Prof. Dr. Mario Martini

Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staats-, Verwaltungs- und Europarecht
an der Deutschen Universität für Verwaltungswissenschaften Speyer,
Leiter des Programmbereichs „Digitalisierung“
am Deutschen Forschungsinstitut für öffentliche Verwaltung,
Mitglied der Datenethikkommission der Bundesregierung

GRUNDLINIEN EINES KONTROLLSYSTEMS FÜR ALGORITHMENBASIERTE ENTSCHEIDUNGSPROZESSE

– Gutachten im Auftrag des
Verbraucherzentrale Bundesverbandes* –

Stand: 1.5.2019

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Zitierempfehlung:

Martini, Kontrollsystem für algorithmenbasierte Entscheidungsprozesse, Speyer, 2019.

INHALTSVERZEICHNIS

A. Out of control? – Algorithmen als Steuerungslotsen der digitalen Welt

Wachsende Rechnergeschwindigkeiten, billigere und größere Speicherkapazitäten, allgegenwärtiger Zugang zum Internet und steigende Mediennutzung in der Bevölkerung machen es möglich: Informationstechnische Systeme sind zu zentralen Steuerungsinstanzen der digitalen Gesellschaft avanciert.[1] Immer nachhaltiger beeinflussen sie unser Leben:[2] Algorithmen helfen Verbrauchern bei der Suche nach dem besten Produkt, Arbeitgebern bei der Personalauswahl, Universitäten bei der Zuteilung ihrer Studienplätze. Sie treffen eigenständig Finanztransaktionsentscheidungen,[3] sagen vorher, welcher Patient voraussichtlich einen Herzinfarkt erleidet, komponieren Musikstücke, erstellen Comics, ja verfassen sogar selbsttätig wissenschaftliche Werke.[4]

Künstliche Intelligenz ist mehr als nur ein weiteres Element im Werkzeugkasten der Technik. Sie hinterlässt in unserem gesellschaftlichen Miteinander und seinen Regeln tiefe Spuren: Lernfähige Softwareanwendungen wirken in Echtzeit in das reale Leben hinein und übertreffen den Menschen bisweilen in seiner kognitiven Leistungskraft. So nimmt die kybernetische Vision einer Zukunft, in der Mensch und Maschine miteinander verschmelzen, Schritt für Schritt Gestalt an.

Die Funktionsweise algorithmenbasierter Entscheidungsprozesse gleicht aber teilweise einer Blackbox. Zum einen bedienen sie sich dynamischer Entscheidungsfindungsverfahren, die von außen – strukturbedingt – kaum mehr nachvollziehbar sind (etwa beim sog. *Deep Learning* mit künstlichen neuronalen Netzen). Zum anderen ist es bei proprietären Softwareanwendungen kraft des Schutzes

---

* Das Gutachten baut – insbesondere in Teil B (S. 8 ff.) – auf dem Aufsatz „Algorithmen als Herausforderung für die Rechtsordnung“ (*Martini*, JZ 2017, 1017 ff.) sowie auf der Monographie „Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz“ (Berlin et al., 2019) auf und integriert diese unmittelbar in die Darstellung. Um das Gutachten nicht zu überfrachten, hält es Literaturnachweise grundsätzlich schlank und verweist stattdessen auf die umfangreichen Literaturnachweise in der Monographie. Internetquellen sind auf dem Stand vom 14.4.2019. Der Verfasser dankt *Jonathan Hain, Matthias Hohmann, Michael Kolain, Anna Ludin*, *Jan Mysegades* und *David Nink* für die sehr gelungene Unterstützung.

[1] Zur wachsenden Bedeutung von Algorithmen bspw. *Coglianese/Lehr*, Georgetown Law Journal 105 (2017), 1147 (1149 ff.); *Hoffmann-Riem*, AöR 142 (2017), 1 (4 f.); *Tutt*, Administrative Law Review 69 (2017), 83 (84 ff.).

[2] *Martini*, JZ 2017, 1017 (1017).

[3] Siehe zu dem ausdifferenzierten normativen Regelungskonzept des algorithmischen Handels *Martini*, Blackbox Algorithmus, 2019, S. 146 ff.

[4] *Pluta*, Algorithmus schreibt wissenschaftliches Buch, golem.de vom 16.4.2019.

der Geschäftsgeheimnisse aus rechtlichen Gründen regelmäßig nicht möglich, im Ernstfall Einblick in den Programmcode zu nehmen.[5]

Algorithmen umweht zwar die Aura der Objektivität und Wahrheit. Sie sind aber keineswegs wertfrei. Vielmehr spiegeln sich in ihrer konkreten Funktionsweise die subjektiven Einstellungen ihrer Schöpfer wider.[6] In einer opak arbeitenden Entscheidungsstruktur lassen sich davon ausgehende *Diskriminierungsrisiken* nicht zuverlässig aufdecken. Eine unzutreffende Datengrundlage, fehlerhafter Code oder eine unsachgemäße Konfiguration eines Entscheidungssystems können sich sowohl auf die Rechte betroffener Personen als auch die Entfaltungschancen im Wettbewerb nachhaltig auswirken.[7]

Um die Risiken automatisierter Entscheidungen und ihre Vorstufen der computergestützten Entscheidungsvorbereitung[8] (zusammen: algorithmenbasierte Entscheidungsprozesse[9]) in grundrechtssensiblen Bereichen zu kontrollieren, ist eine „One size fits all"-Lösung zwar vergleichsweise leicht umsetzbar und deshalb reizvoll. Sie ginge jedoch an der komplexen Realität des Regelungsgegenstandes vorbei. Dafür sind die Erscheinungs- und Anwendungsformen algorithmenbasierter Entscheidungsprozesse in den vielfältigen Lebensbereichen und wirtschaftlichen Sektoren einer digitalisierten Gesellschaft zu disparat. Es bedarf vielmehr eines ausgewogenen Schutzsystems,[10] das sich

---

[5] Davon abzugrenzen ist sog. Open-Source-Software: Hier ist der Programmcode öffentlich zugänglich (etwa über GitHub.com). Es besteht dann zwar Transparenz über die Verarbeitungsgrundlage. Der Kreis der Personen, die eine Softwareanwendung gleichsam auf Herz und Nieren überprüfen können, weil sie die komplexen Zusammenhänge verstehen und einordnen können, ist jedoch verhältnismäßig klein. Hinzu kommt, dass jede Softwareanwendung jeweils einzelne Programmteile durch individuelle Konfigurationen erweitert. Der durchschnittliche Verbraucher ist deshalb letztlich auch bei offenem Programmcode auf eine Mittler- und Prüfinstanz im Umgang mit digitalen Anwendungen angewiesen.

[6] *Martini*, Blackbox Algorithmus, 2019, S. 48 ff.

[7] Zu den Risiken der Intransparenz, Diskriminierung und Monopolisierung von Markt- und Meinungsmacht bereits *Martini*, JZ 2017, 1017 (1017 ff.).

[8] Das Gutachten versteht „automatisierte Entscheidungen" insoweit in einem weiteren Umfang als in Art. 22 Abs. 1 DSGVO. Die Vorschrift erfasst nur solche Entscheidungen, in denen kein wesentliches menschliches Dazwischentreten (i. S. eines eigenen Entscheidungsbeitrags) stattfindet, vgl. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 22 DSGVO, Rn. 17.

[9] Gebräuchlich ist auch die Bezeichnung „ADM" – *algorithmic decision-making*.

[10] Zur intensiven Diskussion siehe etwa *Busch*, Algorithmic Accountability, 2018; *Ernst*, JZ 2017, 1026 (1026, 1031 ff.); *Herberger*, NJW 2018, 2825 (2826 ff.); *Hoffmann-Riem*, AöR 142 (2017), 1 (20 ff.); *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 132 ff.; *Schwintowski*, NJOZ 2018, 1601 (1606 ff.); *Wischmeyer*, AöR 143 (2018), 1 (18 ff.). Für die internationale Diskussion vgl. *Citron/Pasquale*, Washington Law Review 89 (2014), 1 ff.; *Edwards/Veale*, Duke Law & Technology Review 16 (2017), 18 (18 ff.) m. w. N. (insbesondere Fn. 4), welche die politische Debatte mit der Diskussion zur unsichtbaren Hand des Marktes im 19. Jahrhundert vergleichen (19 f.); *Pasquale*, The Black Box Society, 2015; *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (239 ff.); *Tufekci*, Colorado Technology Law Journal 13 (2015), 203 (203 ff.). Bezogen auf den Anwendungsfall „Autonome Fahrzeuge" etwa *Gasser*, Grundlegende und spezielle Rechtsfragen für

aus einem Set ausdifferenzierter, passgenauer Regulierungsinstrumente zusammensetzt.[11] Auf seiner Grundlage sollte der Gesetzgeber die einzelnen gesetzlichen Pflichten mit der jeweiligen Gefahrenlage synchronisieren, die sich mit spezifischen Anwendungsformen und Geschäftsfeldern verbindet.

Vor dieser Hintergrundfolie entwickelt das Gutachten ein verbraucherpolitisches Regulierungskonzept, das sich der Zielsetzung verschreibt, Betroffene im Einzelfall angemessen zu schützen, ohne die wirtschaftlichen Chancen neuer Technologien zu verkennen. Jede zusätzliche Regulierung sollte dabei insbesondere immer auch den (bürokratischen) Aufwand für (insbesondere kleinere und mittlere) Unternehmen sowie gemeinnützige Vereine antizipieren und auf das notwendige Maß beschränken. Wie sich die denkbaren Ansatzpunkte im Einzelnen zu einem Gesamtkonzept zusammenfügen und auf welche Akteure sie zugreifen sollen, um die Risiken, welche Algorithmen und Künstliche Intelligenz in den Alltag der Verbraucher hineintragen, ethisch-rechtlich einzuhegen, ist im Kern eine Frage gesellschaftlich-politischer Verständigung. Das Gutachten macht sich zur Aufgabe, die Debatte um einige Facetten zu bereichern.

B. Regulierungsinstrumente

I. Transparenzanforderungen

Der fehlende Einblick in das Arsenal einer Softwareanwendung entwaffnet Betroffene. Ob eine algorithmenbasierte Entscheidung sachgerecht ist, kann nämlich nur prüfen, wer die Datengrundlage, Handlungsabfolge und Gewichtung der Entscheidungskriterien kennt – und versteht.[12] Aus diesem Grunde etabliert die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) das Gebot der Transparenz ausdrücklich als einen ihrer zentralen Grundsätze („in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“ – Art. 5 Abs. 1 lit. a DSGVO). Transparenz ist eine notwendige Grundbedingung, um Vertrauen in informationstechnische Systeme aufzubauen und

autonome Fahrzeuge, in: Maurer/Gerdes/Lenz et al. (Hrsg.), Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, 2015, S. 543 (556 ff.); mit Blick auf die Autocomplete-Funktion von *Google Search* siehe *Kastl*, GRUR 2015, 136 (136 ff.); *Müller-Hengstenberg/Kirn*, MMR 2014, 307 (307 ff.). Zu Diskriminierungen durch datengestützte Einstellungsassistenten im Arbeitsrecht *von Lewinski/de Barros Fritz*, NZA 2018, 620 (620 ff.). Für den Unterbereich Robotik vgl. *Beck*, JR 2009, 225 (225 ff.); *Spranger/Wegmann*, Öffentlich-rechtliche Dimensionen der Robotik, in: Beck (Hrsg.), Jenseits von Mensch und Maschine, 2012, S. 105 (105 ff.).

[11] Gemeint ist dabei keine kumulative Umsetzung aller denkbaren Regulierungsinstrumente, sondern ein Baukasten denkbarer Reformansätze, die Anwendung finden können, soweit sie im Einzelfall sachgerecht sind.

[12] *Martini*, JZ 2017, 1017 (1018).

eine informierte Entscheidung treffen zu können. Um den Einzelnen nicht vollständig über den Inhalt algorithmenbasierter Verfahren im Unklaren zu lassen, legt die DSGVO den datenschutzrechtlich Verantwortlichen in ihren Art. 12 ff. weitreichende Informations- und Auskunftspflichten auf.[13] Im Ergebnis bleibt das Pflichtenheft des neuen Datenschutzrechts aber hinter dem rechtspolitisch Wünschenswerten noch zurück.

1. Ex-ante-Kennzeichnungs- und Informationspflicht

a) Status quo de lege lata

Für (voll)automatisierte Entscheidungsverfahren etablieren Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DSGVO eine besondere Informationspflicht des Verantwortlichen.[14] Die Vorschriften tragen ihm nicht nur auf, Betroffene über „das Bestehen einer automatisierten Entscheidungsfindung" zu informieren, den Einsatz solcher Verfahren also zu *kennzeichnen*.[15] Er muss ihnen auch – zumindest in den Fällen des Profilings[16] – aussagekräftige Informationen zu den Modalitäten der Verarbeitung an die Hand geben: Sowohl die *involvierte Logik* sowie die *Tragweite* als auch auf die angestrebten *Auswirkungen* einer *vollständig automatisierten Verarbeitung* hat er offenzulegen (vgl. auch ErwGrd 60 S. 1 und 2).

In den offenen „Kelch der Verbraucherhoffnungen" schenkt die DSGVO jedoch auch einen Wermutstropfen ein: Die Kennzeichnungs- und Informationspflichten gelten nicht vorbehaltlos. Die Normen verweisen vielmehr auf Art. 22 DSGVO. Damit schränken sie die normative Reichweite des Pflichtengehalts erheblich ein: Sie treffen den datenschutzrechtlich Verantwortlichen nur, soweit Gegenstand der Verarbeitung *eine vollständig automatisierte Entscheidungsfindung* ist.[17] Einer er-

[13] Zur Systematik der Betroffenenrechte im Überblick, vgl. *Franck*, RDV 2016, 111 (111 ff.).
[14] Ihr steht ein inhaltlich deckungsgleiches Auskunftsrecht des Betroffenen gegenüber (Art. 15 Abs. 1 lit. h DSGVO); siehe auch *Martini*, Blackbox Algorithmus, 2019, S. 177 ff. sowie unten S. 13 f.
[15] Eine ähnliche Kennzeichnungspflicht kennt das Recht des Hochfrequenz- und algorithmischen Handels bereits. Sie soll zum einen für höhere Informationstransparenz sorgen, die Aufsicht erleichtern sowie die Regelkonformität flankierend absichern, vgl. § 16 Abs. 2 Nr. 3 BörsG und § 72 Abs. 1 Nr. 10 WpHG; näher *Martini*, Blackbox Algorithmus, 2019, S. 151.
[16] Der genaue Sinngehalt des Einschubs „zumindest in diesen Fällen" gibt Rätsel auf (dazu ausführlich *Martini*, Blackbox Algorithmus, 2019, S. 182 ff.). Aus ErwGrd 63 S. 3 DSGVO lässt sich schließen, dass der Unionsgesetzgeber die Informationspflicht zur Logik und Tragweite nur in den Fällen absolut setzen wollte, „in denen die Verarbeitung auf Profiling beruht" (vgl. auch ErwGrd 60 S. 3 DSGVO). Denkbar ist aber auch eine etwas weitere Auslegung: Die Informationspflicht greift dann nicht nur im Falle des Profilings, sondern bei *allen* (vollständig) automatisierten Verfahren. Der Wortlaut der Vorschriften lässt jedenfalls Raum für beide Deutungen.
[17] *Martini*, JZ 2017, 1017 (1020).

weiterten Informationspflicht unterliegen also lediglich Entscheidungen, die *ohne jeglichen (entscheidenden) menschlichen Einfluss* zustande kommen[18] – nicht aber die algorithmenbasierte *Unterstützung* menschlicher Entscheidungen.[19] Dadurch hinterlässt die DSGVO eine spürbare Regulierungslücke; ein wirksames Algorithmenkontrollregime für Szenarien, in denen eine Softwareanwendung die Entscheidung eines Menschen lediglich vorbereitet oder unterstützt, fehlt.[20]

b) Handlungsempfehlung de lege ferenda

Pro futuro sollte die Rechtsordnung dem Katalog an Informationspflichten größere Reichweite verschaffen: Sowohl die Kennzeichnungspflicht als auch die Pflicht, den Betroffenen Informationen darüber zu vermitteln, welche Logik und Tragweite ein algorithmisches Verfahren hat, sollten de lege ferenda im Grundsatz *bei allen grundrechtssensiblen Softwareanwendungen*[21] greifen[22] – etwa bei der Kreditvergabe auf der Grundlage eines Score-Wertes oder bei Profiling-Verfahren, wenn bspw. ein soziales Netzwerk Menschen in Persönlichkeitskategorien einteilt.[23] Das gilt umso mehr in Fällen, in denen der Einzelne ohne oder sogar gegen seinen Willen zum Objekt computergestützter Datenauswertungen wird – bspw. wenn der *Staat* Scoring-Software nutzt, um über Maßnahmen der Berufsförderung für Arbeitslose zu entscheiden.[24]

Eine (obligatorische) Kennzeichnung muss der Verbraucher auch ohne Schwierigkeiten tatsächlich erfassen können, wenn sie Sinn stiften soll. Sie muss dafür mehr sein als ein störender oder umständlich formulierter Datenschutzhinweis, den Verbraucher außer Acht lassen. Deshalb empfiehlt

[18] Eine bloß formale menschliche Entscheidung, die nicht auf die inhaltliche Entscheidung Einfluss nimmt, also ein bloßes „Abzeichnen“ lässt Art. 22 Abs. 1 DSGVO greifen, vgl. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 22 DSGVO, Rn. 17.
[19] *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 22 DSGVO, Rn. 16 ff.; *Martini*, JZ 2017, 1017 (1020).
[20] Anders verhält es sich bei der Regulierung des algorithmischen Handels mit Finanzinstrumenten. Hier unterwirft der Normgeber die Finanzdienstleistungsunternehmen auch den algorithmenspezifischen Pflichten, wenn deren algorithmische Softwarehandelssysteme lediglich bestimmen, dass ein Mensch den Auftrag eingeschränkt weiterbearbeiten soll, Art. 4. Abs. 1 Nr. 39 RL 2014/65/EU vom 15.5.2014, ABl. Nr. L 173 v. 12.6.2014, S. 349 i. V. m. Art. 18 der Delegierten Verordnung (EU) Nr. 2017/565 vom 25. April 2016, ABl. L 87 vom 31.3.2017, S. 1.
[21] Zu einem Ansatzpunkt, um die Grundrechtssensibilität im Einzelfall zu konkretisieren, siehe unten S. 45 ff.
[22] Siehe bereits *Martini*, JZ 2017, 1017 (1020); zustimmend *Busch*, Algorithmic Accountability, 2018, S. 58 ff. und *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 161. Die Kennzeichnungspflicht als Gebot von „Fairness und Gerechtigkeit” verstehend *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (271).
[23] Zu inhaltlichen Anforderungen an die Zulässigkeit des Profilings siehe unten S. 19 ff.
[24] So ist es in Österreich geplant; siehe dazu bspw. *Fanta*, Österreichs Jobcenter richten künftig mit Hilfe von Software über Arbeitslose, netzpolitik.org vom 13.10.2018.

sich eine flankierende Pflicht, *visuell leicht erfassbare Symbole* für die Kennzeichnung zu verwenden.[25] Die DSGVO steht standardisierten Bildsymbolen zwar aufgeschlossen gegenüber (Art. 12 Abs. 7 S. 1 DSGVO). Sie stellt es aber in das Ermessen des Verantwortlichen, von ihnen Gebrauch zu machen. Perspektivisch ist es auch denkbar, verschiedene algorithmenbasierte Systeme – ähnlich wie bei der Energieeffizienzklassifizierung oder der Hygieneampel für Gastronomiebetriebe – nach ihrer Grundrechtssensibilität in einem Ampelsystem zu rastern und das Ergebnis (etwa „hohe Sensibilität“) dem Verbraucher leicht erfassbar mitzuteilen. Art. 13 Abs. 2 bzw. Art. 14 Abs. 2 DSGVO könnte nach dem Vorbild der folgenden Grundidee eine Ergänzung erfahren:

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten: […]

g) [bzw. h)] bei grundrechtssensiblen[26] Softwareanwendungen den Hinweis darauf, dass eine algorithmenbasierte Auswertung erfolgt, sowie aussagekräftige Informationen über die involvierte Logik und Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

2. Ex-post-Information

a) Begründungspflicht

Entscheidungsergebnisse einer Softwareanwendung sind für einen Nutzer nicht schon dann vollständig nachvollziehbar, wenn er *ex ante* abstrakte Informationen zu den wesentlichen Entscheidungsparametern erhält. Verstehen wird er sie vielmehr erst dann, wenn er Gründe dafür erkennt, warum das System in seinem konkreten Fall so und nicht anders entschieden hat – insbesondere wenn es seinen Antrag ablehnt. Um diesem Bedürfnis nachzukommen, könnte der Gesetzgeber den Verantwortlichen verpflichten, die konkreten Entscheidungsergebnisse gegenüber Betroffenen zu erläutern. Anders als im Falle einer Informationspflicht i. S. d. Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DSGVO (die grundsätzlich vor der Verarbeitung greift) müsste der Verantwortliche dann nicht

[25] *Martini*, JZ 2017, 1017 (1020); zustimmend *Busch*, Algorithmic Accountability, 2018, S. 59; kritisch zur Frage der inhaltlichen Ausgestaltung einer Kennzeichnungspflicht *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 162.

[26] Das Tatbestandsmerkmal der „Grundrechtssensibilität“ bedürfte dann einer (Legal-)Definition und einer Konkretisierung im Wege delegierter Rechtsetzung (dazu unten S. 45 ff.).

nur die Funktionsweise des algorithmenbasierten Entscheidungsprozesses *allgemein* beschreiben. Vielmehr müsste er das individuelle Ergebnis nachvollziehbar machen, nachdem es ergangen ist.

aa) Rechtslage de lege lata

Eine einzelfallbezogene Begründungspflicht für algorithmenbasierte Entscheidungen ist der DSGVO bislang unbekannt: Eine solche erwächst weder unmittelbar aus Art. 22 Abs. 3 DSGVO (als Teil der Pflicht, für vollständig automatisierte Entscheidungen Schutzmaßnahmen zu treffen) noch lässt sie sich aus ErwGrd 71 UAbs. 1 S. 4 DSGVO[27] oder als Element der Auskunfts- und Informationspflichten (Art. 12 ff. DSGVO) hinreichend klar als allgemeine Pflicht aus der DSGVO herauslesen.[28]

bb) Empfehlung de lege ferenda

Eine Begründungspflicht kann einerseits dann hilfreiche Transparenzimpulse setzen, wenn eine Softwareanwendung Entscheidungen vollautomatisiert selbst trifft. Nichts anderes gilt andererseits in den Fällen, in denen sie in einen (menschlichen) Entscheidungsprozess – etwa als Assistenzsystem – integriert ist. Eine Begründung lässt den Betroffenen dann so weit in die Blackbox hineinblicken, wie es erforderlich und angemessen ist, um die Grundlagen der Entscheidung nachvollziehen und sie ggf. anfechten zu können.[29]

cc) Grenzen einer Begründungspflicht

Systemen maschinellen Lernens eine Begründung für ihre Entscheidungen abzuringen, ist bislang nicht nur technisch außerordentlich anspruchsvoll. Eine solche Pflicht leitet auch einen Paradigmenwechsel ein: In privatrechtlichen Rechtsgeschäften müssen Vertragspartner die Erwägungen, die sie

[27] Der Erwägungsgrund spricht zwar von einem Recht „auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung". Diese Wendung findet sich aber in dem verfügenden Teil der Verordnung (der alleine materielle Pflichten auslösen kann) nicht wieder. Das hat seinen tieferen Grund: Die Formulierung ist dahin zu verstehen, dass die DSGVO dem Verantwortlichen nicht generell eine Erläuterung abverlangt, sondern nur dann, wenn der Betroffene von seinem Recht Gebrauch gemacht hat, seinen eigenen Standpunkt darzulegen. Das deutet der Passus „nach einer entsprechenden Bewertung" („*reached after such an assessment*") an. Sie rekurriert grammatisch auf die Darlegung des eigenen Standpunkts, bezieht sich damit also auf einen engen Radius denkbarer Fälle. Hat der Verantwortliche Betroffenen die Möglichkeit eröffnet, ihre Einwände vorzubringen und eine Erläuterung zu erhalten, ob und wie diese Berücksichtigung gefunden haben, sieht der Unionsgesetzgeber ihre Interessen hinreichend berücksichtigt. Dazu auch *Martini*, Blackbox Algorithmus, 2019, S. 191.

[28] Dazu im Einzelnen *Martini*, Blackbox Algorithmus, 2019, S. 190 ff.

[29] Dazu auch *Mittelstadt/Allo et al.*, Big Data & Society 2016, 1 (7); eine Begründungspflicht gegenüber einer Kontrollbehörde fordert *Tutt*, Administrative Law Review 69 (2017), 83 (110).

zu einem Verhalten veranlasst haben, grundsätzlich nicht offenlegen – auch nicht bei Entscheidungen, die auf einem komplexen Motivbündel beruhen.[30] Selbst das AGG verlangt Privatrechtssubjekten in diskriminierungsanfälligen Kontexten nicht zwingend ab, ihre Entscheidungen zu begründen.

Ebenso wie in der analogen sollte auch in der digitalen Welt Private (anders als den Staat, § 39 VwVfG) aber nicht generell eine Begründungspflicht treffen. Eine solche lässt sich im Grundsatz nur durch die *strukturelle Eigenart algorithmenbasierter Entscheidungen* legitimieren:[31] Ihren Prozessen unterlaufen im Vergleich zum Menschen andere, bisweilen überraschende Fehler.[32] Sie operieren auf einer quantitativen Grundlage phänotypischer Ähnlichkeiten und stochastischer Schlüsse: Algorithmen erkennen Korrelationen, aber keine Kausalzusammenhänge. Dort, wo sich das Fehlerrisiko von Fehlschlüssen der Scheinkausalität oder sonstiger struktureller Risiken algorithmenbasierter Verfahren verwirklicht und die Grundrechte aufgrund der sensiblen Wirkungen der Entscheidung ein besonderes Schutzbedürfnis auslösen, ist eine Begründungspflicht sachgerecht. Dies gilt vor allem dann, wenn der Entscheidung in persönlichkeitsrechtlich sensiblen Feldern rechtliche Wirkung zukommt.[33]

Eine Pflicht, algorithmenbasierte Entscheidungen zu begründen, findet auch dort ihre Grenze, wo sie Geschäftsgeheimnisse, insbesondere den Quellcode eines Entscheidungssystems, ans Licht der Öffentlichkeit[34] bringt oder sonstige überwiegende, grundrechtsrelevante Interessen Dritter entgegenstehen (etwa wenn eine Begründung auch Informationen über mittelbar Betroffene, z. B. personenbezogene Daten der Referenzgruppe, offenlegt).[35]

[30] *Martini*, Blackbox Algorithmus, 2019, S. 192 f.
[31] *Martini*, Blackbox Algorithmus, 2019, S. 195 ff.; *Hoeren/Niehoff*, RW 9 (2018), 47 (57 ff.).
[32] Einen Überblick über Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung liefert *Zweig*, Wo Maschinen irren können, 2018, S.21 ff.
[33] Siehe dazu im Einzelnen unten S. 45 ff.
[34] Anders verhält es sich, wenn hinreichende Vorkehrungen für den Schutz der Geheimnisse bestehen – etwa durch eine behördliche Überprüfung unter Wahrung der Geheimhaltung. Noch weitergehend fordern *Whittaker/Crawford et al.*, AI Now Report 2018, Dezember 2018, S. 22 von Unternehmen, dass sie auf den Schutz ihrer Geschäftsgeheimnisse bei algorithmischen Systeme verzichten, um effektive externe Kontrollen zu ermöglichen. Zum urheber-, patentrechtlich und geheimnisschutzrechtlichen Status quo, vgl. *Martini*, Blackbox Algorithmus, 2019, S. 33 ff.
[35] *Martini*, Blackbox Algorithmus, 2019, S. 197; zustimmend *Busch*, Algorithmic Accountability, 2018, S. 60.

b) Recht auf Einblick in die Daten- und Entscheidungsgrundlage

aa) De lege lata

Die DSGVO verleiht Betroffenen das Recht, (kostenfrei) in die Datengrundlage Einblick zu nehmen: Der Verantwortliche muss ihnen neben Informationen über die Verarbeitung (Art. 15 Abs. 1 DSGVO) auch eine Kopie seiner personenbezogenen Daten, die Gegenstand der Verarbeitung sind (Art. 15 Abs. 3 DSGVO), zur Verfügung stellen.[36] Dadurch können Betroffene überprüfen, ob alle Daten, die in die Entscheidung eingeflossen sind, korrekt, vollständig und aktuell sind.[37]

Ein Einblick in die Klassifikationen, die ein Profiling-Instrument über einen Menschen im Einzelfall getroffen hat („emotional stabil", „konservativ", „mit einer Wahrscheinlichkeit von 70 % homosexuell"), geht damit jedoch nicht ohne Weiteres einher. Das Auskunftsrecht erstreckt sich im Grundsatz auf die Daten, die Eingang in den Verarbeitungsprozess gefunden haben, nicht aber auch in vollem Umfang auf das Verarbeitungsergebnis.[38] Das Auskunftsrecht findet seine Grenze nach dem Willen des Unionsgesetzgebers insbesondere an den Rechten „und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse[n] oder Rechte[n] des geistigen Eigentums" sowie der Meinungs- und Berufsfreiheit (ErwGrd 63 S. 5, Art. 15 Abs. 4 i. V. m. Abs. 3 und 1 DSGVO).

Auch aus dem Berichtigungsanspruch des Art. 16 S. 1 DSGVO erwächst Betroffenen kein Recht darauf, Einblick in eine Profilbewertung zu erhalten und deren Berichtigung zu verlangen.[39] Dieser Anspruch richtet sich seinem Sinn nach auf die Daten*grundlage*, die einer Richtigkeitsprüfung nach

[36] Auf der Grundlage des Art. 15 Abs. 3 DSGVO hat das LAG Baden-Württemberg bspw. jüngst einen Arbeitgeber dazu verpflichtet, einem Mitarbeiter eine Kopie sämtlicher ihn betreffender „Leistungs- und Verhaltensdaten" zur Verfügung zu stellen (Urt. v. 20.12.2018, Az. 17 Sa 11/18, Rn. 203 ff.); vgl. hierzu *Härting*, Mit der DSGVO zum "Golden Handshake" – von der Sprengkraft des "Rechts auf Kopie", https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/ (02.04.2019).

[37] Vgl. auch sub specie vollständig automatisierter Entscheidungen i. S. d. Art. 22 DSGVO: ErwGrd 71 UAbs. 2 S. 1 DSGVO mit dem Gebot, „technische und organisatorische Maßnahmen" zu „treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Strukturen, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden"; zur weitergehenden französischen Regelung *Martini*, Blackbox Algorithmus, 2019, S. 186.

[38] Dazu im Einzelnen *Martini*, Blackbox Algorithmus, 2019, S. 199 ff.

[39] Demgegenüber kann das Recht auf Löschung (Art. 17 Abs. 1 DSGVO) auch die Ergebnisse eines Datenverarbeitungsprozesses umfassen (also z. B. die Resultate eines Profilings); so auch *Kamann/Braun*, in: Ehmann/Selmayr (Hrsg.), DSGVO, 2. Aufl., 2018, Art. 17, Rn. 36. Allerdings nützt Art. 17 Abs. 1 DSGVO dem Adressaten algorithmenbasierter Entscheidungen nur in den Fällen, in denen der Verantwortliche noch keine Entscheidung gefällt hat und dem Betroffenen somit Gelegenheit bleibt, die Löschung der Daten zu verlangen. Der Verantwortliche darf dann, wenn ein Löschungsgrund vorliegt (Art. 17 Abs. 1 lit. a bis lit. f DSGVO), seine Entscheidung dann nicht mehr auf diese Datengrundlage stützen. Ein Recht, in algorithmenbasierte Profilergebnisse Einblick zu nehmen oder dem Verantwortlichen abzuverlangen, eine algorithmenbasierte Entscheidung nachträglich zu korrigieren, die er auf Grundlage personenbezogener Daten getroffen hat, statuiert Art. 17 Abs. 1 DSGVO hingegen nicht.

intersubjektiv überprüfbaren Kriterien zugänglich ist („richtiger personenbezogener Daten", Art. 16 S. 1 DSGVO). Die DSGVO etabliert insoweit nicht stillschweigend ein Recht, anderen abzuverlangen, die Meinung offenlegen zu müssen, die sie sich als Folge eines Verarbeitungsprozesses über andere gebildet haben.[40]

bb) De lege ferenda – Recht auf sachgerechte algorithmische Schlussfolgerungen?

Ein Regulierungsansatz, der das Ziel verfolgt, algorithmische Verfahrensmuster verständlich zu machen, kann auch über die Entscheidungsgrundlagen der Verarbeitung hinausreichen: Die Rechtsordnung ist gut beraten, nicht nur *Verarbeitungsprozesse* mit personenbezogenen Daten, sondern auch und gerade die *Folgerungen* in den Blick zu nehmen, die am Ende der Verarbeitung bestimmter Daten stehen[41] – insbesondere dann, wenn eine Softwareanwendung, die auch die Präferenzen eines Nutzers prognostiziert, im Ergebnis rufschädigend wirken kann und kaum überprüfbar ist.[42] Der Schutz richtet sich dann nicht mehr alleine – wie grundsätzlich im Konzept des Art. 15 Abs. 1, Abs. 3 S. 1 DSGVO – auf den Daten-Input. Der rechtliche Blick fällt dann vielmehr auch auf den Daten-Output, also die Verarbeitungsergebnisse, insbesondere algorithmische Schlussfolgerungen (sog. Inferenzen), sowie Referenzdatensätze.[43] Schließt bspw. ein Algorithmus aus dem Umstand, dass ein Nutzer einer Online-Plattform den Mauszeiger nur langsam bewegt, auf eine geringe Kundenzufriedenheit, kann diese Hypothese in tatsächlicher Hinsicht angreifbar sein (etwa weil der Nutzer schlicht müde oder seine Hardware langsam ist) – und schlimmstenfalls auch Rechte verletzen. Denkbar ist es insofern, dem Einzelnen die Möglichkeit zu eröffnen, die Kontrolle über algorithmische Klassifizierungen, die ihn betreffen, zu erlangen: Dann könnte er Inferenzen, die nicht verifizierbar sind oder eine hohe Fehleranfälligkeit aufweisen, gegenüber einem Verantwortlichen bestreiten. Damit der Betroffene ein solches Recht effektiv ausüben kann, müsste der Anbieter nicht nur erklären, warum die Daten für eine Schlussfolgerung erforderlich sind und diese wiederum für

[40] Etwas anderes gilt auch nicht für das Widerspruchsrecht im Sinne des Art. 21 Abs. 1 S. 1 DSGVO. Es räumt dem Betroffenen nicht die Möglichkeit ein, inhaltlich Einfluss auf das Ergebnis der Datenverarbeitung zu nehmen. Die Vorschrift betrifft vielmehr das „Ob" einer Datenverarbeitung, nimmt also einer Verarbeitung ggf. die grundsätzlich bestehende Rechtsgrundlage aus Art. 6 DSGVO.

[41] *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (270 f.); *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (1 ff.) des Typoskripts.

[42] *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (3) des Typoskripts.

[43] Zur Problematik statistischer Inferenzen und Referenzdatensätze auch *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 35; dazu und zum Folgenden auch *Martini*, Blackbox Algorithmus, 2019, S. 205 f.

den Entscheidungsprozess relevant ist. Er müsste auch erläutern, ob die Methoden der Datenerhebung sowie der Schlussfolgerung verlässlich sind.[44] Rechtstechnisch könnte der Gesetzgeber eine solche Vorgabe prinzipiell dadurch konstruieren, dass er die bestehenden *Informationspflichten* der Anbieter algorithmischer Anwendungen inhaltlich erweitert.[45]

Ein subjektives Recht, Einblick in Profilbildungsmaßnahmen zu nehmen, schießt allerdings ebenso wie ein Recht auf bestimmte Entscheidungs*ergebnisse* schnell über das Ziel hinaus: Die Rechtsordnung kennt zwar ein Recht auf Selbstdarstellung des Einzelnen als Teil seines Allgemeinen Persönlichkeitsrechts,[46] nicht aber ein Recht darauf, dass Dritte die eigene Person in einer bestimmten Weise sehen. Weder in der analogen noch in der digitalen Welt ist ein solches Recht für einen wirksamen Persönlichkeitsschutz generell geboten (auch wenn etwa eine tiefschürfende Big-Data-Analyse das Risiko für die Privatheitsentfaltung erhöht). Entscheidend ist vielmehr, dass die Modellannahmen, auf denen Profiling-Wertungen beruhen, valide sind. Diese Prüfung ist in den Händen einer Aufsichtsbehörde am besten verortet. Sie bringt die entscheidenden Kenntnisse mit, um nicht nur im Einzelfall zuverlässig prüfen zu können, welche Daten in ein Modell nicht eingehen dürfen und welche Schlussfolgerungen unter welchen Voraussetzungen zulässig und gerechtfertigt sind. Ein individuell einklagbares Recht auf sachgerechte Schlussfolgerungen kollidiert insbesondere mit den berechtigten Geheimhaltungsinteressen und der grundsätzlichen Entscheidungsfreiheit des Softwareanwenders (als Ausdruck seiner wirtschaftlichen Entfaltungsfreiheit), ohne für einen wirksamen Persönlichkeitsschutz zwingend erforderlich zu sein. Es ist auch nur bedingt sinnstiftend, wenn private Betroffene mit einem Anbieter in eine Diskussion darüber einzutreten versuchen, ob dessen Einstufungen mit der eigenen Einschätzung übereinstimmen. Wertungen sind intersubjektiv nicht überprüfbar und damit grundsätzlich nicht einklagbar.[47] Wirksamer als ein Recht darauf, zu erfahren, was jemand oder ein Computer über eine andere Person „denkt“, oder ein Recht auf sachgerechte Schlussfolgerungen in das Repertoire der Rechtsordnung aufzunehmen, ist bei genauerem

[44] *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (57 f.) des Typoskripts; ähnlich in Bezug auf die Einführung von Positivlisten mit entscheidungsrelevanten und sachlich gerechtfertigten Attributen *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 91.
[45] *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (57 f.) des Typoskripts; die Autoren befürworten auch den Regelungsgehalt aus § 28 BDSG a. F., wollen jedoch zusätzlich eine Informationspflicht etablieren; a. a. O, 60 f.
[46] Dazu gehören insbesondere das Recht am eigenen Bild, am eigenen Wort und am eigenen Namen sowie das Recht auf Gegendarstellung; vgl. dazu bspw. *Martini*, JA 2009, 839 (841).
[47] So gewährt die Rechtsordnung dem Einzelnen auch kein gerichtlich durchsetzbares Recht, rufschädigende Meinungen widerrufen zu lassen. Der Einzelne kann ausschließlich deren Unterlassung für die Zukunft verlangen. Vgl. dazu ergänzend *Martini/Kühl*, Jura 2014, 1221 (1227).

Hinsehen daher eine andere Maßnahme: Die Rechtsordnung sollte die Rechtmäßigkeit des Verarbeitungsmodells und seiner Grundannahmen, also die algorithmenbasierte Entscheidungsvorbereitung, *objektivrechtlich* durch angemessene normative Vorgaben und staatliche Kontrolle absichern.[48]

3. Ausweitung und Veröffentlichung einer Folgenabschätzung

Das Datenschutzrecht steht mit seinem Raster eines grundsätzlichen Verbots mit Erlaubnisvorbehalt, das pauschal alle Verarbeitungen unter eine Gefährlichkeitsvermutung stellt, in dem Verdacht, einem allzu holzschnittartigen Schwarz-Weiß-Muster zu folgen.[49] Ein Ansatz *risiko*adjustierter Regulierung unternimmt den richtigen Schritt, das Kontrollregime stärker auf die tatsächlichen Gefährdungen auszurichten, die von einer Verarbeitung ausgehen, um datenschutzrechtliche Konflikte im digitalen Zeitalter problemadäquater zu bewältigen. Als Ausdruck dieses Kontrollansatzes[50] erlegt Art. 35 DSGVO Verantwortlichen auf, ihre Datenverarbeitungsvorgänge umfassend selbst zu prüfen. Die Folgenabschätzung i. S. d. Art. 35 Abs. 1 DSGVO etabliert jedoch keine umfassende Risikoanalyse. Sie erfasst ausschließlich die Folgen für den *Schutz personenbezogener Daten* (und damit zuvorderst „klassische“ datenschutzrechtliche Schutzinteressen).[51] *Sonstige Schutzgüter* – wie etwa das Vermögen, das Eigentum oder die körperliche Integrität – muss der Verantwortliche demgegenüber nicht zwangsläufig und unmittelbar in sein Prüfradar integrieren („Abschätzung der Folgen […] für den Schutz personenbezogener Daten“ – Art. 35 Abs. 1 S. 1 DSGVO): Bedeutung haben sie nur für die Frage, *ob* eine Folgenabschätzung durchzuführen ist („für die Rechte und Freiheiten natürlicher Personen“), nicht aber für den inhaltlichen *Prüfungsumfang* („Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten“).[52]

[48] Für eine wirksame zivilgesellschaftliche Überprüfung – etwa durch die Wissenschaft, durch Verbände oder die „IT-Community“ – ist es zugleich sinnvoll, die öffentlichen Einsichtsmöglichkeiten nicht zu weit abzusenken. Auf die „Intelligenz der Masse“ sollte die Rechtsordnung nicht vollständig verzichten.
[49] Dazu bspw. ausführlich *Martini*, Blackbox Algorithmus, 2019, S. 159 ff.
[50] Dazu etwa *Böhning*, ZD 2013, 421 (422); *Härting/Schneider*, CR 2015, 819 (822 ff.); *Veil*, ZD 2015, 347 (348 ff.).
[51] *Martini*, Blackbox Algorithmus, 2019, S. 209 f.
[52] Siehe dazu auch im Einzelnen *Martini*, Blackbox Algorithmus, 2019, S. 209 f.

Das Regelungskonzept der DSGVO springt dadurch zu kurz. Es ist sachgerecht, Diensteanbietern, die grundrechtssensible oder in anderer Weise potenziell gefährdende Algorithmen einsetzen, eine *thematisch umfassende* Risiko- bzw. Folgenabschätzung[53] abzuverlangen, bevor sie ihre Softwareanwendungen am Markt einsetzen.[54]

An die Vorgabe, eine Risiko- oder Folgenabschätzung zum Einsatz bestimmter risikogeneigter[55] algorithmischer Verfahren durchzuführen, sollte die Rechtsordnung auch die Pflicht knüpfen, deren Ergebnisse *der Öffentlichkeit zugänglich* zu machen.[56] Um die Effektivität des Regulierungsinstruments zu erhöhen, könnte ein *öffentliches Register* die Aufgabe übernehmen, die Folgenabschätzungen (in den Grenzen berechtigten Geheimnisschutzes) zu sammeln und zugänglich zu machen. Vergleichbare Register existieren bspw. für öffentliche Beurteilungen und Risikoanalysen, die Unternehmen im Rahmen der Arzneimittelzulassung erstellen müssen.

II. Inhaltskontrolle

Um einen rechtmäßigen Einsatz algorithmenbasierter Systeme zu gewährleisten, sind inhaltliche Kontrollvorgaben essenziell, die zielgenau auf das jeweilige Betriebsrisiko reagieren. Für sie muss die Rechtsordnung nicht nur tragfähige Maßstäbe entwickeln (1.), sondern auch schlagkräftige Institutionen vorhalten, die sicherstellen, dass Betreiber die Regeln in praxi einhalten (2.).

[53] Die Rechtsordnung kann dem Anbieter einer Softwareanwendung dabei durchaus auch überantworten, bisher unerkannte Gefahren für alle betroffenen Rechtsgüter zu ermitteln; vgl. dazu bspw. die entsprechenden Regelungen im Gefahrstoffrecht: Art. 5 ff. VO (EU) Nr. 1272/2008.
[54] *Martini*, Blackbox Algorithmus, 2019, S. 209 f.; mit einem ähnlichen Ansatz („*Algorithmic Impact Assessments*“) für das US-Amerikanische Recht: *Reisman/Schultz et al.*, Algorithmic Impact Assessments, April 2018, S. 7 ff.
[55] Zu möglichen Regulierungsschwellen unten S. 41 ff.
[56] Dazu bereits *Martini*, JZ 2017, 1017 (1022). Ausführlich dazu *Martini*, Blackbox Algorithmus, 2019, S. 210 ff.

1. Kontrollmechanismen

a) Ex-ante-Kontrolle bei algorithmenbasierten Entscheidungsprozessen in sensiblen Anwendungsfeldern

Um Betroffene bei besonders gefahrträchtigen Anwendungen wirksam zu schützen, ist ein staatliches Ex-ante-Kontrollverfahren vorstellbar, das Softwareanwendungen *vor ihrem Einsatz* durchlaufen müssen.[57] Ein Verfahren der Marktzulassung bürdet Unternehmen jedoch beträchtlichen bürokratischen Aufwand auf und kann dadurch wirtschaftliche Wertschöpfung ausbremsen. Im Regelfall schießt es über das Ziel hinaus.

Sachgerecht kann ein präventives Zulassungsverfahren aber einerseits bei algorithmenbasierten Verfahren sein, welche die Verwaltung bei der Prüfung und Zuteilung von Leistungen (z. B. Studienplätzen, Sozialleistungen und Subventionen) einsetzt, andererseits bei Anwendungen, von denen schwerwiegende Grundrechtsbeeinträchtigungen,[58] insbesondere Gesundheitsschäden, ausgehen (z. B. Pflegeroboter)[59]. Auch für Anwendungen, die sich erheblich auf solche lebensweltlichen Bereiche auswirken können, die für eine freiheitlich-demokratische Ordnung (insbesondere Wahlen oder die öffentliche Meinungsbildung) von systemischer Bedeutung sind, kann eine Vorabkontrolle sachgerecht sein.[60]

b) Konkretisierende Regelungen für die Zulässigkeit des Profilings, insbesondere Gebot mathematisch-statistischer Validität algorithmenbasierter Entscheidungen

Art. 22 Abs. 1 DSGVO setzt einen wichtigen, präventiv wirkenden Baustein in das Gebäude der Algorithmenregulierung ein: Er verleiht Betroffenen ein Abwehrrecht gegen automatisierte Entscheidungen. Sein Wirkradius ist gleichwohl eng: Er erfasst nicht generell das Profiling, sondern nur Ent-

[57] Dazu und zum Prüfungsinhalt eines solchen Kontrollverfahrens bereits *Martini*, JZ 2017, 1017 (1021); vgl. auch *Busch*, Algorithmic Accountability, 2018, S. 59 ff.
[58] Softwarebetreiber sind als Private zwar nicht unmittelbar grundrechtsgebunden. Die Grundrechte strahlen aber insbesondere dort, wo die Entfaltung von Lebenschancen in Rede steht, mittelbar in das Privatrechtsverhältnis hinein. Auf dem Gedanken dieser mittelbaren Bindung baut unausgesprochen auch das Regime der DSGVO in vielen Teilen auf.
[59] Teilweise unterliegen Softwareanwendungen solchen Zulassungserfordernissen bereits aufgrund sektorspezifischer Regelungen, z. B. des Medizinproduktegesetzes.
[60] Siehe auch die Ausführungen zu möglichen Regulierungsschwellen unten S. 41 ff.

scheidungen, die *ohne maßgeblichen* menschlichen Einfluss zustande kommen (z. B. den vollautomatischen Steuerbescheid, vgl. § 155 Abs. 4 AO).[61] Für die Mehrzahl algorithmischer Entscheidungsverfahren löst Art. 22 DSGVO die Regelungsaufgaben daher nicht vollständig.

Die Formulierung der Norm ist in Teilen sibyllinisch. Einerseits erfasst sie lediglich Entscheidungen, die „ausschließlich" von einer automatisierten Verarbeitung ausgehen. Andererseits lässt sie es ausreichen, dass die Entscheidung auf der automatisierten Verarbeitung *beruht* („beruhenden Entscheidung"). Das insinuiert auf den ersten Blick, dass zwischen automatisierter Verarbeitung und Entscheidung auch Zwischenschritte, z. B. menschliche Einwirkungen, treten können. Art. 22 DSGVO schließt das in der Tat auch nicht aus. Dem Topos „ausschließlich auf einer automatisierten Verarbeitung" lässt sich aber nur dann ein innerer Sinn einhauchen, wenn zwischen ihr und der Entscheidung *keine nennenswerten Zwischenschritte* treten, es sich also bei der menschlichen Intervention um eine rein formale Bestätigung einer Computerentscheidung ohne weitere innere Prüfung handelt.[62]

Aus Sicht des Verbraucherschutzes ist es prima facie reizvoll, den Tatbestand des Art. 22 Abs. 1 DSGVO rechtspolitisch auch *auf teilautomatisierte Entscheidungen auszudehnen*, genauer: auf „überwiegend oder ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung[en]".[63] Das Schwarz-Weiß-Muster *des Verbots* zu erweitern, das Art. 22 Abs. 1 DSGVO ausspricht, wird den Herausforderungen der digitalen Welt jedoch nicht ohne Weiteres gerecht; insbesondere schösse ein allgemeines Profiling-Verbot über das Ziel hinaus.[64] Angemessen und zielführend sind vielmehr konkretisierende Qualitätsanforderungen an algorithmenbasierte

[61] *Buchner*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 22, Rn. 15 f.; *Hoeren/Niehoff*, RW 9 (2018), 47 (63).

[62] Im Bereich des algorithmischen Handels mit Finanzinstrumenten unterwirft der Normgeber die Finanzdienstleistungsunternehmen den algorithmenspezifischen Pflichten bereits dann, wenn deren algorithmische Softwarehandelssysteme lediglich bestimmen, dass ein Mensch den Auftrag eingeschränkt weiterbearbeiten soll, Art. 4. Abs. 1 Nr. 39 RL 2014/65/EU v. 15.5.2014, ABl. L 173 v. 12.6.2014, S. 349 i. V. m. Art. 18 der Delegierten Verordnung (EU) 2017/565 v. 25.4.2016, ABl. L 87 v. 31.3.2017, S. 1.

[63] Automatisierte Entscheidungen in Fertigungsprozessen der Industrie, der Robotik usw. wären hiervon nicht betroffen, soweit eine Datenverarbeitung keinen Personenbezug aufweist und die DSGVO damit keine Anwendung findet; vgl. Art. 2 Abs. 1 DSGVO, Art. 2 Abs. 2 VO (EU) 2018/1807; vgl. auch auch *Reisman/Schultz et al.*, Algorithmic Impact Assessments, April 2018, S. 13.

[64] Das bedeutet nicht, dass das Schutzbedürfnis der Betroffenen es nicht rechtfertigen kann, Profiling-Analysen in spezifischen Sachbereichen unter bestimmten Umständen zu untersagen. Das macht Art. 6 Abs. 2a UAbs. 2 a. E. des Entwurfs der E-Privacy-VO v. 19.10.2018 paradigmatisch deutlich: Er sieht vor, dass der Anbieter elektronischer Kommunikationsnetzwerke oder -dienste die Metadaten der Kommunikationen (z. B. den Aufenthaltsort des Absenders einer elektronischen Nachricht) nicht nutzen darf, um Profiling-Analysen zu erstellen. Allerdings soll diese absolute Grenze des Profilings nicht gelten, wenn die Verarbeitung der Metadaten mit der Einwilligung des Nutzers oder auf Grundlage

Profiling-Maßnahmen, die dem sensiblen Instrument normative Leitplanken setzen. Dazu gehören insbesondere Sicherungsmechanismen, die Fehler und Risiken algorithmenbasierter Profiling-Verfahren reduzieren. Fehlerfrei ist eine algorithmenbasierte Entscheidung nämlich nur dann, wenn die Informationen, die in die später getroffene Entscheidung einfließen, nach mathematisch-statistischen Erkenntnissen überhaupt relevant sein können.[65] Die Rechtsordnung sollte den Verantwortlichen qualitative normative Vorgaben an die Hand geben,[66] die regeln, welche Daten, Grundannahmen und mathematischen Berechnungsverfahren Eingang in die Entscheidung finden und welche Auswertungsmechanismen zur Anwendung kommen dürfen.[67] Verbraucher sollten darauf vertrauen können, dass die Systeme ausschließlich aufgrund valider Annahmen und Modelle arbeiten (vgl. auch ErwGrd 71 UAbs. 2 DSGVO[68]).[69] § 31 Abs. 1 Nr. 2 BDSG macht insoweit für den engen Regelungsbereich des Scorings den Anfang. Anforderungen an valide mathematisch-statistische Verfahren sollte der (unionale) Normgeber[70] jedoch nicht nur für das Scoring, sondern auch für das – viel weiter gesteckte – Feld algorithmenbasierter Profiling-Auswertungsinstrumente (z. B. sozialer Netzwerke) formulieren.[71]

Was ein valides mathematisch-statistisches Verfahren im Einzelnen ausmacht, erschließt sich nicht von selbst, sondern bedarf weiterer Konkretisierung. Der deutsche Gesetzgeber hat die Frage im BDSG offengelassen. Die Rechtsordnung sollte Normanwendern – sei es auf gesetzlicher, sei es (in den Grenzen der Wesentlichkeitslehre) auf untergesetzlicher Ebene durch Rechtsverordnung[72] – konkrete Vorgaben dafür an die Hand geben, welche methodischen Anforderungen die Verfahren im Einzelnen erfüllen müssen. Darüber hinaus sollte sie präzisierende Vorgaben zur Frage treffen,

eines Gesetzes erfolgt, das dazu dient, ein öffentliches Ziel im Sinne des Art. 23 Abs. 1 lit. c - lit. e, lit. i oder lit. j DSGVO zu sichern, s. Art. 11 Abs. 1 des Entwurfs der E-Privacy-VO v. 19.10.2018.

[65] *Martini*, Blackbox Algorithmus, 2019, S. 257.

[66] Ähnlich *Wachter/Mittelstadt*, Columbia Business Law Review 2019, 1 (61) des Typoskripts.

[67] *Martini*, Blackbox Algorithmus, 2019, S. 257 ff. Ebenso stellt sich die umgekehrte Frage, ob statistisch relevante Daten unter Umständen zwingend in den Entscheidungsprozess einfließen müssen, dazu *Domurath/Neubeck*, Verbraucher-Scoring aus Sicht des Datenschutzrechts, Oktober 2018, S. 23.

[68] Erwägungsgründe sind nicht bindend, sondern Interpretationshilfen des unionsrechtlichen Gesetzesaktes.

[69] Dazu, dass die Rechtsordnung die Kontrolle objektiv-rechtlich und nicht subjektiv-rechtlich ausgestalten, insbesondere kein Recht auf sachgerechte Schlussfolgerung implementieren sollte, oben S. 15 f.

[70] § 31 Abs. 1 Nr. 2 BDSG ist mit dem Anwendungsvorrang der DSGVO nicht vereinbar. Dazu bspw. *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 22 DSGVO, Rn. 44.

[71] *Martini*, Blackbox Algorithmus, 2019, S. 257.

[72] Ausführlich zur delegierten Rechtsetzung unten S. 53 ff.

wann ein Verantwortlicher bestimmte Modelle und Profil-Zuordnungen („wertkonservativ", „homosexuell", „unzuverlässig" etc.) nicht mehr wählen darf, weil sie sich als nicht hinreichend gesichert oder persönlichkeitsverletzend erweisen.

Aufgabe dieser Vorgaben ist es, operationalisierbare qualitative Anforderungen an das Verhältnis zwischen der Datengrundlage und dem Ergebnis des algorithmischen Datenverarbeitungsprozesses zu formulieren.[73] Sie legen Mindestanforderungen fest, welche die Grundannahmen und mathematischen Berechnungsverfahren (etwa auch die Gewichtung einzelner Berechnungsfaktoren), die dem algorithmischen Rechenmodell zugrunde liegen, erfüllen müssen. Wer Verarbeitungsmodelle verwendet, die persönlichkeitssensible Entscheidungen treffen, muss dann insbesondere sicherstellen und nachweisen können, dass ein statistisch valider Zusammenhang zwischen dem Ausgangsdatum und dem angestrebten Auswertungsergebnis existiert: Nur solche Kriterien, die für die Entscheidung nachweisbar erheblich und normativ zulässig sind, dürfen Eingang in das Entscheidungsmodell finden.[74]

Um die widerstreitenden Grundrechtspositionen des Softwarebetreibers auf der einen sowie der Entscheidungsadressaten auf der anderen Seite auszutarieren, sollten die Anforderungen an die Validität der mathematischen Modelle sowie die Sachnähe der zugrunde gelegten Informationen parallel zu der Entscheidungstragweite und dem Schadenspotenzial algorithmenbasierter Verfahren anwachsen. Zu den Qualitätsmerkmalen einer guten Modellierung gehört es insbesondere, Unsicherheiten und Spekulationsgrade ausweisen zu können, die eine sensible Entscheidung determinieren.[75]

c) Betreiberpflichten: Pflicht, rechtmäßige, insbesondere diskriminierungsfreie Entscheidungsergebnisse herzustellen

Wer lernfähige Softwareanwendungen in grundrechtssensiblen Anwendungsfeldern einsetzt, sollte fortlaufenden Pflichten unterliegen, seine Systeme zu kontrollieren. Ihn sollten insbesondere – ähn-

[73] Zum Folgenden *Martini*, Blackbox Algorithmus, 2019, S. 257 ff.
[74] *Martini*, Blackbox Algorithmus, 2019, S. 257 ff.
[75] *Martini*, Blackbox Algorithmus, 2019, S. 259.

lich wie im Immissionsschutzrecht – dynamische Betreiberpflichten treffen, die ihn für die Entscheidungsergebnisse und die Verfahrensrichtigkeit des Systems in die Verantwortung nehmen:[76] Sie verpflichten die Betreiber, die Entscheidungsergebnisse ihrer Software nicht nur vor ihrem Einsatz zu testen[77] und zu analysieren, sondern auch, im Anschluss daran begleitend zu überprüfen, ob sie mit den Wertvorgaben der Rechtsordnung[78] in Einklang stehen.

Mit dieser Betreiberpflicht muss eine wirksame externe Kontrolle korrelieren, die sicherstellt, dass die Dienste die Anforderungen tatsächlich einhalten, welche die Rechtsordnung an sie stellt.

aa) Diskriminierungsrechtliche Inpflichtnahme der Betreiber

Zu den zentralen Risiken, die von algorithmischen Entscheidungsmustern einer Softwareanwendung ausgehen, zählen diskriminierende Ergebnisse. Denn Algorithmen spiegeln die Vorurteile und gesellschaftlichen Ungleichgewichte wider, die sich in ihren Trainingsdaten und Codes eingraviert haben: Lernfähige Systeme bilden die Vorurteile und Ungleichbehandlungen der sozialen Realität ab. Sozial oder rechtlich unerwünschte Differenzierungen finden dadurch – häufig unerkannt – auch ihren Weg in algorithmenbasierte Entscheidungsergebnisse. Identifiziert bspw. ein lernendes System aufgrund von Korrelationsberechnungen die Zahl der geleisteten Arbeitsstunden als aussagekräftiges Kriterium für die Kategorie »hervorragend« einer Mitarbeiterleistungsbeurteilung und richtet seine Differenzierungen an diesem Muster aus, diskriminiert es dadurch Frauen grundsätzlich mittelbar. Denn Frauen arbeiten deutlich überproportional in Teilzeit, um familiäre Betreuungspflichten wahrzunehmen. Ähnlich wird ein Algorithmus, der mit Methoden des *machine learnings* Schüler mit hohem Leistungspotenzial für ein Förderprogramm identifizieren soll, im Zweifel auch linguistische Besonderheiten ihres sozialen Milieus oder Wohnortes berücksichtigen, wenn zuvor Schüler mit ähnlichen Faktoren im Durchschnitt weniger erfolgreich waren.[79] In einer algorithmenbasierten Welt, die den Einzelnen auf der Grundlage tief analysierender Auswertungsinstrumente nach vielfältigen Kategorien zu durchleuchten in der Lage ist, ist der Einzelne mithin immer häufiger

[76] Dazu ausführlich *Martini*, Blackbox Algorithmus, 2019, S. 256 ff.
[77] Dazu ausführlich *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 146. *Schmid*, CR 2019, 141 ff. leitet eine Kontrollpflicht des Betreibers zur „integrierten Produktbeobachtung“ für automatisierte und vernetzte Systeme aus den Verkehrssicherungspflichten des Deliktsrechts her.
[78] Auch gesellschaftliche und ökonomische Folgen (jenseits kartellrechtlicher oder sonstiger wettbewerbsrechtlicher Grenzen) einzubeziehen, würde das Prüfungsprogramm schnell überfordern.
[79] *Whittaker/Crawford et al.*, AI Now Report 2018, Dezember 2018, S. 21 f.

Rasterungen und Differenzierungen ausgesetzt, die nicht auf seine persönlichen Eigenschaften zurückgehen, sondern auf (mitunter diskriminierungsanfällige) Gruppenmerkmale, die er erfüllt.

(1) Erweiterung des AGG

Die Aufgabe, diskriminierungsgefährdete Personen vor ungerechtfertigten Ungleichbehandlungen einfachgesetzlich zu schützen, nimmt in Deutschland das *Allgemeine Gleichbehandlungsgesetz* (AGG) wahr.

Es ist fragmentarisch konzipiert: Weder erfasst es alle Formen denkbarer Ungleichbehandlung (z. B. wegen unterschiedlicher Preisbereitschaft) noch alle Lebensbereiche, in denen Diskriminierungen vorkommen können. Es erstreckt sich damit auch nicht auf alle Erscheinungsformen, in denen algorithmenbasierte Entscheidungssysteme in die Rechtssphäre des Einzelnen eindringen können.[80] Es fokussiert sich vielmehr auf die Bereiche Arbeit, Bildung, Soziales und Massengeschäfte.

Um das normative Gerüst des AGG zu einem Antidiskriminierungsgesetz für algorithmenbasierte Verfahren auszubauen, das alle Lebensbereiche erfasst, könnte der Gesetzgeber den § 2 AGG um eine neue Nr. 9 (alternativ die Vorschrift des § 19 Abs. 1 AGG) erweitern, d. h. den Anwendungsbereich des AGG auf alle Ungleichbehandlungen ausdehnen, die *„auf einer algorithmenbasierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen“.*

Das AGG blickt zugleich aber auch auf eine lange Geschichte rechtsmissbräuchlicher Entschädigungsverfahren („AGG-Hopper“) zurück.[81] Bei rechtspolitischen Bemühungen, den Anwendungsbereich des AGG auszudehnen, ist daher Achtsamkeit geboten. Als Teil eines vorsichtig tastenden regulatorischen Ansatzes kann es sich deshalb alternativ empfehlen, den Anwendungsbereich des AGG nicht *generell* auf algorithmenbasierte Verfahren (ggf. mit umfangreichen Gegenausnahmen) auszuweiten, sondern ihn um *einzelne Sachbereiche* besonders grundrechtssensibler Entscheidungen zu ergänzen, die sich nachhaltig auf Lebenspläne auswirken können (wie z. B. „Verbraucherverträge, die auf der Grundlage eines Scorings zustande kommen“), oder einzelne risikoträchtige Verfahren in den normativen Radius des AGG zu integrieren (etwa Methoden der Gesichtserkennung).[82]

[80] Im Einzelnen dazu *Martini*, Blackbox Algorithmus, 2019, S. 231 ff.
[81] Im Einzelnen dazu *Martini*, Blackbox Algorithmus, 2019, S. 237 f. Eine einordnende Zusammenfassung zu dieser Thematik findet sich bei *Bauer/Krieger*, NZA 2016, 1041 (1041 f.) m. w. N. Zur strafrechtlichen Beurteilung des AGG-Hoppings vgl. *Brand/Rahimi-Azar*, NJW 2015, 2993 (2993 ff.).
[82] Im Einzelnen dazu *Martini*, Blackbox Algorithmus, 2019, S. 236 ff., 337 ff.

(2) Technische Schutzmaßnahmen gegen mittelbare Diskriminierungen

Regulatorische Antworten auf das Diskriminierungspotenzial, das in lernenden Softwareanwendungen steckt, sehen sich in besonderer Weise der Herausforderung ausgesetzt, die Gefahr mittelbarer Ungleichbehandlungen zu bändigen, deren Ursache in einer diskriminierenden Datengrundlage liegt.[83] Um ihnen entgegenzuwirken, sollte der Gesetzgeber an der Stellschraube „Auswahl und Gestaltung der Trainingsdatensätze“ ansetzen. Betreiber sollte die Pflicht treffen, technische Schutzmaßnahmen zu ergreifen, die Diskriminierungen durch sachgerechten Zuschnitt und angemessene Kontrolle der Trainingsdaten zu verhindern suchen. Denkbar ist es insbesondere, mit normierten Standarddatensätzen zu operieren oder Schlüsseldaten einer Kontextbindung zu unterwerfen.[84]

bb) Qualitätsvorgaben für die Verfahrensgerechtigkeit

Um der Gefahr rechtswidriger Entscheidungsergebnisse entgegenzutreten, sind zusätzlich zu einer Betreiberpflicht für diskriminierungsfreie Entscheidungsergebnisse qualitative Vorgaben an Entscheidungsalgorithmen sachgerecht. Der Normgeber sollte Betreibern ein Mindestmaß an technischen und mathematischen prozeduralen Qualitätsgarantien abverlangen, welche die Rechtmäßigkeit der algorithmenbasierten Ergebnisse durch Verfahrensvorgaben absichern. Ihre Aufgabe ist es, sicherzustellen, dass das Programm auf einem prozedural rechtmäßigen Weg zu seinen Entscheidungen gelangt. Dazu können insbesondere Sicherungsmechanismen gehören, welche die Qualität der verarbeiteten Daten, des Entscheidungsmodells und spezifischer Verarbeitungsvorgaben verbürgen.

cc) Verpflichtung, ein Risikomanagementsystem zu betreiben und eine verantwortliche Person zu benennen

Wer in grundrechtssensiblen Softwareanwendungen[85] (lernende) Algorithmen implementiert, sollte nicht nur eine *Risikoprognose* treffen müssen, wie sie ihm Art. 35 Abs. 1 S. 1 DSGVO vor-

[83] Dazu ausführlich *Martini*, Blackbox Algorithmus, 2019, S. 239 ff.
[84] Dazu ausführlich *Martini*, Blackbox Algorithmus, 2019, S. 243 ff.
[85] Zur Konkretisierung der Regulierungsschwellen siehe unten S. 41 ff.

schreibt. Er sollte vielmehr grundsätzlich auch ein *Risikomanagementsystem* in seine Datenverarbeitungsprozesse implementieren müssen.[86] Bislang schreibt die DSGVO Verantwortlichen ein solches System nicht vor. Darin offenbart sich eine normative Lücke. Der Unionsgesetzgeber könnte sie bspw. dadurch schließen, dass er die allgemeinen Pflichten Verantwortlicher in Art. 25 Abs. 1 DSGVO um die Pflicht erweitert, ein wirksames Risikomanagementsystem einzuführen und zu betreiben, soweit sie sensible algorithmenbasierte Verfahren einsetzen, welche nachhaltige Schäden hervorrufen können.[87]

Ein Risikomanagementsystem gibt dem Verantwortlichen als Verlängerung der zeitlich vorgelagerten Folgenabschätzung auf, festzustellen, inwieweit sich Gefahren realisiert haben, und auf sie ggf. zu reagieren. Soweit sich im System Anhaltspunkte für Fehler einstellen, kann es bspw. eine (menschliche) Kontrolle der automatisierten Entscheidung auslösen. Dadurch kann es dazu beitragen, dass es in algorithmenbasierten Prozessen nicht zu unvorhergesehenen, insbesondere diskriminierenden Entscheidungen kommt.

Für das Risikomanagementsystem sollten die Betreiber (jedenfalls ab einer bestimmten Größenordnung und Sensibilitätsschwelle) eine verantwortliche Person benennen müssen. Diese müsste nicht nur in der Lage sein, die Risiken eines Systems auf der Grundlage besonderer Kenntnisse der Statistik, Mathematik und Informatik einzuschätzen. Sie sollte ggf. auch haftungsrechtlich zur Verantwortung gezogen werden können. Ähnlich wie Aktuaren (§ 141 Abs. 5 Versicherungsaufsichtsgesetz – VAG) käme den Risikomanagern die Aufgabe zu, Fehler algorithmenbasierter Systeme, die sich auf ihre Entscheidungsvorschläge auswirken, zu identifizieren, unternehmensintern darauf aufmerksam zu machen und auf Abhilfe hinzuwirken.

Denkbar sind auch *allgemeine Berichts- oder Informationspflichten* für besonders sensible algorithmenbasierte Entscheidungsverfahren, um die Öffentlichkeit über die Risikoentwicklung eines Systems zu unterrichten. Im Falle einer Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 4 Nr. 12 DSGVO (etwa im Falle eines Daten-Lecks) muss der Verantwortliche die betroffenen Personen de lege lata bereits benachrichtigen, wenn „voraussichtlich ein hohes Risiko für die persönlichen

[86] Dazu bereits *Martini*, JZ 2017, 1017 (1022). Etwaige organisatorische Plichten bestehen im Bereich des algorithmischen Handels mit Finanzinstrumenten bereits, § 80 Abs. 2–5 WpHG i. V. m. DelVO (EU) 2017/589: dazu näher *Martini*, Blackbox Algorithmus, 2019, S. 148 ff.

[87] Zur inhaltlichen Konkretisierung der Frage, wer unter diese Personengruppe fällt, siehe unten S. 42 ff. Unterhalb einer kritischen Sensibilitätsschwelle könnte der Gesetzgeber die Entscheidung, einen Risikomanager zu benennen, in die Verantwortung und Entscheidungshoheit des Betreibers legen, diesen dafür bei der Aufsicht privilegieren, soweit die Tätigkeit des Risikomanagers den Nachweis zu erbringen vermag, dass der Verantwortliche seine Pflichten ordnungsgemäß erfüllt.

Rechte und Freiheiten“ der Betroffenen besteht (Art. 34 Abs. 1 DSGVO). Eine Informationspflicht, die unterhalb dieser Verletzungsschwelle ansetzt, insbesondere über aufgetretene und abgewendete Risiken informiert, kann das Risikobewusstsein bzw. Vertrauen der Verbraucher stärken sowie die Anbieter im Idealfall ergänzend zu tauglichen Risikominderungsstrategien anhalten.

d) Behördliche Kontrolle während des Betriebs

Wo der Einzelne nur sehr begrenzt Einblick in die Rechtmäßigkeit algorithmenbasierter Prozesse nehmen kann und sich deren Lösungsparameter dynamisch wandeln, wächst einer begleitenden staatlichen Rechtmäßigkeitskontrolle der Anwendungen umso größere Bedeutung zu. Das hoheitliche Prüfverfahren nimmt Softwaresysteme mit Blick darauf unter die Lupe, ob die Voraussetzungen für einen rechtmäßigen Einsatz dauerhaft vorliegen.[88] Neben Kontrollalgorithmen (aa) können insbesondere behördliche Auskunfts- und Einsichtsrechte (bb) ein wichtiger Baustein fortlaufender behördlicher Prüfmechanismen sein.

aa) Ergebniskontrolle, insbesondere Kontrollalgorithmen

Kontrollalgorithmen analysieren die Entscheidungsergebnisse einer Softwareanwendung systematisch auf Auffälligkeiten, insbesondere diskriminierende Tendenzen.[89] Kontrollalgorithmen werten aus, welche Faktoren der implementierte Algorithmus besonders stark gewichtet und ob die behauptete Beziehung zwischen Sachverhalt und Ergebnis mit dem tatsächlichen Entscheidungsverhalten übereinstimmt oder nicht.[90]

bb) Behördliche Auskunfts- und Einsichtsrechte, insbesondere Zugangsrechte/Schnittstellen für Tests und externe Kontrollen

In dem Einsatz von Kontrollalgorithmen sollte sich eine wirksame behördliche Prüfung nicht erschöpfen. Eine valide externe Analyse, ob der Dienst den Anforderungen der Rechtsordnung entspricht, lässt sich regelmäßig nämlich nur dann herstellen, wenn staatliche Kontrollinstanzen im Bedarfsfall nicht nur *Einblick in den Quellcode* erhalten, sondern auch in die *Lernmechanismen*, die zugrunde liegende *Datenbasis* sowie die hervorgebrachten *Ergebnisse*.[91]

[88] *Martini*, Blackbox Algorithmus, 2019, S. 249 f.
[89] Dazu bereits *Martini*, JZ 2017, 1017 (1022); zustimmend *Busch*, Algorithmic Accountability, 2018, S. 66.
[90] *Martini*, Blackbox Algorithmus, 2019, S. 250 f.
[91] *Martini*, JZ 2017, 1017 (1022).

Damit Behörden überprüfen können, ob Softwareanwendungen rechtliche Anforderungen einhalten, muss der Gesetzgeber behördliche Auskunfts- und Einsichtsrechte etablieren, die mit den materiell-rechtlichen Betreiberpflichten korrespondieren.[92] Eine denkbare normative Grundlage bzw. konkretisierungsfähige Blaupause liefert die Regelung des Art. 58 Abs. 1 DSGVO: Sie legt einen (umfassenden) Katalog der Untersuchungsbefugnisse fest („alle Informationen bereitzustellen", „Untersuchungen durchzuführen", „Zugang zu allen personenbezogenen Daten und Informationen […] zu erhalten") und ermöglicht Datenschutzaufsichtsbehörden dadurch, datenschutzrechtlich relevante Sachverhalte in tatsächlicher und rechtlicher Hinsicht umfassend zu ermitteln und aufzuklären.[93]

Ein weiteres normatives Vorbild liefert § 32e Abs. 5 und 6 GWB. Er erlaubt es dem Bundeskartellamt, verbraucherrechtliche Sektoruntersuchungen durchzuführen.[94] Auch für den Sonderbereich des algorithmischen Handels mit Finanzinstrumenten hat der Gesetzgeber insoweit analogiefähige Regelungen getroffen (§ 6 Abs. 4 WpHG, § 3 Abs. 4 Nr. 5 BörsG n. F. i. V. m. § 7 Abs. 3 S. 1 BörsG).[95]

Den legitimen Geheimhaltungsinteressen der betroffenen Diensteanbieter[96] lässt sich dabei durch vertraulichkeitswahrende Instrumente, insbesondere In-camera-Verfahren (vgl. § 99 Abs. 1 S. 2 VwGO; vgl. auch § 30 VwVfG), sachgerecht Rechnung tragen.[97]

(1) Schnittstelle für Tests und externe Kontrollen

Von außen lassen sich algorithmenbasierte Entscheidungssysteme nur dann wirksam kontrollieren, wenn die Betreiber des jeweiligen Systems einen technischen Echtzeitzugang zu dem gerade tatsächlich verwendeten System errichten. Eine schlagkräftige Kontrolle algorithmenbasierter Systeme[98] impliziert deshalb eine technische Möglichkeit, das tatsächlich tagesaktuell genutzte System untersuchen und testen zu können. Dafür bedarf es einer Schnittstelle bei dem Verantwortlichen,

[92] Dazu bereits *Martini*, Blackbox Algorithmus, 2019, S. 262; ähnlich auch *Whittaker/Crawford et al.*, AI Now Report 2018, Dezember 2018, S. 22.
[93] Vgl. zum Regelungsgehalt *Selmayr*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl., 2018, Art. 58, Rn. 11 ff.; *Boehm*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 58, Rn. 13 ff.
[94] *Busch*, Algorithmic Accountability, 2018, S. 66 f.
[95] Die Vorschriften setzen die Vorgaben des Art. 17 RL 2014/65/EU um; näher *Martini*, Blackbox Algorithmus, 2019, S. 153 f.
[96] Zu den patent-, urheber- und grundrechtlichen Fragen des Schutzes von Geschäftsgeheimnissen vgl. *Martini*, Blackbox Algorithmus, 2019, S. 33 ff.
[97] *Martini*, Blackbox Algorithmus, 2019, S. 253 ff.
[98] Instruktiv dazu aus technischer Sicht *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 44 ff.

die einen jederzeitigen Zugriff ermöglicht.[99] Die Rechtsordnung sollte der zuständigen Aufsichtsbehörde gesetzlich verbürgen, auf eine solche Schnittstelle zugreifen zu dürfen. Spiegelbildlich sollte sie die Betreiber verpflichten, mithilfe geeigneter IT-Komponenten eine solche Zugriffmöglichkeit vorzuhalten, um eine behördliche Introspektion zu ermöglichen. Von besonderer Relevanz ist die Forderung nach staatlicher Aufsicht für Scoring-Software im Bereich der Kreditvergabe, insbesondere bei Auskunfteien. Entsteht bspw. der Verdacht, dass eine Score-Formel einzelne Gruppen systematisch benachteiligt, lässt sich dieser von außen nur schwer erhärten und belegen. Selbst die groß angelegte Datensammelaktion *OpenSCHUFA* ist aufgrund fehlender Datenmenge und -diversität alsbald an ihre Grenzen gestoßen.[100]

Auf den ersten Blick ist es reizvoll, die zu schaffende behördliche Schnittstelle für weitere Institutionen zu öffnen, die sich der Aufgabe verschrieben haben, die Rechte Betroffener zu schützen – etwa für Organisationen, die Verbandsklagerechte genießen oder als Schiedsstelle eine Befriedungsfunktion wahrnehmen.[101] Wenn aber private Dritte Zugang zu den Systemen erhalten, gehen damit nachhaltige Gefahren für die Berufs- und Eigentumsfreiheit der Betreiber, insbesondere ihre Geschäftsgeheimnisse einher: Tiefgehende Systemtests auf der Grundlage einer Schnittstelle können Einblicke in das betriebliche „Tafelsilber“ eines Unternehmens eröffnen und dadurch unverhältnismäßig stark in die Rechte der Betreiber eingreifen. Im Extremfall können Tests auch die Funktionsfähigkeit der Systeme, insbesondere ihre Stabilität und Leistungsfähigkeit, beeinträchtigen.[102] Keineswegs ist auch immer eindeutig, ob ein einzelnes Testergebnis tatsächlich einen Systemfehler oder vielmehr ein Phantom aufzeigt und dem Test daher eine Beweisfunktion zukommt.[103] Bislang fehlt es auch noch an gemeinsamen normativen und technischen Rahmenbedingungen für das Testen: Die Qualität der Tests sowie ordnungsgemäße Testverfahren bedürfen zunächst einer rechtlichen Absicherung.[104] Mit Blick auf die zahlreichen Risiken ist anstelle eines originären Schnittstellenzugriffs Dritter ein (mit dem strafprozessualen Klageerzwingungsverfahren bzw. dem prozessua-

[99] Denkbar wäre zudem eine automatisierte aufsichtsbehördliche Echtzeitüberwachung in besonders sensiblen Bereichen. So überwacht seit dem 15. November 2018 ein konsolidiertes Überwachungssystem CAT (Consolidated Audit Trails) die US-amerikanischen Kapitalmärkte, dazu auch *Martini*, Blackbox Algorithmus, 2019, S. 155.
[100] Vgl. den Zwischenbericht der Initiative, abrufbar unter https://algorithmwatch.org/de/zwischenbilanz-der-open-schufa-datenspende/; vgl. hierzu auch *Busch*, Algorithmic Accountability, 2018, S. 69.
[101] Siehe zu potenziellen Verbandsklagerechten und Schiedsstellen unten S. 37 f.
[102] Zu diesem Zweck kann es bspw. sachgerecht sein, die Anzahl der zulässigen Zugriffe zu begrenzen.
[103] Dazu *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 150 f.
[104] *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 158 f.

len Vorlagerecht vergleichbares) durchsetzbares *Antragsrecht* für autorisierte Verbraucherverbände und Schutzorganisationen vorzugswürdig. Die privaten Einrichtungen könnten dann – unter im Einzelnen zu spezifizierenden Voraussetzungen – einen behördlichen Test erzwingen. Dafür müssten sie Anhaltspunkte für eine rechtswidrige algorithmische Praxis darlegen und nachweisen, dass sie ihre Verbandsklagerechte (bzw. gesetzlich verbürgten Mitwirkungs- und Schutzrechte zugunsten der Personengruppen, für die sie auf den Posten gestellt sind, vgl. bspw. § 27 f. AGG) anderenfalls nicht angemessen wahrnehmen können.

(2) Protokollierungspflichten der Dienstanbieter

Ein System der Kontrolle algorithmenbasierter Systeme, das Rechtsverletzungen eines algorithmenbasierten Entscheidungssystems nicht mit geeigneten Instrumenten ex post nachweisbar macht, hat einen „blinden Fleck“. Zu einer sachadäquaten begleitenden Regulierung gehört daher eine Pflicht, die Programmabläufe einer Software, die nachhaltige Schäden verursachen, bspw. substanzielle Ersatzpflichten auslösen können, zu protokollieren.[105]

Eine strikte Pflicht zur Verfahrensdokumentation ist aber nicht der einzig normativ gangbare Weg. Die Entscheidung über die Tiefe der Dokumentation könnte die Rechtsordnung (in nicht hochgradig grundrechtssensiblen Einsatzbereichen) in die Hände des Verantwortlichen legen – an eine fehlende bzw. unzureichende Protokollierung aber eine gesetzliche Beweislastumkehr knüpfen:[106] Wenn ein Betroffener gegen den Betreiber eines algorithmenbasierten Entscheidungssystems gerichtlich vorgeht und Anhaltspunkte für eine rechtswidrige Verarbeitung darlegt, müsste der Betreiber mit Hilfe seiner Protokolle nachweisen, dass das System zum entscheidenden Zeitpunkt alle rechtlichen Vorgaben eingehalten hat. Gelingt ihm der entlastende Beweis nicht, trägt der Verantwortliche das Risiko der Unaufklärbarkeit. Eine solche Konstruktion wird Unternehmen im Zweifel dazu anhalten, jedenfalls in denjenigen Bereichen Protokollierungen einzubauen, in denen sie hohe Schadensersatz- oder Unterlassungsansprüche gewärtigen müssen.

[105] Eine Dokumentations- (§ 80 Abs. 3 S. 1, 2 WpHG) und Auskunftspflicht (§ 80 Abs. 3 S. 3 WpHG; § 6 Abs. 4 WpHG, § 3 Abs. 4 Nr. 5 BörsG i. V. m. § 7 Abs. 3 S. 1 BörsG) über algorithmenbasierte Entscheidungsprozesse hat der Gesetzgeber für einen Sonderbereich bereits geregelt: für den algorithmischen Handel auf den Finanzmärkten. Die verfahrensrechtlichen Pflichten sollen insbesondere Marktmanipulation unterbinden bzw. aufdecken. Sie bestehen jedoch nur gegenüber den zuständigen Aufsichtsbehörden. Siehe dazu *Martini*, Blackbox Algorithmus, 2019, S. 148 ff., 153 f.
[106] Dazu bereits *Martini*, JZ 2017, 1017 (1022).

2. Institutionelle Ausgestaltung des Kontrollsystems

Entschließt sich der Gesetzgeber dazu, ein behördliches Kontrollregime für grundrechtssensible Softwareanwendungen zu etablieren, steht er vor der Frage, in wessen Hände er die Aufgabe legen sollte.[107] Denkbar sind sowohl eine einheitliche Aufsichtsbehörde für Maßnahmen der Algorithmenregulierung (a), eine Unterstützungseinheit, welche die verschiedenen, bereits existierenden Aufsichtsbehörden mit Sachverstand unterstützt (b), als auch eine Integration außerbehördlicher Kontrollmechanismen in ein Gesamtkonzept (c).

a) Einheitliche Aufsichtsbehörde?

Die staatliche Aufsicht über sensible Softwareanwendungen ist gegenwärtig durch einen Patchwork-Charakter geprägt: Sie ist auf eine Vielzahl unterschiedlicher Behörden verteilt – vom Bundeskartellamt[108] über die Landesmedienanstalten, die BaFin sowie die Börsenaufsicht (für den algorithmischen Handel mit Finanzinstrumenten) und die Antidiskriminierungsstelle des Bundes (§ 25 AGG) bis hin zu den datenschutzrechtlichen Aufsichtsbehörden.

Die Idee, die parzellierten Ressourcen künftig in dem Kompetenzbereich einer einzigen bundeseinheitlichen Vollzugsinstanz zu konzentrieren, hat durchaus Charme:[109] Eine zentrale Stelle könnte den technischen Sachverstand, der erforderlich ist, um die vielfältigen Aufgaben der Algorithmenregulierung wahrzunehmen, (zeitnah) aufbauen und bündeln. Dafür ist es prinzipiell auch denkbar, eine gänzlich neue Behörde,[110] möglicherweise auf unionaler Ebene,[111] zu schaffen.[112]

De Regulierung algorithmenbasierter Entscheidungsprozesse repräsentiert allerdings ihrem Wesen nach eine Querschnittsmaterie, die spezialisierten Sachverstand in den unterschiedlichen Teilbereichen der Kontrolle fordert – vom Wettbewerbs- über das Datenschutz- bis hin zum Antidiskriminierungsrecht. Ohne eine profunde Sachkompetenz in den einzelnen Teilbereichen der Regulierung

[107] Zum Folgenden *Martini*, Blackbox Algorithmus, 2019, S. 268 ff.
[108] *Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz*, Verbraucherrecht 2.0, Dez. 2016, S. 8, 69 ff.; vgl. auch die Forderung der Bundestagsabgeordneten *Marcus Held* und *Matthias Heider* in *Ludwig*, Mehr Arbeit fürs Kartellamt, Süddeutsche Zeitung Online vom 21.11.2016; vgl. auch *Kieck*, PinG 2017, 67 (67 ff.) und *Körber*, WuW 2018, 173 (173).
[109] *Martini*, Blackbox Algorithmus, 2019, S. 268 f.
[110] *Anonymous*, LfDI Rheinland-Pfalz: Macht der Algorithmen – Macht ohne Kontrolle?, 2015, 04675; für eine „Agentur für ADM-Systeme“ oder eine „projektbezogene“ Lösung *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 159, 173 ff.
[111] *Wachter/Mittelstadt et al.*, International Data Privacy Law 7 (2017), 76 (98).
[112] *Martini*, Blackbox Algorithmus, 2019, S. 270.

kommt daher auch eine Vollzugsbehörde nicht aus, die sich der Aufsicht über algorithmenbasierte Systeme verschrieben hat.[113] So fehlt es den datenschutzrechtlichen Aufsichtsbehörden an AGG-Fachkompetenz und der Antidiskriminierungsstelle an vertiefter datenschutzrechtlicher Expertise. Die BaFin wiederum verfügt zwar – kraft ihrer Aufsichtsbefugnisse für den algorithmischen Wertpapierhandel[114] – womöglich über die breiteste Expertise im Umgang mit behördlichen Kontrollverfahren für algorithmenbasierte Prozesse, ist aber zugleich nicht der Aufgabe des Privatheitsschutzes, sondern des Schutzes der Handelssysteme verschrieben.

Vor allem gießt das komplexe Regelungsgeflecht der föderalen Kompetenzordnung Wasser in den Wein der Zielvorstellung, eine bundeseinheitliche „Algorithmenbehörde“ einzurichten: Der Vollzug der *Bundes*gesetze liegt grundsätzlich in den Händen der Länder (Art. 83 ff. GG). Der Bund verfügt über nur wenige Vollzugskompetenzen und -behörden (Art. 86 f. GG).[115] Für den Vollzug von *Landes*gesetzen, z. B. der Landesdatenschutzgesetze, fehlt ihm die Regelungsmacht vollends; diesen behält die Verfassung ausschließlich den Ländern vor. Dass die Bundes- und Landesbeauftragten für die *datenschutzrechtliche* Aufsicht zuständig sind, ist überdies unionsrechtlich verbürgt. Kraft des Anwendungsvorrangs des Unionsrechts könnte die Bundesrepublik ihnen diese Kompetenz in einem nationalen Alleingang also gar nicht mehr aus der Hand nehmen: Die Mitgliedstaaten müssen die datenschutzrechtlichen Aufsichtsbehörden als eigene Aufsichtsinstanz mit Unabhängigkeit beibehalten und hinreichend ausstatten (vgl. insbesondere Art. 52 Abs. 1 und 4 DSGVO).[116] Im Ergebnis werden die vielgestaltigen Aufgaben einer Algorithmenregulierung auf nicht absehbare Zeit also weiter in den Händen der spezialisierten Fachbehörden verbleiben (müssen).[117]

b) Unterstützungseinheit

Dass sich mehrere Behörden die hoheitliche Durchsetzung gesetzlicher Vorgaben für Softwareanwendungen teilen, schließt nicht aus, eine technisch versierte Unterstützungseinheit aus der Taufe

[113] *Whittaker/Crawford et al.*, AI Now Report 2018, Dezember 2018, S. 4 schlagen deshalb (im US-Amerikanischen Kontext) einen sektorspezifischen Regulierungsansatz vor.
[114] Zu dem Referenzgebiet „Hochfrequenz- und algorithmischer Handel mit Finanzinstrumenten“ siehe ausführlich *Martini*, Blackbox Algorithmus, 2019, S. 142 ff.
[115] Zu alledem *Martini*, Blackbox Algorithmus, 2019, S. 268 f.
[116] Kraft seiner Kompetenz für das Recht der Wirtschaft (Art. 74 Abs. 1 Nr. 11 GG) wäre der Bund jedoch verfassungsrechtlich nicht daran gehindert, die Zuständigkeit für die Aufsicht über die nicht-öffentlichen Stellen in die Hände des Bundesbeauftragten für Datenschutz und Informationsfreiheit zu legen.
[117] *Martini*, Blackbox Algorithmus, 2019, S. 270.

zu heben: Sie könnte den Aufsichtsbehörden dabei helfen, ihre Vollzugsmaßnahmen vorzubereiten.[118] Denkbar ist insbesondere eine *bundeseinheitliche Service-Einheit*. Ähnlich wie bspw. die *Physikalisch-Technische Bundesanstalt* (PTB)[119] oder das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) könnte sie als Bundesoberbehörde technischen Sachverstand aufbauen, um komplexe (v. a. auch lernfähige) Softwareanwendungen effektiv kontrollieren zu können, und den bestehenden Vollzugsbehörden als technische Ermittlungsinstanz gewonnene Erkenntnisse zur Verfügung stellen. Die Fachbehörde könnte ihre hoheitlichen Befugnisse dann auf dieser verbreiteten Wissensgrundlage durchsetzen. Die neue Einrichtung könnte darüber hinaus daran mitwirken, Methoden und Instrumente zu entwickeln, die rechtliche Vorgaben in technische Standards überführen, oder ihr gar mit hochspezialisierten Prüfteams bei einzelnen Maßnahmen zur Seite stehen. Eine verfassungsrechtliche Kompetenz, eine solche bundesrechtliche Service-Einheit zu etablieren, kann der Bund aus Art. 87 Abs. 3 S. 1 GG ableiten.

c) Ergänzung durch außerbehördliche Kontrollmechanismen

Ergänzend zur originären staatlichen Aufgabenerfüllung kann der Staat grundsätzlich auch private Institutionen *als Verwaltungshelfer* in die Rechtsdurchsetzung eines Algorithmenregulierungssystems einbeziehen.

Ein Verwaltungshelfer nimmt Hilfstätigkeiten bei der Erledigung öffentlicher Aufgaben im Auftrag und nach Weisung der betrauenden Behörde wahr. Er agiert als verlängerter Arm der Verwaltung, mithin wie ein Werkzeug; die Verwaltung behält die Aufsicht und bleibt stets Herrin der Entscheidungen (Werkzeugtheorie).[120] Sein Handeln ist dem Hoheitsträger unmittelbar zuzurechnen.[121] Der Einsatzradius zulässiger Verwaltungshilfe endet aber grundsätzlich dort, wo der Private öffentlich-rechtliche Befugnisse in abschließender Weise wahrnimmt.

Eine Funktion als Verwaltungshelfer, die mit der Aufgabe technischer Validierung und Bewertung algorithmenbasierter Verfahren zumindest im konzeptionellen Ansatz vergleichbar ist, füllen bspw.

---

[118] *Martini*, Blackbox Algorithmus, 2019, S. 271 f.; ähnlich auch *Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz*, Verbraucherrecht 2.0, Dez. 2016, S. 75 und *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 172 ff. mit Vorschlägen für eine „Digitalagentur" bzw. eine „Agentur für ADM-Systeme".

[119] Die PTB ist eine wissenschaftlich-technische Bundesoberbehörde im Geschäftsbereich des *Bundesministeriums für Wirtschaft und Energie*.

[120] Zur Werkzeugtheorie und ihrer Entwicklung etwa *Kiefer*, NVwZ 2011, 1300 (1302).

[121] Dazu bspw. *Reimer*, in: Posser/Wolff (Hrsg.), BeckOK VwGO, 47. Ed. (Stand: 1.11.2018), § 40, Rn. 80.

zwei in der Öffentlichkeit wenig bekannte Einrichtungen aus: die Deutsche Einheit Fernstraßenplanungs- und -bau-Gesellschaft GmbH (DEGES) und das Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG). Die *DEGES* nimmt unterstützende Aufgaben bei der Planung und Baudurchführung von Bundesfernstraßen wahr.[122] Das I*QWiG* versucht, die Komplexität und Vielfalt medizinischer Wirkungszusammenhänge zu ergründen, indem es den aktuellen medizinischen Wissensstand evidenzbasiert analysiert. Bei der Kosten-Nutzen-Bewertung von Arzneimitteln hat der Gesetzgeber ihm eine Schlüsselrolle zuerkannt (§ 31 Abs. 2a S. 3 SGB V i. V. m. § 35b Abs. 1 S. 3 SGB V). Darüber hinaus stellt es allgemein verständliche Gesundheitsinformationen zu diagnostischen und therapeutischen Verfahren bereit. Seine Analysen sind Verwaltungsinterna; es erbringt lediglich Dienstleistungen für die staatliche Aufgabenerfüllung in privater Rechtsform (§ 139a Abs. 1 S. 2 SGB V).[123] Eigene hoheitliche Entscheidungsmacht hat es nicht inne, ist aber in die Vorbereitung von Verwaltungsentscheidungen eingebunden.

Nach dem Vorbild des IQWiG könnte der Staat – als Baustein einer unechten funktionellen Privatisierung – eine private Gesellschaft gründen, die Dienstleistungen bei der Prüfung algorithmenbasierter Anwendungen und der Vorbereitung etwaiger aufsichtlicher Maßnahmen erbringt. Ihre privatrechtliche Organisationsstruktur kann ihr – im Vergleich zu einer behördlichen Verfassung – womöglich ein größeres Maß an Flexibilität und Gestaltungsfreiheit bei der Aufgabe gewähren, kompetentes Personal zu gewinnen und ihre inhaltlichen Aufgaben auf technisch hohem Niveau wahrzunehmen.

Umgekehrt setzt die private Rechtsform dem zulässigen Handlungsradius einer privaten „Algorithmenprüfungsgesellschaft“ jedoch enge Grenzen. Denn eine solche Einrichtung käme in Berührung mit Geschäftsgeheimnissen der Unternehmen, die sie beaufsichtigt, und wäre durch Tests etc. eng darin eingebunden, sensible Aufsichtsfunktionen wahrzunehmen. Vor diesem Hintergrund bedürfte es jedenfalls intensiver rechtlicher Sicherungsmaßnahmen, um die Risiken, die aus der Entscheidung für eine private Organisationsform erwachsen, wirksam einzuhegen. Das Aufgabenspektrum einer solchen privaten Prüfungsgesellschaft unterschiede sich vor diesem Hintergrund bspw. von dem des IQWiG. Dieses nimmt Kosten-Nutzen-Bewertungen nämlich typischerweise auf der Grundlage einer Analyse *veröffentlichter* wissenschaftlicher Studien vor, ohne aber selbst invasive Hoheitsrechte ausüben zu dürfen oder Einsichtnahmerechte zu genießen.

[122] Dazu *Martini*, WiVerw 2009, 195 (203 ff.).
[123] Dazu *Martini*, WiVerw 2009, 195 (204).

Anstelle einer Konzeption als Verwaltungshelfer ist aber im Grundsatz auch eine *Beleihung* rechtlich abbildbar: Der Staat könnte einen privaten Rechtsträger damit betrauen, die hoheitliche Aufgabe wahrzunehmen, algorithmenbasierte Verfahren *zu kontrollieren* – ähnlich wie der TÜV die technische Sicherheit von Fahrzeugen prüft oder Notare hoheitliche Aufgaben bei der Übertragung von Grundstücken wahrnehmen. Die Beleihung unterscheidet sich von der Verwaltungshilfe dadurch, dass natürliche oder juristische Personen des Privatrechts selbstständig einzelne hoheitliche Aufgaben *im eigenen Namen* wahrnehmen. Im Außenverhältnis sind sie dann Behörde i. S. d. § 1 Abs. 4 VwVfG und Teil der Staatsverwaltung. Zulässig ist eine solche Betrauung aber nur auf der Grundlage einer gesetzlichen Ermächtigung:[124] Sie muss insbesondere sicherstellen, dass die private Unterstützungseinheit nicht die Geschäftsgeheimnisse der Softwarebetreiber verletzt, die sie kontrollieren soll.

d) Zwischenergebnis

Um den Vorgaben der Rechtsordnung in der digitalen Welt mehr Durchschlagskraft zu verleihen, ist der Gesetzgeber aufgerufen, das staatliche Kontrollsystem auch institutionell anzupassen. Nur so kann er die Herausforderung bewältigen, die Risiken komplexer algorithmenbasierte Systeme einzudämmen und ihr enormes Potenzial auf gemeinwohlorientierte Bahnen zu lenken.

Eine staatliche Unterstützungseinheit auf Bundesebene zu errichten, ist ein sachgerechter Schritt, um die existierenden Fachbehörden des Datenschutz-, Medien-, Finanzdienstleistungs- und Wettbewerbsrechts mit umfangreicher und interdisziplinär geprägter Kompetenz technisch schlagkräftig aufzustellen. Ähnlich wie das BSI in dem Aufgabenfeld „IT-Sicherheit“ zu einer wichtigen Instanz der Sicherheit durch Prävention, Detektion und Reaktion im digitalen Zeitalter herangewachsen ist, kann sich eine (neue) staatliche Unterstützungseinheit für algorithmenbasierte Entscheidungsprozesse als ein wirksamer technischer Baustein eines Kontrollsystems für grundrechts- bzw. wettbewerbssensible Software etablieren. Der neuen Institution könnte der Staat auch Instrumente der Markt- und Produktüberwachung an die Hand geben, um (etwa bei der Überwachung unternehmensinterner Kontrollsysteme) eine umfassende Kontrolle auszuüben. Einzelbereiche der staatlichen Aufsicht – etwa einzelne Zertifizierungs- oder Auditaufgaben – könnte der Gesetzgeber per Gesetz auch Beliehenen zur Wahrnehmung im eigenen Namen übertragen oder Verwaltungshelfern als Assistenzfunktion der Verwaltung anvertrauen.

[124] Dazu etwa *Schmidt am Busch*, DÖV 2007, 533 (538); *Kiefer*, NVwZ 2011, 1300 (1300).

III. Ex post-Schutz

Dass Verbraucher in die Entscheidungsvorgänge einer Softwareanwendung nicht hineinblicken können, bleibt nicht ohne Auswirkungen auf ihre faktische Möglichkeit, gegen rechtswidrige Praktiken wirksam, ggf. gerichtlich, vorzugehen. Auch das Haftungs- (1.) und das Prozessrecht (2.) sollten deshalb auf die Wissensasymmetrien reagieren, die von algorithmenbasierten Systemen ausgehen können.[125]

1. Haftung

a) Beweislastverteilung

Wer die Abläufe im Maschinenraum einer Softwareanwendung nicht durchdringt, kann Verletzungshandlungen, Kausalitätszusammenhänge und Verschulden des Verantwortlichen kaum erkennen – geschweige denn im Rahmen eines Rechtsschutzverfahrens beweisen.[126] Die Rechtsordnung sollte dem Verbraucher daher Beweiserleichterungen gewähren, um seine prozessualen Verteidigungsmöglichkeiten zu wahren.[127]

Das Risiko, dass sich strukturelle informationelle Schieflagen zulasten des Einzelnen auswirken, teilt die Haftung für Schäden von Softwareanwendungen mit der Arzt- und Produzentenhaftung.[128] Um prozessuale Waffengleichheit zu schaffen, hat der Gesetzgeber für diese Rechtsmaterien eine Beweislastumkehr verankert (vgl. § 1 ProdHaftG; § 630h Abs. 5 BGB). Ähnlich wie dort sollte er dem Nutzer grundrechtssensibler Softwareanwendungen im Haftungsprozess mit einem abgestuften System der Beweislastverteilung entgegenkommen.[129] Es genügt dann, dass der Betroffene Tatsachen vorträgt, die mit überwiegender Wahrscheinlichkeit darauf schließen lassen, dass unzulässige Parameter Eingang in die Verarbeitung gefunden haben.[130] Dafür könnte er sich etwa auf die Erkenntnisse eines Testverfahrens stützen.[131] Die Beweisvermutung kann der Verantwortliche dann nur durch Vorlage protokollierter Programmabläufe, den Nachweis hinreichender Aufsicht über das

[125] Dazu bereits *Martini*, JZ 2017, 1017 (1023 f.); hierzu auch *Busch*, Algorithmic Accountability, 2018, S. 68 f.
[126] *Martini*, Blackbox Algorithmus, 2019, S. 274 f.; vgl. hierzu auch *Whittaker/Crawford et al.*, AI Now Report 2018, Dezember 2018, S. 22 ff.
[127] *Martini*, Blackbox Algorithmus, 2019, S. 274 f.
[128] Dazu bereits *Martini*, JZ 2017, 1017 (1023 f.).
[129] Dazu bereits *Martini*, JZ 2017, 1017 (1023 f.).
[130] Ähnlich für das Antidiskriminierungsrecht des AGG BAG, NJW 2018, 1497 (1499, Rn. 23 m. w. N.).
[131] Zu den Erkenntnismethoden Blackbox- und Whitebox-Tests, *Martini*, Blackbox Algorithmus, 2019, S. 44 ff. Zu der Forderung nach einer Schnittstelle bereits oben S. 28 f.

technische Verfahren oder Beweise, welche die Kausalitätsvermutung anderweitig erschüttern, widerlegen.[132]

b) Gefährdungshaftung?

Von Softwareanwendungen geht – anders als etwa von Kraftfahrzeugen – nicht generell eine Betriebsgefahr aus. Deshalb ist eine Gefährdungshaftung nach dem Vorbild der Tierhalter-, Straßenverkehrs- und Arzneimittelhaftung für algorithmenbasierte Verfahren nur in besonders sensiblen Einsatzbereichen[133] (etwa bei dem Einsatz von Pflegerobotern) sachgerecht. Um eine verschuldensunabhängige Haftung zu rechtfertigen, müssen besonders nachhaltige Schäden für gewichtige Rechtsgüter, insbesondere Leib und Leben, zu befürchten sein.[134]

2. Rechtsschutz

a) Abmahnbefugnisse für Wettbewerber

Der Staat kann auch die Wachsamkeit und Expertise konkurrierender Marktteilnehmer fruchtbar machen, um Verbraucher vor unzulässigen, aber zugleich undurchsichtigen Softwareanwendungen zu schützen:[135] Unternehmen verspüren regelmäßig einen ökonomischen Anreiz, rechtswidrige Praktiken ihrer Konkurrenten zu unterbinden. Daher sollte der Gesetzgeber die Abmahnbefugnisse in § 12 Abs. 1 Satz 1, § 8 Abs. 3 Nr. 1, Abs. 1 i. V. m. § 5 Abs. 1 Satz 1 und 2 Nr. 6 UWG bzw. i. V. m. § 3 Abs. 3 UWG um den Tatbestand diskriminierender oder sonst persönlichkeitsverletzender Softwareanwendungen erweitern.

Mit einer Abmahnbefugnis gehen jedoch gleichzeitig auch Missbrauchsanreize einher, sie weniger in den Dienst des Wettbewerbsschutzes als des finanziellen Eigeninteresses der Rechtsdienstleister zu stellen. Diesem Risiko sollte der Gesetzgeber im Gegenzug durch Sicherungsmechanismen entgegenwirken – z. B. indem er den Kostenersatz für Abmahnungen auf Fixbeträge deckelt. Auswüchsen einer „Abmahn-Industrie“ sollte die Rechtsordnung keinen Nährboden bereiten.[136]

---

[132] Dazu bereits *Martini*, JZ 2017, 1017 (1024).
[133] Zu möglichen Ansatzpunkten für Regulierungsschwellen unten S. 41 ff.
[134] Dazu bereits *Martini*, JZ 2017, 1017 (1024).
[135] Dazu bereits *Martini*, JZ 2017, 1017 (1024).
[136] *Martini*, Blackbox Algorithmus, 2019, S. 305 f.

b) Verbandsklagerecht der Verbraucherverbände und Einrichtung von Schiedsstellen

Wer als Verbraucher eine Rechtsverletzung erleidet, die ihn nicht nachhaltig in seiner gesamten Lebensführung beeinträchtigt, neigt typischerweise nicht dazu, die finanziellen und zeitlichen Risiken auf sich zu nehmen, die ihm ein gerichtliches Verfahren abverlangt.[137] Als Schutzpatrone eines fairen Marktgeschehens verfügen Verbraucherverbände regelmäßig über den längeren Atem, um Unternehmen in einem langen Rechtsstreit die Stirn zu bieten. Es empfiehlt sich daher, das Verbandsklagerecht auf der Grundlage des UKlaG durch eine Ergänzung des § 2 Abs. 2 UKlaG auf Fälle algorithmischer Entscheidungsfindung auszudehnen.[138] Um Missbrauch zu verhindern, sollte die Verbandsklagebefugnis aber ausschließlich solchen geprüften und registrierten Vereinigungen vorbehalten sein, die nicht gewinnorientiert agieren; auch die Regeln ihres Kostenersatzes sollten strikt im Dienste des Zwecks stehen, Missbrauch und Umgehungstendenzen abzuwehren.

Ergänzend kann eine staatlich geförderte *Schlichtungsstelle* als Instanz der alternativen Konfliktbewältigung die Schwelle und Kosten einer Rechtsdurchsetzung für Verbraucher senken (vgl. insbesondere §§ 2 ff. VSBG).[139] Als Vorbilder können etwa die Schlichtungsstelle für den öffentlichen Personenverkehr („söp“) oder die „Clearingstelle EEG|KWKG“ dienen (die für Streitigkeiten und abstrakte Fragen im Bereich des EEG zuständig ist [§ 81 Abs. 2 und 3 EEG 2017]).

IV. Selbstregulierung

Wo sowohl der Staat als auch die Nutzer nur über beschränkte Problembewältigungskompetenzen verfügen, während die Hersteller auf überlegenes Wissen zurückgreifen können, können Instrumente der Selbstregulierung ihre Vorzüge ausspielen. In einem Kontrollsystem algorithmenbasierter Prozesse können private Akteure im Grundsatz eine wichtige Ergänzungsfunktion übernehmen, die neben die klassische staatliche Aufsicht tritt, indem sie Private in die Vollzugsverantwortung einbezieht. Bei der Aufgabe, technische und ethische Standards zu etablieren, sowie bei der Zertifizierung und Auditierung nehmen die Normungsinstitute sowie Wirtschaftsverbände in vielen Rechtsbereichen bereits wichtige Aufgaben der Selbstregulierung wahr.

[137] Dazu bereits *Martini*, JZ 2017, 1017 (1024 f.).
[138] *Martini*, JZ 2017, 1017 (1024).
[139] Dazu bereits *Martini*, JZ 2017, 1017 (1025).

1. Auditierung

Wenn der Staat Qualitätsanforderungen für Algorithmen, Trainingsprozesse lernfähiger Systeme oder Datensätze definiert, kann er Privaten die Möglichkeit einer Zertifizierung eröffnen.[140] Praktische Anwendung findet ein solches staatlich legitimiertes Zertifizierungssystem unter Einbeziehung privater Kontrollstellen bereits bspw. im Bereich der ökologischen Landwirtschaft (sog. Bio-Siegel).[141] Im Datenschutzrecht hebt nun auch Art. 42 DSGVO die Möglichkeit aus der Taufe, dass sich Verantwortliche einer Zertifizierung mit Datenschutzsiegeln und -prüfzeichen unterziehen. Eine akkreditierte Stelle könnte dann etwa überprüfen, ob ein Gesichtserkennungssystem den Anforderungen eines speziell für diese Technologie konzipierten Privacy-by-Design-Zertifizierungsstandards (Art. 25 Abs. 1, 3 DSGVO) entspricht.

Eine einmalige Prüfung im Rahmen einer Zertifizierung, die ausschließlich *vor* dem Einsatz einer Softwareanwendung stattfindet, ist mit Blick auf die Dynamik moderner Softwaresysteme aber nur bedingt tauglich, um die intendierten Schutzzwecke zu erreichen. Sachgerechter ist eine fortlaufende Auditierung der Systeme über ihren *gesamten Lebenszyklus* hinweg. Eine Blaupause dafür, wie es gelingen kann, den Sachverstand Privater in die Gestaltungsmöglichkeit einer behördlichen Markt- und Produktüberwachung einzugliedern, kann etwa die *Öko-Audit-Verordnung* liefern.

Wenn sich die Anwender aktiv in die Rechtsgestaltung einbringen, kann das die Markttransparenz insgesamt steigern. Verbraucher können sich dann – ähnlich wie bei Lebensmitteln – auf der verbesserten Informationsgrundlage eines aussagekräftigen Automatisierungsverfahrens bewusst für (oder gegen) ein Produkt oder einen Dienst mit bestimmten Qualitätsstandards entscheiden.[142] Im Idealfall wächst das gesellschaftliche und individuelle Vertrauen in digitale Anwendungen.

---

[140] So z. B. für Qualitätsanforderungen in Form von Testverfahren *Schweighofer/Sorge et al.*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Oktober 2018, S. 67 f.

[141] Vgl. Verordnung (EG) Nr. 834/2007 des Rates v. 28.6.2007 über die ökologische/biologische Produktion und die Kennzeichnung von ökologischen/biologischen Erzeugnissen und zur Aufhebung der Verordnung (EWG) Nr. 2092/91 und das Gesetz zur Einführung und Verwendung eines Kennzeichens für Erzeugnisse des ökologischen Landbaus (Öko-Kennzeichengesetz) neu gefasst durch Bekanntmachung vom 20.1.2009 (BGBl. I S. 78); zuletzt geändert durch Artikel 404 der Verordnung v. 31.8.2015 (BGBl. I S. 1474).

[142] *Reisman/Schultz et al.*, Algorithmic Impact Assessments, April 2018, S. 16 sehen eine wirksame Anreizstruktur für Unternehmen insbesondere darin, dass sie durch gesteigertes Vertrauen der Verbraucher einen Wettbewerbsvorteil erlangen können.

2. Algorithmic Responsibility Codex

Bislang hat sich weder in der nationalen noch in der unionalen Rechtsordnung ein privater Kodex als Leitmaßstab für den unternehmerischen Umgang mit algorithmenbasierten Entscheidungsprozessen etabliert, der als relevante Größe zu staatlichen Vorgaben hinzutritt. Das hat viele Ursachen. Dazu trägt nicht zuletzt bei, dass einerseits die Hersteller und Betreiber heterogenen Branchen angehören und die Nutzerinteressen nur einen schwachen Organisationsgrad aufweisen. Zwar erblicken derzeit immerhin die ersten privaten Ethik-Kodizes, die Gütekriterien für algorithmenbasierte Anwendungen und Künstliche Intelligenz postulieren, das Licht der Welt.[143] Der (empirische) Blick in die Selbstregulierungspraxis der Vergangenheit relativiert jedoch hochfliegende Hoffnungen darauf, dass Empfehlungen eines Kodex die ethischen Entscheidungen der Programmierer im Rahmen der Softwareentwicklung auch tatsächlich signifikant beeinflussen.[144] Die Durchschlagskraft vieler gängiger Kodizes litt in der Vergangenheit darunter, dass sie in ihren Aussagen zu vage und in ihren Wirkungen ohne Sanktionen bleiben; oftmals beschränken sie sich in weiten Teilen darauf, die geltende Rechtslage wiederzugeben.[145]

Ansatzpunkte für eine regulierte Selbstregulierung „mit Biss“ kann das Konzept des aktienrechtlichen „Corporate Governance Kodex“ liefern (§ 161 AktG).[146] Der Kodex der Regierungskommission „Deutscher Corporate Governance Kodex“ ist als privates Regelwerk konzipiert. Er bindet die Regelungsadressaten nicht unmittelbar. Jedoch müssen sich die betroffenen Gesellschaften kraft § 161 Abs. 1 AktG dazu erklären, ob und inwieweit sie die Empfehlungen des Kodex umgesetzt haben. Soweit sie seine Empfehlungen in ihrer Geschäftspraxis nicht implementieren, müssen sie ihre Entscheidung begründen. Das Regulierungsmodell folgt damit dem Leitprinzip „comply or explain“. Es erzeugt dadurch mittelbaren Befolgungsdruck.[147] Zwar steht auch der Corporate Governance Kodex

[143] Vgl. etwa das Statement mit Prinzipienkatalog der *Association for Computing Machinery: ACM US Public Policy Council/ACM Europe Council*, Statement on Algorithmic Transparency and Accountability, http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf (25.10.2018); die Prinzipien des hochrangig besetzten Thinktanks *Future of Life Institute*, Asilomar AI Principles, https://futureoflife.org/ai-principles (25.10.2018); die Prinzipien der jährlichen Konferenz zum *Fair, Accountable and Transparent Machine Learning: Diakopoulos/Friedler et al.*, Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, https://www.fatml.org/resources/principles-for-accountable-algorithms (25.10.2018). Eine Zusammenfassung und Bewertung aus deutscher und europäischer Sicht bieten: *Rohde*, Gütekriterien für algorithmische Prozesse, 2018, S. 8 ff.; *Floridi/Cowls et al.*, Minds & Machines 28 (2018), 689 ff.

[144] *McNamara/Smith et al.*, ESEC/FSE ’18, November 4–9, 2018, Lake Buena Vista, FL, USA, S. 4 des Typoskripts.

[145] Ähnlich kritisch auch *Whittaker/Crawford et al.*, AI Now Report 2018, Dezember 2018, S. 29 ff.

[146] *Martini*, JZ 2017, 1017 (1023); zustimmend *Busch*, Algorithmic Accountability, 2018, S. 68.

[147] Vgl. beispielhaft *Hölters*, in: ders. (Hrsg.), AktG, 3. Aufl., 2017, § 161, Rn 3.

in seiner konkreten gegenwärtigen Ausgestaltung in der Kritik.[148] Das normative Konzept, das ihm zugrunde liegt, ist aber als solches schlüssig.

Nach dem Grundmuster des § 161 Abs. 1 AktG könnte der Gesetzgeber einen „Algorithmic Responsibility Codex" initiieren.[149] Einer Kommission, die sich aus Vertretern der relevanten Stakeholder (insbesondere der Verbraucherverbände, der Zivilgesellschaft, der Softwareunternehmen, der Verwaltung, der Wissenschaft) rekrutiert, erteilt der Gesetzgeber dann den Auftrag, Empfehlungen dafür zu formulieren, wie algorithmenbasierte Entscheidungsprozesse in grundrechtssensiblen Lebensbereichen zum Einsatz kommen sollten. Wer sich solcher Softwareanwendungen bedient, muss sich dann dazu erklären, ob und inwieweit er den Empfehlungen folgt.

Decken Kontrollmechanismen auf, dass das tatsächliche Verhalten des Unternehmens der öffentlichen Erklärung widerspricht, löst das nach der Logik des Kodex nicht nur eine Sanktionswirkung des Marktes aus, mit der ein nachhaltiger Reputationsverlust bei Verbrauchern korrespondiert. Falsche Erklärungen sollten auch bußgeldbewehrt sein.

Eine gesetzliche Regelung könnte in ihren Grundzügen lauten:

(1) Anbieter grundrechtssensibler Softwareanwendungen[150] erklären jährlich, dass sie den […] Empfehlungen der „Regierungskommission Algorithmic Responsibility Codex" entsprechen oder welche Empfehlungen sie nicht anwenden und warum nicht.

(2) Die Erklärung ist auf der Internetseite des Anbieters dauerhaft öffentlich zugänglich zu machen.

(3) Erweist sich eine Erklärung als nachweislich fehlerhaft, kann die zuständige Behörde ein Bußgeld i. H. v. … verhängen. […]

C. Regulierungsschwellen: Kriterienkatalog für die Konkretisierung des Pflichtenniveaus und des Normadressatenkreises

Wenn der Gesetzgeber Softwareanbietern Maßnahmen der Algorithmenregulierung aufträgt, schützt er damit nicht nur Verbraucher und andere Betroffene. Er belastet damit auch Unternehmen

[148] Vgl. etwa *Nowak/Rott et al.*, ZGR 2005, 252 (274, 276, 278 f.); *Bernhardt*, BB 2008, 1686 (1690 f.).
[149] *Martini*, JZ 2017, 1017 (1023).
[150] Zur Konkretisierung dieses Tatbestandsmerkmals im Wege exekutivischer Selbstprogrammierung siehe S. 45 ff.

mit Erfüllungspflichten, bürokratischem Aufwand und weiteren Kostenbürden, welche die wirtschaftliche Wertschöpfung nachhaltig beeinträchtigen können. Gerade bei dezentral vernetzten oder lernfähigen Systemen können Regulierungsmaßnahmen so einschneidend aufwendig sein, dass sie die Wirtschaftlichkeit des Systemeinsatzes unterminieren.[151] Nicht zuletzt deshalb ist regulatorisches Augenmaß geboten.

Ein Regulierungsansatz, der alle Anwendungen über einen Leisten schlägt, spränge vor diesem Hintergrund zu kurz. Dafür sind die unterschiedlichen Softwareanwendungen und -anbieter auch zu vielgestaltig. Ein gesetzliches System der Regulierung algorithmenbasierter Verfahren sollte daher nicht einer Rasenmäher-Methode folgen und jeden Betreiber treffen, der Algorithmen in seine Softwareanwendungen implementiert. Vielmehr sollte es sich von dem Gebot der Risikoadäquanz leiten lassen: Gesetzliche Handlungspflichten greifen nur bzw. erst dort, wo sie im Einzelfall tatsächlich geboten sind, um Gefahren einzudämmen, die von algorithmenbasierten Anwendungen ausgehen. Der Gesetzgeber ist mithin aufgerufen, geeignete Regulierungsschwellen zu identifizieren, damit seine Gebote einerseits zielgenau die richtigen Adressaten treffen, er andererseits aber nicht gleichsam die falsche Tür bewacht, sondern sich die Rechtsbefolgungskosten auf ein Maß begrenzen, das die wirtschaftliche Entwicklung und technische Innovationen nicht unangemessen ausbremst. Diese Schwellen inhaltlich zu definieren (I.) und Verfahrenswege zu finden, um einzelne Anwendungen in die Schwellenwerte einzuordnen (II.), gehört zu den wichtigsten, aber auch herausforderndsten Aufgaben des Gesetzgebers im Umgang mit algorithmenbasierten Verfahren.

I. Inhaltliche Konkretisierungsmaßstäbe

Regulierungsschwellen können sich an allgemeinen, insbesondere quantitativ messbaren Kriterien orientieren, die nicht nach dem Sachbereich fragen, in dem eine Software zur Anwendung kommt (1.). Umgekehrt kann es aber auch sinnvoll sein, Regulierungsschwellen bewusst nach den spezifischen Anwendungsgebieten auszurichten und danach zu clustern (2.) bzw. beide Modelle zu kombinieren (3.)

[151] *Martini*, Blackbox Algorithmus, 2019, S. 109 f.; vgl. auch *Reichwald/Pfisterer*, CR 2016, 208 (211).

1. Allgemeine Regulierungsschwellen

a) Feste Schwellen (z. B. Zahl der Mitarbeiter, Umsatz)

Einen ersten normativen Versuch, sich an eine geeignete Regulierungsschwelle heranzutasten, unternimmt im Datenschutzrecht die Vorschrift des Art. 30 Abs. 5 DSGVO: Er zieht eine Trennlinie für Verfahrensgebote allgemein bei einer Unternehmensgröße von 250 Mitarbeitern. Alle Verantwortlichen, die unter dieser Schwelle bleiben, befreit der Unionsgesetzgeber grundsätzlich[152] von der Pflicht, ein Verfahrensverzeichnis zu führen.

Die *Zahl der Mitarbeiter* kann zwar einen Anhaltspunkt für den Grad an technischen und organisatorischen Maßnahmen bieten, die einem Unternehmen *zumutbar* sind. Sie sagt als solche aber nur etwas darüber aus, wie viele Personen *als Arbeitnehmer* von einer Schließung des Betriebs betroffen wären – einen Rückschluss auf die Zahl der betroffenen *Verarbeitungsvorgänge*, geschweige denn deren datenschutzrechtliche Sensibilität, erlaubt sie hingegen nicht. Die Mitarbeiterzahl taugt daher nur in sehr begrenztem Umfang als Kriterium, um Regulierungsschwellen zu definieren, jenseits derer Akteure einer Regulierung zu unterwerfen sind.

Das Kartellrecht beschreitet (ebenso wie das Recht algorithmischen Handels mit Finanzinstrumenten[153]) einen etwas anderen Weg als die DSGVO: Es greift als Grenzschwelle auf den *Umsatz* zurück (vgl. etwa § 35 Abs. 1 GWB – „Umsatzerlöse von mehr als 500 Millionen Euro“ – bzw. Art. 1 Abs. 2 der VO (EG) Nr. 139/2004). Der Umsatz lässt einen Rückschluss auf die Marktdurchdringung zu, die ein Angebot erfahren hat. Unter den Bedingungen der Netzökonomie zeigen die Erfahrungen im Kartellrecht aber auch, dass Umsatzschwellen im digitalen Bereich als valides Aufgreifenskriterium ihre Trennschärfe einbüßen.[154] Daher hat der Gesetzgeber jüngst § 18 Abs. 2a, 3a GWB den Eigengesetzlichkeiten der Digitalwirtschaft angepasst: Bei der Marktstellung eines Unternehmens sind

[152] Die Verpflichtung bleibt allerdings bestehen, wenn die Verarbeitung regelmäßig erfolgt, besondere personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten betrifft oder aus sonstigen Gründen ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt. Vgl. zu dieser Regelung *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 30 DSGVO, Rn. 26 ff.

[153] Der Gesetzgeber geht davon aus, dass von hochfrequentem Handel auf Grund des erhöhten Handelsvolumens ein höheres Risiko ausgeht als von rein algorithmischem Handel. Deshalb unterliegt der Hochfrequenzhandel einem grundsätzlichen Erlaubnisvorbehalt und erweiterten Dokumentationspflichten, näher *Martini*, Blackbox Algorithmus, 2019, S. 147 ff.

[154] Gewinnschwellen übernehmen im digitalen Bereich kaum erfolgsversprechende Abgrenzungsfunktionen; vgl. etwa die Übernahme von *WhatsApp* durch *Facebook: Bundeskartellamt,* Gemeinsamer Leitfaden zur neuen Transaktionswert-Schwelle in der Fusionskontrolle in Deutschland und Österreich – öffentliche Konsultation, Pressemitteilung v. 14.5.2018; *Anonymous*, EU prüft Übernahme von WhatsApp, Focus Online vom 14.7.2014.

seither insbesondere Netzwerkeffekte sowie der Marktvorteil, über einen Zugang zu Daten zu verfügen, zu berücksichtigen. Ob der Dienstleister das Angebot im engeren Sinne entgeltlich oder im Austausch gegen Daten erbringt, ist für die kartellrechtliche Wertung nicht mehr maßgeblich.

Ob die neuen Kriterien bestimmt genug und auch praktikabel sind, muss sich im Praxistest erst noch beweisen.[155] Jedenfalls lösen sie als Schwellenkriterien eine wertungsintensive Prüfung der Kartellbehörden aus: Sie müssen auf der Grundlage eines komplexen Kriterien-Bündels feststellen, ob die Rechtsfolge des § 18 GWB im konkreten Fall eintritt.[156] Diesen tastend experimentellen Weg hat der Gesetzgeber offenbar bewusst mit dem Ziel beschritten, das GWB innovationsoffen zu halten[157] und der Vorschrift des § 18 GWB keine starren Grenzen zu ziehen.[158]

Als gesetzgeberische Anknüpfungsschwelle für die *persönlichkeitsrechtliche* Seite der Regulierung algorithmenbasierter Systeme eignen sich die Kriterien des § 18 Abs. 2a, 3a GWB aber nur sehr bedingt: Der Umsatz eines Unternehmens sagt wenig darüber aus, ob die verarbeiteten Daten oder die getroffenen Entscheidungen für die Rechte des Einzelnen oder die Gesellschaft substanzielle Risiken auslösen. Der Fokus des (marktordnenden) Kartellrechts ist insoweit seinem Wesen nach ein anderer als derjenige des Schutzes der Endnutzer: Jener richtet sich auf *Implikationen eines Unternehmens für den Wettbewerb*. Die Regulierung algorithmenbasierter Verfahren hat demgegenüber vorrangig den Schutz der Verbraucher als Marktteilnehmer und Träger von Persönlichkeitsrechten im Blick. Das Beispiel *Cambridge Analytica* hat der Öffentlichkeit eindrücklich vor Augen geführt, dass es keiner Milliardenumsätze bedarf, um die kollektive Privatsphäre zu bedrohen. Das Kriterium der Umsatzschwelle kann daher für die Marktrelevanz eines Angebots allenfalls einen ersten Orientierungsrahmen liefern. Denkbar ist es aber, an den Umsatz anzuknüpfen, um kleine Unternehmen gezielt aus einem Regulierungskorsett zu *befreien*, das ihre innovative Entfaltungskraft zu sehr einzuschnüren droht.[159]

[155] Vgl. *Podszun/Schwalbe*, NZKart 2017, 98 (101).
[156] Vgl. etwa *Paal*, in: Gersdorf/Paal (Hrsg.), BeckOK InfoMedR, 21. Ed. (Stand: 1.8.2018), § 18 GWB, Rn. 9.
[157] Vgl. BT-Drucks. 18/10207, S. 48 f. („Einzelfallwürdigung", „auf der Grundlage einer Gesamtbetrachtung aller gegebenen Umstände"); vgl. auch *Podszun/Schwalbe*, NZKart 2017, 98 (100).
[158] Die kartellrechtliche Literatur spricht bei derm Versuch, digitale Märkte abzugrenzen und Marktmacht zu beurteilen, von einem „Suchprozess der Praxis", vgl. *Podszun/Schwalbe*, NZKart 2017, 98 (102).
[159] So etwa Art. 17 Abs. 6 RL der neuen Urheberrechts-Richtlinie mit Blick auf Ausnahmen von der Anbieter-Verantwortung für Konstellationen, in denen Nutzer Online-Inhalte teilen („deren Jahresumsatz (…) 10 Millionen EUR nicht übersteigt").

b) Anzahl der (potenziell) Betroffenen

Eine wirksame Regulierung algorithmenbasierter Verfahren zielt zwar vorrangig darauf, Einzelschäden bei Individuen zu vermeiden. Die Zahl der (potenziell) Betroffenen indiziert aber auch eine signifikant erhöhte Ausstrahlungswirkung einer möglichen Rechtsverletzung. Wie risikoträchtig eine Software ist, hängt daher nicht zuletzt davon ab, wie viele Personen ihre Anwendungen konkret betreffen. Die Anzahl der Grundrechtsträger, die als Subjekt oder Objekt mit einem algorithmenbasierten Verfahren in Berührung kommen (werden), ist daher ein wichtiger Gradmesser dafür, ob Regulierungsmaßnahmen angezeigt sind. Auch Art. 35 Abs. 1 S. 1 DSGVO knüpft die Pflicht, eine Datenschutzfolgenabschätzung zu betreiben, zu Recht daran, welchen „Umfang" die Verarbeitung hat.

Einen ähnlichen Anknüpfungspunkt wählt auch der französische Gesetzgeber: Er reguliert Plattformen mit einer Anzahl von über 5 Millionen Verbindungen pro Monat strenger als solche mit geringerer Reichweite. Nur große Plattformen müssen (neben allgemeinen Transparenzvorschriften, die ihnen insbesondere abverlangen, Informationen über ihre wirtschaftliche Abhängigkeit preiszugeben) auch – behördlich kontrolliert – (selbst gesetzte) gute Verhaltensweisen bzw. -regeln („*bonnes pratiques*") befolgen.[160]

Einer treffsicheren Prognose, wo eine kritische Schwelle des Zulässigen im jeweiligen Einzelfall sachgerecht anzusiedeln ist, ist das Kriterium „Zahl der betroffenen Personen" allerdings seiner Natur nach nur eingeschränkt zugänglich. Setzt der Normgeber eine bestimmte Zahl fest, sagt sie nur bedingt etwas darüber aus, in wie vielen Fällen bspw. das Risiko eines Grundrechtseingriffs tatsächlich besteht oder wie intensiv diese Eingriffe sein könnten. Auch die Höhe des Einzelschadens lässt das Kriterium außer Acht. So nutzen Millionen Menschen eine Taschenrechner-App, ohne dass von ihr

[160] Art. D111-15 (in Kraft seit 1.1.2019) Code de la consommation: „I.-Le seuil du nombre de connexions au-delà duquel les opérateurs de plateformes en ligne sont soumis aux obligations de l'article L. 111-7-1 est fixé à cinq millions de visiteurs uniques par mois, par plateforme, calculé sur la base de la dernière année civile. […]";
Art. 111-7-1 Code de la consommation: „Les opérateurs de plateformes en ligne dont l'activité dépasse un seuil de nombre de connexions défini par décret élaborent et diffusent aux consommateurs des bonnes pratiques visant à renforcer les obligations de clarté, de transparence et de loyauté mentionnées à l'article L. 111-7. […]";
Art. 111-7 Code de la consommation: „[…] II.-Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur:
1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder;
2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne;
3° La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale, lorsque des consommateurs sont mis en relation avec des professionnels ou des non-professionnels […]".

per se eine Gefahr für deren Persönlichkeitsrechte ausgeht. Von einem kollaborationsfähigen Roboter, der mit 80 Exemplaren in dem Sonder-Marktsegment „Transport chemischer Stoffe“ zum Einsatz kommt, können demgegenüber ungleich größere Gefahren ausgehen. Eine *ausschließlich* „quantitative“ Betrachtung droht also, die tatsächlichen Gefahrenherde schnell zu übersehen. Sie ist als solche noch kein zuverlässiges Schwellenkriterium.

c) Grundrechtssensibilität als Schutzzweckzusammenhang

Die Suche nach einer geeigneten Aufgriffsschwelle sollte sich vor allem von dem Ziel leiten lassen, das hinter jeglicher Regulierung algorithmenbasierter Entscheidungssysteme steht: Sie ist im Kern Ausdruck staatlicher Schutzpflichten für die menschenwürdenahen Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung sowie die Gleichheitsgrundrechte („Sie [sc. die Menschenwürde] zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt“ [Art. 1 Abs. 1 S. 2 GG bzw. Art. 1 S. 2 GrCH]). Dann liegt es nahe, die *Grundrechtssensibilität* einer algorithmischen Entscheidung zum Anknüpfungspunkt für Regulierungsschwellen zu erheben: Je tiefer eine Anwendung in grundrechtlich geschützte Sphären eindringt, desto stärker ist nicht nur das Bedürfnis nach Transparenz, Gleichbehandlung sowie fairen Marktchancen, sondern umso eher sind auch Eingriffe in die Eigentums- und Berufsfreiheit verfassungsrechtlich rechtfertigbar bzw. geboten. Konsequenterweise heben auch Art. 24 Abs. 1 S. 1, 25 Abs. 1 S. 1, 32 Abs. 1 S. 1 und Art. 35 Abs. 1 S. 1 DSGVO auf die Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen ab.

Eine Blaupause für eine gestufte Regulierungskaskade liefert insbesondere das Arzneimittelrecht.[161] So teilt der Gesetzgeber den Arzneimittel*zugang* in drei Kategorien ein:[162] freiverkäuflich, apothekenpflichtig und verschreibungspflichtig.[163] Die Rasterung des Arzneimittelrechts ist wirkstofforientiert. Das Recht der Algorithmenregulierung ist in Anbetracht der Vielfalt seiner Anwendungsbereiche demgegenüber auf einen vielschichtigeren Kriterienkatalog angewiesen.

---

[161] Zu dem Referenzfeld der Arzneimittel*zulassung* siehe *Martini*, Blackbox Algorithmus, 2019, S. 131 ff.

[162] Seine rechtliche Konkretisierung nehmen die Verordnung über die Verschreibungspflicht von Arzneimitteln (Arzneimittelverschreibungsverordnung – AMVV) sowie die Verordnung über apothekenpflichtige und freiverkäufliche Arzneimittel (Arzneimittelverkaufsverordnung – AMVerkV) vor.

[163] *Freiverkäufliche Arzneimittel* lösen keine allgemeinen Gesundheitsrisiken aus und sind deshalb auch in Drogerien oder Supermärkten erhältlich – vgl. § 36 Abs. 1 S. 1 AMG. Für sie hält der Gesetzgeber eine Einschränkung des freien Erwerbs nicht für erforderlich, bspw. für Vitaminpräparate. *Apothekenpflichtige* Arzneimittel sind solche, die zwar keiner Verschreibung bedürfen, bei denen der Normgeber aber aufgrund ihrer Nebenwirkungen die Beratung eines Apothekers für geboten erachtet. Bei hohen Anwendungsrisiken gilt (für in Anlage 1 der AMVV festgeschriebene Stoffe) die

Um die Grundrechtssensibilität einer Softwareanwendung zu beurteilen, empfiehlt sich ein Schichtenmodell, das insbesondere nach der Intensität der Auswirkung auf die Entfaltung der Persönlichkeit in konkreten Anwendungsfällen differenziert – insbesondere danach, ob die Öffentlichkeitssphäre, die alltägliche Sozialsphäre oder aber die engere Privatsphäre als Kernbereich privater Lebensführung berührt ist. Auch dies kann jedoch nur ein erster Anhaltspunkt der Annäherung sein. Denn die einzelnen Lebensbereiche sind zum einen nicht hermetisch gegeneinander abgeschirmt, sondern die Übergänge sind fließend. Zum anderen kann eine Persönlichkeitsentfaltung auch gerade dadurch sensibel sein, dass sie in der Öffentlichkeit stattfindet.

aa) Ausstrahlungen auf Grundrechte jenseits des Rechts auf informationelle Selbstbestimmung

Besonderen Schutz sollte der Gesetzgeber dort gewähren, wo algorithmenbasierte Verfahren nicht nur auf die informationelle Selbstbestimmung, sondern auch nachhaltig auf sonstige Grundrechte einwirken. Dann verdichtet sich der objektiv-rechtliche Gehalt der Grundrechte am stärksten zu einer Schutzpflicht des Staates. Das gilt insbesondere für Ausstrahlungen auf das *Recht auf Leben und körperliche Unversehrtheit* (Art. 2 und 3 GRCh, Art. 2 Abs. 2 S. 1 GG), den *Gleichbehandlungsgrundsatz* (Art. 20 GRCh, Art. 3 GG [einschließlich der speziellen Diskriminierungsverbote aus Art. 21-26 GRCh, Art. 3 Abs. 2 und 3 GG) sowie die *Religionsfreiheit* (Art. 10 GrCH, Art. 4 GG), die *Meinungsfreiheit* (Art. 11 GRCh, Art. 5 GG), die *Versammlungs- und Vereinigungsfreiheit* (Art. 12 GRCh, Art. 8 Abs. 1, 9 Abs. 1 GG), die *Berufsfreiheit* (Art. 15 Abs. 1 und 16 GRCh, Art. 12 Abs. 1 GG), das *Eigentumsrecht* (Art. 17 GRCh, Art. 14 Abs. 1 GG), das *Gebot effektiven Rechtsschutzes* (Art. 47 Abs. 1 GRCh, Art. 19 Abs. 4 GG) sowie den *Fair-trial-Grundsatz* und das daraus abgeleitete Gebot der Waffengleichheit (Art. 47 Abs. 2 GRCh, Art. 6 EMRK).

Auch insoweit ist aber besonderes regulatorisches Augenmaß angezeigt: Privatwirtschaftliche Anwender algorithmenbasierter Verfahren sind in der Regel nicht unmittelbar grundrechtsverpflichtet (Art. 51 Abs. 1 S. 1 GRCh, Art. 1 Abs. 3 GG). Sie sind vielmehr selbst Grundrechtsträger: Sie können sich etwa auf ihre Berufs-, Vertrags- oder Eigentumsfreiheit berufen, um regulatorische Übergriffe

Verschreibungspflicht. Sie gefährden typischerweise die Gesundheit auch bei bestimmungsgemäßem Gebrauch, werden in erheblichem Umfang nicht bestimmungsgemäß gebraucht oder ihre Wirkweise ist der medizinischen Wissenschaft nicht allgemein bekannt, so dass sie nach der Wertung des Gesetzgebers nur unter ärztlicher Überwachung zum Einsatz kommen sollen. Vgl. BR-Drs. 359/18, S. 1.

des Staates abzuwehren. Eine sachgerechte Regulierung muss deshalb darauf zielen, die konkurrierenden Freiheits- und Gleichheitsrechte der Personen im Wege der praktischen Konkordanz möglichst grundrechtsschonend gegeneinander auszugleichen.

bb) Gefahr, Verbraucher aus wichtigen Lebensbereichen auszugrenzen – Teilhaberelevanz und Verfügbarkeit von Ausweichmöglichkeiten

In Ausnahmefällen kann das Handeln Privater andere Grundrechtsträger so stark in ihrer Lebensführung beeinträchtigen, dass sie ausnahmsweise einer besonderen – unmittelbaren – Grundrechtsbindung unterliegen.[164] Dieser Fall tritt insbesondere dann ein, wenn die Handlungsmacht einzelner privater Anbieter so groß ist, dass sie Menschen aus zentralen Lebensbereichen ausgrenzen kann. Tragende Gründe können dafür vor allem die gesellschaftliche Bedeutung bestimmter Leistungen oder die soziale Übermacht einer Seite sein, die aus der Abhängigkeit von einer Leistung erwächst (z. B. weil Betroffene nicht auf äquivalente alternative Angebote ausweichen können).[165] Diese Kriterien hat das BVerfG für Stadionverbote entwickelt. Sie eignen sich aber als Wertungskategorien auch als Erheblichkeitsschwelle für eine Regulierung algorithmenbasierter Verfahren, die auf die Schutzpflicht des Staates aus Art. 3 GG rekurriert: Gewährt eine algorithmenbasierte Anwendung – sei es aufgrund ihrer Marktmacht,[166] sei es aufgrund ihrer inhaltlichen Ausrichtung – den Zugang zu zentralen Lebensbereichen und übernimmt damit eine Gatekeeper-Funktion für die Entfaltung individueller Lebensentwürfe, ist es gerechtfertigt, sie strengeren normativen Anforderungen zu unterwerfen. Dort, wo demgegenüber dem Verbraucher in reicher Zahl Alternativen zur Verfügung stehen, die seine Bedürfnisse und Interessen in äquivalenter Weise befriedigen (also ein vollständig funktionsfähiger Markt besteht), schwächt sich das Bedürfnis nach Regulierung ab. Dann tritt die Eigenverantwortung des Betroffenen für eine sachgerechte Auswahlentscheidung in den Vordergrund.

Mit dieser Elle gemessen, ist es etwa angezeigt, die größten Auskunfteien einer regulatorischen Pflicht zu unterwerfen, die sicherstellt, dass die Entscheidungskriterien einer Score-Formel mit den Wertvorstellungen der Gesellschaft vereinbar sind. Denn Menschen sind wichtige Teilbereiche des alltäglichen Lebens nicht mehr zugänglich, wenn die Auskunftei ein Bild einer nicht kreditwürdigen Person von ihnen zeichnet. So ist es etwa sehr schwierig bis unmöglich, ein Konto zu eröffnen, einen

[164] Vgl. etwa zu Art. 3 Abs. 1 GG BVerfG, NVwZ 2018, 813 (815, Rn. 33).
[165] Zu all dem BVerfG, NVwZ 2018, 813 (815, Rn. 33).
[166] Vgl. dazu etwa *Weinzierl*, Warum das Bundesverfassungsgericht Fußballstadion sagt und Soziale Plattformen trifft, JuWissBlog Nr. 48/2018 vom 24.5.2018.

Handyvertrag oder einen Mietvertrag abzuschließen, wenn die SCHUFA zu dem Ergebnis kommt, eine Person verfüge über eine schlechte Bonität. Wenn die Information der Auskunftei aber auf einer falschen Datengrundlage, unzutreffenden Modellannahmen oder darauf beruht, dass die Software eine Person mit einem Namensvetter verwechselt, wird der Einzelne schnell zum Opfer eines unglücklichen Zufalls. Steuert in bestimmten Sektoren des Arbeitsmarkts ein Software-System die Bewerberauswahl fast ausschließlich oder überwiegend, wie etwa die Analysesoftware der Firma „HireVue“,[167] kommt ihm gegenüber den Bewerbern eine ähnliche Monopolstellung zu wie einem Kredit-Score einer Auskunftei.

Die Kriterien „aus zentralen, teilhaberelevanten Lebensbereichen ausgrenzen“ oder „soziale Mächtigkeit einer Seite“ sind aber abstrakt nur wenig rechtssicher operationalisierbar. Weder der Betroffene oder eine Aufsichtsinstanz noch der Betreiber können mit ihrer Hilfe ohne Weiteres rechtssicher abschätzen, ob die konkrete Regulierungsschwelle nun greift oder nicht. Als alleiniger gesetzlicher Abgrenzungsmaßstab eignen sie sich deshalb nur sehr bedingt. Sinnvoller ist es daher, sie als Orientierungsrahmen zu nutzen, um auf ihrer Grundlage entweder sektorspezifische Regulierungsschwellen für einzelne Anwendungen einzuziehen oder den Vollzugsinstanzen in den Grenzen des Parlamentsvorbehalts eine wertende Entscheidung für oder gegen die Regulierung zu überantworten.

cc) Besonders geschützte Datenkategorien

Greift eine Softwareanwendung auf besonders geschützte Datenkategorien im Sinne des Art. 9 Abs. 1 und Art. 10 DSGVO (vgl. auch ErwGrd 51 ff.) zurück, geht davon ein starkes Signal dafür aus, dass sie sensibel und regulierungsbedürftig ist (vgl. auch Art. 35 Abs. 3 lit. b DSGVO). Unter den Merkmalskranz sensibler Daten fallen insbesondere die rassische und ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung, genetische und biometrische Daten, Gesundheitsdaten sowie Daten zum Sexualleben und zur sexuellen Orientierung. Auch Daten über Kinder genießen besonderen Schutz (vgl. auch Art. 8 DSGVO; ErwGrd 38).

[167] Siehe dazu etwa *Wischmeyer*, Der Computer, der mich einstellte, brand eins vom 4.12.2017.

d) Zwischenfazit

Algorithmenbasierte Verfahren maßgeschneidert zu regulieren, ist nicht deshalb so knifflig, weil keinerlei Abgrenzungs- und Prognosekriterien existieren. Im Gegenteil: Es gibt zu viele relevante Faktoren, um eine einfache und treffsichere Abgrenzung vornehmen zu können. Isoliert an einzelne Aspekte, etwa die Zahl der potenziell Betroffenen, anzuknüpfen, um Regulierungsschwellen zu bestimmen, ist allenfalls in eng begrenzten Teilbereichen praktikabel. Eine *One size fits all*-Lösung wird auch der Vielfalt algorithmischer Verfahren, ihrer jeweiligen Zielrichtung sowie den unterschiedlichen grundrechtlichen Risikosphären nicht gerecht. Ein allgemeiner Maßstab, wie z. B. die Kategorie „mit grundrechtlichen Risiken verbunden“ oder die „rechtliche Wirkung oder ähnlich erhebliche Beeinträchtigung“ (Art. 22 Abs. 1 DSGVO), wäre zwar als kleinster gemeinsamer Nenner tauglich, zugleich aber zu unspezifisch, um daran konkrete Rechtsfolgen und Einstufungen zu knüpfen. Je nach Wirtschaftssektor und Nutzungsbereich algorithmenbasierter Entscheidungsprozesse werden daher für die Gefahrenprognose letztlich – nolens volens – unterschiedliche Parameter und Kriterien die regulatorische Marschrichtung bestimmen müssen.

2. Bereichsspezifische Regulierungsschwellen – Identifikation regelungsbedürftiger Anwendungen

Versucht der Gesetzgeber, eine Regulierungskaskade zu entwickeln, die den unterschiedlichen Risikostufen angemessen Rechnung trägt, kann es sinnvoll sein, bereichsspezifisch tastend vorzugehen: In einem ersten Schritt lassen sich gezielt besonders risikoreiche Sektoren identifizieren, die sowohl einer strengeren behördlichen Aufsicht als auch strengeren Pflichten unterworfen sind – von einem präventiven Kontrollmechanismus der Zulassung über eine Folgenabschätzung bis hin zu strengen Haftungsmaßstäben. Weniger einschneidende Pflichten – etwa Test- und Audit-Zugangsrechte für Kontrollinstanzen oder Transparenz- und Kennzeichnungspflichten – könnte der Gesetzgeber demgegenüber tendenziell breiter streuen, um im Einzelfall aufsichtliche Kontrollen durchführen und Risiken entgegenwirken zu können. Als Sektoren, die der Gesetzgeber für ein strengeres Regulierungsregime in Betracht ziehen sollte, kommen insbesondere in Betracht:

- Systeme, die *Gesundheitsdaten verarbeiten* und deren Entscheidungen Heilbehandlungen beeinflussen (insbesondere Gesundheits-Apps) oder deren Entscheidungen *körperliche Schäden* nach sich ziehen können (z. B. Pflegeroboter);

- *Auskunftei*-Scoring und Profiling, soweit davon (wie heute typischerweise) der Zugang zu wichtigen Lebensbereichen abhängt;
- algorithmenbasierte Entscheidungsprozesse bei *Versicherungen*, die für die Lebensführung wesentlich sind (z. B. Krankenversicherung, Kfz-Haftpflicht, Hausrat, Dienstunfähigkeit);
- neue Technologien, die ein *besonderes Maß an Auswertungsintensität* ermöglichen, insbesondere Gesichtserkennung, Key-logging, Sentimentanalyse, digitale Sprach-Assistenten sowie Smart-Home-Anwendungen (Siri, Alexa etc. [„Internet der Stimme"], insbesondere soweit mit ihnen das Risiko einhergeht, Daten unautorisiert zu erheben und zu versenden sowie Angriffe von außen zu ermöglichen oder Emotionen, Stimmungen bzw. sonstige Informationen aus dem Kernbereich privater Lebensführung zu analysieren) und personalisierte digitale Bildungsangebote;
- *autonomes Fahren*, insbesondere Fahrverhaltensanalyse;
- Anwendungen, die nachhaltig auf die *Meinungsbildung* der Bevölkerung ausstrahlen können, z. B. Social Bots, Bewertungsportale;
- algorithmenbasierte Entscheidungen des *Arbeitslebens* (Bewerberauswahl intern und extern; Leistungskontrolle durch Scoring oder Profiling);
- Mensch-Maschine-Kollaboration, z. B. Cobots, Exoskelette[168] oder digitale Arbeitsbrillen;
- private oder staatliche systematische Überwachung öffentlich zugänglicher Bereiche[169] sowie Smart-City- Konzepte, die mithilfe von Sensoren den Pulsschlag des örtlichen Gemeinwesens messen und Daten aus unterschiedlichen Quellen zu einem lokalen Steuerungskonzept zusammenführen;
- *staatlich* eingesetzte algorithmenbasierte Entscheidungsverfahren, auch solche zur Vorbereitung bzw. Unterstützung einer Entscheidung, insbesondere in der Justiz und Verwaltung.

3. Kombinationslösung

Ein wirksames Regulierungs- und Kontrollsystem für algorithmenbasierte Verfahren, das alle Risikoaspekte berücksichtigen will, sollte nicht nur regelungsbedürftige Sektoren bereichsspezifisch identifizieren, sondern auch allgemeine Kriterien der Gefahren in der *Zusammenschau* mehrerer Einzelaspekte als Maßstab heranziehen und miteinander verbinden. Bei der Herkulesaufgabe, kritische

[168] Dazu *Martini/Botta*, NZA 2018, 625 (625 ff.).
[169] Vgl. auch Art. 35 Abs. 3 lit. c DSGVO.

Regulierungsschwellen zu definieren, führt letztlich nur eine *Risikogesamtbetrachtung* zum Erfolg.[170]

a) Risikofaktoren

Seinem Wesen nach bestimmt sich das Risiko einer Softwareanwendung aus dem Zusammenspiel zweier Faktoren: Es ist das Produkt aus Eintrittswahrscheinlichkeit und Schadensschwere.[171] Zu den Risikofaktoren, welche die Schadensschwere determinieren können, gehören insbesondere die Art (aa) und das Ausmaß (bb) des Schadens.

aa) Art des Schadens

Typische Gefahren, die aufgrund der *Art* des drohenden Schadens Regulierungsbedarf auslösen, sind insbesondere

- eine Diskriminierung von Personen, insbesondere durch Systeme, die in substanziellem Umfang besondere Kategorien personenbezogener Daten oder Daten über Straftaten (vgl. Art. 9 f. DSGVO) verarbeiten;[172]
- nur schwer reversible Schäden, insbesondere
    - Rufschädigung, Identitätsdiebstahl oder -betrug,
    - der Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen,
    - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung personenbezogener Daten sowie der unbefugte Zugang zu ihnen;[173]
- Entscheidungen, die auf einer umfassenden Bewertung persönlicher Aspekte beruhen und nachhaltige Beeinträchtigungswirkung entfalten können, etwa Profilbildungsmaßnahmen – besonders dann, wenn sie mit Standortdaten verknüpft sind;[174]

[170] Dieses Verständnis liegt auch dem Risikobegriff der DSGVO zugrunde, wie er insbesondere in Art. 24 Abs. 1 S. 1, Art. 25 Abs. 1, Art. 32 Abs. 1, Art. 35 Abs. 1 DSGVO zum Ausdruck kommt.
[171] *Martini*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 35 DSGVO, Rn. 15b; vgl. auch ErwGrd 90 S. 1 sowie *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", WP 248, 4.10.2017, S. 9 ff.
[172] Vgl. auch die normative Wertung des Art. 35 Abs. 3 lit. b DSGVO.
[173] Vgl. auch ErwGrd 75, 83 S. 3 DSGVO sowie 85 S. 1 DSGVO.
[174] Vgl. auch Art. 35 Abs. 3 lit. a DSGVO.

- die Herauslösung von (insbesondere sensiblen) Daten aus dem ursprünglichen Verarbeitungskontext, um sie neuen Verarbeitungszwecken im Rahmen einer Big-Data-Analyse zuzuführen.

bb) Ausmaß des Schadens

Gefahren, die sich aus dem *Ausmaß* des Schadens ergeben, sind insbesondere:

- Auswirkungen auf eine Vielzahl Betroffener;[175]
- die Ausstrahlung auf andere Grundrechte jenseits des Rechts auf informationelle Selbstbestimmung, insbesondere Leib und Leben sowie Versammlungs- und Meinungsfreiheit;[176]
- der Umfang, die Umstände, die Häufigkeit und Dauer der Verarbeitung bzw. Speicherung. Je mehr Daten in ein Auswertungsnetz eingehen, je engmaschiger die Software die Daten miteinander verknüpft, je sensibler der Kontext, in dem die Verarbeitung stattfindet, je länger die Verarbeitung dauert und je häufiger sie erfolgt, umso größer ist typischerweise die Sensibilität, die von dem Verarbeitungsvorgang ausgeht (vgl. auch Art. 24 Abs. 1 S. 1, Art. 25 Abs. 1 und Art. 35 Abs. 1 S. 1 DSGVO).

b) (Qualitative) Risikoschwellenkonkretisierung

Obgleich das Bedürfnis nach leicht bestimmbaren Abgrenzungskategorien hoch ist: Die notwendige Gesamtbetrachtung kann schwerlich allein mit einer quantitativen Anknüpfungsschwelle operieren. Sie muss auch *wertende* Elemente einbinden – insbesondere muss sie berücksichtigen, ob die Kombination der einzelnen Aspekte eine zuvor festgelegte (auch qualitative) Schwelle erreicht. Die Entscheidung darüber, ob die Risikoschwelle überschritten ist, kann der Normgeber aber im Grundsatz abstrakt in Positiv- und Negativlisten[177] treffen.

[175] Siehe dazu bereits oben S. 44 f.
[176] Siehe dazu bereits oben S. 47.
[177] Vgl. das ähnliche Regelungsmodell des Art. 35 Abs. 4 und 5 DSGVO. Siehe auch die Positivliste der BfDI, https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html (24.4.2019).

II. Verfahrensrechtliche Instrumente der Konkretisierung – Grenzen der Delegation von Regelungsmacht

Da sich technische Innovationen der digitalen Welt in rasantem Zyklus fortschreiben, ist der Gesetzgeber bei dem Unterfangen, Regulierungsschwellen zu konkretisieren, auf eine Prognoseentscheidung angewiesen. Diese ist ihrem Wesen nach mit Unsicherheiten behaftet. Nicht alle Entwicklungen und Risiken lassen sich zuverlässig und abschließend antizipieren. Ein zu enges normatives Korsett zu schnüren, nimmt dann auch die Bewegungsfreiheit, um auf die Besonderheiten des Einzelfalls passgenau reagieren können. Schon vor dem 21. Jahrhundert sah es *Georg Jellinek* als nahezu „unmöglich" an, „das reale Leben des Staates a priori ausnahmslos durch Gesetz leiten zu wollen".[178] Ein gangbarer Ausweg aus einem statischen Normierungslabyrinth kann darin bestehen, der Exekutive einen Konkretisierungskorridor zu eröffnen, um die Treffsicherheit der normativen Steuerungsvorgaben auch unter den dynamischen Bedingungen schnell fortschreitender technischer Entwicklungen zu erhalten und auf situative Steuerungsnöte adäquat reagieren zu können. Insbesondere könnte der Normgeber für die einzelnen Regulierungs- und Kontrollinstrumente Ausnahmetatbestände und Flexibilisierungsklauseln implementieren, die es – abhängig von einer kategorisierenden Einzelfallbewertung – gestatten, von einer gesetzlichen Grundregel abzuweichen.

Exekutivische Bewertungsverfahren, die den Regulierungsbedarf im Einzelfall eruieren und adjustieren sollen, kennt die Rechtsordnung zuhauf – vom Verfahren der Marktdefinition und Marktanalyse nach § 10 f. TKG (mit Beurteilungsspielraum der Regulierungsbehörde, § 10 Abs. 2 S. 2 TKG) über die Befreiung von der Verpflichtung, ein Angebot für eine Zielgesellschaft abzugeben und zu veröffentlichen (§ 37 Abs. 1 WpÜG), sowie die Befreiung von der Passpflicht (§ 2 Abs. 1 Passgesetz) bis hin zum baurechtlichen Dispens auf der Grundlage des § 31 Abs. 2 BauGB.

Soll die Verwaltung in Zukunft auch algorithmenbasierte Entscheidungsprozesse bewerten, könnte sie sowohl der potenziellen Schadenshöhe (insbesondere mit Blick auf die Grundrechtsrelevanz, die Zahl der Betroffenen etc.) als auch der Eintrittswahrscheinlichkeit jeweils einen Risikowert zuweisen, den sie zu einer wertenden Gesamtentscheidung aggregiert. Die Risikowerte gleicht sie dann mit den Schwellenwerten ab, die der Gesetzgeber zuvor festgelegt hat.

[178] *Jellinek*, Gesetz und Verordnung, 1919 (1887), S. 369.

Ist die Risikoschwelle erreicht, ist es dann aber auch notwendig, den (wirtschaftlichen) Interessen des Anbieters – gleichsam in einer „umgekehrten Folgenabschätzung" – Rechnung zu tragen. Sowohl die Legislative als auch die kontrollierende Behörde sind an das Prinzip der Verhältnismäßigkeit – auch und gerade gegenüber den privatwirtschaftlichen Akteuren der Digitalwirtschaft – gebunden. In die Waagschale für eine Rückausnahme fallen dabei insbesondere der notwendige Ressourcenaufwand, die praktische Umsetzbarkeit der zusätzlichen Pflichten (etwa mit Blick auf Start-ups) sowie das Risiko, dass Geschäfts- und Betriebsgeheimnisse an die Öffentlichkeit gelangen könnten.

Die Einschätzung darüber, ob bestimmte Pflichten zu beachten sind, lässt sich prinzipiell auch im Wege einer „Selbstkategorisierung" auf das Regulierungsobjekt bzw. den Betreiber des algorithmenbasierten Entscheidungssystems selbst übertragen. Eine Fehleinschätzung könnte die Rechtsordnung sowohl mit (verschärfter) Haftung, insbesondere einer Verschiebung der Beweislast und Verschuldensvermutung, als auch mit Sanktionen beantworten. Ein System der Selbsteinschätzung kann nicht zuletzt bürokratischen und finanziellen Aufwand minimieren – ist doch der Betreiber schneller als eine Aufsichtsbehörde dazu in der Lage, auf Veränderungen der realen Ausgangsbedingungen zu reagieren in der Lage. Allerdings verbindet sich mit einem solchen Ansatz zum einen ein erhebliches Maß an Rechtsunsicherheit. Zum anderen sind Risikoselbsteinschätzungen nur dort verantwortbar, wo sich absehbare Risiken unterhalb einer kritischen Schwelle bewegen, die keine tiefgreifende Regulierung (und insbesondere: keine eng gestrickte staatliche Aufsicht) erfordert.

1. Normkonkretisierung in der nationalen Rechtsordnung

a) Verfassungsrechtliche Rahmenbedingungen – Rechtsverordnungen als Instrument der Normkonkretisierung

Regulierungs- und Kontrollinstrumente durch normative Leitvorgaben operationabel auszugestalten, behält die Funktionenordnung des Grundgesetzes grundsätzlich dem Parlament vor. Als Gravitationszentrum der demokratischen Willensbildung ist es dazu berufen, die zentralen politischen Steuerungsentscheidungen des Gemeinwesens zu treffen.

Das Parlament genießt jedoch kein Rechtsetzungsmonopol.[179] Die *normative Feinsteuerung* darf es – in den Grenzen des Art. 80 GG – der Exekutive anvertrauen. Es kann dem Verordnungsgeber insbesondere die Rechtsmacht zugestehen, Ausnahmen von gesetzlichen Regulierungspflichten im

[179] *Martini*, AöR 133 (2008), 155 (160).

Wege delegierter Rechtsakte zu definieren bzw. umgekehrt in bestimmten Bereichen die konkrete Reichweite regulatorischer Pflichten normkonkretisierend zu spezifizieren.

Von dieser gestuften Regelungstechnik macht bspw. das Immissionsschutzrecht bei einer wichtigen Weichenstellung Gebrauch: Der Anhang 1 zur 4. BImSchV definiert konstitutiv alle Anlagen, die genehmigungsbedürftig i. S. d. § 4 Abs. 1 S. 3 BImSchG i. V. m. § 1 Abs. 1 S. 1 der 4. BImSchV sind. Ein solcher Weg ist auch als Teil eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse im Grundsatz gangbar: Der Gesetzgeber könnte die Konkretisierung derjenigen Softwareanwendungen, die einer spezifischen regulierungsbedürftigen Risikoklasse unterfallen, einer Rechtsverordnung überantworten. Umgekehrt könnte der Gesetzgeber dem Verordnungsgeber zugestehen, für einzelne normative Regelungsinstrumente mit niedrigschwelligen delegierten Rechtsakten sektorspezifisch Ausnahmen oder Befreiungen vorzusehen, um mit der Dynamik und den Reaktionsbedürfnissen der digitalen Welt Schritt zu halten. Der Delegatar – namentlich die Bundesregierung oder eines ihrer Ministerien – könnte dann einzelne Sektoren oder Anwendungsformen gezielt von grundsätzlich allgemein geltenden Regeln ausnehmen – oder einzelne seiner Rechtspflichten sektorspezifisch für einzelne Anwendungen modifizieren und feinjustieren. Einen ähnlichen Ansatz verfolgt der Normgeber auch im Baurecht in Gestalt der BauNVO (siehe jeweils Abs. 3 der §§ 2-9 BauNVO) sowie im Gentechnikrecht (bspw. in § 30 sowie u. a. §§ 17b, 18 Abs. 3, 36 GenTG).[180] So gestattet etwa § 17b Abs. 1 S. 2 GenTG der Exekutive, einzelne Produkte unterhalb eines zuvor festgelegten Schwellenwertes durch Rechtsverordnung von der ansonsten obligatorischen Kennzeichnungspflicht (vgl. Art. 21 RL 2001/18/EG) auszunehmen, sofern bei ihnen zufällige oder technisch nicht zu vermeidende Anteile von gentechnisch veränderten Organismen nicht auszuschließen sind. Ein solches „normativ-iteratives“ Vorgehen – also Risikoschwellenwerte festzulegen bzw. Anwendungssektoren zu konkretisieren und ihren Pflichtenradius via Rechtsverordnung detailliert zu kategorisieren – wählt der Normgeber auch im Wasserrecht: § 57 Abs. 2 WHG ermächtigt die Exekutive dazu, die Anforderungen an den „Stand der Technik“ beim Einleiten von Abwasser in Gewässer durch Rechtsverordnungen festzulegen.[181] Davon hat der Verordnungsgeber in 57 Anhängen zur Abwasserverordnung Gebrauch gemacht und en détail konkretisiert, welche Anforderungen und

[180] Die Rechtsprechung hat die Normkonkretisierungsbefugnis der Verwaltung im Gentechnikrecht höchstrichterlich bestätigt, siehe etwa BVerwG, NVwZ 1999, 1232 (1233 f.).
[181] Vgl. zur Vorgängervorschrift § 7a WHG a. F., für welche die Rechtsprechung der Verwaltung eine Normkonkretisierungsbefugnis zugesprochen hat, BVerwGE 107, 338 (340 ff.).

Grenzwerte bei spezifischen Einleitungsprozessen im Einzelnen zu beachten sind – vom häuslichen und kommunalen Abwasser über die Milchverarbeitung bis hin zu Wollwäschereien.

b) Grenzen normativer Delegation von Regelungsmacht an Private, insbesondere eine technisch-ethisch besetzte Expertenkommission

Statt den Umweg einzuschlagen, Rechtsmacht an die Exekutive zu delegieren, hat auf den ersten Blick ein anderer Gedanke Charme: Für den Gesetzgeber ist es verlockend, die Aufgabe, Sektoren oder Anwendungsformen von einer sonst allgemein geltenden Regelung auszunehmen, unmittelbar einer *Expertenkommission* zu übertragen.

Der Idee, es einem interdisziplinären Gremium zu überlassen, geltendes Recht zu konkretisieren, stellt die Verfassung jedoch unüberwindbare Grenzen in den Weg. Denn Art. 80 GG steckt einen engen verfassungsrechtlichen Rahmen dafür ab, normative Regelungsmacht zu delegieren: Das Grundgesetz ermöglicht zwar Normsetzung, arbeitsteilig und dekonzentriert zu organisieren, um das Parlament zu entlasten und die Rechtsnormen den Bedürfnissen einer dynamischen Gesellschaft zeitgerecht anzupassen.[182] Als Ausfluss des Demokratie- und Gewaltenteilungsprinzips definiert Art. 80 GG zugleich aber abschließend die Voraussetzungen, unter denen eine delegierte Normsetzung möglich ist. Weder der Verordnungsgeber noch der parlamentarische Gesetzgeber darf von ihnen abweichen. Die Verfassung bindet es bewusst an hohe Voraussetzungen (insbesondere hinsichtlich Inhalt, Zweck und Ausmaß der Ermächtigung), *die Verwaltung* mit eigener Regelungsmacht zu betrauen. Im Umkehrschluss ergibt sich daraus, dass andere Formen, Rechtsmacht zu delegieren – insbesondere sie privaten Akteuren anzuvertrauen – erst recht unzulässig sind. Art. 80 Abs. 1 S. 4 GG gestattet zwar eine weitere Subdelegation von Regelungsmacht: Sie ist zulässig, soweit ein Gesetz vorsieht, „daß eine Ermächtigung weiter übertragen werden kann“ und die Exekutive die Ermächtigung via Rechtsverordnung überträgt.[183] Taugliche Delegatare sind aber ausschließlich staatliche, also in die ununterbrochene demokratische Legitimationskette eingebundene

[182] *Martini*, AöR 133 (2008), 155 (160).
[183] Vgl. zur gesetzlichen Delegationssperre des Art. 80 GG ausführlich bspw. *Martini*, AöR 133 (2008), 155 (159 ff.).

Einrichtungen. Art. 80 GG fungiert insoweit als Sicherungsring der Demokratie: Er soll die „Unverbrüchlichkeit des demokratischen Legitimationszusammenhanges“[184] für jede Staatstätigkeit absichern. Deshalb schließt er es konsequenterweise aus, originäre Regelungsmacht an nicht-staatliche Gremien zu delegieren.[185]

Unzulässig sind insbesondere dynamische Verweisungen auf Normwerke, die nicht auf dem förmlichen Weg, den die Verfassung für den Erlass von Normen vorsieht,[186] zustande gekommen sind – bspw. der Verweis auf eine DIN-Norm „in der jeweils geltenden Fassung“. Der Gesetzgeber muss vielmehr für jeden konkreten Normakt die Verantwortung in Kenntnis seines konkreten Inhalts übernehmen.[187] In der Sache überträgt der Gesetzgeber ansonsten Privaten legislative Gewalt in verfassungswidriger Weise: Ihnen stünde die Tür offen, sich die zentrale Aufgabe, demokratisch legitimierte Regeln für das Gemeinwesen zu definieren, zu Eigen zu machen und Grundrechte Dritter eigenmächtig einzuschränken. Das ausdifferenzierte Delegationssystem des Art. 80 GG – und damit sein Sinngehalt als Bollwerk der verfassungsrechtlichen Funktionenordnung – ließe sich mühelos unterlaufen.

Während dynamische Verweisungen die Grenzen zulässiger Normdelegation überschreiten,[188] sind *statische* Verweisungen auf Regelwerke privater Einrichtungen, z. B. Industrienormen des DIN, zulässig.[189] Deren Inhalt ist nämlich zu dem Zeitpunkt, zu dem das Gesetz in Kraft tritt, fix. Der Normgeber kann ihn in seinen Willen aufnehmen und sich durch normative Entscheidung zu ihrem Inhalt bekennen.[190] Mit dieser Zielrichtung macht der Gesetzgeber von der Möglichkeit, auf private Normen statisch zu verweisen, insbesondere im Umweltrecht und Technikrecht vielfach Gebrauch –

[184] *Martini*, AöR 133 (2008), 155 (161).
[185] *Lepa*, AöR 105 (1980), 337 (359); *Kloepfer*, Umweltrecht, 4. Aufl., 2016, S. 153 m. w. N.
[186] Vgl. dazu im Einzelnen *Becker*, Kooperative und konsensuale Strukturen in der Normsetzung, 2005, S. 381 ff.; zu praktischen Anwendungsfällen insbesondere *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, S. 173 ff.
[187] *Kloepfer*, Umweltrecht, 4. Aufl., 2016, S. 154.
[188] Dogmatisch bemerkenswert (und verfassungsrechtlich unzulässig) ist unter dem Gesichtspunkt der Funktionenordnung des Grundgesetzes der Änderungsvorbehalt, den § 113 S. 5 GWB dem Bundestag im Hinblick auf die VgV zugesteht: Er kann die Verordnung durch Beschluss ändern; vgl. hierzu *Fandrey*, in: Kulartz/Kus/Portz et al. (Hrsg.), 4. Aufl., 2016, § 113, Fn. 8 f. Das Parlament wird dadurch – außerhalb der verfassungsrechtlich vorgezeichneten Formen der Gesetzgebung – (durch Beschluss) zum Verordnungsgeber. Solche Änderungsvorbehalte hebeln die Dogmatik des Art. 80 GG aus. Vgl. zur verfassungsrechtlichen Problematik der parlamentarischen Änderungsvorbehalte in Verordnungsermächtigungen *Saurer*, NVwZ 2003, 1176 (1177 ff.); *Martini*, AöR 133 (2008), 155 (176). Zulässig wäre eine Änderung der Verordnung nur durch verordnungsänderndes *Gesetz*.
[189] *Kloepfer*, Umweltrecht, 4. Aufl., 2016, S. 154 m. w. N.
[190] Zu den urheberrechtlichen Implikationen einer Inkorporation privater Regelwerke in Gesetze siehe § 5 Abs. 1 UrhG bzw. zur Verweisung § 5 Abs. 3 UrhG.

etwa in den Verweisen des § 3 Abs. 1 der 1. BImSchV und § 2 Abs. 8, 19, § 6 Abs. 1 der 13. BImSchV auf private Normen des DIN e. V.[191]

Verfassungsrechtlich zulässig ist es auch, wenn eine sachverständig besetzte Kommission an der Normsetzung lediglich *mitwirkt* – etwa indem sie Vorschläge für den delegierten Gesetzgeber entwickelt. Denn mitwirkende Beratung ist mit Normsetzung nicht ohne Weiteres gleichzusetzen; der demokratischen Legitimation bedürfen vielmehr allein (unmittelbar verbindliche) normative Gebote mit Entscheidungscharakter.

Bezieht der Staat Private in einen hoheitlichen Entscheidungszusammenhang ein, der in verbindliche Normen mündet, muss er aber seiner Legitimationsverantwortung angemessen gerecht werden. Er muss insbesondere das Entscheidungsumfeld angemessen demokratiesichernd ausgestalten,[192] namentlich ein hinreichendes Gesamtlegitimationsniveau herstellen.[193] Insbesondere muss er den Rahmen für die organisationsinterne Entscheidungsbildung des Sachverständigengremiums vorgeben und die Entscheidungsfindung transparent gestalten.[194] Die Anforderungen daran, wie stark der Staat den Entscheidungsprozess durch formale und materielle Vorgaben einhegen muss, steigen dabei mit der Durchschlagskraft privater Normsetzungsentwürfe.[195] Solange Regelungsvorschläge einer Expertenkommission *nicht verbindlich* sind und der Staat den normgebenden Prozess aus eigener Kraft steuert, ist es regelmäßig zulässig, dass eine Expertenkommission Vorschläge unterbreitet, das geltende Recht auf eine bestimmte Art und Weise zu konkretisieren.

So könnte eine juristisch, technisch, ethisch und ökonomisch besetzte Expertenkommission dem Normgeber Vorschläge unterbreiten, welche Sektoren oder Anwendungsformen er von den allgemeinen Regelungen für algorithmenbasierte Entscheidungsprozesse ausnehmen sollte. Der Gesetzgeber könnte es der Exekutive auch als verfahrensrechtliche Vorgabe mit auf den Weg geben, bei der Vorbereitung delegierter Rechtsakte eine Expertenkommission oder eine Gruppe Sachverständiger zu beteiligen. Davon macht der Gesetzgeber in anderen Normbereichen bereits Gebrauch. So gesteht bspw. § 1 Abs. 2 S. 2 Mindestlohngesetz einer ständigen Kommission der Tarifpartner, der

[191] Auch die TA Luft und TA Lärm verweisen als bindende Verwaltungsvorschrift vielfach auf Richtlinien des VDI und Normen des DIN Vgl. bspw. Ziffer 5.1.1 letzter Satz sowie Ziffer 5.2.6.3 der TA Luft oder Ziffer 2.6 und Ziffer A.1.6 (Anlage) der TA Lärm.
[192] *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, S. 84; *Ruffert*, Rechtsquellen und Rechtsschichten des Verwaltungsrechts, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts Bd. I, 2. Aufl., 2012, S. 1163 (1214 f.).
[193] BVerfGE 47, 253 (273); 83, 60 (73); 93, 37 (68); 107, 59 (94).
[194] *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, S. 84.
[195] *Augsberg*, Rechtsetzung zwischen Staat und Gesellschaft, 2003, S. 85.

sog. Mindestlohnkommission, ein Vorschlagsrecht zu. § 36 Abs. 1 S. 1 AMG formuliert bspw. gar eine Pflicht, Sachverständige anzuhören, bevor eine Rechtsverordnung ergeht..

Ein praktisch wichtiges Beispiel einer exekutiven Normkonkretisierung, die auf der Grundlage einer externen Beratung durch zahlreiche andere Einrichtungen ergeht, sind die „Technischen Anleitungen" im Sinne des § 48 BImSchG – die *TA Luft und TA Lärm*: Die Bundesregierung erlässt nach Anhörung gemäß § 51 BImSchG und mit Zustimmung des Bundesrates allgemeine Verwaltungsvorschriften im Sinne des Art. 84 Abs. 2 GG, um das (in Landeseigenverwaltung zu vollziehende) BImSchG zu konkretisieren. Als *normkonkretisierende Verwaltungsvorschriften*, die auf wissenschaftlich fundierten Aussagen beruhen und in einem vielschichtigen Abwägungsmechanismus ergehen, der für ein hohes Maß an Sachverstand und Sachrichtigkeit und Legitimation durch Verfahren[196] verbürgt,[197] binden die TA Luft und TA Lärm nicht nur die Verwaltung selbst. Sie entfalten auch gegenüber den Gerichten begrenzte Außenwirkung.[198]

Beide Wege – normkonkretisierende Verwaltungsvorschrift und statischer Verweis auf private Normwerke – kann der Normgeber auch einschlagen, um konkrete Schwellen oder Kriterien dafür festzulegen, wann Regulierungsinstrumente zu algorithmenbasierten Verfahren konkret greifen. So könnte der Gesetzgeber die einzelnen Regulierungswerkzeuge (in den Grenzen der Grundrechtswesentlichkeit)[199] auf der Tatbestandsseite vergleichsweise offen formulieren. Darauf aufbauend könnte er die Exekutive ermächtigen – unter Mitwirkung aller relevanten Stakeholder – Kriterien dafür zu erarbeiten, unter welchen Voraussetzungen welche Regulierungswerkzeuge eingreifen oder ausgeschlossen sind. Auf diese Weise könnte er ein abstraktes, weit formuliertes Regelwerk durch Rechtsverordnungen und allgemeine Verwaltungsvorschriften in seinen Details konkretisieren. Denkbar ist es auch, dass der Gesetzgeber auf spezifizierte Kriterienkataloge (etwa privater Normungsinstitute) statisch verweist und ihren Inhalt in seinen Willen teilweise aufnimmt.[200]

[196] Dazu tragen insbesondere die Anhörung der beteiligten Kreise und die Zustimmung des Bundestages bei. Sowohl in den Erstentwurf des Ministeriums als auch in der Beteiligung nach § 51 BImSchG sind in reichem Umfang private, sachverständige Stellen eingebunden (namentlich ein „Kreis von Vertretern der Wissenschaft, der Betroffenen, der beteiligten Wirtschaft, des beteiligten Verkehrswesens […]").

[197] Zunächst galten sie als antizipierte Sachverständigengutachten; BVerwGE 55, 250 (256 ff.).

[198] Vgl. etwa BVerwGE 72, 300 (320 f.); 129, 209 (212, Rn. 12).

[199] Die wesentlichen Entscheidungen der Grundrechtsausübung müssen stets beim Parlament verbleiben; er darf diese nicht delegieren. Vgl. dazu etwa BVerfGE 47, 46 (55).

[200] Ob es einem in erster Linie technisch besetzten Gremium – etwa dem Konsortium einer DIN-Norm – gelingen kann, rechtliche Vorgaben im Hinblick auf Ausnahmetatbestände passgenau zu konkretisieren, fragt sich jedoch.

2. Unionsrechtliche Rahmenbedingungen der Normkonkretisierung

Instrumente exekutiver Normkonkretisierung kennt nicht nur das nationale Recht, sondern auch das Recht der Europäischen Union. In den Feldern „Datenschutz“ und „Kartellrecht“ steuert es bereits heute immer stärker zentrale Entscheidungsvorgaben.

a) Delegierte Rechtsakte der Kommission

Der Vertrag über die Arbeitsweise der Europäischen Union (AEUV) gestattet es dem Unionsgesetzgeber, der Kommission legislative Befugnisse zu übertragen. Er installiert dafür das Instrument delegierter Rechtsakte (Art. 290 Abs. 1 UAbs. 1 S. 1 AEUV). Ermächtigt ein EU-Rechtsakt die Kommission dazu, von dem Instrument Gebrauch zu machen, kann sie es nutzen, um den Basisrechtsakt zu ergänzen und (formal) zu ändern.[201]

Mit Blick auf ihre Ergänzungsbefugnis sind delegierte Rechtsakte mit Rechtsverordnungen des deutschen Rechts im Sinne des Art. 80 GG funktional vergleichbar. Auch sie sollen dafür sorgen, dass allgemeine Sekundärrechtsakte (Verordnungen und Richtlinien) auf mitgliedstaatlicher und unionaler Ebene vollzugsfähig sind.[202]

Im Bereich des algorithmischen Handels mit Finanzinstrumenten hat die Europäische Union bereits gezielt auf Instrumente der exekutivischen Gesetzeskonkretisierung zurückgegriffen. Drei delegierte Verordnungen der Kommission[203] konkretisieren sowohl den Anwendungsbereich[204] und die Mindestgrößen[205] als auch die einzelnen organisatorischen Pflichten[206] beim algorithmischen Handel mit Finanzinstrumenten.

---

[201] *Weiß*, EuR 2016, 631 (642 f.).

[202] Daneben kennt das unionsrechtliche Primärrecht das Mittel des Durchführungsrechtsakts (Art. 291 Abs. 2 AEUV). Einen solchen zu erlassen, liegt grundsätzlich in den Händen der Kommission (in Ausnahmefällen des Rates). Ein solches Konkretisierungsverfahren sieht etwa das Rechtsregime für Beihilfen vor: Auf der Grundlage des Art. 109 AEUV kann der Rat Durchführungsverordnungen erlassen. Davon macht er in der sog. Gruppenfreistellungsverordnung Gebrauch. Sie konkretisiert, unter welchen Voraussetzungen einzelne Fördermaßnahmen in den einzelnen Sektoren dem beihilfenrechtlichen Pflichtenregime unterliegen. Ähnlich sind die Gruppenfreistellungsverordnungen im Kartellrecht nach Art. 101 Abs. 3 AEUV konzipiert, die kraft § 2 Abs. 2 GWB auch im deutschen Kartellrecht gelten.

[203] Delegierte Verordnung (EU) 2017/589 v. 19.7.2016, ABl. L 87 v. 31.3.2017, S. 417; Delegierte Verordnung (EU) 2017/565 v. 25.4.2016, ABl. L 87 v. 31.3.2017, S. 1; Delegierte Verordnung (EU) 2017/588 v. 14.7.2016, ABl. L 87 v. 31.3.2017, S. 411.

[204] Art. 18 DelVO (EU) 2017/565.

[205] Art. 2 DelVO (EU) 2017/588.

[206] DelVO 2017/589.

Wesentliche Teile eines Gesetzgebungsaktes (im Sinne des Art. 289 Abs. 3 AEUV) dürfen delegierte Rechtsakte jedoch nicht ergänzen oder ändern. Vielmehr muss ein übertragender Rechtsakt Ziele, Inhalt, Geltungsbereich und Dauer der Befugnisübertragung auf die Kommission ausdrücklich festlegen.[207] Dieser sog. Wesentlichkeitsvorbehalt soll verhindern, dass die Kommission das Heft des Handelns unter Verstoß gegen die Institutionenordnung an sich zieht, indem sie normative Leitfragen eines Regelungsgegenstandes regelt (Art. 290 Abs. 1 UAbs. 2 S. 2 AEUV). Ähnlich wie Art. 80 Abs. 1 GG verfolgt der Vorbehalt das Ziel, die Rechtsetzung gegen potenziell ausufernde Delegationen der Gesetzgebungs- und somit Gestaltungsmacht auf die Exekutive abzusichern. Im Gegensatz zum Wesentlichkeitsvorbehalt des deutschen Verfassungsrechts stellt der Begriff der Wesentlichkeit für den EuGH jedoch nicht auf die Grundrechtsausübung[208], sondern den maßgeblichen Einfluss auf den jeweiligen Politikbereich („Aspekte eines Bereichs“) ab.[209]

Die *Kommission* ist nicht befugt, einzelne Befugnisse, die das Unionsrecht ihr übertragen hat, auf weitere Institutionen zu verlagern.[210] Der *unionale Gesetzgeber* delegiert Befugnisse teilweise aber selbst an weitere, sekundärrechtlich eingerichtete Institutionen, deren Aufgabe es ist, Fachexpertise zu bündeln.[211] Er lagert damit Entscheidungen auf spezialisierte Gremien aus, die sodann auf die Entscheidungsfindung der Kommission maßgeblich inhaltlichen Einfluss nehmen oder sogar selbst

[207] Siehe Art. 290 Abs. 1 UAbs. 2 S. 1 AEUV.
[208] Dazu oben Fn. 199 sowie BVerfG, NJW 1998, S. 2515 (2520): „wesentlich für die Verwirklichung der Grundrechte“.
[209] „Wesentlich sind […] Bestimmungen, durch die die grundsätzlichen Ausrichtungen der Gemeinschaftspolitik umgesetzt werden.“ EuGH, Rs. C–240/90, *Deutschland/Kommission*, Slg. 1992, I–5383, ECLI:EU:C:1992:408, Rn. 37.
[210] Vgl. *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Hrsg.), EUV/AEUV, 65. Erg.-Lfg. (Stand: Aug. 2018), Art. 290 AEUV, Rn. 30.
[211] *Weiß*, EuR 2016, 631 (631).

rechtsetzend tätig sind. Im europäischen Verwaltungsverbund stehen dafür exemplarisch *Agenturen* (wie die Europäische Umweltagentur[212], das Europäische Markenamt[213], die Europäische Verteidigungsagentur[214]) oder die drei Europäischen *Finanzaufsichtsbehörden* (die Bankaufsichtsbehörde [EBA][215], die Wertpapier- und Marktaufsichtsbehörde [ESMA][216] und die Versicherungsaufsichtsbehörde [EIOPA]).[217] Der EuGH hat die abstrakte Möglichkeit, einzelne Aufgaben an Agenturen zu übertragen, für zulässig befunden.[218] Gerade im Bereich der Wertpapieraufsicht hat sich die Delegation quasi-legislativer Befugnisse in den letzten Jahren stetig weiter entwickelt: Art. 28 VO (EU) Nr. 236/2012[219] räumt der ESMA einen Ermessensspielraum ein, sog. Leerverkäufe zu regeln. Die Letztentscheidung (bspw. über ein Verbot von Leerverkäufen) liegt deshalb nicht mehr bei der Kommission, sondern bei der Agentur selbst.[220]

b) Leitlinien

Neben delegierten Rechtsakten kennt das Unionsrecht auch *nicht-rechtsförmliche Handlungsinstrumente*, insbesondere Leitlinien. Ihre Aufgabe ist es, eine programmierende Konkretisierungsleistung des materiellen Gesetzesvollzugs vorzunehmen. Im nationalen Recht sind sie am ehesten mit Verwaltungsvorschriften vergleichbar: Sie erweitern die administrative Normkonkretisierung sowie ko-

[212] Konstituiert durch Verordnung (EWG) Nr. 1210/90 des Rates vom 7. Mai 1990 zur Errichtung einer Europäischen Umweltagentur und eines Europäischen Umweltinformations- und Umweltbeobachtungsnetzes, ABl. L 120/01 v. 11.5.1990. Die Grundlagen der Umweltpolitik sind nun in den Art. 191 ff. AEUV niedergelegt.

[213] Ursprünglich eingerichtet durch Verordnung (EG) Nr. 40/94 des Rates vom 20. Dezember 1993 über die Gemeinschaftsmarke, ABl. L 11/1 v. 14.1.1994.

[214] Vgl. Art. 42 Abs. 3 UAbs. 2 EUV.

[215] Konstituiert durch Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission, ABl. L 331/12 v. 15.10.2010.

[216] Konstituiert durch Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission, ABl. L 331/84 v. 15.12.2010.

[217] Eingerichtet durch Verordnung (EU) Nr. 1094/2010 2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr.716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission, ABl. L 331/48 v. 15.12.2010.

[218] Vgl. EuGH, Rs. C-270/12, *Vereinigtes Königreich/Parlament und Rat*, ECLI:EU:C2014:18, Rn. 79.

[219] Verordnung (EU) Nr. 236/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 über Leerverkäufe und bestimmte Aspekte von Credit Default Swaps.

[220] Der EuGH befand, dass die Befugnisse, die der ESMA zustehen, ausreichend umgrenzt seien, um zu verhindern, dass sich Entscheidungen der Wirtschaftspolitik zu weit von der Exekutive auf Einrichtungen mit entfernt abgeleiteter demokratischer Legitimation verlagern; EuGH, Rs. C-270/12, *Vereinigtes Königreich/Parlament und Rat*, ECLI:EU:C2014:18, Rn. 41 ff., insbes. Rn. 48 und 53.

operative Vollzugsprogrammierung und geben den exekutivischen Akteuren konkrete Handlungsanweisungen an die Hand. So nutzt die EU-Kommission Leitlinien bspw., um Einschätzungen darüber abzugeben, ob im Beihilfenrecht staatliche Begünstigungen rechtmäßig sind.[221] Im Rahmen der gemeinsamen Strukturfondsverwaltung steuern Leitlinien die Grundsätze und Prioritäten, um eine gleichwertige räumliche Entwicklung innerhalb der EU zu fördern (sog. Kohäsionspolitik). Auch im Kartell- und Telekommunikationsrecht sowie im Rahmen der Energieregulierung erfüllen Leitlinien eine wichtige Konkretisierungsfunktion, indem sie normative Zielvorstellungen des Unionsrechts operationalisieren. So fungieren Leitlinien im Telekommunikationsrecht als Instrument, um die komplexe Aufgabe der Marktanalyse und Bewertung zu bewältigen, ob ein Akteur über eine beträchtliche Marktmacht verfügt.[222]

Gerade im Datenschutzrecht bringt die Union die programmierende Wirkung, die Leitlinien entfalten können, in jüngerer Zeit besonders zur Geltung: Leitlinien sind eines der zentralen Handlungsinstrumente des Europäischen Datenschutzausschusses (EDSA).[223] Um die einheitliche Auslegung unbestimmter Rechtsbegriffe der DSGVO zu gewährleisten,[224] fällt ihm die Aufgabe zu, mithilfe von Leitlinien die Löschung von Links auf der Grundlage des Art. 17 Abs. 2 DSGVO, die Regelungen des Art. 22 Abs. 2 DSGVO für das Profiling oder die Übermittlung personenbezogener Daten an Drittstaaten für den Verwaltungsvollzug binnenwirksam zu operationalisieren.[225]

Dem Instrument der Leitlinie kann de lege ferenda auch eine wichtige Konkretisierungsfunktion zukommen, um die zahlreichen unbestimmten Rechtsbegriffe der Risikosteuerung algorithmenbasierter Verfahren näher zu bestimmen und auf dieser Grundlage im Zusammenspiel mit delegierten Rechtsakten ein geeignetes Risikoschwellenkonzept für die DSGVO zu entwerfen.

[221] Siehe dazu exemplarisch aus der Rechtsprechung des EuGH: EuGH, Rs. C-526/14, *Kotnik ua*, ECLI:EU:C:2016:570, Rn. 69 sowie EuGH, Rs. C-189/02 P, *Dansk Rörindustrie*, Slg. 2005, I-5425, Rn. 209 ff.

[222] Art. 15 Abs. 2 der Telekommunikations-Rahmen-RL, Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, ABl. EG 2002, L 108, S. 33 ff. geändert durch Art. 1 ÄndRL 2009/140/EG v. 25. 11. 2009 (ABl. EG L 337, S. 37), § 11 Abs. 3 S. 1 TKG; siehe auch *Britz*, EuR 2006, 46 (46 ff.).

[223] Vgl. Art. 70 Abs. 1 S. 2 lit. d–j, k und m DSGVO. Daneben hat er insbesondere auch die Kompetenz, rechtsförmlich durch Beschluss zu handeln – jedoch nur einzelfallbezogen, Art. 65 Abs. 1 DSGVO.

[224] Siehe Art. 70 Abs. 1 S. 1 DSGVO.

[225] Siehe Art. 70 Abs. 1 S. 2 lit. d, f, j DSGVO.

III. Zwischenergebnis: Grundgerüst eines normativen Risikoschwellensystems für algorithmenbasierte Entscheidungsprozesse

Im Epizentrum der Bemühungen, sachgerechte Regulierungsschwellen zu konkretisieren, steht die Frage, in welchem Ausmaß eine Softwareanwendung die Grundrechte der Betroffenen zu beeinträchtigen droht und daher Regulierungsbedarf auslöst. Ausgehend von einer Bewertung, ob und wie stark das System Grundrechte berührt, sollte ein Regulierungssystem Sensibilitätsstufen identifizieren, anhand derer Verantwortliche und ggf. auch Aufsichtsbehörden eine konkrete bzw. typisierte Anwendung verschiedenen Regulierungsniveaus zuordnen können.

Je eher und stärker Leib und Leben betroffen sein können (etwa bei der Steuerungssoftware eines pilotierten Fahrzeugs oder eines Pflegeroboters), desto eher ist grundsätzlich ein tieferer Eingriff in die Berufs- und Eigentumsfreiheit eines Softwareanbieters gerechtfertigt – etwa via Marktzulassungskontrolle staatlicher Behörden.[226] Umgekehrt gilt: Je stärker eine Regulierungsmaßnahme die Freiheiten der Anbieter und Betreiber beschneidet, umso größer ist der Legitimationsbedarf und umso größer muss der Schutzgehalt sein, den die Maßnahmen erzielen.

Ein wichtiger Schritt ausgewogener Regulierung besteht darin, eine Unterschwelle solcher Softwareanwendungen zu definieren, die keiner zusätzlichen Kontrolle bedürfen,[227] weil sie sich unterhalb einer kritischen Schwelle der Grundrechtsrelevanz bewegen. Für alle algorithmenbasierten Verfahren, die dem Negativkatalog nicht unterfallen, griffe dann ein abgestuftes Regulierungssystem:

Auf einer *ersten Stufe* ermittelt eine staatliche Stelle das prognostizierte Risiko für typisierte Grundanwendungen (etwa *Data Mining* oder *Scoring*).[228] Dem Instrument der Folgenabschätzung, welches die DSGVO bereits kennt, kann dabei eine wichtige Stellschraubenfunktion zukommen: Es ist dazu prädestiniert, ein verfahrensrechtliches Sensorium bereitzustellen, um den Risikograd einer Anwendung in Risikoklassen einzuordnen. In diese Richtung könnte und sollte der unionale Gesetzgeber das Instrument weiterentwickeln und daran ein abgestuftes Pflichtenregime unterschiedlicher Tiefe knüpfen. Bei bestehender, aber nur geringfügiger Grundrechtsrelevanz kann bspw. die

[226] Als Blaupause könnte insoweit im Grundsatz das Arzneimittelrecht wirken, vgl. etwa § 21 AMG.
[227] So bedürfen etwa im Arzneimittelrecht homöopathische und traditionelle pflanzliche Arzneimittel keiner Marktzulassung; ihre Hersteller müssen sie lediglich staatlich registrieren, vgl. §§ 38, 39a AMG.
[228] Zu unterscheiden wäre etwa zwischen einer „hohen“, einer „erheblichen“ und einer „geringen“ Sensibilität.

Pflicht entfallen, zu einem bestimmten Produkt bzw. Entscheidungssystem eine umfassende Folgenabschätzung zu veröffentlichen und so für die Öffentlichkeit kontrollierbar zu machen. Entbehrlich könnten dann etwa auch Protokollierungspflichten oder eine Schnittstelle für den behördlichen Zugriff sein.

An die grobe Risikoklassenzuordnung kann sich – auf einer *zweiten Stufe* – eine Feinjustierung anschließen: Mit Hilfe organisatorischer, technischer und rechtlicher Maßnahmen kann der Verantwortliche die Grundrechtssensibilität der Softwareanwendung verringern. Soweit die flankierenden Risikominderungsschritte die Grundrechtsrelevanz erheblich senken, könnte eine Anwendung dann eine Privilegierung genießen. Das sollte insbesondere dort der Fall sein, wo der Betreiber selbst adäquate Schutzmaßnahmen trifft, um Risiken zu minimieren.[229]

Als Instrumente, die eine „hohe" auf eine „normale" Grundrechtssensibilität absenken, können insbesondere zum Einsatz kommen:

- die tatsächliche und überprüfbare Anonymisierung oder jedenfalls Pseudonymisierung[230] weiter Teile der Datenverarbeitung,
- synthetische anstatt personenbezogene Daten,[231]
- eine sog. starke Verschlüsselung für bestimmte Datenpakete sowie
- der vollständige oder teilweise Verzicht auf Daten im Sinne des Art. 9 Abs. 1 sowie Art. 10 DSGVO bzw. Maßnahmen einer differential privacy.[232]

Auch freiwillige Transparenzmaßnahmen können die Grundrechtssensibilität reduzieren. Denkbar sind neben der Veröffentlichung (anonymisierter) Vergleichsgruppen etwa auch regelmäßige überobligatorische Überprüfungen der Datengrundlage, die für den algorithmischen Entscheidungsprozess relevant ist (insbesondere im Hinblick auf etwaige Diskriminierungen). Die Prüfergebnisse könnten ihrerseits einer Veröffentlichungspflicht unterliegen.

---

[229] Um bewährte Methoden einer *privacy by design* (Art. 25 Abs. 2 DSGVO) zu klassifizieren und für die Bewertung einer Vielzahl von Softwareanwendungen fruchtbar zu machen, könnte der Normgeber auf Instrumente delegierter Rechtsmacht zurückgreifen oder statische Verweise auf private Normen vorsehen.

[230] Vgl. Art. 25 Abs. 1 DSGVO, der die Pseudonymisierung beispielhaft als technisch-organisatorische Maßnahme hervorhebt, um Datenschutzgrundsätze umzusetzen. Vgl. *Hartung*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 25 DSGVO, Rn. 16.

[231] Vgl. hierzu bspw. *Drechsler/Jentzsch*, Synthetische Daten, 2018, S. 5 ff.

[232] *Martini*, Blackbox Algorithmus, 2019, S. 243.

Die Darlegungslast dafür, dass eine Privilegierung greift, sollte – entsprechend dem Grundgedanken der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO – grundsätzlich beim Anbieter bzw. Betreiber liegen und aufsichtsbehördlich überprüfbar sein. So entsteht ein Anreiz, Softwarelösungen – im Einklang mit Art. 25 Abs. 2 DSGVO – von Beginn an (jedenfalls auch) dem Persönlichkeitsschutz zu verschreiben. Prämiert würden sie dafür mit einer abgeschwächten Kontrollintensität.[233] Die Aufsichtsbehörde erteilt dafür einen feststellenden Dispens, damit die Herabstufung in eine geringere Sensibilitätsstufe wirksam wird.

An die Einordnung in die verschiedenen Sensibilitätsstufen knüpfen sich dann unterschiedliche Pflichtenniveaus: Bei einer „hohen Grundrechtssensibilität“ kann der Gesetzgeber es bspw. zur Pflicht erheben, ein Zertifizierungsverfahren oder ein externes Audit durchlaufen zu müssen, einer Aufsichtsbehörde bzw. der technischen Serviceeinheit[234] per Schnittstelle einen fortwährenden kontrollierenden Zugriff auf die Softwareumgebung zu gewähren sowie eine Begründungspflicht zu implementieren.

[233] Um Umgehungsstrategien einen Riegel vorzuschieben, muss es aber zugleich spürbare Sanktionen für Unternehmen geben, die das Risikoniveau vorsätzlich oder grob fahrlässig zu niedrig einstufen. Wie Art. 24 Abs. 3 und Art. 40 f. DSGVO paradigmatisch deutlich machen, ist es dem Datenschutzrecht nicht fremd, dass Verantwortliche adäquate Selbsteinschätzungen vornehmen und dafür „belohnt“ werden; Art. 24 DSGVO ist allerdings eine Generalnorm, deren konkreten Pflichtenkanon der Unionsgesetzgeber bislang nicht klar spezifiziert hat, vgl. *Hartung*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 24 DSGVO, Rn. 24.

[234] Vgl. oben S. 32 f.

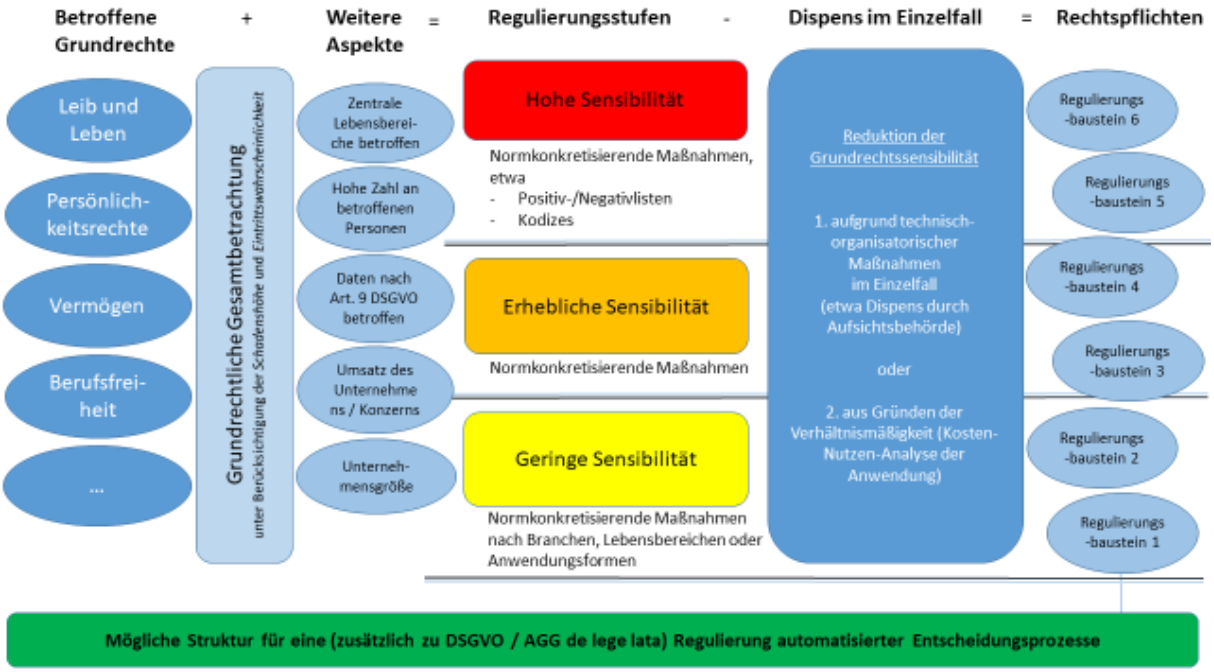

Abbildung 1: Stark vereinfachtes Grundgerüst eines Regulierungskonzeptes für algorithmenbasierte Entscheidungsprozesse

Quelle: Michael Kolain

D. Regelungskompetenz: Umsetzung der Regulierungsvorschläge im Mehrebenensystem – Zusammenfassung

Der Unionsgesetzgeber hat in der DSGVO wichtige Pflöcke für eine Regulierung algorithmenbasierter Anwendungen eingeschlagen. Ihr Rohbau bedarf jedoch einer Auskleidung. Insbesondere für die algorithmische *Assistierung* menschlicher Entscheidungen („Teilautomatisierung“) weist die Architektur der DSGVO noch eine empfindliche Schutzlücke auf.

Der deutsche Gesetzgeber kann diese nicht ohne Weiteres in Eigenregie füllen. Denn die DSGVO entfaltet in ihrem Anwendungsbereich – der Verarbeitung und dem freien Verkehr personenbezogener Daten (Art. 1 Abs. 1 DSGVO) – grundsätzlich eine Sperrwirkung gegenüber nationalen Regelungen: Sie reklamiert für sich den Anspruch, das Datenschutzrecht grundsätzlich unionsweit vollständig zu harmonisieren. Die Mitgliedstaaten dürfen eigene, ergänzende Regelungen deshalb lediglich insoweit treffen, als ihnen die DSGVO das hinreichend klar in (ihren zahlreichen) Öffnungsklauseln gestattet (vgl. insbesondere ErwGrd 8 DSGVO).[235]

[235] *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 3 ff.

Auch die Regelungsfelder des Anti-Diskriminierungsrechts[236] sowie Teile des Wettbewerbs- und Lauterkeitsrechts[237] sind bereits nachhaltig unionsrechtlich überformt. Dem nationalen Gesetzgeber sind daher bei vielen denkbaren Reformbemühungen zu einem guten Teil Fesseln angelegt.[238]

Die Regulierung algorithmenbasierter Verfahren auf der Ebene des Unionsrechts anzusiedeln, folgt auch rechtspolitisch einem sachgerechten Konzept: In einem globalisierten digitalen Kosmos büßen nationale Grenzen ihre Bedeutung zusehends ein; allein unionsweite Regelungen sind in der Lage, durchsetzungsfähige Standards zu setzen. Zwar ist das deutsche Regelungsniveau des Datenschutzes sowohl im weltweiten wie auch im europäischen Vergleich traditionell bereits hoch angesiedelt und feinsinnig elaboriert. Was auf den ersten Blick als Ausdruck einer deutschen Technikskepsis daherkommt, ist nicht zuletzt das Produkt der historischen Erfahrung zweier totalitärer Regime. Sie spiegelt sich bis heute in einer besonderen Sensibilität vieler Deutscher in Fragen der informationellen Selbstbestimmung.

So sehr es in diesem Lichte nachvollziehbar ist, mit gutem Beispiel Maßstäbe zu setzen, statt auf eine EU-weite Einigung zu warten: Mit neuen nationalstaatlichen Regelungen stieße Deutschland im Zweifel ein *forum shopping*[239] innerhalb Europas an. Mitgliedstaatliche Regulierungsalleingänge für algorithmische Entscheidungssysteme münden (soweit überhaupt unionsrechtlich zulässig) nicht selten darin, dass sich die Unternehmen der Digitalwirtschaft vorzugsweise in Staaten mit einer größeren „digitalen Freiheit“ und einem niedrigeren Datenschutzniveau niederlassen. Dadurch schmälern sich im Ergebnis zugleich die Chancen der Verbraucher, hohe Schutzstandards wirksam durchsetzen zu können.

[236] Vgl. insbesondere die RL 2000/43/EG, 2000/78/EG, 2004/113/EG und 2006/54/EG.
[237] Vgl. zum Wettbewerbsrecht vor allem die Art. 101 ff. AEUV sowie die aufgrund Art. 103 Abs. 1 AEUV erlassenen Rechtsakte; vgl. zum Lauterkeitsrecht etwa die RL 2005/29/EG, der der EuGH vollharmonisieren Charakter zugeschrieben hat, EuGH (Plus Warenhandelsgesellschaft), Urt. v. 14.1.2010, ECLI:EU:C:2010:12, Rn. 41.
[238] Vgl. für das Datenschutzrecht *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 4 ff.
[239] *Forum shopping* meint die Unternehmensstrategie, das Nebeneinander bestehender Gerichtszuständigkeiten strategisch auszunutzen, um rechtliche oder tatsächliche Vorteile zu erzielen, vgl. etwa *Schack*, Internationales Zivilverfahrensrecht, 7. Aufl., 2017, S. 97.

I. Transparenzpflichten

1 Kennzeichnungspflichten („Ob“) und inhaltsbezogene Informationspflichten („Wie“)

Als ein Regulierungsbaustein einer europäischen Normarchitektur für algorithmenbasierte Entscheidungsprozesse können Transparenzanforderungen sowie gesetzliche Inhaltskontrollmechanismen der Informationsasymmetrie entgegenwirken, die den Einsatz von Algorithmen prägt:[240] Wer Dienstleistungen, Kommunikationsmittel und Plattformen nutzt, die ihre ökonomische Triebkraft komplexen Algorithmen verdanken, kann regelmäßig nicht vollständig überblicken, geschweige denn überprüfen, ob seine Daten in einer Weise einfließen, die mit seinem Selbstbestimmungsrecht in Einklang steht. Dem typischen Verbraucher verschließt sich bspw., ob ein Unternehmen einzelne Daten zu einem Persönlichkeitsprofil verquickt, sie in Simulationen Künstlicher Intelligenz einspeist oder sie – entgegen den datenschutzrechtlichen Vorgaben – unbefugt an Dritte weitergibt.

Welcher Ebene es zusteht, die Transparenzpflichten – also etwa eine Kennzeichnungs- und eine inhaltsbezogene Informationspflicht sowie eine Ex-post-Begründungspflicht[241] – für rechtsrelevante algorithmenbasierte Verfahren (über ihre enge Begrenzung auf Art. 22 DSGVO hinaus) zu erweitern,[242] bestimmt sich zuvorderst nach den unionsrechtlichen Vorgaben der Art. 12 ff. DSGVO i. V. m Art. 1 Abs. 2 S. 2, Art. 16 Abs. 2 AEUV, Art. 4 Abs. 3 S. 3 EUV. Die Vorschriften des Art. 13 Abs. 2 lit. f bzw. Art. 14 Abs. 2 lit. g DSGVO, Art. 15 Abs. 1 lit. h, Art. 22 DSGVO ziehen für den Teilbereich vollständig automatisierter Entscheidungen einen grundsätzlich abschließenden normativen Schutzrahmen.

Sollen diese Informationspflichten fortan im Grundsatz nicht nur für vollautomatisierte Verfahren, sondern auch für sonstige grundrechtssensible algorithmenbasierte Verfahren gelten, steht der Normgeber vor der Herausforderung, den erweiterten Adressatenkreis der (bußgeldbewehrten) Informationspflichten exakt zu benennen, um einerseits die Bürokratiekosten nicht zu überdehnen, die sich mit Informationspflichten verbinden, und andererseits keine Rechtsunsicherheit zu erzeugen. Denkbar ist insoweit insbesondere eine „Ampel-Rasterung“, um die ausgeweiteten Informationspflichten nach dem Sensibilitätsgrad der Anwendungen abzustufen. Positiv- und Negativlisten,

[240] Dazu oben S. 8 ff.
[241] Der Normgeber könnte dieses als „Recht auf Erläuterung der Entscheidung und Erklärung des Entscheidungsprozesses“ ausgestalten und seinen Umfang insbesondere an § 39 VwVfG orientieren. Verbraucher könnten dann nicht nur – wie in der derzeitigen Fassung der Art. 13–15 DSGVO – Tragweite und Logik des algorithmischen Vorgehens nachvollziehen, sondern die Entscheidung selbst auch besser verstehen und ggf. wirksamer Rechtsschutz suchen.
[242] Dazu oben S. 10 f.

die konkretisieren, welche Anwendungen den Informationspflichten unterliegen und welche von ihnen befreit sind, könnte der Unionsgesetzgeber in einer Anlage zu den Art. 12 ff. formulieren.

Will der *nationale Gesetzgeber* von dem Datenschutzniveau der Art. 12 ff. DSGVO für betroffene Verbraucher abweichen, eröffnet ihm Art. 23 DSGVO dazu zwar einen Spielraum.[243] Die mitgliedstaatliche Regelungsbefugnis ist jedoch nicht nur an hohe Voraussetzungen geknüpft. Sie erschöpft sich auch darin, den Pflichtenrahmen *nach unten* aufzuweichen. Neue Pflichten zu begründen, die über den Kanon der Art. 12 ff. DSGVO *hinausgehen*, steht dem Mitgliedstaat ausweislich des Wortlauts des Art. 23 Abs. 1 DSGVO („beschränkt werden“) nicht zu. Eine ergänzende Regulierung in der Sachmaterie des Datenschutzrechts, welche bestehende Informationspflichten erweitert, müsste also wiederum auf EU-Ebene erfolgen.[244]

2. Pflicht zur Veröffentlichung einer *umfassenden* Folgenabschätzung

Ebenso wie Informationspflichten kann der nationale Gesetzgeber auch die gesetzliche Vorgabe, eine *umfassende* Folgenabschätzung durchzuführen, die sich nicht nur auf die persönlichkeitsrechtlichen Auswirkungen einer Verarbeitung kapriziert, und sie zu veröffentlichen,[245] nicht ohne Weiteres im Alleingang etablieren. Den Mitgliedstaaten sind insoweit kompetenziell die Hände gebunden; Art. 35 DSGVO kommt eine Sperrwirkung zu.

Dem nationalen Gesetzgeber verbleibt jedoch die Möglichkeit, sektorale Folgenabschätzungen für *andere* als datenschutzrechtliche Folgewirkungen sensibler Softwareanwendungen verpflichtend vorzusehen. Um den Umfang und Inhalt der Folgenabschätzung auf eine *allgemeine Technikfolgenabschätzung* auszudehnen, kann sich der Unionsgesetzgeber insbesondere nicht ohne Weiteres auf die Kompetenz stützen, eine sekundärrechtliche Verordnung zu erlassen. Denn damit verließe er den originären Anwendungsbereich des Datenschutzrechts. Art. 16 AEUV reicht dafür jedenfalls bei engem Verständnis als Kompetenzgrundlage nicht hin. Eine allgemeine Technikfolgenabschätzung als Erweiterung der Datenschutz-Folgenabschätzung lässt sich aber auf das Finalprogramm der

[243] Eine absenkende Abweichung muss insbesondere ein übergeordnetes Schutzziel – etwa die öffentliche Sicherheit – sicherstellen (Art. 23 Abs. 1 DSGVO), den Wesensgehalt der Grundrechte achten und insgesamt verhältnismäßig sein. Der Katalog des Art. 23 Abs. 1 DSGVO ist abschließend. Vgl. dazu auch *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., 2018, Art. 23 DSGVO, Rn. 11 ff.

[244] Ähnliches gilt für den Vorschlag, Newsaggregatoren-Diensten eine Verpflichtung aufzuerlegen, Einblick in ihr technisches Verfahren der Nachrichtenauswahl und -priorisierung zu gewähren. Dazu *Martini*, JZ 2017, 1017 (1021).

[245] Dazu oben S. 17 f.

Art. 114 S. 2 und 115 AEUV, namentlich die Regelungskompetenz für die Rechtsangleichung im Binnenmarkt, gründen. Ein Nebeneinander einer unionalen Datenschutz-Folgenabschätzung und einer ergänzenden nationalen Folgenabschätzung für die nicht datenschutzspezifischen Folgen wäre auch – nicht zuletzt mit Blick auf den Aufwand, den es verursacht – steuerungspolitisch verfehlt. Denn im Kernfokus einer Folgenabschätzung für algorithmenbasierte Entscheidungsprozesse steht im Regelfall die Frage, wie es mit personenbezogenen Daten umgeht.

Eine Pflicht, die Datenschutz-Folgenabschätzung zu *veröffentlichen*, könnte der Unionsgesetzgeber im Wege eines neuen Art. 35 Abs. 1 S. 2a DSGVO verwirklichen („*Verantwortliche, die sensible Softwareanwendungen betreiben, sind verpflichtet, die wesentlichen Inhalte und Ergebnisse der Folgenabschätzung auf ihrer Homepage zu veröffentlichen und bei jeder neuen Folgenabschätzung zu aktualisieren*“). Prima facie ist es erwägenswert, die Verpflichtung auf diejenigen Fälle zu begrenzen, in denen auch eine Konsultation der Aufsichtsbehörden geboten ist (Art. 36 Abs. 1 DSGVO), um insbesondere kleineren und mittleren Unternehmen keinen geschäftsschädigenden Bürokratieaufwand abzuverlangen. Allerdings soll eine Veröffentlichung Betroffenen gerade auch dann ein Bild über Risiken eines Dienstes vermitteln, wenn dieser noch nicht marktführend ist.

II. Inhaltskontrolle

1. Instrumente

Auch (neue) Aspekte einer Inhaltskontrolle algorithmenbasierter Anwendungen[246] können die Mitgliedstaaten nicht mehr ohne Weiteres selbst in Gesetze gießen: Die Regelungskompetenz liegt insoweit unterdessen überwiegend in Brüssel. Nur der Unionsgesetzgeber kann etwa dem Vorschlag, die Betreiber bestimmter algorithmenbasierter Entscheidungsverfahren zu verpflichten, ein Risikomanagementsystem in ihre Datenverarbeitungsprozesse zu integrieren, durch einen entsprechenden Passus (z. B. in Art. 25 Abs. 1 DSGVO) Geltung verschaffen. Denn bei einem Risikomanagement handelt es sich um ein Instrument einer originären datenschutzrechtlichen Compliance, das den Prozess der Datenverarbeitung (für den die DSGVO einen unionsrechtlichen Anwendungsvorrang reklamiert) unmittelbar steuert.

Die Union ist insbesondere gut beraten, den Gedanken des ErwGrd 71 UAbs. 2 DSGVO für algorithmenbasierte Verfahren (insbesondere Profiling) in ihren verfügenden Teil (vorzugsweise in Art. 25

[246] Dazu oben S. 18 ff.

Abs. 1 DSGVO oder einen neuen Art. 22a DSGVO) aufzunehmen – und zwar nicht nur, soweit sie Teil vollautomatisierter Verfahren im Sinne des Art. 22 DSGVO sind. Dann sind Verantwortliche unmittelbar und sanktionsbewehrt dazu verpflichtet, „geeignete mathematische oder statistische Verfahren" zu etablieren, sowie ihre Methoden und Datengrundlage regelmäßig zu kontrollieren, um Fehler zu minimieren.

Immerhin verbleibt dem nationalen Gesetzgeber aber grundsätzlich die Regelungsmacht, *das AGG* auf die Bedürfnisse algorithmenbasierter Ungleichbehandlungen anzupassen. Auch das Antidiskriminierungsrecht ist zwar unionsrechtlich überformt. Allerdings nehmen die einschlägigen unionsrechtlichen Richtlinien keine Vollharmonisierung vor. Den Mitgliedstaaten verbleiben daher eigene Gestaltungsspielräume. Auch die DSGVO schlägt durchaus einzelne diskriminierungsrechtliche Grenzpflöcke ein (Art. 22 Abs. 2, 3 und 4 sowie Art. 9 Abs. 1 DSGVO). Die Kompetenzermächtigung für das unionale Datenschutzrecht (Art. 16 Abs. 2 AEUV) endet jedoch grundsätzlich dort, wo nicht der *Vorgang* der Datenverarbeitung, sondern dessen *Ergebnis* (also der Inhalt einer algorithmenbasierten Entscheidung) Gegenstand der Regulierung ist.

Auch in den übrigen Bereichen eines Kontrollsystems für algorithmenbasierte Verfahren verbleibt dem nationalen Gesetzgeber nur ein sehr schmaler Gestaltungsspielraum: Die *verfahrensrechtlichen Pflichten der Verantwortlichen* (Mitwirkungs-, sowie Auskunfts- und Protokollierungspflichten und die Pflicht, ein Risikomanagementsystem zu betreiben)[247] konkretisiert die DSGVO grundsätzlich abschließend selbst (Art. 30, 31 DSGVO). Die *Rechenschaftspflicht* des Art. 5 Abs. 2 DSGVO spezifiziert die Union (positiv wie negativ) aus eigener Regelungsmacht (vgl. auch Art. 28 Abs. 3 S. 2 lit. a, Art. 30 Abs. 1 und 2, 33 Abs. 5 S. 1, Art. 49 Abs. 6 DSGVO).

Dem nationalen Gesetzgeber ist es insbesondere verwehrt, ein generelles präventives Kontrollverfahren für datenverarbeitende Systeme zu etablieren. Eine Zulassungspflicht unterspült den unionsrechtlichen Anspruch, die Anforderungen an den Umgang mit personenbezogenen Daten unionsweit zu harmonisieren. In Art. 6 DSGVO hat die Union diesen Anspruch (mit Ausnahme des öffentlichen Sektors – Art. 6 Abs. 1 UAbs. 1 lit. e sowie lit. c – inhaltlich abschließend ausgefüllt.

Die Mitgliedstaaten können eigene Gesetze aber grundsätzlich in Bereichen erlassen, in denen sie *keine spezifisch datenschutzrechtlichen Pflichten* begründen, sondern seine Schutzpflicht für andere Rechtsgüter insbesondere die Gesundheit, die Meinungsfreiheit und die demokratische Ordnung

[247] Dazu oben S. 25 f. und S. 27 ff.

oder die Ausgestaltung arbeitsrechtlicher Beziehungen wahrnimmt (vgl. auch insbesondere Art. 85 Abs. 2, Art. 88 Abs. 1 DSGVO). Die Mitgliedstaaten dürfen daher insbesondere *Zulassungskontrollen für gesundheitsmedizinische Softwareanwendungen* aus eigenem Recht begründen, um das Recht auf Leben und Gesundheit Betroffener zu schützen. Ähnliches gilt bspw. für *Produktzulassungspflichten* für Pflegeroboter oder hochautomatisiertes Fahren (etwa im Rahmen der StVO).

2. Regulierungsschwellen

An welcher Schwelle ein staatliches Regulierungs- und Kontrollsystem für algorithmenbasierte Verfahren ansetzen soll, gehört zu den heikelsten Steuerungsaufgaben einer Algorithmengesetzgebung. Die regulatorischen Anstrengungen, um algorithmenbasierte Risiken sachgerecht zu domestizieren, müssen nicht nur eine hohe Detailschärfe, sondern auch ein ausgewogenes Pflichtenheft entwickeln, um Rechtssicherheit und Verhältnismäßigkeit gleichermaßen zu wahren. Alleine an Einzelaspekte – etwa die Anzahl der potenziell Betroffenen oder die Eintrittswahrscheinlichkeit eines Schadens – anzuknüpfen, wird der Vielfalt algorithmenbasierter Verfahren nicht gerecht. Es bedarf insoweit bereichsspezifischer Lösungen und einer (auch qualitativen) Gesamtbetrachtung, die Raum für Ausnahmen und Befreiungen lässt.[248]

Ein staatliches Regulierungs- und Kontrollsystem sollte jedenfalls an die Grundrechtssensibilität und Marktrelevanz des algorithmischen Entscheidungsprozesses anknüpfen. Auf einer *ersten Stufe* könnte das prognostizierte Risiko der Grundanwendung (etwa Scoring in zentralen Lebensbereichen) als Teil einer umfassenden Folgenabschätzung stehen (hohe, erhebliche oder geringfügige Grundrechtsrelevanz). Anschließend könnten – in einer *zweiten Stufe* – technische oder organisatorische sowie rechtliche Maßnahmen Berücksichtigung finden, um der Grundrechtssensibilität im Einzelfall Rechnung zu tragen.[249] Von dieser Kategorisierung ausgehend, könnte die Rechtsordnung dann anordnen, welche einzelnen Kontrollinstrumente eingreifen bzw. entfallen.

3. Institutionelle Ausgestaltung des Kontrollsystems

Die Regulierung algorithmenbasierter Verfahren muss darauf angelegt sein, die Anforderungen an Transparenz und Diskriminierungsfreiheit der Systeme nicht nur zu fördern, sondern auch konsequent durchzusetzen. Daran wird sich ihr Erfolg im Ergebnis bemessen. Für eine staatliche Aufsicht,

[248] Dazu oben S. 41 ff.
[249] Dazu oben S. 63 ff.

die kraft angemessener sachlicher Ausstattung und personelle Kompetenz in der Lage ist, in dem Hase-Igel-Wettlauf zwischen technischer Entwicklung und ihrer Kontrolle mitzuhalten, bedarf es maßgeschneiderter institutioneller und organisationsrechtlicher Rahmenbedingungen.

Dafür künftig eine separate Aufsichtsbehörde aus der Taufe zu heben, ist rechtspolitisch weder zielführend noch aussichtsreich.[250] Denn die Regulierung algorithmenbasierter Entscheidungsprozesse beschreibt eine komplexe Querschnittsmaterie, die ein einheitliches Aufsichtsdach nur schwer abzudecken vermag. Sie weist einerseits eine hohe Sachnähe zum Datenschutz-, anderseits aber auch enge Bezüge zum Antidiskriminierungs- und Wettbewerbsrecht auf. Vor diesem Hintergrund lässt sich eine neue Behörde nicht errichten, ohne zugleich die Aufgaben der bestehenden Fachbehörden zu beschneiden. Die fachbehördliche Ausgestaltung der Aufsichtsstruktur liegt zwar grundsätzlich in den Händen der Mitgliedstaaten. Die Union etabliert in den Art. 51 ff. DSGVO allerdings zahlreiche abweichungsfeindliche Vorgaben. Dazu gehört insbesondere die Pflicht, die datenschutzrechtlichen Aufsichtsbehörden als eigene Aufsichtsinstanz mit Unabhängigkeit beizubehalten und auszustatten (Art. 52 ff. DSGVO).

Möglich und sinnvoll ist es hingegen, dass der Bundesgesetzgeber eine staatliche *Unterstützungseinheit* errichtet. Sie könnte den verschiedenen, bereits existierenden Aufsichtsbehörden des Bundes und der Länder mit Sachverstand passgenau zuarbeiten.[251] Dadurch entstünde ein nationales Kompetenzzentrum, das seine wissenschaftlich fundierte Expertise gezielt in die facettenreichen Aufsichts- und Rechtsstrukturen einbringen kann. Seine Serviceleistung könnte etwa darin bestehen, öffentliche Standards zu erarbeiten oder interdisziplinäre Prüfteams vorzuhalten, zu schulen und methodisch anzuleiten. Ergänzend könnte der Gesetzgeber die neue Stelle institutionell auch um Elemente einer Markt- und Produktüberwachungseinheit anreichern.[252] Denkbar (aber nur bedingt bzw. nur in einzelnen Teilbereichen empfehlenswert) ist es nicht zuletzt, private Institutionen als Verwaltungshelfer oder Beliehene in die Aufsicht einzubeziehen.[253]

[250] Dazu oben S. 30 ff.
[251] Dazu oben S. 32 f. Das wäre bereits zum jetzigen Zeitpunkt, insbesondere ohne Anpassungen der DSGVO, möglich.
[252] Ähnliche Aufsichtsstrukturen existieren etwa für Arzneimittel, den Hochfrequenzhandel oder Kraftfahrzeuge.
[253] Siehe oben S. 33 f.

III. Haftung und Rechtsschutz

Eine Gefährdungshaftung in besonders sensiblen Bereichen (etwa bei digitalisierten medizinischen Anwendungen oder Pflegerobotern),[254] Abmahnbefugnisse für Wettbewerber,[255] Verbandsklagerechte[256] oder eine „Nebenfolgen-Kompetenz" für Zivilgerichte[257] regeln jeweils kein klassisches Datenschutzrecht: Sie knüpfen nicht unmittelbar an den „Schutz natürlicher Personen bei der *Verarbeitung* personenbezogener Daten" (vgl. Art. 1 Abs. 1 DSGVO) an. Die DSGVO erlegt dem nationalen Gesetzgeber insoweit grundsätzlich[258] keine kompetenzrechtlichen Beschränkungen für eigene legislatorische Bemühungen auf. Die Forderung, ein gesondertes Verbandsklagerecht der Verbraucherverbände und Schiedsstellen mitgliedstaatlich normativ zu verankern,[259] sieht die DSGVO in Art. 80 sogar ausdrücklich vor. Die Regulierungsvorschläge zu Haftung und Rechtsschutz[260] sind somit einer mitgliedstaatlichen Umsetzung im Grundsatz zugänglich.

IV. Selbstregulierung

Nationale Initiativen, welche die Instrumente der Selbstregulierung stärken (sollen), begrüßt das unionale Datenschutzrecht ausdrücklich (Art. 40 Abs. 1 DSGVO; siehe auch Art. 35 Abs. 8 sowie Art. 24 Abs. 3 DSGVO). Es gibt allerdings auch die Gestaltungsformen vor, in denen die Mitgliedstaaten solche Instrumente der Selbstregulierung entfalten dürfen. Das Selbstregulierungsmodell *„comply or explain"* kennt die DSGVO bislang nicht. Dem nationalen Gesetzgeber ist es daher verwehrt, jenseits der Selbstregulierungsformen der DSGVO einen (sanktionsbewehrten) „Algorithmic Responsibility Codex" nach dem Vorbild des Corporate Governance Kodex aus eigener Machtvollkommenheit einzuführen.[261] Auch rechtspolitisch sachgerechte Auditierungssysteme,[262] die Verantwortlichen Anreize setzen, das Schutzniveau ihrer Datenverarbeitungsprozesse kontinuierlich zu erhöhen, behält sich die Union in Art. 42 DSGVO selbst vor.

---

[254] Dazu oben S. 36 f.
[255] Dazu oben S. 37.
[256] Dazu oben S. 37 f.
[257] Dazu *Martini*, JZ 2017, 1017 (1024 f.).
[258] Der BGH erkennt insoweit erhebliche Rechtsunsicherheit. Er hat dem EuGH im Vorabentscheidungsverfahren die Frage vorgelegt, ob die Regelungen in Art. 22 bis 24 der Richtlinie 95/46/EG (Datenschutz-Richtlinie) einer nationalen Regelung entgegenstehen, die - wie § 8 Abs. 3 Nr. 3 UWG - gemeinnützigen Verbänden zur Wahrung der Interessen der Verbraucher die Befugnis einräumt, im Falle einer Verletzung von Datenschutzvorschriften gegen den Verletzer vorzugehen. BGH, Beschl. v. 11.4.2019 – I ZR 186/17.
[259] *Martini*, JZ 2017, 1017 (1024 f.).
[260] Im Einzelnen oben S. 35 ff. sowie bereits *Martini*, JZ 2017, 1017 (1023 f.).
[261] Dazu oben S. 39 ff.
[262] Dazu oben S. 38 f.

V. Regulierungsvorschläge nach Musterbeispielen (Übersicht)

Die Rasterungen eines Regulierungssystems lassen sich auf einzelne typische Anwendungsszenarien *stark vereinfachend* tabellarisch herunterbrechen; die jeweiligen Einstufungen sind dabei vorläufige Grundsatzwertungen, die je nach Ausgestaltung, Verbreitungsgrad und konkretem Einsatzszenario der Anwendung unterschiedlich ausfallen können. Die Tabelle skizziert eher eine methodische Herangehensweise als ein finalisiertes Gefahreneinstufungskonzept:

	Smart-home-Anwendungen (z.B. Haushaltsroboter)	Präferenzsoftware im Unterhaltungsbereich (z.B. *Facebook*-Startseite; Netflix-Vorschläge)	Individuelle Preissetzung	Bewertungsportale (z.B. Bewertungen von Ärzten, Dienstleistern, Lehrkräften)	Sprachbasierte Assistenzsysteme (z.B. Alexa)	Gesichtserkennungssoftware	Bewerberauswahl (Arbeits- u. Ausbildungsplätze)	Staatliche KI-Anwendungen	Medizinische Anwendungen (z. B. Bildauswertung zur Tumorerkennung)	Pflegeroboter	Autonome Fahrzeuge
Kennzeichnungspflicht	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Informationspflicht zur Logik des Systems	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Begründungspflicht	–	–	✓	–	–	–	✓	✓	✓	✓	–

Folgen-abschätzung	✓	–	–	–	✓	✓	✓	✓	✓	✓	✓
Ex-ante-Zulassungskontrolle (im Grundsatz)	–	–	–	–	–	✓	–	✓	✓	✓	✓
Erweiterung des Diskriminierungsschutzes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kontrollalgorithmen	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Behördliche Auskunfts– u. Einsichtsrechte, Mitwirkungspflichten	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Risikomanagement, insb. Benennung einer verantwortlichen Person	–	–	✓	✓	✓	✓	✓	✓	✓	✓	✓
Beweislasterleichterung	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Protokollierungspflicht (im Grundsatz)	–	u. U. ✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gefährdungshaftung	–	–	–	–	–	–	–	–	✓	✓	✓
Abmahnbefugnisse für Wettbewerber	✓	✓	✓	✓	✓	✓	✓	–	✓	✓	✓

Verbands-klagebefug-nis der Ver-braucher-schutzver-bände	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
grundsätzli-che Pflicht, sich zu ei-nem „Algo-rithmic Responsibili-ty Codex“ zu erklären	✓	✓	✓	✓	✓	✓	✓	u. U. ✓	✓	✓	✓

E. Literaturverzeichnis

ACM US Public Policy Council/ACM Europe Council, Statement on Algorithmic Transparency and Accountability, http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf (25.10.2018).

Anonymous, EU prüft Übernahme von WhatsApp, Focus Online vom 14.7.2014.

– LfDI Rheinland-Pfalz: Macht der Algorithmen – Macht ohne Kontrolle?, ZD-Aktuell, 2015, 04675.

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", WP 248, Brüssel, 4.10.2017.

Augsberg, Steffen, Rechtsetzung zwischen Staat und Gesellschaft, Möglichkeiten differenzierter Steuerung des Kapitalmarktes, Berlin, 2003.

Bauer, Jobst-Hubertus/*Krieger*, Steffen, 10 Jahre AGG – Tops und Flops, NZA 2016, S. 1041–1046.

Beck, Susanne, Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR 2009, S. 225–230.

Beck, Susanne (Hrsg.), Jenseits von Mensch und Maschine, Ethische und rechtliche Fragen zum Umgang mit Robotern, Künstlicher Intelligenz und Cyborgs, Baden-Baden, 2012.

Becker, Florian, Kooperative und konsensuale Strukturen in der Normsetzung, Tübingen, 2005.

Bernhardt, Wolfgang, Sechs Jahre Deutscher Corporate Governance Kodex - Eine Erfolgsgeschichte?, BB 2008, S. 1686–1692.

Böhning, Björn, Datenschutz – Die Debatte muss geführt werden, ZD 2013, S. 421–422.

Brand, Christian/*Rahimi-Azar*, Shahin, „AGG-Hopping" – eine Einnahmequelle mit strafrechtlichen Risiken, NJW 2015, S. 2993–2997.

Britz, Gabriele, Vom Europäischen Verwaltungsverbund zum Regulierungsverbund? – Europäische Verwaltungsentwicklung am Beispiel der Netzzugangsregulierung bei Telekommunikation, Energie und Bahn, EuR 2006, S. 46–77.

Bundeskartellamt, Gemeinsamer Leitfaden zur neuen Transaktionswert-Schwelle in der Fusionskontrolle in Deutschland und Österreich – öffentliche Konsultation, Pressemitteilung v. 14.5.2018, Bonn.

Busch, Christoph, Algorithmic Accountability, Osnabrück, 2018.

Citron, Danielle Keats/*Pasquale*, Frank, The Scored Society: Due Process for Automated Predictions, Washington Law Review 89 (2014), S. 1–33.

Coglianese, Cary/*Lehr*, David, Regulating by Robot, Administrative Decision Making in the Machine-Learning Era, Georgetown Law Journal 105 (2017), S. 1147–1223.

Diakopoulos, Nicholas/*Friedler*, Sorelle A./*Arenas*, Marcelo/*Barocas*, Solon, et al., Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, https://www.fatml.org/resources/principles-for-accountable-algorithms (25.10.2018).

Domurath, Irina/*Neubeck*, Irene, Verbraucher-Scoring aus Sicht des Datenschutzrechts, Working Paper, Berlin, Oktober 2018.

Drechsler, Jörg/*Jentzsch*, Nicola, Synthetische Daten, Innovationspotential und gesellschaftliche Herausforderungen, Berlin, 2018.

Edwards, Lilian/*Veale*, Michael, Slave to the algorithm?, Why a 'right to explanation' is probably not the remedy you are looking for, Duke Law & Technology Review 16 (2017), S. 18–84.

Ehmann, Eugen/*Selmayr*, Martin (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl., München, 2018.

Ernst, Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, S. 1026–1036.

Fanta, Alexander, Österreichs Jobcenter richten künftig mit Hilfe von Software über Arbeitslose, netzpolitik.org vom 13.10.2018.

Floridi, Luciano/*Cowls*, Josh/*Beltrametti*, Monica/*Chatila*, Raja, et al., AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds & Machines 28 (2018), S. 689–707.

Franck, Lorenz, Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO), RDV 2016, S. 111–119.

Future of Life Institute, Asilomar AI Principles, https://futureoflife.org/ai-principles (25.10.2018).

Gasser, Tom Michael, Grundlegende und spezielle Rechtsfragen für autonome Fahrzeuge, in: Maurer, Markus/Gerdes, J. Christian/Lenz, Barbara u. a. (Hrsg.), Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, Berlin, 2015, S. 543–574.

Gersdorf, Hubertus/*Paal*, Boris P. (Hrsg.), Beck'scher Online-Kommentar Informations- und Medienrecht, 22. Ed. (Stand: 1.8.2018), München, 2018.

Grabitz, Eberhard/*Hilf*, Meinhard/*Nettesheim*, Martin (Hrsg.), Das Recht der Europäischen Union, EUV/AEUV, Losebl. (Stand: 65. Erg.-Lfg.) Bd. 1, München, 2018.

Härting, Niko, Mit der DSGVO zum "Golden Handshake" – von der Sprengkraft des "Rechts auf Kopie", https://www.cr-online.de/blog/2019/03/29/mit-der-dsgvo-zum-golden-handshake-von-der-sprengkraft-des-rechts-auf-kopie/ (02.04.2019).

Härting, Niko/*Schneider*, Jochen, Das Ende des Datenschutzes – es lebe die Privatsphäre, Eine Rückbesinnung auf die Kern-Anliegen des Privatsphärenschutzes, CR 2015, S. 819–827.

Herberger, Maximilian, "Künstliche Intelligenz" und Recht, Ein Orientierungsversuch, NJW 2018, S. 2825–2829.

Hoeren, Thomas/*Niehoff*, Maurice, KI und Datenschutz – Begründungserfordernisse automatisierter Entscheidungen, RW 9 (2018), S. 47–66.

Hoffmann-Riem, Wolfgang, Verhaltenssteuerung durch Algorithmen, Eine Herausforderung für das Recht, AöR 142 (2017), S. 1–42.

Hoffmann-Riem, Wolfgang/*Schmidt-Aßmann*, Eberhard/*Voßkuhle*, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts Bd. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl., München, 2012.

Hölters, Wolfgang (Hrsg.), Aktiengesetz, 3. Aufl., München, 2017.

Jellinek, Georg, Gesetz und Verordnung, Staatsrechtliche Untersuchungen auf rechtsgeschichtlicher und rechtsvergleichender Grundlage, Tübingen, 1919 (1887).

Kastl, Graziana, Algorithmen – Fluch oder Segen?, GRUR 2015, S. 136–141.

Kieck, Annika, Zum Verhältnis von Datenschutz- und Kartellaufsicht, PinG 2017, S. 67–72.

Kiefer, Günther, Die Beleihung, (K)ein unbekanntes Wesen?, NVwZ 2011, S. 1300–1303.

Kloepfer, Michael, Umweltrecht, 4. Aufl., München, 2016.

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

Kühling, Jürgen/*Buchner*, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München, 2018.

Kühling, Jürgen/*Martini*, Mario/*Heberlein*, Johanna/*Kühl*, Benjamin, et al., Die DSGVO und das nationale Recht, Erste Überlegungen zum nationalen Regelungsbedarf, Münster, 2016.

Kulartz, Hans-Peter/*Kus*, Alexander/*Portz*, Norbert/*Prieß*, Hans-Joachim (Hrsg.), Kommentar zum GWB-Vergaberecht, 4. Aufl., Köln, 2016.

Lepa, Manfred, Verfassungsrechtliche Probleme der Rechtsetzung durch Rechtsver-ordnung, AöR 105 (1980), S. 337–369.

von Lewinski, Kai/*de Barros Fritz*, Raphael, Arbeitgeberhaftung nach dem AGG infolge des Einsatzes von Algorithmen bei Personalentscheidungen, NZA 2018, S. 620–625.

Ludwig, Kristiana, Mehr Arbeit fürs Kartellamt, Süddeutsche Zeitung Online vom 21.11.2016.

Martini, Mario, Normsetzungsdelegation zwischen parlamentarischer Steuerung und legislativer Effizienz – auf dem Weg zu einer dritten Form der Gesetzgebung?, AöR 133 (2008), S. 155–190.

– Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, JA 2009, S. 839–845.

– Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, S. 1017–1025.

– Blackbox Algorithmus, Grundfragen einer Regulierung Künstlicher Intelligenz, New York et al., 2019.

Martini, Mario/*Botta*, Jonas, Iron Man am Arbeitsplatz? – Exoskelette zwischen Effizienzstreben, Daten- und Gesundheitsschutz, Chancen und Risiken der Verschmelzung von Mensch und Maschine in der Industrie 4.0, NZA 2018, S. 625–637.

Martini, Mario/*Kühl*, Benjamin, Staatliches Informationshandeln, Jura 2014, S. 1221–1236.

Maurer, Markus/*Gerdes*, J. Christian/*Lenz*, Barbara/*Winner*, Hermann (Hrsg.), Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, Berlin, 2015.

McNamara, Andrew/*Smith*, Justin/*Murphy-Hill*, Emerson, Does ACM's Code of Ethics Change Ethical Decision Making in Software Development?, ESEC/FSE '18, November 4–9, 2018, Lake Buena Vista, FL, USA.

Mittelstadt, Brent Daniel/*Allo*, Patrick/*Taddeo*, Mariarosaria/*Wachter*, Sandra/*Floridi*, Luciano, The ethics of algorithms, Mapping the debate, Big Data & Society 2016, S. 1–21.

Müller-Hengstenberg, Claus D./*Kirn*, Stefan, Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der "Verselbstständigung" technischer Systeme, MMR 2014, S. 307–313.

Nowak, Eric/*Rott*, Roland/*Mahr*, Till, Wer den Kodex nicht einhält, den bestraft der Kapitalmarkt?, Eine empirische Analyse der Selbstregulierung und Kapitalmarktrelevanz des Deutschen Corporate Governance Kodex, ZGR 2005, S. 252–279.

Paal, Boris P./*Pauly*, Daniel A. (Hrsg.), Datenschutz-Grundverordnung - Bundesdatenschutzgesetz, 2. Aufl., München, 2018.

Pasquale, Frank, The Black Box Society, The Secret Algorithms That Control Money and Information, Cambridge, 2015.

Pluta, Werner, Algorithmus schreibt wissenschaftliches Buch, golem.de vom 16.4.2019.

Podszun, Rupprecht/*Schwalbe*, Ulrich, Digitale Plattformen und GWB-Novelle: Überzeugende Regeln für die Internetökonomie?, NZKart 2017, S. 98–106.

Posser, Heinrich/*Wolff*, Heinrich Amadeus (Hrsg.), Beck'scher Online-Kommentar VwGO, 47. Ed. (Stand: 1.10.2018), München.

Reichwald, Julian/*Pfisterer*, Dennis, Autonomie und Intelligenz im Internet der Dinge, CR 2016, S. 208–212.

Reisman, Dillon/*Schultz*, Jason/*Crawford*, Kate/*Whittaker*, Meredith, Algorithmic Impact Assessments, A practical framework for public agency accountability, April 2018.

Rohde, Noëlle, Gütekriterien für algorithmische Prozesse, Eine Stärken- und Schwächenanalyse ausgewählter Forderungskataloge, Gütersloh, 2018.

Ruffert, Matthias, Rechtsquellen und Rechtsschichten des Verwaltungsrechts, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts Bd. I, Methoden, Maßstäbe, Aufgaben, Organisation, 2. Aufl., München, 2012, S. 1163–1256.

Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Verbraucherrecht 2.0, Verbraucher in der digitalen Welt, Berlin, Dez. 2016.

Saurer, Johannes, Die Mitwirkung des Bundestages an der Verordnungsgebung nach § 48b BImSchG, NVwZ 2003, S. 1176–1182.

Schack, Haimo, Internationales Zivilverfahrensrecht, Mit internationalem Insolvenz- und Schiedsverfahrensrecht, 7. Aufl., München, 2017.

Schmid, Alexander, Pflicht zur „integrierten Produktbeobachtung" für automatisierte und vernetzte Systeme, CR 2019, S. 141–147.

Schmidt am Busch, Birgit, Die Beleihung, Ein Rechtsinstitut im Wandel, DÖV 2007, S. 533–542.

Schweighofer, Erich/*Sorge*, Christoph/*Borges*, Georg/*Schäfer*, Christoph, et al., Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Gutachten der Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e.V. im Auftrag des Sachverständigenrats für Verbraucherfragen, Berlin, Oktober 2018.

Schwintowski, Hans-Peter, Wird Recht durch Robotik und künstliche Intelligenz überflüssig?, NJOZ 2018, S. 1601–1609.

Spranger, Tade Matthias/*Wegmann*, Henning, Öffentlich-rechtliche Dimensionen der Robotik, in: Beck, Susanne (Hrsg.), Jenseits von Mensch und Maschine, Ethische und rechtliche Fragen zum Umgang mit Robotern, Künstlicher Intelligenz und Cyborgs, Baden-Baden, 2012, S. 105–118.

Tene, Omer/*Polonetsky*, Jules, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 11 (2013), S. 239–273.

Tufekci, Zeynep, Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency, Colorado Technology Law Journal 13 (2015), S. 203–218.

Tutt, Andrew, An FDA for Algorithms, A New Agency, Administrative Law Review 69 (2017), S. 83–123.

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, Eine erste Bestandsaufnahme, ZD 2015, S. 347–353.

Wachter, Sandra/*Mittelstadt*, Brent, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review 2019, S. 1–84.

Wachter, Sandra/*Mittelstadt*, Brent/*Floridi*, Luciano, Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation, International Data Privacy Law 7 (2017), S. 76–99.

Weinzierl, Quirin, Warum das Bundesverfassungsgericht Fußballstadion sagt und Soziale Plattformen trifft, JuWissBlog Nr. 48/2018 vom 24.5.2018.

Weiß, Wolfgang, Dezentrale Agenturen in der EU-Rechtsetzung, EuR 2016, S. 631–666.

Whittaker, Meredith/*Crawford*, Kate/*Dobbe*, Roel/*Fried*, Genevieve, et al., AI Now Report 2018, Dezember 2018.

Wischmeyer, Nils, Der Computer, der mich einstellte, brand eins vom 4.12.2017.

Wischmeyer, Thomas, Regulierung intelligenter Systeme, AöR 143 (2018), S. 1–66.

Zweig, Katharina Anna, Wo Maschinen irren können, Arbeitspapier der Bertelsmann-Stiftung, Gütersloh, 2018.

Über den Autor

Prof. Dr. Mario Martini ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften, Stellvertretender Direktor des Deutschen Forschungsinstituts für öffentliche Verwaltung und Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“). Seit dem Sommer 2018 ist er Mitglied der Datenethikkommission der Bundesregierung und Fellow am CAIS. Vor seiner Tätigkeit in Speyer hatte er eine Professur für Staats- und Verwaltungsrecht an der Ludwig-Maximilians-Universität München inne.

Im Jahr 2006 habilitierte er sich an der Bucerius Law School mit einer Arbeit zu dem Titel »Der Markt als Instrument hoheitlicher Verteilungslenkung«. In der Zeit zwischen 2001 und 2007 war er dort als wissenschaftlicher Assistent und Habilitand am Lehrstuhl für Öffentliches Recht einschließlich Völker- und Europarecht (Prof. Dr. Jörn Axel Kämmerer) tätig. Im Anschluss an das Rechtsreferendariat in Rheinland-Pfalz (1998 – 2000) war er von 1995 bis 1998 als wissenschaftlicher Mitarbeiter an der Johannes-Gutenberg-Universität Mainz tätig. Dort wurde er im Jahre 1999 mit einer umweltrechtlichen Arbeit zu dem Thema »Integrierte Regelungsansätze im Immissionsschutzrecht« promoviert.

Jüngste Veröffentlichungen:

1. Monographien

- Blackbox Algorithmus – Grundfragen eine Regulierung künstlicher Intelligenz, Springer Verlag, 2019, 423 S.
- Zwischen Agora und Arkanum: die Innenministerkonferenz als Gegenstand des Informationsrechts, Verlag Duncker & Humblot, Berlin 2018, 284 S.
- Die Landarztquote - verfassungsrechtliche Zulässigkeit und rechtliche Ausgestaltung, Verlag Duncker & Humblot, 235 S., 2017 (mit Jan Ziekow).
- Verwaltungsprozessrecht und Allgemeines Verwaltungsrecht - eine systematische Darstellung in Text-Bild-Kombination, Verlag Vahlen, München, 2017, 243 S.

2. Aufsätze

- Facebook, die Lebenden und die Toten – Der digitale Nachlass aus telekommunikations- und datenschutzrechtlicher Sicht, JZ 2019, S. 235-241 (mit Thomas Kienle).
- Subsumtionsautomaten ante portas? - Zu den Grenzen der Automatisierung in verwaltungsrechtlichen (Rechtsbehelfs-)Verfahren, DVBl 2018, S. 1128 - 1138 (mit David Nink).
- Iron Man am Arbeitsplatz? - Exoskelette zwischen Effizienzstreben, Daten- und Gesundheitsschutz, NZA 2018, 625-637 (mit Jonas Botta).
- Das neue Sanktionsregime der DSGVO – ein scharfes Schwert ohne legislativen Feinschliff (gemeinsam mit David Wagner und Michael Wenzel), Teil 1: VerwArch 2018, S. 163-189, Teil 2: VerwArch 2018, S. 296-335.