulassungsregime für das Profiling, sondern legt fest, dass „the collection and processing of personal data in the context of profiling" fair, rechtmäßig und angemessen sein und einem bestimmten Zweck dienen müssen, siehe *Europarat*, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Europarat, 23.11.2013, S. 10, dort unter 3.A. Dies entspricht der Anwendung des Rechtmäßigkeitsgrundsatzes auf die im Rahmen der Profilbildung verarbeiteten Daten, also dem, was die DSGVO schon aktuell vorsieht. Vgl., wenn auch sehr allgemein, *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 290.

neue Zulassungsfrage aufwerfen, nicht in der Profilbildung an sich, sondern in den einzelnen Erkenntnissen, die hierbei erzeugt werden.

cc) Eigenes Zulassungsregime für neu generierte Daten

Auch eine eigenständige Zulassungsentscheidung hinsichtlich neu generierter Daten[143] ist nicht sinnvoll. Dies wäre schon nicht schutzverstärkend. Denn bereits bei der Zulassungsentscheidung hinsichtlich des Rohdatums für die Profilbildung erfolgt eine Angemessenheitsprüfung der neu erzeugten Daten. Eben da die Erzeugung dieser neuen Daten die maßgebliche Folge der Verarbeitung des Rohdatums in der Profilbildung ist, bezieht die Entscheidung über die Datenfreigabe auch eine Angemessenheitsprüfung der zu bildenden Profilinhalte mit ein. Eine neue Zulassungsfrage wird so mit der Erzeugung der neuen Daten gar nicht erst aufgeworfen.[144] Bei der Weiterverarbeitung der Profilinhalte bei der Profilverwendung wirkt diese Zulassungsentscheidung fort.[145] Eine Schutzlücke entsteht dann nicht. Im Übrigen wäre eine solche Pflicht zur Freigabe eines jeden erzeugten Profilinhalts mit unternehmerischen Interessen kaum vereinbar.[146] Darüber hinaus würde der betroffenen Person ein Recht zugestanden, nicht allein über Daten, sondern sogar über die Interpretation dieser Daten verfügen zu können. Mit einer freiheitlichen Kommunikationsordnung wäre dies nicht vereinbar. Ein solcher Ansatz würde dazu führen, dass die betroffene Person tatsächlich im Sinne eines absolut verstandenen informationellen Selbstbestimmungsrechts über Wissen und Zuschreibungen Dritter umfassend verfügen könnte.[147]

dd) Einführung profilspezifischer Zulassungstatbestände

Darüber hinaus besteht aber auch kein Bedarf für eigene, dann profilingspezifische Zulassungstatbestände.[148] Bereits in Art. 6 Abs. 1 DSGVO hat der Unionsgesetzgeber ein hinreichend offenes Zulassungsregime etabliert, das auch profilspezifische Wertungen einbeziehen kann. Während die dezentralen Zulassungstatbestände nach Art. 6 Abs. 1 lit. a) und lit. b) DSGVO ohnehin keine

---

[143] Vgl. zu einem solchen Vorschlag Gola, DS-GVO/*Schulz*, Art. 7 Rn. 36; Gola, DS-GVO/*Schulz*, Art. 6 Rn. 155.

[144] Eingehend *Lorentz*, Profiling, 2019, S. 184–186, 332, 335.

[145] So auch *dies.*, Profiling, 2019, S. 254.

[146] Angedeutet bei *dies.*, Profiling, 2019, S. 185.

[147] Siehe oben Kapitel 4 A. I. 2. a) sowie Kapitel 4 A. II. 3. b). Ähnliche Gedanken bei *Martini*, Blackbox Algorithmus, 2019, S. 207. Siehe auch BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 23. Juni 2020, 1 BvR 1240/14, Rn. 16: „Das allgemeine Persönlichkeitsrecht vermittelt kein Recht, in der Öffentlichkeit so dargestellt zu werden, wie es dem eigenen Selbstbild und der beabsichtigten öffentlichen Wirkung entspricht".

[148] Ebenso *Lorentz*, Profiling, 2019, S. 335–338; *Wenhold*, Nutzerprofilbildung durch Webtracking, 2018, S. 269 f.

inhaltlichen Vorgaben machen, erlaubt aber auch die inhaltlich kaum vorstrukturierte Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO profilspezifische Wertungen. Hier bietet es sich gleichwohl an, diese Interessensabwägung präziser hinsichtlich der Profilbildung zu konturieren.[149] Oben wurde bereits ausgeführt, wie dies aussehen könnte.[150]

ee) Generierung neuer Daten als Transparenzproblem

Nach all dem erfolgt die Zulassungsentscheidung über das Profiling und die einzelnen Profilinhalte effektiv und hinreichend über die Zulassungsentscheidung hinsichtlich des Rohdatums. Notwendig ist dann aber, dass Rohdatum und Profilinhalt hinreichend verknüpft, aus dem Rohdatum also mögliche Profilinhalte vorhersehbar sind. Die Zulassungsfrage hinsichtlich der Einzelinferenzen ist damit tatsächlich eine Frage der Vorhersehbarkeit und damit der Transparenz.[151]

b) Innovationspotentiale hinsichtlich der Einwilligung: Umgestaltung des Zulassungsregimes in zentrale Datenverwaltungssysteme

Weitere Innovationspotentiale liegen vor allem in technischen Methoden zur Erleichterung der Einwilligungserteilung. Oben wurden mit automatisierten Einwilligungssystemen derartige technische Verfahren vorgestellt. Der Unionsgesetzgeber könnte derartige technische Schutzmechanismen stärken, indem er sie explizit normiert und rechtsklare Bedingungen aufstellt.

Dieser technische Datenschutz ließe sich darüber hinaus effektivieren, indem nicht die Einwilligungsentscheidung und -erteilung automatisiert wird, sondern das gesamte Zulassungsregime technisch abgewickelt wird. Dem Verantwortlichen wird dann automatisiert der Zugriff auf personenbezogene Daten versperrt, wenn seine Verarbeitung nicht den Datenschutzpräferenzen der betroffenen Person entspricht. Dies bedeutet im Ergebnis einen Systemwechsel: Nicht die betroffene Person muss die Vereinbarkeit der Datenverarbeitungsbedingungen eines Verantwortlichen mit eigenen Datenschutzpräferenzen prüfen und entsprechend ihre Einwilligung erteilen oder versagen, sondern der Verantwortliche muss sicherstellen, dass seine Datenverarbeitungen den Datenschutzpräferenzen der betroffenen Personen genügen. Andernfalls können sie technisch nicht auf die Daten zugreifen. Notwendig müsste damit der faktische Erstzugriff von Verantwortlichen durch (Erst-)Erhebung unterbunden und ein bei der betroffenen Person zentralisiertes Datenmanagement eingeführt werden.

---

[149] So auch *Lorentz*, Profiling, 2019, S. 337 f.; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 4 Nr. 4 Rn. 8.

[150] Siehe Kapitel 5 B. II. 2. b) bb).

[151] So auch *Lorentz*, Profiling, 2019, S. 185, 187, 254.

Zwei Modelle erscheinen dabei besonders vielversprechend: Einmal eine technische Verknüpfung von Daten und datenschutzrechtlichen Präferenz der betroffenen Person (aa)), einmal ein zentrales Datenmanagementtool in Gestalt von Personal Information Management Systems (PIMS) (bb)).

aa) Datenschutzpräferenzen als Standardeinstellung (Sticky Policies)

Die technische Absicherung, dass der Verantwortliche nur dann Zugang zu personenbezogenen Daten einer Person erhält, wenn er deren Datenschutzpräferenzen einhalten kann, wird im technischen Bereich unter dem Begriff der Datenschutzpräferenzen als Standardeinstellung diskutiert.[152] Die Standardeinstellung dient gewissermaßen als technischer Schutzwall: Nur wenn der Verantwortliche diese Datenschutzpräferenzen einhält, kann er technisch auf die Daten zugreifen. Die Daten werden also dem Erstzugriff durch den Verantwortlichen enthoben, bei der betroffenen Person zentralisiert abgespeichert und mit der Standardeinstellung versehen. Eine technische Methode ist dabei die Verknüpfung von Daten und Datenschutzpräferenzen (Sticky Policies).[153]

Dieses Modell erscheint durchaus zukunftsfähig, auch die Artikel 29 Datenschutzgruppe befürwortet diese Technologie.[154] In rechtlicher Hinsicht stellen sich aber einige Fragen. So ist schon unklar, inwieweit Sticky Policies eine Einwilligung darstellen können.[155] Für Unsicherheit sorgt insbesondere, auf welche Weise ein Wechsel des dezentralen Zulassungsregimes des Art. 6 Abs. 1 DSGVO, das bislang anhand einzelfallbezogener Zulassungsprüfungen der vom Verantwortlichen erhobenen Daten durch die betroffene Person funktionierte, reibungsfrei zu einem Zulassungsregime ausgebaut werden kann, in dem die Daten primär der betroffenen Person zugesprochen werden, diese dann

---

[152] Eingehend *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 46 f. Die Systeme können auch so genutzt werden, dass autonome Systeme auf Seiten der betroffenen Person und des Verantwortlichen anhand der Datenschutzpräferenzen der betroffenen Person die Datenschutzbedingungen im Einzelfall aushandeln, siehe hierzu *Jakobi/Stevens/Seufert u.a.*, i-com 19 (2020), 31, 41.

[153] Zum Begriff siehe auch *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 9. Typischerweise werden hierfür Public-Key-Verschlüsselungsverfahren (Public-key Encyption) genutzt. Vgl. zum Begriff und zu gängigen Verfahren *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 47. Hierfür werden entweder die Daten(sätze) und Datenschutzpräferenzen gekoppelt oder die Datenschutzpräferenzen in Form von Protokollen hinterlegt. Vgl. unter Zitierung verschiedener Forschungsprojekte hierzu *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 11.

[154] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, 16.09.2014, S. 8.

[155] Siehe *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 47, die auf umfassende Forschungsbedarfe verweisen.

generell-abstrakt Kriterien für die Angemessenheit von Datenverarbeitungen festgelegt und am Ende der Verantwortliche die Zulässigkeit prüft. Im Übrigen stellen sich die bereits im Rahmen der Einwilligungsassistenten vorgestellten Probleme, insbesondere hinsichtlich der Bestimmtheit und Aktualisierung[156] der Datenschutzpräferenzen sowie der Überforderung der betroffenen Person.[157] Vor allem aber bestehen hinsichtlich der technischen Umsetzung noch viele offene Fragen, sodass fraglich ist, ob sich für die Sticky Policies überhaupt Märkte entwickeln würden.[158] Das tatsächliche Innovationspotential ist daher, zumindest nach dem aktuellen Stand, äußerst ungewiss.[159]

bb) Personal Information Management Systems und persönliche Datenräume

Personal Information Management Systems (PIMS)[160] stehen bereits seit Längerem auf der Forschungs- und Förderungsagenda verschiedener unionaler und

---

[156] Vgl. *Miorandi/Rizzardi/Sicari u.a.*, IEEE Transactions on Knowledge and Data Engineering 32 (2020), 2481, 2498.

[157] Betroffene Personen werden zu einer umfassenden Definition von Datenschutzpräferenzen für eine Vielzahl von Verarbeitungszwecken, -verfahren, und -konstellationen gezwungen sein, die sie tendenziell überfordern könnten. Vgl. *dies.*, IEEE Transactions on Knowledge and Data Engineering 32 (2020), 2481, 2497.

[158] Kritisch auch *Miorandi/Rizzardi/Sicari u.a.*, IEEE Transactions on Knowledge and Data Engineering 32 (2020), 2481, 2497; *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 11.

[159] Sehr kritisch auch *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 47: „[T]he proposed model cannot be a substitute of consent, but rather a facilitator for user's overall control and choice". *Miorandi/Rizzardi/Sicari u.a.*, IEEE Transactions on Knowledge and Data Engineering 32 (2020), 2481, 2497 problematisieren, dass mit den mitwandernden Datenschutzpräferenzen auch der Umfang der von den autonomen Systemen zu verarbeitenden Informationen steigt, was deren Leistungskraft mindern kann. Siehe zu weiteren technischen Herausforderungen *dies.*, IEEE Transactions on Knowledge and Data Engineering 32 (2020), 2481, 2498 f.

[160] Der Begriff der PIMS wird sehr unterschiedlich verstanden. In einem engen Verständnis werden damit technische Einrichtungen beschrieben, die der betroffenen Person eine zentralisierte Steuerung ihrer Daten in ihrer Gesamtheit ermöglichen, so etwa *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41–43; *Poikola/Kuikkaniemi/Honko*, MyData, Ministry of Transport and Communications Finland, 2015. In einem weiten Verständnis erfassen PIMS auch Datenschutzmodelle, in denen der Datenschutz an Dritte ausgelagert wird, entweder an automatisierte Systeme, so *Verbraucherzentrale Bundesverband*, Neue Datenintermediäre, Bundesverband der Verbraucherzentralen und Verbraucherverbände, 15.9.2020, S. 5 f.; *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 10, oder an (menschliche) Datentreuhänder, *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 133; ähnlich *Europäische Kommission*, An emerging offer of „personal information management services", Januar 2016, S. 15; *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal

privater Datenschutzinitiativen,[161] im Vorschlag zum DGA nehmen sie eine prominente Rolle ein.[162] PIMS stellen eine technische (Schnittstellen-)Plattform dar, auf der betroffene Personen zentral und zweck-, anwendungs- und diensteübergreifend ihre Daten in ihrer Gesamtheit verwalten können.[163] Hierzu werden die Daten zentralisiert in sogenannten Datenräumen[164] gespei-

---

Information Management (PIM), 20.10.2016, S. 8. In allen Fällen geht es um eine Zentralisierung und Abstrahierung vom einzelnen Datum, in den letztgenannten Fällen auch um eine Externalisierung der Datenkontrolle. Vgl. *Riechert*, Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, Dezember 2016, S. 48, die präzisierend von dezentralen – dann geht es lediglich um eine Zentralisierung, bei der dann die betroffene Person das Datenmanagement übernimmt – und zentralen PIMS – dann geht es um Externalisierung des Datenschutzes, das Datenmanagement wird also von Dritten durchgeführt – sprechen. Im Rahmen dieser Arbeit sind mit PIMS allein solche im engen Verständnis gemeint.

[161] *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 7; *Europäische Kommission*, An emerging offer of „personal information management services", Januar 2016, S. 18 f.; siehe auch bereits *Europäische Kommission*, Für eine florierende datengesteuerte Wirtschaft, 02.07.2014, S. 12. Befürwortend auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 140. Zu verschiedenen marktreifen Versionen von PIMS siehe *Europäische Kommission*, An emerging offer of „personal information management services", Januar 2016, S. 4–6; *Janssen/Cobbe/Singh*, Internet Policy Rev. 9 (2020), 1, 3. Siehe auch die Initiative aus Finnland mit einem umfassend ausgearbeiteten Modell: *Poikola/Kuikkaniemi/Honko*, MyData, Ministry of Transport and Communications Finland, 2015. Zu einem solchen Modell siehe etwa *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 7.

[162] Siehe Art. 5 DGA sowie Erwägungsgrund 21 des DGA.

[163] *Janssen/Cobbe/Singh*, Internet Policy Rev. 9 (2020), 1, 2. Siehe eingehend unter Vorstellung verschiedener derzeit gängiger Programme *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41–43, 63-65. Mit dem System „MyData" stellen *Poikola/Kuikkaniemi/Honko*, MyData, Ministry of Transport and Communications Finland, 2015 ein derartiges PIMS vor.

[164] Auch bezeichnet als personal data stores, personal data vaults, personal data lockers. Siehe eingehend *Europäische Kommission*, An emerging offer of „personal information management services", Januar 2016, S. 3; *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 47. Vgl. auch *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 8. Teilweise wird der Begriff der Personal Data Stores auch mit Personal Information Management Systems gleichgesetzt, siehe *Janssen/Cobbe/Singh*, Internet Policy Rev. 9 (2020), 1, 2. Diese Datenräume werden entweder lokal auf einem bestimmten Gerät oder geräte- und dienstübergreifend in einer Cloud errichtet. Bei cloudbasierten Ausgestaltungsformen gibt es sowohl Formen, bei denen die Daten in den Clouds gespeichert werden, als auch solche, bei denen die Daten in ihren ursprünglichen Quellen verbleiben und lediglich Verlinkungen erstellt werden. Zu den verschiedenen Ausgestaltungsformen siehe *Verbraucherzentrale Bundesverband*, Neue Datenintermediäre, Bundesverband der Verbraucherzentralen und Verbraucherverbände, 15.9.2020, S. 6 Fn. 15; *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Per-

chert und nur aus dieser heraus freigegeben.[165] Über ein technisches Kontrollinstrumentarium kann die betroffene Person die Bedingungen für die Datenverarbeitung und den Datenzugang für Dritte festlegen,[166] sowie sonstige Betroffenenrechte, etwa Auskunfts- oder Berichtigungsrechte, ausüben.[167] Verarbeitende Stellen müssen demnach, um eine Verarbeitung durchführen zu können, den Weg über die PIMS gehen, ein Direktzugriff auf Daten ist ihnen verwehrt.[168] Zu Einwilligungsinstrumenten werden die PIMS dadurch, dass die Daten für Dritte unzugänglich bleiben, solange die betroffene Person die Verarbeitung bzw. den Zugang zu seinen Daten nicht gestattet.[169] Die Gewährung oder Verweigerung des Datenzugangs erfolgt auch hier automatisiert; insoweit gehen in den PIMS Elemente der Einwilligungsassistenten auf. Im Ergebnis stellen sich PIMS als geräte- und serviceübergreifende Kombination von Einwilligungsassistenten und Datenschutzpräferenzen als Standardeinstellungen (Sticky Policies) dar.

Dieser Ansatz verspricht gegenüber bloßen Einwilligungsassistenten bedeutende Steuerungsvorteile. Die Zentralisierung der Kontrolle in einen Datenraum erlaubt eine holistisch-abgestimmte, feingranulare Steuerung der Datenverarbeitungsvorgänge, ebenso wie dynamische Anpassungen.[170] Zugleich vereinfacht das zentralisierte Datenverwaltungssystem den Datenzugang für verarbeitende Stellen, die die betroffene Person nicht mehr um die Freigabe einer

---

sonal Information Management (PIM), 20.10.2016, S. 8. Vgl. auch *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 11-23, 24 sowie *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41.

[165] Anstelle der Einzelabfrage und -abgabe einer Einwilligungserklärung erfolgt über die PIMS ein „One-Stop-Shop" über das Datenmanagementtool, vgl. *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 35.

[166] *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 9 „Kontrollkonsole"; *Janssen/Cobbe/Singh*, Internet Policy Rev. 9 (2020), 1, 4 f. „transparency and control measures".

[167] *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 11 f.

[168] Dies erfolgt über eine Schnittstelle. Der Datenzugriff erfolgt technisch entweder externalisiert, indem die Daten an die verarbeitende Stelle übermittelt werden, oder internalisiert, indem der verarbeitenden Stelle die Verarbeitung innerhalb des persönlichen Datenraums gestattet wird – dann verlassen die Daten den persönlichen Datenraum also nicht. Vgl. *ders.*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 8.

[169] Zum Zusammenhang von PIMS und datenschutzrechtlicher Einwilligung (zugleich mit Hinweis auf die Grenzen eines einwilligungsbasierten Datenschutzes) siehe eingehend *Janssen/Cobbe/Singh*, Internet Policy Rev. 9 (2020), 1, 2, 18-21.

[170] *Horn/Riechert/Müller*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 36. Allgemein befürwortend hinsichtlich PIMS äußerst sich auch *Dornis*, ZfPW 8 (2022), 310, 341.

jeden Datenverarbeitung ersuchen müssen.[171] Verantwortliche können zudem den Zugang zum gesamten Datenset auf einmal, nicht nur zu einzelnen Daten erhalten.[172] Im Übrigen bietet das Datenverwaltungssystem die bereits im Rahmen der Einwilligungsassistenten ausgeführten Vorteile zur Stärkung der Datenschutzkompetenz. Die Herausforderungen, wie sie für die Automatisierung der Einwilligung bereits dargelegt wurden, stellen sich aber auch hier: fehlende Bestimmtheit und Informiertheit[173] oder der Abstimmungsbedarf mit dem (aktuellen) Willen der betroffenen Person[174] fordern auch hier spezifische Schutzinstrumente und gesetzgeberische Klarstellungen. Auch ist, wie bei den Sticky Policies unklar, wie PIMS in das Zulassungsregime des Art. 6 Abs. 1 DSGVO integriert werden können.[175] Sinnvollerweise ist daher für PIMS im Allgemeinen eine spezifische Vorschrift vorzusehen.[176]

Aus der technischen Perspektive steht die Entwicklung von PIMS erst noch am Anfang, ihre Leistungskraft und wirtschaftliche Bedeutung lässt sich noch

---

[171] Siehe hierzu eingehend *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 135. Plakativ auch *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 14: „PIMS könnte man als Vermittler oder ‚Plattformen' bezeichnen, die als Verbindung zwischen den beiden Seiten des Marktes fungieren, nämlich einerseits natürlichen Personen, die ihre Daten zur (Wieder-)Verwendung anbieten, und andererseits Organisationen, die diese Daten (wieder-)verwenden wollen". Auf die Doppelfunktionalität eines Datenmanagementsystems weisen auch *Poikola/Kuikkaniemi/Honko*, MyData, Ministry of Transport and Communications Finland, 2015, S. 4 hin.

[172] *European Union Agency for Network and Information Security*, Privacy by design in big data, 2015, S. 48. Schließlich wird in PIMS auch ein Ansatzpunkt für die seit Langem diskutierte Monetarisierung von Datentransaktionen gesehen, so etwa *Janssen/Cobbe/Singh*, Internet Policy Rev. 9 (2020), 1, 2. Eher zurückhaltend *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 15 f.

[173] Vgl. *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 10 f. sowie eingehend *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41; *Riechert*, Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, Dezember 2016, S. 46–47, 52.

[174] *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 11.

[175] Vgl. *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 10 f.; *Kettner/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement, ConPolicy Institut für Verbraucherpolitik, 5.9.2020, S. 41 f.

[176] So auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 123, die zusätzlich für die Einführung von Qualitätsstandards und Kontrollmechanismen auf nationaler Ebene sowie für eine sektorspezifische Verpflichtung zur Einführung von PIMS wirbt. Auf Verhaltenskodizes und Zertifizierungsregelungen setzt *Europäischer Datenschutzbeauftragter*, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM), 20.10.2016, S. 16.

nicht ermessen. Aufgrund gezielter Förderung in den letzten Jahren ist man hier aber bereits deutlich weiter als etwa bei Sticky Policies. Durch eine Integration von PIMS in die DSGVO könnte die Entwicklung von PIMS weiter vorangetrieben werden.

4. Ergebnis

Eine Zulassungskontrolle hinsichtlich des Maschinellen Lernverfahrens bzw. des Modells oder des Lösungsalgorithmus liegt jenseits des Regulierungsauftrags der DSGVO. Reformbestrebungen in diese Richtung sind daher nicht sinnvoll. Die quantitative und qualitative Überforderung des Einzelnen lässt vielfach am dezentralen Regulierungsmechanismus der DSGVO, wie er insbesondere in der Einwilligung niedergelegt ist, zweifeln. Eine Umgestaltung des Rechtmäßigkeitsgrundsatzes in ein zentralisiertes Zulassungsregime ist aber mit grundlegenden Wertungen des Datenschutzrechts unvereinbar.

Eine Zulassungsentscheidung hinsichtlich der Profilbildung erscheint dagegen sinnvoll. Reformen bedarf es hierfür aber nicht, denn bereits mit der Rechtmäßigkeitsprüfung hinsichtlich der verarbeiteten Rohdaten erfolgt eine hinreichende Zulassungsprüfung. Um diese zu effektivieren, ist die Vorhersehbarkeit von abgeleiteten Profilen zu stärken; dies ist eine Frage der Transparenz. Ein Verbot des Profilings überzeugt nicht, ebenso wenig eine Zulassungsentscheidung einzelner Profilinhalte: Beides ist mit einer freiheitlichen Kommunikationsordnung nicht vereinbar und widerspricht Grundwertungen des Datenschutzrechts. Die Zulassungstatbestände in Art. 6 Abs. 1 DSGVO sind ausreichend: Sie sind hinreichend offen ausgestaltet, um profilingspezifische Wertungen zu integrieren.

Reformoptionen hinsichtlich des Rechtmäßigkeitsgrundsatzes betreffen im Ergebnis das „Wie“, nicht das „Ob“ der Zulassungsprüfung. Im dezentralen Regulierungsregime der DSGVO stehen Reformen im Fokus, die die betroffene Person bei ihrer Einwilligungserteilung unterstützen. Bestrebungen, die auf eine quantitative Absenkung der Zulassungsfragen abzielen – so broad consent-Modelle sowie generalisierte Einwilligungserklärungen – überzeugen nicht: Während bei broad consent-Modellen der Steuerungsanspruch letztlich zurückgefahren wird, fehlt es für generalisierte Einwilligungserklärungen an der notwendigen Vergleichbarkeit zweckübergreifender Datenverarbeitungen. Vielversprechend sind dagegen zeitliche Staffelungen der Einwilligungserklärungen, bei denen die Zulassungsentscheidungen in Einzelpakete aufgeteilt und jeweils unmittelbar vor Stattfinden einer Datenverarbeitung an die betroffene Person herangetragen werden. Die Aufteilung der Einzelpakete sollte dabei risikobasiert erfolgen. Treuhänderische Datenverwaltungseinrichtungen versprechen keine guten Lösungen, insbesondere verlagern sie die Problematik der Steuerungsüberforderung nur auf die Bevollmächtigung. Dagegen erscheinen technische Einrichtungen, die die Einwilligungsentscheidung entspre-

chend der Datenschutzpräferenzen der betroffenen Personen automatisiert vornehmen, sinnvoll: Sie entlasten die betroffene Person und regen diese zudem zu Reflexion über datenschutzrechtliche Fragen an. Dieser technische Datenschutz lässt sich noch effektivieren, indem nicht die Einwilligungserteilung automatisiert wird, sondern technisch abgesichert wird, dass Verantwortliche nur Zugriff auf personenbezogene Daten erhalten, wenn ihre Datenverarbeitungen den Datenschutzpräferenzen betroffener Personen entsprechen. Die technische Verknüpfung von Daten und Datenschutzpräferenzen (Sticky Policies) ist derzeit technisch noch unausgereift. Dagegen existieren für zentralisiert-automatisierte Datenverwaltungstools, sogenannte Personal Information Management Systems – PIMS, erste marktfähige Modelle. Bei diesen werden Daten in persönlichen Datenräumen zentral gespeichert und können von betroffenen Personen über technische Anwendungen verwaltet werden. Sinnvoll erscheint die Einführung einer eigenen Vorschrift für PIMS, um diese rechtssicher für das gesamte Regulierungssystem der DSGVO nutzbar zu machen.

Rechtsinnovationen für die vertragsimmanente Zulassung bieten sich vor allem in Form von Automatisierungen der Vereinbarung von Datenschutzbedingungen, die über Smart Contracts technisch umgesetzt werden können. Eine Automatisierung der Interessensabwägung ist derzeit technisch nicht denkbar. Fortentwicklungen des Art. 6 Abs. 1 lit. f) DSGVO sind vor allem im Hinblick auf Präzisierungen der Interessensabwägung bezüglich autonomer Systeme geboten. Sinnvoll erscheint es, bestimmte Kriterien für die Modell- und Profilbildung sowie die Profilverwendung aufzustellen sowie typisierte Abwägungskonstellationen darzulegen.

III. Reformoptionen für den Transparenzgrundsatz

Die unzureichende Transparenz autonomer Systeme ist besondere Herausforderung dieser neuen Technologie, zugleich ist die (Betroffenen-)Transparenz, wie an verschiedenen Stellen der Arbeit herausgestellt wurde, von besonderer Bedeutung für einen effektiven Datenschutz. Für die Weiterentwicklung des Transparenzgrundsatzes der DSGVO werden teilweise grundlegende Reformen vorgeschlagen, die nicht jenseits des Regulierungs- und Innovationsrahmens der DSGVO liegen (1.). Der Umgang mit der fehlenden Nachvollziehbarkeit autonomer Systeme für betroffene Personen stellt dabei vor besondere Probleme. Es lohnt, diese Fragestellung vor die Klammer zu ziehen (2.), bevor dann weitere Innovationsmöglichkeiten des Transparenzgrundsatzes im bestehenden (3.) sowie noch zu schaffenden Recht (4.) vorgestellt werden.

1. Innovationsräume im Hinblick auf den Transparenzgrundsatz

Die Intransparenz autonomer Systeme erfordert Einblicke in die algorithmischen Verarbeitungen und Ergebnisse. Mit der DSGVO lassen sich solche besonderen, d.h. nicht auf die bloßen Datenverarbeitungsumstände bezogenen In-

formationspflichten allerdings nur bedingt umsetzen (a)). Einen gegenteiligen Ansatz verfolgen Reformbewegungen, die ganz grundlegend in Zweifel ziehen, ob sich eine betroffenenbezogene Transparenz überhaupt herstellen lässt und diese die ihr zugeschriebenen Steuerungsleistungen erbringen kann. Auch dies ist mit den Regulierungskonzept der DSGVO unvereinbar (b)).

a) Interregulative Abgrenzung: nur begrenzte algorithmenspezifische Transparenz

Wenn teilweise gefordert wird, die besonderen, d.h. die in Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO normierten, verarbeitungs- und algorithmenspezifischen Informationspflichten auf jede Datenverarbeitung, bei der Algorithmen aus Maschinellen Lernverfahren eingesetzt werden[177] oder die dem Training von Algorithmen dient,[178] zu erstrecken, überzeugt nicht.[179] Die DSGVO beschränkt sich eben auf datenverarbeitungsspezifische Gefährdungen und Schutzinstrumente, die Algorithmen liegen jenseits dieses Regulierungsauftrags. Dagegen öffnet sich die DSGVO Regulierungsfragen im Hinblick auf die Profilbildung[180] sowie die automatisierte Entscheidung.[181] Bei diesen ist eine Erstreckung des Informationspflichtenprogramms auf das algorithmische Auswertungsverfahren und deren Ergebnisse richtig.

---

[177] So etwa *Martini*, Blackbox Algorithmus, 2019, S. 185 f., der eine Ausweitung auf sämtliche Algorithmenanwendungen mit grundrechtssensitiver Wirkung, insbesondere Maschinelle Lernverfahren, fordert.

[178] In diese Richtung wohl die *Garante per la protezione dei dati personali*, Provvedimento dell' 11 aprile 2023, 11.04.2023, S. 6, die umfangreiche Informationen zur zugrundeliegenden Logik des Trainingsverfahrens für die Erstellung des Lösungsalgorithmus von ChatGPT fordert.

[179] Gegen eine Ausweitung der Informationspflichten auf sämtliche Datenverarbeitungen spricht sich auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 150 aus. Auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192 fordert allein Ausweitungen der besonderen Informationspflichten auf bestimmte Entscheidungssysteme, nicht aber auf sämtliche Datenverarbeitungssysteme. Ebenso *Sesing*, MMR 24 (2021), 288, 290 f.

[180] Eine Ausweitung der besonderen Informationspflichten hinsichtlich der Profilbildung wird vielfach befürwortet. Siehe nur *Wachter/Mittelstadt*, CBLR 2019, 494, 514; *Lorentz*, Profiling, 2019, S. 341; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192. Zumindest für risikohafte Profilbildungen Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53. Sehr allgemein eine Transparenz hinsichtlich der Profilbildung fordern *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336; *Gutwirth/Hert*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 271, 290; *Hildebrandt*, in: Bus (Hrsg.), Digital enlightenment yearbook 2012, 2012, S. 41, 49–52.

[181] Siehe bereits oben Kapitel 5 A. Hinsichtlich des Transparenzgrundsatzes erfolgt diese Öffnung spezifisch in den besonderern Transparenzvorschriften der Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO.

Bei der Profilbildung folgt dies daraus, dass über den Algorithmus – also das Modell – die Rohdaten mit einem „Mehr“ aufgeladen werden.[182] Dieses „Mehr“ bleibt aber intransparent und kann gerade deshalb Autonomiegefährdungen auslösen.[183] Zugleich unterbindet das Modell aufgrund seiner Intransparenz den Steuerungsmechanismus der DSGVO.[184] Dies gilt vor allem für den Rechtmäßigkeitsgrundsatz: Wenn aufgrund des Modells Profilinhalte nicht mehr vorhersehbar sind, ist auch eine Zulassungsprüfung nicht mehr sinnvoll möglich.[185] Dies gilt aber auch für den Transparenzgrundsatz: Wenn Profilinhalte nicht vorhersehbar und nicht rückverfolgbar sind, können Betroffenenrechte nicht ausgeübt, außerrechtliche Resilienzmechanismen nicht aktiviert und die Einwilligung nicht sinnvoll erteilt werden.[186] Die bloße Kenntnis von datenverarbeitungsbezogenen Umständen, insbesondere dem Zweck, reicht nicht mehr aus. Einblicke in das Profilbildungsverfahren, damit auch das Modell, und darüber hinaus in Profilinhalte sind demnach notwendig, um datenverarbeitungsspezifische Gefährdungen aufzuheben und die Regulierungsinstrumente der DSGVO zu aktivieren.

Bei der automatisierten Entscheidung rechtfertigt sich die Öffnung des Transparenzgrundsatzes auf das Algorithmische daraus, dass die Gefährdung vornehmlich in der algorithmischen Entscheidungsarchitektur liegt. Es ist dann die für die betroffene Person intransparente Verknüpfung von Datum bzw. Datenverarbeitungsergebnis und Entscheidungsinhalten, die autonomiegefährdend wirkt.[187] Um diese aufzuheben, bedarf es gewisser Einblicke in den Lösungsalgorithmus und seiner Ergebnisse. Diese Transparenzbedarfe bestehen auch dann, wenn die Entscheidung nicht ausschließlich automatisiert ist. Die besonderen Informationspflichten sind daher überzeugenderweise auch auf teilautomatisierte Entscheidungen zu erstrecken, dies allerdings nur, soweit diese rechtliche Wirkungen oder erhebliche Beeinträchtigungswirkungen zeigen, sich also als risikohaft darstellen.[188] Nur so besteht ein Regulierungs-, hier

---

[182] Siehe hierzu bereits unter Kapitel 4 B. IV. 2. sowie Kapitel 4 C. IV. 2. bb).

[183] Siehe oben Kapitel 2 C. IV. 2. b) aa). Siehe hierzu auch *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336; *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 449.

[184] Siehe hierzu eingehend unter Kapitel 4 B. IV. 1. c).

[185] Siehe oben Kapitel 4 C. IV. 2. c) aa).

[186] Siehe oben Kpaitel 4 D. IV. 2. b).

[187] Siehe bereits oben Kapitel 5 B. I. 1. a) cc). Siehe zur Gefährdung aufgrund der Intransparenz der algorithmischen Entscheidungsarchitektur Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 3; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 1.

[188] So auch *Sesing*, MMR 24 (2021), 288, 290 f. Er stellt darauf ab, dass das Risiko der teilautomatisierten Entscheidungen denjenigen von vollständig automatisierten Entscheidungen wertungsmäßig gleichkommt. In diese Richtung auch Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53, der für eine Anwendung des Art. 13 Abs. 2 lit. f) DSGVO auf eine jede „Proflingmaßnahme“ eintritt, deren Risiko dem der automatisierten Entschei-

genauer: ein Transparenzbedarf. Dies stellt zugleich einen angemessenen Ausgleich mit Interessen des Verantwortlichen an der Geheimhaltung der algorithmischen Entscheidungsarchitektur her sowie mit dessen privatautonomer Freiheit, im Verhältnis zwischen Privaten keine Gründe für eine Entscheidung liefern zu müssen[189] und ermöglicht damit letztlich auch Innovation, die andernfalls aus wirtschaftlichen Gründen nicht betrieben würde.[190]

Bei Profilverwendungen jenseits der automatisierten Entscheidung ist ein Einblick in den Lösungsalgorithmus nicht erforderlich.[191] Wie beschrieben,[192] geht die Gefährdung hier nicht von der algorithmischen Entscheidungsarchitektur, sondern von den vertieften Erkenntnissen über die Einzelperson aus. Diese ermöglichen besonders manipulative personalisierte Werbungen oder begründen Selbstbestärkungseffekte im Rahmen der Informationsfilterung.

Vielfach liegen die Gefährdungsursachen, etwa Selbstbestärkungseffekte, aber auch Manipulationen, im fehlenden Risikobewusstsein sowie in einer unzureichenden Medienkompetenz, betroffener Personen. Insoweit erscheint die Investition in Bildung und Aufklärung als ein wichtiges Instrument.[193] Dies ist aber kein Transparenzauftrag im klassischen Sinne, vor allem keiner, der an den Verantwortlichen gerichtet ist. Gefordert sind vielmehr staatliche und private Bildungs- und Aufklärungsinitiativen.

---

dung vergleichbar ist. Einen risikobasierten Ansatz, dort für die Existenz eines Rechts auf Erklärung, schlägt auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 187–192 vor. Vgl. auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 192, die für die Regulierung (teil-)automatisierter Entscheidungen allgemein, dann also auch die transparenzbezogenen Vorschriften, einen risikobasierten Regulierungsansatz befürwortet. Siehe allgemein zu einer Erweiterung des Anwendungsbereichs der Vorschrift des Art. 22 DSGVO auch oben Kapitel 5 B. I. 1. A) cc) sowie Kapitel 5 B. I. 3. b).

[189] Siehe hierzu 63 S. 5. Siehe zu diesen Erwägungen auch, wenngleich im Rahmen des Umfangs der Erläuterungspflichten, *Sesing*, MMR 24 (2021), 288, 291; Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54. Zur Privatautonomie *Martini*, Blackbox Algorithmus, 2019, S. 192 f.; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 6.

[190] Vgl. allgemein zu dieser Erwägung Paal/Pauly DS-GVO/*Martini*, Art. 22 Rn. 8.

[191] AA *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 187–192, der ein Recht auf Erklärung für sämtliche automatisierte Anwendungen befürwortet, soweit diese risikoreich sind. Auch *Martini*, Blackbox Algorithmus, 2019, S. 185 f. fordert eine Anwendung der besonderen Transparenzvorschriften für sämtliche grundrechtssensitive Algorithmenanwendungen.

[192] Siehe oben Kapitel 5 B. I. 1. b).

[193] Siehe hierzu auch *Wischmeyer*, AöR 143 (2018), 1, 64. Siehe zu Vorschriften zu derartiger Aufklärungs- und Bildungsarbeit in der DSGVO bereits Kapitel 4 D. II. 2. c).

b) Intraregulative Abgrenzung: keine Abschaffung, sondern Ergänzung der Betroffenentransparenz

Dass die Transparenz überhaupt zum Schutzinstrument taugt, ihre Funktionen auf instrumenteller, funktionaler und instrumentell-funktionaler Ebene tatsächlich erfüllen kann, wird zudem vielfach, vor allem von Seiten der Verhaltensökonomie, in Zweifel gezogen. Nach einschlägigen Studien lassen sich Personen in komplexen Entscheidungssituationen primär von irrationalen Beweggründen, wie Emotionen,[194] individuellen Überzeugungen[195] oder sonstigen, auch kurzfristigen Anreizen[196] leiten.[197] Informationsangebote können sogar selbst zur Heuristik werden: Umfangreiche Informationen werden nach diesen Studien als Hinweis für eine besondere Vertrauenswürdigkeit[198] oder aber für eine besondere Gefährlichkeit[199] eines Systems gedeutet, dies gänzlich unabhängig von ihrer tatsächlichen Gefährlichkeit. Diese Effekte verstärken sich, je komplexer und umfangreicher das Informationsangebot ausfällt.[200] Darüber hinaus neigen Personen dazu, die kurzfristigen Vorteile aus der Nutzung autonomer Systeme gegenüber den unsicheren und sich erst in einer fernen Zukunft

---

[194] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 237 f. Zu beobachtbaren verhaltensökonomischen Rationalitäten einer Einwilligungsentscheidung, die in der Summe darauf hindeuten, dass diese Entscheidung gerade nicht informationsbasiert erfolgt, siehe eingehend *ders.*, Informationelle Selbstgefährdung, 2015, S. 227–318.

[195] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 237 beschreibt den Umstand, dass betroffene Personen Datenschutzerklärungen deshalb nicht lesen, da sie glauben, die Risiken und Chancen einer Datenverarbeitungstechnik zutreffend einschätzen zu können. Bestätigt wird dies durch die Studie von *Jensen/Potts/Jensen*, Int. J. Hum. Comput. 63 (2005), 203, 212–214. Diesen Schluss legen auch die Befragungen des *Eurobarometer*, Special Eurobarometer 487a – March 2019, Directorate-General for Justice and Consumers; Europäische Kommission, März 2019, S. 51 f. nahe, in der 11 % der Befragten angaben, dass sie Datenschutzerklärungen deshalb nicht lesen würde, da sie sich bereits als hinreichend geschützt betrachteten.

[196] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 83. Zu den verschiedenen Anreizstrukturen anstelle der Information bzw. tatsächlichen Risikolage und Datenschutzpräferenz siehe eingehend *ders.*, Informationelle Selbstgefährdung, 2015, S. 227–240.

[197] Siehe allgemein zu verhaltensökonomischen Erkenntnissen bezüglich der Einwilligung *Jarovsky*, EDPL 4 (2018), 447, 449; *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 356 f. Siehe auch unter Zitierung zahlreicher Studien *Yeung*, iCS 20 (2017), 118, 125.

[198] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 83, 274-276. Diesen Schluss legt auch die Studie durch *Eurobarometer*, Special Eurobarometer 487a – March 2019, Directorate-General for Justice and Consumers; Europäische Kommission, März 2019, S. 51, 54 nahe, wonach die Befragten bereits den Umstand der Existenz von Datenschutzerklärungen für ausreichend erachteten, um dem Dienst zu vertrauen, und deren Lektüre nicht für notwendig hielten.

[199] *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 83, 335-337.

[200] *Ders.*, Informationelle Selbstgefährdung, 2015, S. 368 f.

realisierenden Nachteilen zu priorisieren.[201] Empirisch ist vielfach belegt worden, dass betroffene Personen trotz Kenntnis von und Sensibilität für (Privatheits-)Gefährdungen durch Datenverarbeitungen ihre Daten teilen (Privcay Paradox).[202] Vor allem aber ist bei all dem problematisch, dass am Ende gar nicht klar ist, auf welche Grundlage Betroffene ihre Datenschutzentscheidungen stützen und ob also die Informationsangebote überhaupt von Relevanz sind.[203] Die funktionale Dimension der Transparenz lässt sich zudem empirisch nicht eindeutig nachweisen. So liefert etwa die Studienlage zum Bestand von Hemm- und Abschreckungseffekten aufgrund der Intransparenz von Datenverarbeitungen keine klaren Ergebnisse.[204] Erst recht ist offen, inwieweit mehr Transparenz diese Effekte aufheben, d.h. die betroffene Person zur Aktivierung von Selbstschutzmechanismen aktivieren könnte.

Vielfach wird daher vorgebracht, dass die Grenzen eines betroffenenbezogenen Transparenz- und Steuerungssystems erreicht sind.[205] Als Alternative

---

[201] Ebenso *Robrecht*, EU-Datenschutzgrundverordnung: Transparenzgewinn oder Information-Overkill, 2015, S. 64. Vgl. auch Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/*Roßnagel*, Art. 5 Rn. 61.

[202] Ob, aus welchen Gründen und unter welchen Bedingungen dieses Paradoxon tatsächlich besteht und was daraus für das Recht folgen sollte, ist Gegenstand fortlaufender interdisziplinärer Forschung. Aus der umfassenden Literatur siehe etwa *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 231–235; *Barth/Jong*, Telematics and Informatics 34 (2017), 1038–1058; *Lutz/Strathoff*, in: Brändli (Hrsg.), Multinationale Unternehmen und Institutionen im Wandel, 2013, S. 81; *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 1 f.; *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 356. Unter Zitierung zahlreicher Studien *Robrecht*, EU-Datenschutzgrundverordnung: Transparenzgewinn oder Information-Overkill, 2015, S. 32–38. Aus psychologischer Sicht siehe etwa *Dienlin*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 305 Eine kritische Bewertung dieses Phänomens unter Zitierung zahlreicher Studien nimmt das *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 23–27 vor. Diese Beobachtungen lassen sich sowohl bei der Einwilligung und ihrer Rücknahme, als auch bei der Ausübung von Betroffenenrechten machen, vgl. *van Ooijen/Vrabec*, J. Consum. Policy 42 (2019), 91–107.

[203] So auch *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 83.

[204] Siehe etwa zu Abschreckungseffekten bei automatisierter Erfassung von Verhalten im Online-Kontext die Studie bei *Staben*, Der Abschreckungseffekt auf die Grundrechtsausübung, 2017, S. 158 f.

[205] So auch *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 8. Sehr kritisch etwa *Mik*, Law Innov. Technol. 8 (2016), 1, 31 f.: „What is needed are actual prohibitions – not more information"; *Spencer*, University of Illinois Law Review 2020, 959, 1004: „But there is strong reason to believe that notice and choice can no longer protect consumer privacy, if indeed it ever could. [...] The more promising approach, then, would be to establish duties or prohibitions that exist regardless of consent". Ebenso *Zarsky*, Theoretical Inquiries in Law 20 (2019), 157, 165, 187: „[R]ather than chase down firms collecting and analyzing information without proper consent, society's shift should be towards regulating their subsequent

werden dann expertengestützte Audits vorgeschlagen. Transparenzpflichten bestehen dann allein gegenüber privaten ExpertInnen oder staatlichen Kontrollstellen.[206] Mit dem Konzept digitaler Autonomie und ihres Schutzes in der DSGVO wäre dies aber unvereinbar. Im Datenschutzrecht ist gerade die Vorstellung prägend, dass die Wahrnehmung digitaler Autonomie besonders über Informationsangebote erreicht werden kann.

2. Ansätze zum Umgang mit fehlender Nachvollziehbarkeit autonomer Systeme

Vier Konstellationen begründen im Wesentlichen eine fehlende Nachvollziehbarkeit autonomer Systeme:[207] Solche, die aufgrund technischer Illiteralität ausgelöst sind, solche, die aufgrund der dynamischen Fortentwicklung der Systeme besteht, solche, die auf menschliche Kognitionsgrenzen zurückzuführen ist, und solche, die in maschinellen Sinnbildungen jenseits menschlicher Konsistenzzusammenhänge ihre Ursache haben.[208] Meist ist nur die vierte Konstellation angesprochen, wenn von fehlender Nachvollziehbarkeit autonomer Systeme die Rede ist, da sie neuartig und für autonome Systeme typisch ist (Black-box-Phänomen).[209] Datenschutzrechtlich laufen alle vier Konstellationen gleich, da im dezentralen Regulierungsregime der DSGVO die Transparenz dezidiert eine Betroffenentransparenz ist.

Für etwaige Weiterentwicklungen des Transparenzgrundsatzes ist es zunächst wichtig, sich zu vergegenwärtigen, dass die Intransparenz von Entscheidungsverfahren und technischen Verfahren weder etwas Neuartiges noch etwas per se Nachteiliges ist (a)). In der Literatur werden verschiedene Methoden vorgeschlagen, um die Verarbeitungen autonomer Systeme in menschlich

---

manipulative (or other abusive) uses". Kritisch zur Leistungsfähigkeit eines Selbstschutzsystems, zumindest in Reinform *Martini*, Blackbox Algorithmus, 2019, S. 226.

[206] Denkbar sind sowohl Selbstaudits, die dann in eine staatliche Aufsichtsarchitektur eingebunden sein müssten, als auch durch private oder staatliche Stellen durchgeführte Fremdaudits. Siehe allgemein Selbstkontrollmechanismen bei intelligenten Systemen etwa *Wischmeyer*, AöR 143 (2018), 1, 62 f. Siehe überdies *Bäcker*, Der Staat 51 (2012), 91, 113; *Martini*, Blackbox Algorithmus, 2019, S. 266–268. Vgl. allgemein zu Vorteilen derartiger Selbstprüfungsmaßnahmen als Steuerungselement technischer Innovation *Hoffmann-Riem*, in: Schulte/Di Fabio (Hrsg.), Technische Innovation und Recht, 1997, S. 3, 25. Siehe eingehend zu Fremdaudits durch private oder staatliche ExpertInnen, dort allgemein hinsichtlich intelligenter Systeme und nicht spezifisch zur DSGVO, *Wischmeyer*, AöR 143 (2018), 1, 62 f.

[207] Siehe zu den verschiedenen Formen der Intransparenz, die autonome Systeme aufweisen, bereits oben Kapitel 4 D. IV. 1.

[208] Hierzu zählt auch die in Kapitel 4 D. IV. 1. e) angesprochene Fallgruppe der auf die Dynamik autonomer Systeme zurückzuführende Intransparenz. Eingehend hierzu bereits oben Kapitel 1 A. II. 2. C) sowie Kapitel 2 A. I. 2. b).

[209] Siehe hierzu bereits oben Kapitel 4 D. IV. 1. e).

nachvollziehbare Konsistenzrahmen zu bringen. Diese Ansätze bieten Lösungsmethoden für alle vier der beschriebenen Konstellationen der Betroffenenintransparenz. Sie werden unter dem Stichwort eines „Rechts auf Erklärung“ diskutiert (b)). Diese Ansätze werden aber nicht zu einer umfassenden (Betroffenen-)Transparenz führen. Eine sinnvolle Steuerung muss daher auch auf transparenzferne Mechanismen setzen (c)).

a) Banalität der Intransparenz von Entscheidungsarchitekturen und technischen Phänomenen

Wenn vielfach als Antwort auf die fehlende Nachvollziehbarkeit Maschineller Lernverfahren eine umfassende Verständlichkeit gefordert wird, so verkennt dies, dass der Mensch schon immer intransparenten Entscheidungs- und Steuerungsarchitekturen ausgesetzt war (aa)), zudem dem Laien technische Verfahren selten im Detail verständlich sind (bb)).

aa) Umgang mit Intransparenzen tradierter Entscheidungsarchitekturen

Die Intransparenz von Entscheidungs- und Steuerungsarchitekturen ist eine Alltäglichkeit: Auch menschliche Entscheider,[210] menschlich-kollektive Entscheidungsgremien[211] oder sonstige staatliche und nicht-staatliche Steuerungsstrukturen (Markt, Hierarchie, Verhandlung, Netzwerk)[212] sind in der Regel nicht, jedenfalls nicht umfassend für die betroffene Person verständlich. Dies führt aber nicht zu Verlusten an Freiheit und Würde. Man hat gute Methoden entwickelt, um mit diesen Intransparenzen umzugehen. In Entscheidungs- und Steuerungsarchitekturen liegen diese vornehmlich in der Begründung und Rechtfertigung von Entscheidungen.[213] Gefordert ist dann nicht eine umfassende Aufdeckung sämtlicher entscheidungstragender Parameter, sondern allein eine Darlegung grundlegender entscheidungsleitender Kriterien, die eine Akzeptanz, sowie eine Kontrolle und Anfechtung der Entscheidung durch die betroffene Person und andere menschliche Kontrollinstanzen erlauben. Am Ende aber bleibt ein großer Teil der tradiert-menschlichen Entscheidungs- und Steuerungsarchitekturen intransparent. Dann bieten Anforderungen an die Qualifikation der menschlichen Entscheider sowie an die inhaltliche Angemes-

---

[210] *Wischmeyer*, AöR 143 (2018), 1, 54, 59-60; *Tutt*, Admin. L. Rev. 69 (2016), 103. Eingehend auch *Bonezzi/Ostinelli/Melzner*, Journal of experimental psychology 151 (2022), 1–9.

[211] *Wischmeyer*, AöR 143 (2018), 1, 54.

[212] *Ders.*, AöR 143 (2018), 1, 44 f.

[213] Vgl. *Martini*, Blackbox Algorithmus, 2019, S. 189 f. sowie mit konkreten Vorschlägen zur Übertragung auf algorithmisch-automatisierte Entscheidungssysteme in staatlicher Hand *Wischmeyer*, AöR 143 (2018), 1, 54–65. Siehe zu weiteren Mechanismen, die dem Menschen ermöglichen, mit der Intransparenz menschlichen Entscheides umzugehen *Tutt*, Admin. L. Rev. 69 (2016), 102 f.

senheit der Entscheidung und des Entscheidungsverfahrens in Kombination mit Selbst- und Fremdkontrollmechanismen effektiven Schutz vor nachteiligen Effekten intransparenter Entscheidungen.[214] Für technische Entscheidungs- und Steuerungsverfahren kann dann nichts anderes gelten: Eine umfassende Transparenz der gesamten Entscheidungsarchitektur erscheint nicht notwendig, um Autonomiegefährdungen und Diskriminierungen effektiv abzuwehren. Ausreichend ist ein Transparenzniveau, das die Abwehr dieser schädlichen Wirkungen erlaubt. Im Übrigen ist Transparenz nicht das einzige und auch nicht notwendig das effektivste Mittel zur Absicherung von Freiheit und Würde im Angesicht automatisierter Entscheidungssysteme.

bb) Umgang mit Intransparenzen technischer Systeme

Darüber hinaus sind auch technische Verfahren dem Laien selten in ihren Details verständlich.[215] Auch darin wird gemeinhin keine Gefahr für die freiheitliche Lebensführung von BürgerInnen bzw. NutzerInnen einer technischen Anwendung erkannt, solange ein Transparenzniveau erreicht wird, das der betroffenen Person eine technikgerechte und sichere Bedienung erlaubt. Technische Kompetenz und Risikobewusstsein sind hier vorwiegend das Ziel. Darüber hinaus wird auch hier der Schutz überwiegend betroffenentransparenzfern, insbesondere über substantielle Qualitätsvorgaben, Haftungsregime und Kontrollen durch ExpertInnen oder Fachbehörden erreicht.[216] Für autonome Systeme gilt dann: Um ihre Gemeinwohlverträglichkeit abzusichern, ist eine umfassende Verständlichkeit sämtlicher technischer Verarbeitungsdetails nicht

---

[214] Vgl. eingehend *Wischmeyer*, AöR 143 (2018), 1, 61–65. Auf die Kontrollfähigkeit von Algorithmen hinsichtlich rechtlicher Anforderungen stellt auch *Hoffmann-Riem*, AöR 142 (2016), 1, 32 ab.

[215] So auch *Tutt*, Admin. L. Rev. 69 (2016), 102 f., der das Beispiel eines Medizinprodukts heranzieht.

[216] Diese (vorrangige) Verpflichtung zur Gewährleistung von Fehlerfreiheit, Angemessenheit und Sicherheit von autonomen Systemen statt (allein betroffenenbezogener) Transparenz wird auch als Rechenschaft (Accountability) bezeichnet, in der Literatur also Accountability der Algorithmen statt (nur) Transparenz gefordert, vgl. etwa *Kroll/Huey/Barocas u.a.*, University of Pennsylvania Law Review 165 (2017), 633–705. Siehe auch die Vorschläge des *European Parliamentary Research Service*, A governance framework for algorithmic accountability and transparency, Europäisches Parlament, April 2019. Das Rechenschaftsprinzip ist in Art. 24 DSGVO auch als datenschutzrechtliches Regulierungsinstrument anerkannt. Siehe auch die Entwürfe Regulierungsregime für Algorithmen von *Martini*, Blackbox Algorithmus, 2019, S. 338–358 oder der *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 185–217, in denen neben der Transparenz eine Vielzahl von Instrumenten, etwa inhaltliche Angemessenheitskriterien, Haftungsregeln sowie Selbst- und Fremdkontrollemechanismen vorgesehen sind. Auch die Regulierungsvorschläge von *Tutt*, Admin. L. Rev. 69 (2016) zielen auf die Sicherstellung von Qualität und Sicherheit von Algorithmen durch Vorgabe materieller Standards und deren Kontrolle ab.

geboten. Wichtig erscheinen demnach Investitionen in die Schulung zum richtigen Umgang mit autonomen Systemen und Risikoaufklärungen.[217] Die (Betroffenen-)Transparenz ist zudem nicht das einzige Instrument, um effektiv die Gemeinwohlverträglichkeit der Technik zu gewährleisten.

b) Rechtsnormative Konzeptionen menschlicher Verständlichkeit: Recht auf Erklärung als Lösungsmodell

In der Literatur werden verschiedene Ansätze diskutiert, wie betroffenen Personen die Outputs autonomer Systeme trotz technischer Illiteralität, dynamischer Fortentwicklung der Systeme, menschlicher Kognitionsgrenzen und fehlender Nachvollziehbarkeit bestimmter selbstlernender Algorithmen verständlich gemacht werden können. Im Ergebnis ist dies nichts anderes als die Definition, was menschliche Verständlichkeit überhaupt bedeutet, um sie dann zu einer rechtsnormativen, justiziablen Vorgabe machen zu können. Als subjektiver Rechtsanspruch wird hieraus ein „Recht auf Erklärung" geformt (Right to Explanation).[218] Verschiedene Ansätze werden dabei vorgeschlagen, von denen nachfolgend die vier in der Debatte vorherrschenden präsentiert werden sollen: Während die einen eine menschliche Lesbarkeit fordern (aa)), halten andere ein kontrafaktisches Erklärungsmodell für zielführend (bb)), wiederum andere prägen ein Recht auf nachvollziehbare Schlussfolgerungen (cc)). Vorgeschlagen wird schließlich ein Begründungsmodell (dd)). Überzeugend ist am Ende eine nachträgliche Erläuterungspflicht, dann auf datenverarbeitungsspezifische Auditabilität abzielende Begründung (ee)) sowie eine vorherige Erläuterungspflicht, deren Ziel die Herstellung auditabilitätsermöglichender Vorhersehbarkeit ist (ff)).

aa) Menschliche Lesbarkeit (Legibility)

Mit dem Modell menschlicher Lesbarkeit[219] soll nicht allein die technische Funktionsweise, sondern das System in seinem Anwendungszusammenhang der betroffenen Person verständlich gemacht werden. Sie soll die Logik sowie die Bedeutung und Konsequenzen eines algorithmischen Entscheidungssystems verstehen können.[220] Dies erfordert Erläuterungen sowohl hinsichtlich der

---

[217] Vgl. zum staatlichen Bildungsauftrag sowie zum Beitrag von Medien und Gesamtgesellschaft hierbei *Wischmeyer*, AöR 143 (2018), 1, 64.

[218] Grundlegend *Goodman/Flaxman*, AI Magazine 38 (2017), 50–57 Siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76 f.; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277.

[219] *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 250.

[220] Vgl. *dies.*, Int. Data Priv. Law 7 (2017), 243, 250: „It is different from mere readability of data or analytics because it includes more details about purposes, finalities, commercial significance and envisaged consequences; but it is also different from explanation/infor-

technischen Algorithmenstruktur (Architecture) wie auch der Implementierungsumstände (Implementation), also etwa Anwendungszwecke, Umfang menschlicher Involvierung oder den Anwendungskontext.[221] Zur Konkretisierung der Inhalte dieser Erläuterungspflichten wird ein Katalog mit verschiedenen fakultativen Merkmalen aufgestellt. Anhand dieses Katalogs soll dann ein Verständlichkeitsprüfung der Systeme (Legibility Test) vom Verantwortlichen durchgeführt und so die Intransparenz des Systems und der Umfang der Erläuterungspflichten bemessen werden.[222]

bb) Kontrafaktische Erklärungen

Andere fokussieren auf die technische Funktionsweise und schlagen ein simulatives Erklärungsmodell in Form kontrafaktischer Erklärungen vor (Counterfactual Explanations).[223] Dabei werden der betroffenen Person die tragenden Entscheidungsparameter offengelegt und zugleich erläutert, welche Änderungen einzelner Parameter zu einer anderen Entscheidung geführt hätten. Nicht offengelegt wird dagegen das Gewicht und die Bedeutung der Parameter. Dies soll die betroffene Person durch ein Simulationsmodell selbst erfahren. Darin kann die betroffene Person einzelne Parameter verändern und die Auswirkungen dieser Veränderungen für den Output beobachten. Am Ende wird so erkenntlich, welche Kriterien die Entscheidung tragen und welche verändert werden müssen, damit das erwünschte Ergebnis, etwa eine Kreditvergabe, ausgegeben wird.[224] Gleichwohl, bereits ab einer bestimmten Komplexität des Systems, d.h. einer bestimmten Anzahl von Parametern und vielschichtigen Verbindungen zwischen diesen, ist es aber kaum mehr denkbar, dass eine betroffene Person durch ein bloßes Austesten tatsächlich die Funktionsweise des

---

mation because it is more ‚proactive', tailored to individual understanding and concrete comprehensibility of the logic and consequences disclosed".

[221] *Dies.*, Int. Data Priv. Law 7 (2017), 243, 258 f.

[222] Eingehend mit ausführlichem Fragenkatalog *dies.*, Int. Data Priv. Law 7 (2017), 243, 259–261.

[223] Als Modell für die Informationspflichten der Art. 13-15 DSGVO schlagen dies vor *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 863–872. Dieses Erklärungsmodell zumindest für spezielle Anwendungssituationen befürwortend *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 187. Ähnlich ist das Erklärungsmodell, das *Edwards/Veale*, SSRN Journal 2017, 61–64.

[224] Siehe hierzu eingehend *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 854–860. Bei einer ablehnenden Entscheidung wird etwa dargelegt, dass diese aufgrund der Vermögensrücklagen X erfolgte, die als unzureichend qualifiziert wurden, bei einer Vermögensrücklage von Y aber eine positive Entscheidung ergangen wäre. Bei einem Simulationsmodell könnte die betroffene Person die Vermögensrücklagen so lange nach oben oder unten korrigieren, bis die Entscheidung im Simulationsmodell in erwünschter Weise erfolgt. Auf diese Weise kann er erkennen, ab welchem Betrag der Vermögensrücklage ein Kredit vergeben würde.

Systems erkennen und Ergebnisse hinreichend prognostizieren oder nachvollziehen kann.

cc) Recht auf nachvollziehbare Schlussfolgerungen

Ein Recht auf angemessene Ableitungen (Right to Reasonable Inferences) formt aus der Verständlichkeitsvorgabe ein inhaltlich-substantielles Kriterium: Entscheidungen dürfen ausschließlich auf Ableitungen gestützt werden, die angemessen, d.h. menschlich verständlich sind.[225] Der Verantwortliche weist diese Angemessenheit nach, indem er die Relevanz und Akzeptabilität der verwendeten Daten, die Akkuratesse und Verlässlichkeit der eingesetzten Daten und Methoden sowie die Relevanz und die Akzeptierfähigkeit der einzelnen Inferenzen darlegt. Im Ergebnis geht es dabei um die inhaltliche Angemessenheit einer automatisierten Entscheidung. Derartige substantielle Richtigkeitsanforderungen an Datenverarbeitungen liegen allerdings jenseits des Regulierungszugriffs der DSGVO.[226]

dd) Begründung und Rechtfertigung

Vorgeschlagen wird schließlich, die Methode zum Umgang mit der intransparenten Entscheidungsinstanz Mensch zu übertragen: Gefordert wird dann eine Begründung bzw. Rechtfertigung der automatisierten Entscheidung, wie sie für Hoheitsakte, insbesondere Gerichtsentscheidungen oder Verwaltungsakte, entwickelt wurde.[227] Maßstab ist dann die menschliche Kontrollierbarkeit, Anfechtbarkeit und Justiziabilität.[228] Die betroffene Person muss befähigt werden, die Fehlerfreiheit, Rechtmäßigkeit und normative Angemessenheit dieses Outputs prüfen, etwaige Defizite vor einer privaten oder staatlichen Instanz geltend zu machen und Anpassungen, Verbesserungen oder Neuberechnungen zu er-

---

[225] Siehe zu diesem Vorschlag *Wachter/Mittelstadt*, CBLR 2019, 494, 572–591. Befürwortend *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 193; *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 260.

[226] Siehe oben Kapitel 5 A. I. Siehe hierzu sowie zu weiteren Kritikpunkten eingehend *Martini*, Blackbox Algorithmus, 2019, S. 206 f.

[227] So etwa *Sesing*, MMR 24 (2021), 288, 292; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 199–201; *Wischmeyer*, AöR 143 (2018), 1, 54–61.

[228] So *Wischmeyer*, AöR 143 (2018), 1, 55–58. Ebenso *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 197–199; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; *Dimitrova*, EDPL 6 (2020), 211, 229; *Kaminski*, BTLJ 34 (2019), 189, 213. Vgl. auch Gola, DS-GVO/*Franck*, Art. 15 Rn. 18: „die Möglichkeit des Eingreiffens […] eröffnen". So auch *Sesing*, MMR 24 (2021), 288, 291 f., demzufolge es solcher Verfahren bedarf, die „die Zuverlässigkeit automatisierter Verfahren messbar [...] machen können". Siehe überdies auch *Hoffmann-Riem*, AöR 142 (2016), 1, 36.

reichen. Dafür sind die wesentlichen Entscheidungskriterien und deren Bedeutung für die Entscheidung in menschliche Verständniskontexte zu setzen.[229]

Dabei geht es vornehmlich um ein instrumentelles Verständnis der Transparenz: Welche Merkmale die Erläuterung aufnehmen muss, hängt von den korrespondierenden Kontroll- und Anfechtungsrechten ab und von den prozessualen und substantiellen Richtigkeitskriterien.[230] Ist ein derartiges Richtigkeitskriterium etwa die Diskriminierungsfreiheit einer automatisierten Entscheidung, muss aus der Erläuterung ersichtlich werden, ob unmittelbar oder mittelbar diskriminierungsrelevante Parameter die Entscheidungsregel und das Entscheidungsergebnis tragen.

Dieser Ansatz ist überzeugend. Im Gegensatz zum Modell der menschlichen Lesbarkeit, der kontrafaktischen Erklärungen wie im Übrigen auch bei einem Recht auf angemessene Schlussfolgerungen, die inhaltlich sehr diffus bleiben, wird über die instrumentelle Dimension der Transparenz präzise und justiziabel definiert, welches Maß an Verständlichkeit gelten muss. Zudem ist dieser Ansatz in ein Gesamtregulierungssystem eingeordnet, denn es ist mit prozessualen und materiellen Vorgaben synchronisiert und erhält hierdurch rechtsklare(re) Konturen.

ee) Auditabilitätsherstellende Begründung und Vorhersehbarkeit

Verbunden mit der datenschutzrechtlichen Auditabilität als Zielvorgabe liefert das Begründungsmodell eine gute Lösung für den Umgang mit Intransparenzen in der DSGVO. Für automatisierte Systeme hat der Unionsgesetzgeber in Art. 22 Abs. 3 DSGVO spezifische Schutzinstrumente vorgesehen. Mit dieser ist das Transparenzverständnis zu koppeln: Es ist eine solche menschliche Verständlichkeit herzustellen, die eine effektive Wahrnehmung des Art. 22 Abs. 3 DSGVO erlaubt.[231] Art. 22 Abs. 3 DSGVO zielt auf eine Überprüfung durch

---

[229] Siehe nur *Martini*, Blackbox Algorithmus, 2019, S. 197; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; *Kaminski*, BTLJ 34 (2019), 189, 213 f. In diese Richtung auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 200 f. Sehr allgemein zu Inhalten der Begründungspflicht, dort dann allein hinsichtlich des Einsatzes autonomer Systeme durch staatliche Akteure, *Wischmeyer*, AöR 143 (2018), 1, 59 f.

[230] Vgl. zu diesem Gedanken *Kaminski*, BTLJ 34 (2019), 189, 213: „the substance of other underlying legal rights often determines transparency's substance".

[231] Zu diesem Ansatz eingehend *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284–286, die dies als „Recht auf Rechtfertigung" bezeichnen. Ebenso Gola, DS-GVO/*Schulz*, Art. 22 Rn. 34; Gola, DS-GVO/*Franck*, Art. 15 Rn. 18. Diese funktionale Verknüpfung betonen auch *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233, 236; *Kaminski*, BTLJ 34 (2019), 189, 213 f.; *Dimitrova*, EDPL 6 (2020), 211, 229. Ähnlich Kuner/Bygrave/Docksey, GDPR/*Polčák/Radim*, Art. 12 Rn. 407: „[R]equest controllers [...] to make [algorithms or computer codes] available in compiled form for testing or reverse engineering". Auch der Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 58 – *SCHUFA Holding* deutet ein solches Verständnis der Informationspflichten

die betroffene Person, im Übrigen auf eine Kontrolle und Abänderung bzw. Übernahme einer automatisierten Entscheidung durch einen menschlichen Entscheider ab.[232] Denkbar ist zwar auch, dass die Selbst- und Fremdkontrolle automatisiert erfolgt; bislang sind hierfür aber nur bedingt technische Methoden entwickelt.[233] Es ist demnach ein Verständlichkeitsniveau zu erreichen, das sowohl der betroffenen Person als auch menschlichen Akteuren auf Seiten des Verantwortlichen sowie staatlichen Institutionen eine Überprüfung der automatisierten Entscheidung erlaubt.[234] Inhaltliche Prüfungskriterien, die eine noch weitere Spezifizierung des Verständlichkeitsniveaus erlaubten, gibt die DSGVO nur bedingt vor, denn über die prozessuale oder inhaltliche Angemessenheit einer automatisierten Entscheidung sagt die DSGVO nichts aus. Der inhaltliche Prüfungsmaßstab bemisst sich demnach nach außerdatenschutzrechtlichen, individuellen Angemessenheitskriterien. Der Unionsgesetzgeber deutet an, dass es vor allem um basale Angemessenheitskriterien wie die Feh-

---

an („Generell sollte der Verantwortliche der betroffenen Person allgemeine Informationen übermitteln, […], die auch für die Anfechtung von ‚Entscheidungen' im Sinne von Art. 22 Abs. 1 DSGVO seitens der betroffenen Person nützlich sind").

[232] Vgl. *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284 f. Art. 22 Abs. 3 DSGVO lässt gleichwohl offen, ob die Anhörung des eigenen Standpunktes sowie die Anfechtung durch einen Menschen oder ein anderes automatisiertes System umzusetzen sind, vgl. hierzu eingehend *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 873. Nach der überwiegenden Ansicht in der Literatur zielen die Art. 22 Abs. 3 DSGVO auf die Übernahme der Entscheidung durch einen Menschen ab. Siehe eingehend *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284, 286. Ebenso Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Weichert*, Art. 22 Rn. 55, 63; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 31; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 57, 59; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 70; Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Atzert*, Art. 22 Rn. 138. Unklar dagegen der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 30 f., der ebenso technische Korrektur- und Kontrollmechanismen benennt.

[233] Sollen technische Verfahren zur Anhörung bzw. Kontrolle eingesetzt werden, müssten autonome Systeme fähig sein, algorithmische Lösungen eines anderen Systems kritisch zu begutachten und zu einem anderen Ergebnis als dem des kontrollierten Systems zu kommen. Da autonome Systeme, insbesondere solche des Maschinellen Lernens, mit denselben bzw. ähnlichen Methoden arbeiten und zur kritischen Selbstdistanz nicht fähig sind, ist eine derartige Nachprüfung, zumindest mit den derzeitigen technischen Verfahren, nur begrenzt denkbar. Zu erwarten sind vielmehr Bestätigungsschleifen der Entscheidung mit kleineren Abweichungen. So auch *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284 f. Zum Fehlen kritischer Selbstdistanz bei automatisierten Systemen siehe auch *Ernst*, JZ 72 (2017), 1026, 1028 f.

[234] *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284 f. Allein auf die betroffene Person abstellend *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 197–199; *Dimitrova*, EDPL 6 (2020), 211, 229; *Kaminski*, BTLJ 34 (2019), 189, 213 f. Vgl. auch Gola, DS-GVO/*Schulz*, Art. 22 Rn. 34.

lerfreiheit und Diskriminierungsfreiheit der Entscheidung geht.[235] Für diese Prüfung bedarf es dann einer menschlich verständlichen Darlegung der tragenden Entscheidungskriterien und deren Bedeutung für die Entscheidung.[236] Dieses Verständnis wird auch von der Norwegischen Datenschutzbehörde geprägt,[237] vom Europäischen Datenschutzausschuss wird es zumindest angedeutet.[238] Was dies im Einzelnen bedeutet, wann also ein Entscheidungskriterium als tragend zu werten ist, ist sogleich noch näher zu erläutern.[239]

ff) Auditabilitätsherstellende Vorhersehbarkeit

Dies ist aber nur die eine Dimension der Transparenz. Im dezentralen Regulierungsregime der DSGVO dienen Transparenzangebote zudem der Ermöglichung der Ausnahmezulassung nach Art. 22 Abs. 2 lit. a) und lit. c) DSGVO. Hierfür bedarf es der Vorhersehbarkeit der Folgen einer automatisierten Entscheidung. Letztlich geht es um die Ermöglichung einer Risikoeinschätzung für die betroffene Person. Es bedarf aber auch eines grundlegenden Verständnisses vom algorithmischen Regelwerk, denn nur so kann die betroffene Person einschätzen, mit welchen Entscheidungsinhalten und Folgen der automatisierten Entscheidung sie rechnen muss. Anders als bei der nachträglichen Informationspflicht zielt die Transparenz hier nicht darauf ab, der betroffenen Person eine inhaltliche Überprüfung der Entscheidung zu ermöglichen. Es ist vielmehr ein solches Verständnisniveau zu erreichen, das der betroffenen Person eine Risikovorhersage ermöglicht, d.h. eine Prognose des Entscheidungsergebnisses und der Folgen anzustellen, um anhand dessen eine Ausnahmezulassung nach Art. 22 Abs. 2 DSGVO zu erteilen.[240] Dafür ist es nicht notwendig, das

---

[235] Siehe Erwägungsgrund 71 S. 6.

[236] *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 286. Sie sprechen von einem „kriterialen Ansatz". Ähnlich Gola, DS-GVO/*Schulz*, Art. 22 Rn. 42; *Kaminski*, BTLJ 34 (2019), 189, 214. Vgl. auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 197–199.

[237] Explizit *Norwegian Data Protection Authority*, Artificial intelligence and privacy, Norwegian Data Protection Authority, Januar 2018, S. 21.: „[T]he data controller must provide as much information as necessary in order for the data subject to exercise his or her rights".

[238] *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 30: „Der Verantwortliche sollte der betroffenen Person allgemeine Informationen übermitteln (vor allem zu bei der Entscheidungsfindung berücksichtigten Faktoren und deren ‚Gewichtung' auf aggregierter Ebene), die auch für die Anfechtung der Entscheidung seitens der betroffenen Person nützlich sind. [...] Die betroffene Person kann eine Entscheidung nur anfechten bzw. ihren Standpunkt nur darlegen, wenn ihr vollkommen klar ist, wie und auf welcher Grundlage die Entscheidung zustande gekommen ist".

[239] Siehe unten Kapitel 5 B. III. 3. a) bb) (2).

[240] Ein solches Recht auf Erklärung ex ante, zumindest bei risikoreichen automatisierten Entscheidungen, fordert auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 201. Angedeutet auch bei *Kaminski*, BTLJ 34 (2019), 189, 214 f., in diese Richtung auch Wolff/

gesamte Regelwerk aufzudecken. Ausreichend ist es, die wesentlichen Entscheidungsparameter und deren Gewicht zu kennen. Auch hierauf ist noch zurückzukommen. Im Ergebnis ist es daher richtig, zwischen vorherigen und nachträglichen Informationspflichten zu unterscheiden.

c) Grenzen eines betroffenenbezogenen Transparenzmodells

Diese Erläuterungsmodelle liefern für die technische Illiteralität sowie für menschliche Kognitionsgrenzen gute Lösungen. Ab einer bestimmten Komplexitätsschwelle wird man aber an Grenzen stoßen. Bei Algorithmen aus Maschinellen Lernverfahren, die menschlich nicht nachvollziehbar sind, wird man eine Verständlichkeit im oben beschriebenen Sinne dagegen nur in beschränktem Maße herstellen können. Um dann noch sinnvoll regulieren zu können, muss zwischen den Arten der Intransparenz unterschieden werden: Soweit die Verfahren noch von ExpertInnen verstanden werden können, können Regulierungsmethoden auf diese umgelegt werden, Transparenzanforderungen also an ExpertInnen gerichtet werden. Anstelle eines dezentralen Regulierungsregimes, wie es die DSGVO etabliert, tritt dann ein zentralisiertes, expertenbasiertes Steuerungssystem.[241] Soweit die Verfahren gänzlich menschlich nicht mehr verständlich sind, bleibt nur, entweder – gegebenenfalls unter Einführung sonstiger Regulierungsmethoden – auf Transparenz zu verzichten oder auf Transparenz zu beharren. Im Ergebnis ist dies eine Entscheidung zwischen Technikermöglichung und Technikverhinderung[242] und fordert eine kluge Abwägungsentscheidung.

In manchen Bereichen wird man womöglich bereit sein, auf menschliche Verständlichkeit zu verzichten und die Ergebnisrichtigkeit oder ein Funktionsoptimum für ausreichend zu halten. Dies verweist auf eine risikobasierte Konstruktion des Verständlichkeitserfordernisses, hierauf ist noch zurückzukommen.[243] Viele stehen einem solchen Ansinnen kritisch gegenüber, sie be-

---

Brink, BeckOK Datenschutzrecht/*Lewinski*, Art. 22 Rn. 55. Vgl. allgemein zu den Transparenzanfordernissen im Rahmen des Art. 22 Abs. 2 lit. c) DSGVO auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 52; Gola, DS-GVO/*Schulz*, Art. 22 Rn. 40.

[241] Ex-ante-Kontrollen durch ExpertInnen, zumindest bei risikoreichen Datenverarbeitungen, fordert etwa *Martini*, Blackbox Algorithmus, 2019, S. 229 f. Den Einbezug von Verbraucherschutz- oder Fachbehörden befürwortet auch der *European Parliamentary Research Service*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Juni 2020, S. 51 f. So auch *Tutt*, Admin. L. Rev. 69 (2016).

[242] So im Ergebnis auch *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 39 f.

[243] Siehe unter Kapitel 5 C. III. a) bb) (2). Siehe zu einem derartigen risikobasierten Ansatz des Transparenzgrundsatzes auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 187–192, dort dann für die Existenz eines Rechts auf Erklärung, sowie Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53 für die Existenz besonderer Informa-

fürchten ein „Ende der Theorie“[244] und bezweifeln, dass a-kausales Wissen tatsächlich brauchbar ist.[245] Sie verweisen überdies darauf, dass ohne Verständlichkeit eine Qualitäts- und Rechtmäßigkeitskontrolle und eine Fehlerbereinigung gar nicht stattfinden kann.[246]

Jenseits der Transparenz bleiben dann nur Regulierungsmethoden, die an den Algorithmen und am Maschinellen Lernverfahren ansetzen und durch inhaltlich-substantielle Vorgaben und umfassende Kontrollmechanismen die Sicherheit und Angemessenheit der autonomen Systeme absichern. Diese Regulierungsmechanismen liegen aber jenseits des Regulierungszugriffs der DSGVO.[247] Sie sollen im Anschluss kurz skizziert werden.

d) Ergebnis

Über die Definition einer rechtsnormativen Verständlichkeit ist es möglich, der fehlenden Nachvollziehbarkeit autonomer Systeme für den technischen Laien

---

tionspflichten jenseits des Art. 22 DSGVO. Siehe auch *Sesing*, MMR 24 (2021), 288, 291; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17, dort für den Inhalt der Informationspflichten hinsichtlich automatisierter Entscheidungen.

[244] So etwa *Anderson*, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, Wired 23.06.2008, https://www.wired.com/2008/06/pb-theory/.

[245] Siehe etwa *Hildebrandt/Koops*, The Modern Law Review 73 (2010), 428, 432; *Martini*, Blackbox Algorithmus, 2019, S. 60; *Anderson*, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, Wired 23.06.2008, https://www.wired.com/2008/06/pb-theory. Siehe auch *Schmarzo*, Is Data Science Really Science?, 02.02.2017 (https://www.linkedin.com/pulse/data-science-really-bill-schmarzo), dessen Aussagen über die Tätigkeit als Data Scientist auf den Erkenntnisgewinn durch Maschinelle Lernverfahren übertragbar sind: „As a data scientist, I can predict what is likely to happen, but I cannot explain why it is going to happen. I can predict when someone is likely to attrite, or respond to a promotion, or commit fraud, or pick the pink button over the blue button, but I cannot tell you why that's going to happen. And I believe that the inability to explain why something is going to happen is why I struggle to call ‚data science' a science“.

[246] Ein bekanntes Beispiel ist ein (wohl vermeintliches) Projekt des amerikanischen Verteidigungsministeriums in den 1980er Jahren zur Erstellung eines künstlichen neuronalen Netzes, das Bilder von Panzern erkennen sollte. Nach einer Trainingsphase mit Fotographien, die Panzer enthielten und solche ohne, gab das künstliche neuronale Netz tatsächlich präzise Ergebnisse aus. Bei Konfrontation mit einem Bildersatz aus einer anderen Serie waren die Ergebnisse allerdings unbrauchbar. Als Ursache hierfür konnte man schließlich aufdecken, dass in der Trainingsphase alle Bilder mit Panzern an einem sonnigen, alle ohne Panzer an einem bewölkten Tag aufgenommen worden waren. So lernte das künstliche neuronale Netz nicht die Panzer, sondern die Beleuchtungslage zu unterscheiden. Vgl. zu diesem Beispiel *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, ^{6}2021, S. 571, 572. In dieser Konstellation ließ sich die Fehlerquelle aufdecken. Je komplexer und divergenter der Trainingsdatensatz ist, desto schwieriger wird es allerdings werden, fehlerhafte Muster des künstlichen neuronalen Netzes aufzudecken, eben da die Inhalte jenes Musters dem Menschen verborgen bleiben.

[247] Siehe unter Kapitel 5 A. I.

zu begegnen. Sinnvollerweise ist diese Verständlichkeit instrumentell, d.h. aus den spezifischen Schutzrechten zu entwickeln. Die DSGVO sieht in Art. 22 Abs. 3 DSGVO ein spezifisches Schutzinstrument für automatisierte Entscheidungen vor. Ziel der Verständlichkeit ist damit eine Begründung, die der betroffenen Person eine Prüfung der Entscheidung anhand individueller Richtigkeitskriterien ermöglicht. Zugleich bedarf es einer Verständlichkeit, die der betroffenen Person eine Prognose von Entscheidungsinhalten erlaubt, um eine Ausnahmezulassung nach Art. 22 Abs. 2 DSGVO zu erteilen. Die inhaltlich vagen Modelle eines Lesbarkeitstests oder einer kontrafaktischen Erläuterung erscheinen dagegen nicht ergiebig. Gleichwohl: Die hier vorgeschlagenen Modelle auditabilitätsherstellender Begründung und Vorhersehbarkeit erlauben nur bis zu einer gewissen Komplexitätsschwelle der eingesetzten selbstlernenden Algorithmen gute Lösungen. Jenseits dessen sind transparenzunabhängige Steuerungsmodelle zu entwickeln.

Die hier vorgestellten Ansätze zur Herstellung menschlicher Verständlichkeit betreffen die inhaltliche Frage der Transparenz autonomer Systeme. Sie adressieren dagegen nicht die Problematik der quantitativen und qualitativen Überforderung hinsichtlich des bereitgestellten Informationsmaterials. Dies betrifft Aspekte der kognitionsfreundlichen Ausgestaltung der Informationen und bedarf eigener Lösungsansätze. Dies zeigt, dass die im Hinblick auf Maschinelle Lernverfahren geführte Debatte zum Recht auf Erklärung verengt ist: Sie bildet nur einen der Teilaspekte eines effektiven Transparenzmodells ab.[248]

3. De lege lata

Vertiefte Informationen zum Auswertungsverfahren autonomer Systeme sind im geltenden Recht allein für automatisierte Entscheidungen vorgesehen. Zur Effektivierung dieses Transparenzprogramms ist der Inhalt näher zu präzisieren (a)). Insbesondere die Einführung eines Rechts auf Erklärung als Methode zum Umgang mit nicht nachvollziehbaren Datenverarbeitungen trägt zu einer Optimierung der Steuerungseffektivität der DSGVO bei. Auch die Ausgestaltung des Informationsmaterials durch visuelle sowie videographische Aufbereitung kann zu einer Stärkung der Betroffenentransparenz beitragen (b)). Auch technische Methoden erscheinen vielversprechend (c)).

---

[248] Vgl. auch *Bygrave*, in: Yeung/Lodge (Hrsg.), Algorithmic regulation, 2019, S. 248, 259: „[I]t is perhaps unfortunate that much of the noise surrounding [the] possible future has emenated from debate around wether or not Article 22 and other parts of the Regulation provide for a right to ex post explanation of automated decisions. The long-term health of human rights and freedoms will not depend simply or even largely on the availabilty of such a right".

a) Inhalt der besonderen Informationspflichten und Recht auf Erklärung

Die besonderen Informationspflichten sind sinnvollerweise nur auf die grundlegende technische Funktionsweise des Entscheidungsalgorithmus zu erstrecken (aa)). Ein Recht auf Erklärung ist ein geeignetes Instrument, um mit der fehlenden Nachvollziehbarkeit von automatisierten Entscheidungen umzugehen (bb)). Auch eine zeitliche Differenzierung des Informationsprogramms trägt zu einer Stärkung des Transparenzgrundsatzes bei (cc)).

aa) Aufdeckung der grundlegenden Funktionsweise

Bereits mit den Erkenntnissen des Kapitels 4 D. wurde klar, dass die Offenlegung des Algorithmus nicht die richtige Lösung sein kann. Dies erwiese sich als innovationsfeindlich und mit unternehmerischen Interessen unvereinbar, vor allem aber wäre für die Steuerungseffektivität nichts gewonnen: Die betroffene Person könnte weder mit dem Quellcode, noch einem Protokoll der Berechnungsschritte, noch mit dem Output etwas anfangen.[249] Dies spricht dafür, nur die grundlegende Funktionsweise der Entscheidungen autonomer Systeme beschreibend darzulegen.[250] Der Transparenzbedarf bemisst sich dabei, hierzu im Anschluss im Rahmen des Rechts auf Erklärung genauer,[251] anhand des Risikos der automatisierten Entscheidung sowie des Umfangs der Intransparenz.[252] Je höher der Transparenzbedarf, desto tiefer und umfassender ist auch die algorithmische Entscheidungsarchitektur zu beschreiben.

bb) Recht auf Erklärung (Right to Explanation)

Die Darlegung der wesentlichen Funktionsweise des Entscheidungsalgorithmus reicht aber nicht aus: Die betroffene Person wird ab einer bestimmten Komplexitätsstufe, erst recht dann bei nicht nachvollziehbaren selbstlernenden Algorithmen, nicht verstehen können, wie ein autonomes System zu einer bestimmten Entscheidung gelangt(e). Es bedarf also zusätzlicher Erläuterung, d.h. Einordnung in menschliche und laienhafte Verständniszusammenhänge.[253]

---

[249] Siehe Kapitel 4 D. III. 3. b aa) (1). Siehe auch Kapitel 4 D. IV. 2. d) aa) sowie Kapitel 4 D. IV. 2. d) ee). Siehe auch Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 57 – *SCHUFA Holding* sowie *Martini*, Blackbox Algorithmus, 2019, S. 181 f.; *Wischmeyer*, AöR 143 (2018), 1, 51 f.

[250] Siehe eingehend mit zahlreichen Nachweisen oben Kapitel 4 D. III. 3. b) aa) (2).

[251] Siehe unter Kapitel 5 B. III. 3. b) bb) (2).

[252] Zu einem solchen risikobasierten Ansatz siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16; *Sesing*, MMR 24 (2021), 288, 291. In diese Richtung auch Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 54. Ähnlich *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 197 f. Vgl. auch *Wischmeyer*, AöR 143 (2018), 1, 63.

[253] Plakativ *Mittelstadt*, Int. J. Commun. 10 (2016), 4996: „Thus, an algorithm is opaque when a user can access but not interpret information about the algorithm". Vgl. auch *Euro-*

Hier setzt das Recht auf Erklärung an. Mit dem Recht auf Erklärung wird eine rechtliche Pflicht zur Bereitstellung ergänzender Erläuterungen zur „involvierten Logik" begründet und also die oben bereits benannten Bestrebungen[254] zur Herstellung menschlicher Verständlichkeit von Entscheidungen autonomer Systeme zu einem subjektiven Anspruch der betroffenen Person auf Erklärung geformt.[255]

Das Recht auf Erklärung hat eine zeitliche und eine inhaltliche Dimension: In temporeller Hinsicht geht es um Transparenzpflichten im Nachgang einer automatisierten Entscheidung, in substantieller Hinsicht um eine Herstellung laienhafter Verständlichkeit einer automatisierten Entscheidung. Die normative Anknüpfung eines solchen Rechts ist in der Literatur äußerst umstritten; dies soll hier nur kurz skizziert werden ((1)). Mit den obigen Ausführungen ist eine Ausgestaltung als auditabilitätsherstellende Begründung überzeugend, deren Inhalt über ein risikobasiertes Verständnis noch näher konkretisiert werden kann ((2)). Hieraus lässt sich auch ableiten, welche bei der automatisierten Entscheidung verwendeten Profilinhalte offenzulegen sind (3).

(1) Normative Anknüpfung eines Rechts auf nachträgliche Erläuterung de lege ferenda

Ein Recht auf Erklärung ist nicht ausdrücklich in der DSGVO normiert.[256] Weder der EuGH noch Europäischer Datenschutzausschuss haben sich bislang zu einem Recht auf Erklärung geäußert.[257] Der Generalanwalt beim EuGH Pikamäe fordert, zumindest für das Kredit-Scoring, „hinreichend detaillierte Erläuterungen zur Methode für die Berechnung des Score-Werts und zu den Gründen

päischer Datenschutzausschuss, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 27 f. sowie Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 56 – *SCHUFA Holding* „geeignete Kommunikationsmittel, die das Verständnis erleichtern".

[254] Siehe Kapitel 5 B. III. 3. b).

[255] Siehe etwa Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76 f.; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277.

[256] In Erwägungsgrund 71 S. 5 ist allerdings von einer „spezifischen Unterrichtung der betroffenen Person" die Rede. Die Diskussion um ein Recht auf Erklärung wurde eingeführt von *Goodman/Flaxman*, AI Magazine 38 (2017), 50–57, die als erstes von einem solchen Recht sprachen, ohne aber die normative Anknüpfung oder die Inhalte näher darzulegen. Sehr umfassend zu den rechtlichen Grundlagen und datenschutzrechtlichen Kohärenz eines Rechts auf Erklärung *Dimitrova*, EDPL 6 (2020), 211–230.

[257] Siehe nur *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 18 f.; *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11.04.2018, S. 26 f.

(…), die zu einem bestimmten Ergebnis geführt haben".[258] Für das Recht auf Erklärung werden drei Anknüpfungspunkte diskutiert: Art. 13 Abs. 2 lit. f), 15 Abs. 1 lit. h) DSGVO in der Gesamtschau[259], allein Art. 15 Abs. 1 lit. h) DSGVO[260] oder Art. 22 Abs. 3 DSGVO[261]. [262] Gegen[263] eine Anknüpfung in Art. 13 und Art. 15 DSGVO wird vorgebracht, dass Art. 13 DSGVO nur vorherige Informationspflichten kennt,[264] gegen eine solche in Art. 15 DSGVO, dass dessen Informationsprogramm mit Art. 13 Abs. 2 lit. f) gleichläuft.[265]

---

[258] Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 58 – *SCHUFA Holding*.

[259] So etwa *Felzmann/Villaronga/Lutz u.a.*, Big Data and Society 6 (2019), 1, 3; *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233–242; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 177; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 15 Rn. 25.

[260] So etwa *Kaminski*, BTLJ 34 (2019), 189, 200; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 255; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 193–195; *Edwards/Veale*, SSRN Journal 2017, 51 Ähnlich *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung, April 2018, S. 30 f. So auch Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 53–58 – *SCHUFA Holding*.

[261] Eingehend *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284–286. Ebenso Gola, DS-GVO/*Schulz*, Art. 22 Rn. 42; Kühling/Buchner, DS-GVO, BDSG/*Buchner*, Art. 22 Rn. 32; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Scholz*, Art. 22 Rn. 57; Sydow, DS-GVO/*Helfrich*, Art. 22 Rn. 71; *Kaminski*, BTLJ 34 (2019), 189, 204, 211-212; *Martini*, Blackbox Algorithmus, 2019, S. 189 f.; Gola, DS-GVO/*Franck*, Art. 15 Rn. 19; *Sesing*, MMR 24 (2021), 288, 292. Erwähnung findet ein solches Recht im Übrigen in Erwägungsgrund 71 S. 4, demzufolge eine „spezifische[.] Unterrichtung der betroffenen Person und […] [eine] Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung" erfolgen soll.

[262] *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233, 235–237 leiten das Recht auf Erklärung aus einer Gesamtschau der Normen Art. 13, Art. 15 und Art. 22 Abs. 3 DSGVO ab.

[263] Sämtliche Ansätze müssen sich entgegenhalten lassen, dass die Vorgängervorschrift des Art. 12 lit. a) letzter Spiegelstrich Datenschutzrichtlinie allein ein Auskunftsrecht vorsah, ohne dass dieses als nachträgliches Erklärungsrecht verstanden wurde. Siehe hierzu *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 85–89 unter ausführlicher Auswertung verschiedener nationaler Umsetzungsakte. Siehe auch *Wischmeyer*, AöR 143 (2018), 1, 50 f. Das Gesetzgebungsverfahren lässt sogar auf Gegenteiliges schließen: Ein Recht auf Erklärung war von Seiten des Europäischen Parlaments vorgeschlagen worden, fand dann aber nicht die notwendigen Mehrheiten. Siehe eingehend hierzu *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 81. Ebenso *Edwards/Veale*, SSRN Journal 2017, 49 f. Plakativ *Temme*, EDPL 3 (2017), 473, 482: „[T]he legal basis for a right to explanation in the GDPR seems rather shaky and inconclusive".

[264] Zu dieser Begrifflichkeit *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 99.

[265] Dies ergibt sich aus der identischen Wortwahl der Vorschriften, so *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 84, 97; *Wachter/Mittelstadt/Russell*, Harv. J. Law Technol. 31 (2018), 841, 870 f.; *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 283; *Martini*, Blackbox Algorithmus, 2019, S. 192. Vgl. auch Plath, DSGVO/BDSG/*Kamlah*, Art. 15 Rn.

Vielfach wird für eine Anknüpfung an Art. 22 Abs. 3 DSGVO geworben, wo das Recht auf Erklärung zwar nicht explizit vorgesehen ist,[266] aber die dort genannten Mindestmaßnahmen überhaupt erst ermöglicht.[267]

(2) Inhalte eines Rechts auf Erklärung: risikobasierte, auditabilitätsherstellende Begründung

Hinsichtlich des Inhalts eines Rechts auf Erklärung werden, dies ist bereits oben ausgeführt worden, verschiedene Ansätze vorgebracht.[268] Überzeugend ist am Ende eine auf datenschutzrechtliche Auditabilität abzielende, d.h. eine die Wahrnehmung der Betroffenenrechte in Art. 22 Abs. 3 DSGVO ermöglichende menschliche Verständlichkeit.[269] Darzulegen sind demnach die grundlegenden Entscheidungsparameter und deren Gewicht für die Entscheidung, die der betroffenen Person eine Prüfung der automatisierten Entscheidung anhand individueller Angemessenheitskriterien, vor allem dann die Fehler- und Diskriminierungsfreiheit, erlaubt. Dabei geht es um eine laienhaft verständliche Aufbereitung, bei selbstlernenden Systemen um eine originäre Einordnung der automatisierten Entscheidung in menschliche Verständniszusammenhänge.

Unklar ist, welche Entscheidungsparameter als grundlegend gelten können. Denn aus mathematischer Sicht ist ein jeder Parameter tragend.[270] Eine Offen-

---

14. Auch auf die prognostische Formulierung in Art. 15 Abs. 1 lit. h) DSGVO („angestrebte Auswirkungen") wird hingewiesen, so *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 283; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 83; *Martini*, Blackbox Algorithmus, 2019, S. 192. Systematische Argumente führt schließlich *Wischmeyer*, AöR 143 (2018), 1, 51 an. Vgl. auch die Kommentarliteratur zu Art. 13 und Art. 15 DSGVO, die vielfacht von einer Inhaltsgleichheit der Vorschriften ausgeht, siehe nur Plath, DSGVO/BDSG/*Kamlah*, Art. 15 Rn. 14; Wolff/Brink, BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 13 Rn. 77. Auch die Artikel 29 Datenschutzgruppe prägt dieses Verständnis, siehe *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 29 f. AA *Selbst/Powles*, Int. Data Priv. Law 7 (2017), 233, 241; *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 195 f.; *Malgieri/Comandé*, Int. Data Priv. Law 7 (2017), 243, 256, die den Fokus auf die Unterschiedlichkeit der Formulierungen legen.

[266] *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 281; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 79–82; *Edwards/Veale*, SSRN Journal 2017, 44 f.

[267] Zu diesem Ansatz ausführlich *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 284–286.

[268] Siehe oben Kapitel 5 B. III. 2. b).

[269] Siehe oben Kapitel 5 B. III. 2. b) ee).

[270] Fließt in einen Kreditscore etwa die Kredithistorie zu 40 %, die Vermögenslage zu 40 %, der Wohnort zu 15 %, das Alter zu 5 % ein, ist auch das Alter ein Merkmal, das den Ausschlag für oder gegen eine Kreditzusage gegeben haben kann. Auch die Definition eines Schwellenwerts ist viel zu pauschal und wird nicht in jeder Anwendungskonstellation zu guten Ergebnissen führen. Bei einem Entscheidungssystem, in dem sämtliche Parameter nur zu 5 % einfließen, müsste etwa, wenn der Schwellenwert auf 10 % festgelegt würde, überhaupt kein Parameter aufgedeckt werden.

legung sämtlicher Entscheidungsparameter würde die betroffene Person allerdings überfordern, ist bei nicht nachvollziehbaren Auswertungsverfahren kaum möglich und würde vor allem schutzwürdige Interessen des Verantwortlichen unangemessen beeinträchtigen.[271] Das Spannungsverhältnis lässt sich nur über eine normative Abwägung und damit einen im Einzelfall zu bestimmenden Inhalt des Rechts auf Erklärung auflösen.

Hierfür lassen sich Kriterien aufstellen. Maßgeblich ist zum einen das Risiko der automatisierten Entscheidung,[272] zum anderen das Maß der Intransparenz und Unverständlichkeit der automatisierten Entscheidungsarchitektur.[273] Dies berücksichtigt, dass in jeder Fallkonstellation unterschiedliche Steuerungs- und also Transparenzbedarfe bestehen und die eingesetzten Algorithmen ein ganz unterschiedliches Maß an Intransparenz aufweisen. Für automatisierte Kreditentscheidungen besteht dann in der Regel ein höherer Transparenzbedarf als für personalisierte Preisbildungen im Kleinstbetragsbereich. Für selbstlernende Algorithmen aus komplexen Maschinellen Lernverfahren besteht ein höherer Aufklärungsbedarf als bei einfachen Wenn-Dann-Entscheidungsregeln. Die betroffene Person wird vor allem ein Interesse an der Offenlegung von Entscheidungsparametern haben, mit denen sie nicht rechnet.[274] Ob

---

[271] So aber wohl *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 285 f., die eine Darlegung ganz allgemein der Entscheidungskriterien verlangen, ohne hierbei Einschränkungen vorzunehmen.

[272] Zu einem derartigen risikobasierten Ansatz siehe auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16; *Sesing*, MMR 24 (2021), 288, 291. Ebenso *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 186. Ähnlich *Wischmeyer*, AöR 143 (2018), 1, 63: „Je gewichtiger die gesellschaftliche Funktion des Entscheidungssystems ist, desto tiefer wird eine solche Analyse dringen müssen". Vgl. überdies *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 197–199. Ähnliche Gedanken bei *Martini*, JZ 72 (2017), 1017, 1021; *Martini*, Blackbox Algorithmus, 2019, S. 347, der für die algorithmenbasierte Nachrichtenauswahl besondere Transparenzpflichten fordert.

[273] Eine Klassifizierung von selbstlernenden Algorithmen anhand ihres Umfangs der Intransparenz schlägt *Tutt*, Admin. L. Rev. 69 (2016), 107 vor. Er entwickelt ein Modell mit fünf Intransparenzstufen: deterministische Algorithmen (whitebox), nicht-deterministische, aber verständliche Algorithmen (grey box), Algorithmen ohne erkenntliche Merkmale (Black Box), Algorithmen, die den Turing-Test bestehen (satient) und Algorithmen, die sich selbst verbessern können (singularity). Vgl. zu einem derartigen am Verständnisnivau des Laien und damit dem Umfang der Intransparenz orientierten Konzept des Rechts auf Erklärbarkeit *Kaminski*, BTLJ 34 (2019), 189, 215.

[274] So auch mit Anwendungsbeispiel *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 197–199. Vgl. zu diesem Ansatz auch *Ernst*, JZ 72 (2017), 1026, 1035, der hieraus aber ein Verbot derartiger überraschender Kriterien in der Entscheidungsfindung nach Art. 22 DSGVO ausspricht (diese sind dann nicht erforderlich nach Art. 22 Abs. 2 lit. c) DSGVO). Mit welchen Entscheidungskriterien eine betroffene Person rechnen muss, ist eine normative Wertungsfrage. Hierfür ist auf den objektive Empfängerhorizont und den Anwen-

ein überraschendes Merkmal aufzudecken ist, bestimmt sich dann aber wiederum anhand des Risikos der Datenverarbeitung. Bei einer automatisierten Kreditvergabe müsste etwa dargelegt werden, dass das Halten eines Haustieres in die Kreditscorebildung einfließt, da es sich um eine risikoreiche Anwendung handelt und dieses Merkmal objektiv überraschend ist. Demgegenüber wird eine Person bei einer personalisierten Preisbildung im Kleinstbetragsbereich kaum ein Interesse daran haben, dass etwa die Wetterlage – ein objektiv überraschendes Merkmal – in die automatisierte Preisberechnung einbezogen wurde.

(3) Inhalte eines Rechts auf Erklärung bei profilbasierten Entscheidungen

Wird die Entscheidung maßgeblich auf ein Profil gestützt, erstreckt sich das Recht auf Erklärung in dem hier vorgestellten Verständnis auch auf verwendete Profilinhalte: Da die Profilinhalte ihrerseits Entscheidungsparameter sind, ist auch über diese zu informieren, wenn die automatisierte Entscheidung sich als risikoreich darstellt. Auch die Sensibilität des Profilinhalts kann ihrerseits, d.h. unabhängig von dem Risiko der automatisierten Entscheidung, risikobegründend sein – hierzu sogleich – und eine Pflicht zur Offenlegung begründen. Auch über die Verwendung besonders umfassender oder tiefgehender Profilinhalte ist demnach zu informieren. Wenn ein Kreditinstitut etwa den Gesundheitszustand einer Person in die Entscheidung einfließen lässt, etwa die Schwangerschaft einer Person – es handelt sich um eine risikoreiche automatisierte Entscheidung sowie einen sensiblen Profilinhalt, der zugleich überraschend ist –, muss dies offengelegt werden.

cc) Zeitliche Differenzierung der Informationspflichten und vorherige Erläuterungspflichten

Auch im Vorhinein bedarf es Informationen zur technischen Funktionsweise. Dort geht es dann darum, eine Ausnahmezulassung nach Art. 22 Abs. 2 lit. a) und c) DSGVO zu ermöglichen sowie Hemmeffekte aufgrund der intransparenten Entscheidungsarchitektur abzuwehren. Ziel ist die Herstellung der Vorhersehbarkeit der Folgen der automatisierten Entscheidung. Bei der Kreditentscheidung ist es gerade essentiell, die Wahrscheinlichkeit einer Vertragszusage oder -absage einschätzen zu können, bei personalisierten Vertragsgestaltungen, ist es dagegen ausreichend, zu wissen, welche Vertragsbedingungen grundsätzlich denkbar sind. Zur Aktivierung dieser Dimension ist notwendig, aber auch ausreichend, die allgemeine Systemfunktionalität für die betroffene Person verständlich zu machen, d.h. grundlegende Entscheidungsparameter und deren Gewicht offenzulegen. Die vorherigen Informationspflichten können demnach

---

dungskontext und Zweck der Anwendung abzustellen. So auch *ders.*, JZ 72 (2017), 1026, 1035.

gegenüber den nachträglichen abstrakter ausfallen.[275] Auch hier ist das Risiko der automatisierten Entscheidung und der Umfang der Intransparenz maßgeblich.[276]

Die fehlende Nachvollziehbarkeit von Verarbeitungen durch autonome Systeme kann auch hier problematisch sein, nämlich dann, wenn die betroffene Person mögliche Ergebnisse überhaupt nicht mehr prognostizieren kann. In diesem Fällen erscheint ein „Recht auf Erklärung" im Vorhinein, d.h. auf Einordnung der erwarteten Ausgaben einer Entscheidung in laienhaft bzw. menschlich verständliche Konsistenzzusammenhänge, geboten.[277] Auch hier ist der Umfang der Erläuterung einzelfallbezogen, dann also anhand des Risikos einer automatisierten Entscheidung und Art und Umfang der Intransparenz zu bestimmen. Ziel ist hierbei allerdings nicht, die betroffene Person zur Prüfung von Fehlern oder der inhaltlichen Unangemessenheit der erst noch erfolgenden Entscheidung zu befähigen, sondern ihr eine Einschätzung der (nachteiligen) Folgen der Entscheidung zu ermöglichen.

b) Kognitionsfreundliche Aufbereitung durch visuelle und videographische Aufbereitung

Um die Intransparenzen aufgrund quantitativer und qualitativer Überforderung des Informationsangebots zu überwinden (Informationsflut, Information Overload),[278] bietet sich eine kognitionsadäquate Ausgestaltung an.[279]

In der Verhaltens- und Kognitionswissenschaft[280] hat man erkannt, dass Informationen in visueller, noch besser videographischer Aufbereitung die Nut-

---

[275] Vgl. zu dieser Differenzierung des Inhalts vorheriger und nachträglicher Informationspflichten auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16; *Wachter/Mittelstadt/Floridi*, Int. Data Priv. Law 7 (2017), 76, 78, wenngleich diese den unterschiedlichen Inhalt der Informationspflichten nicht mit dem abweichenden Informationsbedarf, sondern damit begründen, dass die konkrete Entscheidung noch gar nicht vorliegt, daher zu dieser also noch keine vertieften Informationen erfolgen können.

[276] Einen einzelfall- und risikobasierten Ansatz der Informationspflichten befürwortet auch *Sesing*, MMR 24 (2021), 288, 291. In diese Richtung auch Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17. Siehe zu diesem risikobasierten Verständnis des Transparenzgrundsatzes auch Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53; *Sesing*, MMR 24 (2021), 288, 290 f., dort gleichwohl für das Bestehen besonderer Informationspflichten, sowie *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 187–192, dieser hinsichtlich des Bestehens eines „Rechts auf Erklärung".

[277] Siehe oben Kapitel 5 B. III. 2. b) ff). Ein solches Recht auf Erläuterung ex ante fordert auch *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, S. 196.

[278] Siehe hierzu bereits Kapitel 4 D. IV. 2. d) aa).

[279] Auch der Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023, Rs. C-634/21, ECLI:EU:C:2023:220, Rn. 56 – *SCHUFA Holding* fordert „geeignete Kommunikationsmittel, die das Verständnis erleichtern".

[280] Eingehend aus der kommunikationswissenschaftlichen Perspektive *Schröder*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019,

zerInnen am besten erreichen, insbesondere bei komplexen Sachverhalten.[281] Anstelle von Textmaterial ist die Darstellung datenschutzspezifischer Informationen in Form von (bewegten) Bildern vorzugswürdig.[282] Dies verlangt eine sorgfältige Bewertung, welche Teile der Informationspflichten überhaupt für die audiovisuelle Aufbereitung geeignet sind,[283] sowie eine Auswahl gut verständlicher – im Übrigen auch einheitlicher[284] – Bilder.[285] Dies ist durchaus anspruchsvoll, kann hier aber nicht weiter vertieft werden.

S. 345. Erkenntnisse des interdiszipilinär angelegten *Design Thinkings* an der Schnittstelle von Marketing-, Design- und Informationstechnik zitiert *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 33 f.

[281] Eingehend *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 18, 41, die von einem „Bildüberlegenheitseffekt" sprechen.; *Schröder*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 345, Rn. 21–24. Vgl. auch *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 41; *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 358 unter Zitierung zahlreicher Studien. Zudem ist nachgewiesen worden, dass diese auf das menschliche Gehirn stärker stimulierend wirken und die Aufmerksamkeit anregen – und also die Motivation schaffen, sich näher mit datenschutzrechtlichem Informationsmaterial zu beschäftigen, vgl. *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 19.

[282] Dies befürwortet auch die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 26, 31–32 sowie das *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 64 f. Ebenso *Strassemeyer*, K&R 16 (2016), 176, 181; *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 19; *Jarovsky*, EDPL 4 (2018), 447, 455; *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 262. Kritisch dagegen *Kamps/Schneider*, K&R 19 (2020), 24, 26.

[283] *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 33.

[284] *Strassemeyer*, K&R 16 (2016), 176, 181; *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 42; *Schröder*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 345, Rn. 13; Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 54; *Jarovsky*, EDPL 4 (2018), 447, 455. Die Notwendigkeit der Vereinheitlichung betont auch die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 31 f.

[285] Zur Notwendigkeit des Erlernens der Bildsprache durch die VerbraucheInnen siehe ausführlich *Schröder*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 345, 17, 24-26. Hierauf weisen auch Ehmann/Selmayr, DS-GVO/*Heckmann/Paschke*, Art. 12 Rn. 54 hin. Im Übrigen wird es eines gewissen Zeitablaufs bedürfen, bis die Verbraucherinnen verschiedene bildliche Darstellungen verinnerlicht hat und mit einem bestimmten Symbol einen spezifischen Informationsgehalt verbindet. Vgl. *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 19.

Vor allem die Verwendung von Warnzeichen erscheint sinnvoll,[286] so etwa in Form von Warnsymbolen für den Einsatz automatisierter Entscheidungen oder autonomer Systeme[287] oder für den Einsatz bestimmter als besonders (autonomie-)gefährdend erachtete Profilverwendungen. Auch die Kennzeichnung nach Risikoabstufungen in der Art der Energieverbrauchskennzeichnung oder der Lebensmittelampel ist vielversprechend.[288] Dem müsste aber eine Risikountersuchung und -bewertung, am besten auf unionaler Ebene für eine möglichst breite und einheitliche Bildsprache, vorausgehen.[289]

Bei bildlichen Darstellungen wird man bei hochkomplexen Datenverarbeitungen schnell an Grenzen kommen,[290] videographische Aufbereitungen, etwa in Gestalt von Erklärvideos oder Tutorials, erscheinen daher vielversprechender.[291] Für die vorherige und nachträgliche Erläuterung der technischen Funk-

---

[286] *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 19; *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 42; *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 358. Dabei können allerdings auch Gewöhnungs- und Abstumpfungseffekte entstehen, die den Warnsignalen ihre Wirkkraft nehmen, vgl. *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 359.

[287] *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336 schlägt die Einführung von flags und icons vor, die auf die Verwendung automatisiert generierter Profile in Entscheidungen hinweisen sollen.

[288] Ein derartiges graphisches Risikobewertungs- und -kennzeichnungssystem schlagen auch *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 360 vor. Die Einführung von „Datenschutzampeln" befürwortet *Martini*, Blackbox Algorithmus, 2019, S. 167. Zu einem Projekt der Carnegie Mellon University in Pittsburgh, in dem ein farbliches Kennzeichnungssystem für verschiedene Risikostufen einer Datenverarbeitung entworfen wurde, siehe eingehend *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 11 f.

[289] Vgl. zu einem entsprechenden Projekt *Efroni/Metzger/Mischau u.a.*, EDPL 5 (2019), 352, 360–364.

[290] Eingehend *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 31; *Schröder*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 345, Rn. 25; Gola, DS-GVO/*Franck*, Art. 12 Rn. 47. Verschiedene, allesamt gescheiterte Initiativen zur Entwicklung einer Bildsprache für die Darstellung des obligatorischen Informationsportfolios der DSGVO stellt *Schröder*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 345, Rn. 16–20 vor.

[291] Befürwortend für intelligente Technologien *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 26. Siehe auch *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 64, 87-88. Aus der Literatur *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider/Werry/Werry u.a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324, Rn. 30 sowie *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 42 f.; *Strassemeyer*, K&R 16 (2016), 176, 182. Zudem sprechen videographische Darstellungen nach wissenschaftlichen Erkenntnissen das kognitive Anreizsystem des Menschen noch besser an als

tionsweise sind diese Darstellungen daher besonders gut geeignet.[292] Auch hier bedarf es jedoch weiterer Untersuchungen, inwieweit sich diese technischen Erläuterungen videographisch darstellen lassen und tatsächlich zu einem technischen Verständnis der betroffenen Person beitragen. Von Rechts wegen können all diese Methoden, d.h. bildliche und videographische Darstellungen, nach Art. 12 Abs. 8 DSGVO nur ergänzend, nicht aber ersetzend zu textbasierten Informationsangeboten ergehen.

c) Technische Informationsmediationsmechanismen

Technische Mechanismen können dazu dienen, das Informationsmaterial besonders verbrauchergerecht zu präsentieren (aa)). Technische Verfahren zur Herstellung menschlicher Verständlichkeit (explainable AI) bieten derzeit noch keine verlässlichen Lösungen (bb)).

aa) Transparenzassistenten und Informationsfiltersysteme

Technische Systeme können zum einen eingesetzt werden, um Datenschutzerläuterungen automatisiert in Bilder oder in eine einfache Sprache zu übertragen, zum anderen die Informationen nach den für die jeweilig betroffenen Personen relevanten Informationen, dann also den Datenschutzpräferenzen der betroffenen Person, zu filtern und verbrauchergerecht sowie geräte- und situationsadaptiv aufzubereiten.[293]

bb) Erklärbare Künstliche Intelligenz (explainable AI, T-Switch)

Die menschenverständliche Aufbereitung von Algorithmen aus Maschinellen Lernverfahren und ihrer Verarbeitungsergebnisse ist ein bedeutendes Forschungsfeld der Künstlichen Intelligenz. Über verschiedene Methoden wird versucht, Auswertungsverfahren und Outputs in ein menschlich verständliches Modell zu übersetzen, entweder parallel zum stattfindenden Analyseprozess

---

rein visuelle Symbole, so auch *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 43.

[292] Vgl. auch *Strassemeyer*, K&R 16 (2016), 176, 182; *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 42 f. Eine Darstellung der technischen Funktionsweise von Big-Data-Analysen in Form von Video-Tutorials befürwortet auch das *Information Comissioner's Office*, Big data, artificial intelligence, machine learning and data protection, 1.3.2017, S. 64.

[293] Eingehend *Ducato/Strowe*, ICC 50 (2019), 649–684 Siehe auch *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 262. Zu verschiedenen Methoden der Transparency Enhancing Technologies siehe etwa *Murmann/Fischer-Hübner*, Usable Transparency Enhancing Tools: A Literature Review, Karlstad University Working Paper, Juli 2017; *Janic/Wijbenga/Veugen*, in: Bella (Hrsg.), 2013 Third Workshop on Socio-Technical Aspects in Security and Trust (STAST), 2013, S. 18.

oder in einem nachträglichen Verfahren.[294] Unterscheiden lassen sich „Whitebox"-Verfahren, bei denen Programmcodes offengelegt und dann menschlich verständlich bzw. laiengerecht aufbereitet werden, und „Blackbox"-Verfahren, bei denen ohne Einblicke in den Programmcode, allein anhand der Analyse von In- und Output menschlich verständliche Entscheidungsfindungsregeln der Systeme entwickelt werden. Es gibt auch zahlreiche Kombinationsformen.[295] Diese Verfahren werden beständig erweitert. Interdisziplinär werden an dieses Forschungsgebiet hohe Erwartungen herangetragen.

Die Leistungskraft dieser Methoden ist allerdings noch unklar: Problematisch ist schon, ob die technischen Erklärungsmodelle, die immer nur Annäherungen darstellen können,[296] die innere algorithmische Struktur tatsächlich hinreichend präzise erfassen können.[297] Die Gefahr der Inkongruenz ist groß, sodass am Ende das Erklärungsmodell, nicht aber der selbstlernende Algorithmus kontrolliert wird.[298] Aus der rechtlichen Perspektive ist unklar, ab welchem

---

[294] Aus den umfassenden Forschungsansätzen siehe etwa die überblicksartige Zusammenstellung aktueller Verfahren bei *Tjoa/Guan*, IEEE transactions on neural networks and learning systems 32 (2021), 4793–4813; *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 574–581, die auf eine menschliche und eine mathematische Interpretabilität abstellen, sowie bei *Adadi/Berrada*, IEEE Access 6 (2018), 52138–52160, die visualisierende, wissensextrahierende, einflussbasierte und beispielsbasierte Erklärungsmethoden unterscheiden. Rechtswissenschaftliche Einordnungen nehmen vor *Käde/Maltzan*, CR 36 (2020), 66, 69 f.; *Martini*, Blackbox Algorithmus, 2019, S. 194 f.

[295] Vgl. *Beck*, Künstliche Intelligenz und Diskriminierung, 2019, S. 99 f.; *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 575.

[296] *Strassemeyer*, in: Taeger (Hrsg.), Die Macht der Daten und der Algorithmen, 2019, S. 31, 40; *Hoeren/Niehoff*, RW 9 (2018), 47, 60. Ebenso *Selbst/Barocas*, Fordham L. Rev. 87 (2018), 1085, 1113.

[297] *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 997. Siehe auch *Hoeren/Niehoff*, RW 9 (2018), 47, 60. Dies ist besonders bei sogenannten „Surrogat-Modellen" der Fall, bei der dem Blackbox-Algorithmus ein verständliches Modell (Whitebox-Modell) zur Seite gestellt wird, das den Blackbox-Algorithmus erläutert (sogenanntes Greybox-Modell). Siehe hierzu *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 575.

[298] Anschaulich *Russell/Norvig*, Artificial Intelligence, [4]2021, S. 997: „[E]xplanations are not decisions: they are stories about decisions. […] [W]e say [a system] is explainable if we can make up a story about what it is doing […]. To explain an uninterpretable black box we need to build, debug, and test a separate explanations system, and make sure it is in sync with the original system. […] [Y]ou require not just an explanation, but also an audit of past decisions". Ebenso *Burrell*, Big Data and Society 3 (2016), 9: „[Finding ways to reveal something of the internal logic of an algorithms] impose[s] a process of human interpretive reasoning on a mathematical process of statistical optimization. […] And yet, explanations that bring forward a human-manageable list of key criteria […] provide an understanding that is at best incomplete and at worst false reassurance".

Präzisionsgrad man die technischen Methoden der Erklärbarkeit auch von Rechts wegen anerkennen kann.[299] Das Recht auf Erklärung bietet hier nur erste Ansätze. Im Ergebnis liegt in diesen technischen Methoden zwar einiges Potential,[300] noch aber sind sie nicht derart ausgereift, dass sie die rechtlichen Anforderungen der DSGVO tatsächlich effektiv umsetzen könnten.[301]

4. De lege ferenda

Legislative Innovationspotentiale liegen vornehmlich in der Erstreckung des algorithmenspezifischen Transparenzprogramms auf die Profilbildung (a)). Um die Problematik der Informationsüberforderung zu adressieren, bietet sich de lege ferenda ein Aufbrechen des relativistischen Transparenzverhältnisses an, um alternative Informationsmärkte zu eröffnen und für die betroffenen Personen nutzbar zu machen (b)).

a) Eigenständige Transparenzbedarfe der Profilbildung

Die besonderen Informationspflichten aus Art. 13 Abs. 2 lit. f), Art. 15 Abs. 1 lit. h) DSGVO sind auch auf die Profilbildung anzuwenden.[302] Dabei sind sowohl Informationen im Vorhinein (aa)), als auch im Nachhinein vorzusehen (bb)). Auch bedarf es Lösungsmethoden für die fehlende Vorhersehbarkeit und Nachvollziehbarkeit bei Profilbildungen durch autonome Systeme (cc)).

aa) Informationen im Vorhinein: „involvierte Logik" und Prognose von Profilinhalten

Um betroffenen Personen die Aktivierung von Resilienzmechanismen zu ermöglichen, ist besonders ein Hinweis auf das Stattfinden eines Profilings notwendig, ebenso die Profilbasiertheit einer Maßnahme.[303] Wird etwa für die per-

---

[299] Hier ist gerade problematisch, dass „menschliche Verständlichkeit" keine programmierbare Eigenschaft ist, da sie nicht bemessbar ist. Siehe auch *Bauckhage/Fürnkranz/Paaß*, in: Görz/Schmid/Braun (Hrsg.), Handbuch der Künstlichen Intelligenz, [6]2021, S. 571, 581: „Wenn Interpretierbarkeit also nicht allein mit geringer Komplexität einhergeht, wie kann sie dann gemessen werden?".

[300] So auch *Strassemeyer*, K&R 16 (2016), 176, 180 f.; *Hoeren/Niehoff*, RW 9 (2018), 47, 59–61. Die Förderung von Techniken der explainable Artificial Intelligence fordert auch die *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 170, 187.

[301] Zurückhaltend auch *Martini*, Blackbox Algorithmus, 2019, S. 194 f.; *Wischmeyer*, AöR 143 (2018), 1, 61. Auf den Punkt bringen es *Kumkar/Roth-Isigkeit*, JZ 75 (2020), 277, 285: Technisch mögliche Erklärbarkeit kann nicht die normativ definierte Erklärbarkeit abbilden, andernfalls schlösse man vom Faktischen auf das Normative.

[302] Siehe oben Kapitel 5 B. III. 1. a).

[303] Dies ist bislang allein in Erwägungsgrund 60 S 3 vorgesehen. Eine eigenständige Normierung fordern auch *Lorentz*, Profiling, 2019, S. 164, 236–237, 341; *Lewinski/Pohl*,

sonalisierte Werbung ein Werbeprofil erstellt, muss hierauf bei Datenerhebung hingewiesen werden. Dies folgt bereits aus dem Zweckbestimmungs- und Rechtmäßigkeitsgrundsatz. Wird eine Werbeanzeige geschaltet, muss zusätzlich darauf hingewiesen werden, dass die Auswahl dieser Werbeanzeige personalisiert erfolgte.

Auch die „involvierte Logik" des Profilbildungsverfahrens ist darzulegen.[304] Die Begründung ist hier aber eine andere als bei der automatisierten Entscheidung: Während es bei dieser die undurchdringliche Entscheidungsarchitektur ist, die Autonomiegefährdungen auslöst, sind es bei der Profilbildung die intransparenten Erkenntnisse jenseits des Rohdatums, in denen Autonomiegefährdungen ihre Ursache haben. Um den in der Profilbildung angelegten Autonomiegefährdungen entgegenzutreten, müssen diese Erkenntnisse vor allem vorhersehbar sein. Vor allem aber kann nur so eine Zulassungsprüfung nach Art. 6 Abs. 1 DSGVO erfolgen.[305] Hierfür ist es dann notwendig, die grundlegende Funktionsweise der Profilbildung darzulegen und also Informationen zum Modell bereitzustellen. Nur so kann die betroffene Person einschätzen, mit welchen Profilinhalten sie durch Freigabe ihres Rohdatums rechnen muss. Ein Aufdecken des Modells ist nicht geboten, wohl aber die Offenlegung der wesentlichen Vergleichsgruppen und Gewichtungen.[306] Der Detailgrad ist wiederum risikobasiert zu bestimmen: Je umfassender, detailreicher und sensibler ein Profil sich darstellt, je fehler- und diskriminierungsanfälliger es ist, je autonomiegefährdender und diskriminierender eine spätere Anwendung, desto mehr und präziser müssen Vergleichsgruppen, Zuordnungskriterien und Gewichtungen benannt werden.[307] Auch hier ist das Maß der Intransparenz von Bedeutung: Über Vergleichsgruppen im Modell, mit denen die betroffene Per-

---

ZD 9 (2018), 17, 22. Schon im aktuellen Recht, dann aber nur, soweit diese Profile und Profilbildungsmaßnahmen in automatisierte Entscheidungen Eingang finden, erkennen derartige Hinweispflichten an Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Schwartmann/Schneider*, Art. 12 Rn. 75; Kuner/Bygrave/Docksey, GDPR/*Zanfir-Fortuna*, Art. 13 Rn. 429. Noch weiter Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16, der dies auch für das Profiling ohne eine automatisierte Entscheidung anerkennt. Zumindest im Rahmen der Einwilligung oder der Rechtfertigung über berechtigte Interessen fordert *Lorentz*, Profiling, 2019, S. 181, 341 einen derartigen Hinweis.

[304] So auch *Lorentz*, Profiling, 2019, S. 185. Ebenso *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 27, 100. In diese Richtung auch *Dimitrova*, EDPL 6 (2020), 211, 229. So auch, zumindest, wenn das Profil im Anschluss für eine automatisierte Enscheidung genutzt wird, *Kaminski*, BTLJ 34 (2019), 189, 214.

[305] Hierauf stützt *Lorentz*, Profiling, 2019, S. 185 die Informationspflichten zur Profilbildung ex ante.

[306] Ebenso *Martini*, Blackbox Algorithmus, 2019, S. 190. Vgl. auch, wenngleich im Rahmen der Einwilligung, *Lorentz*, Profiling, 2019, S. 241.

[307] Vgl., dort im Rahmen des Kreditscoriongs, *Sesing*, MMR 24 (2021), 288, 291; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 17.

son nicht rechnet, ist zu informieren, aber nur dann, wenn sich die Profilbildung als insgesamt risikoreich darstellt. Dass etwa bei einer Werbeprofilerstellung auf ein Suchtverhalten einer Person ermittelt wird, stellt sich als risikoreiche, zugleich überraschende Profilbildungsmaßnahme dar; hierüber muss informiert werden.[308]

Die Aufklärung über die „involvierte Logik" allein genügt dann nicht, wenn die betroffene Person trotz Kenntnis von den grundlegenden Inhalten des Modells nicht präzise vorhersagen kann, welche Profilinhalte gebildet werden können. Damit müssen Profilinhalte, mit denen die betroffene Person nicht rechnet, vorab aufgedeckt werden. In Abwägung mit unternehmerischen Interessen gilt dies allerdings nur, wenn hieran ein besonderes Interesse besteht, d.h. die Profilbildung insgesamt oder einzelne Ableitungen ein hohes Risiko aufweisen.[309] Wird etwa bei einem Kredit-Scoring der Gesundheitszustand einer Person ermittelt – es handelt sich um einen sensiblen Profilinhalt sowie eine risikoreiche Anwendung und eine überraschende Ableitung –, so ist hierüber zu informieren.[310]

bb) Informationen im Nachhinein: Offenlegung der Profilinhalte

Nachträgliche Informationspflichten erscheinen auch bei der Profilbildung wichtig, lassen sich derzeit aber allein aus der funktionalen Dimension der Transparenz ableiten. Denn Betroffenenrechte im Sinne des Art. 22 Abs. 3 DSGVO gibt es für die Profilbildung noch nicht.[311] Nachträgliche Informationspflichten sind aber auch für die funktionale Dimension der Transparenz von

---

[308] Vgl. zu einer ähnlichen Einschätzung hinsichtlich des Bestehens einer Schwangerschaft, *Lorentz*, Profiling, 2019, S. 220. Siehe allgemein zum besonderen Risikopotential der Ermittlung von Suchtverhalten in Vertragsbeziehungen *Wagner/Eidenmüller*, ZfPW 5 (2019), 220, 231 f.

[309] Vgl. zu ähnlichen Erwägungen, wenngleich im Rahmen der Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO hinsichtlich der Profilbildung, *Lorentz*, Profiling, 2019, S. 219–221; *Artikel 29 Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, 09.04.2014, S. 50. Ihnen zufolge muss eine Rechtfertigung nach Art. 6 Abs. 1 lit. f) DSGVO ausscheiden, wenn eine Inferenz sich als überraschend darstellt und die Profilbildung insgesamt nachteilig auf die Rechte und Interessen der betroffenen Person auswirkt.

[310] Während oben – siehe unter Kapitel 5 B. III. 3. a) bb) (3) – bei der automatisierten Entscheidung darzulegen ist, dass der Gesundheitszustand ein Entscheidungsparameter der automatisierten Entscheidung ist, geht es hier darum, dass der Gesundheitszustand ermittelt wird.

[311] Wenn allerdings das Profil in die automatisierte Entscheidung Eingang findet, kann auch ein fehlerhaftes Profil zu fehlerhaften Entscheidungen führen. Das Betroffenenrecht nach Art. 22 Abs. 3 DSGVO ließe sich insoweit auch auf das Profilbildungsverfahren erstrecken. Die Vorschrift bezieht sich derzeit aber nur auf die automatisierte Entscheidung, soll also die Kontrolle und Anfechtung aufgrund der Verwendung eines fehlerhaften Profilinhalts ermöglichen, nicht aber die Kontrolle und Anfechtung der fehlerhaften Profilbildung.

Bedeutung: Sie können die betroffene Person befähigen, Hemmeffekte abzubauen und verhaltensökonomischen Einwirkungen entgegenzuwirken. Nachträgliche Informationen über grundlegende Aspekte, dann des konkreten Profilbildungsverfahrens, d.h. des tatsächlich verwendeten Modells und der dortigen Vergleichsgruppen, Zuordnungskriterien und Gewichtungen können daher hilfreich sein.[312]

Wichtig ist aber vor allem ein nachträglicher Einblick in die einzelnen Profilinhalte. Der Unionsgesetzgeber sollte daher ein Recht betroffener Personen auf umfassenden Einblick in ihr Profil normieren.[313] Nur so lassen sich im Ergebnis Intransparenz und Unkontrollierbarkeit von Erkenntnissen über die betroffene Person und die Informationsasymmetrie zwischen Verantwortlichem und betroffenen Personen überwinden, die Ursache sind für Autonomiegefährdungen und Diskriminierungen. Ohne derartige Einblicke sind die betroffenen Personen gegenüber diesen Autonomiegefährdungen und Diskriminierungen überdies schutzlos gestellt. Da die Gefährdung in der Intransparenz der Erkenntnisse, nicht in deren Inhalten liegt, ist es nicht überzeugend, nur die wesentlichen oder nur risikoreichen Profilinhalte mitzuteilen. Vielmehr muss der Verantwortliche Auskunft über das gesamte Profil geben.[314] Um dabei einen angemessenen Ausgleich mit den grundrechtlich geschützten Interessen des Verantwortlichen herzustellen, bedarf es hierfür vor allem verfahrensmäßige Absicherungen. Zudem sollten allein die Profilinhalte, nicht aber Details zum Profilbildungsverfahren offengelegt werden.[315]

cc) Lösungen für fehlende Nachvollziehbarkeit und Vorhersehbarkeit

Bei der Profilbildung ist die fehlende Nachvollziehbarkeit autonomer Systeme von besonderer Brisanz. Ein „Recht auf Erklärung" erscheint bei der Profilbil-

---

[312] Zu diesem Ansatz auch Kühling/Buchner, DS-GVO, BDSG/*Bäcker*, Art. 13 Rn. 53. Sehr allgemein *Koops*, in: Hildebrandt/Gutwirth (Hrsg.), Profiling the European Citizen, 2008, S. 326, 336. Vgl. auch *Lorentz*, Profiling, 2019, S. 341, wenngleich diese derartige nachträgliche Informationspflichten zum Profilbildungsverfahren allein im Falle profilgestützter automatisierter Entscheidungen befürwortet.

[313] Ebenso *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 367 f. sowie *Lorentz*, Profiling, 2019, S. 249, die diese Offenlegungspflicht schon in das geltende Recht, dann in Art. 15 Abs. 1 lit. h) DSGVO, einliest. In diese Richtung auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 18: „[Z]udem muss [der Verantwortliche] Informationen zum Profil und Details zu den Segmenten, in die die betroffene Person eingeteilt wurde, mitteilen". So auch *Artikel 29 Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, 02.04.2013, S. 47: „[T]o ensure transparency, data subjects/ consumers should be given access to their ‚profiles'".

[314] Inhaltliche Einschränkungen sehen auch *Lorentz*, Profiling, 2019, S. 249; *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 367 f. nicht vor.

[315] Ähnlich *Hermstrüwer*, Informationelle Selbstgefährdung, 2015, S. 368.

dung wenig ergiebig, denn Kontroll- und Anfechtungsrechte im Sinne des Art. 22 Abs. 3 DSGVO gibt es (derzeit) noch nicht. Allerdings lässt sich aus der funktionalen sowie der funktional-instrumentellen Dimension der Transparenz ein vergleichbares Recht auf verständliche Ausgestaltung[316] herleiten: Nicht nachvollziehbare Profilbildungen führen zu intransparenten Informationsemergenzen und können Autonomiegefährdungen begründen, nicht nachvollziehbare und damit nicht vorhersehbare Profilbildungen sind über den Rechtmäßigkeitsgrundsatz, vor allem die Einwilligung, nicht mehr steuerbar. Überdies nützt die nachträgliche Offenlegung von Profilinhalten der betroffenen Person wenig, wenn sie diese nicht verstehen kann, da es sich um Ausgaben künstlicher neuronaler Netze handelt, oder sich diese für die betroffene Person als willkürlich darstellen. Zusätzlich müssen demnach prognostizierte bzw. nachträglich offengelegte Profilinhalte in menschliche Verständniszusammenhänge gesetzt werden. Dies ist aber nicht stets notwendig, sondern nur für solche Profilinhalte, bei denen aufgrund ihres Risikos oder des Risikos der Profilbildung insgesamt ein besonderer Verständlichkeitsbedarf besteht. Maßgeblich ist damit die Sensibilität der einzelnen Ableitung, aber auch die des Profils insgesamt sowie der Profilverwendung.

b) Alternative Informationsmärkte: Einbezug von ExpertInnen und Adressierung der Gesamtöffentlichkeit

In der Verbraucherökonomie ist seit Langem bekannt, dass ein Informationsgefälle zwischen betroffenen Personen und Anbietern einer Ware oder Dienstleistung nachteilige Effekte für VerbraucherInnen sowie den Markt insgesamt freisetzen kann.[317] Zur Überwindung dieses Informationsgefälles hat man vor

---

[316] Dies unterscheidet sich vom oben beschriebenen Recht auf angemessene Ableitungen: Während es dort um eine inhaltliche Anforderung an die Datenverarbeitung geht, nämlich, dass nur Ableitungen verwendet werden dürfen, die inhaltlich angemessen erscheinen, ist das Recht auf verständliche Aufbereitung eine prozedurale Anforderung. Es zielt auf die ergänzende, nachträgliche Erklärung der Einzelinferenz ab.

[317] Zurück geht dies auf institutionsökonomische Gedanken von *Akerlof*, The Quarterly Journal of Economics 84 (1970), 488–500. Am Anwendungsbeispiel des Gebrauchtwagenhandels herausgearbeitet, dass die ungleiche Verteilung von Wissen über gute (plums) und schlechte (lemons) Gebrauchtwagen zwischen VerkäuferInnen und VerbraucherInnen zu einem Marktversagen führen kann. Da VerbraucherInnen regelmäßig nicht wissen, ob es sich bei einem KfZ um einen lemon handelt, orientieren sie sich an der Durchschnittsqualität der KfZ und dem hierfür üblichen Preis. Die notwendigen Informationen zu besorgen, erweist sich für VerbraucherInnen als kostspielig oder gar unmöglich. Sie sind dann nicht bereit, den angemessenen Preis für einen guten Gebrauchtwagen zu zahlen, sodass für VerkäuferInnen kein Interesse am Verkauf guter Gebrauchtwagen mehr besteht. Der Markt für gute Gebrauchtwagen bricht daher zusammen. Hätten VerbraucherInnen dagegen Zugang zu Fachwissen, käme es nicht zu einem derartigen Marktversagen. Die Überwindung der Informationsasymmetrie liegt daher im allgemeinen wirtschaftlichen Interesse. Übertragen auf auto-

allem den Zugang von VerbraucherInnen zu alternativen Informationsmärkten erkannt, wie sie ExpertInnen sowie die Gesamtöffentlichkeit eröffnen.[318] Dieser Ansatz lässt sich auf den Transparenzgrundsatz der DSGVO übertragen. Der Einbezug von ExpertInnen erscheint aufgrund der technischen Komplexität autonomer Systeme von besonderer Wichtigkeit.[319] Diese sollten neben betroffenen Personen Einblicke in die Techniken erhalten und ihre Erkenntnisse dann mit den betroffenen Personen teilen.[320] Dies böte zugleich die Möglichkeit einer besseren Erforschung autonomer Systeme in ihrer sozioökonomischen Einbettung.[321] Die Fachöffentlichkeit könnte dann entweder als individuelle Beratungsfunktion fungieren[322] oder in Form von an die allgemeine Öffentlichkeit gerichteten Berichten, zB durch Veröffentlichung von Audit-Ergebnissen, mit den betroffenen Personen in Kontakt treten.[323] Dabei bedarf es

---

nome Systeme könnte das fehlende Wissen um deren Funktionsfähigkeit zu einem Vertrauensverlust und zu einer Verbreitung qualitativ minderwertiger autonomer Systeme führen. Siehe zu diesen Gedanken auch *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 233 f.

[318] Dies gerade deshalb, da es sich für VerbraucherInnen als zu ressourcenaufwändig oder aufgrund fehlender Fachkenntnis als unmöglich erweisen kann, den notwendigen Wissensstand zu erreichen. Vgl. *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 234.

[319] So fordert etwa auch *Martini*, Blackbox Algorithmus, 2019, S. 350 f. Kontrollen – hier dann von Algorithmen – durch private ExpertInnen. Zur Bedeutung von privaten ExpertInnen für die Steuerung von intelligenten Systemen siehe auch eingehend *Wischmeyer*, AöR 143 (2018), 1, 63. Die Regulierungsarchitektur der DSGVO sieht dies bereits vor, da private ExpertInnen Normierungen anstoßen können, etwa über die Entwicklung von Verhaltenskodices nach Art. 40, 41 DSGVO oder Zertifizierungen nach selbst entwickelten Standards nach Art. 42, 43 DSGVO.

[320] Die Algorithmenkontrolle durch private ExpertInnen, deren Ergebnisse dann mit der Öffentlichkeit geteilt werden, erscheint auch der *Norwegian Data Protection Authority*, Big Data, September 2013, S. 52 als gute Lösung in einem Big-Data-Umfeld. Der Unionsgesetzgeber sieht bereits aktuell eine Beteiligung privater ExpertInnen an verschiedenen Stellen vor und hat also deren Bedeutung für einen effektiven Datenschutz erkannt. Als Teil „interessierter Kreise" können sie nach Art. 70 Abs. 4 DSGVO vom Datenschutzausschuss angehört werden, als Vertreter der Verantwortlichen oder der Auftragsverarbeiter können sie Verhaltensregeln entwerfen, Art. 40 Abs. 2 und 5 DSGVO, und sind in jedem Fall bei der Ausarbeitung zu beteiligen. Als zertifizierte Stellen können sie Zertifizierungen erteilen und materielle Zertifizierungskriterien entwickeln, Art. 42 Abs. 5 S. 1 DSGVO, schließlich nach Art. 80 DSGVO im Namen der betroffenen Person Beschwerde einreichen.

[321] So auch, wenngleich zur Big-Data-Analyse, *dass.*, Big Data, September 2013, S. 54. Ebenso *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 28–29, 32.

[322] Dies wird nur vereinzelt diskutiert. So sieht etwa *Wischmeyer*, AöR 143 (2018), 1, 63 hinsichtlich der Kontrolle intelligenter Systeme durch NutzerInnen die Möglichkeit der Beauftragung von Sachverständigen vor.

[323] So etwa *Martini*, Blackbox Algorithmus, 2019, S. 167. In diese Richtung auch, dann für intelligente Systeme, *Wischmeyer*, AöR 143 (2018), 1, 62. Öffentliche Audits der Algorithmen fordert auch, dann allgemein im Rahmen der Big-Data-Analyse, *Norwegian Data Protection Authority*, Big Data, September 2013, S. 52. Vgl. zu Audits von intelligenten

Vorkehrungen, vor allem verfahrensmäßiger Natur, zur Absicherung der grundrechtlich geschützten Interessen der Verantwortlichen.[324] Auch die Gesamtöffentlichkeit bildet einen alternativen Informationsmarkt ab; vom technischen Verständnis Einzelner kann dann die Allgemeinheit profitieren.[325] Zugleich können über die Gesamtöffentlichkeit Disziplinierungseffekte öffentlicher Beblickung aktiviert werden.[326] Eine Adressierung der Gesamtöffentlichkeit kann durch allgemeine Berichte im Anschluss die Prüfung von autonomen Systemen erfolgen. Diese können von Seiten der Aufsichtsbehörden oder Verbrauchereinrichtungen sowie privaten ExpertInnen bereitgestellt werden,[327] aber auch von Seiten der Verantwortlichen.[328]

5. *Ergebnis*

Innovationspotentiale des Transparenzgrundsatzes in Anbetracht autonomer Systeme betreffen allein die Erweiterung besonderer Informationspflichten, d.h. von Einblicksrechten in die technischen Aspekte der Profilbildung und automatisierter Entscheidung. Während beim Zweckfestlegungs- und Rechtmäßigkeitsgrundsatz[329] die allgemeinen Regeln, also solche, die sich auf Daten-

---

Systemen durch private ExpertInnen auch *Wischmeyer*, AöR 143 (2018), 1, 62 f. Auch im DSA ist ein entsprechendes Einblicksrecht für Forschungseinrichtungen vorgesehen, siehe Art. 40 Abs. 4 DSA; nicht aber, dass diese als Gutachter für betroffene Personen fungieren sollen.

[324] So auch *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 35. Entsprechende Vorkehrungen sind auch im DSA getroffen. So dürfen etwa nur bestimmte, nämlich nur zertifizierte Forschungseinrichtungen, Anfragen stellen, diese müssen begründet sein, siehe Art. 40 Abs. 4 und Abs. 8 DSA.

[325] Ähnliche Gedanken, wenngleich im Hinblick auf die Durchführung von Algorithmenkontrollen, bei *Martini*, Blackbox Algorithmus, 2019, S. 251–253.

[326] Die disziplinierenden Effekte im Hinblick auf die ordnungsgemäße Durchführung der Datenschutzfolgenabschätzung nach Art. 35 DSGVO durch eine Veröffentlichung des Abschlussberichts betont auch *ders.*, Blackbox Algorithmus, 2019, S. 210 f. Vgl. ausführlich zur Ideengeschichte von Transparenz als Machtkontrollinstrument, wenngleich im Hinblick auf die Transparenz algorithmischer Systeme, *Ananny/Crawford*, New Media & Society 20 (2018), 973, 974–977.

[327] Berichtspflichten von Audits interdisziplinär besetzter Fachgremien fordert auch *Zuiderveen Borgesius*, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, 2018, S. 29.

[328] Eine Selbstprüfung ist in Art. 35 DSGVO bereits vorgesehen. Diese gilt dann überzeugenderweise nur für risikohafte Datenverarbeitungen. Die Verantwortlichen müssten dann, was bislang nicht vorgesehen ist, die abschließenden Berichte hierzu veröffentlichen. Eine Veröffentlichung der Ergebnisse einer Datenschutzfolgenabschätzung fordert auch die *Artikel 29 Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, S. 27. Ebenso *Martini*, Blackbox Algorithmus, 2019, S. 210 f.

[329] *Tutt*, Admin. L. Rev. 69 (2016).

verarbeitungen beziehen, ausreichend sind, liegt das Regulierungspotential der DSGVO hinsichtlich der Transparenz allein im Überschneidungsbereich datenverarbeitungsspezifischer und algorithmischer Regulierung.

Eine Erweiterung derartiger Informationspflichten ist für die Profilbildung geboten. Die Profilbildung sowie die Profilbasiertheit eines Dienstes ist kenntlich zu machen, überdies ist im Vor- und Nachhinein das Profilbildungsverfahren in seinen grundlegenden Zügen zu beschreiben. Es ist ein nachträgliches umfassendes Einblicksrecht in Profilinhalte einzuführen. Bei der automatisierten Entscheidung wie auch beim Profiling ist keine Algorithmentransparenz, sondern allein eine Darstellung der grundlegenden Funktionsweise gefordert. Während dies im Vorhinein die Systemfunktionalität im Allgemeinen beinhaltet, beziehen sich nachträgliche Informationspflichten auf den konkret gewählten Algorithmus, d.h. das konkrete Modell oder den konkreten Lösungsalgorithmus und deren Berechnungsschritte und Ergebnisse.

Innovativer Lösungen bedarf es vor allem im Hinblick auf den Umgang mit (für den Laien) nicht nachvollziehbaren Verarbeitungen durch autonome Systeme und Überlastungen durch quantitativ wie qualitativ überfordernde Informationsangebote. Für die fehlende Nachvollziehbarkeit bietet die Transparenz zumindest begrenzt eine Lösungsmöglichkeit. Technische Verfahren zur Herstellung menschlicher Verständlichkeit (explainable AI) erlauben derzeit noch keine verlässlichen Lösungen. Dagegen bietet das Recht auf Erklärung einen sinnvollen Lösungsansatz. Es verlangt nicht umfassende Verständlichkeit, sondern ein rechtsnormatives Verständlichkeitsniveau. Jenes Niveau bestimmt sich anhand der Transparenzbedarfe für die Wahrnehmung der Betroffenenrechte in Art. 22 Abs. 3 DSGVO, muss also die betroffene Person sowie Dritte zur Überprüfung der Entscheidung anhand individueller Angemessenheitskriterien, vor allem die inhaltliche Richtigkeit und Diskriminierungsfreiheit der Systeme, befähigen. Dies entspricht einer Begründung oder Rechtfertigung: Darzulegen sind die wesentlichen Kriterien und deren Bedeutung für die Entscheidung. Die Wesentlichkeit bestimmt sich dabei nach dem Risiko der Anwendung und der Unverständlichkeit der algorithmischen Entscheidungsarchitektur. Für Erläuterungen im Vorhinein ist dieser Ansatz übertragbar, bezieht sich dort dann auf die generelle Systemfunktionsweise. Am Ende verbleiben aber weite Bereiche, die menschlich unverständlich bleiben. Hier kommt man mit transparenzbezogenen Instrumenten nicht weiter. Derartige Regulierungsmethoden liegen dann aber jenseits des Regulierungszugriffs der DSGVO.

Um der Überlastung der betroffenen Person durch ein Informationsüberangebot entgegenzuwirken, bietet bereits das Recht auf Erklärung Lösungen für die laienbezogene Intransparenz. Darüber hinaus können visuelle und videographische Darstellungsformen, vor allem in Gestalt von Warn- und Risikokennzeichnungen kognitionsfreundlich aufbereitet werden. Auch technische Assistenzsysteme erleichtern betroffenen Personen die Informationsaufnahme. Des Weiteren ist das Transparenzrechtsverhältnis zu öffnen: Auch ExpertInnen

sollten Einblicke in die autonomen Systeme erhalten, zudem die Gesamtöffentlichkeit adressiert werden.

C. Ausblick: Regulierungsbedarfe und -optionen jenseits der DSGVO: Regulierung Maschineller Lernverfahren

Die Untersuchung verweist auf einen regulativen blinden Fleck der DSGVO, nämlich das Modell bzw. den Lösungsalgorithmus und das zugrundeliegende Maschinelle Lernverfahren. Nach den Erkenntnissen der Arbeit ist dies zunächst unproblematisch, da von diesen Verfahren (noch) keine Gefährdungen für betroffene Personen ausgehen. Sofern dabei allerdings nicht nachvollziehbare Algorithmen erstellt werden, blockieren diese die Regulierungsmechanismen auf Stufe der Profilbildung und -verwendung, bei denen es zu konkreten Gefährdungen für betroffene Personen kommt. Der Rechtmäßigkeitsgrundsatz funktioniert dann nicht mehr, vor allem aber können auch außer(daten)schutzrechtliche Resilienz- und Widerstandsmechanismen betroffener Personen gegen Autonomiegefährdungen nicht wirken. Nach den Prämissen des Datenschutzrechts entsteht eine intransparente Verarbeitungsarchitektur, die Einschüchterungs- und Abschreckungseffekte auslöst und per se autonomiegefährdend ist. Lässt sich eine hinreichende Vorhersehbarkeit bzw. Nachvollziehbarkeit nach den Vorschlägen dieser Arbeit nicht herstellen, bedarf es transparenzunabhängiger Regulierungsmechanismen. Damit rücken Modell und Lösungsalgorithmus und deren Erstellungsmethode und also das Maschinelle Lernverfahren in den Fokus. Wenn dort hinreichend abgesichert werden kann, dass es später erst gar nicht zu Autonomiegefährdungen und Diskriminierungen kommt, entfallen die späteren Regulierungsbedarfe, dann auch datenschutzrechtliche, hinsichtlich der Profilbildung und -verwendung. Die Intransparenz kann dann hingenommen werden. Es geht damit um Fragen der inhaltlichen Angemessenheit der selbstlernenden Algorithmen und ihrer Verwendung. Die DSGVO verweist so, zumindest in ihrer aktuellen Konzeption als Daten-, nicht als Algorithmenrecht, auf Regulierungsbedarfe, die sie selbst nicht beantworten kann. Der technikneutrale Ansatz kommt hier also an Grenzen. Einmal mehr zeigt dies auf, dass autonome Systeme sinnvoll nur durch verschiedene, klug aufeinander abgestimmte Rechtsinstrumente reguliert werden können.

Wenngleich diese nicht vom Untersuchungsauftrag dieser Arbeit gedeckt sind, soll gleichwohl knapp skizziert werden, wie eine Regulierung von Modell und Lösungsalgorithmus und deren Maschinellen Lernverfahren aussehen könnten. Eine solche Regulierung ist mit Blick auf die Steuerungseffektivität sinnvoll, da andernfalls bedeutende Regulierungslücken blieben. Es bedarf

aber einer Abwägung mit unternehmerischen Interessen und mit dem Interesse der Innovationsförderung. Nur bei besonders risikoreichen autonomen Systemen erscheint daher eine derartige Regulierung geboten, also solchen mit einem hohen Autonomiegefährdungs- und Diskriminierungspotential, und es erscheint sinnvoll, die Regelung nach dem Risikograd zu differenzieren. Transparenzferne Regulierungsmechanismen können nur am Input oder Output ansetzen und bestimmte inhaltliche Angemessenheitskriterien formulieren (I.). Mit dem KI-Gesetz-E hat der Unionsgesetzgeber bereits einen Vorschlag für eine derartige Regulierung erarbeitet, der inhaltlich aber viele Fragen offenlässt (II.)

I. Vorgabe inhaltlicher Angemessenheitskriterien: Qualitätsvorgaben, Risikomanagement und Verbote

Wenn das Maschinelle Lernverfahren, die darin aufgefundene Regelstruktur und die konkreten Entscheidungen selbstlernender Algorithmen nicht menschlich überprüft werden können, bleibt zur Verhinderung unerwünschte Ergebnisse, nur die inhaltliche Angemessenheit des Erstellungsverfahrens oder der Ausgabe eines autonomen Systems abzusichern. Dabei muss zunächst präzise definiert werden, welche Ergebnisse überhaupt unerwünscht sind. In der Perspektive dieser Arbeit geht es dann also um die Unterbindung von Diskriminierungen und Autonomiegefährdungen. Denkbar sind Vorgaben zum Trainingsverfahren (1.), am Ergebnis ansetzende Audit- und Risikomanagementsysteme (2.) und Verbote.

1. Qualitätsvorgaben für das Trainingsverfahren

Vorgeschlagen werden vor allem qualitative Anforderungen an die verwendeten Trainingsdaten[330] sowie der Methoden und Verfahren des Maschinellen Lernverfahrens[331] und der hieraus gebildeten Algorith-

[330] Zu einem Qualität und Diskriminierungsfreiheit sichernden Rechtsrahmen für Trainingsdaten siehe eingehend *Hacker*, ZGE 12 (2020), 239–271; *Hacker*, NJW 73 (2020), 2124, 2144 f. Vgl. zu Qualitätsanforderungen hinsichtlich der Trainingsdaten auch *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 191; *Wischmeyer*, AöR 143 (2018), 1, 25.

[331] Siehe allgemein zur Notwendigkeit regulatorischer Absicherung der qualitativen Anforderungen Maschineller Lernverfahren, insbesondere hinsichtlich der Fehlerfreiheit, Diskriminierungsfreiheit und Sicherheit des Maschinellen Lernverfahrens *Tutt*, Admin. L. Rev. 69 (2016), 108; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 190 f. Sehr allgemein auch *Wischmeyer*, AöR 143 (2018), 1, 25. Vgl. spezifisch im Hinblick auf Sicherstellung der Diskriminierungsfreiheit von selbstlernenden Algorithmen *Martini*, Blackbox Algorithmus, 2019, S. 243–245; *Wischmeyer*, AöR 143 (2018), 1, 28 f. Zu Erweiterungen der Produkthaftungsrichtlinie 85/374/EWG auf Software siehe *Hacker*, NJW 73 (2020), 2124, 2145.

men.[332] Nicht sämtliche Fehlentwicklungen lassen sich aber in materielle Vorgaben übersetzen. Inhaltlichen Vorgaben lassen sich für die Fehler- sowie Diskriminierungsfreiheit machen,[333] nicht aber für sensible, tiefgehende oder umfassende Profilbildungen. Die Einhaltung dieser substantiellen Vorgaben müsste dann durch Hersteller, Entwickler oder Verwender selbst, d.h. durch Selbstaudits, sichergestellt werden.[334] Auch private ExpertInnen[335] oder staatliche Institutionen, etwa Aufsichtsbehörden, sind sinnvollerweise in dieses Kontrollsystem einzubeziehen.[336]

2. *Audit- und Risikomanagementsysteme*

Eine Methode, die weder menschliche Verständlichkeit fordert noch die Aufstellung konkreter substantieller Vorgaben an Trainingsverfahren und Algorithmen, ist die Einrichtung von Audit- und Risikomanagementsystemen: Entwickler oder Verwender werden verpflichtet, die Ausgaben und Auswirkungen ihrer Systeme auf bestimmte unerwünschte Fehlentwicklungen hin zu prüfen und effektive Gegenmaßnahmen zu ergreifen.[337] Auch Dritte, etwa Interessens-

---

[332] Vgl. *Tutt*, Admin. L. Rev. 69 (2016), 108.

[333] Siehe zu Schwierigkeiten und Grenzen einer präzisen rechtlichen Beschreibung von unerwünschten Diskriminierungen, mit denen auch mittelbare Diskriminierungen effektiv unterbunden werden können, *Martini*, Blackbox Algorithmus, 2019, S. 239–243.

[334] Zu Selbstkontrollverfahren hinsichtlich Maschineller Lernverfahren und dabei gebildeter Algorithmen vgl. etwa *Burrell*, Big Data and Society 3 (2016), 9. Siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 259, 352; *Wischmeyer*, AöR 143 (2018), 1, 61 f.

[335] Dies im Rahmen regulierter Selbstregulierung, also etwa in Form von Zertifizierungen von autonomen Systemen, siehe hierzu *Martini*, Blackbox Algorithmus, 2019, S. 323 f. Angedeutet bei *Wischmeyer*, AöR 143 (2018), 1, 65. Zur Möglichkeit des Einbezugs technischer Verfahren, d.h. von Kontrollalgorithmen siehe *Martini*, Blackbox Algorithmus, 2019, S. 251.

[336] Zur Kontrolle der Einhaltung der substantiellen Vorgaben durch staatliche Einrichtungen mit entsprechender technischer Expertise siehe *Martini*, Blackbox Algorithmus, 2019, S. 207, 253–254, 268–273; *Wischmeyer*, AöR 143 (2018), 1, 62 f. Zur Einführung eines staatlichen Zulassungssystems von Algorithmen des Maschinellen Lernens siehe *Tutt*, Admin. L. Rev. 69 (2016), 111, 122; *Hacker*, NJW 73 (2020), 2124, 2145.

[337] Explizit *Casey/Farhangi/Vogl*, BTLJ 34 (2019), 143, 183 f.: „In contrast to a remedial ‚right to explanation' invoked on an individual basis by downstream data subjects, properly implemented auditing and DPbD can provide the evidence necessary to inform and vet the design and deployment of more fair, accountable, and transparent algorithmic systems". Siehe etwa zu möglichen Ausgestaltungsformen von Auditsystemen unter Einbezug verschiedener Fehlentwicklungen, Testmethoden und Anwendungsbereiche *Brown/Davidovic/Hasan*, Big Data and Society 8 (2021), 1; *Bandy*, Problematic Machine Behavior: A Systematic Literature Review of Algorithm Audits, 03.02.2021. Spezifisch zu Risikomanagementsystemen *Martini*, Blackbox Algorithmus, 2019, S. 265–268; *Datenethikkommission*, Gutachten der Datenethikkommission der Bundesregierung, Oktober 2019, S. 188. Siehe auch *Burrell*, Big Data and Society 3 (2016), 9 hinsichtlich diskriminierender Effekte. Auf die Effektivität von Selbstaudits von automatisierten Entscheidungssystemen zur Unterbin-

gruppen,[338] oder staatliche Stellen[339] könnten derartige Audits durchführen. Der Vorteil dieser Methode liegt auch darin, dass das autonome System in seiner Gesamtheit und in seiner sozioökonomischen Einbettung betrachtet wird. Hierfür müsste es allerdings gelingen, spezifische Fehlentwicklungen, Akzeptabilitätsgrenzen und Risikoniveaus für einzelne Anwendungsbereiche präzise zu benennen. Gerade im Hinblick auf die hier vorgestellten Autonomiegefährdungen wird erkenntlich, wie anspruchsvoll dies ist. Problematisch ist zudem, dass die Fehlentwicklungen nicht allein technische, sondern etwa auch sozio-psychologische Ursachen haben, und vielfach unklar ist, auf welche Weise Anbieter autonomer Systeme gegensteuern könnten. So ist etwa bei Selbstbestärkungs- und präemptiven Effekten auf Online-Plattformen (Filterblasen, Echokammern) in der Forschung noch ungeklärt, wie effektive Gegenmaßnahmen aussehen könnten.[340]

3. Verbote

Denkbar ist schließlich ein Verbot bestimmter Verwendungen autonomer Systeme. Die Verständlichkeit von Verfahren und Ergebnis ist dann entbehrlich. Für ein derartiges Verbot kann auch die Intransparenz ein Kriterium sein. Zu

---

dung von Verzerrungen, Fehlern und Diskriminierungen weist bereits der *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 30–31, 36–37 hin. Er bezieht diese Audits explizit auch auf die Mechanismen und Verfahren und also auf die Algorithmen, die bei der Profilbildung und -verwendung zum Einsatz kommen.

[338] Dies etwa im Rahmen von Zertifizierungen, siehe hierzu *Martini*, Blackbox Algorithmus, 2019, S. 323 f. Vgl. auch *Europäischer Datenschutzausschuss*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 25.05.2018, S. 37; *European Parliamentary Research Service*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Juni 2020, S. 52.

[339] Zu Risikoprüfungen und Audits durch staatliche Einrichtungen siehe *Mittelstadt*, Int. J. Commun. 10 (2016), 4998; *Hacker*, NJW 73 (2020), 2124, 2146. Siehe auch eingehend *European Parliamentary Research Service*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Juni 2020, S. 51 f., der zudem ein umfassende Algorithmenverträglichkeitsprüfung im Sinne einer Umweltverträglichkeitsprüfung (Algorithmic Impact Assessment) vorschlägt, siehe *ders.*, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Juni 2020, S. 53–63.

[340] Siehe hierzu bereits oben Kapitel 3 B. I. 1. a). Siehe zu verschiedenen technischen Möglichkeiten *Resnick/Garrett/Kriplean u.a.*, in: Bruckman (Hrsg.), Proceedings of the 2013 conference on Computer supported cooperative work companion, 2013, S. 95; *Hess*, How to Escape Your Political Bubble for a Clearer View, The New York Times 03.03.2017, https://www.nytimes.com/2017/03/03/arts/the-battle-over-your-political-bubble.html.; *Gao/Lei/Chen u.a.*, CIRS: Bursting Filter Bubbles by Counterfactual Interactive Recommender System, 4.4.2022.

verbieten sind dann also Systeme, die menschlich nicht verständlich sind.[341] Ähnlich wirkte im Übrigen ein Gebot menschlicher Verständlichkeit.[342] Hier ist allerdings besondere Sensibilität gefragt, denn Verbote wirken technikhinderlich und greifen in erheblichem Maße in unternehmerische Interessen ein, zudem sind diese paternalistisch-bevormundend. Sinnvoll erscheint eine Differenzierung nach dem Transparenzbedarf sowie dem Risiko der Anwendung. Es wird Anwendungen geben, bei denen die laiengerechte Verständlichkeit des Entscheidungsergebnisses gerade maßgeblich für Akzeptierfähigkeit des Systems ist.[343] Dies ist etwa bei automatisierten Entscheidungen der Fall. Auch hier kommt es aber auf die Bedeutung der Entscheidung für die betroffene Person an. In anderen Konstellationen sorgt bereits die inhaltliche Richtigkeit für Akzeptierfähigkeit. So liegt dies vor allem in Fällen automatisierter Steuerung, d.h. etwa bei Informationsfilterdiensten. Dann ist es allein das Risiko der Anwendung, anhand dessen die Sinnhaftigkeit eines Verbots zu ermessen ist. Mit dem Fokus dieser Arbeit müssten also Anwendungen mit inakzeptabler Diskriminierungsanfälligkeit oder Autonomiegefährdungspotential unterbunden werden. Sinnvoll erscheint eine bereichsspezifische Differenzierung, etwa nach Informationsfiltersystemen und Markt sowie Marktbereichen (Werbung). Im Ergebnis bedarf die Einführung von Verboten einer sorgfältigen Prüfung und weiterer interdisziplinärer Forschung zu den Folgen und zur Akzeptanzfähigkeit (intransparenter) autonomer Systeme.

II. Bewertung des KI-Gesetz-E der Europäischen Kommission

Mit dem KI-Gesetz-E hat die Europäische Kommission einen Ansatz vorgelegt, mit dem eine derartige Regulierung von Modell und Lösungsalgorithmus erfolgen könnte.[344] Dabei hat er einige der hier vorgestellten Mechanismen integriert.[345] Es soll hier keine vertiefte Kritik dieses Regelungsvorschlags erfol-

---

[341] Ausdrücklich ein Verbot von menschlich nicht verständlichen Verarbeitungsmethoden fordert Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 13 Rn. 16; Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Dix*, Art. 12 Rn. 12. Zu Verboten selbstlernender, opaker Algorithmen in bestimmten Anwendungsbereichen siehe *Burrell*, Big Data and Society 3 (2016), 9. Zu Verboten bei Informationsfilterdiensten siehe *Mittelstadt*, Int. J. Commun. 10 (2016), 4998.

[342] Ein Gebot der Erheblichkeit, d.h. der nachweisbaren Relevanz von Entscheidungsvariable und Ergebnis bei besonders risikoreicher Profilbildungen und Anwendungen, etwa dem Scoring, fordern *Martini*, Blackbox Algorithmus, 2019, S. 257–259, 352–353; *Ernst*, JZ 72 (2017), 1026, 1035.

[343] Siehe zu diesem Ansatz auch *Burrell*, Big Data and Society 3 (2016), 9. Dies befürwortet auch *Ertel*, Grundkurs Künstliche Intelligenz, ^{5}2021, S. 343 f.

[344] Siehe hierzu bereits eingehend Kapitel 3 B. II. 3. b).

[345] So enthält der Entwurf insbesondere Qualitätsanforderungen hinsichtlich der Datensätze, Art. 10 KI-Gesetz-E, ein Risikomanagementsystem, Art. 9 KI-Gesetz-E, sowie Verbote bestimmter Anwendungen, Art. 5 KI-Gesetz-E.

gen. Bereits bei einer ersten groben Einschätzung lässt sich aber erkennen, dass der Vorschlag zwar in die richtige Richtung geht, aber die Regulierungsmechanismen unzureichend ausgestaltet. Vertieftere Anforderungen gelten ohnehin nur für Hochrisikosysteme[346] Ob damit auch sämtliche regulierungsnotwendige Modelle und Lösungsalgorithmen erfasst sind, ist fraglich.[347] Das Risikomanagementsystem ist zudem sehr vage gestaltet.[348] Schon der Risikobegriff ist nicht definiert oder konkretisiert.[349] Ob, unter welchen Umständen und auf welche Weise Autonomiegefährdungen und Diskriminierungen zu prüfen sind und wie dem entgegenzuwirken ist, lässt sich dem Entwurf nicht entnehmen. Der Vorschlag stellt Transparenzpflichten auf,[350] lässt aber offen, welches Verständnisniveau gefordert ist und erlaubt auch keine Differenzierungen nach dem Transparenzbedarf im Einzelfall.[351] Bei striktem Verständnis müsste man die Vorschrift als Verbot menschlich unverständlicher Systeme verstehen.[352] Verbote sieht der KI-Gesetz-E für inakzeptable Systeme vor. Auch Ma-

---

[346] Definiert in Art. 6 KI-Gesetz-E. Kritisch zu dieser engen Fassung des Anwendungsbereichs *McCarthy Mark, Propp, Kenneth*, Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation, Lawfare, 28.04.2021. Vgl. auch *Chamberlain*, European Journal of Risk Regulation 13 (2022), 1, 7.

[347] Die im Rahmen dieser Arbeit vorgestellten Referenzbeispiele lassen sich nur teilweise als Hochrisikosysteme einordnen. Automatisierte Kreditentscheidungen sind im Anhang III Nr. 5 lit. b) aufgeführt, allerdings nur, soweit es dabei um die Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen geht. Personalisierte Preisgestaltungen unterfallen dem Anhang nicht. Personalisierte Werbemaßnahmen sind nicht aufgeführt, ebenso wenig Informationsfilterdienste. Vgl. zur Einordnung von Informationsfilterdiensten und Empfehlungssystemen auch *McCarthy Mark, Propp, Kenneth*, Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation, Lawfare, 28.04.2021. Kritisch auch *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 532; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 593 f.; *Hoffmann*, K&R 20 (2021), 369, 371, die zahlreiche Beispiele aufführen, die nach dem KI-Gesetz-E keine Hochrisikosysteme darstellen, obschon sie mit einem hohen Schädigungspotential aufwarten.

[348] Das Risikomanagementsystem wird allgemein befürwortet, siehe etwa *Hoffmann*, K&R 20 (2021), 369, 371 f.

[349] Sehr allgemein ist im KI-Gesetz-E von Risiken für die Gesundheit, Sicherheit und die Grundrechte die Rede. Siehe etwa Erwägungsgründe 1, 32, 38, 43, 50 und 58, siehe auch Art. 7 Abs. 1 lit. b), Art. 53 Abs. 2 KI-Gesetz-E. Kritisch hierzu *Cooman*, Market and Competition Law Review 6 (2022), 49, 56; *Hoffmann*, K&R 20 (2021), 369, 372.

[350] Art. 13, Art. 14 Abs. 4 lit. a) und lit. c) KI-Gesetz-E.

[351] *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 533; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 596; *Varošanec*, Int. Rev. Law Comput. Technol. 36 (2022), 95, 103. Siehe auch *Ebers*, RDi 1 (2021), 588, 590. Kritisch auch im Hinblick auf die fehlende Berücksichtigung von unternehmerischen Interessen *Hoffmann*, K&R 20 (2021), 369, 372 f.

[352] Vgl. zu diesen Erwägungen *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 534; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 596. Siehe

nipulationen sind hier angesprochen[353] ebenso wie diskriminierende Systeme, dies allerdings nur in Gestalt von staatlichen Social-Scoring-Systemen.[354] Die Auflistung erscheint sehr knapp,[355] zudem sind die Vorschriften vielfach äußerst unbestimmt. Insbesondere bei personalisierten Werbemaßnahmen ist nicht klar, unter welchen Umständen diese untersagt sein sollen.[356]

D. Ergebnis

Ziel dieses Kapitels war es, aufzuzeigen, was die DSGVO im Hinblick auf die Regulierung autonomer Systeme leisten kann und was nicht. Datenschutzrecht adressiert allein Datenverarbeitungen, präziser: datenverarbeitungsspezifische Risiken, und begegnet diesen mit datenverarbeitungsbezogenen Steuerungsmechanismen. Was vor oder jenseits der Datenverarbeitung steht, insbesondere also Algorithmen oder Entscheidungen ist datenschutzrechtlich nicht von Interesse.

---

zur faktischen Verbotswirkung eines Transparenz- und Verständlichkeitsgebots bereits *Hoeren/Niehoff*, RW 9 (2018), 47, 60; *Ertel*, Grundkurs Künstliche Intelligenz, [5]2021, S. 343.

[353] Siehe Art. 5 Abs. 1 lit. a) und b) KI-Gesetz-E.

[354] Art. 5 Abs. 1 lit. c) KI-Gesetz-E. Dass das Scoring durch Privatpersonen nicht aufgenommen ist, kritisiert etwa *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 11.

[355] Kritisch auch *Ebert/Spiecker gen. Döhmann*, NVwZ 40 (2021), 1188, 1193: „Die Liste […] entbehrt aber einer leitenden Systematik". Ähnlich *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97, 112 „The prohibitions range throughthe fantastical, the legitimising, and the ambiguous". Bemängelt wird etwa, dass die Liste Emotionserkennungssysteme nicht enthält, so *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 531; *Europäischer DatenSchutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 12. Kritisiert wird auch, dass überindividuelle Schutzgüter wie etwa der Umweltschutz, gänzlich ausgeblendet bleiben, so *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 537; *Kalbhenn*, ZUM 65 (2021), 663, 673. Der enumerative Ansatz macht das Regulierungsregime zudem starr und undynamisch, so *Ebers/Hoch/Rosenkranz u.a.*, RDi 1 (2021), 528, 531; *Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter*, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18.06.2021, S. 9; *Ebers/Hoch/Rosenkranz u.a.*, Multidisciplinary Scientific Journal 4 (2021), 589, 592; *Heiss*, EuCML 10 (2021), 252, 254. Vgl. auch *Chamberlain*, European Journal of Risk Regulation 13 (2022), 1, 6.

[356] Kritisiert wird auch, dass manipulative Übergriffe nicht per se, sondern nur verboten sind, soweit sie kausal zu physischen oder psychischen Schäden führen, so *Veale/Zuiderveen Borgesius*, CRi 22 (2021), 97, 99.

Weiterentwicklungspotentiale der DSGVO betreffen vor allem den Regulierungszugriff der DSGVO auf die Profilbildung sowie automatisierte Entscheidungen. Diese sind jeweils eigenen, besonderen datenschutzrechtlichen Vorschriften zu unterwerfen. Für das Profiling rechtfertigt sich dies daraus, dass hier Erkenntnisse jenseits der Rohdaten gewonnen werden, für die automatisierte Entscheidung daraus, dass dabei eine nicht vorhersehbare nachteilige Folge mit einem Datum bzw. einem Datenverarbeitungsergebnis verknüpft wird. Um den in Art. 22 DSGVO normierten besonderen Regulierungszugriff auf automatisierte Entscheidungen auszuweiten, sollten hierunter auch Maßnahmen gefasst sowie teilautomatisierte Entscheidungen – dies über einen Kausalitätsnachweis – aufgenommen werden. Die Beschränkung auf nachteilige rechtliche oder tatsächliche Folgen ist dagegen richtig; erst dies begründet den besonderen Regulierungsbedarf automatisierter Entscheidung. Die Modellbildung ebenso wie die Erstellung eines Lösungsalgorithmus in einem Maschinellen Lernverfahren liegen dagegen jenseits des Regulierungsauftrags der DSGVO.

Hinsichtlich des Zweckfestlegungsgrundsatzes sind keine Innovationen der DSGVO angezeigt. Ein Einbezug der Profilbildung in den Rechtmäßigkeitsgrundsatz ist nicht notwendig: Bereits durch die Rechtmäßigkeitsprüfung des Rohdatums ist eine Zulassungsprüfung der Profilbildung möglich, die in Art. 6 Abs. 1 DSGVO benannten Zulassungsgründe erscheinen zudem ausreichend. Ein Verbot der Profilbildung ist ebenso wenig überzeugend wie die Einführung einer Zulassungsprüfung einzelner Profilinhalte. Der Rechtmäßigkeitsgrundsatz fordert im Ergebnis vor allem Weiterentwicklungen, um der hohen Anzahl und Komplexität der datengetriebenen autonomen Systeme zu begegnen. Eine Reduktion der Zulassungsentscheidungen ist aber kein ergiebiger Weg: Sowohl broad consent-Modelle als auch generalisierte Einwilligungen führen nicht zu sinnvollen Lösungen. Vielversprechend ist aber eine nach dem Risiko der Datenverarbeitungen bestimmte zeitliche Staffelung der Zulassungsentscheidungen. Darüber hinaus bieten technische Einrichtungen gute Lösungen. Bereits Einwilligungsassistenten sind vielversprechend, noch effektiver erscheint die Einführung von Personal Information Management Systems (PIMS), die aber einen Systemwandel hin zu einem Modell einer zentralisierten Datenspeicherung und -verwaltung durch die betroffene Person erfordern. Auch für die vertragsimmanente Zulassung sind Erleichterungen der Zulassungsprüfung durch technische Applikationen möglich, dann in Gestalt von Smart Contracts. Weiterentwicklungen hinsichtlich der Interessensabwägung sind nur in Gestalt einer Konkretisierung der Abwägungskriterien möglich, da nach dem derzeitigen technischen Stand diese Abwägungsentscheidung nicht automatisierbar ist.

Der Transparenzgrundsatz avanciert zum wesentlichen Instrument für die effektive Steuerung autonomer Systeme. Um Transparenzbedarfe autonomer Systeme zu fassen, bedarf es zunächst einer Erweiterung der algorithmenspe-

zifischen Informationspflichten auf die Profilbildung. Bei der Profilbildung ist auf das Stattfinden der Profilbildung ebenso wie auf die Profilbasiertheit hinzuweisen. Auch über die involvierte Logik ist im Vor- und Nachhinein aufzuklären. Zudem sind erwartete Profilinhalte zu prognostizieren, soweit sie sich als überraschend darstellen und die Profilbildung insgesamt risikoreich erscheint. Schließlich ist ein umfassendes nachträgliches Einblicksrecht in Profilinhalte zu etablieren.

Um einer quantitativen und qualitativen Überforderung durch Informationsbereitstellung entgegenzutreten, bietet sich die Verwendung visueller und videographischer Darstellungsformen, insbesondere Warn- und Risikokennzeichnungen an. Auch Informationsfilterdienste sind sinnvoll. Schließlich ist das Transparenzrechtsverhältnis hinsichtlich ExpertInnen und der Gesamtöffentlichkeit zu öffnen, um betroffenen Personen Zugänge zu den von diesen geschaffenen alternativen Informationsmärkten zu ermöglichen und das Transparenznetzwerk insgesamt zu stärken.

Innovationsbedarfe bestehen vor allem im Hinblick auf die fehlende Nachvollziehbarkeit der Verarbeitung durch autonome Systeme. Bei automatisierten Entscheidungen ist die Einführung eines (nachträglichen) Rechts auf Erklärung sinnvoll. Inhaltlich zielt es auf eine Begründung ab und dies in Korrespondenz mit Art. 22 Abs. 3 DSGVO: Die automatisierte Entscheidung ist auf solche Weise menschlich verständlich zu machen, dass die betroffene Person diese prüfen und anfechten, ein menschlicher Akteur diese kontrollieren und abändern könnte. Hierfür sind die wesentlichen Entscheidungsparameter und deren Gewicht darzulegen. Die Wesentlichkeit des Entscheidungsparameters bestimmt sich nach dem Risiko der Anwendung und dem Maß der Unverständlichkeit für die betroffene Person. Diese menschlich verständliche Aufbereitung ist auch im Vorhinein einer automatisierten Entscheidung zu liefern, sie korrespondiert dort mit der Zulassungsentscheidung nach Art. 22 Abs. 2 DSGVO. Die Leistungsfähigkeit technischer Verfahren zur Herstellung menschlicher Verständlichkeit (explainable AI) ist derzeit noch zu ungewiss, um diese rechtlich verwerten zu können. Diese Ansätze lassen sich auch auf Informationspflichten zum Profilbildungsverfahren übertragen. Prognostizierte bzw. nachträglich offengelegte Profilinhalte müssen in laienhaft verständliche Konsistenzzusammenhänge eingeordnet werden, allerdings nur, wenn sich die einzelne Ableitung oder die Profilbildung insgesamt als risikoreich darstellt. Am Ende werden dann aber Bereiche bleiben, die nicht laienhaft bzw. menschlich verständlich sind. Diesen kann teilweise mit expertenbezogen Transparenzmodellen begegnet werden. Bei menschlich gänzlich unverständlichen Verfahren sind nur transparenzunabhängige Regulierungsmethoden möglich, die an den Algorithmen und dem Maschinellen Lernverfahren ansetzen. Kurz wurde skizziert wie dies aussehen könnte: Sinnvoll erscheint die Aufstellung substantieller Kriterien und die Einbindung in ein Selbst- und Fremdkontrollsystem, im Einzelfall sind für besonders risikoreiche Systeme

auch Verbote denkbar. Dies verweist dann aber auf Regulierungsbedarfe jenseits der DSGVO. Der KI-Gesetz-E geht in die richtige Richtung, ist aber vielfach zu unpräzise.

Fazit

Gegenstand dieser Untersuchung war die Frage, welchen Beitrag die DSGVO zur Regulierung autonomer Systeme als eine bestimmte Anwendung von Systemen Künstlicher Intelligenz leisten kann und dies im Hinblick darauf, ob sie zur Eindämmung von Autonomiegefährdungen und Diskriminierungen ausreichend ist. Im Folgenden sollen die wesentlichen Erkenntnisse der Arbeit zusammengefasst werden (A.) und eine abschließende Schlussbetrachtung angestellt werden (B.).

A. Zusammenfassung in Thesen

I. Technische Grundlagen autonomer Systeme

1. Gegenstand der Arbeit sind individualisierte autonome Systeme, die zur Interaktion mit dem Menschen bestimmt sind, dies in Form personalisierter Dienste sowie in Form automatisierter Entscheidungen. Das Maschinelle Lernen ist hierfür Schlüsseltechnologie.

2. Zur technischen Realisierung generieren autonome Systeme Benutzerprofile in einem zweistufigen Profilbildungsverfahren, bei dem aus den Daten einer Vielzahl von NutzerInnen unter Anwendung Maschineller Lernverfahren ein Gruppenprofil (Modell) erstellt und dieses auf die Einzelperson (Profil) angewandt wird. Dies erlaubt Erkenntnisse über die Einzelperson jenseits der von ihr bereitgestellten Rohdaten. Zur Auslösung einer automatisierten Anwendung bedarf es der Profilverwendung, d.h. der Verarbeitung des Profils und gegebenenfalls weiterer Daten in einem Lösungsalgorithmus, der seinerseits in einem Maschinellen Lernverfahren erstellt werden kann.

II. Soziokulturelle Bewertungen autonomer Systeme

1. Das durch das Maschinelle Lernverfahren gewonnene Wissen über eine Gruppe oder Person (Modell und Profil) oder eine Problemlösung (Lösungsalgorithmus) unterscheidet sich von menschlichem Wissen sowie von Erkenntnissen, die bisher anhand von Big-Data-Analyseverfahren gewonnen werden konnten.

2. Autonome System versprechen ein hohes Maß an Objektivität und Akkuratesse, Transparenz und Beeinflussbarkeit sowie den Zugang zu neuen Wissensquellen. Autonome Systeme sind aber auch potentiell fehleranfällig und verzerrt (biased), funktionsbedingt beschränkt, intransparent und deterministisch. Ob man eher die Chancen oder die Risiken der autonomen Systeme in den Vordergrund stellt, hängt von individuellen Überzeugungen ab, insbesondere von der Einstellung gegenüber Technik im Allgemeinen und autonomer Systeme im Besonderen sowie von der Auffassung über die richtige Verteilung staatlicher und privater Verantwortung.

3. Autonome Systeme wirken auf einzelne Interessensfelder, nämlich auf Markt, Gleichheit, Würde und Freiheit und begründen konkrete Regulierungsbedarfe. Sie können Wissens- und Machtasymmetrien hervorrufen, Diskriminierungen, Ungleichbehandlungen, Fragmentierungen und Segmentierungen auslösen, die materielle Fairness gefährden, zu unzutreffenden und entindividualisierenden Darstellungen und unerwünschten Informationsemergenzen führen, Verkürzungen äußerer Verhaltensfreiheit bedingen sowie – in Form von verhaltensökonomischen Effekten, präemptiven Realitätsgestaltungen, Manipulationen und Abschreckungs- und Hemmeffekten – Beeinträchtigungen innerer Verhaltensfreiheit hervorrufen. Die vorliegende Untersuchung fokussiert auf diese letztgenannte Fallgruppe, also Autonomiegefährdungen, bezieht aber auch Aspekte der Diskriminierung ein.

III. Grundlegende Fragen zur Regulierung autonomer Systeme

1. Als Bewertungsmaßstab dieser Arbeit wurde derjenige einer normativen Angemessenheit bzw. Rationalität gewählt. Die DSGVO war danach zu bewerten, inwieweit sie eine gute bzw. optimale regulative Antwort auf die aufgeworfenen Regulierungsbedarfe bietet. Abgestellt wurde auf die tatsächliche Wirkung ihrer Rechtsinstrumente und deren Fähigkeit, einen Ausgleich zwischen den kollidierenden Interessen der am Einsatz autonomer Systeme beteiligten Personen sowie zwischen Innovationsermöglichung und Innovationslenkung herzustellen.

2. Derzeit werden verschiedene Ansätze für eine Regulierung autonomer Systeme diskutiert, unterscheiden lassen sich tradiert-punktuelle und innovativ-technikspezifische Methoden. Zu den tradierten Methoden zählen Initiativen zur Plattformregulierung, Regulierungsansätze im Bereich des Verbraucherschutzes und der Marktregulierung sowie dem Antidiskriminierungsrecht, überdies Regulierungsprojekte, die Privatheit, materielle Fairness sowie die Menschenwürde absichern sollen. Innovative Regulierungsmethoden konstruieren ein Recht auf menschliche Entscheidung, schlagen die Anerkennung einer (Teil-)Rechtspersönlichkeit für autonome Systeme vor oder treten für die Einführung eines Algorithmen- oder Roboterrechts oder eines Rechtsakts für Künstliche Intelligenz ein.

3. Nach dem normativen Konzept erbringt die DSGVO einen Beitrag zur Regulierung autonomer Systeme, indem sie die durch diese durchgeführten Verarbeitungen personenbezogener Daten einer Regulierung unterwirft und datenverarbeitungsspezifische Regulierungsbedarfe mit datenschutzrechtlichen Instrumenten beantwortet. Sie soll natürliche Personen vor den Beeinträchtigungen ihrer subjektiven Rechte schützen, die durch die Unkontrolliertheit und Intransparenz der Verarbeitung der ihr zugeordneten Daten ausgelöst sind. Die DSGVO etabliert kein Recht auf informationelle Selbstbestimmung, sondern schafft eine objektiv-rechtliche Datenstrukturierungsarchitektur. Die DSGVO ist technikneutral ausgestaltet. Der übergeordnete Zweck der DSGVO liegt in der Gewährleistung digitaler Autonomie. Hierfür errichtet die DSGVO im Verhältnis zwischen Privaten ein dezentrales Regulierungsregime. Digitale Autonomie bedeutet dabei nicht individuelle Datenkontrolle, sondern Mitbestimmung der betroffenen Person an der Gestaltung ihrer digitalen sozialen und wirtschaftlichen Beziehungen.

IV. Bewertung der Regulierungszugriffe DSGVO

1. Die Untersuchung hat gezeigt, dass die DSGVO einen umfassenden, dabei differenzierenden Regulierungszugriff auf autonome Systeme bietet: Sie kommt auf sämtlichen Verarbeitungsstufen – Modell- und Profilbildung sowie Profilverwendung – zur Anwendung, erlaubt Anpassungen der Regulierungsintensität nach dem Risikograd der jeweiligen Verarbeitungsstufe und erlaubt Kooperationen der Regulierung zwischen den einzelnen Verarbeitungsstufen. Auf Verarbeitungsziel und -technik kommt es nicht an. Mit der Regulierung automatisierter Entscheidungen öffnet sie sich zudem algorithmen- und automatisierungsspezifischen Regulierungsbedarfen.

2. Allerdings sieht die DSGVO keinen spezifischen Zugriff auf die Modellbildung sowie die Erstellung des Lösungsalgorithmus und also das Maschinelle Lernverfahren vor, im Übrigen auch keine eigenständige Vorschrift für das Profiling. Schließlich erfährt auch die Profilverwendung keine besondere Regulierung, da der überwiegende Teil von Anwendungen autonomer Systeme keine automatisierte Entscheidung nach Art. 22 DSGVO darstellt, insbesondere nicht automatisierte Steuerungen wie die Informationsfilterung oder die personalisierte Werbung. Autonome Systeme werden daher vorwiegend über die allgemeinen Datenschutzvorschriften reguliert.

3. Dies führt zu deutlichen Regulierungsschwächen. Nach den Erkenntnissen der Arbeit sind Modell wie auch Lösungsalgorithmus besonders regulierungsbedürftig, liegen in ihnen doch wesentliche Ursachen für Autonomiegefährdungen und Diskriminierungen. Zugleich führen Modell und Lösungsalgorithmus aufgrund ihrer fehlenden Nachvollziehbarkeit zur Schwächung der datenschutzrechtlichen Instrumente. Die Profilbildung löst besondere Regulierungsbedarfe aus, da sie umfassende, dabei für die betroffene Person intrans-

parente Erkenntnisse über eine Person erlaubt. Dies begründet eigene Autonomiegefährdungen unabhängig von einer automatisierten Entscheidung. Art. 22 DSGVO ist zu strikt bemessen. Bloße Outputs eines Systems unterfallen der Vorschrift nicht, auch teilautomatisierte Entscheidungen und das Phänomen des Automation Bias, d.h. der faktischen Vorwegbindung menschlicher Entscheider an das maschinelle Ergebnis, bleiben unberücksichtigt.

V. Bewertung des Zweckfestlegungsgrundsatz

1. Der Zweckfestlegungsgrundsatz erscheint als ein sinnvolles und effektives Regulierungsinstrument autonomer Systeme. Vor allem das Gebot der Zweckbestimmung erweist sich als angemessenes Instrument zum Umgang mit nicht nachvollziehbaren Datenverarbeitungen.

2. Im Hinblick auf das Maschinelle Lernverfahren setzt der Zweckfestlegungsgrundsatz sinnvolle Steuerungsimpulse, ohne allzu innovationshinderlich zu wirken. Das Gebot der Zweckbestimmung verlangt keine Prognose von Verarbeitungsergebnissen. Der Einsatz ergebnisoffener Maschineller Lernverfahren ist damit zulässig, solange Anwendungskontext und Grobinhalte benannt werden. Nur wenn die Inhalte selbstlernender Algorithmen gänzlich jenseits menschlicher Verständniszusammenhänge liegen oder das Maschinelle Lernverfahren bewusst anwendungsoffen geführt wird, stellt sich der Zweckbestimmungsgrundsatz dem entgegen. Da hier die Risiken nicht mehr überschaubar wären, ist dies richtig. Überdies ist eine Mehrfachverwendung von (Trainings-)Daten überwiegend zulässig. Aufgrund des geringen Risikos der Modellbildung ist regelmäßig von einer Zweckkompatibilität auszugehen, solange der Verantwortliche auf Mehrfachverwendungen von (Trainings-)Daten hinweist. Nur bei der Mehrfachverwendung sensibler Daten oder dem Zukauf unstrukturierter Daten liegt eine unzulässige Zweckänderung vor. Auch dies ist sinnvoll, da für diese Datensätze erhöhte Risiken bestehen.

3. Auch hinsichtlich der Anwendung selbstlernender Algorithmen schafft der Zweckfestlegungsgrundsatz einen angemessenen Interessenausgleich. Bei der Profilbildung verlangt der Zweckbestimmungsgrundsatz keine Vordefinition von Profilinhalten und ermöglicht damit die Aufdeckung bislang unbekannter Persönlichkeitsmerkmale einer Person und auch solcher, die im Einzelnen menschlich nicht vorhersehbar sind. Er verhindert aber ergebnisoffene, kontextlose Profilbildungen, ebenso solche, die sich aufgrund fehlender Nachvollziehbarkeit des Modells menschlich überhaupt nicht mehr verstehen lassen. Derartige Profile sind besonders autonomiegefährdungs- und diskriminierungsanfällig, regulative Einschränkungen erscheinen daher geboten. Bei der Profilverwendung stellt der Zweckbestimmungsgrundsatz nicht vor Herausforderungen, denn an sich völlig frei entwickelnden selbstlernenden Algorithmen besteht in der Praxis kein Interesse; so dies der Fall ist, ist es aber richtig, dass diese unterbunden werden.

VI. Bewertung des Rechtmäßigkeitsgrundsatz

1. Der Rechtmäßigkeitsgrundsatz erlaubt es, auf sämtlichen Verarbeitungsstufen materielle, dabei an das Risiko angepasste Angemessenheitsbedingungen für die Verarbeitungen durchzusetzen. Auch Risikomerkmale der jeweilig vor- oder nachgehenden Verarbeitungsstufe können bei der Angemessenheitsprüfung berücksichtigt werden. Der Rechtmäßigkeitsgrundsatz erlaubt so eine differenziert-koordinative Regulierung. Bei der Profilbildung und -verwendung ist im Grundsatz die Annahme richtig, dass die Gefährdungen mit dem zu verarbeiteten Datum verknüpft sind, sodass mit der Zulassung des Datums auch über die Angemessenheit der Profilbildung bzw. Profilverwendung entschieden werden kann. Die Untersuchung hat dann aber zu dem Ergebnis geführt, dass der Rechtmäßigkeitsgrundsatz in weiten Teilen unzureichend ist.

2. Bei der Prüfung der Modellbildung wurde erkenntlich, dass und warum das Maschinelle Lernverfahren durch die DSGVO nicht reguliert werden kann. Mit ihrem atomistischen, partikularistischen, datenbezogenen und individualistischen Ansatz geht die DSGVO an den Regulierungsfragen des Maschinellen Lernverfahrens vorbei, denn dort liegt die Gefährdung im Datenkollektiv sowie im Trainingsverfahren insgesamt, vor allem aber in der algorithmischen Mustererkennung, d.h. in der stochastisch-algorithmischen Interpretation der Daten. Dass Dritte oder eine (Minderheiten-)Gruppe gefährdet sind, kann die DSGVO nicht abbilden.

3. Über die Zulässigkeit der Profilbildung und einzelner Profilinhalte anhand von Rohdaten kann bereits nach dem geltenden Recht entschieden werden. Voraussetzung ist aber, dass die Profilinhalte hinreichend voraussehbar sind. Dem Einsatz selbstlernender Algorithmen, die menschlich nicht mehr verständlich sind, stellt sich der Rechtmäßigkeitsgrundsatz entgegen, nämlich dann, wenn diese Profilinhalte generieren, mit denen die betroffene Person nicht rechnet.

4. Nämliches gilt bei der Profilverwendung: Auch hier kann über die Angemessenheit einer automatisierten Entscheidung oder Steuerung entschieden werden, indem über die Freigabe des Datums hierzu entschieden wird, allerdings nur, wenn die Folgen dieser Freigabe abschätzbar sind. Bei der Profilverwendung muss eine Zulassung ausscheiden, wenn aufgrund der fehlenden Nachvollziehbarkeit selbstlernender Algorithmen die Folgen der Profilverwendung nicht mehr überschaubar sind. Problematisch ist hier zudem, dass die fehlende Vorhersehbarkeit der Profilbildung fortwirkt. Es werden dann nämlich Profilinhalte verarbeitet, die der betroffenen Person nicht bekannt sind. Herausfordernd ist des Weiteren, dass die Autonomiegefährdungen und Diskriminierungen nicht durch die einzelne Profilverwendung, sondern erst durch die Ubiquität und Dauerhaftigkeit automatisierter Entscheidungen und Steuerungen, also inkrementell entstehen.

5. Auf sämtlichen Verarbeitungsstufen ist die hohe Datenmasse sowie die Komplexität der Verarbeitungsverfahren problematisch. Dies kann auf Seiten der betroffenen Person wie auch des Verantwortlichen sowie staatlicher Aufsichtsinstitutionen Lähmungseffekte freisetzen (Control Overload). Die Notwendigkeit der Einzelzulassung und die damit einhergehenden Pflichten für den Verantwortlichen wirken innovationsfeindlich.

VII. Bewertung des Transparenzgrundsatz

1. Der Transparenzgrundsatz erweist sich damit als das wesentliche Regulierungsinstrument der DSGVO. Er bildet die Grundlage, dass die Rechtmäßigkeitsprüfung sinnvoll durchgeführt werden kann und Betroffenenrechte nach Art. 22 Abs. 3 DSGVO ausgeübt werden können. Indem Profilinhalte und Profilverwendungsergebnisse im Vor- und Nachhinein transparent gemacht werden, kann zudem die wesentliche Ursache von Autonomiegefährdungen beseitigt werden. Für Diskriminierungen schafft die Transparenz die Grundlage, dass diese aufgedeckt und beseitigt werden können.

2. Die Untersuchung hat fünf Arten der Intransparenz identifiziert: eine rechtliche Intransparenz, d.h. die Verweigerung von Einblicken aufgrund schutzwürdiger unternehmerischer Interessen, eine faktische adressatenbezogene Intransparenz aufgrund der technischen Illiteralität betroffene Personen, eine faktische dynamische Intransparenz aufgrund der beständigen Fortentwicklung der Systeme, sodass sich aus Erkenntnissen über den vergangenen Zustand eines Systems nichts über aktuelle oder zukünftig entwickelte Ergebnisse der Systeme entnehmen lässt, eine faktische kognitionsbedingte Intransparenz aufgrund menschlicher Kognitionsgrenzen sowie schließlich eine faktische menschliche Intransparenz aufgrund originär-epistemischer Sinnaufladung durch autonome Systeme, die dem Menschen unverständlich ist. Die letztgenannte wird gemeinhin als Blackbox-Phänomen bezeichnet.

3. Die Untersuchung hat gezeigt: Der Transparenzgrundsatz bietet nur sinnvolle Lösungen, soweit er gerade in das Algorithmische hineinreicht, und er setzt voraus, dass die beschriebenen fünf Arten der Intransparenz überwunden werden können.

4. Derartige algorithmenspezifische Transparenzangebote sieht die DSGVO für automatisierte Entscheidungen vor und integriert dabei auch die Profilbildung. Sie fordert überdies eine laiengerechte Darstellung des Informationsangebots. Die rechtliche sowie die auf technischer Illiteralität begründete Intransparenz kann so überwunden werden.

5. Bei der Modellbildung, d.h. dem Maschinellen Lernverfahren sieht die DSGVO keine Transparenzangebote vor. Eigenständige Informationspflichten hinsichtlich des Profilings gewährt die DSGVO, zumindest nach der überwiegenden Ansicht, nicht. Auch Einblicksrechte in Profilinhalte im Nachhinein sind nicht vorgesehen.

6. Der konkrete Inhalt der Pflicht zur Information über die „involvierte Logik" im Hinblick auf automatisierte Entscheidungen sorgt für einige rechtliche Unsicherheiten. Die DSGVO sieht keine Lösungen für die quantitative und qualitative Informationsüberforderung (information overload) vor, sie bestärkt diese sogar eher noch. Einen Ausgleichsmechanismus für Konstellationen, in denen eine Betroffenentransparenz faktisch nicht hergestellt werden kann, sieht die DSGVO nicht vor. Soweit Verfahren und Ergebnisse nicht für den Laien, wohl aber für ExpertInnen verständlich sind, droht das dezentrale Regulierungsregime der DSGVO zu kippen. Die Transparenzanforderungen sind in besonderem Maße innovationshinderlich: Eine umfassende Aufdeckung steht unternehmerischen Interessen entgegen. Soweit eine menschliche bzw. eine laienhafte Verständlichkeit der Verarbeitungstechniken zum Gebot gemacht wird, können die meisten selbstlernenden Algorithmen nicht zulässigerweise genutzt werden.

VIII. Innovationspotentiale der DSGVO

1. Die aufgezeigten Regulierungsdefizite können teilweise durch Anpassungen der DSGVO behoben werden. Teilweise liegen sie aber jenseits des normativen Regulierungsauftrags der DSGVO und verweisen damit auf eigenständige, technikspezifische Normierungsbedarfe.

2. Weiterentwicklungen der DSGVO sind vor allem im Hinblick auf die Profilbildung sowie die automatisierte Entscheidung geboten. Bei der automatisierten Entscheidung bedarf es einer eigenständigen Begründung des Regulierungsbedarfs, da hier die Gefährdungslage vorwiegend eine nicht-datenverarbeitungsspezifische ist. Dies erfolgt über das Tatbestandsmerkmal der rechtlichen Wirkungen und der erheblichen Beeinträchtigungen. Eine Regulierung der Modellbildung bzw. der Erstellung des Lösungsalgorithmus, d.h. der Maschinellen Lernverfahren muss dagegen andernorts erfolgen, denn hier stellen sich allein algorithmenbezogene Regulierungsbedarfe, die nicht vom Regulierungsauftrag der DSGVO gedeckt sind.

3. Für die Profilbildung sind eigene Vorschriften in der DSGVO vorzusehen. Der Einführung einer eigenständigen Zulassung des Profilings bedarf es nicht, zudem auch nicht einer Zulassung einzelner erzeugter Profilinhalte. Bereits über die Zulassung des Rohdatums für die Profilbildung lassen sich diesbezügliche Angemessenheitsfragen umfassend prüfen. Voraussetzung ist aber, dass die aus dem Rohdatum generierten Profilinhalte vorhersehbar sind. Ein Verbot ist nicht interessensgerecht, die Einführung eigener, dann profilingspezifischer Zulassungstatbestände bedarf es nicht. Besondere Transparenzvorschriften, dann also für das Profilerstellungsverfahren, sind auch für das Profiling vorzusehen. Auf die Profilbildung ist hinzuweisen, ebenso auf die Profilbasiertheit eines Dienstes. Das Modellbildungsverfahren ist in seinen Grundzügen darzulegen, wesentliche erwartete Profilinhalte sind vorab zu benennen,

sofern diese sich als im Einzelfall überraschend darstellen und sich die Profilbildung insgesamt als risikoreich darstellt. Maßgeblich für den Umfang dieser Informationspflichten ist das Risiko der Profilbildung und der Umfang der Intransparenz. Im Nachhinein ist das konkret verwendete Modell zu erläutern, zudem ist ein umfassender Einblick in das Profil zu gewähren. Inwieweit weitere Schutzinstrumente mit Blick auf die Profilbildung sinnvoll sind, liegt jenseits des Untersuchungsrahmens dieser Arbeit.

4. Art. 22 DSGVO ist auch auf Maßnahmen zu erstrecken. Um den Automation Bias rechtlich zu fassen, bietet sich de lege lata ein materielles Verständnis des ausschließlichen Beruhens an; anhand einer multikriterialen Einzelfallprüfung ist dann zu bewerten, ob im Einzelfall die faktische Vorwegbindung der formalen gleichkommt. Die Tatbestandsvoraussetzung der rechtlichen Wirkungen und faktischen erheblichen Beeinträchtigungen kann über das Aufstellen von Kriterien konkretisiert werden. De lege lata ist eine Ersetzung des Tatbestandsmerkmals der Ausschließlichkeit des Beruhens durch das einer Kausalität sinnvoll.

5. Die Regulierungsdefizite des Rechtmäßigkeitsgrundsatzes können über den Transparenzgrundsatz, vor allem aber über die Reduktion von Anzahl und Komplexität der Zulassungsentscheidungen überwunden werden. Der normative Regulierungsauftrag der DSGVO steht einer Erstreckung auf eine Algorithmenprüfung entgegen, ebenso der Einrichtung eines zentralisierten Zulassungsregimes, bei der staatlicherseits oder von Seiten des Verantwortlichen inhaltliche Angemessenheitskriterien definiert werden.

6. Im geltenden Recht erscheint die Einführung einer risikobasierten zeitlichen Staffelung von Einwilligungsentscheidungen sinnvoll. Auch die Einführung von Einwilligungsassistenten ist vielversprechend. Die vertragsimmanente Zulassung kann über eine Automatisierung in Form von Smart Contracts erleichtert werden. Bei der Interessensabwägung ist eine Automatisierung nach derzeitigem technischem Stand nicht möglich, allerdings kann die Abwägungsentscheidung durch das Aufstellen von Kriterien und durch Referenzbeispiele in Bezug auf autonome Systeme erleichtert werden. De lege lata liegen Innovationspotentiale in der Entwicklung von zentralen Datenverwaltungssystemen. Vielversprechend sind dabei vor allem Personal Information Management Systems (PIMS).

7. Hinsichtlich des Transparenzgrundsatzes bedarf es Mechanismen für eine kognitionsfreundliche Aufbereitung des Informationsangebots, was über visuelle und video-graphische Darstellungen, insbesondere durch Risikokennzeichnung, sowie durch Informationsassistenzsysteme möglich ist. Technische Verfahren zur Herstellung von menschlicher Verständlichkeit autonomer Systeme (explainable AI) sind derzeit noch zu unausgereift, um rechtlich verwertet werden zu können. De lege lata ist das Transparenzverhältnis der DSGVO zu öffnen und so alternative Informationsmärkte zu erschließen, wie sie durch ExpertInnen sowie die Gesamtöffentlichkeit entstehen können.

8. Im Zentrum stehen Methoden zum Umgang mit unüberwindlichen (Betroffenen-)Intransparenzen. Ausgangspunkt der Überlegungen war die Erkenntnis, dass der Mensch schon immer in einem Umfeld der Intransparenz lebt. Hierfür hat er gute Ausgleichsmechanismen gefunden, die sich übertragen lassen. Entscheidend ist, ein normatives Verständlichkeitsniveau autonomer Systeme zu definieren. Überzeugend ist ein instrumenteller Ansatz: Für Transparenzpflichten im Nachhinein ist notwendig eine Begründung, die mit den Betroffenenrechten in Art. 22 Abs. 3 DSGVO gekoppelt ist. Die Einführung eines nachträglichen Rechts auf Erklärung, d.h. auf zusätzliche laienhafte Erläuterung der Ergebnisse, ist daher sinnvoll. Darzulegen sind dann in menschlich verständlicher Weise die grundlegenden Entscheidungsparameter und deren Gewicht, sodass eine inhaltliche Prüfung durch die betroffene Person und Dritte erfolgen kann (Auditabilität). Die Wesentlichkeit ist anhand des Risikos im Einzelfall und dem Umfang der Intransparenz zu bestimmen. Aber auch für Transparenzpflichten im Vorhinein bedarf es der menschlichen Verständlichkeit. Hier ist notwendig eine Erläuterung, die der betroffenen Person eine Risikoeinschätzung nach Art. 22 Abs. 3 DSGVO erlaubt. Diese bezieht sich dann auf die grundlegende Systemfunktionalität. Soweit eine derartige Begründung bzw. Erläuterung nicht möglich ist, bedarf es alternativer Regulierungsmechanismen, die ohne eine Betroffenentransparenz auskommen.

9. Diese Erwägungen sind auch auf Informationspflichten hinsichtlich der Profilbildung zu übertragen. Die Profilinhalte sind im Nachhinein sowie im Vorhinein, soweit sie menschlich nicht nachvollziehbar sind, in menschlich und laienhaft verständliche Konsistenzzusammenhänge einzuordnen, allerdings nur, soweit die Profilbildung sich als risikohaft darstellt.

IX. Grenzen des Datenschutzrechts

Erkenntlich werden am Ende die regulativen Grenzen der DSGVO: Sie liegen dort, wo Verfahren und Ergebnisse autonomer Systeme laienhaft bzw. menschlich nicht mehr verständlich dargestellt werden können. Die Regulierung muss hier an den Algorithmen oder der automatisierten Anwendung ansetzen, liegt dann aber jenseits der DSGVO. Eine solche Regulierung müsste etwa materielle Qualitätsvorschriften für das Maschinelle Lernverfahren aufstellen oder ein am Output und der Performance orientiertes, expertenbezogenes Audit- und Risikomanagementsystem vorsehen. Im Einzelfall können Verbote gerechtfertigt sein. Der KI-Gesetz-E der Europäischen Kommission geht in die richtige Richtung, ist aber noch zu unpräzise ausgestaltet.

B. Schlussbetrachtung

Am Ende konnte nachgewiesen werden: Die DSGVO wird an Grenzen geführt aufgrund der hohen Menge verarbeiteter Daten, der Komplexität der Verarbeitung und der fehlenden Nachvollziehbarkeit selbstlernender Algorithmen. Die Regulierungsschwächen der DSGVO liegen überdies darin begründet, dass Gefährdungen autonomer Systeme ihre Ursache in den selbstlernenden Algorithmen haben. Aufgrund der atomistischen, partikularistischen, individualistischen und datenbezogenen Perspektive kann sie Gefährdungen nicht adressieren und wirkt innovationshinderlich. Aufgrund der Technikneutralität und des global-umfassenden, partiell auch ins Algorithmische hineinreichenden und für Differenzierungen offenen Regulierungsansatzes setzt die DSGVO aber auch sinnvolle Regulierungsakzente. Die aufgezeigten Regulierungsdefizite lassen sich teilweise durch Weiterentwicklungen der DSGVO überwinden, Lösungen bieten vor allem Methoden des technischen Datenschutzes. Damit gelingt es aber nicht, sämtliche Regulierungsdefizite einzudämmen. Insbesondere für die Problematik fehlender menschlicher Nachvollziehbarkeit bedarf es eines regulativen Zugriffs auf das Maschinelle Lernverfahren, den die DSGVO nicht bietet. Auch reguliert die DSGVO Algorithmen oder automatisierte Anwendungen nicht. Hier liegen die Grenzen des technikneutralen Regulierungsansatzes und damit der DSGVO. Ob ergänzendes regulatives Tätigwerden geboten ist und wie dieses aussehen könnte, muss im politischen Diskurs geklärt werden.

Literaturverzeichnis

Sämtliche Online-Quellen wurden zuletzt am 30.06.2023 aufgerufen.

Aarts, Emile/Encarnação, José, Into Ambient Intelligence, in: dies. (Hrsg.), True Visions – The Emergence of Ambient Intelligence, Heidelberg 2006, S. 1–16.

— (Hrsg.), True Visions – The Emergence of Ambient Intelligence, Heidelberg 2006.

Abel, Ralf B., Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO, ZD 8 (2018), S. 304–307.

Access Now, Prohibit emotion recognition in the Artificial Intelligence Act November 2021, https://www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf.

Adadi, Amina/Berrada, Mohammed, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), IEEE Access 6 (2018), S. 52138–52160.

Afsar, M. Mehdi/Crump, Trafford/Far, Behrouz, Reinforcement learning based recommender systems: A survey 15.01.2021, https://arxiv.org/pdf/2101.06286.

Akerlof, George A., The Market for „Lemons": Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics 84 (1970), S. 488–500.

Akyürek, Metin (Hrsg.), Staat und Recht in europäischer Perspektive – Festschrift Heinz Schäffer, Wien/München 2006.

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005.

—, Umgang mit personenbezogenen Informationen und Daten, in: Albers, Marion/Hoffmann-Riem, Wolfgang (Hrsg.), Grundlagen des Verwaltungsrechts – Informationsordnung, Verwaltungsverfahren, Handlungsformen, 2. Aufl., München 2012, S. 107–234.

—, Realizing the Complexity of Data Protection, in: Gutwirth, Serge/Leenes, Ronald/sw Hert, Paul (Hrsg.), Reloading data protection – Multidisciplinary insights and contemporary challenges, New York 2014, S. 213–235.

—, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, S. 11–35.

Albers, Marion/Hoffmann-Riem, Wolfgang (Hrsg.), Grundlagen des Verwaltungsrechts – Informationsordnung, Verwaltungsverfahren, Handlungsformen, 2. Aufl., München 2012.

Albrecht, Jan Philipp, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 32 (2016), S. 88–98.

Ali, Shereen H./El Desouky, Ali I./Saleh, Ahmed I., A New Profile Learning Model for Recommendation System based on Machine Learning Technique, Inf Softw Technol. 6 (2016), S. 1–6.

Allen, Anita L., Privacy-as-Data Control – Conceptual, Practical, and Moral Limits of the Paradigm, Connectivut Law Review 2000, S. 861–875.

Allen, Tom/Widdison, Robin, Can Computers make contracs?, Harv. J. Law Technol. 9 (1996), 26-52.

Alpaydın, Ethem, Machine learning, Cambridge (Massachusetts) 2021.

An, Jisun/Quercia, Daniele/Crowcroft, Jon, Fragmented social media, in: Schwabe, Daniel (Hrsg.), Proceedings of the 22nd international conference on World Wide Web companion, Republic and Canton of Geneva 2013, S. 51–52.

Ananny, Mike/Crawford, Kate, Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, New Media & Society 20 (2018), S. 973–989.

Anderson, Chris, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, Wired 23.06.2008.

Andraško, Jozef/Mesarčík, Matúš/Hamuľák, Ondrej, The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework, AI and Society 36 (2021), S. 623–636.

Andreotta, Adam J./Kirkham, Nin/Rizzi, Marco, AI, big data, and the future of consent, AI and Society 36 (2021), S. 1–14.

Aneesh, Aneesh, Global Labor: Algocratic Modes of Organization, Sociological Theory 27 (2009), S. 347–370.

Angwin, Julia/Mattu, Surya/Larson, Jeff, The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review 01.09.2015, https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review-pro.

Anrig, Bernhard/Browne, Will/Gasson, Mark, The Role of Algorithms in Profiling, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 65–79.

Arora, Neeraj/Dreze, Xavier/Ghose, Anindya/Hess, James D./Iyengar, Raghuram/Jing, Bing/Joshi, Yogesh/Kumar, V./Lurie, Nicholas/Neslin, Scott/Sajeesh, S./Su, Meng/Syam, Niladri/Thomas, Jacquelyn/Zhang, Z. John, Putting one-to-one marketing to work: Personalization, customization, and choice, Marketing Letters 19 (2008), S. 305–321.

Arora, Nidhi/Ensslen, Daniel/Fiedler, Lars/Liu, Wei Wei/Robinseon, Kelsey/Stein, Eli/Schüler, Gustavo, The value of getting personalization right – or wrong – is multiplying 12.11.2021, https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying.

Artikel 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" 20.06.2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_de.pdf.

—, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting – WP 171 22.06.2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf.

—, Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes 23.03.2012, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/10_wp_29_wp191_/10_wp_29_wp191_de.pdf.

—, Opinion 03/2013 on purpose limitation – WP 203 02.04.2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

—, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation 13.05.2013, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf.

—, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG – WP 217 09.04.2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_de.pdf.

—, Stellungnahme 5/2014 zu Anonymisierungstechniken – WP 216 10.04.2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.

—, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge 16.09.2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_de.pdf.

—, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" – WP 248 rev.01 04.04.2017, zuletzt überarbeitet und angenommen am 04.10.2017, https://ec.europa.eu/newsroom/article29/items/611236/en.

—, Leitlinien für Transparenz gemäß der Verordnung 2016/679 – WP 260 rev.01 29.11.2017, zuletzt überarbeitet und angenommen am 11. 04.2018, https://ec.europa.eu/newsroom/article29/items/622227/en.

—, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 10.04.2018, https://ec.europa.eu/newsroom/article29/redirection/document/53343.

Association for Computing Machinery (Hrsg.), The 34th Annual ACM Symposium on Applied Computing, April 8–12, 2019, New York 2019.

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019.

Augusto, Juan/Mccullagh, Paul, Ambient Intelligence: Concepts and applications, Computer Science and Information Systems 4 (2007), S. 1–27.

Ausloos, Jef/Dewitte, Pierre, Shattering one-way mirrors – data subject access rights in practice, Int. Data Priv. Law 8 (2018), S. 4–28.

Aztiria, Asier/Augusto, Juan Carlos/Orlandini, Andrea (Hrsg.), State of the art in AI applied to ambient intelligence, Amsterdam u.a. 2017.

Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, Der Staat 51 (2012), 91-116.

Badesow, Jürgen, Das Rad neu erfunden – Zum Vorschlag für einen Digital Markets Act, ZEuP 29 (2021), S. 217–226.

Bakshy, Eytan/Messing, Solomon/Adamic, Lada A., Exposure to ideologically diverse news and opinion on Facebook, Science 348 (2015), S. 1130–1132.

Bambauer, Jane/Zarsky, Tal, The Algorithm Game, Notre Dame Law Review 94 (2018), S. 1–48.

Ban, Gah-Yi/Keskin, Bora N., Personalized Dynamic Pricing with Machine Learning – High-Dimensional Features and Heterogeneous Elasticity, Management Science 67 (2021), S. 5549–5568.

Bandy, Jack, Problematic Machine Behavior: A Systematic Literature Review of Algorithm Audits 03.02.2021, https://arxiv.org/pdf/2102.04256.

Bao, Wang/Lianju, Ning/Yue, Kong, Integration of unsupervised and supervised machine learning algorithms for credit risk assessment, Expert Systems with Applications 128 (2019), S. 301–315.

Barocas, Solon/Selbst, Andrew D., Big Data's Disparate Impact, Cal. L. Rev. 104 (2016), S. 671–732.

Barth, Susanne/Jong, Menno D.T. de, The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, Telematics and Informatics 34 (2017), S. 1038–1058.

Bauberger, Stefan/Beck, Birgit/Burchardt, Aljoscha/Remmers, Peter, Ethische Fragen der Künstlichen Intelligenz, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 907–934.

Bauckhage, Christian/Fürnkranz, Johannes/Paaß, Gerhard, Vertrauenswürdiges, transparentes und robustes Maschinelles Lernen, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 571–600.

Bauckhage, Christian/Hübner, Wolfgang/Hug, Ronny/Paaß, Gerhard, Tiefe neuronale Netze, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 509–570.

Bauckhage, Christian/Hübner, Wolfgang/Hug, Ronny/Paaß, Gerhard/Rüping, Stefan, Grundlagen des Maschinellen Lernens, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 429–508.

Baur, Dorothea, Algorithmic decision-making and social division – acknowledging the political context of AI, 21.2.2019, https://dorotheabaur.medium.com/algorithmic-decision-making-and-social-division-acknowledging-the-political-context-of-ai-e071e34524bb.

Bayamlıoğlu, İbrahim Emre/Baraliuc, Irina/Janssens, Liisa/Hildebrandt, Mireille (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen 2019.

Beck, Susanne, Brauchen wir ein Roboterrecht? – Ausgewählte juristische Fragen zum Zusammenleben von Menschen und Robotern, in: Japanisch-Deutsches Zentrum (Hrsg.), Mensch-Roboter-Interaktionen aus interkultureller Perspektive – Japan und Deutschland im Vergleich, Berlin 2012, S. 124–146.

—, Der rechtliche Status autonomer Maschinen, AJP/PJA 2017, S. 183–191.

—, Künstliche Intelligenz und Diskriminierung – Herausforderungen und Lösungsansätze, München 2019.

Beck, Ulrich, Risikogesellschaft – Auf dem Weg in eine andere Moderne, Berlin 1968.

Beckhusen, Michael G., Das Scoring-Verfahren der SCHUFA im Wirkungsbereich des Datenschutzrechts, BKR 5 (2005), S. 335–344.

Beierle, Christoph/Kern-Isberner, Gabriele, Methoden wissensbasierter Systeme – Grundlagen, Algorithmen, Anwendungen, 6. Aufl., Wiesbaden/Heidelberg 2019.

Bella, Giampaolo (Hrsg.), 2013 Third Workshop on Socio-Technical Aspects in Security and Trust (STAST), Piscataway 2013.

Bender, Emily M./Gebru, Timnit/McMillan-Major, Angelina/Shmitchell, Shmargaret, On the Dangers of Stochastic Parrots, in: Coscia, Michele (Hrsg.), Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, New York 2021, S. 610–623.

Berger, Ariane, Digitales Vertrauen – eine verfassungs- und verwaltungsrechtliche Perspektive, DVBl 132 (2017), S. 804–808.

Berger, Daniel, Vermarktete Facebook die Gefühle seiner Nutzer?, Heise Online 02.05.2017.

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Computer sagt Nein Kreditkartenantrags – 300.000 Euro Bußgeld gegen Bank nach mangelnder Transparenz über automatisierte Ablehnung eines 31.5.2023, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2023/20230531_PM_Bussgeld_Bank.pdf.

Beschorner, Thomas/Meckel, Miriam, Mut zum Träumen, Die Zeit 1.7.2018.

Bessi, Alessandro/Zollo, Fabiana/Del Vicario, Michela/Puliga, Michelangelo/Scala, Antonio/Caldarelli, Guido/Uzzi, Brian/Quattrociocchi, Walter, Users Polarization on Facebook and Youtube, PloS one 11 (2016), e0159641.

Betzler, Monika (Hrsg.), Autonomie der Person, Münster 2013.

Bhatia, Richa, Understanding the difference between Symbolic AI and Non Symbolic AI, Analytics India Magazine 27.12.2017.

Bietti, Elettra, Consent as a Free Pass – Platform Power and the Limits of the Informational Turn, Pace Law Review 40 (2020), S. 310–398.

Binns, Reuben, Imagining Data, between Laplace's Demon and the Rule of Succession, in: Bayamlıoğlu, İbrahim Emre/Baraliuc, Irina u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 130–133.

Blum, Peter, Wege zu besserer Gesetzgebung – sachverständige Beratung, Begründung, Folgeabschätzung und Wirkungskontrolle, München 2004.

Bobbert, Monika/Werner, Micha H., Autonomie/Selbstbestimmung, in: Lenk, Christian/Duttge, Gunnar/Fangerau, Heiner (Hrsg.), Handbuch Ethik und Recht der Forschung am Menschen, Place of publication not identified 2014, S. 105–114.

Boehme-Neßler, Volker, Unscharfes Recht – Überlegungen zur Relativierung des Rechts in der digitalisierten Welt, Berlin 2008.

—, Das Ende des Staates? Zu den Auswirkungen der Digitalisierung auf den Staat, ZöR 64 (2009), S. 145–199.

—, Das Ende der Anonymität – Wie Big Data das Datenschutzrecht verändert, DuD 40 (2016), 419-423.

—, Die Macht der Algorithmen und die Ohnmacht des Rechts – Wie die Digitalisierung das Recht relativiert, NJW 70 (2017), S. 3031–3037.

Bogner, Alexander (Hrsg.), Ethisierung der Technik – Technisierung der Ethik – Der Ethik-Boom im Lichte der Wissenschafts- und Technikforschung, Baden-Baden 2013.

Bomhard, David/Merkle, Marieke, Europäische KI-Verordnung – Der aktuelle Kommissionsentwurf und praktische Auswirkungen, RDi 1 (2021), S. 276–283.

Bonezzi, Andrea/Ostinelli, Massimiliano/Melzner, Johann, The human black-box – The illusion of understanding human better than algorithmic decision-making, Journal of experimental psychology 151 (2022), S. 1–9.

Bonß, Wolfgang, Vom Risiko – Unsicherheit und Ungewißheit in der Moderne, Hamburg 1995.

Borenstein, Jason/Wagner, Alan R./Howard, Ayanna, Overtrust of Pediatric Health-Care Robots – A Preliminary Survey of Parent Perspectives, IEEE Robot. Automat. Mag. 25 (2018), S. 46–54.

Bostrom, Nick, Superintelligence – Paths, dangers, strategies, Oxford 2014.

Bozdag, Engin, Bias in algorithmic filtering and personalization, Ethics Inf. Technol 15 (2013), S. 209–227.

Bramer, Max (Hrsg.), Artificial intelligence – An international perspective, Berlin 2009.

Brändli, Sandra (Hrsg.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, Bern 2013.

Braun Binder, Nadja, Artificial Intelligence and Taxation – Risk Management in Fully Automated Taxation Procedures, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 295–306.

Bräutigam, Peter/Schmidt-Wudy, Florian, Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung – Ein Diskussionsbeitrag zum anstehenden Trilog der EU- Gesetzgebungsorgane, CR 31 (2015), S. 56–63.

Breuer, Rüdiger/Kloepfer, Michael/Marburger, Peter/Schröder, Meinhard (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, Heidelberg 1994.

Breunig, Christian/Handel, Marlene/Kessler, Bernhard, ARD/ZDF-Onlinestudie 2020 – Massenkommunikation 2020: Nutzungsmotive und Leistungsbewertungen der Medien, Media Perspektiven 2020, S. 602–625.

Bringsjord, Selmer/Govindarajulu, Naveen Sundar, Artificial Intelligence, in: Zalta, Edward N. (Hrsg.), The Stanford Encyclopedia of Philosophy, Standford 2020.

Brink, Stefan/Wolff, Heinrich Amadeus/Ungern-Sternberg, Antje von (Hrsg.), BeckOK Datenschutzrecht, 44. Aufl., München 2023 (zit. BeckOK Datenschutzrecht, Wolff/Brink/*Bearbeiter*).

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung – Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007.

—, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Wolfgang/Brandt, Edmund/Schuler-Harms, Margarete (Hrsg.), Offene Rechtswissenschaft – Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010, S. 561–596.

—, Freie Entfaltung der Persönlichkeit (Art. 2 I 1 GG) – Verfassungsversprechen zwischen Naivität und Hybris?, NVwZ 38 (2019), S. 672–677.

Brkan, Maja, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, Int. J. Law Inf. Technol. 27 (2019), S. 91–121.

—, Freedom of Expression and Artificial Intelligence – On Personalisation, Disinformation and (Lack Of) Horizontal Effect of the Charter, SSRN Journal 9.4.2019, S. 1–17.

Bröhmer, Jürgen, Transparenz als Verfassungsprinzip – Grundgesetz und Europäische Union, Tübingen 2004.

Brown, Shea/Davidovic, Jovana/Hasan, Ali, The algorithm audit: Scoring the algorithms that score us, Big Data and Society 8 (2021), 1-8.

Brownsword, Roger, Knowing Me, Knowing You – Profiling, Privacy and the Public Interest, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 345–363.

Brownsword, Roger/Scotford, Eloise/Yeung, Karen (Hrsg.), The Oxford handbook of law, regulation, and technology, Oxford/New York, NY 2017.

Brownsword, Roger/Yeung, Karen (Hrsg.), Regulating technologies – Legal futures, regulatory frames and technological fixes, Oxford 2008.

Broy, Manfred/Kuhrmann, Marco, Einführung in die Softwaretechnik, Berlin/Heidelberg 2021.

Bruckman, Amy (Hrsg.), Proceedings of the 2013 conference on Computer supported cooperative work companion, New York 2013.

Brühl, Volker, Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, Goethe Universität Frankfurt, Frankfurt, http://hdl.handle.net/10419/191736.

Brundage, Miles/Avin, Shahar/Clark, Jack/Toner, Helen/Eckersley, Peter/Garfinkel, Ben/Dafoe, Allan/Scharre, Paul/Zeitzoff, Thomas/Filar, Bobby/Anderson, Hyrum/Roff, Heather/Allen, Gregory C./Steinhardt, Jacob/Flynn, Carrick/hÉigeartaigh, Seán Ó./Beard, Simon/Belfield, Haydn/Farquhar, Sebastian/Lyle, Clare/Crootof, Rebecca/Evans, Owain/Page, Michael/Bryson, Joanna/Yampolskiy, Roman/Amodei, Dario, The Malicious Use of Artificial Intelligence – Forecasting, Prevention, and Mitigation 20.02.2018, https://arxiv.org/pdf/1802.07228.

Bucheli, Roman, Willkommen in der Angsthasengesellschaft, NZZ 07.07.2018.

—, Wir sind auf dem besten Weg, in der Null-Risiko-Gesellschaft zu versauern, NZZ 19.02.2020.

Buchholtz, Gabriele, Artificial Intelligence and Legal Tech: Challenges to the Rule of Law, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 175–198.

—, Artificial Intelligence and Legal Tech:Challenges to the Rule of Law, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 175–198.

Büchi, Moritz/Fosch-Villaronga, Eduard/Lutz, Christoph/Tamò-Larrieux, Aurelia/Velidi, Shruthi/Viljoen, Salome, The chilling effects of algorithmic profiling – Mapping the issues, Leiden März 2020, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3379275_code2485522.pdf?abstractid=3379275&mirid=1.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

—, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 40 (2016), S. 155–161.

—, Datenverarbeitungen im nicht-öffentlichen Bereich, in: Tinnefeld, Marie-Theres/Buchner, Benedikt u.a. (Hrsg.), Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht, 6. Aufl., Berlin/Boston 2018, S. 403–476.

—, Grundsätze des Datenschutzrechts, in: Tinnefeld, Marie-Theres/Buchner, Benedikt u.a. (Hrsg.), Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht, 6. Aufl., Berlin/Boston 2018, S. 220–332.

Bughin, Jacques/Hazan, Eric/Ramaswamy, Sree/Chui, Michael/Allas, Tera/Dahlström, Peter: Henke, Nicolaus/Trench, Monica, Artificial Intelligence – the next digital frontier?, McKinsey Global Institute Juni 2017, https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx.

Bughin, Jacques/Seong, Jeongmin/Manyika, James/Chui, Michael/Joshi, Raoul, Modeling the Impact of AI on the World Economy September 2018, https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2018/2018-09-05%20-%20mgi%20ai-studie%20dampfmaschine/mgi-studie_notes_from_the_frontier_2018.pdf.

Bührer, Torben, Das Menschenwürdekonzept der Europäischen Menschenrechtskonvention, Göttingen 2020.

Buiten, Miriam C., The Digital Services Act from Intermediary Liability to Platform Regulation, JIPITEC 12 (2021), S. 361–380.

Bull, Hans Peter, Sinn und Unsinn des Datenschutzes – Persönlichkeitsrecht und Kommunikationsfreiheit in der digitalen Gesellschaft, Tübingen 2015.

—, Der „vollständig automatisiert erlassene" Verwaltungsakt – Zur Begriffsbildung und rechtlichen Einhegung von „E-Government", DVBl 132 (2017), S. 409.

—, Über die rechtliche Einbindung der Technik – Juristische Antworten auf Fragen der Technikentwicklung, Der Staat 58 (2019), S. 57–100.

Bumke, Christian, Autonomie im Recht, in: Bumke, Christian/Röthel, Anne (Hrsg.), Autonomie im Recht – Gegenwartsdebatten über einen rechtlichen Grundbegriff, Tübingen 2017, S. 3–44.

Bumke, Christian/Röthel, Anne (Hrsg.), Autonomie im Recht – Gegenwartsdebatten über einen rechtlichen Grundbegriff, Tübingen 2017.

Bundesregierung, Strategie Künstliche Intelligenz der Bundesregierung – AI made in Germany November 2018, https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie.pdf.

—, Strategie Künstliche Intelligenz der Bundesregierung – Fortschreibung 2020 Dezember 2020, https://www.bmbf.de/bmbf/shareddocs/downloads/files/201201_fortschreibung_ki-strategie.pdf?__blob=publicationFile&v=1.

Bunnenberg, Jan Niklas, Privates Datenschutzrecht 2020.

Burgelman, Jean-Claude/Punie, Yves, Information, Society and Technology, in: Aarts, Emile/Encarnação, José (Hrsg.), True Visions – The Emergence of Ambient Intelligence, Heidelberg 2006, S. 17–34.

Buri, Ilaria/van Hoboken, Joris, The Digital Services Act (DSA) proposal – a critical overview, University of Amsterdam 28.10.2021, https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.

Burkart, Nadia/Huber, Marco F., A Survey on the Explainability of Supervised Machine Learning, Journal of Artificial Intelligence Research 70 (2021), S. 245–317.

Burrell, Jenna, How the machine 'thinks' – Understanding opacity in machine learning algorithms, Big Data and Society 3 (2016).

Bus, Jacques (Hrsg.), Digital enlightenment yearbook 2012, Amsterdam/Washington, D.C 2012.

Bygrave, Lee A., Data protection law – Approaching its rationale, logic and limits, The Hague 2002.

—, Minding the Machine v2.0 – The EU General Data Protection Regulation and Automated Decision Making, in: Yeung, Karen/Lodge, Martin (Hrsg.), Algorithmic regulation, 2019, S. 248–262.

Calo, Ryan, Digital Market Manipulation, Geo. Wash. L. Rev. 82 (2014), 995-1051.

Calvano, Emilio/Calzolari, Giacomo/Denicolò, Vincenzo/Pastorello, Sergio, Algorithmic Pricing What Implications for Competition Policy?, Review of Industrial Organization 55 (2019), S. 155–171.

Calvary, Gaelle/Delot, Thierry/Sedes, Florence/Tigli, Jean-Yves (Hrsg.), Computer Science and Ambient Intelligence, Hoboken 2013.

Campbell, Thomas A., Artificial Intelligence: An overview of state initatives, FutureGrasp 2019, https://www.researchgate.net/profile/Thomas-Campbell-10/publication/334731776_ARTIFICIAL_INTELLIGENCE_AN_OVERVIEW_OF_STATE_INITIATIVES/links/5d3dc631a6fdcc370a67d5cf/ARTIFICIAL-INTELLIGENCE-AN-OVERVIEW-OF-STATE-INITIATIVES.pdf?origin=publication_detail.

Canhoto, Ana/Backhouse, James, General Description of the Process of Behavioural Profiling, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 47–57.

Carson, Audrey B., Public Discourse in the Age of Personalization – Psychological Explanations and Political Implications of Search Engine Bias and the Filter Bubble, Journal of Science Policy and Governance 7 (2015), S. 1–13.

Casey, Bryan/Farhangi, Ashkon/Vogl, Roland, Rethinking Explainable Machines – The GDPRs Right to Explanation Debate and the Rise of Algorithmic Audits in Enterprise, BTLJ 34 (2019), S. 143–188.

Castelluccia, Claude/Le Métayer, Daniel, Understanding algorithmic decision-making – Opportunities and challenges, Europäisches Parlament, Brüssel März 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf.

Cate, F. H./Mayer-Schonberger, V., Notice and consent in a world of Big Data, Int. Data Priv. Law 3 (2013), S. 67–73.

Chamberlain, Johanna, The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation – Some Comments from a Tort Law Perspective, European Journal of Risk Regulation 13 (2022), S. 1–13.

Chatzigiannakis, Ioannis/Ruyter, Boris de/*Mavrommati, Irene* (Hrsg.), Ambient Intelligence – 15th European Conference, AmI 2019, Rome, Italy, November 13–15, 2019, Proceedings, Cham 2019.

Chin, Jeannette/Callaghan, Vic/Allouch, Somaya Ben, The Internet-of-Things – Reflections on the past, present and future from a user-centered and smart environment perspective, JAISE 11 (2019), S. 45–69.

Chivot, Eline/Castro, Daniel, The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy 13.5.2019, https://www2.datainnovation.org/2019-reform-the-gdpr-ai-a4.pdf.

Chomsky, Noam/Roberts, Ian/Watumull, Jeffrey, The False Promise of ChatGPT, The New York Times 08.03.2023.

Chui, Michael/Hall, Bryce/Mayhew, Helen/Singla, Alex/Sukharevsky, Alex, The state of AI in 2022 – and a half decade in review, McKinsey & Company Dezember 2022, https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai%20in%202022%20and%20a%20half%20decade%20in%20review/the-state-of-ai-in-2022-and-a-half-decade-in-review.pdf.

Chui, Michael/Harryson, Martin/Manyika, James/Roberts, Roger/Chung, Rita/van Heteren, Ashley/Nel, Pieter, Applying AI for Social Good, McKinsey Global Institute Dezember 2018, https://ec.europa.eu/futurium/en/system/files/ged/mgi-applying-ai-for-social-good-discussion-paper-dec-2018.pdf.

Cintia Ganesha Putri, Debby/Leu, Jenq-Shiou/Seda, Pavel, Design of an Unsupervised Machine Learning-Based Movie Recommender System, Symmetry 12 (2020), S. 185–212.

Citron, Danielle Keats/Pasquale, Frank, The Scored Society – Due Proces for Automated Predictions, The Washington Law Review 89 (2014), S. 1–33.

Claes, Erik/Duff, Antony/Gutwirth, Serge (Hrsg.), Privacy and the criminal law, Antwerpen 2006.

Clement, Reiner/Schreiber, Dirk/Bossauer, Paul/Pakusch, Christina (Hrsg.), Internet-Ökonomie – Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft, 4. Aufl., Berlin/Heidelberg 2019.

Colonna, Liane/Greenstein, Stanley (Hrsg.), Law in the era of artificial intelligence, Visby/Stockholm 2022.

Conrad, Isabell, Recht des Datenschutzes – § 34, in: Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019, Rn. 1–880.

Cook, Diane J./Augusto, Juan C./Jakkula, Vikramaditya R., Ambient intelligence – Technologies, applications, and opportunities, Pervasive and Mobile Computing 5 (2009), S. 277–298.

Cooman, Jerome de, Humpty Dumpty and High-Risk AI Systems – The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act, Market and Competition Law Review 6 (2022), S. 49–88.

Corbett-Davies, Sam/Goel, Sharad, The Measure and Mismeasure of Fairness – A Critical Review of Fair Machine Learning, Stanford University 14.8.2018, arXiv:1808.00023v2.

Cornils, Matthias, Vielfaltssicherung bei Telemedien, AfP 49 (2018), S. 377–387.

Corrales, Marcelo/Fenwick, Mark/Forgó, Nikolaus (Hrsg.), New Technology, Big Data and the Law, Singapore 2017.

Coscia, Michele (Hrsg.), Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, New York 2021.

Council on Artificial Intelligence, Recommendation of the Council on Artificial Intelligence, OECD Legal Instruments 2022, https://legalinstruments.oecd.org/api/print?ids=648&lang=en.

Coutaz, Joëlle/Crowley, James L., Ambient Intelligence: Science or Fad?, in: Calvary, Gaelle/Delot, Thierry u.a. (Hrsg.), Computer Science and Ambient Intelligence, Hoboken 2013, S. 1–13.

Culik, Nicolai/Döpke, Christian, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen – Analyse möglicher Auswirkungen der DS-GVO, ZD 7 (2017), S. 226–230.

Custers, Bart, Profiling as Inferred Data – Amplifier Affects and Positive Feedback Loops, in: Bayamlıoğlu, İbrahim Emre/Baraliuc, Irina u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, 112–115.

Custers, Bart/Uršič, Helena, Big data and data reuse – a taxonomy of data reuse for balancing big data benefits and personal data protection, Int. Data Priv. Law 6 (2016), S. 1–12.

Custers, Bart/van der Hof, Simone/Schermer, Bart/Appleby-Arnold, Sandra/Brockdorff, Noellie, Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law, SCRIPed 10 (2013), S. 435–457.

D'Aloia, Antonio/Errigo, Maria Chiara (Hrsg.), Neuroscience and Law – Complicated Crossings and New Perspectives, Cham 2020.

Dalla Corte, Lorenzo, Scoping Personal Data – Towards a Nuanced Interpretation of the Material Scope of EU Data Protecton Law, European Journal of Law and Technology 10 (2019), S. 1–26.

Damm, Werner/Kalmar, Ralf, Autonome Systeme, Informatik Spektrum 40 (2017), S. 400–408.

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 6 (2016), S. 307–314.

Danaher, John, The Ethics of Algortihmic Outsourcing in Everyday Life, in: Yeung, Karen/Lodge, Martin (Hrsg.), Algorithmic regulation, 2019, S. 98–117.

Danckert, Burkhard/Mayer, Frank J., Die vorherrschende Meinungsmacht von Google – Bedrohung durch einen Informationsmonopolisten?, MMR 13 (2010), S. 219–222.

Dastin, Jeffrey, Amazon scraps secret AI recruiting tool that showed bias against women, Reuters 11.10.2018.

Datenethikkommission, Gutachten der Datenethikkommission der Bundesregierung, Bundesministerium des Inneren, für Bau und Heimat, Berlin Oktober 2019, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.html;jsessionid=45733EB7626BC2BF8CB68295514528C2.2_cid334?nn=11678504.

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke (Hrsg.), EU-DSGVO und BDSG – Kompaktkommentar: EU-Datenschutz-Grundverordnung (EU-DSGVO), neues Bundesdatenschutzgesetz (BDSG), weitere datenschutzrechtliche Vorschriften, 2. Aufl., Frankfurt am Main 2020 (zit. Däubler/Wedde/Weichert/Sommer, EU-DSGVO/*Bearbeiter*).

Davenport, Thomas H./Harris, Jeanne G., Automated decision making comes of age – After decades of anticipation, the promise of automated decision-making systems is finally becoming a reality in a variety of industries, MIT Sloan Management Review 46 (2006), S. 1–10.

Deakin, Simon F./Markou, Christopher (Hrsg.), Is law computable? – Critical perspectives on law and artificial intelligence, Oxford u.a. 2020.

Delisle, Marc/Weyer, Johannes, Datengenerierung, in: Kolany-Raiser, Barbara/Heil, Reinhard u.a. (Hrsg.), Big Data und Gesellschaft – Eine multidisziplinäre Annäherung, Wiesbaden 2018, S. 84–101.

Delko, Krim, Hype und Realität in den Strassen von San Francisco, NZZ 09.08.2018.

Deutscher Ethikrat, Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz, Berlin 20.03.2023, https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf.

Di Fabio, Udo, Sicherheit in Freiheit, NJW 61 (2008), S. 421–425.

Die Medienanstalten, Mediengewichtungsstudie 2020-I – Gewichtungsstudie zur Relevanz der Medien für die Meinungsbildung in Deutschland, Kantar Media Research, Berlin 2020, https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Themen/Forschung/Mediengewichtungsstudie/Die_Medienanstalten_Mediengewichtungsstudie_2020-I.pdf.

Dienlin, Tobias, Das Privacy Paradox aus psychologischer Perspektive, in: Specht-Riemenschneider, Louisa/Werry, Nikola u.a. (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2019, S. 305–323.

Dignum, Virginia, Responsible Artificial Intelligence – How to Develop and Use AI in a Responsible Way, Cham 2019.

Dimitrova, Diana, The Right to Explanation under the Right of Access to Personal Data, EDPL 6 (2020), S. 211–230.

Djeffal, Christian, Artificial Intelligence and Public Governance: Normative Guidelines for Artificial Intelligence in Government and Public Administration, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 277–293.

—, The Normative Potential of the European Rule on Automated Decisions: A New Reading for Art. 22 GDPR, ZaöRV 80 (2020), S. 847–879.

Döbel, Inga/Leis, Miriam/Vogelsang, Manuel Molina/Neustroev, Dmitry/Petzka, Henning/Rüing, Stefan/Voss, Angelika/Wegele, Martin/Welz, Juliane, Maschinelles Lernen – Kompetenzen, Anwendungen und Forschungsbedarf, Fraunhofer-Gesellschaft, München 2018, https://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/Publikationen/Fraunhofer_Studie_ML_201809.pdf.

Domingos, Pedro, A few useful things to know about machine learning, Communications of the ACM 2012 (2012), S. 78–87.

Donath, Philipp B./Bretthauer, Sebastian/Dickel-Görig, Marie/Drehwald, Jennifer/Gourdet, Sascha/Heger, Alexander/Henrich, Christina/Hoffmann, Julia/Kirchbach, Cornelia/Kring, Jennifer/Lang, Lea Isabelle/Neumann, Theresa/Plicht, Sandra/Stix, Carolin/Völzmann, Berit/Wolckenhaar, Leonard/Zimmermann, Sören (Hrsg.), Verfassungen – ihre Rolle im Wandel der Zeit – 59. Assistententagung Öffentliches Recht Frankfurt am Main 2019, Baden-Baden 2019.

Dornis, Tim W., Personalisierte Vertragsanbahnung und Privatautonomie, ZfPW 8 (2022), S. 310–344.

Dörr, Dieter/Natt, Alexander, Suchmaschinen und Meinungsvielfalt – Ein Beitrag zum Einfluss von Suchmaschinen auf die demokratische Willensbildung, ZUM 58 (2014), S. 829–847.

Dörr, Dieter/Schuster, Simon, Suchmaschinen im Spannungsfeld zwischen Nutzung und Regulierung – Rechtliche Bestandsaufnahme und Grundstrukturen einer Neuregelung, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014, S. 262–323.

Drackert, Stefan, Die Risiken der Verarbeitung personenbezogener Daten – Eine Untersuchung zu den Grundlagen des Datenschutzrechts, Berlin 2014.

Drewes, Stefan, Dialogmarketing nach der DSGVO ohne Einwilligung der Betroffenen – Berechtigte Unternehmensinteressen bleiben maßgebliche Rechtsgrundlage, CR 32 (2016), S. 721–729.

Drexl, Josef, Bedrohung der Meinungsvielfalt durch Algorithmen, ZUM 61 (2017), S. 529–543.

Dreyer, Stephan, Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, S. 135–144.

Dreyer, Stephan/Schulz, Wolfgang, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme? – Potenziale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen, Bertelsmann Stiftung April 2018, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/BSt_DSGVOundADM_dt.pdf.

Drinóczi, Tímea, Legislative Process, in: Karpen, Ulrich/Xanthaki, Helen u.a. (Hrsg.), Legislation in Europe – A comprehensive guide for scholars and practitioners, Oxford/Portland 2017, S. 33–52.

Ducato, Rossana/Strowe, Alain, Limitations to Text and Data Mining and Consumer Empowerment – Making the Case for a Right to „Machine Legibility", ICC 50 (2019), S. 649–684.

Dudenredaktion, Profiling, Duden Online-Wörterbuch 2023, https://www.duden.de/rechtschreibung/Profiling.

Dudley, John J./Kristensson, Per Ola, A Review of User Interface Design for Interactive Machine Learning, ACM Transactions on Interactive Intelligent Systems 8 (2018), S. 1–37.

Duhigg, Charles, How Companies Learn Your Secrets, The New York Times Magazine 16.02.2012.

Dukino, Claudia, Was ist Künstliche Intelligenz? Eine Definition jenseits von Mythen und Moden, Fraunhofer-Gesellschaft, 14.3.2019, https://blog.iao.fraunhofer.de/was-ist-kuenstliche-intelligenz-eine-definition-jenseits-von-mythen-und-moden/.

Duprat, Jean-Pierre/Xanthaki, Helen, Legislative Drafting Techniques/Formal Legistics, in: Karpen, Ulrich/Xanthaki, Helen u.a. (Hrsg.), Legislation in Europe – A comprehensive guide for scholars and practitioners, Oxford/Portland 2017, S. 109–128.

Dushimimana, Bernard/Wambui, Yvonne/Lubega, Timothy/McSharry, Patrick E., Use of Machine Learning Techniques to Create a Credit Score Model for Airtime Loans, Journal of Risk and Financial Management 13 (2020), S. 180.

Dwork, Cynthia/Hardt, Moritz/Pitassi, Toniann/Reingold, Omer/Zemel, Rich, Fairness Through Awareness 20.04.2011, https://arxiv.org/pdf/1104.3913.

Eaton, Kit, Artificial Intelligence Makes the Phone a Personal Assistant, The New York Times 18.05.2016.

Ebers, Martin, Beeinflussung und Manipulation von Kunden durch Behavioral Microtargeting – Verhaltenssteuerung durch Algorithmen aus der Sicht des Zivilrechts, MMR 21 (2018), S. 423–428.

—, Standardisierung Künstlicher Intelligenz und KI-Verordnungsvorschlag, RDi 1 (2021), S. 588–597.

Ebers, Martin/Gamito, Marta Cantero (Hrsg.), Algorithmic Governance and Governance of Algorithms – Legal and Ethical Challenges, Cham 2021.

Ebers, Martin/Hoch, Veronica R. S./Rosenkranz, Frank/Ruschemeier, Hannah/Steinrötter, Björn, The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), Multidisciplinary Scientific Journal 4 (2021), S. 589–603.

Ebers, Martin/Hoch, Veronica R.S./Rosenkranz, Frank/Ruschemeier, Hannah/Steinrötter, Björn, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf – Eine kritische Bewertung durch Mitglieder der Robotics & AI Law Society (RAILS), RDi 1 (2021), S. 528–537.

Ebert, Andreas/Spiecker gen. Döhmann, Indra, Der Kommissionsentwurf für eine KI-Verordnung der EU – Die EU als Trendsetter weltweiter KI-Regulierung, NVwZ 40 (2021), S. 1188–1193.

Eckhardt, Jens, Wann ist ein IoT-Gerät datenschutzrelevant?, DuD 45 (2021), S. 107–113.

Eckhardt, Jens/Kramer, Rudi, EU-DSGVO – Diskussionspunkte aus der Praxis, DuD 37 (2013), S. 287–294.

Edelman, Gilad, Why Don't We Just Ban Targeted Advertising, Wired 22.3.2020.

Edwards, Lilian/Veale, Michael, Slave to the Algorithm? Why a Right to Explanationn is Probably Not the Remedy You are Looking for, SSRN Journal 2017.

Efroni, Zohar/Metzger, Jakob/Mischau, Lena/Schirmbeck, Marie, Privacy Icons – A Risk-Based Approach to Visualisation of Data Processing, EDPL 5 (2019), S. 352–366.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO – Datenschutz-Grundverordnung: Kommentar, 2. Aufl., München/Wien 2018 (zit. Ehmann/Selmayr, DS-GVO/*Bearbeiter*).

Eichel, Florian/Matt, Christian/Tovar Galván, Rorick, Chancen und Hürden von Entscheidungsunterstützungssystemen und künstlicher Intelligenz bei der Rechtsanwendung, Wirtschaftsinformatik & Management 12 (2020), S. 392–403.

Eichendorfer, Johannes, Privatheit im Internet als Vertrauensschutz – Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, Der Staat 55 (2016), S. 41–67.

Eidenmüller, Horst, The Rise of Robots and the Law of Humans, ZEuP 25 (2017), S. 765–777.

Eifert, Martin, Autonomie und Sozialität – Schwierigkeiten rechtlicher Konzeptionalisierung ihres Wechselspiels am Beispiel der informationellen Selbstbestimmung, in: Bumke, Christian/Röthel, Anne (Hrsg.), Autonomie im Recht – Gegenwartsdebatten über einen rechtlichen Grundbegriff, Tübingen 2017, S. 365–384.

Eifert, Martin/Hoffmann-Riem, Martin (Hrsg.), Innovationsfördernde Regulierung, Berlin 2009.

Eifert, Martin/Hoffmann-Riem, Wolfgang (Hrsg.), Innovationsverantwortung – Innovation und Recht III, Berlin 2009.

Eisenberger, Iris, Innovation im Recht, Wien 2016.

Eke, Christopher I./Norman, Azah A./Shuib, Liyana/Nweke, Henry F./Eke, Christopher Ifeanyi/Norman, Azah Anir/Nweke, Henry Friday, A Survey of User Profiling – State-of-the-Art, Challenges and Solutions, IEEE Access 7 (2019), S. 144907–144924.

Elliott, Christopher, Your Very Own Personal Air Fare, The New York Times 09.08.2005.

Emmenegger, Sigrid, Gesetzgebungskunst – Gute Gesetzgebung als Gegenstand einer legislativen Methodenbewegung in der Rechtswissenschaft um 1900 – Zur Geschichte der Gesetzgebungslehre, Tübingen 2020.

Enders, Peter, Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 50 (2018), S. 721–727.

Erdélyi, Olivia J./Goldsmith, Judy, Regulating Artificial Intelligence – Proposal for a Global Solution 22.05.2020, https://arxiv.org/pdf/2005.11072.

Ernst, Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 72 (2017), S. 1026–1036.

—, Artificial Intelligence and Autonomy – Self-Determination in the Age of Automated Systems, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 53–73.

Ernst, Hartmut/Schmidt, Jochen/Beneken, Gerd Hinrich, Grundkurs Informatik – Grundlagen und Konzepte für die erfolgreiche IT-Praxis – eine umfassende, praxisorientierte Einführung, 7. Aufl., Wiesbaden 2020.

Ernst, Stefan, Die Einwilligung nach der Datenschutzgrundverordnung – Anmerkungen zur Definition nach Art. 4 Nr. 11 DSGVO, ZD 7 (2017), S. 110–114.

Ertel, Wolfgang, Grundkurs Künstliche Intelligenz – Eine praxisorientierte Einführung, 5. Aufl., Wiesbaden/Heidelberg 2021.

Espinoza, Javier/Murgia, Madhumita, The four problems with Europe's vision of AI, Financial Times 26.02.2020.

Eubanks, Virginia, Automating inequality – How high-tech tools profile, police, and punish the poor, New York January 2018.

Eurobarometer, Special Eurobarometer 487a – March 2019 – „The General Data Protection Regulation" Report, Directorate-General for Justice and Consumers; Europäische Kommission März 2019, https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf.

Europäische Kommission, Vorschlag für Verordnung des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – KOM(2012) 11 endgültig, Europäische Kommission, Brüssel 25.01.2012.

—, Für eine florierende datengesteuerte Wirtschaft – Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Brüssel 02.07.2014.

—, An emerging offer of „personal information management services" – Current state of service offers and challenges Januar 2016, file:///C:/Users/jwoaa01/AppData/Local/Temp/pims_report_for_publication_40118.pdf.

—, Online-Plattformen im digitalen Binnenmarkt – Chancen und Herausforderungen für Europa, Brüssel 25.05.2016.

—, Künstliche Intelligenz für Europa, Brüssel 25.04.2018.

—, Künstliche Intelligenz für Europa, Europäische Kommission, Brüssel 25.04.2018, https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-237-F1-DE-MAIN-PART-1.PDF.

—, Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss – Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, Europäische Kommission, Brüssel 19.02.2020.

—, Weißbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, Europäische Kommission, Brüssel 19.2.2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

—, Leitlinien zur Transparenz des Rankings gemäß der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates 8.12.2020.

—, Begründung Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union – Gesetz über Künstliche Intelligenz, Brüssel 21.04.2021.

Europäischer Datenschutzausschuss, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 – Bestätigung der Leitlinien der Artikel 29 Datenschutzgruppe vom 03.10.2017, zuletzt überarbeitet und angenommen am 06.02.2018, Brüssel 25.05.2018, https://ec.europa.eu/newsroom/article29/redirection/document/54169.

—, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen – Version 2.0, Brüssel 08.10.2019, https://edpb.europa.eu/sites/

default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de_0.pdf.

—, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Brüssel 04.05.2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

—, Guidelines 8/2020 on the targeting of social media users – Version 1.0, Europäischer Datenschutzausschuss, Brüssel 02.09.2020, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

—, Opinion 1/2021 on the Proposal for a Digital Services Act 10.02.2021, https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

—, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR) 05.12.2022, https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf.

Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 18.06.2021, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

Europäischer Datenschutzbeauftragter, Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM) – Stellungnahme 9/2016 20.10.2016, https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_de.pdf.

Europäisches Parlament, Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI)) – 2013/C 33 E/10, Europäisches Parlament 6.7.2011, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52011IP0323&from=DE.

—, Zivilrechtliche Regelungen im Bereich Robotik – Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)), Europäisches Parlament, Straßburg 16.02.2018, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_DE.pdf.

Europarat, The protection of individuals with regard to automatic processing of personal data in the context of profiling – Recommendation CM/Rec(2010)13 and explanatory memorandum, Europarat, Straßburg 23.11.2013, https://rm.coe.int/16807096c3.

European Parliamentary Research Service, A governance framework for algorithmic accountability and transparency, Europäisches Parlament, Brüssel April 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf.

—, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence Juni 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

European Union Agency for Network and Information Security, Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics 2015, https://www.enisa.europa.eu/publications/big-data-protection/@@download/fullReport.

Extended Working Group on Ethics of Artificial Intelligence, Preliminary Study on the technical and legal aspects relating to the desirability of a standard-setting instrument on the ethics of artificial intelligence, World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), Paris 21.03.2019, https://unesdoc.unesco.org/ark:/48223/pf0000367422.

Fachforum Autonome Systeme im Hightech-Forum, Autonome Systeme – Chancen und Risiken für Wirtschaft, Wissenschaft und Gesellschaft, Deutsche Akademie der Technikwissenschaften; Hightech Forum, Berlin April 2017, https://www.acatech.de/publikation/fachforum-autonome-systeme-chancen-und-risiken-fuer-wirtschaft-wissenschaft-und-gesellschaft-abschlussbericht/download-pdf/?lang=de.

Fagganella, Daniel, Your Feed is All You: The Nuanced Art of Personalization at Facebook 18.08.2016, https://www.vice.com/en/article/d7ywxa/facebook-newsfeed-personalization-hussein-mehanna.

Fast, Ethan/Horvitz, E., Long-Term Trends in the Public Perception of Artificial Intelligence 02.12.2016, https://arxiv.org/abs/1609.04904.

Fawcett, Tom/Provost, Foster, Combining Data Mining and Machine Learning for Effective User Profiling, in: Simoudis, Evangelos/Han, Jiawei/Fayyad, Usama M. (Hrsg.), Proceedings / Second International Conference on Knowledge Discovery & Data Mining, Menlo Park, Calif. 1996, S. 8–13.

Federal Trade Commission, Data Brokers – A Call for Transparency and Accountability Mai 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Felzmann, Heike/Villaronga, Eduard Fosch/Lutz, Christoph/Tamò-Larrieux, Aurelia, Transparency you can trust – Transparency requirements for artificial intelligence between legal norms and contextual concerns, Big Data and Society 6 (2019), 1-14.

Finck, Michèle, Smart contracts as a form of solely automated processing under the GDPR, Int. Data Priv. Law 9 (2019), S. 78–94.

Finck, Michèle/Biega, Asia J., Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems, Technology and Regulation 2021, S. 44–61.

Finck, Michèle/Pallas, Frank, They who must not be identified – distinguishing personal from non-personal data under the GDPR, Int. Data Priv. Law 10 (2020), S. 11–36.

Flamme, Florian, Schutz der Meinungsvielfalt im digitalen Raum – Transparenzpflichten für Intermediäre im nationalen und europäischen Vergleich, MMR 24 (2021), S. 770–774.

Flaxman, Seth/Goel, Sharad/Rao, Justin M., Filter Bubbles, Echo Chambers, and Online News Consumption, Public Opinion Quarterly 80 (2016), S. 298–320.

Floridi, Luciano (Hrsg.), The Onlife Manifesto – Being Human in a Hyperconnected Era, Cham 2015.

—, Group Privacy: A Defence and an Interpretation, in: Taylor, Linnet/Floridi, Luciano/van der Sloot, Bart (Hrsg.), Group Privacy – New Challenges of Data Technologies, Cham 2017, S. 83–100.

Floridi, Luciano/Sanders, J. W., On the Morality of Artificial Agents, Minds and Machines 14 (2004), S. 349–379.

Forde, Aidan, The Conceptual Relationship between Privacy and Data Protection, Camb. L. Rev. 2016, S. 135–149.

Forgó, Nikolaus/Hänold, Stefanie/Schütze, Benjamin, The Principle of Purpose Limitation and Big Data, in: Corrales, Marcelo/Fenwick, Mark/Forgó, Nikolaus (Hrsg.), New Technology, Big Data and the Law, Singapore 2017, S. 17–42.

Formosa, Paul, Robot Autonomy vs. Human Autonomy – Social Robots, Artificial Intelligence (AI), and the Nature of Autonomy, Minds & Machines 31 (2021), S. 595–616.

Foucault, Michel, Überwachen und Strafen – Die Geburt des Gefängnisses, Frankfurt am Main 1977.

Frias-Martinez, E./Chen, S. Y./Liu, X., Survey of Data Mining Approaches to User Modeling for Adaptive Hypermedia, IEEE Transactions on Systems, Man and Cybernetics 36 (2006), S. 734–749.

Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017.

Friedewald, Michael/Vildjiounaite, Elena/Punie, Yves/Wright, David, Privacy, identity and security in ambient intelligence – A scenario analysis, Telematics and Informatics 24 (2007), S. 15–29.

Frischmann, Brett M./Selinger, Evan, Re-engineering humanity, Cambridge u.a. 2018.

Fuster, Gloria González/Gellert, Raphaël, The fundamental right of data protection in the European Union: in search of an uncharted right, Int. Rev. Law Comput. Technol. 26 (2012), S. 73–82.

Galetzka, Christian, Web-Analytics/Retargeting und automatisierte Einzelfallentscheidung, K&R 18 (2018), S. 675–680.

Galli, Federico, Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD, in: Ebers, Martin/Gamito, Marta Cantero (Hrsg.), Algorithmic Governance and Governance of Algorithms – Legal and Ethical Challenges, Cham 2021, S. 109–135.

Gams, Matjaz/Gjoreski, Martin (Hrsg.), Artificial Intelligence and Ambient Intelligence, Basel 2021.

Gams, Matjaz/Gu, Irene Yu-Hua/Härmä, Aki/Muñoz, Andrés/Tam, Vincent, Artificial intelligence and ambient intelligence, JAISE 11 (2019), S. 71–86.

—, Artificial intelligence and ambient intelligence, JAISE 11 (2019), S. 71–86.

Gao, Chongming/Lei, Wenqiang/Chen, Jiawei/Wang, Shiqi/He, Xiangnan/Li, Shijun/Li, Biao/Zhang, Yuan/Jiang, Peng, CIRS: Bursting Filter Bubbles by Counterfactual Interactive Recommender System 4.4.2022, https://arxiv.org/pdf/2204.01266.

Garante per la protezione dei dati personali, Provvedimento del 30 marzo 2023 – n. 112 30.03.2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

—, Comunicato del 31 marzo 2023 31.03.2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847.

—, Provvedimento dell‘ 11 aprile 2023 11.04.2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702.

Gärner, Christoph, Bekämpfung von Fake News, in: Grabenwarter, Christoph/Holoubek, Michael/Leitl-Staudinger, Barbara (Hrsg.), Regulierung von Kommunikationsplattformen, Wien, Baden-Baden 2022, S. 89–112.

Gasson, Mark/Browne, Will, Reply: Towards a Data Mining de Facto Standard, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 58–64.

Gausling, Tina, Künstliche Intelligenz im digitalen Marketing – Datenschutzrechtliche Bewertung KI-gestützter Kommunikations-Tools und Profiling-Maßnahmen, ZD 9 (2019), S. 335–341.

—, Datenschutzrechtliche Informationspflichten – Kapitel 8.3, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, S. 379–390.

Geese, Alexandra, Why the DSA could save us from the rise of authoritarian regimes, Verfassungsblog 08.11.2022, ttps://verfassungsblog.de/dsa-authoritarianism/.

Gellert, Raphaël, We Have Always Managed Risks in Data Protection Law, EDPL 2 (2016), 481-492.

—, Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies, Int. Data Priv. Law 11 (2021), S. 196–208.

—, The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?, Journal of Ethics and Legal Technologies 3 (2021), S. 15–33.

Gellert, Raphaël/Gutwirth, Serge, The legal construction of privacy and data protection, CLSR 29 (2013), S. 522–530.

Geminn, Christian, Die Regulierung Künstlicher Intelligenz – Anmerkungen zum Entwurf eines Artificial Intelligence Act, ZD 11 (2021), S. 354–359.

Geminn, Christian/Roßnagel, Alexander, Datenschutz-Grundverordnung verbessern – Änderungsvorschläge aus Verbrauchersicht, Baden-Baden 2020.

Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2023 (zit. Gierschmann/Schlender/Stenzel/Veil, DS-GVO/*Bearbeiter*).

Giesbrecht, David, This is how Netflix's top-secret recommendation system works, Wired 22.08.2017.

Gigerenzer, Gerd, Technik braucht Menschen, die sie beherrschen, Spektrum 12.11.2015, https://www.spektrum.de/kolumne/technik-braucht-menschen-die-sie-beherrschen/1375950.

Glatzner, Florian, Profilbildung und algorithmenbasierte Entscheidungen, DuD 44 (2020), S. 312–315.

Gleixner, Alexander, Personalisierte Preise im Onlinehandel und Europas „New Deal for Consumers", VuR 35 (2020), S. 417–421.

Gleß, Sabine/Seelmann, Kurt (Hrsg.), Intelligente Agenten und das Recht, Baden-Baden 2016.

Goddard, Kate/Roudsari, Abdul/Wyatt, Jeremy C., Automation bias – a systematic review of frequency, effect mediators, and mitigators, Journal of the American Medical Informatics Association 19 (2012), S. 121–127.

Godoy, Daniela/Amandi, Analia, User profiling in personal information agents: a survey, Knowledge Engineering Review 20 (2005), S. 329–361.

Gola, Peter/Heckmann, Dirk/Brand, Thimo/Brandenburg, Anne/Braun, Frank/Bronner, Pascal (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz – Kommentar, 3. Aufl., München 2022 (zit. Gola, DS-GVO/*Bearbeiter*).

Goldfarb, Avi/Tucker, Catherine E., Privacy Regulation and Online Advertising, Management Science 57 (2011), S. 57–71.

Goldsteen, Abigail/Ezov, Gilad/Shmelkin, Ron/Moffie, Micha/Farkash, Ariel, Anonymizing Machine Learning Models 26.7.2020, https://arxiv.org/pdf/2007.13086.

Golla, Sebastian, In Würde vor Ampel und Algorithmus – Verfassungsrecht im technologischen Wandel, in: Donath, Philipp B./Bretthauer, Sebastian u.a. (Hrsg.), Verfassungen – ihre Rolle im Wandel der Zeit – 59. Assistententagung Öffentliches Recht Frankfurt am Main 2019, Baden-Baden 2019, S. 183–202.

Golland, Alexander, Datenschutzrechtliche Fragen personalisierter Preise – Herausforderungen von Algorithmen im Schnittbereich von Ethik, Ökonomie und Datenschutz, CR 36 (2020), S. 186–194.

González Fuster, Gloria, The Emergence of Personal Data Protection As a Fundamental Right of the EU, Cham 2014.

González Fuster, Gloria/Gutwirth, Serge, Opening up personal data protection – A conceptual controversy, CLSR 29 (2013), S. 531–539.

Goodfellow, Ian/Bengio, Yoshua/Courville, Aaron, Deep learning, Cambridge (Massachusetts)/London (Vereintes Königreich) 2016.

Goodman, Bryce/Flaxman, Seth, European Union Regulations on Algorithmic Decision-Making and a „Right to Explanation", AI Magazine 38 (2017), S. 50–57.

Görz, Günther/Braun, Tanya/Schmid, Ute, Einleitung, in: dies. (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 1–26.

Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021.

Grabenwarter, Christoph/Breuer, Marten/Bungenberg, Marc (Hrsg.), Europäischer Grundrechteschutz – Zugleich Band 2 der Enzyklopädie Europarecht, 2. Aufl., Baden-Baden u.a. 2022.

Grabenwarter, Christoph/Holoubek, Michael/Leitl-Staudinger, Barbara (Hrsg.), Regulierung von Kommunikationsplattformen, Wien/Baden-Baden 2022.

Grafanaki, Sofia, Drowning in Big Data – Abundance of Choice, Scarcity of Attention and the Personalization Trap, a Case for Regulation, Rich J. L. Techn. 24, S. 1–66.

Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 68 (2017), S. 585–636.

Guggenberger, Leonidas, Einsatz künstlicher Intelligenz in der Verwaltung, NVwZ 38 (2018), S. 844–850.

Gurkaynak, Gonenc/Yilmaz, Ilay/Haksever, Gunes, Stifling artificial intelligence: Human perils, CLSR 32 (2016), S. 749–758.

Gutwirth, Serge/Hert, Paul de, Regulating Profiling in a Democratic Constitutional State, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 271–293.

Gutwirth, Serge/Leenes, Ronald/Hert, Paul de (Hrsg.), Reloading data protection – Multidisciplinary insights and contemporary challenges, New York 2014.

Gwiasda, Benjamin/Greve, Ruth/Kemper, Thomas/Moir, Joshua/Müller, Sabrina/Schönberger, Arno/Stöcker, Sebastian/Wagner, Julia/Wolff, Lydia (Hrsg.), Der digitalisierte Staat – Chancen und Herausforderungen für den modernen Staat, Baden-Baden 2020.

Haase, Martin Sebastian, Datenschutzrechtliche Fragen des Personenbezugs – Eine Untersuchung des sachlichen Anwendungsbereiches des deutschen Datenschutzrechts und seiner europarechtlichen Bezüge, Tübingen 2015.

Habermas, Jürgen, Faktizität und Geltung – Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats, 5. Aufl., Frankfurt am Main 1997.

Hackenberg, Wolfgang, Big Data und Datenschutz – 15.2, in: Hoeren, Thomas/Sieber, Ulrich u.a. (Hrsg.), Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, 58. Aufl., München 2022.

Hacker, Philipp, Teaching fairness to artificial Intelligence – Existing and novel strategies against algorithmic discrimination under EU law, Common Mark. Law Rev 55 (2018), S. 1143–1186.

—, Ein Rechtsrahmen für KI-Trainingsdaten, ZGE 12 (2020), S. 239–271.

—, Europäische und nationale Regulierung von Künstlicher Intelligenz, NJW 73 (2020), S. 2124–2147.

Hagendorff, Thilo, The Ethics of AI Ethics: An Evaluation of Guidelines, Minds and Machines 30 (2020), S. 99–120.

Hahn, Isabel, Purpose Limitation in the Time of Data Power – Is There a Way Forward?, EDPL 7 (2021), S. 31–44.

Hajek, Stefan, So funktioniert die Erfolgsformel von Spotify, WirtschaftsWoche 03.04.2018.

Halberstam, Yosh/Knight, Brian, Homophily, group size, and the diffusion of political information in social networks: Evidence from Twitter, J. Public Econ. 143 (2016), S. 73–88.

Hannig, Theresa, Pantopia – Roman, Frankfurt März 2022.

Hanson, Jon D./Kysar, Douglas A., Taking Behavioralism Seriously – Some Evidence of Market Manipulation, Harv. L. Rev. 112 (1999), S. 1420–1572.

Hardy, Quentin, Just the Facts. Yes, All of Them., The New York Times 24.03.2012.

Härtel, Ines, Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren, Landes- und Kommunalverfassung 29 (2019), S. 49–60.

Härting, Ines, Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren, Landes- und Kommunalverfassung 29 (2019), 49-60.

Härting, Niko, Profiling: Vorschläge für eine intelligente Regulierung – Was aus der Zweistufigkeit des Profiling für die Regelung des nicht-öffentlichen Datenschutzbereichs folgt, CR 4 (2014), S. 528–536.

Hartl, Korbinian, Suchmaschinen, Algorithmen und Meinungsmacht – Eine verfassungs- und einfachrechtliche Betrachtung, Wiesbaden 2017.

Häuselmann, Andreas, The ECJ's First Landmark Case on Automated Decision-Making – a Report from the Oral Hearing before the First Chamber, 29.02.2023, https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber.

Heckelmann, Martin, Zulässigkeit und Handhabung von Smart Contracts, NJW 71 (2018), S. 504–510.

Heiden, Uwe an der (Hrsg.), Hat der Mensch einen freien Willen? – Die Antworten der großen Philosophen, Stuttgart 2008.

Heinze, Martin/Fuchs, Thomas/Reichies, Friedel M. (Hrsg.), Willensfreiheit – eine Illusion? – Naturalismus und Psychiatrie, Berlin/Lengerich 2006.

Heiss, Stefan, Artificial Intelligence Meets European Union Law – The EU Proposals of April 2021 and October 2020, EuCML 10 (2021), S. 252–257.

Helberger, Natali, Diversity by Design, Journal of Information Policy 1 (2011), S. 441–469.

Helberger, Natali/van Drunen, Max/Vrijenhoek, Sanne/Möller, Juditz, Regulation of news recommenders in the Digital Services Act – empowering David against the Very Large Online Goliath 26.2.2021, https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large.

Helbing, Dirk, „Big Nudging" – zur Problemlösung wenig geeignet – Big Data zur Verhaltenssteuerung?, Spektrum der Wissenschaft 12.11.2015.

Helfrich, Marcus, Kreditscoring und Scorewertbildung der SCHUFA – Datenschutzrechtliche Zulässigkeit im Rahmen der praktischen Anwendungen, Baden-Baden 2010.

—, Scoring reloaded?, ZD 3 (2013), S. 473–474.

Heller, Christian, Post-privacy – Prima leben ohne Privatsphäre, München 2011.

Heller, Martin, Was ist Deep Learning?, Computerwoche 27.08.2022.

Hengst, Floris/Grua, Eoin Martino/el Hassouni, Ali/Hoogendoorn, Mark, Reinforcement learning for personalization – A systematic literature review, DS 2020, S. 1–41.

Hennemann, Moritz, Personalisierte Medienangebote im Datenschutz- und Vertragsrecht, ZUM 61 (2017), S. 544–552.

—, Die personalisierte Vertragsanbahnung, AcP 219 (2019), S. 818–854.

—, Artificial Intelligence and Competition Law, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 361–388.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung 2015.

—, Die Regulierung der prädiktiven Analytik: eine juristisch-verhaltenswissenschaftliche Skizze, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, S. 99–116.

—, Artificial Intelligence and Administrative Decisions Under Uncertainty, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 199–223.

Hernández Ramos, Mario/Heydt, Volker, Legislative Language and Style, in: Karpen, Ulrich/Xanthaki, Helen u.a. (Hrsg.), Legislation in Europe – A comprehensive guide for scholars and practitioners, Oxford/Portland 2017, S. 129–144.

Herrmann, Stefan, Völkerrechtliche Jurisdiktionsgrundlagen für den Datenschutz im Netz, Tübingen 2020.

Hert, Paul de/*Gutwirth, Serge*, Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in: Claes/Duff/Gutwirth (Hrsg.), Privacy and the criminal law, Antwerpen 2006, S. 61–104.

Hert, Paul de/*Gutwirth, Serge/Poullet, Yves* (Hrsg.), Reinventing Data Protection?, Dordrecht 2009.

Hess, Amanda, How to Escape Your Political Bubble for a Clearer View, The New York Times 03.03.2017.

High-Level Expert Group on Artificial Intelligence, A defintion of AI: Main capabilites and disciplines – Definition developed for the purpose of the AI HLEG's deliverables, Europäische Kommission, Brüssel 8. April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.

—, Ethics Guidelines for Trustworthy AI, Europäische Kommission, Brüssel 8.4.2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Hildebrandt, Mireille, Profiling: From Data to Knowledge – The challenges of a crucial technology, DuD 30 (2006), S. 548–552.

—, Defining Profiling: A New Type of Knowledge?, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 17–29.

—, Profiling and the Identity of the European Citizen, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 303–326.

—, Profiling and the rule of law, Identity in the Information Society IDIS 1 (2008), S. 55–70.

—, The Dawn of a Critical Transparency Right for the Profiling Era, in: Bus, Jacques (Hrsg.), Digital enlightenment yearbook 2012, Amsterdam, Washington, D.C 2012, S. 41–56.

—, Smart technologies and the end(s) of law – Novel entanglements of law and technology, Cheltenham/Northampton (Massachusetts) 2016.

—, Code-driven Law: Freezing the Future and Scaling the Past, in: Deakin, Simon F./Markou, Christopher (Hrsg.), Is law computable? – Critical perspectives on law and artificial intelligence, Oxford u.a. 2020.

Hildebrandt, Mireille/Gutwirth, Serge, Concise Conclusions: Citizens out of Control, in: dies. (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 365–368.

— (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008.

Hildebrandt, Mireille/Koops, Bert-Jaap, The Challenges of Ambient Lawand Legal Protection in the Profiling Era, The Modern Law Review 73 (2010), S. 428–460.

Hildebrandt, Mireille/Tielemans, Laura, Data protection by design and technology neutral law, CLSR 29 (2013), S. 509–521.

Hildebrandt, Mireille/Vries, Katja de (Hrsg.), Privacy, due process and the computational turn – The philosophy of law meets the philosophy of technology, Abingdon 2013.

Hilgendorf, Eric, Zur Steuerung technischer Entwicklungen durch Recht und Moral – am Beispiel der Informationstechnik in der Medizin, in: Spiecker gen. Döhmann, Indra/Wallrabenstein, Astrid (Hrsg.), IT-Entwicklungen im Gesundheitswesen: Herausforderungen und Chancen, Frankfurt am Main u.a. 2016, S. 75–88.

Hill, Hermann, Scientific Regulation – Automatische Verhaltenssteuerung durch Daten und Algorithmen, in: Hill, Hermann/Schliesky, Utz (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, Baden-Baden 2015, S. 267–287.

Hill, Hermann/Schliesky, Utz (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, Baden-Baden 2015.

Hochrangige Expertengruppe für künstliche Intelligenz, Ethik-Leitlinien für eine vertrauenswürdige Künstliche Intelligenz, Europäische Kommission, Brüssel 10. April 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Hoeren, Thomas/Niehoff, Maurice, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, RW 9 (2018), S. 47–66.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd/Albrecht, Florian/Altenhain, Karsten (Hrsg.), Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, 58. Aufl., München 2022.

Hof, Hagen/Wegenroth, Ulrich (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2. Aufl., Berlin 2010.

Hof, Wegenroth Hg,

Hoffmann, Hanna, Regulierung der Künstlichen Intelligenz, K&R 20 (2021), S. 369–374.

Hoffmann, Raphael, Profilbildung unter der DSGVO – Digitale Persönlichkeitsprofile im Spannungsfeld zwischen Unternehmensinteresse und Persönlichkeitsrecht, Baden-Baden 2020.

Hoffmann-Riem, Wolfgang, Innovationen durch Recht und im Recht, in: Schulte, Martin/Di Fabio, Udo (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis, Heidelberg 1997, S. 3–32.

—, Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 123 (1998), S. 514–540.

—, Vorüberlegungen zur rechtswissenschaftlichen Innovationsforschung, in: Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.), Rechtswissenschaftliche Innovationsforschung – Grundlagen, Forschungsansätze, Gegenstandsbereiche, Baden-Baden 1998, S. 11–28.

—, Innovationssteuerung durch die Verwaltung – Rahmenbedingungen und Beispiele, Die Verwaltung 33 (2000), S. 155–182.

—, Innovationsoffenheit und Innovationsverantwortung durch Recht – Aufgaben rechtswissenschaftlicher Innovationsforschung, AöR 131 (2006), S. 255–277.

—, Recht als Instrument der Innovationsoffenheit und der Innovationsverantwortung, in: Hof, Hagen/Wegenroth, Ulrich (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2. Aufl., Berlin 2010, S. 387–399.

—, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2016), S. 1–42.

— (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018.

—, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: ders. (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, S. 11–80.

—, Artificial Intelligence as a Challenge for Law and Regulation, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 1–32.

Hoffmann-Riem, Wolfgang/Brandt, Edmund/Schuler-Harms, Margarete (Hrsg.), Offene Rechtswissenschaft – Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010.

Hoffmann-Riem, Wolfgang/Fritzsche, Saskia, Innovationsverantwortung – zur Einleitung, in: Eifert, Martin/Hoffmann-Riem, Wolfgang (Hrsg.), Innovationsverantwortung – Innovation und Recht III, Berlin 2009, S. 12–43.

Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts – Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl., München 2012.

Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.), Rechtswissenschaftliche Innovationsforschung – Grundlagen, Forschungsansätze, Gegenstandsbereiche, Baden-Baden 1998.

Hofmann, Franz, Der maßgeschneiderte Preis – Dynamische und individuelle Preise aus lauterkeitsrechtlicher Sicht, WiRO 62 (2016), S. 1074–1082.

Hofmann, Franz/Freiling, Felix, Personalisierte Preise und das Datenschutzrecht – Anforderungen an die datenschutzrechtliche Einwilligung, ZD 10 (2020), S. 331–335.

Hopt, Klaus J. (Hrsg.), Corporate governance in context – Corporations, states, and markets in Europe, Japan, and the US, Oxford 2005.

Horn, Nikolai/Riechert, Anne/Müller, Christian, Neue Wege bei der Einwilligung im Datenschutz – Technische, rechtliche und ökonomische Herausforderungen, Leipzig 2017, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_Studie_Neue_Wege_zur_Einwilligung_final.pdf.

Hornung, Gerrit, Erosion traditioneller Prinzipien des Datenschutzrechts durch Big Data, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, 81-98.

—, Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything", in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden/Heidelberg 2018, S. 315–336.

Hornung, Gerrit/Wagner, Bernd, Der schleichende Personenbezug – Die Zwickmühle der Re-Identifizierbarkeit in Zeiten von Big Data und Ubiquitous Computing, CR 2019, S. 565–574.

Huang, Ming-Hui/Rust, Roland T., A strategic framework for artificial intelligence in marketing, Journal of the Academy of Marketing Science 49 (2021), S. 30–50.

Humerick, Matthew, Taking AI Personally – How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, Santa Clara High Technology Law Review 34 (2018), S. 393–418.

Ignatidou, Sophia, AI-driven Personalization in Digital Media – Political and Societal Implications, The Royal Institute of International Affairs, International Security Department, London Dezember 2019, https://www.chathamhouse.org/sites/default/files/021219%20AI-driven%20Personalization%20in%20Digital%20Media%20final%20WEB.pdf.

Information Comissioner's Office, Big data, artificial intelligence, machine learning and data protection 1.3.2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

—, Big data, artificial intelligence, machine learning and data protection 01.03.2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

Ingold, Albert, Meinungsmacht des Netzes – Macht im Netz II: Rechtliche Herausforderungen aktueller Regulierungsvorstellungen für digitalisierte Öffentlichkeiten, MMR 23 (2020), S. 82–86.

Introna, Lucas D./Nissenbaum, Helen, Shaping the Web: Why the Politics of Search Engines Matters, The Information Society 16 (2000), S. 169–185.

Iphofen, Ron/Kritikos, Mihalis, Regulating artificial intelligence and robotics: ethics by design in a digital society, Contemporary Social Science 2019, S. 1–15.

Isensee, Josef, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates. Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982 – erweiterte Fassung, Berlin 1983.

Islam, Sheikh Rabiul/Eberle, William/Ghafoor, Sheikh Khaled/Ahmed, Mohiuddin, Explainable Artificial Intelligence Approaches: A Survey 23.01.2021, https://arxiv.org/pdf/2101.09429.

Jakobi, Timo/Stevens, Gunnar/Seufert, Anna-Magdalena/Becker, Max/Grafenstein, Maximilian von, Web Tracking Under the New Data Protection Law: Design Potentials at the Intersection of Jurisprudence and HCI, i-com 19 (2020), S. 31–45.

Jamison, Mark, European Commission's AI Regulations Would Limit Possibility, American Enterprise Institute, 27.02.2020, https://www.aei.org/articles/european-commissions-ai-regulations-would-limit-possibility.

Janic, Milena/Wijbenga, Jan Pieter/Veugen, Thijs, Transparency Enhancing Tools (TETs): An Overview, in: Bella, Giampaolo (Hrsg.), 2013 Third Workshop on Socio-Technical Aspects in Security and Trust (STAST), Piscataway 2013, S. 18–25.

Janssen, Heleen/Cobbe, Jennifer/Singh, Jatinder, Personal information management systems: a user-centric privacy utopia?, Internet Policy Rev. 9 (2020), S. 1–24.

Japanisch-Deutsches Zentrum (Hrsg.), Mensch-Roboter-Interaktionen aus interkultureller Perspektive – Japan und Deutschland im Vergleich, Berlin 2012.

Jaquet-Chiffelle, David-Olivier, Reply: Direct and Indirect Profiling in the Light of Virtual Persons, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 34–43.

Jarass, Hans D. (Hrsg.), Charta der Grundrechte der Europäischen Union – Unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK: Kommentar, 4. Aufl., München 2021 (zit. Jarass, GRCh/*Bearbeiter*).

Jarovsky, Luiza, Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs), EDPL 4 (2018), S. 447–458.

Jensen, Carlos/Potts, Colin/Jensen, Christian, Privacy practices of Internet users: Self-reports versus observed behavior, Int. J. Hum. Comput. 63 (2005), S. 203–227.

Jezic, Gordan/Chen-Burger, Yun-Heh Jessica/Kusek, Mario (Hrsg.), Agents and Multi-agent Systems: Technologies and Applications 2019 – 13th KES International Conference, KES-AMSTA-2019 St. Julians, Malta, June 2019 Proceedings 2020.

Jia, Jian/Jin, Ginger Zhe/Wagman, Liad, The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment, Marketing Science 40 (2021), S. 661–684.

Julián, Vicente/Carneiro, João/Alonso, Ricardo S./Chamoso, Pablo/Novais, Paulo (Hrsg.), Ambient Intelligence—Software and Applications—13th International Symposium on Ambient Intelligence, Cham 2023.

Jung, Heike/Jung-Müller-Dietz-Neumann (Hrsg.), Recht und Moral – Beiträge zu einer Standortbestimmung, Baden-Baden 1991.

Jürgens, Pascal/Stark, Birgit/Magin, Melanie, Gefangen in der Filter Bubble? – Search Engine Bias und Personalisierungsprozesse bei Suchmaschinen, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014, S. 98–135.

Just, N./Latzer, M., Governance by algorithms – reality construction by algorithmic selection on the Internet, Media, Culture & Society 39 (2017), S. 238–258.

Käde, Lisa/Maltzan, Stephanie von, Die Erklärbarkeit von Künstlicher Intelligenz (KI) – Entmystifizierung der Black Box und Chancen für das Recht, CR 36 (2020), S. 66–72.

Kalbhenn, Jan Christopher, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, ZUM 65 (2021), S. 663–674.

Kamarinou, Dimitra/Millard, Christopher/Singh, Jatinder, Machine Learning with Personal Data, Queen Mary School of Law 7.11.2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811.

Kaminski, Margot E., The Right to Explanation, Explained, BTLJ 34 (2019), S. 189–218.

Kamp, Meike/Körffer, Barbara/Meints, Martin, Profiling of Customers and Consumers – Consumer Loyalty Programms and Scoring Practices, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 201–211.

Kamp, Meike/Rost, Martin, Kritik an der Einwilligung – Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen., DuD 37 (2013), S. 80–83.

Kamps, Michael/Schneider, Florian, Transparenz als Herausforderung: Die Informations- und Meldepflichten der DSGVO aus Unternehmenssicht, K&R 19 (2020), S. 24–29.

Kane, Robert (Hrsg.), The Oxford handbook of free will, 2. Aufl., Oxford/New York 2011.

Kanoje, Sumitkumar/Girase, Sheetal/Mukhopadhyay, Debajyoti, User Profiling Trends, Techniques and Applications, IJAFRC 2014.

Karg, Moritz, Die Renaissance des Verbotsprinzips im Datenschutz, DuD 37 (2013), S. 75–79.

Karpen, Ulrich, Gesetzgebungs-, Verwaltungs- und Rechtsprechungslehre – Beiträge zur Entwicklung einer Regelungstheorie, Baden-Baden 1989.

—, Zum Stand der Gesetzgebungswissenschaft in Europa, in: Schreckenberger, Waldemar (Hrsg.), Grundfragen der Gesetzgebungslehre – Aktualisierte Vorträge eines Seminars zur Gesetzgebungslehre (1996) an der Deutschen Hochschule für Verwaltungswissenschaften Speyer, Berlin 2000, S. 11–31.

—, Gesetzgebungslehre – neu evaluiert – Legistics—freshly evaluated, Baden-Baden 2006.

—, Introduction, in: Karpen, Ulrich/Xanthaki, Helen u.a. (Hrsg.), Legislation in Europe – A comprehensive guide for scholars and practitioners, Oxford/Portland 2017, 1-16.

Karpen, Ulrich/Xanthaki, Helen/Mader, Luzius/Voermans, Wim/Cormacain, Ronan (Hrsg.), Legislation in Europe – A comprehensive guide for scholars and practitioners, Oxford/Portland 2017.

Kaulartz, Markus, Personenbezug von KI-Modellen – Kapitel 8.9, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, S. 462–477.

Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020.

Keller, Daphne, The EU's new Digital Services Act and the Rest of the World, Verfassungsblog 07.11.2022, https://verfassungsblog.de/dsa-rest-of-world/.

Kellner, Anna, Die Regulierung der Meinungsmacht von Internetintermediären, Baden-Baden 2019.

Kennedy, K./Mac Namee, B./Delany, S. J./O'Sullivan, M./Watson, N., A window of opportunity: Assessing behavioural scoring, Expert Systems with Applications 40 (2013), S. 1372–1380.

Kerkmann, Christof, Künstliche Intelligenz: Wirtschaft warnt vor „massiven Einschränkungen" durch AI Act, Handelsblatt 6.1.2022.

Kersten, Jens, Die Konsistenz des Menschlichen. Post- und transhumane Dimensionen des Autonomieverständnisses, in: Bumke, Christian/Röthel, Anne (Hrsg.), Autonomie im Recht – Gegenwartsdebatten über einen rechtlichen Grundbegriff, Tübingen 2017, S. 315–352.

Kersting, Norbert/Mehl, Max, Echokammern im deutschen Bundestagswahlkampf 2017. – Die ambivalente Rolle der Prominenz, ZParl 49 (2018), S. 586–602.

Kert, Erki, Facebook can now be your only source of credit information, 10.01.2014, https://www.bigdatascoring.com/another-breakthrough-in-social-media-credit-scoring.

Kettner, Sara Elisa/Thorun, Christian/Spindler, Gerald, Innovatives Datenschutz-Einwilligungsmanagement – Abschlussbericht, ConPolicy Institut für Verbraucherpolitik, Berlin 5.9.2020, https://cortina-consult.com/wp-content/uploads/090620_Datenschutz_Einwilligung_compressed.pdf.

Kim, Kuinam/Joukov, Nikolai (Hrsg.), Information Science and Applications 2017 – ICISA 2017, Singapore 2017.

Kipker, Dennis-Kenji/Birreck, Piet/Niewöhner, Mario/Schnorr, Timm, Rechtliche und technische Rahmenbedingungen der „Smart Contracts" – Eine zivilrechtliche Betrachtung, MMR 23 (2020), S. 509–513.

Klar, Manuel, Die extraterritoriale Wirkung des neuen europäischen Datenschutzrechts, DuD 41 (2017), S. 533–537.

—, Künstliche Intelligenz und Big Data – algorithmenbasierte Systeme und Datenschutz im Geschäft mit Kunden, BB 74 (2019), S. 2243–2252.

Kleine, Nadine, Die historische Ambivalenz von Technikpessimismus und Technikoptimismus – Zur gesellschaftlichen Technikbewertung in der BRD, in: Zoglauer, Thomas/Weber, Karsten/Friesen, Hans (Hrsg.), Technik als Motor der Modernisierung, Freiburg, München 2018, S. 57–80.

Kloepfer, Michael/Franzius, Claudio, Technik und Recht im wechselseitigen Werden – Kommunikationsrecht in der Technikgeschichte, Berlin 2002.

Kluth, Winfried, Entwicklungen und Perspektiven der Gesetzgebungswissenschaft, in: Kluth, Winfried/Krings, Günter u.a. (Hrsg.), Gesetzgebung – Rechtsetzung durch Parlamente und Verwaltungen sowie ihre gerichtliche Kontrolle, Heidelberg u.a. 2014, S. 3–39.

Kluth, Winfried/Krings, Günter/Augsberg, Steffen/Burkiczak, Christian/Huber, Peter M. (Hrsg.), Gesetzgebung – Rechtsetzung durch Parlamente und Verwaltungen sowie ihre gerichtliche Kontrolle, Heidelberg u.a. 2014.

Knote, Robin/Janson, Andreas/Eigenbrod, Laura/Söllner, Matthias, The What and How of Smart Personal Assistants – Principles and Application Domains for IS Research, Multikonferenz Wirtschaftsinformatik 2018 06.03.2018, https://www.researchgate.net/profile/Andreas-Janson/publication/324497089_The_What_and_How_of_Smart_Personal

_Assistants_Principles_and_Application_Domains_for_IS_Research/links/5ad0788fa6fdcc878412197f/The-What-and-How-of-Smart-Personal-Assistants-Principles-and-Application-Domains-for-IS-Research.pdf?origin=publication_detail.

Kokott, Juliane/Sobotta, Christoph, The distinction between privacy and data protection in the jurisprudence of the CJEUand the ECtHR, Int. Data Priv. Law 3 (2013), S. 222–228.

Kolany-Raiser, Barbara/Heil, Reinhard/Orwat, Carsten/Hoeren, Thomas (Hrsg.), Big Data und Gesellschaft – Eine multidisziplinäre Annäherung, Wiesbaden 2018.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 20.12.2021, https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf.

Koops, Bert-Jaap, Reply: Some Reflections on Profiling, Power Shifts and Protection Paradigms, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 326–337.

—, The trouble with European data protection law, Int. Data Priv. Law 4 (2014), S. 250–261.

Koreng, Ansgar, Netzneutralität und Meinungsmonopole, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014, S. 245–261.

Kosta, Genia, Social credits and security: embracing the world of ratings, Kaspersky Daily, https:/kaspersky/www.kaspersky.com/blog/social-credits-and-security.

Kranzberg, Melvin, Technology and History: „Kranzberg's Laws", Technology and Culture 27 (1986), S. 544.

Kraus, Matthias/Ludwig, Bernd/Minker, Wolfgang/Wagner, Nicolas, Assistenzsysteme, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 859–906.

Kreile, Johannes/Thalhofer, Thomas, Suchmaschinen und Pluralitätsanforderungen – Ist ohne gesetzliche Regelung der Suchmaschinen der Pluralismus und die Meinungsvielfalt in Gefahr?, ZUM 58 (2014), S. 629–638.

Kreitz, Christoph/Frank, Mario, Automatische Inferenz, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 143–188.

Kreye, Andrian/Hunger, Felix, Künstliche Intelligenz: die Entschlüsselung unserer Gefühle, SZ 22.01.2023.

Kroll, Joshua A./Huey, Joanna/Barocas, Solon/Felten, Edward W./Reidenberg, Joel R./Robinson, David G./Yu, Harlan, Accountable Algorithms, University of Pennsylvania Law Review 165 (2017), S. 633–705.

Krönke, Christoph, Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 55 (2016), S. 319–351.

—, Artificial Intelligence and Social Media, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 145–173.

Kruse, Johannes, Neurojurisprudenz – Potenziale und Perspektiven, NJW 73 (2020), S. 137–139.

—, Neurowissenschaft der Grundrechte – Potenziale einer Neurojurisprudenz im Völker- und Verfassungsrecht, NJW 75 (2022), S. 2091–2092.

Kugelmann, Dieter, Datenfinanzierte Internetangebote – Regelungs- und Schutzmechanismen der DSGVO, DuD 40 (2016), S. 566–570.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung BDSG – Kommentar, 3. Aufl., München 2020 (zit. Kühling/Buchner, DS-GVO, BDSG/*Bearbeiter*).

Kumkar, Lea Katharina/Roth-Isigkeit, David, Erklärungspflichten bei automatisierten Datenverarbeitungen nach der DSGVO, JZ 75 (2020), S. 277–286.

Kunaver, Matevž/Požrl, Tomaž, Diversity in recommender systems – A survey, Knowledge-Based Systems 123 (2017), S. 154–162.

Kuner, Christopher/Bygrave, Lee A./Docksey, Christopher (Hrsg.), The EU General Data Protection Regulation (GDPR) – A Commentary, Oxford, UK 2020 (zit. Kuner/Bygrave/Docksey, GDPR/*Bearbeiter*).

Kuner, Lisa, Und raus bist du! – KI im Bewerbungsprozess, FAZ 09.08.2021.

Kurzweil, Ray (Hrsg.), The age of intelligent machines, Cambridge (Massachusetts) 1990.

—, The singularity is near – When humans transcend biology, New York 2005.

Kwon, Kwiseok/Kim, Cookhwan, How to design personalization in a context of customer retention: Who personalizes what and to what extent?, Electronic Commerce Research and Applications 11 (2012), S. 101–116.

Laitinen, Arto/Sahlgren, Otto, AI Systems and Respect for Human Autonomy, Frontiers in artificial intelligence 4 (2021), S. 1–14.

Larson, Jeff/Mattu, Surya/Kirchner, Lauren Kirchner, Angwin, Julia, How We Analyzed the COMPAS Recidivism Algorithm, ProPublica 23.05.2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

Laux, Johann/Wachter, Sandra/Mittelstadt, Brent, Taming the few – Platform regulation, independent audits, and the risks of capture created by the DMA and DSA, CLSR 43 (2021), S. 1–12.

—, Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk, Regulation & Governance 17 (2023), S. 1–30.

Lawless, W. F./Mittu, Ranjeev/Sofge, Donald/Russell, Stephen (Hrsg.), Autonomy and Artificial Intelligence: A Threat or Savior?, Cham 2017.

Layton, Roslyn, The Authoritarian Paternalism of EU Tech Policy, 13.03.2020, https://www.aei.org/technology-and-innovation/the-authoritarian-paternalism-of-eu-tech-policy.

LeCun, Yann/Bengio, Yoshua/Hinton, Geoffrey, Deep learning, Nature 521 (2015), S. 436–444.

Leenes, Ronald, Reply: Addressing the Obscurity of Data Clouds, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 293–302.

—, Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology, Legisprudence 5 (2011), S. 143–169.

Leerssen, Paddy, Algorithm Centrism in the DSA's Regulation of Recommender Systems, Verfassungsblog 29.03.2022, https://verfassungsblog.de/roa-algorithm-centrism-in-the-dsa/.

Leese, Matthias, The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union, Security Dialogue 45 (2014), S. 494–511.

Lehtiniemi, Tuukka/Kortesniemi, Yki, Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach, Big Data and Society 4 (2017), 1-11.

Dürig, Günter/Herzog, Roman/Scholz, Matthias (Hrsg.), begründet von *Maunz, Theodor/Dürig, Günter/Herzog, Roman*, Grundgesetz – Kommentar, 99. Aufl., München 2023 (zit. Dürig/Herzog/Scholz, GG/*Bearbeiter*).

Leistner, Matthias/Antoine, Lucie/Sagstetter, Thomas, Big Data – Rahmenbedingungen im europäischen Datenschutz- und Immaterialgüterrecht und übergreifende Reformperspektive, Tübingen 2021.

Lenk, Christian/Duttge, Gunnar/Fangerau, Heiner (Hrsg.), Handbuch Ethik und Recht der Forschung am Menschen, Place of publication not identified 2014.

Lenk, Klaus, Die neuen Instrumente der weltweiten digitalen Governance, Verwaltung und Management 22 (2016), S. 225–280.

Lerche, Peter, Werbung und Verfassung – Studie im Auftrag des Zentralausschusses der Werbewirtschaft, München 1967.

Lessig, Lawrence, Code – Version 2.0, 2. Aufl., New York 2006.

Lewandowski, Dirk/Kerkmann, Friederike/Sünkler, Sebastian, Wie Nutzer im Suchprozess gelenkt werden – Zwischen technischer Unterstützung und interessengeleiteter Darstellung, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014, S. 75–97.

Lewinski, Kai von, Die Matrix des Datenschutzes – Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2021.

Lewinski, Kai von/*Pohl, Dirk*, Auskunfteien nach der europäischen Datenschutzreform, ZD 9 (2018), S. 17–23.

Lewis-Kraus, Gideon, The Great A.I. Awakening – How Google used artificial intelligence to transform Google Translate, one of its more popular services – and how machine learning is poised to reinvent computing itself, The New York Times Magazine 18.12.2016.

Libet, Benjamin, Unconscious cerebral initiative and the role of conscious will in voluntary action, Behavioral and Brain Sciences 8 (1985), S. 529–539.

Liesem, Kerstin, Pionierleistung mit Signalwirkung – Die regulative Einhegung von Medienintermediären im Medienstaatsvertrag, AfP 51 (2020), S. 277–283.

Ligthart, Sjors/van Toor, Dave/Kooijmans, Tijs/Douglas, Thomas/Meynen, Gerben (Hrsg.), Neurolaw – Advances in Neuroscience, Justice & Security, Cham 2021.

Linderkamp, Jörn, Der digitale Preis – eine automatisierte Einzelfallentscheidung? – Personalisierte Preisgestaltungen im Kontext des Datenschutzrechts, ZD 10 (2020), S. 506–511.

Littwin, Frank, Grundrechtsschutz gegen sich selbst – Das Spannungsverhältnis von grundrechtlichem Selbstbestimmungsrecht und Gemeinschaftsbezogenheit des Individuums, Frankfurt am Main/Berlin 1993.

Liu, Juntao/Wu, Caihua, Deep Learning Based Recommendation: A Survey, in: Kim, Kuinam/Joukov, Nikolai (Hrsg.), Information Science and Applications 2017 – ICISA 2017, Bd. 424, Singapore 2017, S. 451–458.

Liu, Liz, Using Unsupervised Learning to Detect Purchase Preferences in Retail Stores, Medium, 08.01.2019, https://medium.com/@tianjiaoliu2012/using-unsupervised-learning-to-detect-purchase-preferences-in-retail-stores-7e5cd592c7ee.

Lobe, Adrian, Lieber Computer, sag mir, wen ich heiraten soll – Die Macht der Datenkonzerne, FAZ 14.09.2016.

Löber, Lena Isabell/Roßnagel, Alexander, Kennzeichnung von Social Bots – Transparenzpflichten zum Schutz integrer Kommunikation, MMR 22 (2019), S. 493–498.

Lohmann, Melinda F., Ein europäisches Roboterrecht – überfällig oder überflüssig?, ZRP 50 (2017), S. 168–171.

Lohr, Jason D./Winston, Maxwell J./Watts, Peter, Legal Practisioner's Approach to Regulating AI Risks, in: Yeung, Karen/Lodge, Martin (Hrsg.), Algorithmic regulation, 2019, S. 224–247.

Longo, Luca/Rizzo, Lucas/Hunter, Elizabeth/Pakrashi, Arjun (Hrsg.), Artificial Intelligence and Cognitive Science 2020.

Lorentz, Nora, Profiling – Persönlichkeitsschutz durch Datenschutz? 2019.

Lücke, Oliver (Hrsg.), Künstliche Intelligenz und Vorschläge zu einer EU-Regulierung, Berlin 2021.

—, Künstliche Intelligenz: wo bleibt eine europäische Grundverordnung?!, in: ders. (Hrsg.), Künstliche Intelligenz und Vorschläge zu einer EU-Regulierung, Berlin 2021, S. 10–63.

Lutz, Christoph/Strathoff, Pepe, Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses, in: Brändli, Sandra (Hrsg.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, Bern 2013, S. 81–99.

Lutz, Marina, Datenschutz im Onlinemarketing, in: Specht-Riemenschneider, Louisa/Werry, Nikola u.a. (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2019, S. 203–250.

Lynskey, Orla, Deconstructing Data Protection – The „added-value" of a right to data protection in the EU legal order, ICLQ 63 (2014), S. 569–597.

Lyon, David, Surveillance as social sorting – Privacy, risk, and digital discrimination, London/New York 2003.

MacCarthy, Mark, AI needs more regulation, not less, Brookings, 09.03.2020, https://www.brookings.edu/research/ai-needs-more-regulation-not-less.

Madden, Mary/Gilman, Michele/Levy, Karen/Marwick, Alice, Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Privacy, Poverty, and Big Data – A Matrix of Vulnerabilities for Poor Americans Americans, Washington University Law Review 95 (2017), S. 53–125.

Magin, Melanie/Steiner, Miriam/Stark, Birgit, Suche im Netz – einseitige oder vielfältige Informationsquelle?, Media Perspektiven 2019, S. 421–429.

Mahler, Tobias, Between Risk Management and Proportionality: The Risk-based Approach in the EU's Artificial Intelligence Act Proposal, in: Colonna, Liane/Greenstein, Stanley (Hrsg.), Law in the era of artificial intelligence, Visby/Stockholm 2022, S. 247–269.

Mainzer, Klaus, Künstliche Intelligenz – Wann übernehmen die Maschinen?, 2. Aufl., Berlin, Heidelberg 2019.

Majeed, Abdul/Khan, Safiullah/Hwang, Seong Oun, Group Privacy: An Underrated but Worth Studying Research Problem in the Era of Artificial Intelligence and Big Data, Electronics 11 (2022), S. 1–34.

Malgieri, Gianclaudio/Comandé, Giovanni, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, Int. Data Priv. Law 7 (2017), S. 243–265.

Manheim, Karl/Kaplan, Lyric, Artificial Intelligence: Risks to Privacy and Democracy, Yale J.L. & Tech. 21 (2019), S. 106.

Mann, Monique/Matzner, Tobias, Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination, Big Data and Society 6 (2019), 1-11.

Mantelero, Alessandro, From Group Privacy to Collective Privacy – Towards a New Dimension of Privacy and Data Protection in the Big Data Era, in: Taylor, Linnet/Floridi, Luciano/van der Sloot, Bart (Hrsg.), Group Privacy – New Challenges of Data Technologies, Cham 2017, S. 139–158.

—, Fundamental rights impact assessments in the DSA, Verfassungsblog 01.11.2022, https://verfassungsblog.de/dsa-impact-assessment/.

Markoff, John, Scientists Worry Machines May Outsmart Man, The New York Times 25.07.2009.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht – Grundlagen, Dimensionen, Verflechtungen, Tübingen 2018.

Martini, Mario, Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 129 (2014), S. 1481–1489.

—, Algorithmen als Herausforderung für die Rechtsordnung, JZ 72 (2017), S. 1017.

—, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz 2019.

Martini, Mario/Drews, Christian/Seeliger, Paul/Weinzierl, Quirin, Dark Patterns – Phänomenologie und Antworten der Rechtsordnung, ZfDR 1 (2021).

Martini, Mario/Nink, David, Wenn Maschinen entscheiden… – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ 36 (2017), S. 1–14.

Martin-Jung, Helmut, Künstliche Intelligenz wird überschätzt, SZ 30.11.2018.

—, Wie die Google-Suche funktioniert, SZ 210.3.2022.

Marx, Iris, Legal Tech – wann kommt der Robo-Richter?, DRiZ 96 (2018), S. 422.

Masing, Johannes, Herausforderungen des Datenschutzes, NJW 65 (2012), S. 2305–2311.

Mattioli, Dana, On Orbitz, Mac Users Steered to Pricier Hotels, The Wall Street Journal 23.8.2012.

Matz, Sandra C./Konsinksi, Mark/Nave, Gideon/Stillwell, Davic J., Psychological targeting as an effective approach to digital mass persuasion, Proceedings of the National Academy of Sciences of the United States of America 114 (2017), S. 12714–12719.

Mayer-Schönberger, Viktor/Cukier, Kenneth/Mallett, Dagmar, Big Data – Die Revolution, die unser Leben verändern wird, München 2013.

Mayer-Schönberger, Viktor/Padova, Yann, Regime Change: Enabling Big Data through Europe's New Data Protection Regulation, Colum. Sci. & Tech. L. Rev. 17 (2016), S. 315–335.

McCarthy, John/Minsky, Marvin/Rochester, Nathaniel/Shannon, Claude E., A Proposal for the Darthmouth Summer Research Project on Artificial Intelligence, Stanford University, Stanford 31. August 1955, http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf.

McCarthy Mark, Propp, Kenneth, Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation, Lawfare 28.04.2021, https://www.lawfareblog.com/machines-learn-brussels-writes-rules-eus-new-ai-regulation.

McDonald, Aleecia M./Lorrie Faith Cranor, The Cost of Reading Privacy Policies, J. Law. Soc. 4 (2008-2009), S. 543–568.

McKnight, William, Life in 2050: How Will AI Shape the Future?, InformationWeek 02.09.2022.

McPherson, Miller/Smith-Lovin, Lynn/Cook, James M., Birds of a Feather: Homophily in Social Networks, Annual Review of Sociology 27 (2001), S. 415–444.

Meckel, Miriam, Ist Künstliche Intelligenz die bessere Demokratin?, Handelsblatt 21.7.2022.

Meents, Jan G., Datenschutz durch KI – Kapitel 8.8, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, S. 445–461.

Mehrabi, Ninareh/Morstatter, Fred/Saxena, Nripsuta/Lerman, Kristina/Galstyan, Aram, A Survey on Bias and Fairness in Machine Learning 23.08.2019, https://arxiv.org/pdf/1908.09635.

Mele, Alfred R. (Hrsg.), Surrounding free will – Philosophy, psychology, neuroscience, Oxford u.a. 2015.

Menczer Filippo/Hills, Thomas, Die digitale Manipulation, Spektrum 02.04.2021.

Mendoza, Isak/Bygrave, Lee A., The Right Not to be Subject to Automated Decisions Based on Profiling, in: Synodinou, Tatiana-Eleni/Jougleux, Philippe u.a. (Hrsg.), EU Internet Law – Regulation and enforcement, Cham 2017, S. 77–98.

Menzel, Wolfgang, Sprachverarbeitung, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 601–672.

Merlec, Mpyana Mwamba/Lee, Youn Kyu/Hong, Seng-Phil/In, Hoh Peter, A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR, Sensors 21 (2021).

Meßerschmidt, Klaus, Gesetzgebungslehre zwischen Wissenschaft und Politik – Entwicklungstendenzen der Legisprudenz – Teil 1, ZJS 1 (2008), S. 111–122.

—, Gesetzgebungslehre zwischen Wissenschaft und Politik – Entwicklungstendenzen der Legisprudenz – Teil 2, ZJS 1 (2008), S. 224–232.

Meta AI, The new AI-powered feature designed to improve Feed for everyone, 5.10.2022, https://ai.facebook.com/blog/facebook-feed-improvements-ai-show-more-less.

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.), begründet von —, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019 (zit. Meyer/Hölscheidt, GRCh/*Bearbeiter*).

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 41 (2017), S. 349–353.

Mik, Eliza, The erosion of autonomy in online consumer transactions, Law Innov. Technol. 8 (2016), S. 1–38.

Miller, Akiva, What Do We Worry About When We Worry About Price Discrimination? – The Law and Ethics of Using Personal Information for Pricing, J. Law Technol. Policy 2014, 41-104.

Miller, Jennifer, Is an Algorithm Less Racist Than a Loan Officer?, The New York Times 18.09.2020.

Miller, Tim, Explanation in Artificial Intelligence: Insights from the Social Sciences 22.06.2017, https://arxiv.org/pdf/1706.07269.

Miorandi, Daniele/Rizzardi, Alessandra/Sicari, Sabrina/Coen-Porisini, Alberto, Sticky Policies: A Survey, IEEE Transactions on Knowledge and Data Engineering 32 (2020), S. 2481–2499.

Misselhorn, Catrin, Maschinenethik und „Artificial Morality" – Können und sollen Maschinen moralisch handeln?, Bundeszentrale für politische Bildung, Bonn 2.2.2018, https://www.bpb.de/shop/zeitschriften/apuz/263684/maschinenethik-und-artificial-morality/.

Mitchell, Tom M./Caruana, Rich/Freitag, Dayne/McDermott, John/Zabowski, David, Experience with a learning personal assistant, Communications of the ACM 37 (1994), S. 80–91.

Mittelstadt, Brent, Auditing for Transparency in Content Personalization Systems, Int. J. Commun. 10 (2016).

Mittelstadt, Brent Daniel/Allo, Patrick/Taddeo, Mariarosaria/Wachter, Sandra/Floridi, Luciano, The ethics of algorithms: Mapping the debate, Big Data and Society 3 (2016), 1-21.

Mocker, Valerie, Digitale Mündigkeit – Warum Finnland für Deutschland ein Vorbild ist, Gewerblicher Rechtsschutz und Urheberrecht 24.6.2019.

Mödinger, Maximilian, Bessere Rechtsetzung – Leistungsfähigkeit eines europäischen Konzepts, Tübingen 2020.

Moeller, Judith/Helberger, Natali, Beyond the filter bubble: concepts, myths, evidence and issues for future debates, University of Amsterdam 2018, https://www.ivir.nl/publicaties/download/Beyond_the_filter_bubble__concepts_myths_evidence_and_issues_for_future_debates.pdf.

Mohabbat-Kar, Resa/Thapa, Basanta E.P./Parycek, Peter (Hrsg.), (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Berlin Juni 2018.

Möller, Kai, Paternalismus und Persönlichkeitsrecht, Berlin 2005.

Moos, Flemming/Rothkegel, Tobias, Nutzung von Scoring-Diensten im Online-Versandhandel – Scoring-Verfahren im Spannungsfeld von BDSG, AGG und DS-GVO, ZD 6 (2016).

Mozur, Paul, Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras, New York Times 08.07.2018.

Müller, Georg, Rechtssetzungslehre zwischen normativen Anforderungen und „Klugheitsregeln", in: Akyürek, Metin (Hrsg.), Staat und Recht in europäischer Perspektive – Festschrift Heinz Schäffer, Wien/München 2006, S. 503–514.

Müller, Vincent C., Ethics of Artificial Intelligence and Robotics, in: The Metaphysics Research Lab, Stanford University (Hrsg.), The Stanford Encyclopedia of Philosophy, Stanford 2020.

Müller-Terpitz, Ralf, Filter als Gefahr für die Meinungspluralität? – Verfassungsrechtliche Erwägungen zum Einsatz von Filtertechnologien, ZUM 64 (2020), S. 365–374.

Mund, Dorothea, Das Recht auf menschliche Entscheidung – Freiheit in Zeiten der Digitalisierung und einer automatisierten Rechtsanwendung, in: Gwiasda, Benjamin/Greve, Ruth u.a. (Hrsg.), Der digitalisierte Staat – Chancen und Herausforderungen für den modernen Staat, Baden-Baden 2020, S. 177–198.

—, Das Recht auf menschliche Entscheidung 2021.

Murmann, Patrick/Fischer-Hübner, Simone, Usable Transparency Enhancing Tools: A Literature Review, Karlstad University Working Paper Juli 2017, http://www.diva-portal.org/smash/get/diva2:1119515/FULLTEXT02.

Myers, Karen/Berry, Pauline/Blythe, Jim/Conley, Ken/Gervasio, Melinda/McGuinness, Deborah/Morley, David/Pfeffer, Avi, Pollack, Martha/Tambe, Milind, An Intelligent Personal Assistant for Task and Time Management, AI Magazine 28 (2007), S. 47–61.

Nabeth, Tierry, Reply: Further Implications?, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 30–34.

Nahmias, Eddy, Wie frei ist der Mensch?, Spektrum 20.08.2015.

Nebel, Bernhard/Wölfl, Stefan, Wissensrepräsentation und Verarbeitung, in: Görz, Günther/Schmid, Ute/Braun, Tanya (Hrsg.), Handbuch der Künstlichen Intelligenz, 6. Aufl., Berlin/Boston 2021, S. 27–55.

Nemitz, Paul, Constitutional democracy and technology in the age of artificial intelligence, Philos Trans A Math Phys Eng Sci 376 (2018).

Nettesheim, Martin, Grundrechtsschutz der Privatheit, in: Nettesheim, Martin/Diggelmann, Oliver u.a. (Hrsg.), Der Schutzauftrag des Rechts – Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, Berlin 2011, S. 7–49.

—, »Leben in Würde«: Art. 1 Abs. 1 GG als Grundrecht hinter den Grundrechten, JZ 74 (2019), S. 1–11.

—, Die unionsrechtliche Regulierung großer Internet-Plattformen – Die Kommissionsentwürfe für einen Digital Markets Act und einen Digital Services Act, Bundestag 11.2.2021.

—, § 10 Privatleben und Privatsphäre, in: Grabenwarter, Christoph/Breuer, Marten/Bungenberg, Marc (Hrsg.), Europäischer Grundrechteschutz – Zugleich Band 2 der Enzyklopädie Europarecht, 2. Aufl., Baden-Baden u.a. 2022.

—, Digitale Autonomie in Vertragsbeziehungen – Zum Verhältnis von Privatautonomie und „Datenkontrolle", Verfassungsblog 12.10.2022, https://verfassungsblog.de/digitale-autonomie/.

—, Critical Comments on the European Data Protection Board's Understanding of Contracts as a Ground to Process Personal Data, EU Law Live Februar Weekend Edition (2023), S. 3–16.

Nettesheim, Martin/Diggelmann, Oliver/Lege, Joachim/Kingreen, Thorsten (Hrsg.), Der Schutzauftrag des Rechts – Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, Berlin 2011.

Ng, Davy Tsz Kit/Leung, Jac Ka Lok/Chu, Samuel Kai Wah/Qiao, Maggie Shen, Conceptualizing AI literacy: An exploratory review, Computers and Education: Artificial Intelligence 2 (2021), S. 1–11.

Niemann, Fabian/Kevekordes, Johannes, Machine Learning und Datenschutz (Teil 1) – Grundsätzliche datenschutzrechtliche Zulässigkeit, CR 36 (2020), S. 17–25.

NíFhaoláin, Labhaoise/Hines, Andrew/Nallur, Vivek, Assessing the Appetite for Trustworthiness and the Regulation of Artificial Intelligence in Europe, in: Longo, Luca/Rizzo, Lucas u.a. (Hrsg.), Artificial Intelligence and Cognitive Science, 2020, S. 133–144.

Nink, David, Justiz und Algorithmen – Über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeiten neuer Technologien in der Rechtsprechung, Berlin 2021.

Nissenbaum, Helen Fay, Privacy in context – Technology, policy, and the integrity of social life, Stanford, California 2010.

Nolte, Georg, Hate-Speech, Fake-News, das »Netzwerkdurchsetzungsgesetz« und Vielfaltsicherung durch Suchmaschinen, ZUM 21 (2017), S. 552–564.

Norberg, Patricia A./Horne, David O./Horne, David A., The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs 41 (2007), S. 100–126.

Norwegian Data Protection Authority, Big Data – privacy principles under pressure September 2013, https://www.datatilsynet.no/globalassets/global/english/big-data-engelsk-web.pdf.

—, Artificial intelligence and privacy, Norwegian Data Protection Authority Januar 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

Ntoutsi, Eirini/Fafalios, Pavlos/Gadiraju, Ujwal/Iosifidis, Vasileios/Nejdl, Wolfgang/Vidal, Maria-Esther/Ruggieri, Salvatore/Turini, Franco/Papadopoulos, Symeon/Krasanakis, Emmanouil/Kompatsiaris, Ioannis/Kinder-Kurlanda, Katharina/Wagner, Claudia/Karimi, Fariba/Fernandez, Miriam/Alani, Harith/Berendt, Bettina/Kruegel, Tina/Heinze, Christian/Broelemann, Klaus/Kasneci, Gjergji/Tiropanis, Thanassis/Staab, Steffen, Bias in Data-driven AI Systems – An Introductory Survey 14.01.2020, https://arxiv.org/pdf/2001.09762.

Nürnberger, Stefan/Bugiel, Sven, Autonome Systeme, DuD 40 (2016), S. 503–506.

Ogus, Anthony I., Regulatory Paternalism: When is it Justified?, in: Hopt, Klaus J. (Hrsg.), Corporate governance in context – Corporations, states, and markets in Europe, Japan, and the US, Oxford 2005, S. 302–320.

Ohly, Ansgar, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, Tübingen 2002.

Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, University of California Law Review 57 (2010), S. 1701–1777.

Oostveen, Manon, Identifiability and the applicability of data protection to big data, Int. Data Priv. Law 6 (2016), S. 229–309.

Orwat, Carsten, Diskriminierungsrisiken durch Verwendung von Algorithmen – Eine Studie, erstellt mit einer Zuwendung der Antidiskriminierungsstelle des Bundes, Baden-Baden/Berlin 2019.

Orwat, Carsten/Folberth, Anja/Bareis, Jascha/Jahnel, Jutta, Wadephul, Christian, Risikoregulierung der KI: normative Herausforderungen und politische Entscheidungen – Stellungnahme zum Weißbuch der Europäischen Kommission „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen", Karlsruher Institut für Technologie (KIT); Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) 14.06.2020, https://publikationen.bibliothek.kit.edu/1000121489/85506536.

Österreichische Datenschutzbehörde, Datenschutzbeschwerde Clearview AI – Bescheid 9.5.2023, https://noyb.eu/sites/default/files/2023-05/Clearview%20Decision%20Redacted.pdf.

Oswald, Stella, Bekämpfung von Hate Speech, in: Grabenwarter, Christoph/Holoubek, Michael/Leitl-Staudinger, Barbara (Hrsg.), Regulierung von Kommunikationsplattformen, Wien, Baden-Baden 2022, S. 67–111.

Otamendi, Javier F./Sutil Martín, Dolores Lucia, The Emotional Effectiveness of Advertisement, Frontiers in psychology 11 (2020), S. 1–12.

Ott, Stephan, Die vorherrschende Meinungsmacht von Google – Eine Replik zu Danckert/Mayer, MMR 2010, 219 ff, MMR 2010, S. 301459.

Oxford University Press (Hrsg.), The Oxford English dictionary, 2. Aufl., Oxford 2023.

Paal, Boris P., Vielfaltsicherung im Suchmaschinensektor, ZRP 48 (2015), S. 34–38.

—, Missbrauchstatbestand und Algorithmic Pricing – Dynamische und individualisierte Preise im virtuellen Wettbewerb, Gewerblicher Rechtsschutz und Urheberrecht 121 (2019), S. 43–53.

—, Spannungsverhältnis von KI und Datenschutzrecht – 8.7, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, 427-444.

Paal, Boris P./Heidtke, Aron, Vielfaltssichernde Regulierung der Medienintermediäre nach den Vorschriften des Medienstaatsvertrags der Länder, ZUM 64 (2020), S. 230–240.

Paal, Boris P./Hennemann, Moritz, Big Data im Recht – Wettbewerbs- und daten(schutz)rechtliche Herausforderungen, NJW 70 (2017), S. 1697–1701.

Paal, Boris P./Pauly, Daniel A./Ernst, Stefan (Hrsg.), begründet von *Paal, Boris P./Pauly, Daniel A.*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2020 (zit. Paal/Pauly, DS-GVO/*Bearbeiter*).

Palka, Adriane, Digitalisierung gefährdet Millionen von Jobs – welche besonders betroffen sind, Handelsblatt 26.4.2018.

Pantoja, Carlos Eduardo/Viterbo, José/Seghrouchni, Amal El-Fallah, From Thing to Smart Thing: Towards an Architecture for Agent-Based AmI Systems, in: Jezic, Gordan/Chen-Burger, Yun-Heh Jessica/Kusek, Mario (Hrsg.), Agents and Multi-agent Systems: Technologies and Applications 2019 – 13th KES International Conference, KES-AMSTA-2019 St. Julians, Malta, June 2019 Proceedings, 2020, S. 57–67.

Paradarami, Tulasi K./Bastian, Nathaniel D./Wightman, Jennifer L., A hybrid recommender system using artificial neural networks, Expert Systems with Applications 83 (2017), S. 300–313.

Pariser, Eli, The filter bubble – What the Internet is hiding from you, London 2011.

Pasquale, Frank, The Black box society – The secret algorithms that control money and information, Cambridge (Massachusetts)/London (Vereintes Königreich) 2015.

Paulus, David/Matzke, Robin, Smart Contracts und das BGB – Viel Lärm um nichts? –, ZfPW 4 (2018), S. 432–465.

Pearson, Bryan, Personalizing Price With AI: How Walmart, Kroger Do It, Forbes 7.9.2021.

Pech, Laurent, The Concept of Chilling Effect – Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU., Open Society European

Policy Institute 2021, https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf.

Peukert, Alexander, Five Reasons to be Skeptical About the DSA, Verfassungsblog 31.08.2021, https://verfassungsblog.de/power-dsa-dma-04/.

Pfeil, Werner, „Der Mensch steht höher als Technik und Maschine" – Benötigen wir ein Grundrecht zum Schutz vor Künstlicher Intelligenz? – Die Corona-Krise und die Entwicklung von Gesichts- und Emotionserkennung sowie einer Tracing-App, InTeR 8 (2020), S. 82–89.

Piao, Guangyuan/Breslin, John G., Inferring user interests in microblogging social networks: a survey, User Modeling and User-Adapted Interaction 28 (2018), S. 277–329.

Pichai, Sundar, Why Google thinks we need to regulate AI, Financial Times 20.01.2020.

Picht, Peter/Richter, Heiko, The proposed EU digital services regulation 2020: data desiderata, München September 2021, https://rds-tue.ibs-bw.de/opac/RDSIndex/Search?lookfor=digital+services+package&type=AllFields.

Pille, Jens-Ulrich, Der Grundsatz der Eigenverantwortlichkeit im Internet, NJW 71 (2018), S. 3545–3550.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG – Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 4. Aufl., Köln 2023 (zit. Plath, DSGVO/BDSG/*Bearbeiter*).

Poikola, Antti/Kuikkaniemi, Kai/Honko, Harri, MyData – A Nordic Model for human-centered personal data management and processing, Ministry of Transport and Communications Finland 2015, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=y.

Poullet, Yves/Rouvroy, Antoinette, The Right to Informational Self-Determination and the Value of Self- Development: Reassessing the Importance of Privacy for Democracy, in: Hert, Paul de/Gutwirth, Serge/Poullet, Yves (Hrsg.), Reinventing Data Protection?, Dordrecht 2009, S. 45–76.

Power, Daniel, What is decision automation?, DSSResources 19.12.2018, http://dssresources.com/faq/index.php?action=artikel&id=6.

Prasad, Rohit, „Ambient intelligence" will accelerate advances in general AI, Amazon Science, 21.01.2021, https://www.amazon.science/blog/ambient-intelligence-will-accelerate-advancements-in-general-ai.

Profiling, in: Oxford University Press (Hrsg.), The Oxford English dictionary, 2. Aufl., Oxford 2023.

Puri, Anuj, A Theory of Group Privacy, Cornell Journal of Law and Public Policy 30 (2021), S. 477–538.

Purtova, Nadezhda, The law of everything. Broad concept of personal data and future of EU data protection law, Law Innov. Technol. 10 (2018), S. 40–81.

Quarch, Benedikt M./Hähnle, Johanna, Zurück in die Zukunft: Gedanken zur Automatisierung von Gerichtsverfahren, NJOZ 20 (2020), S. 1281–1286.

Rademacher, Timo, Predictive Policing im deutschen Polizeirecht, AöR 142 (2017), S. 366–416.

Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen 2021.

Raji, Behrang, Rechtliche Bewertung synthetischer Daten für KI-Systeme, DuD 45 (2021), S. 303–309.

Ramos, Carlos/Augusto, Juan Carlos/Shapiro, Daniel, Ambient Intelligence – the Next Step for Artificial Intelligence, IEEE Intelligent Systems 23 (2008), S. 15–18.

Rao, Ashwini/Schaub, Florian/Sadeh, Norman, What do they know about me? Contents and Concerns of Online Behavioral Profiles, Carnegie Mellon University Pittsburgh 04.06.2015, https://arxiv.org/pdf/1506.01675.

Raposo, Vera Lúcia, Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence, Int. J. Law Inf. Technol. 30 (2022), S. 88–109.

Raue, Benjamin/Heesen, Hendrik, Der Digital Services Act, NJW 75 (2022), S. 3537–3543.

Redding, Sophia, Künstliche Intelligenz im Bewerbungsprozess:, Tagesspiegel 19.07.2021.

Reding, Viviane, Sieben Grundbausteine der europäischen Datenschutzreform, ZD 2 (2012), S. 195–198.

Reed, Chris, Taking Sides on Technology Neutrality, SCRIPed 4 (2007), S. 263–284.

—, How should we regulate artificial intelligence?, Philos Trans A Math Phys Eng Sci 376 (2018), S. 1–12.

Reich, Norbert, Innovationssteuerung im Privatrecht, in: Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.), Rechtswissenschaftliche Innovationsforschung – Grundlagen, Forschungsansätze, Gegenstandsbereiche, Baden-Baden 1998, S. 330–350.

Reidenberg, Joel R., Lex Informatica: The Formulation of Information Policy Rules through Technology, Texas Law Review 76 (1998), S. 553–593.

Reinhardt, Jörg, Konturen des europäischen Datenschutzgrundrechts – Zu Gehalt und horizontaler Wirkung von Art. 8 GRCh, AöR 142 (2017), S. 528–565.

Reisch, Lucia/ Büchel, Daniela/Gigerenzer, Gerd/Zander-Hayat, Helga/Joost, Gesche/Micklitz, Hans-Wolfgang/Oehler, Andreas/Schlegel-Matthies, Kirsten/Wagner, Gert G., Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, Gutachten des Sachverständigenrats für Verbraucherfragen, Berlin Dezember 2016, https://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_SVRV-.pdf.

Resnick, Paul/Garrett, R. Kelly/Kriplean, Travis/Munson, Sean A./Stroud, Natalie Jomini, Bursting your (filter) bubble, in: Bruckman, Amy (Hrsg.), Proceedings of the 2013 conference on Computer supported cooperative work companion, New York 2013, S. 95–100.

Retica, Aaron, Homophily, New York Times Magazine 10.12.2006.

Rich, Elaine, User Modeling via Stereotypes, Cognitive Science 3 (1979), S. 329–354.

Richter, Philipp, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 39 (2015), S. 735–740.

—, Big Data, Statistik und die Datenschutz-Grundverordnung, DuD 40 (2016), S. 581–586.

Riechert, Anne, Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten – Studie im Auftrag der Stiftung Datenschutz, Frankfurt (Main) Dezember 2016, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf.

Rieder, Bernhard/Hofmann, Jeanette, Towards platform observability, Internet Policy Rev. 9 (2020), S. 1–28.

Robinette, P./Li, Wenchen/Allen, Robert/Howard, A./Wagner, A., Overtrust of robots in emergency evacuation scenarios, 2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI) 2016, S. 101–108.

Robrecht, Bettina, EU-Datenschutzgrundverordnung: Transparenzgewinn oder Information-Overkill, Edewecht 2015.

Rogosch, Patricia, Die Einwilligung im Datenschutzrecht, Baden-Baden 2012.

Roose, Kevin, We Need to Talk About How Good A.I. Is Getting, The New York Times 24.08.2022.

—, The Brilliance and Weirdness of ChatGPT, The New York Times 07.12.2022.

Rössler, Beate, Autonomie – Ein Versuch über das gelungene Leben, Berlin 2017.
Roßnagel, Alexander, Rechtswissenschaftliche Technikfolgenforschung – Umrisse einer Forschungsdisziplin, Baden-Baden 1993.
—, Ansätze zu einer rechtlichen Steuerung des technischen Wandels, in: Breuer, Rüdiger/Kloepfer, Michael u.a. (Hrsg.), Jahrbuch des Umwelt- und Technikrechts, Heidelberg 1994, S. 425–461.
—, Notwendige Schritte zu einem modernen Datenschutzrecht, in: Roßnagel, Alexander/Abel, Ralf Bernd (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, S. 361–384.
—, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 8 (2005), S. 71–75.
—, Datenschutz in einem informatisierten Alltag – Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin 2007.
—, „Technikneutrale" Regulierung: Möglichkeiten und Grenzen, in: Eifert, Martin/Hoffmann-Riem, Martin (Hrsg.), Innovationsfördernde Regulierung, Berlin 2009, S. 323–337.
—, Innovation als Gegenstand der Rechtswissenschaft, in: Hof, Hagen/Wegenroth, Ulrich (Hrsg.), Innovationsforschung – Ansätze, Methoden, Grenzen und Perspektiven, 2. Aufl., Berlin 2010, S. 9–22.
—, Big Data – Small Privacy? – Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 3 (2013), S. 562–567.
—, Wie zukunftsfähig ist die Datenschutz-Grundverordnung? – Welche Antworten bietet sie für die neuen Herausforderungen des Datenschutzrechts?, DuD 40 (2016), S. 561–565.
—, Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? – Bedeutung der Grundsätze für die datenschutzrechtliche Praxis, ZD 9 (2018), S. 339–344.
Roßnagel, Alexander/Abel, Ralf Bernd (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.
Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden/Heidelberg 2018.
Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der DS-GVO, ZD 3 (2013), S. 103–108.
Rouvroy, Antoinette, Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, Studies in Ethics, Law, and Technology 2 (2008), S. 1–51.
—, Of Data and Men: Fundamental Rights and Liberties in a World of Big Data, Straßburg 11.01.2016, http://www.crid.be/pdf/public/8137.pdf.
Rubinstein, Ira S./Hartzog, Woodrow, Anonymization and Risk, Washington Law Review 91 (2016), S. 703–758.
Russell, Stuart/Dewey, Daniel/Tegmark, Max, Research Priorities for Robust and Beneficial Artificial Intelligence, AI Magazine 36 (2015), S. 105–114.
Russell, Stuart J., Human compatible – Artificial intelligence and the problem of control, New York 2019.
Russell, Stuart J./Norvig, Peter, Artificial Intelligence – A modern approach, 4. Aufl., Boston 2021.
Rustici, Chiara, GDPR Profiling and Business Practice – Squaring the circle: How to apply the GDPR rules to the commercial and techological realities of profiling?, CRi 18 (2018), S. 34–43.
Sadok, Hicham/Sakka, Fadi/El Maknouzi, Mohammed El Hadi, Artificial intelligence and bank credit analysis: A review, Cogent Economics and Finance 10 (2022), S. 1–12.

Sadri, Fariba, Ambient intelligence – A Survey, ACM Computing Surveys 43 (2011), S. 1–66.

Samuelson, William/Zeckhauser, Richard, Status quo bias in decision making, Journal of Risk and Uncertainty 1 (1988), S. 7–59.

Sandfuchs, Barbara, Privatheit wider Willen?, Tübingen 2015.

Sartor, Giovanni, New aspects and challenges in consumer protection – Digital services and artificial intelligence, Europäisches Parlament, Luxemburg April 2020, http://www.europarl.europa.eu/supporting-analyses.

Sarunski, Maik, Big Data – Ende der Anonymität? – Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern, DuD 40 (2016), S. 424–427.

Schauer, Frederick, Profiles, Probabilities, and Stereotypes, Cambridge, Mass. 2006.

Schefzig, Jens, Big Data = Personal Data? – Der Personenbezug von Daten bei Big Data-Analysen, K&R 14 (2014), 772-778.

Scheibehenne, Benjamin/Greifeneder, Rainer/Todd, Peter M., Can There Ever Be Too Many Options? A Meta-Analytic Review of Choice Overload, Journal of Consumer Research 37 (2010), S. 409–425.

Scherer, Matthew U., Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, Harv. J. Law Technol. 29 (2016), S. 353–400.

Schermer, Bart W., The limits of privacy in automated profiling and data mining, CLSR 27 (2011), S. 45–52.

Scherzberg, Arno, Innovationen und Recht: Zum Stand der rechtswissenschaftlichen Innovationsforschung, in: Hoffmann-Riem, Wolfgang/Brandt, Edmund/Schuler-Harms, Margarete (Hrsg.), Offene Rechtswissenschaft – Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010, S. 273–308.

Scheufen, Marc, Künstliche Intelligenz und Haftungsrecht: die e-Person aus ökonomischer Sicht, Wirtschaftsdienst 99 (2019), S. 411–414.

Schiaffino, Silvia/Amandi, Analia, Intelligent User Profiling, in: Bramer, Max (Hrsg.), Artificial intelligence – An international perspective, Berlin 2009, S. 193–216.

Schimmele, Tanja, Staatliche Verantwortung für diskursive Integrität in öffentlichen Räumen 2019.

Schirmer, Jan-Erik, Artificial Intelligence and Legal Personality: Introducing „Teilrechtsfähigkeit" – a Partial Legal Status Made in Germany, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 123–142.

Schläger, Uwe/Thode, Jan-Christoph (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, 2. Aufl., Berlin 2022.

Schleipfer, Stefan, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 7 (2017), S. 460–466.

Schmarzo, Bill, Is Data Science Really Science?, 02.02.2017, https://www.linkedin.com/pulse/data-science-really-bill-schmarzo.

Schmid, Gregor/Grewe, Max, Digital Services Act: Neues „Grundgesetz für Onlinedienste"? – Auswirkungen des Kommissionsentwurfs für die Digitalwirtschaft, MMR 24 (2021), S. 279–282.

Schmid, Tobias/Braam, Laura/Mischke, Julia, Gegen Meinungsmacht – Reformbedürfnisse aus Sicht eines Regulierers – Macht im Netz I: Herausforderungen für die Sicherung der Meinungs- und Medienvielfalt, MMR 23 (2020), S. 19–23.

Schneider, Ingrid/Ulbricht, Lena, Ist Big Data fair? – Normativ hergestellte Erwartungen an Big Data, in: Kolany-Raiser, Barbara/Heil, Reinhard u.a. (Hrsg.), Big Data und Gesellschaft – Eine multidisziplinäre Annäherung, Wiesbaden 2018, S. 198–207.

Schneiders, Pascal, Jeder kriegt einen eigenen Preis, FAZ 08.04.2015.

Schönmann, Markus, Bonitätsmanagement (einschl. Scoring), in: Schläger, Uwe/Thode, Jan-Christoph (Hrsg.), Handbuch Datenschutz und IT-Sicherheit, 2. Aufl., Berlin 2022, S. 369–403.

Schreckenberger, Waldemar (Hrsg.), Grundfragen der Gesetzgebungslehre – Aktualisierte Vorträge eines Seminars zur Gesetzgebungslehre (1996) an der Deutschen Hochschule für Verwaltungswissenschaften Speyer, Berlin 2000.

Schreurs, Wim/Hildebrandt, Mireille/Kindt, Els/Vanfleteren, Michaël, Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group-Profiling in the Private Sector, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 241–264.

Schröder, Kay, Potentiale der Informationsvisualisierung im Datenschutz – eine kommunikationswissenschaftliche Betrachtung, in: Specht-Riemenschneider, Louisa/Werry, Nikola u.a. (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2019, S. 345–359.

Schröder, Meinhard, Rahmenbingungen der staatlichen Regulierung von Social Bots, DVBl 133 (2018), S. 464–494.

Schulte, Laura, Transparenz im Kontext der DSGVO, PinG 5 (2017), S. 227–230.

Schulte, Martin/Di Fabio, Udo (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis, Heidelberg 1997.

Schulz, Wolfgang/Dankert, Kevin, Die Macht der Informationsintermediäre – Erscheinungsformen, Strukturen und Regulierungsoptionen, Friedrich-Ebert-Stiftung, Bonn.

Schulze-Fielitz, Helmuth, Instrumente der Innovationssteuerung durch Öffentliches Recht – insbesondere Umweltrecht, in: Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.), Rechtswissenschaftliche Innovationsforschung – Grundlagen, Forschungsansätze, Gegenstandsbereiche, Baden-Baden 1998, S. 291–329.

Schuppert, Gunnar Folke, Innovationssteuerung im Verwaltungsorganisationsrecht, in: Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.), Rechtswissenschaftliche Innovationsforschung – Grundlagen, Forschungsansätze, Gegenstandsbereiche, Baden-Baden 1998, S. 171–207.

Schürmann, Kathrin, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz – Bewertung und Minimierung der Risiken, ZD 12 (2022), S. 316–321.

Schwabe, Daniel (Hrsg.), Proceedings of the 22nd international conference on World Wide Web companion, Republic and Canton of Geneva 2013.

Schwartmann, Rolf, Zwei Säulen für die Demokratie, FAZ 26.05.2019.

—, Wenn Maschinen die Macht übernehmen, FAZ 25.02.2023.

Schwartmann, Rolf/Hermann, Maximilian/Mühlenbeck, Robin L., Eine Medienordnung für Intermediäre – Das Zwei-Säulen-Modell zur Sicherung der Vielfalt im Netz, MMR 22 (2019), S. 498–503.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), begründet von *Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter/Atzert, Michael/Buchmann, Antonia*, DS-GVO/BDSG – Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl. 2020 (zit. Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG/*Bearbeiter*).

Schweitzer, Heike/Peitz, Martin, Datenmärkte in der digitalisierten Wirtschaft – Funktionsdefizite und Regelungsbedarf? 18.10.2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf.

Seele, Peter/Dierksmeier, Claus/Hofstetter, Reto/Schultz, Mario D., Mapping the Ethicality of Algorithmic Pricing: A Review of Dynamic and Personalized Pricing, Journal of Business Ethics 170 (2021), S. 697–719.

Seidel, Christian, Personale Autonomie als praktische Autorität, Deutsche Zeitschrift für Philosophie 59 (2011), S. 897–915.

—, Selbst bestimmen – Eine philosophische Untersuchung personaler Autonomie, Berlin/Boston 2016.

Selbst, Andrew D./Barocas, Solon, The Intuitive Appeal of Explainable Machines, Fordham L. Rev. 87 (2018), S. 1085–1139.

Selbst, Andrew D./Powles, Julia, Meaningful information and the right to explanation, Int. Data Priv. Law 7 (2017), S. 233–242.

Sesing, Andreas, Grenzen systemischer Transparenz bei automatisierter Datenverarbeitung – Umfang und Grenzen der Pflicht zur Bereitstellung aussagekräftiger Informationen über die involvierte Logik, MMR 24 (2021), S. 288–292.

Shi, Si/Tse, Rita/Luo, Wuman/D'Addona, Stefano/Pau, Giovanni, Machine learning-driven credit risk: a systemic review, Neural Computing and Applications 34 (2022), S. 14327–14339.

Shi, Wenbo, Recommendation Systems: A Review – A summary of recommender system methods, Towards Data Science 03.02.2020.

Shiller, Benjamin R., Personalized Price Discrimination Using Big Data, Brandeis University 29.07.2019, https://www.brandeis.edu/economics/RePEc/brd/doc/Brandeis_WP108.pdf.

Siebenhaar, Hans-Peter, EU-Parlament will Überregulierung von KI verhindern, Handelsblatt 19.10.2020, https://www.handelsblatt.com/politik/international/kuenstliche-intelligenz-eu-parlament-will-ueberregulierung-von-ki-verhindern/26281962.html.

Simanowski, Roberto, Wir halten uns für den Endpunkt der Schöpfung. Doch vielleicht ist der Mensch nur ein Zwischenwirt der Vernunft, NZZ 16.10.2020.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014 (zit. Simitis, BDSG/*Bearbeiter*).

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra/Albrecht, Jan Philipp (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, Baden-Baden 2019 (zit. Simitis/Hornung/Spiecker gen. Döhmann, DS-GVO/*Bearbeiter*).

Simoudis, Evangelos/Han, Jiawei/Fayyad, Usama M. (Hrsg.), Proceedings / Second International Conference on Knowledge Discovery & Data Mining, Menlo Park, Calif. 1996.

Skansi, Sandro, Introduction to deep learning – From logical calculus to artificial intelligence, Cham 2018.

Skistims, Hendrik, Rechtsgrundlagen für datenverarbeitende KI – 8.2, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, S. 352–378.

Skitka, Linda J./Mosier, Kathleen L./Burdick/Mark, Does automation bias decision-making?, Int. J. Hum. Comput. 51 (1999), S. 991–1006.

Smeddinck, Ulrich, Gesetzgebungsmethodik und Gesetzestypen, in: Kluth, Winfried/Krings, Günter u.a. (Hrsg.), Gesetzgebung – Rechtsetzung durch Parlamente und Verwaltungen sowie ihre gerichtliche Kontrolle, Heidelberg u.a. 2014, S. 69–93.

Smith, Craig S., Dealing With Bias in Artificial Intelligence, The New York Times 19.11.2019.

—, A.I. Here, There, Everywhere, The New York Times 23.02.2021.

Smith, Kerri, Taking aim at free will, Nature 477 (2011), S. 23–25.

Smuha, Nathalie A., From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence, Law Innov. Technol. 13 (2021), S. 57–84.

Solove, Daniel J., The digital person – Technology and privacy in the information age, New York, NY 2004.

—, Privacy Self-Management and the Consent Dilemma, Harv. L. Rev. 126 (2013), S. 1880–1903.

Solum, Lawrence B., Legal Personhood for Artificial Intelligences, N.C. L. Rev. 70 (1992), S. 1231–1288.

Sönnichsen, Birthe, Mein Helfer, der Pflege-Roboter, Tagesschau 10.03.2020.

Soon, Chun Siong/Brass, Marcel/Heinze, Hans-Jochen/Haynes, John-Dylan, Unconscious determinants of free decisions in the human brain, Nature neuroscience 11 (2008), S. 543–545.

Specht-Riemenschneider, Louisa/Bienemann, Linda, Informationsvermittlung durch standartisierte Bildsymbole, in: Specht-Riemenschneider, Louisa/Werry, Nikola u.a. (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2019, S. 324–344.

Specht-Riemenschneider, Louisa/Werry, Nikola/Werry, Susanne/Apel, Simon/Beyer-Katzenberger, Malte/Widjaja, Thomas (Hrsg.), Datenrecht in der Digitalisierung, Berlin 2019.

Spencer, Shaun B., The Problem of Online Manipulation, University of Illinois Law Review 2020, S. 959–1006.

Spiecker gen. Döhmann, Indra/Tambou, Olivia/Bernal, Paul/Hu, Margaret/Molinaro Corlos A./Negre, Elsa/Sarlet, Wolfgang I./Schertel Mendes, Laura/Witzleb, Normann/Yger, Florian, Multi-Country. The Regulation of Commercial Profiling– A Comparative Analysis, EDPL 2 (2016), S. 535–554.

Spiecker gen. Döhmann, Indra/Wallrabenstein, Astrid (Hrsg.), IT-Entwicklungen im Gesundheitswesen: Herausforderungen und Chancen, Frankfurt am Main u.a. 2016.

Spiekermann, S./Pallas, F., Technology paternalism – wider implications of ubiquitous computing, Poiesis & Praxis 4 (2006), S. 6–18.

Spindler, Gerald, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? – eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 20 (2015), S. 766–776.

—, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E) – Ansatz, Instrumente, Qualität und Kontext, CR 37 (2021), S. 361–374.

—, Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act – Teil 2: Große und besonders große Plattformen, Gewerblicher Rechtsschutz und Urheberrecht 123 (2021), S. 653–662.

—, Der Vorschlag für ein neues Haftungsregime für Internetprovider- der EU-Digital Services Act – Teil 1, Gewerblicher Rechtsschutz und Urheberrecht 123 (2021), S. 545–553.

Sprenger, Reinhard K., Ohne Moral geht es nicht. Aber wir moralisieren alles – und das ist falsch, NZZ 11.04.2018.

Staben, Julian, Der Abschreckungseffekt auf die Grundrechtsausübung – Strukturen eines verfassungsrechtlichen Arguments, Tübingen 2017.

Stach, Christoph/Steimle, Frank, Recommender-based privacy requirements elicitation – EPICUREAN, in: Association for Computing Machinery (Hrsg.), The 34th Annual ACM Symposium on Applied Computing, April 8–12, 2019, New York 2019, S. 1500–1507.

Stalla-Bourdillon, Sophie/Knight, Alison, Anonymous Data v. Personal Data – A False Debate – An EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Journal 34 (2017), S. 284–322.

Stark, Birgit, Don‘t be evil – Die Macht von Google und die Ohnmacht der Nutzer und Reguliere, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014, S. 1–19.

Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014.

Stark, Birgit/Magin, Melanie/Jürgens, Pascal, Navigieren im Netz – Befunde einer qualitativen und quantitativen Nutzerbefragung, in: Stark, Birgit/Dörr, Dieter/Aufenanger, Stefan (Hrsg.), Die Googleisierung der Informationssuche – Suchmaschinen zwischen Nutzung und Regulierung, Berlin/Boston 2014, S. 20–74.

—, Ganz meine Meinung? – Informationsintermediäre und Meinungsbildung – eine Mehrmethodenstudie am Beispiel von Facebook, Düsseldorf August 2017.

Stark, Birgit/Stegmann, Daniel, Are Algorithms a Threat to Democracy? – The Rise of Intermediaries: A Challenge for Public Discourse, AW AlgorithmWatch gGmbH, Berlin 26.05.2020, https://algorithmwatch.org/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf.

Statistika, Marktanteile von Social-Media-Seiten nach Seitenabrufen weltweit bis November 2022, https://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit/.

—, Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Januar 2022 Januar 2022, https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/.

—, Beliebteste soziale Netzwerke in Deutschland im Jahr 2022 November 2022, https://de.statista.com/prognosen/999733/deutschland-beliebteste-soziale-netzwerke.

—, Marktanteile von ausgewählten Suchmaschinen bei der Desktop-Suche und bei der mobilen Suche in Deutschland im November 2022 Dezember 2022, https://de.statista.com/statistik/daten/studie/301012/umfrage/marktanteile-der-suchmaschinen-und-marktanteile-mobile-suche/.

Steck, Harald/Baltrunas, Linas/Elahi, Ehtsham/Liang, Dawen/Raimond, Yves/Basilico, Justin, Deep Learning for Recommender Systems: A Netflix Case Study, AI Magazine 42 (2022), S. 7–18.

Steege, Hans, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz – Rechtsvergleichende Überlegungen und relevante Einsatzgebiete, MMR 22 (2019), S. 715–721.

Steinbach, Armin, Rationale Gesetzgebung, Tübingen 2017.

Steinbach, Kathrin, Regulierung algorithmenbasierter Entscheidungen 2021.

Stern, Stefan, Don't be deluded by the exaggerated claims made for AI, Financial Times 27.02.2023.

Stiemerling, Oliver, „Künstliche Intelligenz" – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge – Eine technische Perspektive, CR 2015, S. 762–765.

Stöcker, Christian/Lischka, Konrad, Wie algorithmische Prozesse Öffentlichkeit strukturieren, in: Mohabbat-Kar, Resa/Thapa, Basanta E.P./Parycek, Peter (Hrsg.), (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Berlin Juni 2018, S. 364–391.

Stone, Peter/Brooks, Rodney/Brynjolfsson, Erik/Calo, Ryan/Etzioni, Oren/Hager, Greg/Hirschberg, Julia/Kalyanakrishnan, Shivaram/Kamar, Ece/Kraus, Sarit/Leyton-Brown, Kevin/Parkes, David/Press, William/Saxenian, Anna Lee/Shah, Julie/Tambe, Milind/Teller, Astro, Artificial Intelligence and Life in 2030 – One Hundred Year Study on Artificial Intelligence September 2016, http://ai100.stanford.edu/2016-report.

Storr, Christine/Storr, Pam, Internet of Things – Right to Data from a European Perspective, in: Corrales, Marcelo/Fenwick, Mark/Forgó, Nikolaus (Hrsg.), New Technology, Big Data and the Law, Singapore 2017, S. 65–96.

Strahilevitz, Lior J., Towards a Positive Theory of Privacy Law, Harv. L. Rev. 126 (2013), S. 2010–2041.

Strahringer, Susanne/Wiener, Martin, Datengetriebene Geschäftsmodelle: Konzeptuelles Rahmenwerk, Praxisbeispiele und Forschungsausblick, HMD Praxis der Wirtschaftsinformatik 58 (2021), S. 457–476.

Strassemeyer, Laurenz, Die Transparenzvorgaben der DSGVO für algorithmische Verarbeitungen, K&R 16 (2016), S. 176–183.

—, Datenschutzrechtliche Transparenz von algorithmischen Entscheidungen und Verarbeitungen mittels Gamification, Ablaufdiagramme und Piktogramme, in: Taeger, Jürgen (Hrsg.), Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI, Edewecht 2019, S. 31–46.

Sunstein, Cass R., Echo chambers – Bush v. Gore, impeachment, and beyond, Princeton 2001.

—, Republic.com 2.0, Princeton 2007.

Susser, Daniel/Roessler, Beate/Nissenbaum, Helen F., Online Manipulation: Hidden Influences in a Digital World, GLTR 4 (2019), S. 1–45.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung – Handkommentar, 2. Aufl., Baden-Baden u.a. 2018 (zit. Sydow, DS-GVO/*Bearbeiter*).

Sydow, Gernot/Kring, Markus, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug – Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 4 (2014), S. 271–276.

Synodinou, Tatiana-Eleni/Jougleux, Philippe/Markou, Christiana/Prastitou, Thalia (Hrsg.), EU Internet Law – Regulation and enforcement, Cham 2017.

Taeger, Jürgen (Hrsg.), Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI, Edewecht 2019.

Taha, Walid M./Taha, Abd-Elhamid M./Thunberg, Johan, Cyber-Physical Systems: A Model-Based Approach, Cham 2021.

Taleb, Nassim Nicholas/Proß-Gill, Ingrid, Der schwarze Schwan – Die Macht höchst unwahrscheinlicher Ereignisse, München 2008.

Taub, Amanda, New technology, same old blind spot?, The New York Times 17.02.2023.

Taylor, Linnet/Floridi, Luciano/van der Sloot, Bart (Hrsg.), Group Privacy – New Challenges of Data Technologies, Cham 2017.

Temme, Merle, Algorithms and Transparency in View of the New General Data Protection Regulation, EDPL 3 (2017), S. 473–485.

Tene, Omer/Polonetsky, Jules, Big Data for All: Privacy and User Control in the Age of Analytics, Northwest. J. Technol. Intellect. Prop. 11 (2013), S. 239–274.

Teubner, Gunther, Digitale Rechtssubjekte?, AcP 218 (2018), S. 155–205.

The Metaphysics Research Lab, Stanford University (Hrsg.), The Stanford Encyclopedia of Philosophy, Stanford 2020.

Tietjen, Daniel/Flöter, Benedikt F., Dynamische und personalisierte Preise: Welche lauterkeitsrechtlichen Schranken gelten für Unternehmen?, GRUR-Prax 9 (2017), S. 546–548.

Tillmann, Tristan/Vogt, Verena, Personalisierte Preise im Big-Data-Zeitalter, VuR 33 (2018), S. 447–455.

Tinnefeld, Marie-Theres/Buchner, Benedikt/Petri, Thomas/Hof, Hans-Joachim (Hrsg.), Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht, 6. Aufl., Berlin/Boston 2018.

Tischbirek, Alexander, Artificial Intelligence and Discrimination: Discriminating Against Discriminatory Systems, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 103–121.

Tischbirek, Alexander/Wihl, Tim, Verfassungswidrigkeit des »Racial Profiling«: Zugleich ein Beitrag zur Systematik des Art. 3 GG, JZ 68 (2013), S. 219–224.

Tjoa, Erico/Guan, Cuntai, A Survey on Explainable Artificial Intelligence (XAI): Toward Medical XAI, IEEE transactions on neural networks and learning systems 32 (2021), S. 4793–4813.

Trute, Hans-Heinrich, Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 53 (1998), S. 822–831.

—, Innovationssteuerung im Wissenschaftsrecht, in: Hoffmann-Riem, Wolfgang/Schneider, Jens-Peter (Hrsg.), Rechtswissenschaftliche Innovationsforschung – Grundlagen, Forschungsansätze, Gegenstandsbereiche, Baden-Baden 1998, S. 208–245.

Tupay, Paloma K./Ebers, Martin/Juksaar, Jakob/Kohv, Kea, Is European Data Protection Toxic for Innovative AI? – An Estonia Perspective, Juridica International 30 (2021), S. 99–110.

Tutt, Andrew, An FDA for Algorithms, Admin. L. Rev. 69 (2016).

Tzanou, Maria, The fundamental right to data protection – Normative value in the context of counter-terrorism surveillance 2019.

Unger, Oliver, Grundfragen eines neuen europäischen Rechtsrahmens für KI, ZRP 53 (2020), S. 234–237.

Valkanova, Monika, Trainieren von KI-Modellen – Kapitel 8.1, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, S. 336–351.

Van den Daele, Wolfgang, Moralisierung in Technikkonflikten, in: Bogner, Alexander (Hrsg.), Ethisierung der Technik – Technisierung der Ethik – Der Ethik-Boom im Lichte der Wissenschafts- und Technikforschung, Baden-Baden 2013, S. 29–50.

van der Hof, Simone/Prins, Corien, Personalisation and its Influence on Identities, Behaviour and Social Values, in: Hildebrandt, Mireille/Gutwirth, Serge (Hrsg.), Profiling the European Citizen – Cross-Disciplinary Perspectives, Dordrecht/London 2008, S. 111–123.

van Ooijen, Iris/Vrabec, Helena U., Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective, J. Consum. Policy 42 (2019), S. 91–107.

van Otterlo, Martijn, A Machine Learning View on Profiling, in: Hildebrandt, Mireille/Vries, Katja de (Hrsg.), Privacy, due process and the computational turn – The philosophy of law meets the philosophy of technology, Abingdon 2013, S. 41–64.

Varošanec, Ida, On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI, Int. Rev. Law Comput. Technol. 36 (2022), S. 95–117.

Vatanparast, Roxana, Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy, ZaöRV 80 (2020), S. 819–845.

Veale, Michael/Edwards, Lilian, Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling, CLSR 34 (2018), S. 398–404.

Veale, Michael/Zuiderveen Borgesius, Frederik, Demystifying the Draft EU Artificial Intelligence Act, CRi 22 (2021), 97-112.

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip – Eine erste Bestandsaufnahme, ZD 5 (2015), S. 347–353.

—, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider – Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, NVwZ 37 (2018), S. 686–696.

—, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 71 (2018), S. 3337–3344.

Verband der TÜV e. V., Verbraucher:innen wollen Sicherheit und Transparenz bei Künstlicher Intelligenz, Verband der TÜV e. V., Berlin 27.01.2020, https://www.vdtuev.de/?tx_epxelo_file[id]=824710&cHash=5b6624273d780ebc87cafc44bc821a35.

Verbraucherzentrale Bundesverband, Neue Datenintermediäre – Anforderungen des vzbv an „Personal Information Management Systems" (PIMS) und Datentreuhänder, Bundesverband der Verbraucherzentralen und Verbraucherverbände 15.9.2020.

Victor, Daniel, Microsoft Created a Twitter Bot to Learn From Users. It Quickly Became a Racist Jerk., The New York Times 24.05.2016.

Vīķe-Freiberga, Vaira/Däubler-Gmelin, Herta/Hammersley, Ben/Pessoa Maduro, Luís Miguel Poiares, A free and pluralistic media to sustain European democracy – The Report of the High Level Group on Media Freedomand Pluralism, High Level Group on Media Freedomand Pluralism Januar 2013.

Vinge, Vinvent, The coming technological singularity – How to survive in the post-human era, San Diego State University, San Diego 01.12.1993, http://hdl.handle.net/2060/19940022856.

Voermans, Wim, Legislation and Regulation, in: Karpen, Ulrich/Xanthaki, Helen u.a. (Hrsg.), Legislation in Europe – A comprehensive guide for scholars and practitioners, Oxford/Portland 2017, S. 17–32.

Vogel, Paul, Künstliche Intelligenz und Datenschutz – Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze 2021.

Völker, Rainer, Wie Menschen entscheiden – Anspruch und Wirklichkeit, Stuttgart 2018.

Voßkuhle, Andreas, Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts – Methoden, Maßstäbe, Aufgaben, Organisation, Bd. 1, 2. Aufl., München 2012, Rn. 1–71.

Wachter, Sandra/Mittelstadt, Brent, A Right to Reasonable Inferences – Re-Thinking Data Protection Law in the Age of Big Data and AI, CBLR 2019, S. 494–620.

—, A Right to Reasonable Inferences: Re-Thinking Data Protection Law n the Age of Big Data and AI, CBLR 2019, S. 494–620.

Wachter, Sandra/Mittelstadt, Brent/Floridi, Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GeneralData Protection Regulation, Int. Data Priv. Law 7 (2017), S. 76–99.

Wachter, Sandra/Mittelstadt, Brent/Russell, Chris, Counterfactual Explanations without Opening the Black Box, Harv. J. Law Technol. 31 (2018), S. 841–887.

Wagner, Ben, Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems, Policy & Internet 11 (2019), S. 104–122.

Wagner, Ben/Janssen, Heleen, A first impression of regulatory powers in the Digital Services Act, Verfassungsblog 04.01.2021.

Wagner, Gerhard/Eidenmüller, Horst, In der Falle der Algorithmen? Abschöpfen von Konsumentenrente, Ausnutzen von Verhaltensanomalien und Manipulation von Präferenzen: Die Regulierung der dunklen Seite personalisierter Transaktionen, ZfPW 5 (2019), S. 220–246.

Wågström, Göran, Why Behavioral Advertising Should Be Illegal, Forbes 05.05.2019.

Wahlster, Wolfgang, Künstliche Intelligenz als Grundlage autonomer Systeme, Informatik Spektrum 40 (2017), S. 409–418.

Walch, Kathleen, Why The Race For AI Dominance Is More Global Than You Think, Forbes 9.2.2020.

Wallace, Elizabeth, Using AI for Dynamic Pricing – The Smarking Example, 20.9.2019, https://opendatascience.com/using-ai-for-dynamic-pricing-the-smarking-example/.

Wallace, Nick, Europe is about to lose the global AI race – thanks to GDPR, Euractive 25.5.2018.

Wallach, Wendell/Allen, Colin, Moral machines – Teaching robots right from wrong, Oxford 2009.

Wallau, Philipp, Die Menschenwürde in der Grundrechtsordnung der Europäischen Union, Göttingen 2010.

Walter, Axel von, Automatisierte Entscheidungsfindung (Art. 22 DSGVO) – Kapitel 8.4, in: Kaulartz, Markus/Braegelmann, Tom (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, München 2020, S. 391–402.

Walter, Sven, Illusion freier Wille? – Grenzen einer empirischen Annäherung an ein philosophisches Problem, Stuttgart 2016.

Wang, Chongren/Xiao, Zhuoyi, A Deep Learning Approach for Credit Scoring Using Feature Embedded Transformer, Applied Sciences 12 (2022), S. 1–14.

Wang, Pei, On defining Artificial Intelligence, J. Artif. Gen. 10 (2019), S. 1–37.

Waters, Richard, Artificial intelligence: A virtual assistant for life, Financial Times 22.2.2015.

Webb, Amy, The Big Nine – How the tech titans and their thinking machines could warp humanity, New York 2019.

Webb, Geoffrey I./Pazzani, Michael J./Billsus, Daniel, Machine Learning for User Modeling, User Modeling and User-Adapted Interaction 11 (2001), S. 19–29.

Weed, Julie, In the Race for Cheap Airfare, It's You vs. the Machine – Travel providers now use software to re-price their offerings, sometimes dozens of times a day, putting travelers at a big disadvantage., New York Times 28.01.2020, Section B, S. 4.

Weichert, Thilo, Big Data und Datenschutz – Chancen und Risiken einer neuen Form der Datenanalyse, ZD 3 (2013), S. 251–259.

—, Scoring in Zeiten von Big Data, ZRP 47 (2014), S. 168–171.

Weiser, Mark, The Computer for the 21st Century, Scientific American 265 (1991), S. 94–104.

Welbers, Kasper/Opgenhaffen, Michaël, Social media gatekeeping: An analysis of the gatekeeping influence of newspapers' public Facebook pages, New Media & Society 20 (2018), S. 4728–4747.

Wenhold, Céline, Nutzerprofilbildung durch Webtracking – Zugleich eine Untersuchung zu den Defiziten des Datenschutzrechts im Zeitalter von Big Data-Anwendungen, Baden-Baden 2018.

Werner, Kathrin, Robotergehirne brauchen Regeln, SZ 16.03.2018.

West, Sarah Myers, Data Capitalism: Redefining the Logics of Surveillance and Privacy, Business and Society 58 (2019), S. 20–41.

Wilson, Daniel H., Robocalypse – Roman, München 2011.

Wischmeyer, Thomas, Regulierung intelligenter Systeme, AöR 143 (2018), S. 1–66.

—, Artificial Intelligence and Transparency: Opening the Black Box, in: Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020, S. 75–101.

Wischmeyer, Thomas/Rademacher, Timo (Hrsg.), Regulating Artificial Intelligence, Cham 2020.

Wisniewski, Pamela J./Knijnenburg, Bart P./Lipford, Heather Richter, Making privacy personal: Profiling social network users to inform privacy education and nudging, Int. J. Hum. Comput. 98 (2017), S. 95–108.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Datenschutzrecht in Bund und Ländern – Grundlagen. Bereichsspezifischer Datenschutz. BDSG; Kommentar, München 2013 (zit. Wolff/Brink, BeckOK Datenschutzrecht/*Bearbeiter*).

— (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 44. Aufl., München 2023 (zit. Wolff/Brink, BeckOK Datenschutzrecht/*Bearbeiter*).

Wong, Janis/Henderson, Tristan, The right to data portability in practice: exploring the implications of the technologically neutral GDPR, IDPL 9 (2019), S. 173–191.

Wood, Molly, A New Kind of E-Commerce Adds a Personal Touch, New York Times 13.8.2014.

Wuttke, Laurenz, Machine Learning vs. Deep Learning – Wo ist der Unterschied?, https://datasolut.com/machine-learning-vs-deep-learning.

Yeung, Karen, 'Hypernudge': Big Data as a mode of regulation by design, iCS 20 (2017), S. 118–136.

—, Algorithmic Regulation: An Introduction, in: Yeung, Karen/Lodge, Martin (Hrsg.), Algorithmic regulation, 2019, S. 1–18.

—, Why Worry about Decision-Making by Machine?, in: Yeung, Karen/Lodge, Martin (Hrsg.), Algorithmic regulation, 2019, S. 21–48.

Yeung, Karen/Lodge, Martin (Hrsg.), Algorithmic regulation 2019.

Yeung, Karen/Weller, Adrian, How is 'transparency' understood by legal scholars and the machine learning community?, in: Bayamlıoğlu, İbrahim Emre/Baraliuc, Irina u.a. (Hrsg.), Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen, 2019, S. 36–40.

Yi, Yumi, Establishing the concept of AI literacy, European Journal of Bioethics 12 (2021), S. 353–368.

Yu, Peter K., The Algorithmic Divide and Equality in the Age of Artificial Intelligence, Flo. L. Rev. 72 (2020), S. 331–389.

Zahariev, Martin, The evolution of EU data protection law on automated data profiling,

Zalta, Edward N. (Hrsg.), The Stanford Encyclopedia of Philosophy, Standford 2020.

Zamboni, Mauro, Goals and Measures of Legislation: Evaluation, in: Jung, Heike/Jung-Müller-Dietz-Neumann (Hrsg.), Recht und Moral – Beiträge zu einer Standortbestimmung, Baden-Baden 1991, S. 109–129.

Zander-Hayat, Helga/Reisch, Lucia A./Steffen, Christine, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, S. 403–410.

Zarsky, Tal, „Mine your own business!": Making the case for the implications of the data mining of personal information in the forum of public opinion, Yale J.L. & Tech. 5 (2003), S. 1–65.

—, The Trouble with Algorithmic Decisions, Science, Technology, & Human Values 41 (2016), S. 118–132.

—, Incompatible: The GDPR in the Age of Big Data, Setton Hall Law Review 47 (2017), S. 995–1020.

—, Privacy and Manipulation in the Digital Age, Theoretical Inquiries in Law 20 (2019), S. 157–188.

Zech, Herbert, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung? – Gutachten A, München 2020.

Zoglauer, Thomas/Weber, Karsten/Friesen, Hans (Hrsg.), Technik als Motor der Modernisierung, Freiburg/München 2018.

Zuboff, Shoshana, The age of surveillance capitalism – The fight for the future at the new frontier of power, London 2019.

Zuiderveen Borgesius, Frederik, Improving Privacy Protection in the area of Behavioural Targeting, Alphen aan den Rijn 2015.

—, Discrimination, artificial intelligence, and algorithmic decision-making, Council of Europe, Straßburg 2018, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

—, Price Discrimination, Algorithmic Decision-Making, and European Non-Discrimination Law, European Business Law Review 31 (2020), S. 401–422.

Zuiderveen Borgesius, Frederik/Poort, Joost, Online Price Discrimination and EU Data Privacy Law, J. Consum. Policy 40 (2017), S. 347–366.

Zuiderveen Borgesius, Frederik/Trilling, Damian/Möller, Judith/Bodó, Balázs/Vreese, Claes H. de/*Helberger, Natali*, Should we worry about filter bubbles?, Internet Policy Rev. 5 (2016), S. 1–16.

Zukerman, Ingrid/Albrecht, David W., Predictive Statistical Models for User Modeling, User Modeling and User-Adapted Interaction 11 (2001), S. 5–18.

Sachregister