Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?

Potenziale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen

von Stephan Dreyer und Wolfgang Schulz

Impressum
© April 2018 Bertelsmann Stiftung
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Verantwortlich
Konrad Lischka
Ralph Müller-Eiselt

Autoren
Stephan Dreyer, Wolfgang Schulz

DOI 10.11586/2018011 https://doi.org/10.11586/2018011

Inhalt

Vorwort

Datenschutz schützt nicht vor allem. Dass Daten datenschutzkonform verarbeitet werden, garantiert nicht die Qualität der Schlussfolgerungen, die Software aus diesen Daten ableitet. Wenn algorithmische Systeme Datenmengen auswerten, birgt nicht nur die Verarbeitung an sich Risiken. Es sind vor allem die Empfehlungen und Entscheidungen von Software, die eine Gefahr für Teilhabe darstellen und sich sowohl auf Einzelne als auch auf soziale Gruppen oder die ganze Gesellschaft auswirken können.

Ein Beispiel: In den USA und Großbritannien werden bis zu 70 Prozent der Bewerber automatisiert von algorithmischen Entscheidungssystemen bewertet und vorausgewählt, bevor ein Recruiter sich die verbliebenen Kandidaten ansieht. Auch in Deutschland setzen erste Unternehmen solche automatisierten Verfahren ein. Vieles spricht dafür, dass diese sich schnell verbreiten werden. Denn sie haben gegenüber menschlichen Entscheidern den Vorteil, dass sie eine Entscheidungslogik konsistent auf alle Fälle anwenden und keinen subjektiven Verzerrungen unterliegen. Wo Menschen sich zum Beispiel (mindestens unterbewusst) vom Namen oder Foto eines Bewerbers beeinflussen lassen, bleibt Software neutral.

Algorithmische Systeme können jedoch genauso gut konsistent diskriminieren. Das Wall Street Journal berichtet von Kyle Behm, einem Studenten, der an einer bipolaren Störung leidet. Er bewarb sich um Aushilfsjobs im Einzelhandel und wurde trotz ausgezeichneter Zeugnisse und Referenzen von mehreren Firmen nicht einmal zum Vorstellungsgespräch eingeladen. Von einem Freund, der bei einem der Unternehmen arbeitete, erfuhr er, dass er Opfer des psychologischen Tests in der Onlinebewerbung geworden war. Die Software hatte seine Bewerbung bei allen Unternehmen aussortiert. Kyle und anderen Bewerbern mit psychischen Erkrankungen blieb so der Zugang zum Arbeitsmarkt verwehrt.

Anders als Kyle erfahren die meisten Bewerber nicht einmal, warum sie abgewiesen wurden. Noch seltener tun sie etwas dagegen. Wenn aber Betroffene automatisierte Entscheidungen nicht verstehen und es keine Beschwerden gibt, können Diskriminierungen Einzelner oder ganzer Gruppen nicht aufgedeckt werden.

Deshalb müssen algorithmische Systeme, die Menschen bewerten, für den Einzelnen nachvollziehbar und auf systematische Fehler überprüfbar sein. Kann Datenschutz, vor allem die neue EU-Datenschutz-Grundverordnung (DSGVO), dazu beitragen? Wenn die neue Verordnung am 25. Mai 2018 wirksam wird, ist das ein wichtiger Schritt für eine europaweite Datenschutzharmonisierung und für mehr Betroffenenrechte. Ob das auch in Bezug auf automatisierte Entscheidungen durch Software und algorithmische Systeme gilt, ergründet das vorliegende Gutachten.

Wolfgang Schulz und Stephan Dreyer setzen sich im Detail mit den entsprechenden Artikeln der DSGVO auseinander und analysieren, ob die neue Verordnung eine bessere Nachvollziehbarkeit und Überprüfbarkeit algorithmischer Entscheidungssysteme fördern kann. Sie prüfen, inwiefern damit einerseits individuelle Interessen wie Persönlichkeitsrechte und andererseits gesellschaftliche Ziele wie Nichtdiskriminierung und Teilhabe abgesichert werden können. Darüber hinaus skizzieren sie mögliche Erweiterungen der DSGVO sowie alternative Steuerungsinstrumente, die die Verordnung ergänzen könnten. Solche zusätzlichen Ansätze sind für algorithmische Systeme notwendig. Denn die Verordnung hat einen eingeschränkten Geltungsbereich und ist durch ihren Fokus auf Individualrechte nicht umfassend in der Lage, gruppen- und gesellschaftsbezogene Werte wie etwa Nichtdiskriminierung zu sichern. Um die Möglichkeiten im Rahmen der DSGVO dahingehend zu erweitern, kommt es vor allem auf eine aktive Datenschutzaufsicht an, die auch die gesellschaftlichen Risiken von ADM-Systemen in den Blick nimmt. Außerhalb der DSGVO bedarf es zudem weiterer Ansätze, die eine tiefer gehende Überprüfbarkeit und Korrigierbarkeit von automatisierten Entscheidungen sicherstellen. Neben verschiedener Möglichkeiten zur Überprüfbarkeit algorithmischer Systeme durch unabhängige Dritte bietet auch das Verbraucherschutzrecht dafür Ansatzpunkte.

Wir veröffentlichen das vorliegende Gutachten als Arbeitspapier, um einen Beitrag zu einem sich schnell entwickelnden Feld zu geben, auf dem auch andere aufbauen können. Wir freuen uns über Erweiterungen, Verbesserungen und natürlich auch konstruktive Kritik. Um einen solchen Diskurs zu erleichtern, veröffentlichen wir das Arbeitspapier unter einer freien Lizenz (CC BY-SA 3.0 DE).

Die Analyse von Wolfgang Schulz und Stephan Dreyer ist Teil des Projekts „Ethik der Algorithmen“, in dem sich die Bertelsmann Stiftung näher mit den gesellschaftlichen Auswirkungen algorithmischer Entscheidungssysteme beschäftigt. Bislang sind in der Reihe „Impulse Algorithmenethik“ eine Sammlung internationaler Fallbeispiele (Lischka und Klingel 2017), eine Untersuchung des Wirkungspotenzials algorithmischer Entscheidungsfindung auf Teilhabe (Vieth und Wagner 2017), eine Analyse des Einflusses algorithmischer Prozesse auf den gesellschaftlichen Diskurs (Lischka und Stöcker 2017) sowie eine Papier zu Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung (Zweig 2018) erschienen.

Ralph Müller-Eiselt
Senior Expert
Taskforce Digitalisierung
Bertelsmann Stiftung

Konrad Lischka
Project Manager
Projekt Ethik der Algorithmen
Bertelsmann Stiftung

Zusammenfassung

In Verfahren algorithmischer Entscheidungsfindung (Algorithmic Decision Making, kurz: ADM-Systeme) bewerten Maschinen Menschen und fällen auf dieser Grundlage eine Entscheidung oder geben eine Prognose oder Handlungsempfehlung ab. Damit birgt nicht die Datenverarbeitung an sich, sondern vor allem die Entscheidung als Konsequenz der Verarbeitung *Risiken* für die Nutzer. Zum einen für Individualrechte, wie informationelle Selbstbestimmung aus dem unmittelbaren Schutzbereich des Datenschutzes, für Persönlichkeitsrechte und individuelle Autonomie. Zum anderen für gruppen- und gesellschaftsbezogene Interessen wie Fairness, Nichtdiskriminierung, soziale Teilhabe und Pluralismus.

Um diese Ziele zu sichern, schlagen Experten *Maßnahmen* vor, mit denen die Verfahren transparent, Einzelentscheidungen erklärbar und revidierbar sowie die Systeme überprüfbar und korrigierbar gemacht werden können. Zudem kann Vielfaltssicherung von ADM-Systemen dazu beitragen, die genannten Interessen zu gewährleisten.

Vor diesem Hintergrund geht das vorliegende Gutachten folgender *Frage* nach: Inwiefern können die ab Mai 2018 geltende EU-Datenschutz-Grundverordnung (DSGVO) und das zeitgleich in Kraft tretende neue Bundesdatenschutzgesetz (BDSG) solche Maßnahmen unterstützen und die durch algorithmische Systeme bedrohten Interessen schützen? Die Analyse macht deutlich: Der Handlungsspielraum der DSGVO insgesamt ist in Bezug auf ADM-Systeme stark eingeschränkt. In den wenigen Anwendungsfällen kann die Verordnung Transparenz und Überprüfbarkeit teilweise herstellen und damit helfen, individuelle Rechte abzusichern. Für gruppen- und gesellschaftsbezogene Ziele wie Nichtdiskriminierung und Teilhabe bietet die DGSVO jedoch kaum Ansatzpunkte. Deshalb bedarf es hier der Diskussion ergänzender Steuerungsansätze auch außerhalb der DSGVO.

Im Einzelnen zeigt die vorliegende Analyse, dass die *Anwendung der DSGVO* auf ADM-Systeme aus mehreren Gründen *eng begrenzt* ist: Die DSGVO verbietet nur vollständig automatisierte Entscheidungen; weiterhin zulässig sind Systeme, die menschliche Entscheidungen vorbereiten und Empfehlungen geben. Damit das Verbot greift, müssen ADM-Systeme eine Entscheidung vollautomatisch auf Grundlage von personenbezogen Daten treffen und die Entscheidung muss rechtliche Relevanz entfalten oder die betroffene Person in anderer Weise erheblich beeinträchtigen. Ist eines dieser drei Kriterien nicht erfüllt, finden die ADM-spezifischen Vorgaben der DSGVO keine Anwendung. Es bleibt allerdings unklar, ab wann bei ADM-Systemen bereits von einer „Entscheidung“ gesprochen werden kann und wann sich eine solche „rechtliche Relevanz“ entfaltet. Auch kann die Regelung kaum die Vielfältigkeit von faktischen Entscheidungssituationen umfassen, in denen Menschen bewusst oder unbewusst eine automatisierte Entscheidung oder Entscheidungsempfehlung unhinterfragt umsetzen. Sowohl der relativ enge Anwendungsbereich des Verbots als auch die breiten gesetzlichen Verbotsausnahmen – allem voran durch eine Einwilligung des Betroffenen – führen letztlich zu wenigen Anwendungsfällen, in denen ein ADM-System tatsächlich unzulässig wäre. *(Teil-)Automatisierte Entscheidungen* werden in unserem Alltag also *gängige Praxis* werden.

Für alle „ausnahmsweise“ zulässigen ADM-Systeme bietet die DSGVO rechtliche Regelungen, die in Teilen geeignet sind, um vor allem *individuelle Interessen der Nutzer abzusichern*: Die datenschutzrechtlich Verantwortlichen von ADM-Systemen müssen gegenüber dem Nutzer *Informations- und Transparenzpflichten* über den Einsatz eines ADM-Systems sowie die grundlegenden Mechanismen der Datenverarbeitung und Entscheidung einhalten. Umfang und Tiefe der Informationspflichten sind jedoch begrenzt. Es ist auch unklar, was mit dem Wortlaut „involvierte Logik“ genau gemeint ist. Zudem ist die Regelung auf den Individualdatenschutz bezogen. Deshalb richtet sich die Erklärung über die „Tragweite und die angestrebten Auswirkungen“ der ADM-Entscheidung in ihrer Tiefe und Verständlichkeit am durchschnittlichen Nutzer aus. Aus einer Transparenz für Betroffene folgt jedoch nicht automatisch ein höherer Grundrechtsschutz in der Praxis.

Bei einer automatisierten Entscheidung haben Betroffene einen *Anspruch auf Auskunft* über den Einsatz eines ADM-Systems sowie die grundlegenden Mechanismen der Datenverarbeitung und Entscheidung. Außerdem haben sie das Recht, einen menschlichen Entscheider hinzuzuziehen. Auch diese Rechte helfen, individuelle Schutzinteressen zu sichern. Sie ermöglichen es, eine automatisierte Entscheidung zu überprüfen und ggf. zu korrigieren. Ein Anspruch auf Einsicht in das System durch Betroffene selbst oder unabhängige Dritte entsteht dadurch jedoch nicht.

System- und prozessbezogene Vorgaben der DSGVO zu Konzeption und Einsatz von ADM-Systemen sind geeignet, um auf Verantwortlichenseite Risiken für den Einzelnen (und indirekt auch für Personengruppen) frühzeitig zu erkennen und Mindestqualitätsstandards zu sichern. Dazu zählen vor allem Privacy by Design, verpflichtende datenschutzrechtliche Folgeabschätzungen und interne Datenschutzvorschriften sowie die Bestellung eines Datenschutzbeauftragten. Diese Regelungsinstrumente haben das Potenzial, bei den Verantwortlichen für ein hohes Reflexionsniveau in datenschutzrechtlichen Belangen zu sorgen und so mindestens individuelle Rechte und Freiheiten zu gewährleisten.

Die genannten Anbieterpflichten können theoretisch noch durch die *Datenschutzaufsicht* verstärkt werden, die über umfassende Auskunfts- und Zutrittsbefugnisse verfügt. Sie kann Prozesse und Folgeabschätzungen im Rahmen einer Datenschutzprüfung einsehen. Ziel dieser Prüfungen ist jedoch wiederum nur der Schutz individueller Rechte.

Für die *Absicherung von gruppen- und gesellschaftsbezogenen Schutzinteressen* wie Nichtdiskriminierung, Teilhabe oder Pluralismus bietet die DSGVO hingegen kaum Potenzial. Voraussetzung dafür wäre eine externe Einsichtnahme in die Interna der ADM-Systeme, um die zugrunde liegenden Konzepte und Prozesse unabhängig überprüfen zu können. Für einen solch tiefen Einblick in das System reichen die DSGVO-Transparenzvorgaben jedoch nicht aus. Fehler bei der Operationalisierung oder Datenauswahl und soziale Wechselwirkungen können deshalb nicht aufgedeckt werden. Auch ein Überblick über die in der Praxis vorherrschende Vielfalt von ADM-Systemen wird durch die fehlende Systemtransparenz erschwert.

Um gruppen- und gesellschaftsbezogene Interessen zu schützen und die dafür notwendige Systemtransparenz und externe Überprüfbarkeit zu verbessern, braucht es *ergänzende Ansätze*. Dazu können bestimmte Ansatzpunkte *innerhalb der DSGVO* gestärkt werden, die vor allem präventiv wirksam werden können. So könnten die Datenschutzbehörden Datenschutzfolgeabschätzungen auch für von der DSGVO ausgenommene ADM-Systeme festlegen. So ließen sich Risiken frühzeitig identifizieren und Mindeststandards garantieren. Zudem könnte im Rahmen der DGSVO die Rolle der Aufsichtsbehörden in der Praxis stärker in Richtung der Aufklärung der Öffentlichkeit und der Sensibilisierung für gesellschaftliche Missstände geführt werden, auch wenn diese keine Durchsetzungsbefugnisse außerhalb von Datenschutzverstößen haben.

Es müssen jedoch über die DGSVO hinaus *weitere Steuerungsinstrumente* diskutiert werden, um überindividuelle und gesellschaftliche Ziele tatsächlich absichern zu können. Zu einer besseren Überprüfbarkeit von ADM-Systemen können Ansätze beitragen, die die Erklärbarkeit der Systeme erhöhen. Wenn die Systeme bereits im Einsatz sind, können erweiterte Transparenzvorgaben die Überprüfung durch externe Dritte gewährleisten, etwa in Form von „in camera“-Verfahren, die die Geheimhaltungsinteressen der Anbieter wahren. Für die Korrigierbarkeit von bereits eingesetzten ADM-Systemen wären Steuerungselemente aus dem Wettbewerbs- und Verbraucherschutzrecht denkbar, die eine schnellere Rechtsdurchsetzung ermöglichen. Vielfalt von ADM-Systemen kann durch Übernahme kartellrechtlicher Regelungsinstrumente unterstützt werden. Auch medienrechtliche Regelungen können zu Pluralismus bei ADM-Systemen beitragen, die Informationsflüsse steuern und die Meinungsbildung beeinflussen. Auf diese Weise sind alternative Steuerungsansätze in der Lage, überindividuelle Interessen zu schützen, die die vor allem auf die Sicherung individueller Interessen ausgerichtete DSGVO nicht abdeckt.

Executive summary

In algorithmic decision-making systems (ADM systems) machines evaluate and assess human beings and, on this basis, make a decision or provide a forecast or a recommendation for action. Thus not only the data processing as such, but above all the decision that results from the processing contains *risks* for the user. On the one hand there are individual rights such as informational self-determination as the scope of protection directly covered by data protection, personality rights and individual autonomy. On the other hand there are group-related and societal interests such as fairness, non-discrimination, social participation and pluralism.

In order to attain these goals, experts have suggested the adoption of certain *measures* which contribute to making ADM procedures transparent, individual decisions explainable and revisable, as well as to making the systems verifiable and rectifiable. Furthermore, ensuring the diversity of ADM systems can make a contribution to safeguarding the mentioned interests.

Against this background the present report focuses on the following *question*: To what extent can the EU General Data Protection Regulation (GDPR), which applies from May 2018, and the new German Federal Data Protection Act (BDSG), which enters into force at the same time, support such measures and protect the interests threatened by algorithmic systems. The analysis demonstrates that the GDPR's room for manoeuvre in the area of ADM systems is quite restricted. In the few cases the regulation applies to it can to some extent create transparency and verifiability and thus help to safeguard individual rights. However, regarding group-related and societal goals such as non-discrimination and participation the GDPR has little to offer. For this reason there is a need to discuss complementary regulatory tools beyond the GDPR.

The present analysis gives a detailed account of why the *application of the GDPR* to ADM systems, for a variety of reasons, is *closely restricted*. The GDPR prohibits only fully automated decision-making. Systems which prepare the basis for human decisions and give recommendations may still be used. For the prohibition to come into effect, ADM systems must make fully automated decisions on the basis of personal data, plus the decisions must have legal consequences or similarly affecting the data subject significantly. If one of these three criteria is missing, the ADM-specific provisions of the GDPR do not apply. However, it is unclear in the case of ADM systems what a "decision" actually is, and under what circumstances it produces "legal effects". Moreover, the regulation can hardly encompass the diversity of actual decision-making situations in which people consciously or unconsciously implement an automated decision or recommendation unquestioningly. Both the relatively narrow scope of application of the prohibition and the broad range of legal exceptions to the prohibition - first and foremost by consent given by the data subject – result in very limited cases in which an ADM system is actually prohibited. Thus *(partly) automated decisions* are going to become a *normal part of our everyday lives*.

For ADM systems that are "exceptionally" permissible under the GDPR the regulation contains legal provisions which can partly safeguard the *individual interests of the users*. Data controllers of ADM systems are subject to *transparency and information obligations* relating to the use of ADM systems in general as well as to the basic mechanisms of data processing and decision-making. However, the scope and depth of such transparency obligations are limited. It also remains unclear what the notion of "logic involved" actually means. Moreover, the regulation focuses on the data protection of the individual. For this reason the scope and comprehensibility of the explanation of the "significance and the envisaged consequences" of the ADM decision is based on and limited by the perspective and cognitive skills of the average user. However, transparency provisions aiming at data subjects do not automatically lead to higher levels of basic rights protection in practical terms.

Regarding ADM systems data subjects have a *right to disclosure* about the use of an ADM system in general as well as regarding the basic mechanisms of data processing and decision-making. Furthermore, they have the right to obtain human intervention. These rights, too, help to safeguard individual rights and freedoms. They make

it possible to verify and – if needed – to overrule the automated decision. However, this does not constitute a right for data subjects or for independent third parties to scrutinize the whole system.

Systemic and procedural GDPR provisions regarding the design and implementation of ADM systems can help the data controller to detect risks for the individual (and indirectly for groups) at an early stage and to ensure minimum quality standards. These include privacy by design obligations, obligatory data protection impact assessments and binding corporate rules, as well as the appointment of a data protection officer. These regulatory tools have the potential to create a high level of awareness with the data controller regarding data protection issues, and thus helping to safeguard individual rights and freedoms.

These controller-related duties can in theory be strengthened by the *data protection authorities*, who are granted encompassing disclosure and access rights. They can scrutinize ADM processes and carry out impact assessments during data protection audits. However, the focus of these audits is only the protection of individual rights, once again.

Yet the GDPR does not offer great potential when it comes to protecting *group-related and societal interests* such as non-discrimination, participation or pluralism. A prerequisite for this would be the option for an external inspection of the internal design of the ADM systems in order to be able to evaluate independently its basic concepts and processes. However, the GDPR transparency rules cannot facilitate such a deep insight into the system. Thus it is not possible to uncover errors or misconceptions in the development and implementation of ADM systems as well as their potential effects on social interactions. Moreover, an overview over the actual diversity of ADM systems is difficult to acquire against the background of system-related intransparency.

In order to protect group-related and societal interests as well as to improve system-related transparency and external evaluation, there is a need for *complementary approaches*. For this purpose certain measures *within the GDPR* can be strengthened. For example, the data protection authorities could also ask for data protection impact assessments for all cases of ADM systems, including those that are not covered by Art. 22 GDPR. This would make it possible to identify risks at an early stage and to guarantee minimum protection standards. Furthermore, within the framework of the GDPR the role of the data protection authorities could shift towards more public information and awareness building regarding potential societal problems, even if the authorities do not have enforcement powers that go beyond dealing with data protection infringements.

However, beyond the scope of GDPR *other regulatory tools* in practice have to be discussed in order to be able to safeguard both supraindividual and societal goals. In order to improve the inspection of ADM systems, certain approaches can contribute to the greater explainability of the systems. In case such systems are already in use, enhanced transparency requirements could provide for better external assessment, e.g. in the form of in-camera proceedings that protect the interests and confidentiality of the data controller. In order to rectify ADM systems already implemented, it seems possible to use regulatory tools from competition law and consumer protection law, since they might result in faster forms of enforcement. The diversity of ADM systems can be supported by adopting regulatory tools provided by cartel law. Furthermore, media law requirements could contribute to pluralism in the case of ADM systems that have an effect on information access and that influence public opinion formation. This way, alternative regulatory approaches can protect supraindividual interests that the GDPR does not cover, since it focuses primarily on safeguarding individual rights and freedoms.

1 Einleitung[1]

Softwaresysteme, die Menschen bewerten und algorithmenbasiert Entscheidungen treffen (Algorithmic Decision Making Systems, kurz: ADM-Systeme), geraten aufgrund der möglichen Konsequenzen ihrer Entscheidungen für den Einzelnen, für Gruppen und für die Gesellschaft als Ganzes zunehmend in den Blick von Politik, Recht und Ethik. Die Bertelsmann Stiftung hat in mehreren Publikationen und Veranstaltungen mögliche durch ADM-Systeme hervorgerufene oder verstärkte Problemlagen und Risiken identifiziert, die Einfluss auf individuelle und gesellschaftliche Zielwerte haben, und als Reaktion darauf dezidierte mögliche Gegenmaßnahmen entwickelt (Bertelsmann-Stiftung 2017a). Mit der ab dem 25. Mai 2018 unmittelbar anzuwendenden EU-Datenschutz-Grundverordnung (DSGVO)[2] und der zeitgleich in Kraft tretenden Novellierung des Bundesdatenschutzgesetzes (BDSG n.F.)[3] gelten neue datenschutzrechtliche Vorgaben, die auch spezifische Vorschriften für die Verarbeitung personenbezogener Daten im Rahmen automatisierter Entscheidungen enthalten. Das Gutachten untersucht vor diesem Hintergrund, inwieweit die Vorgaben aus DSGVO und BDSG n.F. eine Grundlage für Maßnahmen zur Minimierung der mit ADM-Systemen verbundenen Risiken und zur Sicherung individueller sowie gruppen- und gesellschaftsbezogener Interessen bieten können und ob ggf. weitere Regelungen im Datenschutzrecht oder in anderen Rechtsbereichen nötig und hilfreich erscheinen.

Das Kurzgutachten ist dabei in mehrere Schritte untergliedert: In Kapitel 2 werden die identifizierten individuellen, gruppenbezogenen und gesellschaftlichen Risiken von ADM-Systemen in verdichteter Form dar- und Maßnahmen zur Interessensicherung vorgestellt. In Kapitel 3 zeigt das Gutachten die für ADM-Systeme geltenden Vorgaben in DSGVO und BDSG n.F. und die sich daraus ergebenden zielwertsichernden Maßnahmen auf. Vor dem Hintergrund der Handlungsbedarfe wird der Rechtsrahmen im Kapitel 4 daraufhin untersucht, ob und inwieweit die Datenschutznormen in der Lage sind, geeignete Instrumente zur Verfügung zu stellen und so Risikopotenziale für den Einzelnen, für Gruppen und für die Gesellschaft zu verringern. In der weiteren Analyse identifiziert Kapitel 5 ADM-bezogene Problemlagen, auf die DSGVO und BDSG derzeit nicht reagieren. Das Gutachten schließt mit einem Ausblick auf alternative Steuerungsansätze und -instrumente innerhalb (Kapitel 6) und außerhalb (Kapitel 7) des datenschutzrechtlichen Rahmens, die auf die offenbleibenden Bedarfe reagieren könnten.

[1] Für die Mitarbeit an der Expertise danken wir Florian Wittner, Florian Riebe, Sonja Lübeck, Lumnie Izeti und Johanna Stelling.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EG Nr. L 119 v. 4.5.2016: 1–88.

[3] BDSG i. d. F. des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU v. 30.6.2017, BGBl I: 2097).

2 Risikopotenziale von ADM-Systemen und Gegenmaßnahmen zur Absicherung von individuellen, gruppen- und gesellschaftsbezogenen Interessen

Automatisierte Entscheidungen bergen für den Einzelnen und die Gesellschaft viele Chancen. Allein die derzeit erprobten Verfahren in der automatisierten medizinischen Diagnostik bei bildgebenden Verfahren zeigen unmittelbar das positive Potenzial automatischer Analyseverfahren. Ähnliches ist für den Einsatz im Bereich des Umweltschutzes beobachtbar, etwa im Bereich des Wasserqualitäts- und Wasserspeichermanagements sowie der Flut- oder Luftverschmutzungsvorhersage. Soweit es um Regelungsstrukturen in Bereichen automatisierter Entscheidungen geht, liegt der Fokus von Recht und Politik aber vor allem auf möglichen Gefährdungen für Rechtsgüter und -interessen, deren Realisierung durch gesetzliche Vorschriften möglichst ausgeschlossen werden soll. Die hier erfolgende Zusammenschau der in der rechtswissenschaftlichen und gesellschaftlichen Debatte vorgebrachten Aspekte und Überlegungen zu ADM-Systemen fokussieren entsprechend in erster Linie auf solche Gefährdungen und Risiken für individuelle Rechte und Freiheiten sowie gruppenbezogene und gesellschaftsbezogene Zielwerte.

Risiken können in allen Phasen des Prozesses auftauchen, in dem ADM-Systeme entwickelt und in einen gesellschaftlichen Kontext eingebettet werden (vgl. dazu auch Zweig 2018). In der Konzeptionsphase können Risiken in Form einer Fehlauswahl eines konkreten analytischen Konzepts bzw. eines bestimmten mathematischen Modells sowie der Daten(vor)selektion vor dem Hintergrund der zu lösenden Aufgabe auftreten.

- Risiken können sich dabei aus der falschen oder jedenfalls für das zu lösende Problem nicht adäquaten Operationalisierung sozialer Phänomene und Konzepte im Ansatz ergeben. Maßnahmen, die die gewählten Konzepte und angelegten Kriterien transparent machen und eine passendere Operationalisierung finden, können dem entgegenwirken.
- Die Ex-ante-Einschätzung der gesellschaftlichen und sozialen Folgen des ADM-Systemeinsatzes kann von Fehlprognosen geprägt sein. Nachträgliche Evaluationen im Sinne einer inhaltlichen Überprüfbarkeit können Fehleinschätzungen aufzeigen.
- Eine mögliche Nutzung in anderen – grundrechtsrelevanten – Einsatzgebieten als bei der Programmierung beabsichtigt kann derartige Ex-ante-Einschätzungen zudem obsolet werden lassen. Folgeabschätzungen sollten deshalb bei jedem Einsatz eines Algorithmus in unterschiedlichen Anwendungsbereichen erneut durchgeführt werden.
- Das Risiko, dass sich die Konzeptionslogik zu sehr auf ökonomische kurzfristige Effizienzgewinne stützt und die gesamtsoziale Angemessenheit des Systems dadurch in den Hintergrund gerät, kann durch die Berücksichtigung gemeinwohlbezogener Interessen im Rahmen von Entwicklungsprozessen wie der Identifikation einer geeigneten Wirkungslogik begrenzt werden.

Im weiteren Prozess wird das System in einen gesellschaftlichen Kontext eingebettet (Implementationsphase). Dabei ergeben sich Risiken, wenn das einmal entwickelte System in der Praxis eingesetzt wird. Erst hier wirken sich die ggf. vorab selektierten Trainingsdaten und das auf Grundlage dieser Daten trainierte System im Einsatz unter Realbedingungen aus.

- Beim Einsatz eines ADM-Systems kann es zu selbstverstärkenden Rückkopplungen kommen, bei denen eine bereits in den selektierten Daten angelegte Verzerrung („Bias“) verstärkt wird. Solche algorithmischen Biaskaskaden ergeben sich aus dem Zusammenspiel von Datenselektion und auf dieser Datengrundlage lernenden Systemen. Als Begegnungsmöglichkeit dieser Risiken werden die Sicherstellung der Falsifizierbarkeit der Systementscheidung, d. h. der Möglichkeit einer Entscheidungsüberprüfung und -korrektur durch einen Menschen, sowie die kritische Evaluation der Datenbasis und der Datenstruktur vorgeschlagen (Barocas und Selbst 2016).

- Auf statistischen Berechnungen beruhende Entscheidungssysteme bergen die Gefahr, besondere Situationen und Einzelsachverhalte nicht hinreichend genug abzubilden („outliers“), was zu der strukturellen Benachteiligung Betroffener führen kann. Dagegen helfen individuelle Einzelfallabwägungen inklusive nachträglicher Korrekturmöglichkeiten.
- Die implementierten Verfahren können je nach Ausgestaltung Blackboxsysteme sein, die intransparente Entscheidungen treffen. Der Entmenschlichung menschenbezogener Bewertungen und der ohnmächtigen Sorge um die maschinelle Kategorisierung der eigenen Person („fear of being categorized“) kann durch Überprüfbarkeit und Einsichtnahme in Logik und Natur zur besseren Einschätzung von Chancen und Risiken eines ADM-Systems begegnet werden (Keats Citron und Pasquale 2014). Auch die Erklärbarkeit von Einzelentscheidungen kann mit Blick auf die möglichen Risiken für eine ausreichende Berücksichtigung von individuellen, gruppen- und gesellschaftsbezogenen Interessen helfen.
- Risiken können außerdem entstehen, wenn die Ergebnisse von ADM-Systemen über den unmittelbaren Entscheidungszweck hinaus genutzt und so zweckentfremdet werden, etwa wenn Entscheidungsergebnisse auf Grundlage aggregierter Datenauswertungen an Dritte weitergegeben werden. Dies kann durch Maßnahmen wie eine starke Zweckbindung verhindert werden.
- Im Bereich der automatisierten Aggregation und Kuratierung von Medieninhalten durch Intermediäre können Netzwerkeffekte zu Marktmacht- und bei einseitiger Priorisierung von Inhalten neue Formen der Meinungsmachtkonzentration entstehen. Als Instrumente werden hier vor allem Transparenz bezüglich der Priorisierungslogiken und Vielfaltsvorgaben diskutiert (Schulz und Dankert 2016).

Weitere identifizierte Risikofelder folgen aus den soziotechnischen Konsequenzen des Einsatzes von ADM-Systemen (Impactphase):

- Die Gefahr, dass aus dem Einsatz von ADM-Systemen gesellschaftlich unangemessene Folgen erwachsen, kann durch die Gewährleistung umfassender Evaluationen, insbesondere mit Blick auf die gesellschaftliche Angemessenheit ihres Einsatzes, verringert werden. Dabei müssten bei Überprüfungen gezielt auch unvorhergesehene soziale Wechselwirkungen berücksichtigt und das sozioökonomische Verhältnis von Vor- und Nachteilen bzw. Nutzen und Risiken betrachtet werden.
- Entstehen Algorithmenmonokulturen, etwa wenn einzelne Entscheidungsarchitekturen und -logiken in einem Sachbereich vorherrschend sind, können andere und ggf. bessere Ansätze verdrängt werden. Die Innovationsarmut führte zu der weitreichenden Anwendung einzelner, weniger ADM-Prozesse und -verfahren. Ansonsten „nur“ durch Entscheidungen eines Einzelsystems Betroffene wären dann systematisch in ihren Teilhabechancen gehemmt. Dem könnte durch Maßnahmen zur Vielfaltssicherung von ADM-Prozessen begegnet werden.

Die identifizierten Problembereiche bergen Risiken in Form der Schaffung oder Verstetigung sozialer Ungleichheit, der Ungleichbehandlung von Gleichen sowie der Entmenschlichung von Entscheidungen, wo Personen zu reinen Objekten mathematischer Berechnungen werden. Auffällig dabei ist, dass neben individuellen Interessen wie Handlungsfreiheit, Persönlichkeitsrechten und Fairness auch gruppenbezogene Ziele wie Nichtdiskriminierung treten. Auch auf der gesamtgesellschaftlichen Ebene weisen die Risikofelder Bezüge auf, vor allem mit Blick auf gesellschaftliche Vielfalt. Ein weiterer normativer Zielwert, der aber die drei Ebenen komplett übergreift, ist soziale Teilhabe: Risiken für Teilhabe, die sich ggf. aus ADM-Systemen ergeben, können sich in ganz unterschiedlicher Weise auf Ebene des Einzelnen, auf Ebene etwa einer Minderheit sowie auf gesamtgesellschaftlicher Ebene manifestieren. Eine klare Zuordnung der Zielwerte der Nichtdiskriminierung zur einzelbezogenen oder gruppenbezogenen sowie der sozialen Teilhabe zur einzelbezogenen, gruppenbezogenen und gesellschaftsbezogenen Ebene ist so nicht möglich. Einige der Zielwerte (insbesondere Autonomie, Persönlichkeitsrechte, Nichtdiskriminierung) sind zudem bereits in Rechtsnormen eingeschrieben, bilden also beispielsweise Gewährleistungsgehalte von Grund- und Menschenrechten auf nationaler, Europäischer oder sogar internationaler Ebene. Andere sind Ausdruck von Werten, die von vielen geteilt werden, und Gegenstand

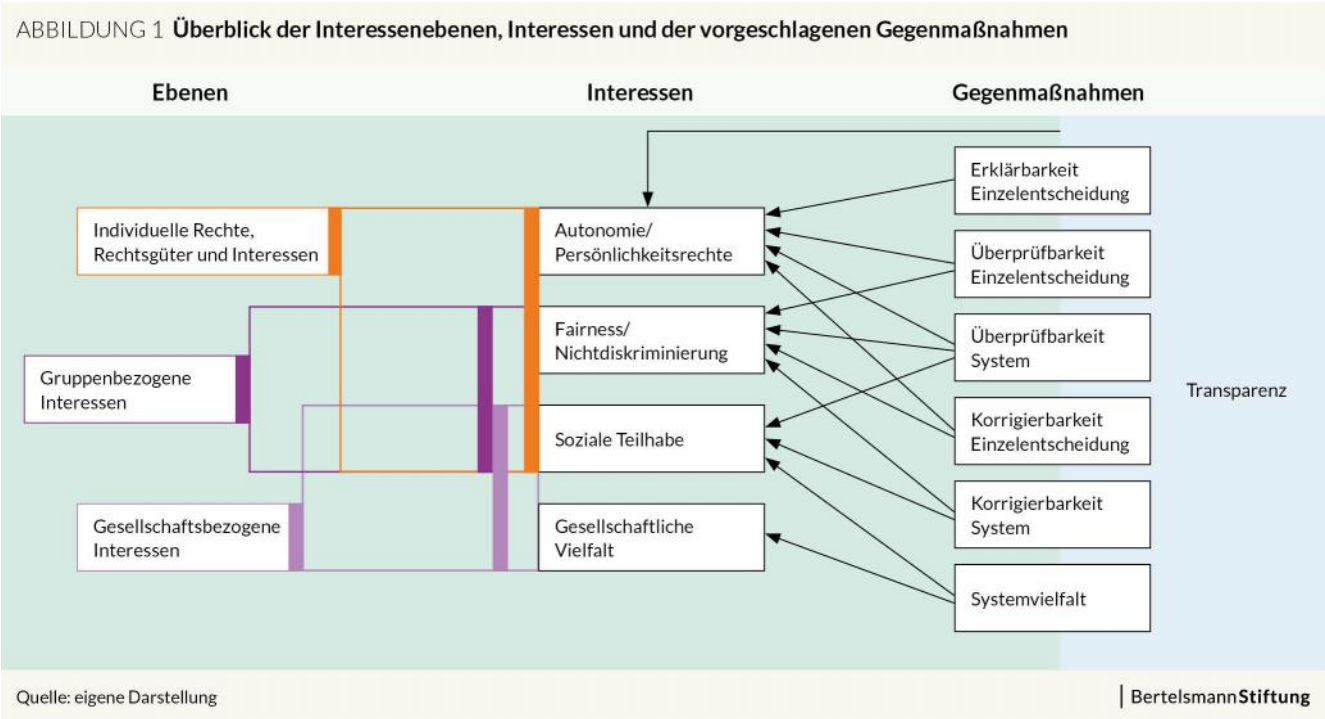
ethischer Diskussionen, ohne dabei aber rechtlich normiert zu sein (Fairness, Teilhabe, Vielfalt). Für die Frage, ob der Staat die (rechtliche) Pflicht hat, zu handeln, bleibt diese Unterscheidung bedeutsam, auch wenn sie in der öffentlichen Debatte nicht immer durchgehalten wird.

Die als Reaktion auf die ADM-Systemen innewohnenden Risikopotenziale vorgeschlagenen Einzelinstrumente lassen sich verdichten zu Ansätzen, die Transparenz, Erklärbarkeit der Einzelentscheidung, Überprüfbarkeit der Einzelentscheidung und des Verfahrens, Korrigierbarkeit der Einzelentscheidung und des Verfahrens und schließlich die Gewährleistung von vielfältigen ADM-Systemen sicherstellen sollen.

Insbesondere Maßnahmen zur Sicherung von Transparenz wird dabei oft der Stellenwert eines universalen Allheilmittels zugeschrieben: Durch das Veröffentlichen von Informationen zu automatisierten Entscheidungsverfahren sollen diese für den Einzelnen besser verstehbar sein und mögliche Fehlannahmen, -konzeptionen oder -entscheidungen für die Öffentlichkeit im besten Falle erkennbar und kritisierbar machen. Neben der Transparenz tragen zur Absicherung von Handlungsautonomie und Persönlichkeitsrechten vor allem einzelentscheidungsbezogene Maßnahmen bei, namentlich Vorgaben, die die Erklärbarkeit, Überprüfbarkeit und Korrigierbarkeit einer konkreten automatisierten Entscheidung sichern. Auch individuelle Interessen der Fairness und Diskriminierungsfreiheit können durch überprüfbare und korrigierbare Einzelentscheidungen gesichert werden. Durch diskriminierende ADM-Systeme sind aber regelmäßig ganze distinkte Bevölkerungsgruppen betroffen, sodass zur Gewährleistung gruppenbezogener Nichtdiskriminierungsinteressen auch die systembezogene Überprüfbarkeit und Korrigierbarkeit des Entscheidungsverfahrens insgesamt notwendig erscheint. Erklärbarkeit, Überprüfbarkeit und Korrigierbarkeit setzen dabei jeweils Wissen über das ADM-System voraus. Das macht Transparenz zu einer Gegenmaßnahme, die sich positiv auf *alle* genannten Zielwerte auswirken kann: unmittelbar auf die autonome Ausübung des informationellen Selbstbestimmungsrechts als Ausfluss der Persönlichkeitsrechte sowie mittelbar als Vehikel zur besseren Erklärbarkeit und Überprüfbarkeit der Einzelentscheidungen und des Gesamtverfahrens.

Für die Absicherung individueller wie gesellschaftlicher sozialer Teilhabe ist neben der Überprüfbarkeit und Korrigierbarkeit einmal implementierter Verfahren auch die Gewährleistung von Systemvielfalt relevant, um durch den in der Praxis einseitigen Einsatz bestimmter ADM-Verfahren systematische und kaum zu umgehende Ausschlussrisiken zu verringern. Die Gewährleistung von ADM-Systemvielfalt ist zudem zentrale Maßnahme, wenn es um die Aufrechterhaltung gesellschaftlicher Vielfalt im Bereich automatisierter Entscheidungssysteme geht.

Abbildung 1: Überblick der Interessenebenen, Interessen und der vorgeschlagenen Gegenmaßnahmen (Quelle: eigene Darstellung)



Aus der Zusammenschau der identifizierten Zielwerte und vorgeschlagenen Maßnahmen zu ihrer Absicherung ergibt sich ein komplexes Geflecht (s. Abbildung 1), das im Folgenden als Grundlage der rechtswissenschaftlichen Analyse dienen soll. Das Gutachten will hier klären, ob und inwieweit die datenschutzrechtlichen Vorgaben aus der DSGVO und dem BDSG n.F. Steuerungsinstrumente im Sinne der oben genannten Maßnahmen vorsehen, die in der Lage sind, die identifizierten individuellen, gruppen- und gesellschaftsbezogenen Interessen tatsächlich abzusichern.

3 Welche Anforderungen die DSGVO an ADM-Systeme stellt: Relevante Instrumente des Datenschutzrechts

Das Datenschutzrecht bietet sich als Betrachtungsgegenstand besonders an, wenn es um Instrumente zur Absicherung von Interessen geht, die von ADM-Systemen beeinflusst werden. Denn es enthält bereits explizit Regeln für algorithmische Systeme: Die ab Mai 2018 gültigen Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) und des zeitgleich in Kraft tretenden neuen Bundesdatenschutzgesetzes (BDSG n.F.) enthalten neben den allgemeingültigen Vorgaben an datenverarbeitende Anbieter auch spezifische Vorgaben für Systeme, die auf Grundlage der Verarbeitung personenbezogener Daten automatisierte Entscheidungen treffen. Das folgende Kapitel identifiziert diejenigen Vorschriften des datenschutzrechtlichen Rahmens, die direkt oder indirekt Maßnahmen zur Gewährleistung der eben beschriebenen Zielwerte vorsehen. Es beschreibt ihren Anwendungsbereich und den Umfang, aber auch mögliche Hürden oder Schwierigkeiten in der Umsetzung.

Der Umstand, dass ganz unterschiedliche Zielwerte abzusichern sind, schließt einen Blick auf das Datenschutzrecht als Prüfungsgegenstand nicht von vornherein aus; bei den ADM-spezifischen Vorgaben tritt eine Vielfalt an Schutzgütern zutage: Als Schutzzweck der DSGVO sieht Art. 1 Abs. 2 DSGVO den Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ vor. Zentraler Schutzgedanke ist damit die Gewährleistung des Grundrechts aus Art. 8 EU-Grundrechtecharta, dem Recht des Einzelnen auf Datenschutz. Das zusätzliche Ziel, sämtliche Grundrechte und Grundfreiheiten ebenfalls zu wahren, verweist auf das Charakteristikum des Datenschutzes als sogenanntes „Vorfeldrecht“: Es schützt zentral immaterielle Positionen wie Handlungsautonomie und Persönlichkeitsrechte (in Deutschland auch in der Ausprägung des Rechts auf informationelle Selbstbestimmung) nicht nur um dieser Rechte wegen, sondern auch, um den aus der Datenverarbeitung in einem zweiten Schritt erwachsenden Gefahren für die Ausübung anderer Rechte und Freiheiten zu begegnen (Bull 2006).

Datenverarbeitung birgt immer auch Risiken für eine Vielzahl verschiedener Grundrechte. Insbesondere Formen der individuellen und gruppenbezogenen Diskriminierung können sich hier ergeben und dadurch vermittelte Beeinträchtigungen bezüglich der Ausübung anderer Grundrechte wie etwa der Gewissens-, der Religionsfreiheit oder der Meinungsfreiheit. Dessen ungeachtet liegt der Fokus der DSGVO auf dem Datenschutz gemäß Art. 8 EU-Grundrechtecharta, sodass nicht davon ausgegangen werden kann, dass automatisch andere relevante Rechte und Werte wie die eben genannten ihrem Rang entsprechend durch die Verordnung mit geschützt werden – im Einzelfall können diese Rechte sogar dem Datenschutz gegenläufige Interessen schützen (z. B. Informationsfreiheit). Bei dem Abstellen auf die Entscheidungs*konsequenzen* automatisierter Entscheidungen verlässt der EU-Verordnungsgeber die unmittelbare Schutzrichtung des Datenschutzes und zielt in erster Linie auf den Schutz vor beeinträchtigenden Wirkungen von Entscheidungen *im Nachgang* einer automatisierten Datenverarbeitung ab. Diese Verlagerung der Basis des Schutzmaßstabs weg von der Datenverarbeitung hin zur Entscheidungskonsequenz ist beachtlich, weil damit die klassischen Steuerungsinstrumente des Datenschutzes für die Erreichung ganz anderer Schutzzwecke eingespannt werden, ohne dass eine Prüfung der Wirksamkeit dieser Steuerungsformen stattgefunden hätte. Es ist auch bemerkenswert, dass weder im Rahmen des Gesetzgebungsverfahrens noch in der Kommentarliteratur bislang systematisch auf diesen (Prämissen-)Wechsel eingegangen worden ist; teils werden beide Stufen – Datenverarbeitung und automatisierte Entscheidung – schlicht synonym verwendet. Die Relevanz der Differenzierung zwischen entscheidungsrelevanter Datenverarbeitung einerseits und der Entscheidung und ihrer Wirkungen andererseits wird mit Blick auf den Schutzzweck des Datenschutzes noch zu thematisieren sein (s. Kapitel 3.1.1 und 3.2.1).

Der Umstand, dass die DSGVO und das BDSG n.F. bekannt, aber noch nicht in Kraft getreten sind, muss bei den folgenden Überlegungen stets berücksichtigt werden: Die hier auf Grundlage der bislang publizierten rechtswissenschaftlichen (Kommentar-)Literatur gemachten Aussagen und Wertungen werden absehbar eine wichtige Rolle in zukünftigen behördlichen und gerichtlichen Entscheidungen spielen. Bis dahin bedeuten juristische Schwierigkeiten in der Interpretation der (teils unbestimmten) Gesetzesbegriffe für Verantwortliche wie für Betroffene zunächst Rechtsunsicherheit.

Vor der Betrachtung der Absicherung von individuellen, gruppen- und gesellschaftsbezogenen Interessen durch einzelne datenschutzrechtliche Instrumente steht die Frage der grundsätzlichen rechtlichen Zulässigkeit von ADM-Systemen nach der DSGVO.

3.1 Grundsätzliches Verbot von reinen ADM-Systemen – mit weitreichenden Ausnahmen

Wären automatisierte Entscheidungen grundsätzlich unzulässig, würden sich im Anwendungsbereich der DSGVO die möglichen Risiken von ADM-Systemen gar nicht erst realisieren können. Und in der Tat geht die DSGVO von dem Grundsatz aus, dass eine Person das Recht hat, nicht einer Entscheidung unterworfen zu werden, die auf einer rein automatisierten Verarbeitung ihrer Daten beruht (Art. 22 Abs. 1 DSGVO). Die Verordnung formuliert diesen Grundsatz vom Wortlaut her als Recht des Einzelnen gegenüber Verantwortlichen, die entsprechende Systeme einsetzen. Mit Blick auf den weiteren Aufbau der Vorschrift – Absatz 1 stellt den Grundsatz auf, Absatz 2 sieht Ausnahmen davon vor, Absatz 3 stellt besondere Anforderungen an Systeme, für die Absatz 1 ausnahmsweise nicht gilt – erscheint die Vorschrift aber als objektive Verbotsnorm. Grundsätzlich ist der Einsatz entsprechender ADM-Systeme also unzulässig. Dieser Grundsatz ist nicht neu: Art. 15 der EG-Datenschutzrichtlinie und der jetzige § 6a BDSG enthalten vergleichbare Vorschriften; beide Normen sind bislang in der rechtlichen Praxis kaum in Erscheinung getreten (s. aber Bygrave 2001). Erst die politischen Diskussionen im Rahmen der DSGVO-Überlegungen haben die Relevanz dieser Normen im Angesicht zunehmender Entscheidungsautomatisierung auf Grundlage personenbezogener Daten verdeutlicht (Zarsky 2017).

Der Anwendungsbereich des Verbots aus Art. 22 Abs. 1 DSGVO ist allerdings – deutlich – beschränkt: Zunächst muss die automatisierte Entscheidung auf Grundlage einer Datenverarbeitung personenbezogener Daten erfolgen (s. Abbildung 2). Werden Daten verarbeitet, die keinen Personenbezug haben, etwa weil sie anonymisiert wurden oder nie einen Bezug zu einem Menschen hatten, so ist der sachliche Anwendungsbereich der Verordnung insgesamt nicht eröffnet (Art. 2 Abs. 1 DSGVO). Auch wenn die Daten von anderen Personen als dem Systemanwender verarbeitet werden, handelt es sich nicht um ein ADM-System im Sinne der Vorschrift.

Art. 21 Abs. 1 DSGVO umfasst zudem nur ADM-Systeme, bei denen die Entscheidung „ausschließlich auf einer automatisierten Verarbeitung“ beruht. Unzulässig sind Systeme, die Entscheidungen ohne jegliches menschliche Eingreifen auf Grundlage einer vorausgegangenen Datenverarbeitung treffen. Eine grundsätzliche Unzulässigkeit jedweder automatisierter Entscheidung oder der ihr zugrunde liegenden Datenverarbeitung ergibt sich aus der DSGVO insoweit nicht. Zunächst muss also das System tatsächlich eine Entscheidung treffen. Das Verbot findet keine Anwendung auf Systeme, die „nur“ automatisiert personenbezogene Daten zur Vorauswahl, Entscheidungsvorbereitung oder als Empfehlungssystem verarbeiten, an deren Ende ein Mensch die finale Entscheidung trifft (Decision Support Systems oder DS-Systeme). Voraussetzung ist dabei, dass die Beteiligung des Menschen innerhalb der Entscheidungsarchitektur ein nicht bloß formaler Akt ist, sondern die entscheidende Person auch faktisch die Möglichkeit zur eigenen Entscheidung auf Grundlage der vorliegenden Daten hat – auch gegen die automatisierte Empfehlung. Letzteres spielt eine zentrale Rolle hinsichtlich des Nutzerrechts auf Hinzuziehung einer menschlichen Person (s. Kapitel 3.4.1). Inwieweit eine Entscheidungsfreiheit der beteiligten Person tatsächlich gegeben ist, kann von der zuständigen Datenschutzaufsicht im Rahmen einer Prüfung kontrolliert werden (zur den Aufsichtsbefugnissen s. Kapitel 4.4). Offen bleibt zu diesem Zeitpunkt angesichts der vielfältigen Ausgestaltungsmöglichkeiten von Entscheidungsarchitekturen im Zusammenspiel von ADM-System und menschlichem Beteiligten, was einen Prozessschritt im Einzelnen zu einer Entscheidung im rechtlichen Sinne werden lässt.

Zuletzt müssen die von derartigen Systemen getroffenen Entscheidungen dem Betroffenen gegenüber eine rechtliche Wirkung entfalten oder ihn in ähnlicher Weise erheblich beeinträchtigen. Eine Entfaltung rechtlicher Wirkung wird überall dort anzunehmen sein, wo mit der Entscheidung eine Änderung des rechtlichen Status des Betroffenen einhergeht, etwa bei der Verwehrung eines Rechtsanspruchs oder dem Erlass eines belastenden

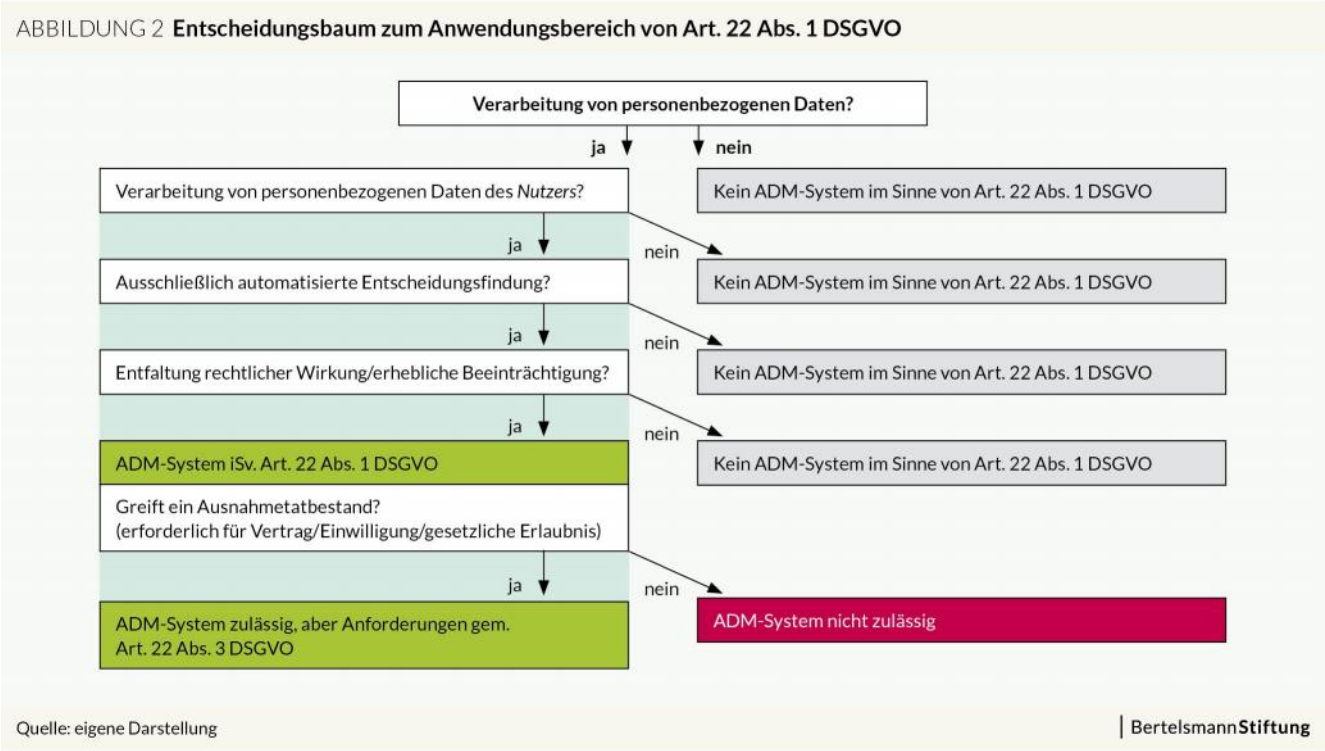
Verwaltungsakts. Inwieweit die Vorschrift auch auf Sachverhalte Anwendung findet, bei denen sich aus der Entscheidung des ADM-Systems lediglich ein rechtlicher Vorteil für den Betroffenen ergibt, ist umstritten. Angesichts der auch dafür nötigen Datenverarbeitung erscheint der Schutzzweck der DSGVO auch dann jedenfalls berührt, zumal zum Zeitpunkt der Datenverarbeitung das Entscheidungsergebnis noch nicht bekannt ist. Im Rahmen privatrechtlicher Verträge, für die der Grundsatz der Privatautonomie gilt, reicht eine ablehnende Entscheidung über einen Vertragsschluss oder eine Vertragszusage unter besonderen Bedingungen nicht zur Entfaltung einer rechtlichen Wirkung. In diesen Fällen wird zwar dem möglichen Wunsch des Betroffenen zu einem bestimmten Vertragsschluss nicht entsprochen, seine Rechtsstellung verändert sich dadurch aber gerade nicht; ggf. jedoch kann eine „erhebliche Beeinträchtigung" damit einhergehen (dazu sogleich). Anders sieht dagegen die Behandlung von Entscheidungen aus, die zu einem Vertragsschluss führen: Dann tritt der Betroffene durch die Annahme in eine neue Rechtsstellung gegenüber dem Verantwortlichen und Art. 22 Abs. 1 DSGVO ist anwendbar.

Die Konkretisierung der Frage, wann eine „erhebliche Beeinträchtigung in ähnlicher Weise" vorliegt, kann in Abgrenzung zu der rechtlichen Wirkung dort erfolgen, wo einem Betroffenen außerhalb von ihm zustehenden Rechtspositionen ein Vertragsschluss ganz verwehrt oder nur zu schlechteren Bedingungen angeboten wird. Eine Beeinträchtigung kann auch dort anzunehmen sein, wo die Entscheidung nicht ausschließlich rechtlich nachteilig ist, etwa wenn ein Vertrag mit dem Betroffenen zustande kommt, aber zu einem höheren Preis oder nur unter Vertragsauflagen. Auch Wirkungen außerhalb rechtlicher Konsequenzen, etwa durch Entscheidungen darüber, welche Onlinewerbeinhalte einem Nutzer gegenüber auf Grundlage von Profilingmaßnahmen ausgespielt werden, können davon umfasst sein. Wann dabei die Stufe der rechtsstellungsgleichen „erheblichen Beeinträchtigung" erreicht ist, ist bislang nicht konkret diskutiert worden. Zentrale Aspekte bei der Bewertung der Erheblichkeit sind jedenfalls die wirtschaftliche oder praktische Bedeutung des Entscheidungsgegenstands sowie die Nachhaltigkeit der Beeinträchtigung. Dagegen sollen lediglich lästige oder als unbequem empfundene Folgen einer automatisierten Entscheidung nicht als erhebliche Beeinträchtigung gelten.

Nicht berücksichtigt wird durch dieses einzelfallbezogene Verständnis der Grad der Beeinträchtigung, der durch den repetitiven Einsatz automatisierter Entscheidungssysteme erfolgt. Entscheiden vielfältige Systeme, die für den gleichen Zweck (z. B. Profiling) eingesetzt werden, gegenüber dem Einzelnen in immer wieder in der gleichen Art und Weise, kann sich daraus über längere Zeitabschnitte und eine Vielzahl von Entscheidungen eine systematische und in ihrer Gesamtheit durchaus relevante Beeinträchtigung ergeben. Mit Blick auf den weit formulierten Schutzzweck der DSGVO, der als Betroffenenrecht auch das Diskriminierungsverbot aus Art. 21 der EU-Grundrechtecharta umfasst, können auch derartig (diskriminierende) Entscheidungen zum Betrachtungsgegenstand einer DSGVO-Prüfung werden. Solange hier keine begriffliche Schärfung der erheblichen Beeinträchtigung in der Rechtsprechungspraxis erfolgt, wird sich die juristische Diskussion zunächst im Rahmen von notwendigen Einzelfallbetrachtungen abspielen müssen.

Aufgeweicht wird der beschriebene Grundsatz der Unzulässigkeit von reinen ADM-Systemen in der Praxis aber nicht nur durch den restriktiven Anwendungsbereich des Verbots aus Art. 22 Abs. 1 DSGVO, sondern auch durch die in Abs. 2 vorgesehenen, weiträumigen Ausnahmetatbestände (Mendoza und Bygrave 2017). So sind Systeme automatisierter Entscheidungen „ausnahmsweise" dann zulässig, wenn (a) die Entscheidung für den Vertragsschluss oder die Vertragserfüllung zwischen Betroffenem und Verantwortlichem erforderlich ist, (b) die ADM-Entscheidung durch eine gesetzliche Vorschrift im Land des Betroffenen für zulässig erklärt wurde oder wenn (c) die Entscheidung mit ausdrücklicher Einwilligung des Betroffenen erfolgt. In den Fällen der ausnahmsweisen Zulässigkeit automatisierter Entscheidungssysteme stellt schließlich Art. 22 Abs. 3 DSGVO spezifische Anforderungen auf (s. Kapitel 3.1.4).

Abbildung 2: Entscheidungsbaum zum Anwendungsbereich von Art. 22 Abs. 1 DSGVO (Quelle: eigene Darstellung)



3.1.1 Ausnahme 1: Erforderlichkeit eines ADM-Systems für Vertragsschluss oder -erfüllung

Der Einsatz reiner ADM-Systeme ist dort zulässig, wo die automatisierte Entscheidung für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist. Dabei muss die automatisierte Entscheidung selbst nicht Gegenstand des Vertrags sein, sondern kann auch nur Entscheidungsgrundlage für einen darauf basierenden Vertragsschluss sein. Damit sieht die DSGVO vor allem dort eine gesetzliche Ausnahme von der Unzulässigkeit reiner ADM-Systeme vor, wo die Erwägungsgründe der Verordnung einen Hauptanwendungsfall von ADM-Systemen überhaupt sehen: Erwägungsgrund 71 nennt etwa automatisierte Entscheidungen über Onlinedarlehensverträge, die von Art. 22 Abs. 1 DSGVO gemeint sind. Diese aber sind dann über die Ausnahme in Art. 22 Abs. 2 Buchstabe a) ausnahmsweise erlaubt.

Problematisch an dieser Ausnahme ist, dass insbesondere in Fällen eines Ungleichgewichts zwischen Verantwortlichem und Betroffenem der Verantwortliche strukturelle Vorteile hat, wenn es um die Formulierung von Vertragszweck und -bestandteilen geht. Durch eine einseitige Bestimmung des Vertragszwecks kann der Verantwortliche auch die Anknüpfungspunkte für eine (vermeintliche) Erforderlichkeit bestimmen und sich praktisch selbst die Erforderlichkeit der automatisierten Entscheidung in den Vertrag schreiben. Dabei kann die tatsächliche Erforderlichkeit Gegenstand rechtlicher Überprüfungen sein: Die Herleitung und Begründung der Erforderlichkeit muss jedenfalls für Außenstehende nachvollziehbar und spezifisch auf Formen automatisierter Entscheidungssysteme gerichtet sein, etwa weil zum Vertragsschluss eine Vielzahl von Einzelaspekten auf Grundlage mathematischer Erfahrungen zu berücksichtigen sind und die automatisierte Entscheidung in unmittelbarem Zusammenhang mit dem Vertragsschluss steht. Eine andere Ansicht lässt bereits den von Betroffenem und Verantwortlichem in beidseitigem Interesse gewollten schnellen Vertragsschluss auf Grundlage eines automatisierten Entscheidungsprozesses genügen. Dies verkennt aber, dass insbesondere mit Blick auf das Einverständnis des Betroffenen der Einwilligungsvorbehalt die speziellere Vorschrift ist; das Erfordernis des Einsatzes von ADM-Systemen bei Vertragsschluss oder -erfüllung zielt gerade auf Fälle ab, in denen die Einwilligung oder das Einverständnis des Betroffenen nicht eingeholt werden müssen.

3.1.2 Ausnahme 2: Nationale Öffnungsklauseln zur Zulässigkeit von ADM-Systemen

Eine weitere Ausnahme vom ADM-Verbot des Art. 22 DSGVO sieht Abs. 2 Buchst. b) für Systeme vor, die aufgrund von Rechtsvorschriften der EU oder der einzelnen EU-Mitgliedstaaten zulässig sind. Voraussetzung dafür ist, dass diese Vorgaben die Rechte und Freiheiten des Betroffenen wahren. In der Praxis können dazu etwa nationale Vorschriften zählen, die ADM-Systeme für zulässig erklären, die der Überwachung oder Verhinderung von Steuerhinterziehung oder Betrug dienen oder die Sicherheit und Zuverlässigkeit eines bereitgestellten Dienstes gewährleisten sollen.

Das neue BDSG sieht in § 37 Abs. 1 eine entsprechende Ausnahmevorschrift vor: Danach sind ADM-Systeme auch in Fällen zulässig, in denen die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag erfolgt und dem Begehren des Betroffenen stattgegeben wurde oder – soweit die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht – dem Begehren nicht vollumfänglich stattgegeben wurde. Im letzteren Fall sichert § 37 Abs. 1 Nr. 2 BDSG n.F. dem Betroffenen spezifische Darlegungs- und Anfechtungsrechte zu, die sich denen aus Art. 22 Abs. 3 DSGVO annähern (s. dazu Kapitel 3.1.4).

3.1.3 Ausnahme 3: Einwilligung des Betroffenen in eine automatisierte Entscheidung

Auch wenn der Einsatz des ADM-Systems nicht für den Vertragsabschluss oder die Vertragserfüllung erforderlich ist, kann eine automatisierte Entscheidung datenschutzrechtlich zulässig sein: Art. 22 Abs. 2 Buchst. c) DSGVO sieht eine Ausnahme auch für diejenigen Fälle vor, in denen der Betroffene gegenüber dem Verantwortlichen seine Einwilligung erteilt hat. Die in der Praxis absehbar hochrelevante Ausnahme macht aus dem grundsätzlichen Verbot von ADM-Systemen im Sinne des Art. 22 Abs. 1 DSGVO faktisch ein Verbot mit Einwilligungsvorbehalt.

Unklar ist dabei allerdings, worauf genau sich die Einwilligung zu beziehen hat: Die zentral von Art. 7 DSGVO gerahmte datenschutzrechtliche Einwilligung betrifft die Einverständniserklärung des Betroffenen in die Verarbeitung seiner personenbezogenen Daten. Der Wortlaut des Art. 22 Abs. 2 Buchst. c) DSGVO bezieht die erforderliche Einwilligung aber auf die automatisierte Entscheidung selbst – ein erneuter Fall, in dem Art. 22 DSGVO nicht zwischen der Datenverarbeitung und der auf dieser Basis berechneten Entscheidung differenziert. In diesem Fall muss die Einwilligung sich entsprechend ausdrücklich nicht nur auf die Datenverarbeitung durch das ADM-System beziehen, sondern zwingend das Einverständnis in die automatisierte Entscheidungsfindung beinhalten. Bei rein unterstützenden Systemen (Decision Support Systems, DS-Systeme) dagegen reichte dagegen eine Einwilligung nur in die Datenverarbeitung. Eine Einwilligung nach Art. 22 Abs. 2 Buchst. c) ist im Vergleich zu einer „normalen“ Einwilligung gemäß Art. 7 DSGVO eine spezifisch erweiterte Erklärung. Dies kann systematische Folgen für die Informationsgrundlage haben, auf deren Grundlage der Betroffene seine informierte Einwilligung abgibt (s. zur Einwilligung bei ADM-Systemen Kapitel 3.3).

3.1.4 Anforderungen an „ausnahmsweise“ zulässige automatisierte Entscheidungen

Die beschriebenen weiten Ausnahmen vom Verbot reiner ADM-Systeme gehen einher mit spezifischen rechtlichen Anforderungen und Grenzen an die Ausgestaltung dieser automatisierten Entscheidungssysteme. Für Fälle zulässiger ADM-Systeme, bei denen die Datenverarbeitung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist oder bei denen eine Einwilligung des Betroffenen vorliegt, sieht Art. 22 Abs. 3 DSGVO spezifische Schutzmaßnahmen vor, die der Verantwortliche einzuziehen hat.

Grundsätzlich ist der Verantwortliche eines ADM-Systems verpflichtet, angemessene Maßnahmen zu treffen, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren“. Dazu zählt die Verordnung mindestens das Recht des Betroffenen gegenüber dem Verantwortlichen auf Hinzuziehung einer menschlichen Person sowie ein Darlegungs- und ein Anfechtungsrecht (s. Kapitel 3.4.1). Alle drei genannten Mindestvorkehrungen zielen dabei auf die Möglichkeit des Betroffenen, den Verantwortlichen zu einer Entscheidungskorrektur zu bringen. An der Rechtmäßigkeit und rechtlichen Wirksamkeit der automatisierten Entscheidung ändern diese Ansprüche nichts. Auch über die konkret genannten Nutzerrechte hinaus kann der Verantwortliche mit Blick auf Art. 22 Abs. 3 DSGVO gehalten sein, weitere nutzerrechtschützende Vorkehrungen

zu treffen. Diese können sich auch auf den Umfang und die Tragweite der Informations-, Auskunfts- und Begründungspflichten erstrecken (s. dazu sogleich).

Eine Grenze besonderer Art für die Zulässigkeit von ADM-Systemen sieht Art. 22 Abs. 4 DSGVO vor: Die Verwendung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO dürfen nicht zur automatisierten Entscheidungsfindung genutzt werden. Zu diesen Daten gehören unter anderem Informationen über rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, genetische oder biometrische Daten sowie Informationen zu Gesundheit, Sexualleben oder die sexuelle Orientierung. Diese Beschränkung der Ausnahmen des ADM-Verbots wird jedoch wieder durch DSGVO-Ausnahmen aufgeweicht: So können entsprechende personenbezogene Daten für automatisierte Entscheidungen sehr wohl genutzt werden, wenn die betroffene Person eingewilligt hat oder eine EU- oder mitgliedstaatliche Rechtsvorschrift dies erlaubt.

Das grundsätzliche Verbot von automatisierten Entscheidungen in Art. 22 DSGVO weist nicht nur einen restriktiven Anwendungsbereich auf, die Verordnung sieht darüber hinaus auch weitflächige Ausnahmeregelungen vor. Automatisierte Entscheidungen werden auch unter dem DSGVO-Regime alltägliche Praxis sein. Decision-Support-Systeme, die den Entscheider bei der menschlichen Entscheidung „lediglich“ unterstützen, können daneben beliebig weitreichend im Rahmen der allgemeinen Anforderungen der DSGVO eingesetzt werden. Zur Klärung der Frage, inwieweit der datenschutzrechtliche Rechtsrahmen ab Mai 2018 zur Sicherung der normativen Zielwerte beiträgt, kommt es insoweit auf die Möglichkeiten der datenschutzrechtlichen Einzelinstrumente an, die im Folgenden untersucht werden.

3.2 Informationspflichten des Verantwortlichen eines ADM-Systems *vor* der Datenverarbeitung

Das Datenschutzrecht geht davon aus, dass die eigenen Rechte mit Blick auf den Datenschutz vor allem von den betroffenen Personen selbst wahrgenommen werden. Je besser der Betroffene darüber Bescheid weiß, wer zu welchem Zweck welche personenbezogenen Daten verarbeiten möchte, desto eher kann er sein Recht auf informationelle Selbstbestimmung tatsächlich wahrnehmen. Transparenzvorgaben in Form gesetzlicher Informationspflichten, die sich an die jeweils datenverarbeitende Stelle richten, sind daher ein klassisches Regulierungskonzept im Datenschutz. Die DSGVO macht in dieser Hinsicht keinen Unterschied: Auch sie verpflichtet die Verantwortlichen, dem Betroffenen gegenüber Transparenz über die beabsichtigte Datenerhebung und -verarbeitung herzustellen. Verantwortlich aus Sicht der datenschutzrechtlichen Anforderungen der DSGVO ist die natürliche oder juristische Person, die die Datenverarbeitung durch das ADM-System zur eigenen Verwendung nutzt, d. h. dass der ursprüngliche Softwareentwickler, der mit dem späteren Einsatz des Systems ggf. gar nichts mehr zu tun hat, dann nicht Verantwortlicher im Sinne des Datenschutzes ist.

Die DSGVO sieht in Art. 13 Abs. 1 und 2 umfassende Informationspflichten vor, denen der Verantwortliche dem Betroffenen gegenüber vor der Erhebung der personenbezogenen Daten nachzukommen hat. Zu den verpflichtenden Informationen zählen unter anderem der Name des Verantwortlichen und dessen Kontaktdaten, die Zwecke, Zweckänderungen und rechtlichen Grundlagen der Datenverarbeitung, die Dauer der Speicherung, ggf. die Empfänger oder Kategorien von Empfängern der Daten und ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland zu übermitteln. Außerdem muss der Betroffene vor der Verarbeitung unter anderem über seine Auskunfts-, Berichtigungs-, Löschungsrechte sowie Widerrufsmöglichkeiten aufgeklärt werden. Auch die Information über das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde gehört zu diesen Informationspflichten. Nach Art. 14 DSGVO gelten vergleichbare Transparenzpflichten auch für Verantwortliche, die die personenbezogenen Daten nicht direkt bei dem Betroffenen erheben, sondern diese aus dritten Quellen erhalten.

An die Gestaltung und Formulierung der Informationen stellt Art. 12 Abs. 1 DSGVO hohe Anforderungen: Sie sollen präzise, transparent und verständlich sein und in einer leicht zugänglichen Form in einer klaren und einfachen

Sprache übermittelt werden. Der Verantwortliche hat auch die Möglichkeit, zusätzlich standardisierte Bildsymbole oder Icons für einen besseren Überblick zu benutzen (s. Art. 12 Abs. 7 DSGVO). Zentral sieht die Verordnung damit ein Genauigkeits- und ein Verständlichkeitsgebot vor. Maßstab für die in der Praxis schwierig zu operationalisierende Verständlichkeit muss dabei der durchschnittliche Empfänger der Information sein. Sie ist also abhängig vom jeweiligen Erhebungskontext zu bestimmen.

Für ADM-Systeme besonders relevant sind mit Blick auf die Informationspflichten Art. 13 Abs. 2 Buchst. f) und Art. 14 Abs. 2 Buchst. g) DSGVO, die Verantwortliche bei der Nutzung von Systemen automatisierten Entscheidungsfindung im Sinne von Artikel 22 verpflichten, dem Betroffenen „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung“ zur Verfügung zu stellen. Der Begriff der involvierten Logik und der konkrete Umfang der aus dieser Vorschrift erwachsenden Informationspflichten ist im Einzelnen umstritten.

3.2.1 Pflicht zur Information über die „involvierte Logik“ und die „Tragweite und Auswirkungen der Datenverarbeitung“

Unterhält ein Verantwortlicher ein nach Maßstäben des Art. 22 DSGVO zulässiges ADM-System, treffen ihn neben den allgemeinen datenschutzrechtlichen Informationspflichten auch solche, die den spezifischen Umstand der automatisierten Entscheidung, die dabei involvierte Logik und die Tragweite der Datenverarbeitung betreffen. Unstrittig erwächst aus dem Wortlaut von Art. 13 Abs. 2 Buchst. f) die Pflicht zur Information des Betroffenen über den Plan, auf Grundlage einer Datenverarbeitung eine automatisierte Entscheidung zu treffen. Über den Einsatz und die Nutzung eines ADM-Systems im Sinne des Art. 22 DSGVO muss also in jedem Fall aufgeklärt werden. Diese Informationspflicht besteht auch dann, wenn der Verantwortliche keine Einwilligung des Betroffenen benötigt; er muss dann zusätzlich auf den Umstand seiner Berechtigung zur Datenerhebung und -verarbeitung ausdrücklich hinweisen, also z. B. darauf, dass die Erhebung für einen Vertragsschluss oder dessen Erfüllung erforderlich ist. An dieser Stelle wird klar, dass die Einschränkungen des Anwendungsbereichs von Art. 22 Abs. 1 DSGVO unmittelbar Auswirkungen auf die ADM-spezifischen Informationspflichten haben: Wird ein lediglich entscheidungsunterstützendes oder empfehlendes Decision Support System (DS-System) genutzt, handelte es sich dabei nicht um einen Fall automatisierter Entscheidung – die Nutzung eines solchen Systems muss der Verantwortliche dann nicht transparent machen. Auch über ADM-Systeme, die wie beschrieben unterhalb der Schwelle der rechtlichen oder tatsächlichen Relevanz bleiben, ist vom Verantwortlichen nicht gesondert zu informieren.

Mit Blick auf die spezifisch für ADM-Systeme geltenden Informationspflichten stellt sich die Frage, welches Ziel die DSGVO hier verfolgt. Bei der Information über das „Ob“ eines ADM-Systems scheint der Schutzzweck nicht zentral auf der Ermöglichung der Wahrnehmung informationeller Selbstbestimmung zu liegen, sondern bereits zuvor die basale Entscheidung zu ermöglichen, nicht Gegenstand einer rein automatisierten Entscheidung zu sein. Noch vor der Gewährleistung der informationellen Selbstbestimmung scheint hier der Schutz der Menschenwürde aufzuscheinen. Erst die Informationspflichten bezüglich der involvierten Logik sowie der Tragweite und Auswirkungen der Datenverarbeitung im Rahmen der automatisierten Entscheidung – das „Wie“ des ADM-Systems – zielen dann auf die Ermöglichung der Ausübung informationeller Selbstbestimmungsrechte hin, namentlich mit einem Fokus auf die Einschätzung der Relevanz der Verarbeitung der eigenen personenbezogenen Daten durch das ADM-System.

Im Einzelnen diskutiert wird dabei, wie weitreichend die Transparenzpflicht bezüglich der „involvierten Logik“ und der „Tragweite und Auswirkungen der Datenverarbeitung“ der automatisierten Entscheidungsfindung zu verstehen ist. Teils wird hier in der (internationalen) rechtswissenschaftlichen Literatur vertreten, dass daraus eine quellcodebezogene Offenlegungspflicht folgt; teils wird die Vorgabe als grundsätzliche Pflicht zur Nutzung erklärbarer ADM-Systeme gesehen (zur Erklärbarkeit s. auch Kapitel 3.4.2 und 7.1). Andere wieder folgern mit Blick auf die möglichen Geheimhaltungsinteressen der Systemanbieter lediglich eine Pflicht zur Kundgabe abstrakter Informationen über Methoden und Kriterien der automatisierten Entscheidung. Alle drei Sichtweisen würden dazu führen, dass die Informationspflichten aus der DSGVO über die bisherige Rechtslage hinausgingen: Im Bereich des Scorings (§ 34 Abs. 4 S. 1 Nr. 4 BDSG) hatte der BGH geurteilt, dass sich Auskunftsrechte lediglich auf die verarbeiteten Daten und nicht auf das einem Scoring zugrunde liegende Berechnungsmodell beziehen (BGH

NJW 2014, 1235). Die Bestimmung des Informationsumfangs bezüglich der involvierten Logik ist für diese Untersuchung besonders relevant, da sich daraus Anforderungen an die Transparenz des ADM-Systems sowie der Einzelentscheidung ergeben können, die theoretisch geeignet sind, positiv auf einzelne der oben beschriebenen Zielwerte einzuzahlen.

Um zu ermitteln, was genau von den Informationspflichten in Bezug auf ADM-Systeme umfasst ist, hilft zunächst der Blick in die – rechtlich nicht verbindlichen – Erwägungsgründe. In Erwägungsgrund 71 stellt der Verordnungsgeber lediglich klar, dass sich der Auskunftsanspruch *nach* der Verarbeitung und automatisierten Entscheidung auf eine Erläuterung der ADM-Entscheidung bezieht (s. dazu Kapitel 3.4.2). Zu dem Umfang der *Vorab*informationen äußern die Erwägungsgründe nicht Konkretes (s. v. a. Erwägungsgrund 60 der DSGVO). Mit Blick auf die zeitliche Vorgezogenheit der Informationspflicht vor die Datenerhebung und -verarbeitung ist zu konstatieren, dass sich die Beschreibung der involvierten Logik jedenfalls noch nicht auf das Ergebnis einer Einzelentscheidung beziehen kann, sondern zu diesem Zeitpunkt noch das automatisierte Entscheidungssystem als abstraktes Ganzes zum Fokus hat. Die Pflicht zur Erläuterung der „Logik" des ADM-Systems zu diesem Zeitpunkt ist gerade nicht die Pflicht der Sicherstellung der Erklärbarkeit oder gar Begründbarkeit einer automatisiert erfolgten Einzelentscheidung (s. Kapitel 3.4.2 und 7.1).

Mit Blick auf den Schutzzweck der DSGVO muss der Schwerpunkt der Erläuterung vor allem auf der Beschreibung der Datenverarbeitung, der Darlegung der Funktionsweise der Bewertung auf Grundlage der Datenverarbeitung und der dafür verwandten Konzepte und Berechnungsmodelle liegen, die für die abschließende Entscheidung eine Rolle spielen bzw. spielen können. Der Betroffene muss – dies ergibt sich aus der Pflicht zur Erläuterung der Tragweite und Auswirkungen des Datenverarbeitung – informiert abschätzen können, welche seiner Daten welche Rolle in der Entscheidungsfindung spielen (können) und inwieweit dies aus individueller Sicht mit der Ausübung seines Rechts auf Datenschutz und der davon geschützten nachfolgenden Grundrechtsausübung (wie z. B. Religionsfreiheit oder Meinungsfreiheit) vereinbar ist. Die Konsequenzen, die sich erst aus der automatisierten Entscheidung selbst ergeben, stehen jedenfalls *vor* der Datenerhebung nicht im Zentrum der Informationspflichten, wohl aber die Information darüber, über welche Entscheidungsmöglichkeiten das ADM-System verfügt und welche Verarbeitungsergebnisse zu welcher Entscheidungsform führen.

Der Umfang dieser im Grundsatz abstrakten Beschreibung des Systems und den hinter der Entscheidung liegenden Annahmen, Wertungen und Konzepten wird gleich durch zwei teils widerstreitende Aspekte eingeschränkt : Zum einen wird die Konkretheit der Informationen beschränkt durch die Geheimhaltungsinteressen des Verantwortlichen. Dort, wo eine Systembeschreibung zu viele Einzelaspekte der Datenverarbeitung und Entscheidungsfindung offenbarte, stehen die um des Rechts auf Datenschutz willen gesetzten Informationspflichten im Widerstreit mit den ebenfalls rechtlich geschützten Positionen der Berufsfreiheit, der unternehmerischen Freiheit sowie der Eigentumsfreiheit des Verantwortlichen und bzw. oder des Systemherstellers (Art. 15, 16, 17 EU-Grundrechtecharta). Zum anderen wird die Form der abstrakten System- und Verarbeitungsbeschreibung von den inhaltlichen Anforderungen an die Informationspflichten bestimmt: Eine mathematische Funktionsbeschreibung des Systems wird für den Durchschnittsnutzer zwar präzise, aber gerade nicht leicht verständlich und damit auch nicht aussagekräftig sein. Die auch für die Erläuterung der involvierten Logik geltende Pflicht einer verständlichen Formulierung beschränkt insoweit ebenfalls die Konkretheit einer mathematisch-technischen Beschreibung des ADM-Systems – ganz unabhängig davon, ob eine solche konkrete Beschreibung angesichts der eingesetzten Architektur überhaupt theoretisch möglich wäre (zur Erklärbarkeit von KI-Systemen s. Kapitel 7.1). Dennoch gerät eine zu abstrakte, zu wenig Einzelheiten offenbarende Beschreibung in Gefahr, der Pflicht zur Vorhaltung „aussagekräftiger" Informationen nicht zu entsprechen.

Der Verantwortliche ist durch diese gegenläufigen Anforderungen angehalten, in Bezug auf die Informationstiefe, den Detailgrad und den Umfang der ADM-Systembeschreibung einen Mittelweg zu finden. Bei der Überprüfung der Anforderungen haben Aufsichtsbehörden und Gerichte Wertungs- und Entscheidungsspielräume sowohl in Hinblick auf die Annahmen bezüglich des jeweiligen Durchschnittsempfängers und seiner kognitiven Fähigkeiten, als auch hinsichtlich der Einschätzung der Einhaltung der Anforderungen an Informationsumfang und ihrer Form und Gestaltung.

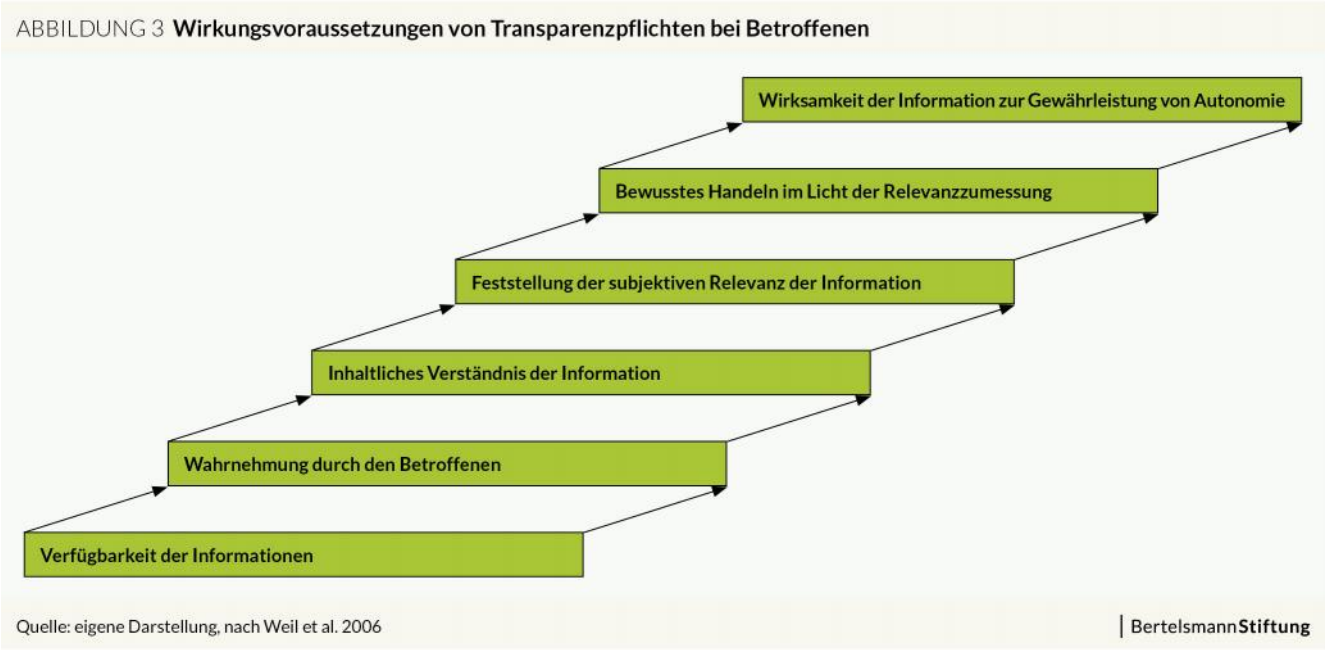
Im öffentlichen Bereich schränken §§ 32 Abs. 1 und 33 Abs. 1 Nr. 1 BDSG n.F. die öffentliche Stellen treffenden Informationspflichten nach Art. 13 und 14 DSGVO ein, wenn ansonsten „die ordnungsgemäße Erfüllung der [...] Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der DSGVO gefährden würde oder die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde“. Gesetzliche Ausnahmen von den Informationspflichten der DSGVO benennt die Verordnung in Art. 23 Abs. 1 DSGVO. Die vom BDSG n.F. genannten Vorbehalte aber passen dazu nicht oder sind jedenfalls nicht konkret genug benannt. Soweit eine Information des Betroffenen unterbleibt, sehen §§ 32 Abs. 2 und 33 Abs. 2 BDSG n.F. spezifische Informationspflichten vor; angesichts der dortigen Anforderungen sollten auch Behörden bei der Nutzung automatisierter Entscheidungsverfahren öffentlich und vorab über diesen Umstand informieren (Martini und Nink 2017).

3.2.2 Wirkungsannahmen und -grenzen datenschutzrechtlicher Transparenzvorschriften bei ADM-Systemen

Informationspflichten sind ein klassischer Steuerungsansatz im Datenschutzrecht. Der unmittelbare Schutzzweck des Datenschutzrechts ist die Gewährleistung des Rechts auf Datenschutz – ein Recht, das zentral auf der Handlungs- und Entscheidungsautonomie des Einzelnen mit Blick auf die ihn betreffenden Daten fußt. Wer wann was über eine Person weiß, soll im Entscheidungsbereich des Individuums liegen, sodass die gesetzliche Absicherung des Rechts in erster Linie auf die Ermöglichung *informierter* Entscheidungen abzielt.

Der zur Absicherung autonomer Entscheidungen nötige Wirkmechanismus informationaler Regulierung ist dabei denkbar komplex (s. Abbildung 3): Zunächst muss die für die Entscheidung notwendige Information überhaupt verfügbar gemacht werden. Dann muss diese von dem Betroffenen auch tatsächlich wahrgenommen werden. An die Wahrnehmung schließt der kognitive Prozess des Verstehens des Mitteilungsinhalts an. Das Verstehen allein reicht aber nicht, sondern der Betroffene muss die verarbeitete Information in sein eigenes Werte- und Normensystem einordnen, um für sich individuell die Relevanz der Information zu bestimmen. Nur wenn der Einzelne die Information für handlungsrelevant hält, wird er sein Handeln ggf. danach ausrichten.

Abbildung 3: Wirkungsvoraussetzungen von Transparenzpflichten bei Betroffenen (Quelle: eigene Darstellung, nach Weil et al. 2006)



Dort, wo Transparenzpflichten über diese komplexen Stufen auf bessere, weil autonomere und informiertere Entscheidungen von Endnutzern bzw. Endverbrauchern abzielen, impliziert die Rechtsordnung, dass der Betroffene stets in der Lage ist, rational und nachvollziehbar zu entscheiden und zu handeln. Dass aber gerade diese Form überlegter Entscheidungen in vielen Sachverhalten – gelinde gesagt – in den Hintergrund rückt, zeigen seit vielen Jahren die Erkenntnisse aus der Verhaltensökonomie (Howells 2005). Dort, wo Informationsverarbeitungskapazitäten erschöpft, die Aufmerksamkeitsspanne überreizt, der Aufmerksamkeitsfokus abgelenkt oder kognitive Fähigkeiten zur antizipatorischen Beurteilung von Handlungskonsequenzen beschränkt sind oder wo Oligopole, starke Netzwerkeffekte oder Lock-in-Effekte, aber auch emotionaler Druck oder objektiv wenig ökonomische Motivationen die Entscheidungsautonomie beschränken, kann auch die Ausübung des Rechts auf informationelle Selbstbestimmung mit Blick auf die Rationalität deutlich beschränkt sein. Transparenzvorschriften entsprechen vor diesem Hintergrund einem in erster Linie theoretischen Steuerungsansatz, der in der Praxis nicht automatisch zur Absicherung der autonomen Rechtsausübung führt (Edwards und Veale 2017: „transparency fallacy"). Die grundrechtssichernde Wirkung von Informationspflichten bleibt im Alltag begrenzt. Anders sähe es lediglich aus, wenn man insbesondere die Informationspflichten zur involvierten Logik so liest, dass nur Systeme eingesetzt werden dürfen, die ein bestimmtes Niveau von Erklärbarkeit gewährleisten. In diesen Fällen hätten die DSGVO-Vorgaben neben der Sicherung von Transparenz auch unmittelbare Wirkung für die Nachvollziehbarkeit von Systementscheidungen.

Insgesamt sieht die DSGVO mit den Informationspflichten aus Art. 13 Abs. 2 Buchst. f) und Art. 14 Abs. 2 Buchst. g) DSGVO Maßnahmen zur Schaffung von Transparenz bezüglich der eingesetzten Modelle vor, die theoretisch auch positive Effekte mit Blick auf die Gewährleistung der individualbezogenen Zielwerte haben können. So kann Transparenz etwa Nichtdiskriminierung sicherstellen, indem diskriminierende Kriterien aufgedeckt und beseitigt werden. Aufgrund der Verständlichkeitsanforderungen sind Umfang und Tiefe der vorzuhaltenden Informationen allerdings begrenzt, sodass insbesondere eine externe Evaluationsmöglichkeit nicht daraus folgt, die aber für das Erreichen der – individuellen, gruppenbezogenen und gesamtgesellschaftlichen – Zielwerte erforderlich wäre. Da die vorzuhaltenden Informationen in Umfang und Tiefe so zu gestalten sind, dass sie für betroffene Laien verständlich sind, bieten sie jedoch keine Grundlage für eine externe Evaluation von ADM-Systemen durch Experten. Eine derartige Überprüfung wäre jedoch erforderlich, um konkrete Risiken für individuelle, gruppenbezogene und gesamtgesellschaftliche Interessen zu erkennen.

3.3 Anforderungen an die Nutzereinwilligung bei automatisierten Entscheidungen

Auch aus den Anforderungen, die die DSGVO an datenschutzrechtliche Einwilligungen stellt, können sich Informationspflichten ergeben, die die unabhängig von einem Einwilligungserfordernis bestehenden Transparenzpflichten konkretisieren oder erweitern und so positive Effekte für die gefährdeten Rechte und Zielwerte haben können. Einwilligungsvorbehalte können dabei vor allem persönliche Autonomie und Persönlichkeitsrechte schützen, indem die Datenverarbeitung und ihre Folgen von einer informierten, bewussten Nutzerentscheidung abhängen – die Entscheidung, ob er sich einer automatisierten Entscheidung und der dazu nötigen Datenverarbeitung unterwerfen möchte, hat der Betroffene selbst.

Wie oben gezeigt ergibt sich dort die Notwendigkeit einer ADM-spezifischen Einwilligung, wo ein System rein automatisierter Entscheidungen rechtliche oder andere beeinträchtigende Konsequenzen für den Betroffenen hat und nicht ein anderer Ausnahmetatbestand vorliegt (Notwendigkeit für Vertragsabschluss/-erfüllung; gesetzliche Erlaubnis). Für die Praxis erscheint die Einwilligung für Verantwortliche als zentrale, rechtssichere Lösung für den Einsatz von ADM-Systemen. Beim Vorliegen einer entsprechenden Einwilligung können auch sensible personenbezogene Daten gemäß Art. 9 DSGVO in die Datenverarbeitung einbezogen werden. Zu differenzieren ist dabei die Einwilligung des Betroffenen in die generelle Datenverarbeitung (Art. 6 und 7 DSGVO) und die spezifische Einwilligung in die Datenverarbeitung im Rahmen eines automatisierten Entscheidungsverfahrens (Art. 22 Abs. 2 Buchst. c) DSGVO).

Für die Wirksamkeit einer Einwilligung stellt die DSGVO eine Vielzahl von Bedingungen auf, die kumulativ erfüllt sein müssen, damit sich ein Verantwortlicher bei der Datenverarbeitung auf den Ausnahmetatbestand des Art. 22 Abs. 2 Buchst. c) DSGVO berufen kann. Neben der Dokumentationspflicht aus Art. 7 Abs. 1 DSGVO treffen den Verantwortlichen Transparenzpflichten bezüglich des Inhalts und der Gestaltung der Einwilligung. Art. 4 Nr. 11 DSGVO setzt fest, dass eine Einwilligung freiwillig, in informierter Weise und unmissverständlich abgegeben werden muss. Dabei kommt es auch auf die inhaltliche Bestimmtheit der Beschreibung des Zwecks der geplanten Datenverarbeitung an. Die Einwilligung muss bei der Abgabe mit anderen Erklärungen zudem gestalterisch so hervorgehoben sein, dass die elektronische Einwilligung bewusst und eindeutig durch den Nutzer erteilt wird. Damit liegt es in der Sphäre des Verantwortlichen, Bedingungen zu schaffen, die aufseiten des Nutzers zu einem grundsätzlichen Einwilligungsbewusstsein führen und eine informierte Einwilligung gewährleisten. Auch auf die Widerrufsmöglichkeit der Einwilligung ist bereits im Vorfeld der Erklärung hinzuweisen (Art. 7 Abs. 3 DSGVO). An Einwilligungen bezüglich der Verarbeitung besonderer Kategorien personenbezogener Daten und an Einwilligungen durch Kinder und Jugendliche unter 16 Jahren stellen Art. 8 und 9 DSGVO weitere Anforderungen.

Diese inhaltlichen Anforderungen an die Einwilligung führen zu einer Transparenzpflicht auch bei ADM-Systemen, die in der Regel mit den Informationspflichten aus Art. 13 Abs. 1, 2 DSGVO gleichlaufen. Die in Art. 13 Abs. 2 Buchst. f) vorgesehene Information über das Bestehen eines ADM-Systems muss allein aus diesem Grund zwingend Teil des Einwilligungsumfangs sein; anderenfalls kann nicht von einer informierten Einwilligung ausgegangen werden. Gleiches gilt für den Fall, dass ein Verantwortlicher sein Datenverarbeitungssystem auf rein automatisierte Entscheidungen umstellt: Auch dann ist eine gesonderte Einwilligung der ggf. bisherigen Nutzer notwendig. Ist eine Einwilligung des Nutzers für ein ADM-System erforderlich, so muss sich die Informiertheit der Einwilligung auch auf die Erläuterungen der involvierten Logik sowie die Tragweite und Auswirkungen der Datenverarbeitung bei der automatisierten Entscheidung erstrecken. Nur wenn der Betroffene vor der Einverständniserteilung abschätzen kann, welche Daten in welcher Form durch das System verarbeitet werden und welche Bedeutung seine Einwilligung hat, liegt die erforderliche Informiertheit vor. Auch die Anforderungen an die Angemessenheit der Maßnahmen zur Wahrung der Rechte des Betroffenen aus Art. 22 Abs. 3 DSGVO sprechen für diese Sichtweise.

Zusätzlich sieht Art. 22 Abs. 2 Buchst. c) DSGVO eine „ausdrückliche“ Einwilligung als Ausnahmetatbestand für die Unzulässigkeit von ADM-Systemen vor. Unklar ist, inwieweit diese Vorgabe zu einer ausdrücklichen Einbeziehung des Bestehens eines ADM-Systems in das Ersuchen um die allgemeine Einwilligung in die Datenverarbeitung nach Art. 7 Abs. 2 DSGVO verpflichtet oder ob für automatisierte Entscheidungen eine davon unabhängige, zweite ausdrückliche Einwilligung erforderlich ist. Die oben beschriebenen Grenzen von Transparenz als Steuerungsressource bei individuellen Erklärungen Einzelner gelten für die datenschutzrechtliche Einwilligung allerdings umso mehr; der Ansatz des Grundrechtsschutzes durch den Vorbehalt einer freiwilligen, informierten Einwilligung in die Datenverarbeitung ist auch hier nachvollziehbar, kann aber je nach Entscheidungssituation faktisch geschwächt sein.

Das Recht des Einzelnen auf Widerruf einer einmal erklärten Einwilligung nach Art. 7 Abs. 3 DSGVO gilt grundsätzlich auch für die Einwilligung in die Datenverarbeitung durch ein ADM-System. Für die Rechtswissenschaft zu klären bleibt hier die Frage nach der Möglichkeit und dem Umgang mit einem Widerruf, der nach der Datenerhebung, aber noch vor der automatisierten Entscheidung erklärt wird.

Insgesamt erscheint der Einwilligungsvorbehalt als Ausnahmefall zulässiger ADM-Systeme theoretisch als geeignetes Instrument, um Betroffenenrechte – insbesondere die Handlungsfreiheit und das Persönlichkeitsrecht – zu gewährleisten. Sowohl mögliche kontextbezogene Schwächungen der Auswahlfreiheit, etwa durch fehlende Alternativen nicht automatischer Entscheidungssysteme, als auch die im Rahmen der Einwilligung vorzuhaltenden Informationen und ihre begrenzten Schutzwirkungen (s. Kapitel 3.2.2) sind aber greifbare Hürden für die Effektivität dieses Schutzinstruments; die Einwilligung als datenschutzrechtliches Hauptinstrument der eigenen Rechtesicherung des Einzelnen wird teils grundsätzlich kritisch hinterfragt (Radlanski 2016).

3.4 Betroffenenrechte *nach* der Verarbeitung personenbezogener Daten durch ADM-Systeme

Zielwertsichernde Instrumente enthält die DSGVO nicht nur für das Vorfeld der Datenverarbeitung. Weitere – vielleicht sogar die zentraleren – Vorgaben zum Schutz der Rechte und Freiheiten des Betroffenen sieht die Verordnung für den Zeitpunkt nach der erstmaligen Datenverarbeitung durch ein ADM-System vor. Dann nämlich weist die DSGVO dem Betroffenen eine ganze Reihe rechtlicher Ansprüche zu. Neben datenschutzrechtlichen Auskunfts- (Art. 15 DSGVO), Widerspruchs- (Art. 21 DSGVO), Berichtigungs- (Art. 16 DSGVO), Einschränkungs- (Art. 18 DSGVO) und Löschungsrechten (Art. 17 DSGVO) sollen auch das Recht auf Datenportabilität (Art. 20 DSGVO) sowie die Beschwerderechte gegenüber der Datenschutzaufsicht (Art. 77 DSGVO) und ggf. bestehende Ansprüche auf Schadenersatz (Art. 82 DSGVO) erwähnt werden. Neben diesen allgemeinen Datenschutzrechten sieht die Verordnung auch ADM-spezifische Vorgaben vor.

3.4.1 Recht auf Hinzuziehen eines menschlichen Entscheiders

Art. 22 Abs. 3 DSGVO verpflichtet die Betreiber von ADM-Systemen zu nutzerrechtssichernden Mindestmaßnahmen, darunter „mindestens“ das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung. Entgegen dem Wortlaut wird davon ausgegangen, dass Art. 22 Abs. 3 DSGVO dem Einzelnen kein subjektives, einklagbares Recht gibt, sondern in erster Linie den Verantwortlichen zu einer bestimmten Ausgestaltung des Entscheidungsverfahrens verpflichtet. Insbesondere die Verpflichtung zur Vorhaltung eines „human in the loop“, der bei einer entsprechenden Antragstellung durch den Nutzer vonseiten des Verantwortlichen zum Verfahren hinzugezogen wird, spiegelt und konkretisiert das grundsätzliche Recht des Einzelnen aus Art. 22 Abs. 1 DSGVO, nicht einer rein automatisierten Entscheidung unterworfen zu werden. Hier tritt erneut der Menschenwürdebezug deutlich zutage (Zarsky 2017). Durch diese Vorgabe wird es Betroffenen ermöglicht, eine zunächst automatisiert erfolgte Entscheidung im Nachgang durch einen Menschen sichten und unter Einbeziehung der erhobenen personenbezogenen Daten sowie der Berücksichtigung der ggf. von ihnen nachgereichten Darlegungen wieder auf eine menschgebundene Entscheidungsfindung stellen zu lassen. Damit die Hinzuziehungsmöglichkeit wie von Art. 22 Abs. 3 impliziert tatsächlich die Betroffenenrechte wahren kann, müssen mindestens zwei Voraussetzungen erfüllt sein. Zum einen muss der Hinzugezogene tatsächlich über eigene Wertungs- und Entscheidungsspielräume verfügen, um eine eigene Einschätzung und Neuentscheidung auf Grundlage der – durch die Darlegung ggf. modifizierten – Sachverhaltslage vorzunehmen und die automatisierte Entscheidung für den Einzelfall zu revidieren. Für eine eigene Bewertung müssen dem hinzugezogenen Entscheider zum anderen gerade bei komplexen Sachverhalten auch die Faktoren für die Herleitung der automatisierten Entscheidung vorliegen, um eine Neubewertung überhaupt zu ermöglichen.

In der rechtswissenschaftlichen Diskussion wird daneben argumentiert, dass das Hinzuziehungsrecht nicht ausnahmslos jedem Betroffenen zur Verfügung steht, da dies sonst im systematischen Widerspruch zu der DSGVO stünde, die in Art. 22 Abs. 3 DSGVO Anforderungen an die gemäß Abs. 2 ausnahmsweise zulässigen ADM-Systeme stellt, für die der Grundsatz der Unzulässigkeit nach Abs. 1 gilt. Stünde das Hinzuziehungsrecht jedem Einzelnen zu, wäre das Verbot-Ausnahme-Prinzip ausgehebelt, da dann theoretisch bei jeder Entscheidung die Möglichkeit einer Hinzuziehung bestünde und entsprechend der Grundsatz der Unzulässigkeit rein automatisierter Entscheidungen ausnahmslos gelten würde. Vor diesem Hintergrund wird der Hinzuziehungsanspruch auf berechtigte Einzelfälle beschränkt gesehen – „zum persönlichkeitsrechtlichen Mindestschutz automatisierter Verfahren gehört die Möglichkeit des Betroffenen, solche Spezifika zu Gehör zu bringen, die dem Einzelfall seine Einzigartigkeit verleihen“ (Martini und Nink 2017: 8). Versteht man die Einschränkung so, dass der Betroffene die Hinzuziehung eines menschlichen Entscheiders stets begründen müsste, ergäbe sich ein strukturelles Problem: Die tiefere Einsicht in das Entscheidungsverfahren ist dem Betroffenen vor allem aufgrund der Verpflichtung zu einer verständlichen Information verwehrt, sodass das Auffinden von Anhaltspunkten für einen begründeten Antrag ggf. erschwert ist. Der einzige Ausweg bliebe dann die Ausübung des Beschwerderechts gegenüber der zuständigen Aufsichtsbehörde. Man kann diese Einschränkung auf begründete Fälle allerdings auch zur Auslegung der Anforderungen an die Erklärbarkeit heranziehen: In diesem Fall müsste mindestens eine

Informationslage geschaffen werden, in der ein objektiver Dritter entscheiden könnte, dass hier ein atypischer Fall vorliegt, der die Hinzuziehung eines menschlichen Entscheiders ausnahmsweise rechtfertigt.

Mit dem Hinzuziehungsanspruch sieht die DSGVO jedenfalls ein Rechtsinstrument vor, dass die Überprüfung einer automatisierten Entscheidung durch einen Menschen im Einzelfall ermöglicht. Die von der hinzugezogenen Person vorgenommene Sichtung der ADM-Entscheidung, die Überprüfung des ggf. durch eine Stellungnahme erweiterten Sachverhalts und die Möglichkeit einer Entscheidungskorrektur erscheinen aus Sicht der Gewährleistung der oben beschriebenen normativen Zielwerte als eine zentrale Maßnahme zur Sicherung individualbezogener Rechte. Allerdings vermittelt das Hinzuziehungsrecht lediglich einen Anspruch auf eine (menschliche) Neuentscheidung, nicht auf eine aus Sicht der Betroffenen bessere Andersentscheidung; die Überprüfungsmöglichkeit mündet insoweit nicht zwingend in einem anderen Ergebnis als die angegriffene automatisierte Entscheidung. Zudem ist die Breite des Anwendungsbereichs des Hinzuziehungsrechts angesichts der noch fehlenden Praxis nicht absehbar und wirkt sich bei einer restriktiven Auslegung des Anspruchs ggf. nur auf einen Bruchteil der praxisrelevanten ADM-Verfahren aus.

3.4.2 Nachträgliches Auskunftsrecht über automatisierte Entscheidung

Ein ebenfalls speziell auf ADM-Systeme abzielender Anspruch nach der Datenverarbeitung ist das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO, das in Buchstabe h) vom Wortlaut her eine den ADM-spezifischen Informationspflichten (s. Kapitel 3.2.1) entsprechende Vorschrift enthält. Der Nutzeranspruch auf nachträgliche Auskunft umfasst damit bei automatisierten Entscheidungen neben den allgemeinen Informationen über Verarbeitungszwecke, Datenkategorien, Speicherdauer und Nutzerrechten auch hier spezifische Aussagen zu der involvierten Logik sowie Erklärungen zu der Tragweite und den angestrebten Auswirkungen der Datenverarbeitung. Beachtenswert ist dabei, dass es sich bei dem Auskunftsanspruch um ein individuelles Recht handelt, das der von der Datenverarbeitung Betroffene nach der Datenverarbeitung ausüben kann. Das kann Konsequenzen für den von der Auskunft umfassten Umfang, den Bezugspunkt sowie die Art und Weise der Informationserbringung haben. Ebenfalls vom Auskunftsanspruch umfasst sind Auskünfte über Vorkehrungen zum Erfüllen der Anforderungen aus Art. 22 Abs. 3 DSGVO, soweit es um angemessene Maßnahmen zum Freiheitsschutz geht (s. Kapitel 3.1.4). Davon umfasst können auch interne prozedurale Vorkehrungen gehören, die etwa auf die Kontrolle, Evaluierung und Optimierung der automatisierten Entscheidungsverfahren abzielen (s. Kapitel 3.5).

Ein problematisierter Aspekt an dem Auskunftsanspruch ist dagegen, dass der Verantwortliche aufgrund der möglichen Ausübung des Rechts auf Auskunft durch einen Betroffenen praktisch dazu gezwungen ist, alle entscheidungsrelevanten Daten zu speichern und für den Fall der Auskunft vorzuhalten – auch, wenn dies aus sonstigen, etwa vertraglichen Gründen, gar nicht nötig wäre. Dies stünde im Gegensatz zu den Grundsätzen der Datensparsamkeit und -minimierung. Vor diesem Hintergrund fordern einzelne Stimmen in der rechtswissenschaftlichen Diskussion jedenfalls die Möglichkeit für Verantwortliche, die Speicherung sachlich und zeitlich begrenzen zu können. Nach dem Ablauf einer solchen Frist wäre der Auskunftsanspruch dann in der Praxis nicht oder nur noch zum Teil erfüllbar.

Was nun aber inhaltlich aus dem Auskunftsanspruch aus Art. 15 Abs. 1 Buchst. h) DSGVO folgt, ist in der rechtswissenschaftlichen Diskussion umstritten. Der herausgelesene Umfang der Auskunftspflichten bei automatisierten Entscheidungen reicht von einer auf die verarbeiteten Daten und die datenverarbeitungsbezogenen Formalia begrenzten Informationspflicht – vergleichbar den Informationspflichten aus Art. 13 und 14 DSGVO (s. Kapitel 3.2; Gola 2017) über kritierienbezogene Protokollpflichten (Ernst 2017) oder die zusätzliche Mitteilung der Auswertungsergebnisse und Entscheidungen (Bäcker 2017) bis hin zu einer entscheidungsbezogenen Begründung (Goodman und Flaxman 2016). Teils wird aus dem rechtlichen Rahmen auch gelesen, dass der zulässige Einsatz von ADM-Systemen nur solche Systeme umfasst, die erklärbar sind („legible systems“, vgl. Malgieri und Comandé 2017). Die Frage, inwieweit aus den spezifischen Anforderungen an das Auskunftsrecht ein *Anspruch auf eine Begründung* der automatisierten Entscheidung erwächst („right to explanation“), wird dabei international kontrovers diskutiert (Selbst und Powles 2017). Eine Ansicht differenziert bei den Transparenzvorgaben die im Rahmen von Art. 13 und 14 DSGVO zu erbringenden Ex-ante-Informationen über die systembezogenen Konzepte und Modelle einerseits und den im Rahmen von Auskunftsansprüchen nach Art. 15

DSGVO zu erbringenden Ex-post-Erläuterungen andererseits, die auf den Einzelfall bezogene Darstellungen und damit das Herunterbrechen der abstrakten Erklärungen auf Einzel(be)wertungen umfassen (Wachter, Mittelstadt und Floridi 2017). Insgesamt wird dabei von einem begrenzten Recht auf Begründung („limited right to explanation“) gesprochen. Ein solches Recht auf Begründung aus Art. 15 Abs. 1 Buchst. h) DSGVO zu lesen, wird – insoweit bleiben die bisherigen Sichtweisen implizit – vor allem mit Blick auf mögliche Gefährdungen in die Vorschrift interpretiert. Geleitet werden diese Forderungen nach der Begründbarkeit von automatisierten Entscheidungen von dem grundsätzlichen nachvollziehbaren Ruf nach besseren Formen von Rechenschaftspflichten („accountability“) für die Verantwortlichen von ADM-Systemen, um kritisierbares Fehlverhalten und -entscheiden der Systeme zu identifizieren und zu kritisieren (zur Sicherung von „accountability“ s. Kapitel 7.2). Damit aber stellen auch diese Forderungen unmittelbar auf die ggf. verbesserungswürdigen Entscheidungen und ihren individuellen, gruppenbezogenen oder gesellschaftlichen Konsequenzen in Form eines Diskriminierungsschutzes ab.

Hier lassen die bisherigen rechtswissenschaftlichen Diskussionen eine differenzierte Auseinandersetzung mit den von der DSGVO verfolgten Schutzzwecken vermissen. Wie oben beschrieben geht es dem Datenschutz in erster Linie um datenbezogene Schutzansätze, verstanden als Vorfeldschutz aber schützt Datenschutzrecht auch nachgelagerte Grundrechte und -freiheiten (s. Kapitel 3). Die Risiken automatisierter Entscheidungen betreffen – sieht man von der dafür erforderlichen Datenverarbeitung ab – nicht zentral und unmittelbar den Schutzbereich des Datenschutzes, sondern Aspekte des verfassungsrechtlichen Persönlichkeitsrechts, soweit es um persönliche Autonomie und Aspekte der Menschenwürde geht, wenn Personen in automatisierten Verfahren zu reinen Objekten mathematisch-probabilistischer Berechnungen werden. Nicht nur datenschutzrechtliche Zielwerte wie die Achtung der Privatsphäre erscheinen mit Blick auf die automatisierten Entscheidungen und ihre Konsequenzen als gefährdet, sondern Zielwerte wie Diskriminierungsfreiheit und gruppen- und gesellschaftsbezogene Ziele, wie Teilhabe und Fairness. Inwieweit aber eine auf Antrag des Betroffenen bestehende Begründungspflicht im Sinne von Art. 15 Abs. 1 Buchst. h) DSGVO zur Sicherung dieser Schutzzwecke überhaupt geeignet ist, wird dabei nicht problematisiert. Relevant wird diese Frage aber gerade mit Blick auf die oben beschriebenen allgemeinen gestalterischen Vorgaben an den Verantwortlichen bei der Information des Nutzers. Die auch hier geltende Pflicht zur nutzerabhängigen Verständlichkeit der Information muss regelmäßig zu der Begrenzung der Tiefe und Detailliertheit der Transparenzangaben führen. Damit erscheint gerade das Auskunftsrechts des Nutzers als in der Regel zu begrenzt, um etwa einen systematischen Bias, fehlerhafte Konzeptannahmen oder Einzelgewichtungen von Entscheidungsfaktoren mit Blick auf eine Diskriminierung von Einzelnen oder Gruppen zu erkennen – zumal die Begründung des Einzelfalls keine Rückschlüsse auf die Systementscheidung in ähnlich gelagerten Fällen zulässt.

Aus dieser mit Blick auf die Schutzzweckerreichung differenzierten Interpretation der ADM-spezifischen Auskunftspflicht ergibt sich, dass eine Begründung der konkreten Entscheidung selbst nicht aus Art. 15 Abs. 1 Buchst. h) folgt. Das Auskunftsrecht des Betroffenen bezieht sich aber sehr wohl auf eine Ex-post-Erklärung des Entscheidungsmodells und die Systemfunktionalität anhand der Kategorien der verarbeiteten Daten inklusive der Darstellung der Gewichtung der Einzelfaktoren im individuellen Fall (s. auch Article 29 Working Party 2017). Das mag faktisch den Grund etwa einer negativen Entscheidung erkennbar machen, der Verantwortliche muss dabei aber weder seine Wahl der Gewichtung noch die Entscheidung im rationalen Sinn begründen, sondern lediglich über das Verfahren ihrer Herleitung informieren. Das Auskunftsrecht ist ausgerichtet auf Information über das Entscheidungsverfahren, nicht auf die Interpretation oder rechtlichen Begründung seiner Ergebnisse.

Damit hilft das Auskunftsrecht bei der Sicherung vor allem der individuell gefährdeten Rechte und Freiheiten wie Persönlichkeitsrechten und dem Interesse an einer fairen Behandlung durch ADM-Systeme. Ein tieferer Einblick in das System, der einen möglichen Entscheidungsbias und daraus ggf. resultierende Diskriminierungen distinkter Gesellschaftsgruppen ermöglichte, ergibt sich aus der Einzelfallerklärung aber nicht.

3.4.3 Exkurs: Verwaltungsrechtliche Begründungspflichten bei behördlichen Entscheidungen

Ein anderer – speziellerer – Rechtsrahmen gilt für automatisierte Entscheidungen im Bereich der öffentlichen Verwaltung, wo gesetzliche Vorgaben – wohlgemerkt aus rechtsstaatlichen, nicht datenschutzrechtlichen Gründen – eine Begründungspflicht vorsehen. Mit dem 1.1.2017 in Kraft getretenen § 35a Verwaltungsverfahrensgesetz (VwVfg) erlaubt der Gesetzgeber grundsätzlich voll automatisierte Verwaltungsentscheidungen, „sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum“ der zuständigen Behörde besteht. Für letztere Sachverhalte kommt ein automatisiertes Verfahren insoweit nicht infrage; außerdem benötigt jedes automatisierte Verwaltungsverfahren eine ausdrückliche Rechtsvorschrift.

Die verfahrensrechtlichen Vorgaben für die Begründung von Verwaltungsakten aus § 39 VwVfG gelten dann aber auch für automatisierte Entscheidungen. Danach ist grundsätzlich jeder schriftliche oder elektronische Verwaltungsakt mit einer Begründung zu versehen, die „die wesentlichen tatsächlichen und rechtlichen Gründe“ für die Entscheidung enthält (§ 39 Abs. 1 S. 2 VwVfG). Ausnahmsweise kann von einer Begründung abgesehen werden, wenn etwa ein Antrag positiv beschieden wird und der Verwaltungsakt nicht in Rechte Dritter eingreift oder wenn die Behörde „Verwaltungsakte mit Hilfe automatischer Einrichtungen erlässt und die Begründung nach den Umständen des Einzelfalls nicht geboten ist“ (§ 39 Abs. 2 Nr. 3 VwVfG). Die Bewertung einfach gelagerter Sachverhalte und entsprechende Verwaltungsakte können insoweit nicht nur automatisch erfolgen, sie benötigen auch keiner Begründung. Verwaltungsverfahren, bei denen ein Ermessen oder ein Beurteilungsspielraum der Behörde eröffnet ist, können dagegen nicht automatisiert werden. Begründungsfrei sind nur solche Verfahren, bei denen der Anwendungsbereich des § 35a VwVfG eröffnet ist und die – mit Blick auf den Einzelfall – keine Begründung erfordern. Die rechtliche Analyse der Vereinbarkeit der verwaltungsrechtlichen Vorgaben zu automatisierten Entscheidungen mit den DSGVO-Anforderungen bleibt aber selbst für diese Fälle insgesamt schwierig (Martini und Nink 2017).

Für aus rechtsstaatlicher Sicht vorteilhafte automatisierte Entscheidungen und solche bei einfachen Fällen sieht das VwVfG damit keine Begründungspflichten vor; für alle anderen ADM-Systeme der Verwaltung aber gilt der Grundsatz der Begründungspflicht, die über das Maß der datenschutzrechtlichen Erklärung hinausgeht. Hier sehen rechtsstaatliche Grundsätze eine Begründung der automatisierten Entscheidung im Rechtssinne vor bzw. verbieten ADM-Systeme in Fällen verwaltungsrechtlicher Spielräume ganz. Damit erscheint die Gewährleistung der individualbezogenen Rechte und Freiheiten in verwaltungsrechtlichen Sachverhalten besonders hoch.

3.5 System- und verfahrensbezogene Pflichten der Anbieter von ADM-Systemen

Neben den direkten, dem Nutzer gegenüber zu erbringenden Transparenzpflichten und den aus Nutzerrechten erwachsenden Anforderungen an die Gestaltung von automatisierten Entscheidungsverfahren können sich aus DSGVO-Vorschriften auch prozessbezogene bzw. systemgestaltende Pflichten ergeben, die die oben beschriebenen Zielwerte – ggf. mittelbar – mit gewährleisten können. So können qualitative Anforderungen an den Einsatz bestimmter automatisierter Berechnungs- bzw. Entscheidungsverfahren, aber auch prozessbezogene Vorgaben an die Konzept- und Implementationsphase dabei helfen, die Interessen und Rechte von Einzelnen, Gruppen und ggf. sogar der Gesellschaft zu gewährleisten.

3.5.1 Verpflichtende Nutzung anerkannter mathematischer Verfahren?

Ein Mindestmaß an Qualitätssicherung bei der Konzeption automatisierter Entscheidungssysteme kann theoretisch dadurch erfolgen, dass der Verantwortliche auf die Nutzung anerkannter mathematischer Verfahren begrenzt ist. Eine solche Vorgabe macht § 31 BDSG n.F. für Scoringverfahren, d. h. für einen engeren Anwendungsbereich als Art. 22 Abs. 1 DSGVO. Aus den Anforderungen an ausnahmsweise zulässige ADM-Systeme (Art. 22 Abs. 3 DSGVO) ergibt sich dagegen keine explizite Beschränkung auf anerkannte Verfahren. Dagegen geht der Verordnungsgeber in Erwägungsgrund 71 der DSGVO davon aus, dass Verantwortliche „geeignete mathematische oder statistische Verfahren für das Profiling verwenden“ sollten. Angesichts der Unverbindlichkeit der Erwägungsgründe und der lediglichen Sollformulierung dort kann sich eine Pflicht zur Nutzung anerkannter mathematischer Verfahren nur im Rahmen der Interpretation anderer Vorschriften der DSGVO ergeben.

Infrage kommen dabei die generelle Pflicht zur Einziehung angemessener Maßnahmen zur Sicherung der Betroffenenrechte bei dem Einsatz von ADM-Maßnahmen aus Art. 22 Abs. 3 DSGVO, die Generalnorm zur Übernahme der Verantwortung durch den Verantwortlichen in Art. 24 Abs. 1 DSGVO, die Berücksichtigung des Stands der Technik bei der Systemkonzeption anhand des Privacy-by-Design-Grundsatzes sowie ggf. die Anforderungen mit Blick auf die Datensicherheit aus Art. 32 Abs. 1 DSGVO. Alle vier Normen verpflichten den Verantwortlichen dazu, zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen des Betroffenen angemessene Maßnahmen zu treffen. Dies schließt aber grundsätzlich die Nutzung von (bislang) nicht anerkannten mathematischen Verfahren nicht aus. Soweit aus den Vorschriften – bei Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO sogar explizit – gelesen wird, dass der Verantwortliche sich an dem Stand der Technik zu orientieren hat, kann die Beschränkung auf anerkannte Verfahren aber ein deutliches Indiz für eine solche Orientierung sein. Die Nutzung ausschließlich anerkannter mathematischer Verfahren kann insoweit indizielle Relevanz bei der Prüfung der Angemessenheit der Maßnahmen entfalten – eine unmittelbare Pflicht auf die Wahl derartiger Verfahren ergibt sich daraus jedoch nicht, soweit der Anbieter lediglich zur Orientierung am Stand der Technik verpflichtet ist und gleichwertige eigene Verfahren einsetzt. Eine derartige restriktive Interpretation wiese zudem das Risiko der Bildung von Algorithmen- oder ADM-Systemmonokulturen auf, für die das oben erwähnte Risiko einer stark begrenzten Systemvielfalt virulent würde. Die Pflicht zur Orientierung am Stand der Technik kann aber dem Grunde nach ausschließen, dass hochgradig fehleranfällige und vollkommen ungeprüfte ADM-Verfahren eingesetzt werden.

3.5.2 Berücksichtigung von „Privacy by Design“

Die DSGVO sieht spezifische Anforderungen an die technische Gestaltung von Datenverarbeitungssystemen vor (Art. 25 Abs. 1 DSGVO). Der als „Privacy by Design“ bezeichnete Steuerungsansatz verpflichtet den Verantwortlichen mit dem Ziel des Rechtsschutzes der Betroffenen zu einer frühestmöglichen – etwa im Rahmen der Produktentwicklung – und auch nach der Systemimplementation andauernden und systematischen Berücksichtigung datenschutzrechtlicher Belange. Dabei gelten die Grundsätze der Datenvermeidung und -minimierung sowie der möglichen Datenanonymisierung und Pseudonymisierung als Richtschnur. Ausdrücklich soll der Verantwortliche dabei technische und organisatorische Maßnahmen treffen, also neben systembezogenen Vorkehrungen auch prozedurale Maßnahmen wie Schulungen oder interdisziplinär besetzte Projektgruppen. Abhängig ist der Umfang der einzuziehenden Maßnahmen von Art, Umfang und den Zwecken der Datenverarbeitung, den damit verbundenen Risiken für den Betroffenen und den für die Implementierung nötigen Kosten. Die Nichtbeachtung dieser Pflichten ist – anders als der im bisherigen § 3a BDSG enthaltene Programmsatz – bußgeldbewehrt.

Die aus dem Einsatz von automatisierten Entscheidungsverfahren erwachsenden Gefährdungen für die Freiheiten und Rechte des Einzelnen sind auf Grundlage dieser Vorschrift im Rahmen der Verfahrensausgestaltung systematisch zu berücksichtigen und ihre Realisierung ist auf Grundlage eines Risikomanagementansatzes durch entsprechende Gegenmaßnahmen zu verhindern. Die Berücksichtigung gruppen- und gesellschaftsbezogener Risiken ist von Art. 25 Abs. 1 DSGVO dagegen nicht einbezogen.

3.5.3 Weitere Pflichten mit möglichen positiven Effekten

Eine Reihe weiterer Vorschriften der DSGVO ist – vergleichbar mit der beschriebenen Verpflichtung datenschutzfreundlicher Technik- und Organisationsausgestaltung aus Art. 25 Abs. 1 DSGVO – zusätzlich in der Lage, aufseiten des Verantwortlichen für einen datenschutzrisikoreflektierten Umgang zu sorgen. Dazu zählen zentral Art. 30 DSGVO mit der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten und die aufgrund von Art. 35 Abs. 3 Buchst. a) DSGVO für ADM-Systeme verpflichtende Vornahme einer datenschutzbezogenen Folgeabschätzung nach Art. 35 DSGVO („Datenschutz-Folgenabschätzung“ (DSFA), englisch: „Data Protection Impact Assessment“ (DPIA)). Beide Vorgaben zusammen führen über Art. 25 Abs. 1 DSGVO zu einer frühen Reflexion über die geplanten Datenverarbeitungsvorgänge im Einzelnen und deren jeweilige Übereinstimmung mit den Vorgaben der DSGVO. Dort, wo Privacy by Design risikomanagementbasiert analysiert und evaluiert – also Risiken minimiert, nicht aber grundsätzlich ausschließt –, zielt die DSFA auf die Identifizierung und das Abstellen jedweden DSGVO-Verstoßes aus Nutzersicht ab. Die Prüfung im Rahmen der DSFA umfasst dabei nicht nur die

technischen Systeme zur Datenverarbeitung und -speicherung, sondern auch die organisatorischen Vorkehrungen aufseiten des Verantwortlichen. Insgesamt führt Art. 35 DSGVO zu einer systematischen Selbstevaluation von Technik und Prozessen beim Einsatz von ADM-Systemen. Wie die DSGVO selbst ist die DSFA-Perspektive dabei aber beschränkt auf die Rechte und Freiheiten sowie die berechtigten Interessen des Einzelnen.

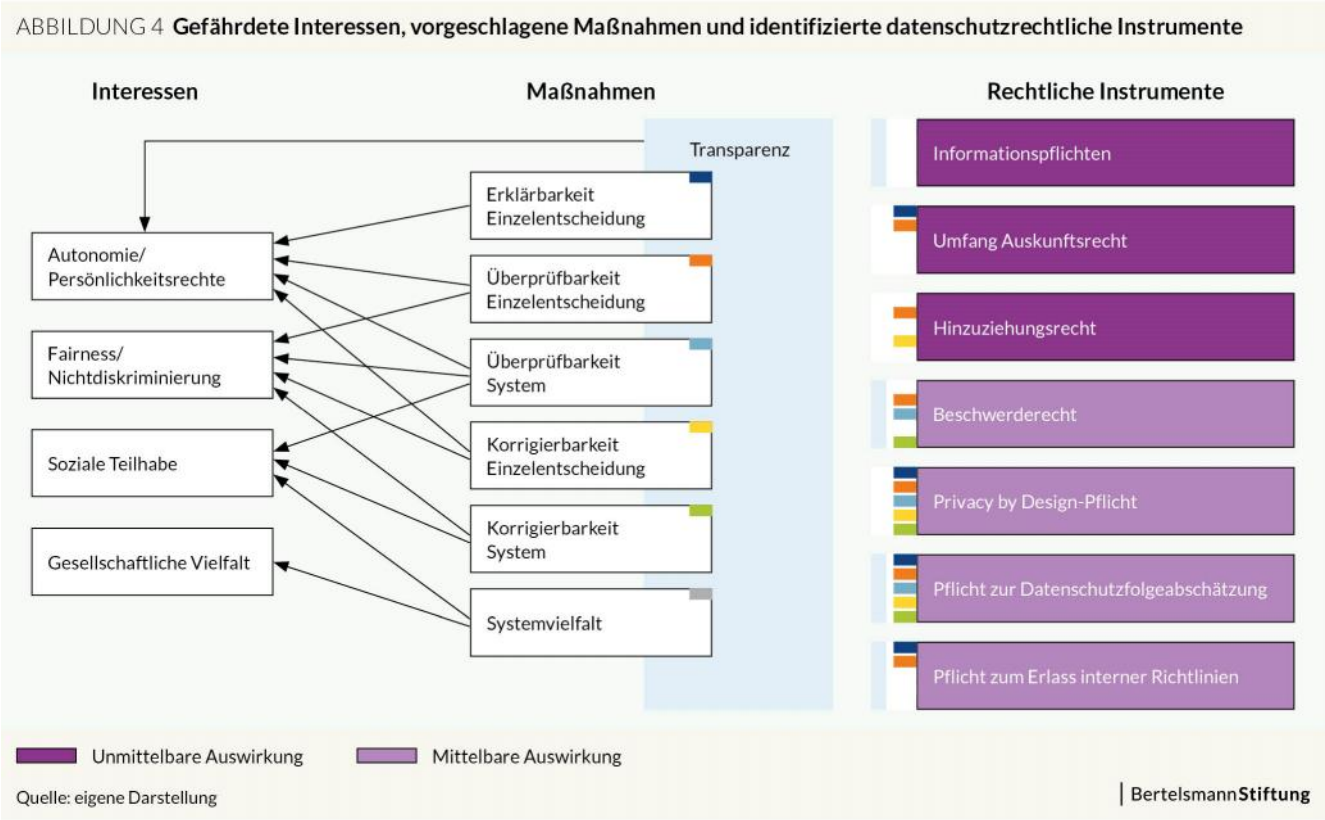
Flankiert werden diese Pflichten durch Art. 47 DSGVO, der den Erlass interner Datenschutzvorschriften bei ADM-Systemen zwingend vorsieht (Art. 47 Abs. 1 Buchst. e)). Diese Vorschriften müssen Regelungen hinsichtlich der Betroffenenrechte enthalten und können so für einen hohen Grad an Datenschutzbewusstsein aufseiten des Verantwortlichen sorgen. Auch die Bestellung eines Datenschutzbeauftragten kann zu einer systematischen Einbeziehung der datenschutzrechtlichen Perspektive bei Planung, Implementation und interner Evaluation helfen. Eine verpflichtende Bestellung beim Einsatz von ADM-Systems ergibt sich aus Art. 37 DSGVO für Anbieter von ADM-Systemen zunächst nicht. Hier sieht aber die Spezialvorschrift aus § 38 Abs. 1 S. 2 BDSG n.F. vor, dass Verantwortliche einen Datenschutzbeauftragten zu bestellen haben, wenn sie nach Art. 35 DSGVO zur Vornahme einer Datenschutz-Folgeabschätzung verpflichtet sind. Dies ist wie oben gezeigt der Fall, sodass sich jedenfalls für Anbieter von automatisierten Entscheidungsverfahren mit Niederlassung in Deutschland eine Pflicht zur Bestellung eines Datenschutzbeauftragten ergibt.

4 Was die DSGVO leisten kann: Ansätze zur Absicherung individueller Interessen

Nach der Bündelung der durch ADM-Systeme gefährdeten Zielwerte und möglicher Gegenmaßnahmen sowie der Identifikation der gesetzlichen Vorgaben von DSGVO und BDSG für automatisierte Entscheidungen mit Schutzpotenzial ist deren Abgleich möglich. Dort, wo keine Schutzinstrumente bestehen, ergeben sich Risikofelder, die rechtlich kaum gerahmt sind und die entsprechend derzeit keine zielwertschützenden Gegenmaßnahmen anbieten. Wichtig ist dabei der Hinweis, dass es sich bei diesem Mapping um hypothetische Schutzauswirkungen handelt: Weder die DSGVO noch das BDSG n.F. sind in Kraft, viele der unbestimmten Rechtsbegriffe und Norminterpretationen sind Gegenstand teils heftiger wissenschaftlicher und politischer Debatten und werden erst nach Inkrafttreten durch Datenschutzpraxis, Aufsichtsbehörden und gerichtliche Spruchpraxis in einen mehr oder wenigen rechtssicheren Status quo überführt werden.

Zur Klärung der Frage, inwieweit der datenschutzrechtliche Rechtsrahmen ab Mai 2018 zur Sicherung der normativen Zielwerte beitragen kann, werden die Zielwerte und die zu ihrer Gewährleistung geforderten Maßnahmen mit den datenschutzrechtlichen Instrumenten des Rechtsrahmens für ADM-Systeme abgeglichen (s. Abbildung 4).

Abbildung 4: Gefährdete Interessen, vorgeschlagene Maßnahmen und identifizierte datenschutzrechtliche Instrumente (Quelle: eigene Darstellung)



Die rechtliche Analyse hat gezeigt, dass der aus DSGVO und BDSG n. F. ergebende Rechtsrahmen Instrumente aufweist, die positive Auswirkungen auf einzelne oder mehrere der geforderten Zielwerte haben können. Diese wirken dabei teils direkt über nutzerbezogene Informationspflichten, Rechte und Antragsmöglichkeiten, teils nur mittelbar durch die Verpflichtung der datenverarbeitenden Stellen zu systembezogenen Vorkehrungen und Ex-ante-Evaluationen und -Bewertungen.

4.1 Transparenzvorgaben stärken Autonomie und Persönlichkeitsrechte der Nutzer

Informationspflichten und Auskunftsrechte sind grundsätzlich dazu in der Lage, auf der Seite des Betroffenen Transparenz herzustellen. Das dadurch zur Verfügung gestellte Wissen über die Existenz und geplante Nutzung eines ADM-Systems, über die Art der erhobenen Daten und die Zwecke der Datenverarbeitung kann dem Betroffenen bei der Einschätzung der Relevanz der Verarbeitung und Entscheidung für seine Autonomie und sein Persönlichkeitsrecht helfen. In Fällen von ADM-Systemen, für die der Verantwortliche eine Einwilligung des Nutzers benötigt, verbessert das Erfordernis einer ausdrücklichen Einbeziehung des Umstands eines automatisierten Entscheidungsverfahrens die Wahrnehmung der Persönlichkeitsrechte. Auf beiden Ebenen bleibt jedoch die begrenzte Wirksamkeit dieser Formen von Transparenz als Grundlage für bewusste und rationale Nutzerentscheidungen. Transparenz führt aber nicht automatisch zu einer Optimierung der Grundrechtewahrnehmung; sie kann die Entscheidungsgrundlage des Betroffenen verbessern, muss es aber nicht (s. Kapitel 3.2.2). Die Informationspflichten richten sich zudem nach der jeweiligen Verstehensmöglichkeit des kontextabhängigen durchschnittlichen Nutzers. Die Informationstiefe bei Informations- wie bei Auskunftspflichten ist so durch die Anforderungen insbesondere an die Verständlichkeit des zur Verfügung gestellten Wissens begrenzt.

Die auf die Einzelentscheidung bezogene Auskunftspflicht inklusive aussagekräftiger Informationen zur involvierten Logik gehen hier weiter, da der Verantwortliche auch auf die Einzelfaktoren der Entscheidung und ihre Relevanz für den Entscheidungsausgang eingehen muss – allerdings auch hier in einer begrenzten, für den Auskunft beantragenden Nutzer verständlichen Form (s. Kapitel 3.4.2). Das Auskunftsrecht ermöglicht es dem Betroffenen jedenfalls für den Einzelfall, die Nachvollziehbarkeit und Richtigkeit grob einzuschätzen und bei der Vermutung einer diskriminierenden Behandlung weitere Rechte geltend zu machen. Als Ansatz für den Schutz der Persönlichkeitsrechte und die Gewährleistung von individueller Fairness und sozialer Teilhabe des Einzelnen sind die erweiterten Auskunftsrechte bei ADM-Systemen insoweit geeignet.

4.2 Hinzuziehungsrechte gewährleisten einen „human in the loop“

Für den Fall einer vermeintlichen Fehlentscheidung oder einer gefühlt unfairen Behandlung hat der Verantwortliche das Verfahren so auszugestalten, dass der Betroffene die Hinzuziehung einer menschlichen Person beantragen kann. Vom Verantwortlichen ernstgenommen führt das Hinzuziehungsrecht so zu einer menschlichen Neubewertung und -entscheidung aufseiten des Anbieters, bei der auch außergewöhnliche Sachverhalte und Sondersituationen in die Entscheidung einbezogen werden können, die von dem ADM-System nicht berücksichtigt werden (konnten). Wie oben gezeigt eröffnet eine Interpretation der DSGVO als Mindestanforderung, dass der Betroffene jedenfalls aus der Erklärung herauslesen können muss, ob er einen Sonderfall darstellt, der ihn ausnahmsweise zum Berechtigten des Hinzuziehungsrechts werden lässt. Das wichtige Hinzuziehungsrecht ermöglicht inzident eine Überprüfung der vom System getroffenen Einzelentscheidung, ist aber vor allem auf die Möglichkeit des menschlichen Neuentscheidens gemünzt. Das Hinzuziehungsrecht erscheint damit als zentrales Rechtsinstrument für die Überprüfungs- und Korrigierbarkeitsmöglichkeit einer einmal getroffenen automatisierten Entscheidung. Beides – Überprüfbarkeit und Korrigierbarkeit – unterstützt die Gewährleistung von Persönlichkeitsrechten und Fairness als normative Zielwerte.

4.3 Positive mittelbare Effekte system- und verfahrensbezogener Vorgaben

Die umfassenden Verpflichtungen von ADM-Systemanbietern zur Beachtung von Privacy-by-Design-Prinzipien, zur Durchführung datenschutzrechtlicher Folgeabschätzungen, die Erstellung interner Richtlinien sowie die Bestellungspflicht eines Datenschutzbeauftragten sind in der Lage, auf Anbieterseite ein hohes Reflexionsniveau mit Blick auf mögliche Risiken des eigenen ADM-Verfahrens herzustellen. So entsteht ein starkes Bewusstsein für die Rechte der Betroffenen, die bereits im frühen Konzeptionsstadium mitgedacht werden müssen und auch nach

Implementierung des Systems für die laufende Kontrolle richtungsgebend sind. Auch die Bestellung eines Datenschutzbeauftragten führt zu einer strukturellen Verortung der Berücksichtigung datenschutzrechtlicher Belange in der Organisation. Insgesamt weisen die system- und verfahrensbezogenen Vorgaben so eine hohe Relevanz für die Berücksichtigung normativer Zielvorgaben auf: Umfassende Berücksichtigungs- und Abschätzungspflichten mit Blick auf die Wahrung der Nutzerrechte haben das Potenzial, dass Verantwortliche ADM-Systeme im Konzeptions- und Implementationsprozess mögliche Risiken für Einzelne – und strukturell auch für Personengruppen (s. Kapitel 5) – frühzeitig erkennen und minimieren können. Für die laufende Kontrolle des Systems – dazu zählt auch die Berücksichtigung der Anfechtungs- und Hinzuziehungsfälle und ihre Hinweise auf eine Fehlfunktion – entwickeln die systembezogenen Pflichten einen starken Anreiz, einfache Verfahren zur Überprüfung und Korrektur von Einzelentscheidungen sowie zum Monitoring des Systems im laufenden Betrieb einzuführen. Nicht zuletzt, weil durch das bestehende Beschwerderecht der Betroffenen jederzeit die zuständige Datenschutzaufsicht hinzugezogen werden kann. Die Verpflichtung, bei der Konzeption und Ausgestaltung von ADM-Verfahren „angemessene Maßnahmen [zu treffen], um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren“ (Art. 22 Abs. 3 DSGVO), zielt dabei auf individuelle Nutzerrechte und -freiheiten und ermöglicht bei Erkennung von Fehlfunktionen interne Maßnahmen des Verantwortlichen, wie die Überprüfbarkeit und Korrigierbarkeit von Einzelentscheidungen und vom Gesamtverfahren, was zu der Gewährleistung von Persönlichkeitsrechten, Fairness und sozialer Teilhabe vor allem des Einzelnen beiträgt.

Da es sich bei den systembezogenen Pflichten um interne Maßnahmen des Verantwortlichen handelt, kommt es für die tatsächliche Umsetzung allerdings auf ein wirksames Anreizsystem an. Die DSGVO und das BDSG n.F. arbeiten dabei mit dem klassischen Ansatz institutionalisierter verwaltungs- und ordnungsrechtlicher Kontrollstellen: den Datenschutzbeauftragten der Länder und des Bundes als institutionalisierten Aufsichtsbehörden (s. dazu Kapitel 4.4).

4.4 Rolle und Möglichkeiten der Aufsichtsbehörden zur Zielwertsicherung

Die Aufsicht über die Einhaltung der gesetzlichen Vorgaben aus DSGVO und BDSG führen die jeweils zuständigen Datenschutzbehörden. Zu ihren zentralen Aufgaben gehört, die Anwendung der DSGVO zu überwachen und durchzusetzen (Art. 57 Abs. 1 Buchst. a) DSGVO). Zu diesem Zweck sind die Aufsichtsstellen mit weitreichenden Einsichtsbefugnissen und Zugangsrechten ausgestattet (Art. 58 Abs. 1 DSGVO), darunter unter anderem die Befugnis

- „den Verantwortlichen, den Auftragsverarbeiter und ggf. den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind“ (Buchst. a)),
- „Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen“ (Buchst. b)),
- „von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten“ (Buchst. e)), und
- „Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten“ (Buchst. f)).

Vor allem in der Kombination dieser Befugnisse wird deutlich, dass die Einsichtnahme und Informationsansprüche der Behörden – anders als die der Betroffenen – nicht durch Anforderungen wie Verständlichkeit oder die Eingrenzung auf den Einzelfall begrenzt sind. Der Prüfungsmaßstab der Aufsichtsbehörden ergibt sich aus ihrer Aufgabe der Überwachung und Durchsetzung der DSGVO-Normen. Schutzrichtung der DSGVO sind wie gezeigt das Recht auf Datenschutz sowie die sonstigen Grundrechte und -freiheiten des Einzelnen. Damit ist grundsätzlich auch der Fokus der aufsichtsführenden Stellen begrenzt auf Verletzungen von individuellen Rechtsgütern oder Risiken für diese (s. aber auch Kapitel 5). Die Aufsichtsstellen sind im Rahmen ihrer Kompetenzen befugt, auf alle Datenverarbeitungsanlagen inklusive die dort laufenden Programme und Datenbanken zuzugreifen. Sie können so die Einhaltung der DSGVO-Vorschriften sehr nah am automatisierten Entscheidungsverfahren prüfen.

Dort, wo ggf. internes Wissen des Verantwortlichen nötig ist, trifft diesen eine umfassende Auskunftspflicht gegenüber der Aufsichtsbehörde. Damit ist die von der DSGVO umrissene Governancestruktur im Datenschutz theoretisch in der Lage, starke Anreize für die tatsächliche Umsetzung der system- und prozessbezogenen Pflichten durch die Verantwortlichen zu setzen. Wenn den Regelungsadressaten bewusst ist, dass alle Konzepte, Folgenabschätzungen und Programme mit ADM-Bezug im Rahmen eines Datenschutzaudits durch die Datenschutzbehörden eingesehen werden können, erhöht dies die Motivation des Verantwortlichen deutlich, entsprechende Projektphasen besonders aufmerksam durchzuführen. Insoweit ist die durch DSGVO und BDSG n.F. vorgesehene Governancestruktur grundsätzlich in der Lage, die Umsetzung der system- und entwicklungsbezogenen Vorgaben zu gewährleisten – und damit die genannten Zielwerte zu unterstützen. In der Praxis wird zu diesen strukturellen Überlegungen vor allem ein entsprechender Kontrolldruck erzeugt werden müssen; inwieweit das mit Blick auf die teils beobachtbaren Kapazitätsgrenzen der Datenschutzbehörden gelingen wird, bleibt abzuwarten.

4.5 Zwischenfazit: Ansatzpunkte in der DSGVO als Grundlage für Maßnahmen zur Absicherung individueller Zielwerte

Datenschutzrecht schützt im Kern Rechte und Freiheiten des Einzelnen: direkt und unmittelbar Handlungsautonomie und Persönlichkeitsrechte, insbesondere das Recht auf Privatsphäre, als Vorfeldrecht aber auch die durch automatisierte Datenverarbeitungen gefährdete Ausübung anderer Grundrechte und -freiheiten. Der individualrechtebezogene Rechtsrahmen ist dabei grundsätzlich in der Lage, eine für den Betroffenen nützliche Transparenz über Funktionsweise und Modelle von ADM-Systemen im jeweiligen Einzelfall herzustellen. Auch die explizite Aufklärung darüber, dass eine automatisierte Entscheidung im Nachgang zur Datenverarbeitung beabsichtigt ist, ermöglicht es dem Einzelnen, eine autonomiewahrende Entscheidung zu treffen. Dabei sind Umfang und Detailgrad der Informationen aber durch die vorgeschriebene Verständlichkeit aus Nutzersicht begrenzt. Hinzu tritt der Umstand, dass Informationspflichten gegenüber dem Endnutzer nur eine begrenzte Wirkung mit Blick auf die (rationale) Wahrnehmung der eigenen Handlungsautonomie haben. Das von Darlegungs- und Anfechtungsrecht gerahmte Recht auf Hinzuziehung einer menschlichen Person mit der anbieterseitigen Möglichkeit einer nachträglichen Kontrolle und Neubescheidung ist gut für die Korrigierbarkeit automatisierter Entscheidungen, hat aber keinen Vorteil für ein tieferes Verständnis der zugrunde gelegten Annahmen und Konzepte durch den Betroffenen. Die Betroffenenrechte der DSGVO helfen damit – in Grenzen – bei der Erreichung normativer Zielwerte wie Handlungsautonomie und Persönlichkeitsrechtsschutz und können Einzelfälle individueller Diskriminierung korrigieren.

Die system- und entwicklungsbezogenen Vorgaben der DSGVO können daneben – untermauert durch umfangreiche Aufsichts- und Kontrollbefugnisse der Datenschutzbehörden – zu einer systematischen Berücksichtigung und hohen Aufmerksamkeit der Anbieter automatisierter Entscheidungsverfahren im Hinblick auf mögliche Rechtsgefährdungen Einzelner führen. Ein hoher Reflexionsgrad und starke Anreize zur Etablierung von risikozentrierten Prozessen können in der Praxis dazu führen, dass automatisierte Entscheidungen in der Konzeptions- und Implementationsphase besonders verantwortungsbewusst vom Verantwortlichen behandelt werden und Verfahren der Überprüfbarkeit und Korrigierbarkeit vorgehalten werden. Der Nachteil dieser Verpflichtungen aber bleibt, dass diese Form der Sicherung ausschließlich innerhalb interner, nicht öffentlicher Überlegungen und Entwicklungsverfahren stattfindet. Damit ergibt sich eine mögliche positive Wirkung nur mittelbar.

5 Was die DSGVO nicht leisten kann: Offene Flanken insbesondere für gruppen- und gesellschaftsbezogene Interessen

Das Regelungsziel der DSGVO bleibt der Schutz von Individualrechten bzw. Grundrechten und -freiheiten des Einzelnen. Die Perspektive eines „strukturellen Grundrechtsschutzes“, d. h. der Sicherung etwa der Vorbedingungen von demokratischen Prozessen und gesellschaftlicher Teilhabe durch die gesellschaftsweite Gewährleistung von Autonomie des Einzelnen deckt nutzerbezogener Datenschutz nicht unmittelbar ab. Individualbezogener Schutz von Rechten und Freiheiten ist daneben nicht in der Lage, gruppenbezogene Zielwerte systematisch mit abzusichern:

Soweit ADM-spezifische Informationspflichten (im Rahmen der Datenerhebung, der Einwilligung, der Verarbeitung oder der Auskunft) die Pflicht zur Verfügungstellung aussagekräftiger Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person enthalten, wird davon nicht die Offenlegung tiefer gehender Entscheidungsparameter und -gewichtungen, der genutzten Algorithmen und ihrer Kombination, des Quellcodes oder der möglichen sozialen Wechselwirkungen umfasst. Die zu erbringenden Informationen über die involvierte Logik einer automatisierten Entscheidung vor der Datenerhebung bleiben auf einem abstrakten Niveau und umfassen das zugrunde liegende Konzept und Informationen über die Datenkategorien sowie das Entscheidungsmodell. Dadurch ist ein Blick in die Tiefen des ADM-Systems nicht möglich; die Möglichkeit struktureller Diskriminierungen lässt sich so regelmäßig nicht erkennen. Mit Blick auf die Auskunftsrechte von Nutzern ist deutlich geworden, dass der Verantwortliche die Entscheidung selbst und die vom System angelegten Gewichtungen nicht begründen muss. Aufgrund der Einzelfalldarstellung ergeben sich auch nicht automatisch Rückschlüsse auf eine mögliche systematische beabsichtigte oder unbeabsichtigte Diskriminierung. Dazu wäre der Zugriff auf eine Vielzahl von Einzelentscheidungen nötig. Auch das für den Einzelnen positive Hinzuziehungsrecht ermöglicht eine system- bzw. verfahrensbezogene Überprüfbarkeit oder die Möglichkeit einer einzelfallübergreifenden Evaluation eines ADM-Systems nicht. Oder anders gesagt: Die für die Einschätzung gruppen- oder gesellschaftsbezogener Risiken erforderliche Transparenz weicht in ihrer Tiefe und ihrem Umfang von dem Transparenzverständnis der Art. 12, 13, 14, 15 und 22 DSGVO, die der Sicherung individueller Grundrechte dienen, ab.

Immerhin können Teile der system- und entwicklungsbezogenen Vorgaben der DSGVO positive (Neben-)Wirkungen für das Erreichen überindividueller normativer Zielwerte haben. Insbesondere die Vorschriften zur systematischen Berücksichtigung von Privacy-by-Design-Konzepten, die Pflicht zu einer Verzeichniserstellung der Datenverarbeitungsvorgänge und die für ADM-Systeme bestehende Pflicht der Durchführung einer datenschutzrechtlichen Folgeabschätzung, aber auch der Erlass interner Datenschutzvorschriften können bei der Etablierung von Entscheidungs- und Entwicklungsprozessen helfen, die jedenfalls auch gruppenbezogene Risiken intern adressieren. Bezogen ist der Blick der internen Prüfungen dabei wie gezeigt auf die Risiken für individuelle Rechte. Da durch systemweite Entscheidungen aber ggf. auch eine Vielzahl von Individuen in ihren Rechten verletzt sein kann, hat der Verantwortliche eine intrinsische Motivation für einen systemweiten Blick möglicher überindividueller Risiken. Durch den tiefen Einblick in das System kann der Verantwortliche hier auch Fehler entdecken, die ganze Nutzergruppen betreffen können. Die systemische Sicht muss insoweit auch und insbesondere auf systematische Risiken abzielen, bleibt aber eine interne Prüfung.

Das macht einen Blick auf die Rolle der Datenschutzbehörden nötig: Durch ihre umfangreichen Auskunfts- und Zutrittsrechte schafft die DSGVO eine Governancestruktur, die die Qualität und die Motivation einer risikofokussierten Entwicklung und Implementation von ADM-Systemen aufseiten des Verantwortlichen deutlich verbessern kann. Abhängig wird die Wirksamkeit dieser mittelbaren Effekte von dem durch die Datenschutzstellen in der Praxis aufgebauten Aufsichts- und Kontrolldruck sein. Der Fokus auch bei den Aufsichtsbehörden ist gerichtet auf die Sicherung individueller Rechte und Freiheiten. Da durch systematische Diskriminierungsmöglichkeiten bei ADM-Systemen eine Vielzahl einzelner Individuen in ihren Rechten betroffen sein kann, ist der Behördenblick bei

Datenschutzaudits grundsätzlich auch auf Gefährdungen gruppenbezogener Interessen eröffnet. Allein die Erreichung gesamtgesellschaftlicher Zielwerte als Aufsichtsperspektive ist den Datenschutzstellen mit Blick auf Kontrollen verwehrt.

An dieser Stelle aber können die erweiterten Aufgaben der Datenschutzbehörden ggf. helfen. Nach Art. 57 Abs. 1 Buchst. b) sollen die Aufsichtsbehörden neben der Kontrolle und Durchsetzung der Datenschutzvorschriften auch die „Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären". Diese Informations- und Sensibilisierungsaufgabe kann – theoretisch – als Möglichkeit dafür gesehen werden, dass die Behörden im Rahmen ihrer Tätigkeiten über die Individualrechtsrisiken hinaus auch soziotechnische Entwicklungen oder mögliche Risiken für gesamtgesellschaftliche Interessen jedenfalls im Blick behalten und ihre Erkenntnisse in diesem Feld kundtun. So kann diese „Metaperspektive" bei einer Vielzahl von Einzelprüfungen etwa zu dem Ergebnis führen, dass die Vielfalt von ADM-Systemen in einzelnen Wirtschaftsbereichen begrenzt ist und daraus zusätzliche Gefahren für soziale Teilhabe erwachsen (s. Kapitel 2). Dafür sind die Behörden angesichts der Vielzahl der datenverarbeitenden Stellen auch auf Hinweise von Betroffenen angewiesen – so erlangt das Beschwerderecht des Betroffenen aus Art. 77 Abs. 1 DSGVO besondere Relevanz auch über den individuellen Rechtsschutz hinaus.

Insgesamt hat die Einzelnutzerzentrierung aber Folgen für die Gewährleistung der oben beschriebenen normativen Zielwerte und Schutzmaßnahmen: Eine tiefgehende Überprüfbarkeit der in der ADM-Prozesslogik hinterlegten Annahmen und Wertungen mit Blick auf deren Risiken für vor allem überindividuelle Zielwerte ergibt sich aus den Informationspflichten, Nutzerrechten und systembezogenen Vorgaben nicht unmittelbar. Dies betrifft auch Einsichtnahmemöglichkeiten in die zugrunde liegende Datenbasis über den Einzelfall hinaus, sodass Fälle struktureller Diskriminierung oder monokulturelle Entwicklungen in der Nutzung von ADM-Systemen nicht systematisch zu ermitteln sind. Im Hinblick auf die oben genannten Einzelrisiken entsteht damit ein Bild, bei dem die Möglichkeiten der Überprüfbarkeit und Korrigierbarkeit von ADM-Systemen auf der Ebene des Gesamtverfahrens in Form einer umfassenden externen Evaluation stark begrenzt sind. Insbesondere durch die Aufgaben im Bereich der Öffentlichkeitssensibilisierung können die Datenschutzbehörden zukünftig ggf. einen erweiterten Blick auf mögliche Risiken auch für die überindividuellen Zielwertere wahrnehmen.

Dennoch bleiben Bereiche, die mit Blick auf die normativen Zielwerte eine nur schwache oder gar keine rechtliche Umhegung aufzeigen: Wegen des Personenbezugs der DSGVO und der Fokussierung auf Individualrechte erscheint der rechtliche Schutz überindividueller Belange – „Gesellschaftliches" – maximal als beiläufig. Sachverhalte herkunftsbezogener Diskriminierung, Verstärkung von Geschlechterstereotypen bis hin zu Fällen von systematischem Rassismus fallen ohne eine individuelle Betroffenheit aus dem von DSGVO und BDSG geschützten Rahmen. Die DSGVO und das BDSG n.F. ermöglichen auch keinen externen Einblick in die interne ADM-Logik, ihre Angemessenheit und ihre Prozesse zur Feststellung des Vorliegens solcher strukturellen Diskriminierungen. Eine dezidierte neutrale Überprüfbarkeit mit Blick auf insbesondere die gruppen- und gesellschaftsbezogenen Zielwerte ist nicht möglich. Auch ein systematischer Überblick über die vorherrschende ADM-Systemvielfalt ist durch den Rechtsrahmen im Datenschutz nicht gewährleistet. Schwierig mit dem derzeitigen Instrumentarium – weil dafür eine einzelfall- und systemübergreifende Makroperspektive nötig ist – ist auch die Erkennbarkeit sozialer Wechselwirkungen: Die nicht durch den Einzelfall, sondern sich erst durch eine Vielzahl von automatisierten Entscheidungen ergebende systematische Andersbehandlung und Diskriminierung distinkter Personengruppen lassen sich durch individualrechtsbezogene Schutz- und Aufsichtsinstrumentarien weder entdecken noch minimieren. Das Gleiche gilt für die strukturelle Schwächung von individuellen Teilhabeinteressen, wenn eine Vielzahl gleicher oder ähnlicher ADM-Systeme den Einzelnen aufgrund einer bestimmten Datenlage systematisch aussortiert. Das Konzept einer „accountability" des Verantwortlichen eines ADM-Systems, verstanden als eine umfassenden Rechenschaftspflicht auch mit Blick auf derartige Wechselwirkungen, ist dem individualrechtssichernden Ansatz des Datenschutzes als Steuerungskonzept fremd.

6 Was die DSGVO leisten könnte: Datenschutzansätze und -instrumente für die verbleibenden Risikopotenziale

Das auf individualbezogene Rechte und Freiheiten ausgerichtete Datenschutzrecht kann mit Blick auf die normativen Zielwerte nicht alle Aspekte umfassen, vor allem in Bereichen gruppenbezogener oder gesellschaftlicher Interessen und Schutzgüter. Im letzten Kapitel sollen daher Regelungsansätze aufgezeigt werden, die die aufgezeigten Maßnahmen des Datenschutzes ergänzen und damit auch jene Interessen absichern können. Im Fokus stehen dabei Instrumente, die auf Zielwertoptimierung, umfassendere Transparenz und Überprüfbarkeit der ADM-Systeme sowie auf Vielfaltssicherung und Korrigierbarkeit abzielen. Zu unterscheiden sind dabei Gestaltungsmöglichkeiten im Rahmen der DSGVO-Praxis einerseits (Kapitel 6) und alternative Regulierungsformen, die außerhalb des Datenschutzrechts liegen, andererseits (Kapitel 7).

Regelungsinstrumente innerhalb der DSGVO können vor allem präventiv ihre Wirkung entfalten und stammen aus den Bereichen sogenannter „weicher Regulierung“ („soft law“). Bei einer Koregulierung bleibt es den Unternehmen selbst überlassen, wie sie im Sinne eines Codes of Conduct unbestimmte Regelungen der Verordnung konkretisieren und auch gesellschaftliche Interessen und Evaluationsmöglichkeiten berücksichtigen. Die erweiterten Gestaltungsmöglichkeiten der Aufsichtsbehörden beziehen sich zum einen auf die Beobachtung der Auswirkungen von ADM-Systemen auf gesellschaftliche Ziele, wenn auch ohne direkte rechtliche Folgen für die Anbieter. Eine weitere Möglichkeit besteht in der Nutzung von DSGVO-Öffnungsklauseln in der deutschen Gesetzgebung.

6.1 Koregulierung: Zertifizierte Verhaltensregeln zur Unterstützung von Wirtschaftsinitiativen

Eine Möglichkeit zur Orientierung der Verantwortlichen auch an überindividuellen Freiheiten und Rechten bieten die auch für ADM-Systeme von der Wirtschaft aufstellbaren Verhaltensregeln gemäß Art. 40 DSGVO. Dieser bildet zusammen mit Art. 41 DSGVO eine koregulative Struktur: Mit Codes of Conduct, also Regeln, die sich (vor allem) Unternehmen und Gruppen von Unternehmen selbst geben können, kann die Wirtschaft selbst die zum Teil unbestimmten Regelungen der Verordnung für sich verbindlich konkretisieren, wenn sie von den zuständigen Stellen anerkannt werden. Wenn es darum geht, komplexe Sachverhalte zu regeln, kann die Einbeziehung von Selbstregulierung hilfreich sein. Dabei wird ein Teil der Regulierung den Regelungsunterworfenen, in der Regel der Industrie, überlassen. Dies hat einige Vorteile, die auch bei ADM-Systemen zum Tragen kommen können, indem das Wissen der Unternehmen einbezogen wird und auf Änderungen im Gegenstandsbereich flexibel und rasch reagiert werden kann. Außerdem – und das ist hier besonders wichtig – kann Selbstregulierung Ziele verwirklichen, die im staatlichen Recht durch ganz unterschiedliche Gesetze gesichert werden; sie muss sich auch nicht an nationale oder EU-Grenzen halten. Allerdings bedarf es oft eines staatlichen Rahmens, damit die Wirtschaft sich tatsächlich wirksam selbst reguliert. In diesen Fällen spricht man von Koregulierung oder „regulierter Selbstregulierung“.

Eine gemäß Art. 41 DSGVO von der Datenschutzaufsicht akkreditierte Stelle wacht dann über die Einhaltung des Codes (und die weitere Akkreditierungsfähigkeit der Fachaufsicht). Diese Codes waren schon früher im Datenschutzrecht vorgesehen, nun aber gibt es ein geordnetes Verfahren und mehr Anreize, sie tatsächlich zu erstellen, denn es wird beispielsweise bei der Verhängung von Bußgeldern positiv berücksichtigt, wenn sich Unternehmen einem Code unterworfen haben.

Ein branchenübergreifender Code oder auch branchenspezifische Lösungen für ADM-Systeme wären ein Weg, um einige der in dieser Studie aufgezeigten Unklarheiten zu beseitigen (z. B. im Hinblick auf von der DSGVO umfasste Entscheidungsarchitekturen oder die konkrete Implementation und Umsetzung von Betroffenenrechten). Zudem wäre es möglich, weitere, nicht auf Individualrechte bezogene Risiken in dem Code zu adressieren. Die

Codeinhalte sind nicht auf die reine Konkretisierung der DSGVO-Normen bestimmt und könnten ggf. auch Selbstverpflichtungen beinhalten, die etwa bei Risiken für gesellschaftliche Interessen eine externe Evaluationsmöglichkeit vorsehen. Auch hier kann der Datenschutz der Ausgangspunkt sein, von dem aus weiterreichende Initiativen entwickelt würden.

Auch im Vorfeld der Schaffung von Verhaltensrichtlinien der Wirtschaft sieht die Verordnung die Aufsichtsbehörden als relevante Akteure: Sie sollen gemäß Art. 40 Abs. 1 DSGVO zusammen mit der EU und den Mitgliedstaaten die Ausarbeitung von Codes of Conduct fördern.

6.2 DSGVO: Erweiterung der Gestaltungsmöglichkeiten der Aufsichtsbehörden

Die rechtliche Analyse der Vorgaben von DSGVO und BDSG n.F. haben gezeigt, dass es mögliche Anknüpfungspunkte für rechtliche Gestaltungsmöglichkeiten auch innerhalb der DSGVO gibt, die den von ADM-Systemen ausgehenden Risiken entgegenwirken können. Diese in der Regel auf ermächtigenden Normen aufbauenden Möglichkeiten erfordern aber das aktive Handeln der jeweils befugten Behörden und/oder Stakeholder: Schon wegen ihrer Einblickmöglichkeiten in die Systeme der Anbieter und ihrer rechtlichen wie technischen Expertise erscheinen die Datenschutzbehörden hier als wichtige Akteure der gesellschaftlichen Debatte über ADM-Systeme. Durch ihre relativ breiten Befugnisse eröffnen sich hier aus Sicht des Rechtsrahmens positive Gestaltungsmöglichkeiten.

Wie in Kapitel 5 beschrieben, können die Behörden bei einem offenen Umgang mit den Sensibilisierungspflichten auch proaktiv gesellschaftliche Interessen in ihre Beobachtungen einbeziehen, ohne dass dies negative rechtliche Folgen für die Verantwortlichen hätte. Gegenüber den Verantwortlichen könnten sie in dieser Hinsicht zwar nur begrenzt vorgehen, da ihre Befugnis zu Aufsichtsmaßnahmen sich ausschließlich auf Verstöße gegen die DSGVO-Vorgaben erstreckt. Sie könnte aber insbesondere die gesellschaftsbezogenen Zielwerte berücksichtigen und die Feststellung möglicher Fehlentwicklungen gegenüber der Öffentlichkeit kundtun, wie etwa die zunehmende Monopolisierung von ADM-Systemen oder Algorithmen in bestimmten Lebensbereichen. Auch können systematische Schwächungen der Rechte von bestimmten Personengruppen durch eine Vielzahl einzelner, ähnlich gelagerter ADM-Verfahren erst durch eine Institution entdeckt werden, die Überblick über eine kritische Masse an Einzelbeschwerden und -verfahren hat. Als Startpunkt einer evidenzbasierten gesellschaftlichen Debatte scheinen die Datenschutzbehörden somit prädestiniert. Dabei müssten sie in den Bereichen außerhalb des aufsichtsrechtlichen Mandats, aber neben der Verschwiegenheitspflicht (Art. 54 Abs. 2 DSGVO) auch das Neutralitätsgebot des Staates wahren und könnten nur generelle Einschätzungen kundtun. Ausgeschlossen erschiene dagegen das „Naming und Shaming“ von Einzelanbietern, soweit deren ADM-Systeme gerade nicht gegen die Rechtsvorschriften verstießen. Gleiches gilt im Übrigen gegenüber den Verantwortlichen: Gesellschaftsbezogene Auffälligkeiten, die nicht gleichzeitig auch in die Rechte und Freiheiten des einzelnen Betroffen eingreifen, kann die Behörde dem Verantwortlichen formell oder informell mitteilen – eine Befugnis zur Durchsetzung einer System- oder Verfahrensänderung hat sie nicht. Allerdings haben sich die Datenschutzbehörden zu hoch spezialisierten Vertretern eines (wichtigen) Interesses entwickelt. Daher müsste ein Forum, in dem die Governance von ADM-Systemen diskutiert wird, auch die Vertreter anderer Interessen mit einbeziehen.

Die Datenschutzaufsicht hat aber neben ihren Aufsichts- und Sensibilisierungsbefugnissen noch weitere Gestaltungsmöglichkeiten aus der DSGVO. So kann sie den Anbietern von ADM-Systemen zusätzliche Verpflichtungen auferlegen: Wie gezeigt, besteht für die automatisierte Entscheidungen ein Verbot-Ausnahme-Grundsatz und die Pflicht zur Durchführung einer datenschutzrechtlichen Folgeabschätzung. Dies gilt aber nur für Systeme im Sinne des Art. 22 Abs. 1 DSGVO, dessen Anwendungsbereich begrenzt ist (s. Kapitel 3.1). Nach Art. 35 Abs. 4 DSGVO aber können die Behörden eine Liste mit Datenverarbeitungsvorgängen erstellen und veröffentlichen, für die zwingend Folgeabschätzungen vorzunehmen sind. Würde die Datenschutzaufsicht von diesem Entscheidungsspielraum Gebrauch machen, so könnte sie ggf. auch Verantwortliche von solchen ADM-Systeme zu einem Impact Assessment verpflichten, die ansonsten außerhalb des Anwendungsbereichs von Art. 22 Abs. 1 DSGVO

lägen. Auf diese Weise wären etwa auch Anbieter von automatisierten Entscheidungssystemen zur Folgeabschätzung verpflichtet, die nicht rein automatisiert entscheiden oder deren Relevanz unterhalb der von Art. 22 Abs. 1 DSGVO geregelten ADM-Verfahren bleibt. So könnte jedenfalls eine überprüfbare Pflicht zur internen frühzeitigen Risikoabschätzung und zur Absicherung von Mindeststandards geschaffen werden. Nicht im Rahmen dieses Gutachten geprüft werden kann, inwieweit eine solche Erweiterung in der Praxis auch verhältnismäßig insbesondere für KMU-Unternehmen wäre.

6.3 Öffnungsklauseln: Restriktivere BDSG-Anforderungen

Daneben bieten auch sogenannte „Öffnungsklauseln" weitere Möglichkeiten, um gesetzliche Vorschriften weiter zu konkretisieren. Die DSGVO selbst sieht Öffnungsklauseln für die einzelnen Mitgliedstaaten vor. Nimmt ein Staat eine solche Klausel in Anspruch, kann er von den Vorgaben der DSGVO abweichen oder diese weiter konkretisieren. Im BDSG n.F. hat der deutsche Gesetzgeber davon Gebrauch gemacht, wie gezeigt auch im Bereich automatisierter Entscheidungen (s. Kapitel 3.1.2): § 37 BDSG n.F. erweitert die ausnahmsweise Zulässigkeit von ADM-Systemen im Bereich der Leistungserbringung bei Versicherungsverträgen. Einige der Öffnungsklauseln können aber auch in beschränkender Art und Weise von den EU-Staaten genutzt werden:

- So könnten Mitgliedstaaten mit Blick auf die Öffnungsklausel in Art. 9 Abs. 2 Buchst. a) DSGVO etwa gesetzliche Vorschriften vorsehen, die eine Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten im Falle von ADM-Systemen gemäß Art. 22 Abs. 1 DSGVO generell ausschließen. Damit wäre in dem jeweiligen Mitgliedstaat dann zumindest die Einwilligung in die Verarbeitung von Daten wie z. B. Ethnie, genetische oder gesundheitliche Daten sowie politische Ansichten im Rahmen von automatisierten Entscheidungen verboten. Diskriminierungen über andere korrelierende Betroffenenmerkmale ließen sich aber auch so nicht ausschließen.
- Auch denkbar wäre bei Bezugnahme auf die Öffnungsklausel in Art. 37 Abs. 4 DSGVO die gesetzliche Verpflichtung zur Bestellung eines Datenschutzbeauftragten, in jedem Fall des Einsatzes eines ADM-Systems, und dies unabhängig von den Anforderungen aus Art. 37 Abs. 1 DSGVO.
- Wäre für die beschriebene mögliche breitere Perspektivenwahrnehmung durch die Aufsichtsbehörden wider Erwarten ein gesetzlicher Auftrag erforderlich, könnte sich eine entsprechende nationale Vorschrift auf Art. 58 Abs. 6 DSGVO berufen.

Damit erscheinen Öffnungsklauseln in der DSGVO grundsätzlich als Möglichkeit, den Bereich der automatisierten Entscheidungen – in engen Grenzen – restriktiver zu regulieren, als die Verordnung vorgibt. Der Hauptkritikpunkt an den (sehr vielen) Öffnungsklauseln aber ließe sich auch für die eben genannten Beispiele vorbringen: Jede nationale Abweichung von den Vorgaben der EU-Verordnung führt zu einer Fragmentierung des Europäischen Regelungsrahmens im Datenschutz und steht damit im Widerspruch zum Verordnungszweck: Der europaweiten Harmonisierung des Datenschutzes durch die Schaffung eines einheitlichen Rechtsrahmens.

Daneben stellt sich auch an dieser Stelle die Grundsatzfrage, ob ausgerechnet das individualrechtsbezogene Datenschutzrecht dasjenige Rechtsregime ist, das sich in zunehmendem Maße auch um die Wahrung der Interessen der Allgemeinheit kümmert. Die „Belastung" des Datenschutzes mit überindividuellen Zielwerten führt wie gezeigt schon jetzt an mehreren Stellen zu systematischen, wenn nicht dogmatischen Brüchen der Vorgaben der DSGVO mit Blick auf die dahinterliegenden Schutzzwecke. Es muss die Frage gestellt werden, ob für die Wahrung gesellschaftsbezogener normativer Zielwerte nicht datenschutzentferntere Steuerungsansätze zu nutzen wären, um datenschutzrechtliche, auf das Individuum bezogene Schutzinstrumente nicht mit überindividuellen Schutzzielen zu überfrachten. Was geführt werden muss, wenn es um automatisierte Entscheidungen geht ist die Debatte um den „Ort" der nicht auf Datenschutz fokussierenden Steuerungsansätze.

So verweisen auch die Regelungen in der DSGVO, die das Verhältnis von maschinellen und menschlichen Elementen der Entscheidung zum Gegenstand haben, auf ein Problem, das über das Datenschutzrecht hinausweist: Die Risiken für Individuen, Gruppen und die Gesellschaft hängen von der Architektur der Entscheidung ab, die diese Elemente in ein Verhältnis setzt. Ob ein Mensch bei einem ADM-Prozess nicht nur formal, sondern materiell das Ergebnis prägen kann, hängt von vielen Faktoren ab, die die Architektur bestimmen. Dabei spielt nicht nur das Recht, das den Gegenstandsbereich ordnet, eine Rolle, wie hier etwa das Datenschutzrecht. Es hängt beispielsweise auch vom Haftungsrecht ab, ob es für einen menschlichen Entscheider rational ist, dem Vorschlag eines ADM-Systems aufgrund einer eigenen Wertung nicht zu folgen oder es schlicht zu übernehmen. Dies bedeutet, dass viele der oben genannten Risiken einer Analyse der die konkrete Entscheidung prägenden Faktoren bedürfen, die über ein Rechtsgebiet hinausgeht. In der Modellierung der Entscheidungsarchitektur und der Bewertung unterschiedlicher Architekturen liegt ein bedeutsames transdisziplinäres Forschungsfeld. Dessen Ergebnisse bedürfen einer intensiven gesellschaftlichen Debatte.

7 Über die DSGVO hinaus: Alternative Steuerungsinstrumente außerhalb des Datenschutzrechts

Mit Blick auf die eben beschriebenen strukturellen Grenzen von Datenschutzrecht erscheint ein kurzer Exkurs in andere Rechtsgebiete mit dem Zweck zielführend, alternative Steuerungsansätze für die Gewährleistung der durch ADM-Systeme bedrohten Zielwerte zu identifizieren. Diese alternativen Instrumente unterscheiden sich in ihrem Fokus. Sie konzentrieren sich etwa auf die Erklärbarkeit bzw. Überprüfbarkeit von ADM-Systemen, haben zum Ziel, Vielfalt von ADM-Systemen zu sichern oder tragen zu einer verbesserten Korrigierbarkeit bei. Sie greifen vor allem nachträglich, wenn die Systeme bereits im Einsatz sind.

7.1 Erklärbarkeit von automatisierten Entscheidungen als Steuerungsansatz

Einer der vorgeschlagenen Regulierungsansätze betrifft die bessere Ausgestaltung der vom Datenschutz unabhängig zu regelnden gesetzlichen Erklärbarkeit von ADM-Systemen. Dabei ist der Hintergrund dieser Forderungen durchaus von unterschiedlichen Zielrichtungen getragen und reicht von dem Recht des Betroffen auf die Beantwortung der Frage nach dem „Warum?“ über eine bessere interne Absicherung gegen fehlerhafte – und damit ggf. ineffiziente oder unökonomische – Systeme bis hin zur Ermöglichung umfassender externer Evaluation.

Die Erklärbarkeit von ADM-Systemen wirft Probleme auf, die sich auch im Datenschutzrecht auswirken (s. Kapitel 3.4.2), aber weit darüber hinaus weisen. Was und wie erklärt werden kann, hängt von den genutzten technischen Systemen ab. So arbeiten viele der ADM-Systeme auf Basis mathematisch-stochastischer Verfahren. Auf Grundlage von großen Datenmengen (Trainingsdaten) bilden die Systeme statistische Korrelationen zwischen (Gruppen-)Merkmalen und z. B. der Wahrscheinlichkeit des Ausfallrisikos einer Kreditlinie. Dadurch können aus Anbietersicht vielfältige Einschätzungen über den Betroffenen getroffen werden, die auf diesen statistischen Methoden beruhen – Kausalbeziehungen aber kennen ADM-Systeme gerade nicht. Sogenannte „determinierte Systeme“, die auf die gleiche Dateneingabe stets eine identische Ausgabe produzieren, können dabei theoretisch so programmiert werden, dass sie eine „Erklärung“ für ihre Entscheidung mit ausgeben. Diese mathematische Erklärung allerdings erfüllt die Rationalitäts- und Konsistenzerwartungen, die Menschen an diesen Begriff haben, regelmäßig nicht. Die Vorhersagen aufgrund der Berechnungen von Variablen in parallelen, mehrdimensionalen Verfahren sind mathematisch darstellbar, aber in der Interpretation durch Menschen so komplex, dass sich – je nach Komplexität des Systems – eine einfache Erklärbarkeit einer Einzelentscheidung im Sinne einer kausalen Begründung nicht ergibt („curse of dimensionality“; Edwards und Veale 2017: 27).

Herausforderungen gibt es auch bei Systemen, die mit sogenannter „künstlicher Intelligenz“ (KI) arbeiten. Der Begriff der KI ist nicht klar definiert. Der kleinste gemeinsame Nenner scheint zu sein, dass es bei dem KI-Einsatz darum geht, die kognitive Leistungsfähigkeit eines Systems zu erhöhen. Das macht diese Systeme auch autonomer. Dabei spielt – je nach Einzelsystem – maschinelles Lernen eine Rolle. Die Systeme werden so programmiert, dass sie selbsttätig Muster in Lerndatensätzen erkennen. Bei dem sogenannten „unüberwachten Lernen“ werden dabei keine Ziele oder Kriterien vorgegeben, sondern das System sucht und identifiziert völlig selbstständig Muster. Derartige, beständig lernende Systeme werden derzeit vor allem in der Entwicklung eingesetzt, und (derzeit noch) weniger in den Produkten, die dem Endnutzer angeboten werden. Bei KI-Systemen kann dadurch allerdings ein Zustand erreicht werden, in dem auch der Entwickler selbst nicht mehr vorhersagen kann, welches Ergebnis ein Input erzeugen wird. Für derartige Systeme bieten sich drei Ansätze an, um das Funktionieren besser verstehen zu können:

- Es wäre zu eruiren, welche systemadäquaten Beschreibungsmöglichkeiten es gibt, etwa Auskunft über die Ziele, die dem System zum Lernen vorgegeben wurden, und Informationen über die Struktur der Lerndaten. Hier stellt sich die Frage, ob die Informationen am Ende ausreichen,

um die jeweiligen Zwecke der Risikokontrolle zu erfüllen, also etwa einem Dritten zu ermöglichen, das System auf Fehler zu prüfen und eine Grundlage für Rechtsschutzmaßnahmen zu haben (s. dazu Kapitel 7.2). Auch vereinfachte Modelle können zum Verstehen beitragen.

- Es könnten Verfahren entwickelt werden, um eine „Erklärbarkeit by Design" zu gewährleisten, also beispielsweise parallel laufende Protokolle, die Systemänderungen mitloggen, oder Testläufe, die Systemzustände beschreiben. Auch in der Informatik sind derartig entkoppelte Systeme der Entscheidungsfindung einerseits und Entscheidungsbegründung andererseits ein relevantes Forschungsfeld, auch und gerade durch dekompositionelle Verfahren (Edwards und Veale 2017), bei denen die im Rahmen des ADM-Systems teils parallel laufenden Einzelmodule und ihre jeweiligen Entscheidungsschritte getrennt voneinander erläutert werden.
- Selbst im Falle komplett erklärbarer automatisierter Entscheidungen bedarf es auch einer Debatte darüber, welche Metriken die Überprüfenden anlegen bzw. anzulegen haben. Wie lässt sich etwa Fairness nicht nur mathematisch, sondern auch mit Blick auf die normativen Zielwerte operationalisieren? Wer entscheidet über die Interpretierbarkeit von Ergebnissen und wer über den Interpretationsansatz? Wie kann im Rahmen von Evaluationen so etwas wie eine „Spruchpraxis" hergestellt werden, damit es nicht zu Divergenzen bei der Anwendung von Prüfkriterien kommt?

Die Diskussion über die drei Aspekte steht noch in den Anfängen und erfordert weitere transdisziplinäre Forschung. Mit Blick auf eine mögliche regulatorische Intervention in Form einer konkreten, einzelfallbezogenen Erklärbarkeitspflicht von automatisierten Entscheidungen wäre dabei zu fragen, welcher Ansatz die Implementation erklärbarer System befördern könnte und inwieweit mit Blick auf die Alternativen überhaupt die Erforderlichkeit dafür bestünde. Der Anspruch, begründbare automatisierte Entscheidungen zu haben, ist grundsätzlich nachvollziehbar, muss sich aber auch dem Vergleich stellen mit der Rationalität menschlicher Entscheidungen (vgl. Ernst 2017). Implizite Erwartungen an beide Entscheidungsmodelle sollten ohne sachlichen Grund nicht voneinander abweichen und auch der Blick auf menschliche Entscheidungsarchitekturen zeigt ggf. irrationale oder verdeckte Entscheidungsaspekte und -parameter (z. B. Formen impliziten Wissens oder impliziter Entscheidungsheuristiken). Während nicht nur automatisierte, sondern auch menschengetroffene staatliche Entscheidungen, bei denen ein Beurteilungs- und Ermessensspielraum besteht, stets einer Begründung bedürfen, ist der Privatautonomie grundsätzlich eigen, dass eine private Partei auch irrationale oder parteiische Entscheidungen treffen kann – jedenfalls, solange die Entscheidung nicht Antidiskriminierungsvorgaben des einfachen Rechts missachtet.

7.2 Erweiterte Transparenz- und Accountability-Vorgaben für die Überprüfung durch Dritte

Die oben beschriebenen Hürden bei der Verbesserung der Zielwertgewährleistung durch Transparenzpflichten kommen dort nicht zum Tragen, wo Dritte mit tiefem Verständnis der Materie und hinreichend hoher Motivation Auswerter entsprechender Informationen sind. Transparenzbasierte Steuerungsvorteile ergeben sich vor allem bei der Einsichtnahme durch Experten auch außerhalb von Behörden, zumal wenn diese nicht nur auf Individualrechte, sondern auch auf gruppen- und gesellschaftsbezogene Zielwerte blicken. Gegen den allzu tiefen Einblick in die Entscheidungssysteme aber sprechen Geheimhaltungsinteressen der Verantwortlichen, deren Wettbewerbsfähigkeit sich ggf. (auch) auf der Nutzung dieser optimierten ADM-Systeme gründet. Soweit also der Zugang von Externen zu diesen Informationen gesetzlich geregelt werden soll, müssten diese entgegenstehenden Rechte Berücksichtigung finden, etwa durch strenge gerichtsähnliche „in camera"-Verfahren, bei denen die Verschwiegenheit der unabhängigen Expertinnen und Experten verpflichtend ist. Die teils geforderte öffentliche Dokumentation von internen Prozessen, Entscheidungen und Softwareprogrammen erscheint jedenfalls grundsätzlich als unverhältnismäßig.

Bezugspunkte für die Offenlegung oder Zugangsgewährung beträfen bei „in camera“-Verfahren die einzelnen ADM-Systembestandteile wie Daten, Datenstruktur und Quellcode, könnten sich aber ggf. auch lediglich auf darüber liegende Ebenen erstrecken, wie den Zugang zu den (internen) Dokumenten, die aufgrund von DSGVO-Vorgaben erstellt wurden, d. h. insbesondere die Folgenabschätzung, die Verzeichnisliste, die internen Richtlinien oder organisatorische wie prozedurale Privacy-by-Design-Maßnahmen. Vorteil von „in camera“-Verfahren wären vor allem eine ausdrückliche Verpflichtung der Experten auf gesellschaftliche Zielwerte bei der Begutachtung von ADM-Systemen; der Nachteil aber bliebe, dass das Verfahren nicht öffentlich bliebe und eine gesellschaftliche Auseinandersetzung insbesondere unter Berücksichtigung von zivilgesellschaftlichen Kräften nur mittelbar aus Erkenntnissen dieser Verfahren informiert wäre. Zudem birgt jede Form der institutionalisierten Begutachtung durch Dritte das Risiko, parallele kontrollrechtliche Verfahren zu der Datenschutzaufsicht zu etablieren, die sich nicht hinreichend voneinander abgrenzen.

7.3 Möglichkeiten externer Überprüfbarkeit ohne Systemeinblick

Ein anderer Ansatz kann in den Forschungsanstrengungen zu sehen sein, die sich auf modell-agnostische Evaluationsverfahren von ADM-Systemen konzentrieren (sogenanntes „black box testing“). Ausgangspunkt derartiger Überlegungen ist der Umstand, dass ein Evaluator eines Systems entweder nicht auf die Interna des Systems Zugriff hat oder dieser Zugriff keine Erkenntnisse über mögliche Diskriminierungen innerhalb des Systems bringt. Ähnlich den Reverse-Engineering-Verfahren bei Software versuchen derartige sogenannte „pädagogische Verfahren“ Evaluationserkenntnisse aus einer systematisierten Befragung dieser Systeme mit Testdaten zu gewinnen („pedagogical rule extraction“). Durch die vielfache und koordinierte Befragung kann das Befragungsverfahren Rückschlüsse auf im System vorherrschende Regeln und Gewichtungen zulassen. Dafür befragt der Evaluator das ADM-Verfahren üblicherweise automatisiert über eine Programmierschnittstelle (Application Programming Interface (API)). Für die flächendeckende Ermöglichung derartiger Verfahren müssten ADM-Anbieter verpflichtet werden, entsprechende APIs zu schaffen. Vorteil von „pedagogical rule extraction“ ist, dass die Evaluation ohne einen Eingriff in den Softwarecode – und damit zentral in den Bereich der Geheimhaltungsinteressen des Anbieters – auskommt. Als Nachteil kommt dagegen die mangelnde Skalierbarkeit derartiger Systeme in Betracht. Auch stellen sich bei diesem Ansatz die Fragen der Kostentragung und der Verantwortungsübernahme für derartige Methoden.

7.4 Mögliche Anwendung von verbraucherschützenden und wettbewerbsrechtlichen Regelungen für verbesserte Korrigierbarkeit

Wettbewerbsrecht gilt als der schnellere und flexiblere Bruder des Ordnungsrechts. Durch eine große Anzahl von „Kontrolleuren“ – d. h. insbesondere Wettbewerber und die klagebefugte Stellen wie Verbraucherschutzzentralen und Wettbewerbsvereine – werden Verstöße gegen das Lauterkeitsgebot schnell entdeckt und angemahnt. Auch im Fall verbraucherschutzrechtlicher Verstöße kann eine rechtliche Entscheidung relativ zügig hergestellt werden. Inwieweit aber Wettbewerbsrecht und Verbraucherschutzrecht als Steuerungsressource bei ADM-Systemen in Betracht kommen, bedarf einer umfassenderen Untersuchung, die hier nicht geleistet werden kann. Im Wettbewerbsrecht ist jedenfalls ein Abstellen auf einen Verstoß gegen eine Datenschutzvorschrift unproblematisch als unlauter zu bewerten, sodass sich bei Nutzung des Wettbewerbsrechts im Vergleich zum ordnungsrechtlichen Datenschutz theoretisch ein Vorteil bei der Durchsetzung bestehenden Rechts ergibt, der auch dem Erreichen der Zielwerte dient. Ähnliches gilt für auf Beseitigung abzielende Unterlassungsbegehren, bei denen unterlassungsklagebefugte Stellen den Verantwortlichen aufgrund vermeintlicher Verstöße gegen Datenschutzvorschriften abmahnen (vgl. § 3 i. V. m. § 2 Abs. 1 Nr. 11 Unterlassungsklagegesetz (UKlaG)). Beschränkt bliebe das Wettbewerbsrecht in seiner Anwendung durch die Inkorporierung der Datenschutzvorschriften aber auch auf die vor allem individualbezogenen Rechte und Freiheiten. Hinzu träte das faktische Problem der Beweisbarkeit eines Datenschutzverstoßes im Bereich etwa diskriminierender ADM-Systeme durch die Klageberechtigten, die in der Regel nur Einblick in Einzelfälle haben. Einen besseren Überblick

könnten diese Klageberechtigten im Falle von Sammelklagen erhalten, bei denen sie eine Vielzahl Betroffener vertreten. Derartige Sammelklagen werden – im Verbraucherrecht – immer wieder diskutiert, ein entsprechendes Rechtsmittel sieht das deutsche Wettbewerbsrecht aber derzeit nicht vor. Im Falle einer zivilgerichtlichen Überprüfung der Ansprüche müsste das Zivilgericht die vermeintlichen Datenschutzverstöße prüfen und sich dabei – jedenfalls im Falle komplexer ADM-Systeme – Sachverständiger bedienen. Damit sind Form und Umfang der Kontrolle bei wettbewerbsrechtlichen Klagen mit der im Datenschutz vergleichbar, nur dass es im Zivilverfahren ggf. Geschwindigkeitsgewinne gibt. Spezifische gesellschaftliche Risiken würden auch hier nicht in den Fokus der rechtlichen Betrachtung kommen. Allerdings kann die parallele Kontrolle durch Gerichte auf Basis des Wettbewerbsrechts auch die Spezialaufsicht etwa durch Datenschutzbehörden schwächen, da nicht gesichert ist, dass Auslegungsspielräume in gleicher Weise genutzt werden.

7.5 Mögliche Anwendung oder Übernahme kartell- und medienrechtlicher Regelungsinstrumente zur Vielfaltssicherung

Insbesondere für einen gesellschaftlichen Pluralismus erscheinen mögliche Konsolidierungs- und Vereinheitlichungstendenzen bei dem Einsatz von ADM-Systemen und den ihnen zugrunde liegenden Algorithmen als Problemfeld. Mit dem Herausschälen weniger Anbieter oder Systeme stellt sich die Frage nach der Anwendbarkeit von kartellrechtlichen Bestimmungen, die Monopolisierungstendenzen jedenfalls bremsen könnten. Damit Kartellrecht Anwendung findet, müssten einzelne Anbieter eine beherrschende Stellung auf dem sachlich und räumlich relevanten Markt innehaben. Die Bestimmung des sachlich (und räumlich) relevanten Marktes ist bei ADM-Systemen allerdings nicht trivial, da die lizensierbaren Systeme oftmals eine abstrakte Funktion erfüllen und dann erst bei der Implementation auf den jeweiligen Einsatzbereich zugeschnitten werden. Andere Systeme werden ausschließlich innerhalb eines Unternehmens für den jeweiligen Zweck entwickelt. Dort kann es zu einer marktbeherrschenden Stellung insoweit nicht kommen. Selbst für inhouse entwickelte Lösungen aber greifen die Entwickler ggf. auf algorithmische Frameworks von Drittanbietern zu, sodass sich hier ggf. Oligopole häufig genutzter Einzelalgorithmen oder Softwarepakete entwickeln, die kartellrechtliche Relevanz entfalten. Dafür wäre aber zunächst eine Marktübersicht erforderlich, die aus den eben genannten Gründen nicht ohne Weiteres erstellbar ist; um einen Überblick über die in der Praxis eingesetzten Systeme und Frameworks zu bekommen, wäre man notwendigerweise auf Informationslieferungen aus der Wirtschaft angewiesen. Doch selbst wenn man hier eine regulatorische Offenbarungspflicht einführte, bliebe der Zugriff des Kartellrechts bei einer angenommenen Anwendbarkeit begrenzt auf die Identifizierung der Stellung im Markt und davon ausgehend auf wirtschaftlichen Gegenmaßnahmen wie Zugangsverpflichtungen oder – am äußersten Ende – Entflechtungsverpflichtungen. Damit böte das Kartellrecht rein hypothetisch einen schwachen Ansatzpunkt zur Verbesserung der Angebotsvielfalt bei ADM-Systemen.

Auch bei der algorithmischen Herstellung von Öffentlichkeit oder der algorithmenbasierten Steuerung von Informationsflüssen und personalisierten Diensten bei der Meinungsbildung können gesellschaftliche Zielwerte wie Vielfalt und Machtpotenziale aus regulatorischer Sicht aufscheinen. Seit Längerem diskutiert die Medienpolitik die Verbesserung der derzeit begrenzten Zugriffsmöglichkeiten der medienrechtlichen Vielfaltskontrolle auf Plattformen und Informationsintermediäre; auch Möglichkeiten eines unmittelbaren Diskriminierungsverbots werden untersucht (Schulz und Dankert 2016). Mit den für ADM-Systeme identifizierten Risiken kommen diese Anbieter vor allem dort in Betracht, wo Plattformen oder Intermediäre automatisiert medieninhaltsbezogene Entscheidungen auf Grundlage der (vermeintlichen) individuellen Nutzerinteressen treffen. Mit einer Erweiterung der medienrechtlichen Anforderungen auf diese Anbieter würden sie Vielfaltspflichten oder Diskriminierungsverbote treffen, die auch Relevanz für die Gestaltung von automatisierten Entscheidungen haben können. Die detaillierte Beantwortung dieser Fragen kann dieses Gutachten nicht leisten, absehbar aber ist, dass sich selbst in diesen Fällen die Vielfaltsanforderungen und Diskriminierungspflichten auf das inhaltliche Ergebnis der Dienste bezögen, nicht auf das Verfahren ihrer Herstellung. Für die vorgefundenen Defizite hinsichtlich der Zielwerte stellte Medienrecht in diesen Fällen insoweit eine Kompensationsmöglichkeit dar, die für die Gewährleistung von

gesellschaftlichem Pluralismus und Nichtdiskriminierung geeignet erscheint, aber nicht unmittelbar zur Systemtransparenz beiträgt.

8 Fazit

Automatisierte Entscheidungen bergen – neben den vielfältigen Potenzialen – Risiken für individuelle normative Zielwerte wie Handlungsautonomie, Persönlichkeitsrechte und faire Behandlung im Sinne einer Nichtdiskriminierung, für gruppenbezogene Ziele wie Nichtdiskriminierung, aber auch für gesellschaftliche Ziele wie Pluralismus und soziale Teilhabe. Die drei zentralen Maßnahmen zum Begegnen dieser Risiken sind Transparenz, Überprüfbarkeit und Korrigierbarkeit der automatisierten Entscheidungen und der ihnen zugrunde liegenden ADM-Systeme. Der ab Mai 2018 geltende Datenschutzrechtsrahmen ist mit Blick auf automatisierte Entscheidungsverfahren nur begrenzt in der Lage, diese Zielwerte vollends zu gewährleisten. Das relativ enge Verständnis automatisierter Entscheidungen und die teils sehr weitreichenden Ausnahmen werden absehbar zu einer Entwicklung führen, in der die Interaktion mit ADM-Systemen alltägliche Praxis sein wird.

Aufgrund der im Kern individualrechtsbezogenen Schutzrichtung des Datenschutzes hält die DSGVO unmittelbar Regelungsinstrumente für die einzelfallbezogene Transparenz, Nachvollziehbarkeit und Korrigierbarkeit einer automatisierten Entscheidung bereit. Insbesondere das Recht auf Hinzuziehung eines Menschen, der die Entscheidung überprüft, den Sachverhalt inklusive nachgereichter Darlegungen bewertet und dann neu entscheidet, kann gegenüber rein automatisierten Verfahren grundsätzlich die Persönlichkeitsrechte des Betroffenen und sein Interesse an einer fairen Behandlung wahren. Soweit der Datenschutzrahmen Informationspflichten auch für die involvierte Logik vorsieht, sind Umfang und Tiefe dieser Informationen auf ein für den durchschnittlichen Nutzer verständliches Niveau begrenzt. Damit schafft die DSGVO einen Rechtsrahmen, der ausschließlich individualbezogene Interessen schützen kann und Einzelentscheidungen überprüf- und revidierbar macht. Einen tieferen, konkreten Einblick in die Funktionsweise des ADM-Systems, der auch Hinweise auf systematische Diskriminierungsrisiken oder negative soziotechnische Konsequenzen liefert, gewähren die Transparenz- und Nutzerrechte in der DSGVO nicht.

Daneben stellt die DSGVO Anforderungen an die Konzeption und Implementation von ADM-Systemen aufseiten des Verantwortlichen, die neben den individuellen Zielwerten – beiläufig und zu kleinen Teilen – auch gruppenbezogene Vorgaben wie Nichtdiskriminierung berücksichtigen können, etwa im Rahmen der Durchführung von datenschutzrechtlichen Folgeabschätzungen oder der Berücksichtigung von Privacy-by-Design-Prinzipien bereits in der Konzeptionsphase. Insgesamt schafft es die Verordnung, bei Anbietern von ADM-Systemen ein hohes Bewusstsein für die individualbezogenen Rechte und Freiheiten der Betroffenen zu schaffen. Der Rechtsrahmen hilft dagegen nur bedingt bei der systematischen Gewährleistung gruppenbezogener und gesellschaftsbezogener Zielwerte.

Auf der Ebene der Datenschutzbehörden sieht die DSGVO breite Auskunftsrechte und Zutrittsbefugnisse vor. Damit sind die Aufsichtsbehörden theoretisch in der Lage, die positiv wirkenden Anbieterverpflichtungen noch zu verstärken. Die vom Anbieter erarbeiteten Prozesse und Strukturen sowie die durchgeführten Folgeabschätzungen etc. sind im Falle einer Datenschutzprüfung komplett von den Behörden einseh- und überprüfbar. Die Perspektive der Behörden ist in diesen Fällen ebenfalls in erster Linie der Schutz der individuellen Rechte. Daneben bestehende Sensibilisierungsaufgaben können aber theoretisch den Beobachtungsumfang der Datenschutzaufsicht erweitern. Auf systematische, den Einzelanbieter übergreifende Fehlentwicklungen könnten die Behörden auf dieser Grundlage ebenfalls hinweisen. Damit können – jedenfalls mit Blick auf die öffentliche Debatte – Datenschutzbehörden auch gesellschaftsbezogene Risiken von ADM-Systemen adressieren. Der weitreichende Kompetenzkatalog jedenfalls lieferte dafür mögliche Ansatzpunkte, die Behörden müssen sich aber aktiv zu dieser Rolle bekennen. Einen Anspruch auf Systemeinsicht und Überprüfung durch unabhängige Dritte wie etwa Wissenschaftler oder technische Experten sieht die DSGVO dagegen nicht vor. Damit bleiben vor allem Gegenmaßnahmen wie Systemtransparenz und Überprüfbarkeit des ADM-Systems sowie die Vielfaltssicherung rechtlich wenig umhegt. Hier bedarf es über das Datenschutzrecht hinausgehender Regulierungsdebatten.

Das Gutachten zeigt vor diesem Hintergrund Ansatzpunkte im Datenschutzrecht und in anderen Rechtsbereichen auf, die bei richtiger Gestaltung den Fachdiskurs befeuern und die Erreichung gesellschaftlich getragener Werte und Normen verbessern können.

Abbildung 5: Positive Effekte der DSGVO vor allem für den Einzelnen, für die Gesellschaft sind ergänzende Ansätze notwendig (Quelle: eigene Darstellung)

Literatur

Article 29 Working Party (2017). „Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679“. WP 251, 3. Oktober 2017. http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 (Download 7.3.2018).

Bäcker, Matthias (2017). „Art. 15. Auskunftsrecht der betroffenen Person“. *Datenschutz-Grundverordnung: DS-GVO. Kommentar*. 1. Auflage. Hrsg. Jürgen Kühling und Benedikt Buchner. München. 387–397.

Barocas, Solon, und Andrew D. Selbst (2016). „Big Data’s Disparate Impact“. *Californian Law Review* (104). 671–732.

Bertelsmann-Stiftung (Hrsg.) (2017a). *Wenn Maschinen Menschen bewerten – Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung*. Gütersloh. (Auch online unter https://algorithmenethik.de/2017/05/02/wenn-maschinen-menschen-bewerten/, Download 8.2.2018.)

Bertelsmann-Stiftung (Hrsg.) (2017b). *Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen*. Gütersloh. (Auch online unter https://algorithmenethik.de/2017/06/19/digitale-oeffentlichkeit-wie-algorithmische-prozesse-den-gesellschaftlichen-diskurs-beeinflussen/, Download 8.2.2018.)

Bull, Hans Peter (2006). „Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?“ *NJW (Neue Juristische Wochenschrift)* 2006. 1617–1624.

Bygrave, Lee A. (2001). „Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling“. *Computer Law & Security Report* (17). 17–24.

Edwards, Lilian, und Michael Veale (2017). „Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking For“. *Duke Law & Technology Review* (16) 18. 18–84.

Ernst, Christian (2017). „Algorithmische Entscheidungsfindung‘ und personenbezogene Daten“. *JZ (Juristische Zeitung) 21*. 1026–1036.

Gola, Peter (Hrsg.) (2017). *Datenschutz-Grundverordnung: DS-GVO. Kommentar*. 1. Auflage. München.

Goodman, Bryce, und Seth Flaxman (2016). „European Union regulations on algorithmic decision-making and a ‚right to explanation‘“. arXiv:1606.08813 [stat.ML]. https://arxiv.org/pdf/1606.08813.pdf (Downolad 7.3.2018).

Howells, Geraint G. (2005). „The Potential and Limits of Consumer Empowerment by Information“. *Journal of Law and Society* (32). 349–370.

Keats Citron, Danielle, und Frank Pasquale (2014). „The scored society: Due Process for automated predictions“. *Washington Law Review* (89). 1–33.

Malgieri, Gianclaudio, und Giovanni Comandé (2017). „Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation“. *International Data Privacy Law*, ipx019. https://doi.org/10.1093/idpl/ipx019 (Download 7.3.2018).

Martini, Mario, und David Nink (2017). „Wenn Maschinen entscheiden ... – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz“. *NVwZ (Neue Zeitschrift für Verwaltungsrecht)* (36) 10. 1–14.

Mendoza Isak, und Lee A. Bygrave (2017). „The Right Not to be Subject to Automated Decisions Based on Profiling“. *EU Internet Law: Regulation and Enforcement*. Hrsg. Tatiani Synodinou, Philippe Jougleux, Christiana Markou und Thalia Prastitou. Cham. 77–98.

Radlanski, Philip (2016). *Das Konzept der Einwilligung in der datenschutzrechtlichen Realität*. Heidelberg.

Schulz, Wolfgang, und Kevin Dankert (2016). *Die Macht der Informationsintermediäre. Erscheinungsformen, Strukturen und Regelungsoptionen*. Bonn.

Selbst, Andrew D., und Julia Powles (2017). „Meaningful information and the right to explanation". *International Data Privacy Law* (7) 4. 233–242.

Wachter, Sandra, Brent Mittelstadt und Luciano Floridi (2017). „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation". *International Data Privacy Law* (7) 2. 76–99.

Weil, David, Archon Fung, Mary Graham und Elena Fagotto (2006). „The Effectiveness od Regulatory Disclosure Policies". *Journal of Policy Analysis and Management* (25) 1. 155–181.

Zarsky, Tal Z. (2017). „Incompatible: The GDPR in the Age of Big Data". *Seton Hall Law Review* (47) 4. 995–1021.

Zweig, Katharina A., unter Mitwirkung von Sarah Fischer und Konrad Lischka (2018). „Wo Maschinen irren können. Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung". *algorithmenathik.de* 5.2.2018. https://algorithmenethik.de/2018/02/05/wo-maschinen-irren-koennen-fehlerquellen-und-verantwortlichkeiten-in-prozessen-algorithmischer-entscheidungsfindung/ (Download 8.2.2018).

Über die Autoren

Prof. Dr. Wolfgang Schulz ist Direktor des Hans-Bredow-Instituts für Medienforschung an der Universität Hamburg. Seit November 2011 hält er zudem die Universitätsprofessur „Medienrecht und Öffentliches Recht einschließlich ihrer theoretischen Grundlagen“ an der Fakultät für Rechtswissenschaft der Universität Hamburg inne. Es handelt sich um eine gemeinsame Besetzung durch die Universität Hamburg und das Hans-Bredow-Institut. Der Schwerpunkt dieser Professur liegt auf der Forschung am Hans-Bredow-Institut. Zunächst fungierte er dort als stellvertretender Geschäftsführer sowie als Leiter des Bereichs Medien- und Telekommunikationsrecht, seit Juli 2001 ist er Mitglied im Direktorium. Im Februar 2012 wurde er zudem zum Direktor des Alexander von Humboldt Instituts für Internet und Gesellschaft in Berlin berufen. Er ist zudem Mitglied des Committee of Experts on Internet Intermediaries (MSI-NET) des Europarates. Zuvor studierte er in Hamburg Rechtswissenschaft und Journalistik. Er lehrt seit 1997 im Schwerpunktbereich Information und Kommunikation des Fachbereichs Rechtswissenschaft der Universität Hamburg; seit Januar 2000 ist er Mitglied des Landesjustizprüfungsamtes. Im Juli 2009 Habilitation durch die Fakultät für Rechtswissenschaft der Universität Hamburg und Erteilung der Venia Legendi für Öffentliches Recht, Medienrecht und Rechtsphilosophie.

Die Schwerpunkte seiner Arbeit sind Kommunikationsfreiheiten, Probleme der rechtlichen Regulierung in Bezug auf Medieninhalte, Fragen des Rechts neuer Kommunikationsmedien und der Rechtsgrundlagen journalistischer Arbeit, aber auch rechtsphilosophische Grundlagen der Kommunikationsfreiheiten und Auswirkungen des Öffentlichkeitswandels auf das Recht. Dazu kommen Arbeiten zu Handlungsformen des Staates, etwa im Rahmen von Konzepten „regulierter Selbstregulierung“ oder von „Informational Regulation“. Viele seiner Arbeiten sind international vergleichend angelegt.

Stephan Dreyer ist Senior Researcher für Medienrecht und Media Governance am Hans-Bredow-Institut für Medienforschung, Hamburg. Das Forschungsinteresse des Juristen gilt dem Recht der neuen Medien, insbesondere rechtlichen Fragestellungen im Schnittbereich von Jugendschutz, Datenschutz und Verbraucherschutz, sowie den Herausforderungen, denen sich rechtliche Steuerung angesichts neuer Technologien, Angebotsstrukturen und Nutzungspraktiken gegenübersieht. Tätigkeitsschwerpunkte am Institut sind neben dem Jugendmedienschutz Untersuchungen zu den Möglichkeiten, Fragen und Grenzen der Steuerung durch Technik und durch Informationspflichten. Zudem führt er steuerungswissenschaftlich orientierte sowie komparative Untersuchungen von Systemen und Instrumenten informations- und kommunikationsbezogener Governance durch. Er ist seit 2002 als wissenschaftlicher Mitarbeiter am Hans-Bredow-Institut tätig. Zuvor hat der Diplom-Jurist Rechtswissenschaften mit dem Schwerpunkt Information und Kommunikation an der Universität Hamburg studiert.

Stephan Dreyer ist juristischer Sprecher des Beschwerdeausschusses und der Gutachterkommission der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM) und Jugendschutz-Sachverständiger bei der Freiwilligen Selbstkontrolle Unterhaltungssoftware GmbH (USK). Er ist Gründungsmitglied des „Center for Social Responsibility in the Digital Age“ (SRDA).

Impulse Algorithmenethik

Alle Veröffentlichungen sind abrufbar unter: https://algorithmenethik.de/impulse/

Impuls Algorithmenethik #1: Konrad Lischka und Anita Klingel. „Wenn Maschinen Menschen bewerten“. Bertelsmann Stiftung 2017. https://doi.org/10.11586/2017025

Impuls Algorithmenethik #2: Kilian Vieth und Ben Wagner. „Teilhabe, ausgerechnet“. Bertelsmann Stiftung 2017. https://doi.org/10.11586/2017027

Impuls Algorithmenethik #3: Konrad Lischka und Christian Stöcker. „Digitale Öffentlichkeit“. Bertelsmann Stiftung 2017. https://doi.org/10.11586/2017028

Impuls Algorithmenethik #4: Katharina Zweig, Sarah Fischer und Konrad Lischka. „Wo Maschinen irren können. Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung“. Bertelsmann Stiftung 2018. https://doi.org/10.11586/2018006

Adresse | Kontakt

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telefon +49 5241 81-0

Dr. Sarah Fischer
Project Manager
Telefon +49 5241 81-81148
sarah.fischer@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de

BertelsmannStiftung