Neue Zeitschrift für Verwaltungsrecht – Extra

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt Prof. Dr. Hermann Weber, Schriftleiter von 1982–2001

Herausgegeben von *Rechtsanwalt Prof. Dr. Rüdiger Breuer,* Bonn – *Prof. Dr. Martin Burgi,* München – *Prof. Dr. Christian Calliess,* Berlin – *Dr. Josef Christ,* Vizepräsident des BVerwG, Leipzig – *Prof. Dr. Klaus-Peter Dolde,* Rechtsanwalt, Stuttgart – *Dr. Frank Fellenberg,* Rechtsanwalt, Berlin – *Dr. Andreas Heusch,* Präsident des VG, Düsseldorf – *Prof. Dr. Thomas Mayen,* Rechtsanwalt, Bonn – *Prof. Dr. Hubert Meyer,* Geschäftsf. Vorstandsmitglied des Niedersächsischen Landkreistages, Hannover – *Prof. Dr. Janbernd Oebbecke,* Münster – *Prof. Dr. Joachim Scherer,* Rechtsanwalt, LL.M., Frankfurt a. M. – *Dr. Heribert Schmitz,* Ministerialrat, Berlin – *Prof. Dr. Friedrich Schoch,* Freiburg – *Dr. Thomas Schröer,* Rechtsanwalt, Frankfurt a. M. – *Prof. Dr. Rudolf Streinz,* München

Schriftleitung: Rechtsanwalt Prof. Dr. Achim Schunder und Rechtsanwältin Dr. Christiane Prause, Beethovenstraße 7 b, 60325 Frankfurt a. M.

10 2017
Seite 1–14
36. Jahrgang
15. Mai 2017

Professor Dr. Mario Martini und Forschungsreferent David Nink*

Wenn Maschinen entscheiden … – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz

§ 35 a VwVfG, § 31 a SGB X und § 155 IV AO machen den Weg für vollautomatisierte Verwaltungsverfahren in deutschen Amtsstuben frei. Die persönlichkeitsrechtlichen Anforderungen, welche die Datenschutz-Grundverordnung an solche Verfahren stellt, engen den bislang bestehenden mitgliedstaatlichen Handlungsspielraum ein; ihre Auswirkungen blieben in der wissenschaftlichen Diskussion bislang unbeleuchtet. Der Beitrag füllt diese Lücke – und wirft einen Blick auf allgemeine regulatorische Herausforderungen des Einsatzes von Algorithmen in der öffentlichen Verwaltung.

I. Die Verwaltungsautomatisierung auf dem Vormarsch

Verwaltungsangebote im Wege der Digitalisierung schneller, einfacher und besser verfügbar zu machen, gehört zu den Glaubensbekenntnissen jeder Regierungserklärung. Die Fortschritte künstlicher Intelligenz liefern auf dem Weg dorthin wichtiges Rüstzeug: Mithilfe maschineller Lernverfahren können Computerprogramme sich administrative Handlungsabläufe aneignen und unmittelbar in die Tat umsetzen. Ihre Automatisierungsleistung senkt nicht nur Verwaltungskosten;[1] im Idealfall trägt sie auch dazu bei, Flüchtigkeitsfehler und Fehleinschätzungen, die Sachbearbeitern aus Fleisch und Blut unterlaufen, zu verhindern oder wenigstens zu reduzieren.[2] Neutralität, Stringenz und Objektivität können positive Nebeneffekte einer Entscheidung sein, die ohne jede menschliche Beeinflussung zustande kommt.[3]

1. Entwicklungen im Besteuerungsverfahren

Im Steuerrecht legt § 155 IV AO die normativen Grundlagen für eine Vollautomatisierung. Seit Anfang 2017 gestattet die Vorschrift den Finanzämtern, Steuerverwaltungsakte – insbesondere die Steuerfestsetzung – *ausschließlich* automationsgestützt vorzunehmen.[4] Zulässig ist dies immer dann, wenn und soweit kein Anlass[5] dazu besteht, dass Amtsträger den Verwaltungsvorgang in persona bearbeiten müssen (§ 155 IV 1 AO).

Die Finanzverwaltung avanciert damit zum Vorreiter der Implementierung vollautomatisierter Verwaltungsverfahren. Einen vergleichbar hohen Grad der Digitalisierung erreicht bislang lediglich das vollautomatisierte gerichtliche Mahnverfahren (§ 689 I 2 ZPO).[6] Auch einige Verfahren im Recht der Ordnungswidrigkeiten laufen partiell automatisiert ab, etwa bei kleineren Straßenverkehrsverstößen;[7] auch manchen Abwasser-, Bau- und Rentenbescheid sowie Gehaltsabrechnungen erlassen die zuständigen Behörden bereits teilautomatisiert.

* *Mario Martini* ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter des Programmbereichs „Digitalisierung" am Deutschen Forschungsinstitut für Öffentliche Verwaltung Speyer. *David Nink* ist in dem Programmbereich Forschungsreferent.

Die Autoren danken insbesondere *Wiebke Fröhlich* sowie *Michael Kolain* für ihre wertvolle Unterstützung. Soweit nicht anders angegeben, wurden Internetquellen zuletzt am 20.3.2017 abgerufen.

1 Vgl. den Gesetzentwurf der Bundesregierung, BT-Drs. 18/7457, 46 f., 58, 119; *Beirat Verwaltungsverfahrensrecht beim BMI*, NVwZ 2015, 1114 (1115); *Siegel*, DVBl 2017, 24 (25); *Braun Binder*, DÖV 2016, 891 (895).

2 *Neumann*, Einsatz von Risikomanagement-Systemen im Vollzug des Steuerrechts – Sachverständigenauskunft vom 13.4.2016, 13.4.2016, 4. Die Gesetzesbegründung (o. Fn. 1) greift diesen Aspekt indes nicht auf.

3 *Schmitz/Prell*, NVwZ 2016, 1273 (1277).

4 Umfasst sind auch die Berichtigung, die Rücknahme, der Widerruf, die Aufhebung und die Änderung der Steuerfestsetzung sowie entsprechende Anrechnungen.

5 Einen solchen kann der Steuerpflichtige selbst setzen, indem er in einem dafür vorgesehenen Freitextfeld der Steuererklärung angibt, warum aus seiner Sicht eine Bearbeitung durch einen Menschen notwendig ist (§ 150 VII 1 AO iVm § 155 IV 3 AO).

6 Vgl. zu Hintergrund und Geschichte der Automation des Mahnverfahrens bereits *Keller*, NJW 1981, 1184; *Mayer*, NJW 1983, 92; *Sujecki*, MMR 2006, 369.

7 Vgl. etwa § 51 I 2 („mit Hilfe automatischer Einrichtungen erstellt") oder § 110 c I 2 OWiG („Dokument automatisiert hergestellt").

2. Entwicklungen im allgemeinen Verwaltungsverfahrensrecht und im Sozialrecht

a) *§ 35 a VwVfG als Türöffner für vollautomatisch erlassene Verwaltungsakte.* Die Reform des Besteuerungsverfahrens ist Teil einer umfassenden Modernisierung des Verwaltungsverfahrensrechts: Auch das VwVfG lässt nunmehr automatisierte Verwaltungsakte zu.

Schon bislang schloss es Automatisierungspläne nicht aus. Verwaltungsverfahren sind grundsätzlich nicht an bestimmte Formen gebunden (§ 10 S. 1 VwVfG); das VwVfG kennt keinen *Numerus clausus* der Handlungsformen.[8] Entsprechend machten § 28 II Nr. 4, § 37 II 1, V 1 und § 39 I 1, II Nr. 3 VwVfG bereits in der Vergangenheit beispielhaft deutlich, dass die Verwaltung sich „automatische Einrichtungen" zunutze machen kann.[9] Auch § 5 I 1 EGovG deutet die grundsätzliche Möglichkeit an, Verwaltungsverfahren elektronisch durchzuführen.

Vollautomatisch erlassene *Verwaltungsakte* erfasst der Wortlaut des § 35 VwVfG jedoch nicht hinreichend klar. Die einen Verwaltungsakt konstituierende „Verfügung, Entscheidung oder andere hoheitliche Maßnahme" knüpft (entsprechend der Vorstellung des historischen Gesetzgebers) an die Willensbetätigung eines Menschen an, der abstrakte gesetzliche Vorgaben auf den Einzelfall herunterbricht. Beim Einsatz vollautomatischer Systeme fehlt es daran: Die Willensentäußerung liegt (vorweggenommen) in der Programmierung und Implementierung des (ggf. autonom lernenden) Systems zu einem Zeitpunkt, in dem der zu entscheidende Einzelfall sich noch nicht in allen seinen Details abzeichnen konnte.[10] Solchen neuen Formen digitalisierter Entscheidungsfindung ebnet der neue § 35 a VwVfG nunmehr in rechtssicherer Weise den Weg. Die Vorschrift adressiert Fälle *vollständig* automatisiert erlassener Verwaltungsakte: Die Entscheidung darf also *ohne jegliche* menschliche Bearbeitung erfolgen.[11] Die für klassische Verwaltungsakte geltenden Vorschriften finden auf diese Fälle nunmehr Anwendung.[12]

§ 35 a VwVfG gestattet vollautomatisierte Verwaltungsverfahren zugleich nicht vorbehaltlos. Voraussetzung ist vielmehr, dass die Entscheidung der Verwaltung weder einen Ermessens- noch einen Beurteilungsspielraum eröffnet.[13] Davon lässt der Gesetzgeber auch keine Ausnahmen zu. Denn normative Gestaltungsspielräume dienen der Wahrung von Einzelfallgerechtigkeit – diese können Algorithmen[14] (noch) nicht zuverlässig herstellen: Ebenso wie die individuelle Beurteilung eines Sachverhalts setzt die Ermessensausübung immer eine einzelfallbezogene menschliche Willensbetätigung voraus.[15] Auch Fälle eines intendierten Ermessens[16] sind einer automatisierten Entscheidung nicht zugänglich. Denn sie erfordern eine individuelle Prüfung auf eine Atypik, die zur Abweichung von der Regelfolge zwingt.[17] Die Neuregelung im Verwaltungsverfahrensrecht zielt damit „vor allem [auf] einfach strukturierte Verfahren".[18] Nur in solchen Standardsituationen können Computeralgorithmen aus Sicht des Gesetzgebers ihre unschlagbare Effizienz und Zielorientierung ausspielen.[19]

Um sicherzustellen, dass eine Behörde für eine vollständig automatisierte Bearbeitung nicht vorschnell Verfahren auswählt, die sich später als ungeeignet entpuppen,[20] etabliert § 35 a VwVfG zusätzlich einen „Normvorbehalt":[21] Die Verwaltung darf Verfahren nicht aus eigenem Antrieb, sondern nur auf Grundlage einer weiteren Rechtsvorschrift vollständig automatisieren. Der Bundes- oder Landesgesetzgeber – bei Selbstverwaltungskörperschaften (in den Grenzen der Grundrechtswesentlichkeit) der Satzungsgeber – muss jeweils ergänzend tätig werden: Nur diesen Akteuren überlässt es das neue Verwaltungsverfahrensrecht, geeignete Verfahren zu dekretieren.

Denkbar ist eine Verfahrensautomatisierung etwa bei der Verlängerung von Personal-, Behinderten- oder Parkausweisen oder dem antragslosen Kindergeld. Die Digitalisierungsflaggschiffe Estland und Österreich haben damit erste Erfahrungen gesammelt.[22] In Deutschland hat die Freie und Hansestadt Hamburg automatisierte Verfahren als einen Baustein ihrer „digital first"-Strategie ausgerufen:[23] Sie hat sich zum Ziel gesetzt, geeignete konkrete Verfahren der Verwaltungsautomatisierung zu identifizieren und zu pilotieren. Das norddeutsche „Tor zur Welt" hat den Ehrgeiz, sich als nationaler Pionier automatisierter Verwaltungsverfahren zu positionieren.

Automatisierte Verwaltungsverfahren laufen Gefahr, Verfahrensrisiken sowie Darlegungs- und Argumentationslasten auf die Bürger zu verlagern sowie verfahrensrechtliche Beratungs- und Betreuungspflichten des Untersuchungsgrundsatzes abzubauen.[24] Um zu verhindern, dass dadurch Fragestellungen, die der Systementwickler nicht berücksichtigt hat, durch das Raster des automatisierten Systems fallen und so –

8 *Schmitz/Prell*, NVwZ 2016, 1273 (1275); die verwaltungsverfahrensrechtlichen Implikationen ausleuchtend *Braun Binder*, NVwZ 2016, 960 (963 f.).

9 Anders als § 35 a VwVfG sind diese Bestimmungen also lediglich auf *Teil*automatisierung ausgerichtet („mit Hilfe"); s. auch *Siegel*, DVBl 2017, 24 (25).

10 BT-Drs. 18/8434, 122, aA *Bull*, DVBl 2017, 409 (415).

11 Das ergibt sich aus dem Wortlaut ebenso wie aus der angestrebten Parallelität zwischen den Regelungen in der AO und im VwVfG, vgl. BT-Drs. 18/7457, 82 zu § 155 IV 1 AO nF: „ohne Prüfung durch Amtsträger"; *Braun Binder*, DÖV 2016, 891 (892). Die Begriffe „ausschließlich automationsgestützt" in § 155 IV 1 AO nF und die Formulierung „vollständig durch automatische Einrichtungen" in § 35 a VwVfG sind in der Sache deckungsgleich. Sehr kritisch zum Begriff „vollständig automatisiert" *Bull*, DVBl 2017, 409 (410 f.), der insbesondere bemängelt, dass der Gesetzgeber nicht festlegt, wo die Grenze zum „elektronisch" oder „mit Hilfe automatischer Einrichtungen" erlassenen Verwaltungsakt liegt. In der Sache ergibt sich die Trennlinie daraus, dass die Neuregelung ihrem Sinn nach nur ohne menschliche Einwirkung ergehende Verwaltungsakte erfassen will.

12 BT-Drs. 18/8434, 122; *Braun Binder*, NVwZ 2016, 960 (963 f.).

13 *Schmitz/Prell*, NVwZ 2016, 1273 (1276); *Braun Binder*, DÖV 2016, 891 (894).

14 Allgemein bezeichnet „Algorithmus" eine eindeutige Handlungsanweisung, welche die Lösung von Problemen in Teilschritten anleitet. Der Beitrag verwendet den Oberbegriff in seiner speziellen digitalen Erscheinungsform iSv „Programmcode" (sc. als [Computer-]Algorithmus).

15 Vgl. BT-Drs. 18/8434, 122.

16 Vgl. *BVerwGE* 72, 1 (6) = NJW 1986, 738 (739 f.); *BVerwGE* 91, 82 (90) = NJW 1993, 744 (746).

17 *Siegel*, DVBl 2017, 24 (26).

18 BT-Drs. 18/8434, 122.

19 *Siegel*, DVBl 2017, 24 (26).

20 Vgl. BT-Drs. 18/8434, 122.

21 Der Begriff „Gesetzesvorbehalt", den die Gesetzesbegründung verwendet, ist missverständlich, s. *Braun Binder*, DÖV 2016, 891 (893). Der Gesetzgeber wollte damit klarstellen, dass der vollautomatisierte Erlass eines Verwaltungsaktes nur auf Basis einer entsprechenden „Rechtsvorschrift" zulässig ist. Das kann neben einem Gesetz auch eine Satzung oder Verordnung sein, s. *Siegel*, DVBl 2017, 24 (26) sowie *Schmitz/Prell*, NVwZ 2016, 1273 (1276). Verwaltungsvorschriften sind hingegen nicht ausreichend.

22 Vgl. etwa *Bohsem*, Von Estland lernen, SZ-online v. 14.6.2016. In Österreich setzt die Regierung auf eine „Digital Roadmap Austria", die zB eine antragslose Verlängerung der Familienbeihilfe und weitere Vereinfachungen ermöglicht, vgl. auch www.digitalroadmap.gv.at./.

23 Vgl. dazu Hmbg-Bürgerschafts-Drs. 21/4472, 5, sowie den Antrag „Digitalisierung braucht starken Datenschutz" einiger Abgeordneter, Hmbg-Bürgerschafts-Drs. 21/6977, 1.

24 *Beirat Verwaltungsverfahrensrecht beim BMI*, NVwZ 2015, 1114 (1115 f.); *Braun Binder*, NVwZ 2016, 960 (964); *dies.*, Jusletter IT vom 25.5.2016, 1 (7, Rn. 12); *Bull*, DVBl 2017, 409 (412); *Heintzen*, DÖV 2015, 780 (784 ff.); *Siegel*, DVBl 2017, 24 (27).

etwa in atypischen Härtefällen – in falsche oder unvollständige Entscheidungen münden, hat der Gesetzgeber als Gegengewicht einen Schutzmechanismus implementiert:[25] Der neue § 24 I 3 VwVfG verpflichtet die Behörden, beim Einsatz automatisierter Einrichtungen tatsächliche Angaben des Beteiligten zu berücksichtigen, die für den Einzelfall bedeutsam sind, im maschinellen Verfahren aber keine Berücksichtigung fänden.

Ein Verfahren ist nur dann vollständig digitalisiert,[26] wenn an seinem Ende kein gedruckter Verwaltungsakt steht: Medienbrüche können die Effizienzvorteile jeder Verwaltungsautomatisierung torpedieren. Vor diesem Hintergrund hat der Gesetzgeber eine zusätzliche Form der *Bekanntgabe* elektronischer Verwaltungsakte zugelassen: § 41 II a VwVfG ermöglicht es der Behörde, den Verwaltungsakt dadurch bekannt zu geben, dass der Adressat ihn über öffentlich zugängliche Netze (sog. Verwaltungsportale) abruft (vgl. auch § 37 II a SGB X und § 122 AO nF).[27]

b) *§ 31 a SGB X.* Auch das Sozialrecht hat im Zuge des Gesetzes zur Modernisierung des Besteuerungsverfahrens eine Anpassung erfahren. Im Gleichlauf mit § 35 a VwVfG gestattet die Vorschrift des § 31 a SGB X den Sozialbehörden nunmehr, vollautomatisch generierte Verwaltungsakte zu erlassen.[28] Gerade in der Sozialverwaltung bieten sich dafür viele routinegeprägte, eher rechen- als entscheidungsintensive Verfahren an, etwa die Gewährung oder Verlängerung standardisierter Sozialleistungen.[29] Anders als das Allgemeine Verwaltungsrecht kennt das Sozialverwaltungsrecht keinen Normvorbehalt – auch keine ausdrückliche Beschränkung der Vollautomatisierung auf gebundene Entscheidungen. Voraussetzung für deren Zulässigkeit ist hier wie im Steuerrecht (§ 155 IV 1 AO aE) lediglich, aber immerhin, dass im Einzelfall kein Anlass für eine Bearbeitung durch einen Amtsträger besteht (§ 31 a S. 1 SGB X).

II. Unionsrechtliche Vorgaben für vollautomatisierte Verfahren

Automatisierte (Verwaltungs-)Verfahren rechtlich zuzulassen und normativ auszugestalten, steht nicht im Belieben des nationalen Gesetzgebers. Im Gegenteil: Das unionale Datenschutzrecht limitiert seinen Handlungsrahmen nachhaltig. Art. 22 I DSGVO spricht ein grundsätzliches Verbot automatisierter Entscheidungsfindung aus (vgl. auch ErwGr 20, 52 und 97); es beansprucht ab dem 25.5.2018 Geltung (Art. 99 II DSGVO).

Der europäische Gesetzgeber reagiert damit auf strukturelle Persönlichkeitsrisiken, die mit der Auslagerung der Verwaltungstätigkeit auf Computerprogramme einhergehen: Eine automatisierte Verwaltungsentscheidung kann den Einzelnen zum bloßen Objekt eines staatlichen Verarbeitungsvorgangs degradieren, der dem Personsein des Betroffenen sowie der Individualität des konkreten Falls keine Beachtung schenkt. Dem bisherigen nationalen Recht ist diese Wertung keineswegs fremd: Art. 22 DSGVO ist in weiten Teilen mit § 6 a BDSG identisch.

1. DSGVO

Art. 22 I DSGVO verbietet nicht jede durch ein Computerprogramm beeinflusste Entscheidung, sondern allein eine solche, der *keine inhaltliche Bewertung durch eine natürliche Person* vorausgeht. Die Vorschrift erfasst also nicht alle Konstellationen, in denen ein Computerprogramm unterstützend in die Entscheidungsvorbereitung eingebunden ist.[30] Sie meint vielmehr nur Konstellationen, in denen ein Algorithmus die alleinige Entscheidung fällt – auch solche, in denen ein Mensch eine *lediglich formale Bearbeitung* vornimmt, ohne über die Handlungsmacht oder eine ausreichende Datengrundlage zu verfügen, um von der bereits automatisiert getroffenen Entscheidung abzuweichen.[31]

Art. 22 I DSGVO erstreckt seinen Verbotsradius auch nicht generell auf *alle* automatisierten Entscheidungen, sondern nur solche, die – wie Verwaltungsentscheidungen typischerweise – für den Betroffenen eine *rechtliche Wirkung* nach sich ziehen oder ihn in vergleichbarer Weise erheblich beeinträchtigen (Art. 22 I DSGVO). Diese kritische Schwelle ist nicht erst bei einer Leistungsverweigerung, sondern auch dann überschritten, wenn ein Antragsteller Leistungen, zB eine Förderung, gleichheitswidrig nicht erhält.[32]

a) *Mindestgarantien (Art. 22 III DSGVO).* Das unionsrechtliche Verbot automatisierter Einzelentscheidungen gilt nicht vorbehaltlos. Art. 22 II DSGVO lässt Ausnahmen zu: für Vertragsverhältnisse (Buchst. a), aufgrund besonderer unionaler oder mitgliedstaatlicher Regelungen (Buchst. b) und im Falle einer ausdrücklichen Einwilligung des Betroffenen (Buchst. c).[33]

Die Ausnahmen stellen dem Verantwortlichen zugleich keine *Carte blanche* aus. Sie sind vielmehr an die Bedingung geknüpft, durch flankierende Schritte hinreichenden Persönlichkeitsschutz sicherzustellen: Der Verantwortliche[34] hat in jedem Einzelfall „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person“ (Art. 22 II Buchst. b und III DSGVO) zu treffen.[35] Die DSGVO bewegt sich damit in der Regelungstradition der Datenschutz-Richtlinie (95/46/EG, DSRL): Deren Art. 15 II Buchst. b knüpfte die Zulässigkeit automatisierter Einzelentscheidungen an Garantien, welche die berechtigten Interessen Betroffener durch geeignete Maßnahmen – bspw. die Möglichkeit, den eigenen Standpunkt geltend zu machen – sicherstellen sollen.[36]

Worin die Mindestgarantien bei vollautomatisierten *Verwaltungsverfahren*[37] im Einzelnen bestehen und wie weit sie reichen müssen, lässt die DSGVO weitgehend offen. Art. 22 III sowie ErwGr 71 UAbs. 2 S. 1 DSGVO deuten ihren notwendigen Inhalt und ihre Zielrichtung zumindest an. Sie sollen einen Grundrechtsschutz durch Verfahren her-

25 Vgl. BT-Drs. 18/8434, 122.
26 Dazu auch *Bull*, DVBl 2017, 409 (410 f.).
27 Zur elektronischen Bekanntgabe über Behördenportale ausführlich *Braun Binder*, NVwZ 2016, 342; *Bull*, DVBl 2017, 409 (413 f.); *Schmitz/Prell*, NVwZ 2016, 1273 (1277 ff.).
28 Die Bekanntgabe solcher Verfügungen über Behördenportale ermöglicht § 37 II a SGB X.
29 Die Gesetzesbegründung nennt beispielhaft die automatische Anpassung laufender Sozialleistungen, vgl. BT-Drs. 18/8434, 121.
30 *Martini* in *Paal/Pauly*, DS-GVO, 2016, Art. 22 Rn. 20.
31 *Kamlah* in *Plath*, BDSG/DSGVO, 2. Aufl. 2016, Art. 22 DSGVO Rn. 6 sowie *ders.*, aaO, § 6 a Rn. 12 f.; zu § 6 a I 2 BDSG bereits BT-Drs. 16/10529, 13.
32 Vgl. zu der Frage, ob die Ablehnung eines Antrags unter Art. 22 I DSGVO fallen kann: *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 28.
33 Ausführlich *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 30 ff.; s. auch *Deuster*, PinG 2016, 75 (77 f.).
34 „Verantwortlicher“ ist jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DSGVO).
35 Siehe auch *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 35 f. Die Formulierung ist inhaltlich nahezu deckungsgleich mit derjenigen des § 6 a II Nr. 2 BDSG: „wenn die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist“.
36 Zum Vergleich des Art. 22 DSGVO mit Art. 15 DSRL *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 14.
37 Für diese verbleibt als Ausnahme von dem Verbot des Art. 22 I DSGVO die Öffnungsklausel des Art. 22 II Buchst. b DSGVO. Der Mindestgarantienkatalog des Art. 22 III DSGVO ist auf diese Fälle nicht unmittelbar anwendbar. Vgl. dazu im Einzelnen II 1 a ff.

stellen: Die Maßnahmen müssen rechtsstaatlichen Standards der Einwirkung und Kontrolle einer Entscheidung genügen (aa–cc) – und sie müssen dem Ziel verschrieben sein, „eine faire und transparente Verarbeitung zu gewährleisten" (dd). Fehlerquellen, die automatisierten Verwaltungsverfahren innewohnen, gilt es also zu minimieren. Der Verantwortliche darf insbesondere nur solche statistischen Verfahren anwenden, die für den konkreten Einsatzbereich geeignet sind. Fehlerhaft in das Verfahren eingespeiste Daten und Diskriminierungsrisiken muss er eliminieren.

aa) *Recht auf persönliches Eingreifen des Verantwortlichen.* Wer von einer vollautomatisierten Entscheidung betroffen ist, muss das Eingreifen eines Menschen in den Datenverarbeitungsprozess verlangen können (Art. 22 III DSGVO iVm ErwGr 71 UAbs. 1 S. 4). Damit dieses Recht nicht leer läuft, muss die eingreifende Person das Ergebnis oder wesentliche Aspekte des Datenverarbeitungsprozesses tatsächlich beeinflussen können.[38]

Zwar proklamiert die DSGVO apodiktisch „das Recht auf Erwirkung des Eingreifens einer Person" vorbehaltlos. Gleichwohl unterliegt es nach seiner Ratio seinerseits Grenzen. Sonst käme das Recht auf Eingreifen einer Person im Ergebnis einem vorbehaltlosen Recht gleich, keiner automatisierten Entscheidung ausgesetzt zu sein. Ein solches wollen Art. 22 II und III DSGVO nach ihrem normativen Anspruch aber gerade ausschließen; sie sollen automatisierten Entscheidungen einen normativ gangbaren Weg in die Anwendungspraxis ebnen. In der Sache formuliert die DSGVO also lediglich ein Recht, das Eingreifen einer natürlichen Person in den Verarbeitungsprozess *aus berechtigten Gründen im Einzelfall* verlangen zu können.

bb) *Recht auf Darlegung des eigenen Standpunkts.* Die DSGVO verbürgt dem Einzelnen das Recht, seinen eigenen Standpunkt darzulegen, etwa um komplizierte Zusammenhänge und Spezifika des Einzelfalls vorzutragen (Art. 22 III DSGVO iVm ErwGr 71 UAbs. 1 S. 4). Damit diese Befugnis nicht zu einer inhaltsleeren Floskel verkommt, ist der Verantwortliche verpflichtet, die dargelegten Aspekte auch *tatsächlich zu berücksichtigen*:[39] Er ist nicht nur dazu angehalten, die Entscheidung zu überprüfen, sondern muss sich mit den Aspekten, die der Betroffene vorbringt, auch inhaltlich auseinandersetzen.

Ob die Berücksichtigung „des eigenen Standpunkts" einer natürlichen Person vorbehalten bleiben muss oder auch durch ein rein maschinelles Verfahren rechtmäßig erfolgen kann, lässt die DSGVO offen; der Wortlaut lässt beide Deutungsmöglichkeiten zu. Nach der Rationalität der Norm ist allein entscheidend, dass der Vortrag des Betroffenen überhaupt in geeigneter Weise Berücksichtigung finden kann und nicht ungehört an dem System „abprallt". Sofern ein technisches Verfahren dies gewährleistet, genügt es den normativen Schutzanforderungen.

Nach derzeitigem Stand der Technik können technische Systeme komplexe menschliche Einlassungen aber nicht hinreichend zuverlässig erfassen. Um prüfen zu können, ob die tatsächlichen Angaben einer Person rechtlich bedeutsam sind, bedarf es namentlich in der Regel einer menschlichen Einzelfallprüfung, welche die Darlegung und Berücksichtigung des Betroffenenstandpunkts hinreichend sichert. Dem Recht auf Darlegung des eigenen Standpunkts genügt insbesondere nicht die Möglichkeit, aus einer enumerativen Liste vorformulierte Aussagen auswählen zu können. Vielmehr müssen die Betroffenen auch unvorhergesehene Sonderfälle und individuelle Sichtweisen darlegen können. Ein System muss deshalb – ggf. durch eine ergänzende Serviceeinheit mit Sachbearbeitern aus Fleisch und Blut – Raum für frei formulierte Eingaben lassen. Andernfalls erweist es sich als ungeeignet, dem Recht auf Darlegung des eigenen Standpunkts zu entsprechen.

cc) *Recht auf inhaltliche Neubewertung.* Schutzmaßnahmen bewahren den Betroffenen grundsätzlich nur dann wirksam vor einer Herabwürdigung zum Entscheidungsobjekt, wenn ihm grundsätzlich die Möglichkeit verbleibt, eine andere Entscheidung herbeizuführen (Art. 22 III DSGVO iVm ErwGr 71 UAbs. 1 S. 4). Ihm muss jedenfalls ein Recht auf Anfechtung[40] der automatisiert getroffenen Entscheidung zustehen. Dass er die Entscheidung bei einer *anderen Stelle* (zB bei einer Aufsichtsbehörde oder vor Gericht) überprüfen lassen kann, genügt der Ratio der Norm dabei nicht. Gemeint ist vielmehr die Anfechtung *beim Verantwortlichen* mit dem Ziel einer inhaltlichen Neubewertung. Der Verantwortliche darf das Anfechtungsrecht auch nicht an unzumutbar hohe (formelle oder inhaltliche) Hürden knüpfen, die Abschreckungseffekte auslösen können. Um seinem normativen Zweck gerecht zu werden, muss es vielmehr niederschwellig ausgestaltet sein.

dd) *Faire und transparente Verarbeitung.* Bezieht die automatisierte Entscheidung Profiling-Maßnahmen, also auf der Grundlage von Persönlichkeitsprofilen erstellte Analysen bzw. Vorhersagen, in die Entscheidung ein, hat der Verantwortliche „geeignete mathematische oder statistische Verfahren" zu verwenden (ErwGr 71 UAbs. 2 S. 1 DSGVO). Damit will der europäische Gesetzgeber Verzerrungen des Persönlichkeitsbildes entgegenwirken, die von untauglichen Berechnungsmodellen ausgehen können,[41] und damit eine faire sowie transparente Verarbeitung gewährleisten.

Die Formulierung „geeignete […] Verfahren" impliziert, dass das Ergebnis der Berechnungen auf einer *korrekten und aktuellen Datengrundlage* basieren muss. Denn nur auf einer validen Faktenbasis kann ein taugliches Berechnungsverfahren zu richtigen Ergebnissen gelangen. Der Verantwortliche hat daher technische und organisatorische Maßnahmen zu treffen, die das Risiko von Fehlern in jedem Arbeitsschritt wirksam minimieren. Faktoren, die als Folge einer Datenauswertung unrichtige personenbezogene Daten generieren

38 Das Gesetz zur Modernisierung des Besteuerungsverfahrens berücksichtigt dies in § 155 IV 3 AO.

39 In welcher Art und Weise der Verantwortliche den Standpunkt zu berücksichtigen hat, regelt die DSGVO nicht. Ficht der Betroffene eine automatisiert getroffene Entscheidung an und legt den eigenen Standpunkt dar – ohne dass er von seinem Recht auf menschliches Eingreifen Gebrauch macht –, kann die Überprüfung der Entscheidung (unter Berücksichtigung des dargelegten Standpunkts) wiederum automatisiert, also allein auf der Grundlage technischer Einrichtungen, erfolgen. Die Effizienz der Automatisierung bleibt so erhalten, ohne Betroffenenrechte zu untergraben. Auch nach einer (menschlichen) Einzelfallprüfung bleibt die weitere automatisierte Bearbeitung zulässig. Die DSGVO schweigt hierzu zwar. Der Schluss ergibt sich jedoch systematisch aus den Rationalitätsgrenzen des Rechts auf Eingreifen einer Person. Vgl. auch *Prell* in *Bader/Ronellenfitsch*, BeckOK VwVfG, 34. Ed. (1.1.2017), § 35 a VwVfG Rn. 18; *Schmitz/Prell*, NVwZ 2016, 1273 (1277).

40 Teilweise auch *Remonstrationsrecht* genannt, s. *Kamlah* in *Plath*, BDSG/DSGVO, Art. 22 DSGVO Rn. 14.

41 Das gilt auch für das Scoring sowie alle vergleichbaren Verfahren, die Teil einer automatisch getroffenen Entscheidung sind. Scoring beschreibt ein mathematisch-statistisches Verfahren zur Berechnung der Wahrscheinlichkeit, mit der eine bestimmte Person ein bestimmtes Verhalten, insbesondere Zahlungsfähigkeit und -willigkeit, an den Tag legen wird, BT-Drs. 16/10529, 1; vgl. auch *von Lewinski* in *Wolff/Brink*, BeckOK DatenschutzR, 19. Ed. (Stand: 1.2.2017), BDSG § 28 b Rn. 1 f.; zur Frage, inwieweit Scoring unter Art. 22 DSGVO fällt *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 24; zustimmend *Buchner* in *Kühling/Buchner*, DS-GVO, 2017, Art. 22 Rn. 38.

(ErwGr 71 UAbs. 2 S. 1 DSGVO), muss er korrigieren. Dazu gehören Fehlerroutinen und Überprüfungsmechanismen (wie zB Stichproben), welche die Datengrundlage überprüfen, sowie Sicherungsmaßnahmen, die für die Integrität, Vertraulichkeit und Authentizität der Daten bürgen (vgl. auch Art. 32 I DSGVO).[42]

Auch offen oder verdeckt diskriminierende Entscheidungsmechanismen – etwa solche, die an das Geschlecht, die Religion, genetische Anlagen oder den Gesundheitszustand anknüpfen – sind Teil des Gefahrenarsenals automatisierter Entscheidungen. Ihnen muss der Verantwortliche durch Sicherungsmechanismen begegnen (ErwGr 71 UAbs. 2 S. 1 und S. 2 DSGVO).

ee) *Weitere Maßnahmen.* Der Katalog der Schutzmaßnahmen, welche Art. 22 III und ErwGr 71 UAbs. 2 DSGVO als normativ zwingend erachten, ist nicht abschließend, sondern lediglich als eine beispielhafte Aufzählung von Mindestgewährleistungen konzipiert. Weitere Maßnahmen schließt er nicht aus, sondern notwendig mit ein („mindestens das Recht …"). Zu ihnen können insbesondere Begründungspflichten oder Pflichten zur Offenlegung aller Entscheidungsparameter sowie regelmäßige Risikofolgenabschätzungen und Routinevalidierungen gehören.[43]

ff) *„Angemessene Maßnahmen" in den Fällen des Art. 22 II Buchst. b DSGVO.* Seinen Katalog der Mindestgarantien erstreckt Art. 22 III DSGVO ausdrücklich nur auf Konstellationen, in denen der Betroffene einwilligt oder die Entscheidung für die Erfüllung eines Vertrages erforderlich ist (die „in Absatz 2 Buchstaben a und c genannten" Fälle). Zulässigkeitstatbestände, in denen die Mitgliedstaaten – wie im Falle automatisierter Verwaltungsverfahren[44] – von der Öffnungsklausel[45] des Art. 22 II Buchst. b DSGVO Gebrauch machen, erfasst Art. 22 III DSGVO demgegenüber nicht.

Dass der Unionsgesetzgeber beide Konstellationen unterschiedlich regelt,[46] überrascht zunächst, folgt aber einer inneren Logik, nämlich der unterschiedlichen normativen Struktur der Regelungen. Beide Normen knüpfen an unterschiedliche Adressaten an: Art. 22 III iVm II Buchst. a und Buchst. c DSGVO richten ihren Verhaltensbefehl unmittelbar an den *Verantwortlichen*; Abs. 2 Buchst. b adressiert demgegenüber die *Mitgliedstaaten*, gesteht ihnen namentlich einen inhaltlich gebundenen Abweichungsspielraum von den Regelungen der DSGVO zu.

In beiden Fällen postuliert die DSGVO in der Sache aber im Grundsatz ein gleichwertiges Schutzniveau: Erlässt ein Mitgliedstaat auf der Grundlage des Abs. 2 Buchst. b eine Regelung, muss diese „angemessene Maßnahmen" sicherstellen – ebenso wie in den Konstellationen der unmittelbar kraft Unionsrechts verankerten Ausnahmetatbestände. Der nationale Gesetzgeber ist dann aber frei darin, zu bestimmen, was „angemessene Maßnahmen" im Einzelnen sind. Der beispielhafte Katalog des Abs. 3 bietet ihm dabei Orientierungsleitlinien, welche ihm die Erwartung des Unionsrechts vor Augen führen; die Mitgliedstaaten können die Freiheiten und Rechte der Betroffenen aber auch auf andere Weise schützen. Relevant ist nur, dass sie im Ergebnis ein hinreichendes Schutzniveau gewährleisten.[47]

b) *Auskunfts- und Informationsrechte bzw. -pflichten (Art. 12 ff. DSGVO).* aa) *Grundsatz.* Wer von einer automatisierten Entscheidung betroffen ist, kann von seinen Rechten nur Gebrauch machen, wenn er überhaupt von der Datenverarbeitung und dem damit verbundenen Risiko erfährt. Zu diesem Zweck erlegen Art. 13 und 14 DSGVO dem Verantwortlichen Informationspflichten auf. Sie sind kein Spezifikum des automatisierten Verwaltungsverfahrens, sondern beanspruchen grundsätzlich für alle Datenverarbeitungsvorgänge Geltung.

Ihren Pflichtenkanon erweitern Art. 13 II Buchst. f bzw. Art. 14 II Buchst. g DSGVO[48] um eine wichtige, auf Big-Data-Prozesse zugeschnittene Note: Der Verantwortliche muss auch darüber aufklären, dass eine automatisierte Entscheidungsfindung stattfindet – ferner aussagekräftige Informationen über die *involvierte Logik* sowie die *Tragweite* und die voraussichtlichen *Auswirkungen* der Verarbeitung mitteilen.[49] So soll der Betroffene nachvollziehen können, dass und wie eine automatisierte Entscheidung zustande gekommen ist. Das ist Ausdruck des Transparenzanspruchs der DSGVO (Art. 5 Abs. 1 Buchst. a, ErwGr 71 UAbs. 2 S. 1 DSGVO).[50]

Wer *keine Information* über eine automatisierte Verarbeitung erhalten hat, eine solche aber vermutet oder für möglich hält, dem gewährt die DSGVO ein Auskunftsrecht: Der Betroffene kann eine Bestätigung darüber verlangen, ob der Verantwortliche ihn betreffende personenbezogene Daten verarbeitet hat und welcher Automatisierungslogik der Vorgang folgt (Art. 15 I Buchst. h DSGVO).[51] Um ihren normativen Zweck zu erreichen, müssen die Mitteilungen und Auskünfte auch für Laien verständlich sein und dem Betroffenen in klarer und einfacher Sprache nahebringen, wie er seine Rechte und Interessen wahrnehmen kann (Art. 12 I 1 DSGVO).

bb) *Mitgliedstaatliche Regelungsspielräume.* Von den ausladend ausgeformten Informationsrechten der Art. 12 ff. DSGVO des Betroffenen darf der nationale Gesetzgeber (ebenso wie von Art. 22 DSGVO) nicht pauschal dispensieren. Art. 23 DSGVO gesteht ihm zwar einen Abweichungsspielraum zu, knüpft diesen jedoch zugleich an enge Grenzen, namentlich: spezifische Schutzziele. Zu ihnen gehören

42 Dazu auch *Martini* in *Paal/Pauly*, DS-GVO, 2016, Art. 32 Rn. 25 ff.
43 Dazu auch die Regulierungsvorschläge unten IV.
44 Etwas anderes gilt, soweit diese sich auf eine ausdrückliche Einwilligung des Betroffenen stützen (Art. 22 II Buchst. c DSGVO). Das dürfte in praxi nur selten der Fall sein.
45 Zu Begriff und Umfang der Öffnungsklauseln der DSGVO ausführlich *Kühling/Martini* et al., Die DSGVO und das nationale Recht, 2016, 2 ff.
46 Anders in Art. 22 IV DSGVO, der nicht zwischen Abs. 2 Buchst. a, Buchst. b und Buchst. c differenziert.
47 Der nationale Gesetzgeber kann bspw. auch hier Begründungspflichten oder Pflichten zur Offenlegung aller Entscheidungsparameter implementieren sowie regelmäßige Risikofolgenabschätzungen und Routinevalidierungen oder besondere Algorithmen-Kontrollmechanismen vorsehen. Dazu im Einzelnen unten IV.
48 Art. 13 DSGVO ist in den Fällen einschlägig, in denen die Datenerhebung direkt beim Betroffenen erfolgt. In allen anderen Fällen greifen die Informationspflichten des Art. 14 DSGVO.
49 Welche konkreten Angaben der Verantwortliche dem Betroffenen, insbesondere zu Einzelheiten der einer Entscheidung zugrunde liegenden Logik sowie zu den verwendeten Grundannahmen, zur Verfügung muss, lässt der Wortlaut weitgehend offen. Vgl. *Schmidt-Wudy* in *Wolff/Brink*, BeckOK DatenschutzR, 19. Ed. (Stand: 1.2.2017), Art. 15 DSGVO Rn. 78.
50 Die Pflicht, dem Betroffenen unaufgefordert das *Vorliegen* einer automatisierten Einzelentscheidung mitzuteilen, bestand bereits unter § 6 a II Nr. 2 BDSG.
51 Art. 13 II Buchst. f, Art. 14 II Buchst. g und Art. 15 DSGVO gestalten diese Pflichtenstellung des Verantwortlichen als ein „Recht" Betroffener aus. Der Ausdruck impliziert, dass die normative Position entfällt, wenn der Betroffene sie nicht (als Anspruch) geltend macht. Das entspricht auch der Systematik der DSGVO: Die Normen sind Teil des Kap. III DSGVO, das die „Rechte der betroffenen Person" bündelt. Auch Art. 22 I gestaltet die DSGVO als „Recht" aus. Der logischen Struktur und ihrem Aussagegehalt entspricht das jedoch nicht, vgl. *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 29; die Vorschrift ist insofern systematisch unglücklich verortet.

insbesondere die öffentliche Sicherheit (Buchst. c), und der „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats" (Buchst. e).

Je nach (bspw. sicherheitssensiblem) Einsatzbereich eines vollautomatisierten Verwaltungsverfahrens können die Informationspflichten der Art. 12 ff. DSGVO die effektive Erreichung der Schutzziele des Art. 23 I Buchst. c – Buchst. j DSGVO im Einzelfall durchaus gefährden. Das alleine genügt aber nicht, um Einschränkungen des Art. 22 DSGVO oder der Informationspflichten zu rechtfertigen. Vielmehr sind sie zusätzlich strikten Verhältnismäßigkeitsbindungen sowie dem Wesensgehaltsgebot der Grundrechte unterworfen: Es bedarf stets einer sorgfältigen Abwägung der kollidierenden Interessen. Fällt sie (ausnahmsweise) zugunsten einer mitgliedstaatlichen Beschränkung aus, muss der nationale Gesetzgeber überdies die zulässigen Zwecke und den Umfang der Beschränkungen sowie die damit verbundenen Risiken hinreichend präzise benennen (Art. 23 II DSGVO).

c) *Besondere Kategorien personenbezogener Daten.* Daten über die rassische und ethnische Herkunft, die Gesundheit, die sexuelle Orientierung oder politische Überzeugungen und sonstige besondere personenbezogene Daten iSd Art. 9 I DSGVO ist eine besonders hohe Persönlichkeitssensitivität eigen. Automatisierte Entscheidungen dürfen daher grundsätzlich nicht auf ihnen beruhen (Art. 22 IV iVm Art. 9 I DSGVO).

Der europäische Gesetzgeber lässt zwar Ausnahmen zu. Er legt die Hürden dafür aber hoch: Der Betroffene muss entweder in die Datenverarbeitung eingewilligt haben (Art. 22 IV iVm Art. 9 II Buchst. a DSGVO) – oder an ihr muss ein erhebliches öffentliches Interesse bestehen (Art. 9 II Buchst. g DSGVO), welches eine nationale oder unionale Norm unter ihren besonderen Schutz stellt. Diese muss dann (ähnlich wie im Fall des Art. 23 I DSGVO) aber zugleich die Verhältnismäßigkeit sowie den Wesensgehalt der Persönlichkeitsrechte wahren und dafür hinreichende Schutzmaßnahmen treffen.[52] Soweit eine Verarbeitung besonderer Datenkategorien „erforderlich ist, um rechtliche Ansprüche […] in einem Verwaltungsverfahren" geltend zu machen oder auszuüben, hält der europäische Gesetzgeber solche Maßnahmen ausdrücklich für ausnahmsweise zulässig (ErwGr 52 S. 3 DSGVO). In ausländerrechtlichen Verarbeitungskontexten kann bspw. das Bedürfnis bestehen, bei Verarbeitungen auf die ethnische Herkunft zurückzugreifen, um den Berechtigungsstatus, zB für Sozialleistungen, fehlerfrei zu prüfen.

d) *Minderjährigenschutz.* Mit Blick auf die persönlichkeitsrechtliche Gefahrenlage, die automatisierte (Verwaltungs-) Entscheidungen auslösen können, „sollten" derartige Verarbeitungen nach dem Willen des europäischen Normgebers kein Kind[53] betreffen (ErwGr 71 UAbs. 1 S. 5 DSGVO). Die DSGVO formuliert damit jedoch kein absolutes Verbot, sondern lässt Raum für Ausnahmen. Das macht auch der Vergleich mit der – insofern strikteren – Trilog-Fassung deutlich: Diese proklamierte noch das normative Gebot, dass die Entscheidung „kein Kind betreffen *darf*".[54] Soll eine automatisierte Entscheidung gegenüber Kindern ausnahmsweise zulässig sein, so muss der Verantwortliche daher geeignete Sicherungsmaßnahmen zum Schutz ihrer Persönlichkeitsrechte treffen. Welche das im Einzelnen sind, deutet Art. 8 DSGVO an. Die Vorschrift ist zwar nicht unmittelbar einschlägig: Sie regelt die Bedingungen für Angebote „von Diensten der Informationsgesellschaft" (Art. 4 Nr. 25 DSGVO iVm Art. 1 I Buchst. b RL (EU) 2015/1535), die „einem Kind direkt gemacht" werden (Art. 8 I UAbs. 1 S. 1 DSGVO). Verwaltungsverfahren fallen typischerweise nicht darunter: Sie werden – anders als Art. 1 I Buchst. b der RL (EU) 2015/1535 voraussetzt – nicht „in der Regel gegen Entgelt" erbracht. Art. 8 DSGVO gibt freilich zumindest Orientierung darüber, welche Anforderungen grundsätzlich zu beachten sind, wenn ein Verantwortlicher personenbezogene Daten junger Menschen unter 16 Jahren[55] verarbeitet: Die Einwilligung des „Träger(s) der elterlichen Verantwortung" ist unverzichtbar (Art. 8 I UAbs. 1 S. 2 DSGVO).[56]

Sollen automatisierte Entscheidungen gegenüber Kindern ausnahmsweise zulässig sein, gehört zu dem gebotenen besonderen Schutz der Persönlichkeitsentwicklung Minderjähriger insbesondere die Aufklärung über spezifische Persönlichkeitsrisiken. Informationspflichten (Art. 13 ff. DSGVO) muss der Verantwortliche zudem in kindgerechter Sprache und Aufmachung nachkommen (Art. 12 I 1 Hs. 2 iVm ErwGr 58 S. 4 DSGVO).[57]

Nimmt man das normative Gebot der DSGVO ernst, die Persönlichkeitsentwicklung von Kindern unter besonderen Schutz zu stellen, dann sind automatisierte Entscheidungen gegenüber dieser Personengruppe mit der Wertentscheidung des Art. 22 I DSGVO im Ergebnis regelmäßig nicht in Einklang zu bringen. Das gilt insbesondere – wiewohl und gerade weil Kinder elektronischen Verfahren besonders zugänglich sind – für automatisierte Entscheidungen mit nachhaltigen Auswirkungen, die Pflichten oder Sanktionswirkungen auslösen können und in ihren Folgen nur schwer rückgängig zu machen sind.

e) *Verzeichnis der Verarbeitungstätigkeiten.* Die DSGVO stellt dem Verantwortlichen nicht gänzlich frei, ob und wie er seine Verarbeitungsvorgänge dokumentiert. Art. 30 I DSGVO erlegt dem Verantwortlichen vielmehr auf, ein umfassendes Verzeichnis aller Datenverarbeitungstätigkeiten zu führen.[58] Diese Pflicht soll den Aufsichtsbehörden eine vorläufige Rechtmäßigkeitsprüfung ermöglichen und die Transparenz der Verarbeitung erhöhen.[59] Gerade bei automatisierten Entscheidungen ist ohne eine Dokumentation der Verarbeitungstätigkeiten eine wirksame Kontrolle typischerweise nur bedingt möglich, laufen sie doch in einer für Dritte nicht erkennbaren Weise ab.

Auch Behörden müssen diesem Rechtsgebot im Rahmen vollautomatisierter Verwaltungsverfahren nachkommen. Das impliziert insbesondere Dokumentationen der Verarbei-

52 S. auch *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 41; weitere Vorschläge zur Realisierung dieses Schutzes – neben den beschriebenen Vorgaben der DSGVO – s. unten IV.

53 Unter „Kind" versteht die DSGVO alle natürlichen Personen, welche noch nicht die Volljährigkeitsgrenze erreicht haben. Das ergibt sich im Umkehrschluss aus Art. 8 I UAbs. 1 S. 2 („das Kind noch nicht das sechzehnte Lebensjahr vollendet"): Auch mit 16 Jahren ist ein Betroffener also noch Kind iSd DSGVO. Die DSGVO sieht den Status als Kind unausgesprochen mit der Volljährigkeit enden.

54 Hervorhebung d. Verf. Vgl. dazu auch *Martini* in *Paal/Pauly*, DS-GVO, Art. 22 Rn. 35. Vgl. auch Art. 8 DSGVO sowie ErwGr 38, 58 S. 4, 65 S. 3 und S. 4.

55 Bei der Festlegung der Altersgrenze gesteht die DSGVO den Mitgliedstaaten einen Abweichungsspielraum zu. Eine Absenkung unter ein Alter von 13 Jahren schließt sie aber aus (Art. 8 I UAbs. 2 DSGVO).

56 Nach deutschem Recht sind das in der Regel die Eltern (§ 1626 I BGB).

57 Bei Angeboten, die sich an Kinder richten, gehen die Anforderungen also über das Merkmal „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" hinaus; sie müssen „in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann" (ErwGr 58 S. 4 DSGVO).

58 Eingehend *Schäffter*, Verfahrensverzeichnis 2.0, 2016, 1 ff.; zum Mindestinhalt des Verzeichnisses *Martini* in *Paal/Pauly*, DS-GVO, 2016, Art. 30 Rn. 6 ff.

59 *Martini* in *Paal/Pauly*, DS-GVO, Art. 30 Rn. 2.

tungsroutinen und Sicherheitsmaßnahmen, welche die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherstellen.

f) *Datenschutz-Folgenabschätzung*. Löst eine Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten der Betroffenen aus, muss der Verantwortliche (bei Verwaltungsverfahren also die zuständige öffentliche Stelle) vorab eine Datenschutz-Folgenabschätzung durchführen (Art. 35 I DSGVO iVm ErwGr 89 S. 3 und 92).[60] Diese Risikoanalyse fungiert als Frühwarnlicht, das den Verantwortlichen zu einer risikobasierten Selbsteinschätzung bewegen soll, um die Gefahren von Persönlichkeitsverletzungen frühzeitig erkennen und eingrenzen zu können.[61]

Die Pflicht zur individuellen Risikoabschätzung entfällt, wenn bereits der Gesetzgeber eine allgemeine (Gesetzes-)Folgenabschätzung durchgeführt und auf diese Weise die möglichen datenschutzrechtlichen Risiken antizipiert hat (Art. 35 X iVm Art. 6 I UAbs. 1 Buchst. c und e DSGVO).[62] In Fällen vollautomatisierter Verwaltungsverfahren dürfte das der Regelfall sein. Denn der Gesetz- bzw. Verordnungsgeber muss die „Geeignetheit" iSd § 35 a VwVfG besonders legitimieren und begründen.

2. DSRL-PS

Verarbeiten Behörden Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten bzw. der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, beansprucht die DSGVO keine Geltung. Vielmehr finden dann die Sonderregelungen der Datenschutzrichtlinie für Polizei und Strafjustiz (DSRL-PS)[63] Anwendung (Art. 2 II Buchst. d DSGVO, Art. 1 I, Art. 2 I DSRL-PS). Ihre Regelungen sind mit denjenigen des Art. 22 DSGVO jedoch strukturell vergleichbar: Die Mitgliedstaaten dürfen eine „automatisierte Entscheidungsfindung im Einzelfall" nur zulassen, sofern das jeweilige Recht geeignete Garantien für die Rechte und Freiheiten des Betroffenen bietet, wie sie auch Art. 22 III DSGVO verlangt (Art. 11 DSRL-PS).

In einem Aspekt geht die DSRL-PS über die DSGVO indes hinaus: Profiling-Maßnahmen, die Diskriminierungen auf der Grundlage besonderer Kategorien personenbezogener Daten nach sich ziehen, sind nicht nur grundsätzlich,[64] sondern generell unzulässig (Art. 11 III DSRL-PS).[65] Das Verbot erstreckt sich (anders als Art. 22 I DSGVO) auch auf Profiling-Maßnahmen, die nicht unmittelbar in eine Entscheidung mit Rechtswirkung münden: Art. 11 III DSRL-PS knüpft nur allgemein an ein Profiling, nicht aber zwingend an eine Entscheidung iSd Abs. 1 an. Die Richtlinie spricht damit (ähnlich wie Art. 3 III GG) ein absolutes Diskriminierungsverbot aus, das der besonderen Sensibilität für die Persönlichkeitsentwicklung und der verdeckten Diskriminierungsanfälligkeit algorithmenbasierter Maßnahmen bei polizeilichen Datenverarbeitungen Tribut zollt.

III. Ausgestaltung des nationalen Regelungsspielraums

1. Verfassungsrechtliche Vorgaben

Lässt der nationale Gesetzgeber kraft des ihm verbleibenden Regelungsspielraums Ausnahmen vom grundsätzlichen Verbot automatisierter Verwaltungsverfahren zu, ist er neben Art. 22 und Art. 12 ff. DSGVO auch den verfassungsrechtlichen Schranken des Grundrechts auf informationelle Selbstbestimmung ausgesetzt. Die Wertungen der DSGVO und des GG laufen insoweit weitgehend parallel: Staatliche Entscheidungen dürfen den Einzelnen nicht zum bloßen Objekt machen und in einer Weise „seine Subjektqualität prinzipiell in Frage" stellen,[66] welche die Achtung des Wertes vermissen lässt, die einem jeden Menschen zukommt.

Allein der Umstand, dass personenbezogene Daten „Objekt" algorithmischer Analyse sind, missachtet nicht grundsätzlich die Subjektqualität des Einzelnen.[67] Diese ist allenfalls dann tangiert, wenn ein Algorithmus den Grundrechtsträger nachteiligen Folgen aussetzt, ohne ihm die Chance zu eröffnen, sich gegen die Entscheidung in angemessener Weise zur Wehr setzen zu können. Dem Recht auf informationelle Selbstbestimmung genügt es daher im Allgemeinen, wenn die Verwaltung sicherstellt, dass der Betroffene in Zweifelsfällen das persönliche Eingreifen eines (menschlichen) Sachbearbeiters verlangen darf, der die Entscheidung des Algorithmus überprüft bzw. korrigiert. Im nationalen Datenschutzrecht hat diesen Anforderungen bislang § 6 a BDSG Rechnung getragen.[68]

2. BDSG-neu

Im künftigen deutschen Datenschutzrecht wird § 37 BDSG-E[69] den bisherigen § 6 a BDSG ablösen. Die Vorschrift dispensiert von dem grundsätzlichen Verbot automatisierter Einzelentscheidungen des Art. 22 I DSGVO. Sie beschränkt sich in ihrem lakonischen Wortlaut allerdings auf Entscheidungen „im Rahmen der Leistungserbringung nach einem Versicherungsvertrag". Für automatisierte *Verwaltungs*verfahren trifft der Entwurf demgegenüber keine Sonderregelungen. Das überrascht, will der deutsche Gesetzgeber doch gerade für das Steuerrecht sowie das verwaltungs- und sozialrechtliche Verfahrensrecht von seinem Regelungsspielraum Gebrauch machen.[70] Ausnahmen von dem Verbot des Art. 22 I DSGVO, mit denen Nationalstaaten die Öffnungsklausel des Art. 22 II Buchst. b DSGVO ausfüllen, unterliegen zwar keinem Zitiergebot. Benennt der Gesetzgeber im Normwortlaut des § 37 BDSG-E aber über „die in Arti-

60 Zum Risikobegriff und zu den inhaltlichen Anforderungen s. *Martini* in *Paal/Pauly*, DS-GVO, 2016, Art. 35 Rn. 14 ff., Rn. 44 ff.
61 *Martini* in *Paal/Pauly*, DS-GVO, Art. 35 Rn. 6 ff.
62 S. auch *Martini* in *Paal/Pauly*, DS-GVO, Art. 35 Rn. 35 ff.
63 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, ABl. EU L 119/89 v. 4.5.2016. Die häufig zu findende Bezeichnung „Richtlinie für den Datenschutz bei Polizei und Justiz" ist etwas irreführend: Die RL gilt nicht für die gesamte Justiz, sondern nur für einen begrenzten Teil der (Straf-)Justiz – etwa für Datenerhebungen im Ermittlungsverfahren, zB nach § 168 c StPO.
64 Vgl. demgegenüber Art. 22 IV DSGVO.
65 Darunter fallen insbesondere Diskriminierungen auf der Grundlage der Rasse oder Ethnie, politischer Meinungen sowie religiöser oder weltanschaulicher Überzeugungen. Auch Profiling-Maßnahmen, welche die Gewerkschaftszugehörigkeit, genetische oder biometrische Daten sowie Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung analysieren, sind nicht zulässig.
66 *BVerfGE* 30, 1 (26).
67 Vgl. *BVerfGE* 109, 279 (312 f.) = NJW 2004, 999 (1001 f.); *Hillgruber* in *Epping/Hillgruber*, BeckOK GG, 32. Ed. (Stand: 1.3.2017), Art. 1 Rn. 13.
68 Die Vorschrift etablierte ein dreistufiges Verfahren: (1.) Information über die Entscheidung, (2.) auf Anfrage Mitteilung und Erläuterung der wesentlichen Entscheidungsgründe, (3.) die Möglichkeit, den eigenen Standpunkt geltend zu machen – um anschließend erforderlichenfalls eine Überprüfung bzw. Neubewertung zu erreichen, *Gola/Klug/Körffer* in *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 6 a Rn. 14; vgl. auch *Deuster*, PinG 2016, 75 (76 f.).
69 Gesetzentwurf der Bundesregierung zur Anpassung des Datenschutzrechts an die VO (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BT-Drs. 18/11325.
70 Er erwähnt dies beiläufig in der Gesetzesbegründung, BT-Drs. 18/11325, 105.

kel 22 Absatz 2 Buchstabe a und c der VO (EU) 2016/679 genannten Ausnahmen“ hinaus explizit weitere nationale Sondertatbestände, wäre es regulatorisch angezeigt, nicht nur die versicherungsvertragsrechtlichen, sondern auch die für Verwaltungsverfahren konzipierten Privilegierungen ebendort zu benennen.[71]

Über Art. 22 I DSGVO hinaus wird das BDSG-neu auch die aus Art. 13 ff. DSGVO erwachsenden Auskunfts- und Informationsrechte[72] des Betroffenen beschränken: § 33 I Nr. 1 BDSG-E ermöglicht es öffentlichen Stellen, auf die Information des Betroffenen nach Art. 14 I, II und IV DSGVO zu verzichten, sofern anderenfalls die ordnungsgemäße Erfüllung ihrer Aufgaben iSd Art. 23 I Buchst. a bis e DSGVO gefährdet wäre oder „sonst dem Wohle des Bundes oder eines Landes Nachteile“ drohen.[73] Ob diese unspezifische Einschränkung mit Art. 23 DSGVO im Einklang steht, ist zweifelhaft. Einen solchen Vorbehalt eines nationalen Schutzziels kennt Art. 23 DSGVO nicht. Er verlangt einen hinreichend konkreten Rekurs auf die spezifischen Tatbestände seines Abs. 1.

Unterbleibt die individuelle Information des Betroffenen aufgrund dieser nationalen Modifikationen der Informationsrechte, nimmt der Gesetzgeber als Kompensation für die damit verbundenen Einschränkungen den Verantwortlichen in die Pflicht, *geeignete* andere Maßnahmen zu ergreifen, insbesondere die entsprechenden Informationen für die Öffentlichkeit in „leicht zugänglicher Form“ bereitzustellen (§§ 32 II, 33 II BDSG-E). Dass in einem Verwaltungsverfahren Entscheidungen automatisiert ergehen können, sollten Behörden vor diesem Hintergrund in jedem Falle vorab kundtun (vgl. Art. 13 II Buchst. f, 14 II Buchst. g DSGVO).

3. VwVfG-neu und AO-neu – Vereinbarkeit mit den Vorgaben der DSGVO

a) *Änderungen des VwVfG*. Die nationalen Normen, welche von dem grundsätzlichen Verbot automatisierter Verwaltungsverfahren des Art. 22 I DSGVO dispensieren, müssen sich einer Konformitätsprüfung am Maßstab der persönlichkeitsrechtlichen Mindestgebote des Unionsrechts stellen.

aa) *§ 35 a VwVfG*. Isoliert betrachtet genügt § 35 a VwVfG den Anforderungen, welche Art. 22 II Buchst. b DSGVO an vollautomatisierte Entscheidungen stellt, noch nicht: Die nationale Norm trifft als solche keine Vorkehrungen zum Schutz des Persönlichkeitsrechts. Sie will nach ihrem eigenen Anspruch automatisierten Verwaltungsverfahren aber auch nur einen verfahrensrechtlichen Rahmen setzen, ohne diesen im Einzelnen auszugestalten. Die konkrete Implementierung einzelner Verfahren bedarf jeweils einer ergänzenden Regelung: Nicht allein § 35 a VwVfG als Grundnorm, sondern der Regelungsverbund des Fachverfahrens mit den verwaltungsverfahrensrechtlichen Sondervorschriften muss als Gesamtkonzept den materiellen Vorgaben des Art. 22 II Buchst. b DSGVO genügen.

bb) *Recht auf Darlegung des eigenen Standpunkts – § 24 I 2 VwVfG*. Zum persönlichkeitsrechtlichen Mindestschutz automatisierter Verfahren gehört die Möglichkeit des Betroffenen, solche Spezifika zu Gehör zu bringen, die dem Einzelfall seine Einzigartigkeit verleihen.[74] Diese kann ein automatisiertes Prüfraster seiner Natur nach nur berücksichtigen, soweit sie sich bereits bei der Einrichtung des jeweiligen Systems antizipieren lassen.[75] In unvorhergesehenen Fallkonstellationen entscheidet das System dann im Zweifel zufällig, fehlerhaft und ohne die Besonderheiten des Einzelfalls zu berücksichtigen. Darauf reagiert die neue Vorschrift des § 24 I 3 VwVfG in gleichsam vorauseilendem Gehorsam gegenüber dem unionsrechtlichen Recht auf Darlegung des eigenen Standpunkts:[76] Individuelle Angaben des Betroffenen müssen Berücksichtigung finden – jedoch nicht pauschal, sondern nur, wenn sie im Einzelfall für die rechtliche Bewertung von Relevanz sind („für den Einzelfall bedeutsame“).[77] Anders als die äquivalente Regelung im Besteuerungsverfahren (§ 88 iVm § 150 VII AO) verlangt § 24 I 3 VwVfG aber nicht Freitextfelder für zusätzliche Angaben. Auf solch strenge Vorgaben hat der Gesetzgeber im VwVfG wegen des potenziell breiteren Anwendungsbereichs bewusst verzichtet.[78] Den Anforderungen des Rechts auf Darlegung des eigenen Standpunkts genügt das als solches jedoch noch nicht. Denn der Einzelfall lässt sich typischerweise gerade nicht formularmäßig abschließend erfassen. Die jeweiligen Fachverfahren werden geeignete Möglichkeiten vorsehen müssen, der Komplexität auftretender Sonderfälle in automatisierten Verfahren Rechnung zu tragen.[79]

b) *Änderungen der AO – legality by design durch Risikomanagementsysteme*. Nicht nur Menschen, sondern auch Computerprogrammen unterlaufen in Verwaltungsverfahren Fehler. Findet keine Einzelfallprüfung durch einen Amtsträger statt, muss die rechtliche Umhegung algorithmenbasierter Verfahren in hinreichendem Maße für die Rechtmäßigkeit der Entscheidungen bürgen; erforderlich ist eine „legality by design“.[80]

Für das (automatisierte) Besteuerungsverfahren hat der Gesetzgeber in § 88 V AO nF einen speziellen Schutzmechanismus implementiert:[81] Ein Risikomanagementsystem soll die Sicherheit und Qualität des automatisierten Verfahrens sicherstellen sowie eine Konzentration der personellen Ressourcen auf die tatsächlich prüfbedürftigen Fälle ermöglichen. Darin liegt zugleich ein schleichender Systemwechsel: Eine automationsgestützte Risikobewertung löst den Grundsatz der Einzelfallprüfung ab.

Dem Risikomanagementsystem ist es nicht darum bestellt, jedes abstrakt denkbare Risiko auszuschalten. Vielmehr soll es Steuerverkürzungen verhindern und gezielt Betrugsfälle aufdecken, eine präventive Wirkung auf die Steuerpflichtigen entfalten sowie die Bearbeitungsqualität durch Standardisierung der Arbeitsabläufe optimieren.[82] Zu diesem Zweck prüft es automatisch, ob bestimmte Angaben in einer Steuererklärung unplausibel sind, und leitet solche Fälle ggf.

71 Eine entsprechende Klarstellung gerade im BDSG-neu ist also nicht zwingend erforderlich, trüge vor diesem Hintergrund aber zu Rechtsklarheit und -sicherheit bei.
72 Siehe dazu oben II 1 b.
73 Vgl. BT-Drs. 18/11325, 101 ff.
74 Dazu oben II 1 a bb.
75 BT-Drs. 18/8434, 122; *Schmitz/Prell*, NVwZ 2016, 1273 (1277).
76 Dazu bereits oben II 1 a bb.
77 Für das Besteuerungsverfahren vgl. BT-Drs. 18/8434, 122. *Siegel*, DVBl 2017, 24 (27) mahnt an, die Möglichkeit, unbedeutenden Vortrag auszublenden (§ 24 I 3 VwVfG), restriktiv zu handhaben.
78 *Schmitz/Prell*, NVwZ 2016, 1273 (1277).
79 Vgl. dazu auch bereits oben II 1 a bb, 6 ff.
80 *Beirat Verwaltungsverfahrensrecht beim BMI*, NVwZ 2015, 1114 (1117): „sachlich richtige und gleichmäßige Anwendung des materiellen Rechts“; vgl. auch *Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz*, Verbraucherrecht 2.0, Dez. 2016, 63 ff., insbes. S. 67; das Konzept ist vergleichbar mit dem (spezielleren Konzept) des „privacy by design“, welches bereits Art. 24 I, 25 II DSGVO vorgeben.
81 Dazu auch *Braun Binder*, NVwZ 2016, 960 (961 f.); *Neumann*, Einsatz von Risikomanagement-Systemen im Vollzug des Steuerrechts – Sachverständigenauskunft vom 13.4.2016, 2. Der Einsatz von Risikomanagementsystemen in den Finanzbehörden ist nicht neu, vgl. *Münch*, DStR 2013, 212 (212 f.). Die Automatisierung des Verfahrens evoziert indes neue (datenschutz-)rechtliche Fragen.
82 Dazu und nachfolgend BT-Drs. 18/7457, 69 f.

einem Sachbearbeiter aus Fleisch und Blut zur Überprüfung weiter: Steuert das Risikomanagementsystem einen Fall zur Bearbeitung durch einen Amtsträger aus, hat dieser – je nach Sachlage – eine punktuelle oder umfassende Ermittlung und Überprüfung durchzuführen. Flankierend tritt eine nach Zufallskriterien vorgenommene (menschliche) Auswertung einzelner Verfahrensvorgänge hinzu, die ua dazu dient, die Wirkung der Aussteuerungsmechanismen zu überprüfen.

Zu der genauen technischen Ausgestaltung des Risikomanagementsystems schweigt das Gesetz.[83] Es lässt insbesondere offen, ob es sich bei ihm um ein sog. lernendes System[84] handeln muss oder darf, das seine Eigenschaften in der Interaktion mit der Außenwelt autonom zu modifizieren in der Lage ist. Gleichzeitig bringt der Gesetzgeber der Funktionsfähigkeit der Software, die dem Kontrollsystem unterlegt ist, zu Recht kein blindes Systemvertrauen entgegen. § 88 V 3 AO benennt vielmehr explizit die an das Risikomanagementsystem zu stellenden *Mindest*anforderungen: Es muss gewährleisten, dass es durch Zufallsauswahl eine hinreichende Anzahl von Fällen zur (umfassenden) Prüfung durch Amtsträger auswählt (Nr. 1) und dann auch tatsächlich eine Prüfung dieser Sachverhalte durch Amtsträger erfolgt (Nr. 2). Auch die Auswahl der zu prüfenden Fälle vertraut der Gesetzgeber nicht ausschließlich dem Risikomanagementsystem an. Es schlägt vielmehr Amtsträgern geeignete Fälle zur Prüfung vor, aus denen diese dann auswählen können (Nr. 3). Um Veränderungen des Systems erfassen und auf Fehler rechtzeitig reagieren zu können, ist es einer regelmäßigen Überprüfung zu unterziehen (Nr. 4). Nur so kann das Risikomanagementsystem seinem gesetzlich festgelegten Ziel gerecht werden, eine qualitativ hochwertige Rechtsanwendung durch bundeseinheitlich abgestimmte Vorgaben – und damit Gleichmäßigkeit sowie Gesetzmäßigkeit – zu erreichen: Das Potpourri der Maßnahmen soll gewährleisten, dass sowohl unplausible als auch signifikant risikobehaftete Fälle weiterhin einer menschlichen Entscheidung unterliegen, in unproblematischen Fällen aber die Effizienzkraft der Automatisierung wirken kann.[85]

Die Strukturvorgaben, denen das Risikomanagementsystem nach dem Willen des Gesetzgebers genügen muss, tragen den Anforderungen, die Art. 22 II Buchst. b DSGVO an automatisierte Verwaltungsentscheidungen stellt, noch nicht hinreichend Rechnung: Die obligatorischen Zufallsstichproben ermöglichen zwar eine fortlaufende Kontrolle der Funktionsweise des Systems, die Fehler korrigiert und das Risiko von Fehlschlüssen minimiert (vgl. ErwGr 71 UAbs. 2 S. 1 DSGVO);[86] sie verlangen auch eine persönliche Prüfung ausgesteuerter Sachverhalte durch Amtsträger ab. Sie verleihen dem Einzelnen insoweit jedoch kein subjektives Recht iSd ErwGr 71 UAbs. 1 S. 4 DSGVO.[87] Ein solches Recht auf persönliches Eingreifen des Verantwortlichen verbürgt aber § 150 VII 1 AO iVm § 155 IV 3 AO: Die Normen eröffnen dem Bürger die Möglichkeit, in einem dafür vorgesehenen Datenfeld entsprechende, aus seiner Sicht besonders prüfbedürftige Angaben zu machen. Gleiches gilt für die Darlegung des eigenen Standpunkts[88] und das Recht auf inhaltliche Neubewertung[89] iSd ErwGr 71 UAbs. 1 S. 4. Der Steuerpflichtige kann hierdurch verhindern, dass eine ausschließlich automationsgestützte Verarbeitung erfolgt (§ 155 IV 3 AO) und damit ggf. (entsprechend den Schutzerwartungen des Art. 22 II Buchst. b DSGVO)[90] eine persönliche Bearbeitung seines Sachverhalts erzwingen. Das betrifft zB Fälle, in denen der Betroffene darauf hinweist, dass er seiner Steuererklärung eine Rechtsauffassung zugrunde legt, die von derjenigen der Finanzverwaltung abweicht.[91] Eine solche Prüfung durch einen Sachbearbeiter aus Fleisch und Blut ist gegenwärtig noch unabdingbar. Einzelfallgerechtigkeit lässt sich auf absehbare Zeit nicht in ein deterministisches Muster gießen oder durch lernende Systeme simulieren.

IV. Bausteine eines Persönlichkeits- und Diskriminierungsschutzes de lege lata und de lege ferenda, insbesondere Algorithmenkontrolle

1. Regulierungsbedürfnis

Eines der zentralen Risiken automatischer Systeme adressiert der Gesetzgeber in § 88 AO sowie in § 155 IV AO, § 35 a VwVfG und § 31 a SGB X nicht ausdrücklich: Computeralgorithmen sind nicht davor gefeit, ihren Selektionsmechanismen diskriminierende Auslesekriterien (zB Religion oder Geschlecht) zugrunde zu legen. Denn Algorithmen fahnden mithilfe stochastischer Methoden nach statistischen Korrelationen in der Datenbasis: Sie schließen von Gruppenmerkmalen auf Fehler und Risiken. Sie können dadurch wichtige Anhaltspunkte für rechtmäßige Eingrenzungen von Kontrollroutinen liefern. Ihrem Wesen nach können sie aber keine Kausalitäten ermitteln, die einen zuverlässigen Rückschluss auf den konkreten Einzelfall zulassen. Daraus erwächst das Risiko von (Gruppen-)Diskriminierungen. Gerade in sozialrechtlichen (Verwaltungs-)Verfahren wird ein effizienzorientierter Algorithmus sein Entscheidungsraster bspw. im Zweifel an der ethnischen Herkunft oder der Konfession ausrichten, wenn es einen statistisch signifikanten Zusammenhang zwischen der Zahl der Fälle von Sozialbetrug und der Tätergruppe „Menschen mit Migrationshintergrund“ oder einen validen Zusammenhang zwischen Steuerbetrug und der Religionszugehörigkeit gibt.[92] Normativ bedingte Beschränkungen der Datenverarbeitung sind ihm in seiner ergebnisorientierten Grundanlage grundsätzlich fremd.

a) *Vergleich zur analogen Welt.* Diskriminierungsrisiken ethnischen, religiösen oder sozialen Profilings sind kein neues Phänomen einer digitalisierten Welt. Sachbearbeiter haben schon in der Vergangenheit auf der Grundlage ihrer Erfahrung sowie Intuition (mitunter vorurteilsbehaftete) Kontrollroutinen entwickelt und ihren Entscheidungen unterlegt, ohne sie offenzulegen. Sowohl menschliche als auch algorithmische Diskriminierungseinflüsse sind nur schwer rekonstru-

83 Zur Kritik bspw. *Neumann in Finanzausschuss des Bundestages*, Wortprotokoll der 75. Sitzung der 18. Wahlperiode, 13.4.2016, 23 ff. sowie in seiner schriftlichen Stellungnahme, 128 ff.

84 Zu den Herausforderungen der Kontrolle maschineller Lernverfahren unten IV 3 c.

85 BT-Drs. 18/7457, 82; vgl. auch S. 70: Das Risikomanagementsystem iSd § 88 V AO will der Gesetzgeber nicht als eine bloße automationsgestützte Plausibilitätsprüfung verstanden wissen.

86 Vgl. bereits oben II 1 a dd.

87 Vgl. bereits oben II 1 a aa.

88 Dazu oben II 1 a bb.

89 Dazu oben II 1 a cc.

90 Siehe dazu oben II 1 a aa.

91 BT-Drs. 18/7457, 49.

92 Eine deutlich höhere relative Kriminalitätsbelastung weist die Polizeiliche Kriminalitätsstatistik (PKS) des Jahres 2015 aus (Bundesministerium des Innern, Polizeiliche Kriminalstatistik 2015, Version 7.0): In manchen Deliktsgruppen sind Menschen ohne deutschen Pass verglichen mit ihrem Anteil an der Bevölkerung überproportional vertreten (PKS 2015, S. 70, Abschn. 9.1, Tabelle T05). Der Anteil Nichtdeutscher an der Gesamtzahl der Tatverdächtigen für verschiedene Delikte beträgt bei der Gewaltkriminalität zB 33,2 %, bei Raubdelikten 38,4 %, bei Betrugsdelikten 31,2 % (davon durch Erschleichen von Leistungen 40,0 %) sowie beim Taschendiebstahl 75,7 %. Dabei darf nicht übersehen werden, dass die PKS wie jede Statistik einer Interpretation, zB im Hinblick auf die Vergleichbarkeit der Grundgesamtheit, bedarf.

ierbar, kann der Betroffene sie doch regelmäßig nur vermuten, nicht aber zuverlässig erkennen.

Ein wichtiger Unterschied besteht jedoch: Die Kontrollroutine einer Software entfaltet – verglichen mit der inneren Einstellung eines einzelnen Sachbearbeiters – ungleich größere Breitenwirkung. Sie ist dazu konzipiert, Sachverhaltskonstellationen flächendeckend zu entscheiden. Das macht sie besonders sensibel und rechtlich kontrollbedürftig.

b) *Einordnung in die Handlungsformenlehre – Algorithmen als Verwaltungsvorschriften.* Aufgrund ihres Charakters als richtlinienähnliche interne Handlungsanweisung ist die Rechtsnatur algorithmischer Entscheidungssteuerungen strukturell mit derjenigen von Verwaltungsvorschriften vergleichbar. Diese helfen als Operationalisierungen abstrakt-genereller Regelungen dabei nachzuvollziehen, welche Gesichtspunkte die Entscheidung der Verwaltung steuern dürfen und nach welchen Leitlinien die Verwaltung Einzelfälle entscheidet. Insoweit gehen die normativen Funktionen von Verwaltungsvorschriften und im Risikomanagementsystem eingesetzter Algorithmen Hand in Hand: Beide Instrumente treffen abstrakte Verhaltensdirektiven für das behördliche Verfahren. Mit dieser Zielrichtung sorgen sie für *Nachvollziehbarkeit* und das erforderliche Maß an *Kontrolle* und *Gleichmäßigkeit* des Verwaltungsvollzugs.

2. Rechtliche Anforderungen an Selektionskriterien

Wenn ein Algorithmus seine Kontrolldichte bzw. -tiefe an statistischen Merkmalen ausrichtet und dadurch eine bestimmte Bevölkerungsgruppe stärker kontrolliert, entspricht dies zwar der Rationalität des Systems: Seine Aufgabe ist es, überprüfungsbedürftige Sachverhalte aus dem Datenstrom herauszufiltern. Die Rechtsordnung verlangt dem Inhaber der Kontrollmacht auch nicht ab, ein ineffizientes Kontrollsystem zu etablieren. Sie verbietet aber bewusst, bestimmte Merkmale zum Gegenstand einer Differenzierung zu erheben, selbst wenn stochastische Erkenntnisse sie als entscheidungsrelevant ausweisen; Diskriminierungsrisiken muss das System entgegenwirken (Art. 22 II Buchst. b iVm ErwGr 71 UAbs. 2 S. 1,[93] Art. 22 IV iVm Art. 9 II DSGVO[94] sowie Art. 21 I GrCh und Art. 3 III GG).[95] Die Rechtsordnung gewichtet insoweit die individuelle Entfaltung ohne Rücksicht auf angeborene oder im Laufe des Lebens erworbene Merkmale, die typischerweise mit einem Benachteiligungsrisiko verbunden sind, höher als den mit ihrer Berücksichtigung verbundenen potenziellen Effizienzgewinn einer behördlichen Kontrollroutine. Die dadurch entstehenden Effizienznachteile, Wohlfahrtsverluste und Missbrauchsmöglichkeiten nimmt das Recht bewusst in Kauf. Automatisierte Entscheidungssysteme stehen damit vor einer Herausforderung: Die Verwaltung muss sicherstellen, dass ihre Algorithmen entsprechend dem Gebot „privacy by design" (Art. 24 I, 25 II DSGVO) den Wertmaßstäben der Rechtsordnung genügen.[96]

Das jeweilige Diskriminierungsrisiko betrifft zwar vorrangig nicht die Verwaltungsentscheidung selbst,[97] sondern die Kontrollauswahl des (Risikomanagement-)Systems – und damit eine der Entscheidung vorgeschaltete Handlung. Auch vorbereitende Handlungen schlagen sich jedoch letztlich in der Entscheidung nieder: Steuert das System den Antrag einer Person (nur) aufgrund ihres Migrationshintergrunds zur besonderen Überprüfung aus, so ist diese Anknüpfung an das Merkmal „Herkunft" auch kausal für die Entscheidung. Eine Kontrolltätigkeit, welche nach Kriterien differenziert, die Art. 3 III GG bzw. Art. 21 I GrCh sowie Art. 22 IV iVm Art. 9 I DSGVO als Anknüpfungspunkt ausnehmen, gestattet die Rechtsordnung staatlichen Organen grundsätzlich nicht. So weit reicht „der lange Arm der Grundrechte" auch in entscheidungsvorbereitende Maßnahmen hinein.

3. Regulierungsstrategien im Umgang mit der Blackbox „Algorithmus"

a) *Offenlegung der eingesetzten Algorithmen?* Wer einer vollautomatisierten Einzelentscheidung ausgesetzt ist, kann Fehler des Entscheidungssystems, insbesondere Diskriminierungen, und sonstige Beeinträchtigungen seines Persönlichkeitsrechts nur schwer erkennen: Der Algorithmus ist für ihn eine Blackbox. Transparenz gehört aber zu den Grundprinzipien persönlichkeitsrechtsadäquater Datenverarbeitung (Art. 5 I Buchst. a DSGVO). Darin liegt auch der tiefere Grund, weshalb Art. 15 I Hs. 2 Buchst. h und Art. 13 II Buchst. f DSGVO Betroffenen Einblick in die „involvierte Logik" gewährt, also ein Recht auf Einsicht in die Bewertungsmaßstäbe verleiht.

Daraus erwächst eine Spannungslage:[98] Legt der Staat den Algorithmus offen, eröffnet er dadurch zugleich die Möglichkeit, dessen Schutzmechanismen zu unterwandern – etwa beim Steuerabzug für Spendenbeträge in vollautomatisierten Steuerverfahren: Grundsätzlich gewährt das System den steuerlichen Abzug von Spenden ohne nähere Prüfung. Ab einem bestimmten kritischen Betrag prüft es dann aber detailliert nach, um Missbräuche zu verhindern. Kennen Betroffene die Höhe dieses Schwellenwertes, können sie die Kontrollfunktionalität des Systems unterlaufen. Die AO verfügt daher, dass *Einzelheiten der Risikomanagementsysteme* nicht veröffentlicht werden dürfen, soweit dies die Gleichmäßigkeit und Gesetzmäßigkeit (Art. 3 I, Art. 20 III GG) der Besteuerung gefährden könnte (§ 88 V 4 AO).[99]

aa) *Reichweite und Grenzen von Informationsansprüchen.* Weder das Gebot der Transparenz (Art. 5 I Buchst. a DSGVO) noch die datenschutzrechtlichen Informationspflichten (Art. 15 I Hs. 2 Buchst. h; Art. 13 II Buchst. f DSGVO) verlangen die vollständige Offenlegung aller Entscheidungsmechanismen der öffentlichen Verwaltung. Es genügt, dass die Entscheidungs*prinzipien* und ihre Grundlagen (auch die Daten, die Eingang in die Entscheidung gefunden haben) als solche nachvollziehbar sind, damit der Betroffene

93 Vgl. oben II 1 a dd.
94 Siehe dazu II 1 c.
95 Mit Blick auf die Wesensgleichheit der Benachteiligungsstruktur gilt das nicht nur für unmittelbare, sondern auch für mittelbare Diskriminierungen – also solche Differenzierungen, welche nicht offen an eines der Merkmale anknüpfen, sich aber faktisch bei der Personengruppe auswirken, die an sich besonderen Diskriminierungsschutz genießt. Vgl. auch Art. 2 II Buchst. b RL 2000/43/EG sowie ErwGr 71 UAbs. 2 S. 1 DSGVO („zu diskriminierenden Wirkungen oder zu Maßnahmen, die eine solche Wirkung haben"); ausdrücklich für das Merkmal Geschlecht: *BVerfGE* 104, 373 (393); für Art. 21 GRCh *Jarass*, Charta der Grundrechte der Europäischen Union, 3. Aufl., 2016, Art. 21 Rn. 10 ff.; vgl. zu Art. 14 EMRK *EGMR*, Urt. v. 13.11.2007, 57325/00 D. H. u. a./Tschechien, NVwZ 2008, 533 (534, Rn. 175 ff.); vgl. auch *Payandeh*, JuS 2015, 695 (696 f.).
96 Ob eine Differenzierung dem System im Wege einer deterministischen Programmierung eingehaucht wird oder es sich diese Entscheidungsroutine als Teil maschinellen Lernens – etwa im Rahmen der Trainingsphase – selbst aneignet, bleibt insoweit ohne Unterschied.
97 Jede Diskriminierung setzt Entscheidungsspielräume voraus. Der Gesetzgeber lässt aber die vollständige Automatisierung jedenfalls in Verwaltungsverfahren des Allgemeinen Verwaltungsrechts bisher nur bei gebundenen Entscheidungen zu.
98 Vgl. zur Einsichtnahme in Score-Werte und in die Score-Formel *BGHZ* 200, 38 = NVwZ 2014, 747 (Score-Werte). Bei einem Algorithmeneinsatz durch Behörden tritt an die Stelle des Geschäftsgeheimnisses das Amtsgeheimnis.
99 Vgl. auch *Braun Binder*, Jusletter IT vom 25.5.2016, 1 (6); *Heintzen*, DÖV 2015, 780 (786 f.).

deren Richtigkeit nachvollziehen und überprüfen (lassen) kann.

Auch die Informationsfreiheitsgesetze des Bundes und der Länder gewähren keinen Anspruch auf Offenlegung aller Einzelheiten des Programmcodes. Sie sind zwar grundsätzlich tatbestandlich einschlägig: Die Funktionsweise des Verfahrensalgorithmus, der in eine automatisierte Entscheidung mündet, ist eine „amtliche Information" iSd § 2 Nr. 1 IFG Bund, die grundsätzlich einer Informationspflicht unterliegt.[100] Soweit das Bekanntwerden von Einzelheiten der Risikomanagementsysteme nachteilige Auswirkungen auf die Kontroll- oder Aufsichtsaufgaben der Finanzbehörden hätte (§ 3 Nr. 1 Buchst. d IFG), schließt das IFG des Bundes den Informationsanspruch jedoch – ähnlich wie die „Angstklausel" des § 88 V 4 AO („nicht veröffentlicht werden") – explizit aus.[101] Davon sind auch zuvor festgelegte Einzelheiten des Risikomanagementsystems umfasst.[102]

Der Ausnahmevorbehalt des § 3 Nr. 1 Buchst. d IFG erstreckt seine Geltung allerdings ausschließlich auf Finanzbehörden des *Bundes*.[103] Denn auf sie beschränkt sich der Anwendungsbereich des IFG Bund. Für die – im Falle von Steuererklärungen im Regelfall tätig werdenden – Finanzbehörden der *Länder* halten einige Landesgesetze[104] eine dem § 3 Nr. 1 Buchst. d IFG entsprechende Parallelnorm vor,[105] andere hingegen nicht.[106] Auch in denjenigen Ländern, die keinen spezifischen Ausnahmevorbehalt kennen, genießt das Veröffentlichungsverbot des § 88 III 3, V 4 AO jedoch Vorrang vor einem aus den Landesinformationsfreiheitsgesetzen abgeleiteten Zugangsanspruch. Denn die Informationsfreiheitsgesetze sind (gegenüber allen anderen Rechtsvorschriften) subsidiär.[107]

Im Ergebnis steht Betroffenen also weder ein Anspruch auf Offenlegung des Programmcodes[108] noch ein Rechtsbehelf unmittelbar gegen einen Algorithmus als solchen zur Seite. Vielmehr bleibt es bei den einfachen Informationspflichten der DSGVO und dem Gleichlauf mit Verwaltungsvorschriften:[109] (Nur) gegen die Einzelentscheidung selbst kann der Bürger wegen Ungleichbehandlung vorgehen (Art. 3 I GG).

bb) *Gesetzliche Operationalisierung der unionsrechtlichen Informationspflicht*. Die Pflicht, Betroffene über „das Bestehen einer automatisierten Entscheidungsfindung" sowie über die involvierte Logik der Entscheidungsalgorithmen zu informieren (Art. 13 II Buchst. f bzw. Art. 14 II Buchst. g DSGVO), lösen die Regelungen über das Besteuerungsverfahren bisher nicht selbst normativ ein. Die Tatsache, dass ihr Steuerbescheid vollständig anhand automatischer Datenverarbeitung erlassen wird, dürfte vielen Bürgern unbekannt sein. Den Finanzbehörden ist daher unionsrechtlich aufgegeben, die Steuerpflichtigen in hinreichendem Umfang – auch über die grundsätzliche Logik des Systems, insbesondere die zentralen entscheidungsleitenden Prinzipien – zu informieren, ohne dadurch jedoch die Funktionsweise des Systems selbst gefährden zu müssen. Der nationale Gesetzgeber muss insoweit freilich nicht zwingend tätig werden: Die Betroffenenrechte ergeben sich bereits unmittelbar aus Art. 12 ff. DSGVO.[110]

b) *Begründungspflicht*. Dem Blackbox-Charakter automatisierter Entscheidungen[111] kann eine Begründungspflicht entgegenwirken, die Betroffenen das Entscheidungsergebnis und seine Entstehung nachvollziehbar macht. Die DSGVO greift dieses Erfordernis in den Auskunft- und Informationspflichten[112] zwar nicht explizit auf. Sie geht aber davon aus, dass dem Betroffenen neben dem Recht auf „Einblick in die involvierte Logik" (Art. 15 I Hs. 2 Buchst. h und Art. 13 II Buchst. f DSGVO) ein „Recht auf Erläuterung" (ErwGr 71 UAbs. 1 S. 4) zukommt. Dieses gewährt die DSGVO allerdings nicht voraussetzungslos: Es bedarf einer Geltendmachung im Einzelfall.

Im deutschen Recht unterliegt die Verwaltung schon *de lege lata* der Pflicht, dem Adressaten die wesentlichen tatsächlichen und rechtlichen Gründe für einen erlassenen Verwaltungsakt mitzuteilen (§ 39 I 2 VwVfG). Von einer Begründung stellt das VwVfG die Verwaltung jedoch explizit dann frei, wenn diese den Verwaltungsakt „mit Hilfe automatischer Einrichtungen erlässt und die Begründung nach den Umständen nicht geboten ist" (§ 39 II Nr. 3 VwVfG). Darunter fallen im Grundsatz auch „vollständig durch automatische Einrichtungen" (§ 35 a VwVfG) erlassene Verwaltungsakte.

Aus der Einschränkung „nach den Umständen" lässt sich jedoch zugleich die normative Wertung ableiten, dass eine Begründung bei automatischen Erlassen nicht *generell* verzichtbar ist. Vielmehr sind die Spezifika des Einzelfalls maßgeblich. Als Gegengewicht zur grundsätzlich fehlenden Nachvollziehbarkeit der Entscheidung ist bei automatisierten Verwaltungsverfahren eine Begründung geboten und eine

100 Gesteht man dem Bürger einen entsprechenden Informationsanspruch zu, richtet er sich kumulativ auf zwei Aspekte: die zur Nachvollziehbarkeit des automatischen Verfahrens nötigen Informationen einerseits (das beinhaltet nicht zwingend den Quellcode des Algorithmus) und Auskünfte zur Funktionsweise des Risikomanagementsystems andererseits. Beschränkte man den Anspruch auf einen dieser beiden Aspekte, wäre es ihm im Grundsatz noch immer versagt, die konkrete Entscheidung nachzuvollziehen.

101 So für das Besteuerungsverfahren BT-Drs. 18/7457, 70; auf dem Gebiet der Auftragsverwaltung legen die obersten Finanzbehörden der Länder die Einzelheiten der Risikomanagementsysteme im Einvernehmen mit dem Bundesministerium der Finanzen fest (§ 88 V 5 AO).

102 Sofern diese Teile des Systems als Betriebs-, Geschäfts- oder Amtsgeheimnis geschützt sind, steht auch § 6 S. 2 IFG einem Informationsanspruch entgegen.

103 BT-Drs. 18/7457, 70.

104 Bis auf Bayern, Hessen, Niedersachsen und Sachsen kennen alle Bundesländer eigene Informationsfreiheits- bzw. Transparenzgesetze.

105 § 4 I Nr. 3 und 4 BWLIFG; § 3 Nr. 1 Buchst. b BremIFG; § 5 Nr. 4 HmbTG; § 14 I 2 Nr. 6 RhPfLTranspG; § 1 SaarlIFG iVm § 3 Nr. 1 Buchst. d IFG Bund; § 3 I Nr. 11 sowie Nr. 1 Buchst. c IZG LSA; § 7 I Nr. 5 ThürIFG.

106 Das BlnIFG hält in seinem § 7 lediglich einen besonderen Schutz von Geschäftsgeheimnissen vor; § 4 II Nr. 4 BbgAIG schließt einen Anspruch aus, „wenn die ordnungsgemäße Erfüllung der Aufgaben der öffentlichen Stelle erheblich beeinträchtigt würde"; auch das IFG M-V verankert keinen expliziten Schutz der Finanzbehörden, sondern lediglich einen allgemeinen „Schutz öffentlicher Belange" (§ 5) und einen „Schutz des behördlichen Entscheidungsprozesses" (§ 6); ähnlich auch das IFG NRW; § 9 IZG-SH schützt öffentliche Belange, erwähnt aber Finanzbehörden nicht explizit – anwendbar ist hier indes die allgemeine Ausnahme für „interne Mitteilungen der informationspflichtigen Stelle, die zum Schutz des behördlichen Entscheidungsprozesses erforderlich sind" (§ 9 II Nr. 2 IZG-SH).

107 § 1 III BWLIFG; § 1 Hs. 2 BbgAIG; § 1 III BremIFG; § 4 II 1 IFG NRW; § 1 S. 1 SaarlIFG iVm § 1 III IFG; offener § 1 III 1 IZG LSA; § 2 III RhPfLTranspG; § 4 II 1 ThürIFG. Manche Landesinformationsfreiheitsgesetze (namentlich § 3 III BlnIFG § 15 HmbTG; § 1 III 1 IFG M-V sowie § 3 S. 2 IZG-SH beschränken die Subsidiarität (entweder ausdrücklich oder nach dem Willen des Gesetzgebers) jedoch auf weitergehende Ansprüche. Ausschlusstatbestände sind davon also nicht umfasst.

108 Die Einsicht in den reinen Quellcode generiert den allermeisten Bürgern auch keinen Mehrwert. Vgl. zum Ganzen auch gerafft *Martini*, DÖV 2017, Heft 11, S. 15 des Typoskripts (im Erscheinen.)

109 Vgl. etwa *Schmitz* in *Stelkens/Bonk/Sachs*, VwVfG, 8. Aufl. 2014, § 1 Rn. 212.

110 Sofern die Voraussetzungen des Art. 23 I DSGVO im Einzelfall vorliegen, kann der Mitgliedstaat aber auch von einzelnen Informations- und Auskunftsrechten dispensieren, s. dazu bereits oben II 1 b bb.

111 Vgl. dazu etwa *Pasquale*, The Black Box Society, 2015, 140 ff. mit konkreten Beispielen und Vorschlägen zur Überwachung großer datenverarbeitender Unternehmen.

112 Siehe dazu oben II 1 b aa.

Befreiung von dem Gebot des § 39 I VwVfG (je nach Komplexitätsgrad und Diskriminierungsrisiko) grundsätzlich nicht gerechtfertigt.[113] Nur so kann die Norm auch ihrem allgemeinen rechtsstaatlichen Zweck gerecht werden, dem Betroffenen die Entscheidung nachvollziehbar darzulegen und Anhaltspunkte für eine Rechtmäßigkeitsprüfung zu verschaffen, der Behörde Selbstvergewisserung zu vermitteln sowie eine gerichtliche Überprüfung zu ermöglichen.[114]

Um dem Recht auf Erläuterung in der Sache gerecht zu werden, darf die Verwaltung auch nicht bei allgemeinen und pauschalen Erläuterungen stehen bleiben, sondern muss die entscheidungsleitenden Gesichtspunkte individuell benennen. Bei vollautomatisierten Verwaltungsverfahren ist es insbesondere denkbar, den Verfahrensschritt der Begründung bereits in den Algorithmus zu implementieren.[115] Zusätzlich zu den Entscheidungsprinzipien, also der grundsätzlichen Funktionsweise des Algorithmus, erfährt der Betroffene dann im Einzelfall (zumindest in den Grundzügen und in den Grenzen des Amtsgeheimnisses), wie es inhaltlich zu der Entscheidung kam und warum das automatische System gerade zu diesem und keinem anderen Ergebnis gekommen ist – im Idealfall durch Angabe abstrakter Zahlen zu Vergleichsgruppen, anhand derer der Betroffene nachvollziehen kann, warum der Algorithmus bei ihm diese und bei anderen jene Entscheidung getroffen hat.[116] Diskriminierungsrisiken lassen sich so bereits auf der Verfahrensebene eingrenzen.

c) *Externe Kontrolle der Algorithmen.* Kann der einzelne Bürger selbst die Entscheidungsstrukturen von Algorithmen nur eingeschränkt kontrollieren, ist umso mehr eine die Kontrolldefizite kompensierende externe Rechtmäßigkeitskontrolle angezeigt. Auf diese Weise lässt sich dem Blackbox-Charakter der eingesetzten proprietären technischen Verfahren grundsätzlich in einer Weise begegnen, die Transparenz und zu schützende Amtsgeheimnisse normativ austariert.

aa) *Präventive Prüfungs- und Zertifizierungspflicht.* Das persönlichkeitsrechtliche Gefährdungsrisiko automatisierter Verfahren indiziert, automatisierte algorithmische Systeme vor ihrem Einsatz in der Verwaltungspraxis einer Zertifizierungspflicht zu unterwerfen,[117] also eine Pflicht zur Kontrolle derjenigen Auswahlkriterien zu unterziehen, die sie dem Risikomanagementsystem unterlegen. Unabhängige Experten könnten die Entscheidungssysteme – ggf. in einem In-camera-Verfahren – anhand ausgewählter Testfälle gezielt auf diskriminierende Auswahlfaktoren überprüfen und zertifizieren.[118] Im Idealfall entwickelt sich daraus eine technisch-normative Standardisierung des Einsatzes der Automatisierungssoftware.

bb) *Nachträgliche, kontinuierliche Routinevalidierung insbesondere lernender Systeme.* Kommen bei automatisierten Verwaltungsverfahren Systeme maschinellen Lernens zur Anwendung, erweist sich deren Kontrolle als eine technisch anspruchsvolle, bislang noch nicht angemessen gelöste Herkulesaufgabe. Bei aller strukturellen Ähnlichkeit zu Verwaltungsvorschriften unterscheiden sich *lernende* Algorithmen von diesen nämlich in einem sensiblen Aspekt: Sie sind nicht deterministischer Natur, also nicht nach dem linearen Modell eines Zeilencodes programmiert, der ein fest gefügtes Schema abarbeitet. Vielmehr können sie ihr Entscheidungsverhalten nach zuvor nicht erkennbaren dynamischen Kriterien ändern: Sie entscheiden autonom, wie sie auf neue Situationen reagieren[119] – ihre Verfahrensweise ist ex ante nicht in jeder Hinsicht voraussehbar.[120] Sie verhalten sich wie Frankensteins Monster: Einmal in der Welt, weiß auch ihr Schöpfer nicht mehr, wie die unbelebte Materie in Zukunft agiert.[121] Änderungsbedingte Fehlentwicklungen lassen sich in einem solchen Modell nicht auf herkömmliche Weise überprüfen und unterbinden.[122] Einer Ex-ante-Kontrolle nach dem Muster einer normativen Richtigkeitskontrolle sind diese Systeme nach aktuellem Stand der Technik nur eingeschränkt zugänglich.[123]

Lernende Algorithmen gewähren zwar nur bedingt Einblick in ihren Verarbeitungsprozess. Sie sind aber einer Ergebnisanalyse zugänglich, die ihre tatsächlichen Wirkungen misst: Massendatenauswertungen können statistisch relevante Verarbeitungszusammenhänge eruieren und so einen Rückschluss auf möglicherweise diskriminierende Filterkriterien des Entscheidungssystems zulassen. Steuert ein Risikomanagementsystem bspw. in Steuerbetrugsverfahren signifikant mehr Menschen mit ausländischen Wurzeln zur menschlichen Überprüfung aus, kann dies womöglich auf diskriminierende Filterkriterien hindeuten, mit denen der Entscheidungsalgorithmus im Laufe der Zeit das – für die Entscheidung an sich irrelevante – Kriterium selbst zur Grundlage seiner Entscheidung gemacht hat.

Auf dieser Grundlage können sachverständige Experten – trotz aller damit verbundenen Schwierigkeiten – auch lernende Systeme mithilfe von Kontrollalgorithmen prüfen und automatisierte Verwaltungsvorgänge mittels Testverfahren daraufhin untersuchen, ob sich in dem Filterergebnis gruppenselektive Merkmale häufen, die für eine Entscheidung grundsätzlich nicht relevant sein dürfen. Programmierer können dann gezielt in die Systeme eingreifen und etwaige

113 Etwas anderes gilt nur dann, wenn die Behörde damit einem Antrag stattgibt und nicht in die Rechte eines anderen eingreift – § 39 II Nr. 1 VwVfG.

114 Gleiches gilt für das Gebot vorheriger Anhörung des § 28 I VwVfG. Die mit § 39 II Nr. 3 VwVfG nahezu wortlautidentische Ausnahme des § 28 II Nr. 4 VwVfG ist ebenso wie dort sehr restriktiv auszulegen. Denn gerade in diesen Fällen ist die Möglichkeit, Gehör zu finden, persönlichkeitsrechtlich indiziert. § 24 I 3 VwVfG trägt dem zu Recht Rechnung. Vgl. dazu auch III 3 a bb.

115 Das ist zumindest dann technisch möglich, wenn die – bislang nur gebundene Entscheidungen betreffenden – Algorithmen auf einem „Wenn-dann-Schema" beruhen und deshalb ohnedies die logisch schlüssigen Entscheidungsvariablen enthalten. Auf maschinelle Lernverfahren wie lernende Algorithmen oder neuronale Netze trifft das jedoch nicht in gleicher Weise zu, vgl. dazu auch Fn. 120.

116 Eine solche Zielsetzung legt ErwGr 71 UAbs. 1 S. 4 DSGVO jedenfalls bei weiter Auslegung nahe.

117 Vgl. insoweit auch die ausführliche Darstellung des Sachverständigen *Linus Neumann* zur Prüfung des von der Finanzverwaltung eingesetzten Risikomanagementsystems bei *Finanzausschuss des Bundestages*, Wortprotokoll der 75. Sitzung der 18. Wahlperiode, S. 25.

118 Vgl. auch (ohne Bezug zu Verwaltungsverfahren) *Geuter*, Machines Of Loving Grace / Brauchen wir einen Leinenzwang für Algorithmen?, Wired.de v. 11.6.2015; *Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz*, Verbraucherrecht 2.0, 7 f.; grundsätzlich *Hoffmann-Riem in Bora/Henkel/Reinhard*, Regulierungswissen in der Regulierung, 2014, 135 (148, 152).

119 Vgl. auch *Schmitz/Prell*, NVwZ 2016, 1273 (1277); *Stiemerling*, CR 2015, 762 (763 ff.). Zur Funktionsweise wissensbasierter Systeme, in denen Verfahren und Wissensbasis voneinander getrennt sind, *Ertel*, Grundkurs Künstliche Intelligenz, 4. Aufl. 2016, 20 ff.

120 Eine anschauliche Beschreibung der technischen Grundlagen neuronaler Netzwerke findet sich etwa bei *Honey*, Die Suche nach dem Babelfisch, Zeit Online v. 23.9.2016; *Schlieter*, Die Herrschaftsformel, 2015, 24 ff; vgl. auch *Schmidhuber*, Neural Networks 61 (2015), 85.

121 Ihr Vorzug besteht umgekehrt darin, „in zunächst unbekannten Umgebungen zu arbeiten und kompetenter zu werden, als [ihr] Ausgangswissen es erlauben würde", vgl. *Russell/Norvig*, Künstliche Intelligenz, 3. Aufl., 2012, 83.

122 Vgl. auch *Tutt*, Administrative Law Review 2016, 1 (12 ff.).

123 Zu den neuen Ansätzen der *Layer-wise Relevance Propagation*, um Entscheidungsmechanismen eines neuronalen Netzwerks nachzuverfolgen: *Beuth*, Die rätselhafte Gedankenwelt eines Computers, Zeit Online v. 24.3.2017 und aus technischer Sicht *Binder/Montavon* et al. in: *Wilson/Kim/Herlands*, Layer-wise Relevance Propagation for Neural Networks with Local Renormalization Layers, 2016, 1 ff.

diskriminierende Mechanismen identifizieren und ggf. korrigieren.

d) *Protokollierung und Beweissicherung.* Zum begleitenden Risikomanagement eines Systems automatisierter Entscheidung gehören eine umfangreiche Protokollierung und Beweissicherung der Programmabläufe.[124] Sie sind Teil der unionsrechtlichen Verpflichtung, ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Art. 30 DSGVO). Ob eine algorithmische Entscheidung diskriminierend ist oder anderweitig gegen Schutzgesetze verstößt, lässt sich insbesondere im Nachhinein nur dann valide feststellen, wenn Änderungen in den Entscheidungsprozessen (v. a. in Konfigurationen maschinellen Lernens) sowie die ihnen zugrunde liegenden Daten fälschungssicher und dauerhaft protokolliert sind.

e) *Abstufung nach Reversibilität.* Mit Blick auf die Risiken vollautomatisierter Verfahren kann es de lege ferenda sinnvoll sein, deren Zulässigkeit von ihrer Reversibilität abhängig zu machen: Vollautomatische Systeme sind zwar nicht generell fehleranfälliger als menschliche Amtsträger. Allerdings sind Algorithmen nur begrenzt in der Lage, die persönlichen Auswirkungen einer Entscheidung bzw. die weitere Entwicklung beim Betroffenen zu antizipieren. Empathie ist Systemen maschinellen Lernens (jedenfalls noch) nicht eigen.[125] Zumindest solche Entscheidungen, die nachhaltige, irreversible Folgen zeitigen (zB Entscheidungen, die in die körperliche Unversehrtheit Betroffener eingreifen oder Abrissverfügungen für ein Wohngebäude), ungebührliche Härten erzeugen oder dazu dienen, solche abzufedern bzw. zu vermeiden, sind Amtsträgern vorzubehalten. In anderen Fällen (zB bei nicht die Lebensgrundlage sichernden Geldzahlungen) ist eine Bearbeitung durch einen Menschen demgegenüber nicht zwingend geboten. In solchen Fällen ist es gerechtfertigt, den Betroffenen auf den (Vollzugs-)Folgenbeseitigungsanspruch sowie andere Ersatzansprüche zu verweisen.[126]

V. Fazit und Ausblick

Rechtlich klar eingehegt und mit Augenmaß eingesetzt, können automatisierte Verwaltungsentscheidungen sowohl Bürgern als auch der Verwaltung Nutzen spenden: Sie beschleunigen Verfahren und senken Bürokratiekosten. Nicht jedes Verfahren und jeder Sachgegenstand eignet sich freilich für eine vollständig maschinelle Abwicklung.[127] Auf absehbare Zeit kommen mit Blick auf den limitierten Erkenntnishorizont algorithmenbasierter Systeme nur gebundene Entscheidungen und standardisierte Verfahren in Betracht. Den Rahmen, dieses Potenzial auszuschöpfen, hat der nationale Gesetzgeber in § 35 a VwVfG, § 31 a SGB X sowie § 155 IV AO abgesteckt.

Automatisierte Verfahren sind für Betroffene regelmäßig eine intransparente „Blackbox". Sie stehen zu Grundprinzipien des Persönlichkeitsschutzes in einer spannungsreichen Beziehung. Betroffene sind deshalb auf angemessene Verfahrensgarantien angewiesen. Den normativen Maßstab dafür setzt in Zukunft nicht mehr vorrangig der nationale Gesetzgeber, sondern die Europäische Union. In ihren Art. 22 und 12 ff. sucht die DSGVO einen sachgerechten Ausgleich zwischen den kollidierenden Interessen: Sie spricht ein grundsätzliches Verbot automatisierter Entscheidung aus, gesteht den Mitgliedstaaten aber einen weiten nationalen Regelungsspielraum zu. Sie müssen als Teil eines Grundrechtsschutzes durch Verfahren Maßnahmen vorsehen, die Beeinträchtigungen für die Persönlichkeitsrechte des Betroffenen verhindern, wenn sie von dem grundsätzlichen Automatisierungsverbot dispensieren.

Wie der nationale Normgeber diese Anforderungen im Einzelnen zu erfüllen hat, gibt die Öffnungsklausel des Art. 22 II Buchst. b DSGVO nicht vor. Sie postuliert lediglich ein *Mindestmaß* an Garantien und Standards. Zu ihnen gehören als sachgerechte Bausteine insbesondere das Recht, ein persönliches (menschliches) Eingreifen verlangen zu dürfen, das Recht auf Darlegung des eigenen Standpunkts sowie auf Anfechtung der Entscheidung und damit korrespondierende Informationsrechte (vgl. auch Art. 22 III aE DSGVO) – ferner regelmäßige Stichproben von Menschenhand.[128] Auf ihrer Grundlage sowie anhand einer Zufallsauswahl des Systems[129] unterziehen Sachbearbeiter einzelne Fälle dann einer individuellen Prüfung. Auf diese Weise lassen sich die Wirksamkeit und Funktionsfähigkeit des automatischen Systems zumindest teilweise kontrollieren.

Risikomanagementsysteme, wie sie etwa bereits heute im Besteuerungsverfahren Einsatz finden, können dazu beitragen, die rechtlichen Steuerungsvorgaben für vollautomatisierte Entscheidungen einzuhalten – und zugleich Rechtssicherheit herstellen. Die Implementierung ebenso wie Kontrolle solcher Systeme ist als Teil eines wirksamen Persönlichkeitsschutzes auch unionsrechtlich zwingend geboten. Denn selbst wenn Algorithmen Irrationalitäten und (unbewusste) Einflüsse menschlicher Vorurteile vermeiden können, sind sie doch nicht fehler- und damit auch nicht diskriminierungsfrei. In ihrer Effizienzorientierung werden sie – etwa bei bestehenden stochastischen Korrelationen zwischen ethnischer Herkunft und dem Missbrauch von Leistungen – auch nach Kriterien selektieren, welche die unionsrechtlichen und nationalen normativen Wertentscheidungen für unzulässig erklären (Art. 22 IV iVm Art. 9 DSGVO; Art. 21 I GrCh, Art. 3 III GG).

Den spezifischen Diskriminierungsrisiken, die Algorithmen innewohnen, wirkt de lege ferenda nicht nur eine Pflicht zur Begründung automatisiert getroffener Entscheidungen entgegen, sondern auch die externe Kontrolle der Steuerungsmechanismen, denen Algorithmen als apokrypher Typ der Verwaltungsvorschrift unterliegen. Als Kontrollinstanzen empfehlen sich unabhängige Prüf- und Zertifizierungsstellen – mit Befugnissen sowohl ex ante (sub specie der Algorithmen selbst) als auch während des Betriebs (insbesondere im Wege einer Evidenzkontrolle durch Kontrollalgorithmen). Eine (nachträgliche) kontinuierliche Überprüfung des Systems in Gestalt einer Routinevalidierung fördert und kontrolliert die Diskriminierungsfreiheit, Stringenz und Transparenz des Verarbeitungsvorgangs. Dazu gehören als wichtige flankierende Bausteine auch eine Beweissicherung und Protokollierung, die Eingang in das Verzeichnis der Verarbeitungstätigkeiten iSd Art. 30 I DSGVO finden.

124 Vgl. auch *Schmitz/Prell*, NVwZ 2016, 1273 (1277).

125 Mithilfe künstlicher Intelligenz und entsprechend großen Lerndatenmengen kann eine Maschine „korrekte" Entscheidungen treffen, die ein Mensch genauso getroffen hätte. Dass sie die Folgen und Auswirkungen für das Leben des Betroffenen im Einzelfall antizipiert und bewertet, ist aber noch Zukunftsmusik.

126 Ist keine Folgenbeseitigung möglich, kommt ein Anspruch auf Entschädigung als Teil eines Amtshaftungsanspruchs (Art. 34 GG, § 839 BGB) in Betracht.

127 Sehr kritisch *Bull*, DVBl 2017, 409 (414 ff.), der auf die Besonderheiten der verschiedenen Verwaltungsaufgaben sowie auf die tatsächlichen Bedürfnisse der Bürger hinweist.

128 Dazu im Einzelnen II 1 a.

129 Vgl. für Risikomanagementsysteme im Besteuerungsverfahren *Finanzausschuss des Bundestages*, Wortprotokoll der 75. Sitzung der 18. Wahlperiode S. 23. Zu einem Beispielsfall fehlerhafter Ermessensausübung bei der Stichprobenerhebung der Statistischen Landesämter im Rahmen der Unternehmens-Dienstleistungsstatistik *BVerwG*, Urt. v. 15.3.2017 – 8 C 6/16.

Wenn IT-Visionäre Recht behalten, stehen wir am Beginn eines Maschinenzeitalters.[130] Die Welt der Score-Werte, die den E-Commerce längst erobert hat, macht auch vor dem öffentlichen Sektor nicht Halt. IBM hat bspw. eine Software entwickelt, die den Anspruch erhebt, auf der Grundlage von Algorithmen zu berechnen, ob ein Einreisender Verbindungen zu Terrororganisationen etc hat oder anerkennungsfähiger Flüchtling ist – eine umfassende Datenanalyse mündet in einen Risiko-Score.[131] So sehr solche algorithmenbasierten Entscheidungsparameter auch das menschliche Grundbedürfnis befriedigen, komplexe Sachverhalte auf klare und einfache Maßgaben herunterzubrechen: Den Menschen und seinen Lebenssachverhalt nicht auf eine reine Zahlenlogik zu reduzieren, gehört auch und gerade in der digitalen Welt zu den vornehmsten Aufgaben eines freiheitlichen Rechtsstaats.

130 Vgl. statt vieler *Ertel*, Grundkurs Künstliche Intelligenz, 12.
131 Vgl. *Lobe*, Ist das ein Flüchtling oder ein Terrorist?, FAZ v. 17.2.2016, 13.