Automatisch erlaubt?

Fünf Anwendungsfälle algorithmischer Systeme auf dem juristischen Prüfstand

BertelsmannStiftung

Automatisch erlaubt?

Fünf Anwendungsfälle algorithmischer Systeme auf dem juristischen Prüfstand

Impressum
© Januar 2020
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Verantwortlich
Carla Hustedt

Autoren
Prof. Dr. Mario Martini, Dr. Jonas Botta, David Nink und Michael Kolain

Lektorat
Rudolf Jan Gajdacz, team 4media&event, München

DOI 10.11586/2019067 https://doi.org/10.11586/2019067

Inhalt

1 Vorwort

Algorithmen sind gekommen, um zu bleiben. Sie haben längst Einzug in unseren Alltag gehalten und bestimmen zunehmend über gesellschaftliche Teilhabe von Menschen. Algorithmische Systeme gewähren bisher Benachteiligten neue Chancen in zentralen Bereichen unseres Lebens wie Bildung, Arbeit oder Gesundheit. Umgekehrt können sie aber auch diskriminierende Muster reproduzieren und soziale Ungleichheit verfestigen.

Die Diskussion über den ethischen Einsatz von Algorithmen kommt selten ohne abschreckende Anwendungsbeispiele aus den USA oder China aus. Die Auseinandersetzung mit solchen Szenarien, die zuweilen an die bekannte Netflix-Serie Black Mirror erinnern, kann helfen, sich als Gesellschaft darüber bewusst zu werden, wie ein alternativer europäischer Weg aussehen sollte. Ein Weg, der dem Gemeinwohl einen höheren Stellenwert einräumt als in den USA und anders als in China ein hohes Maß an individueller Freiheit wahrt. Ein solches Zielbild, das Werte und Wettbewerbsfähigkeit miteinander verbindet, erfordert einen rechtlichen Rahmen, der diese Balance klug austariert.

Die Entwicklung konkreter Regulierung, wie sie bspw. die Präsidentin der Europäischen Kommission, Ursula von der Leyen, für die ersten hundert Tage ihrer Amtszeit angekündigt hatte,[1] erfordert eine klare Problemanalyse. Die Frage, in welchem Umfang dem missbräuchlichen Einsatz algorithmischer Systeme bereits heute rechtliche Grenzen gesetzt sind und wo Lücken bestehen, muss Startpunkt der Debatte über Regulierungsbedarfe sein. Insbesondere in sensiblen Bereichen, wie bei richterlichen Entscheidungen, der Vergabe von Studienplätzen oder bei der Unterstützung von Polizeiarbeit, gilt es, den bestehenden Rechtsrahmen zu überprüfen.

Die Autorengruppe um Professor Mario Martini hat die aktuelle politische Aufmerksamkeit für das Thema zum Anlass genommen, diese Übung für fünf prominente Beispiele des Einsatzes algorithmischer Systeme zu übernehmen: In dieser Studie stellen sie vor, ob und unter welchen Bedingungen algorithmische Systeme in Deutschland bei der Studienplatzvergabe, in der Studienberatung, bei der Prognose von Straftaten zur Steuerung der Polizeiarbeit, bei richterlichen Entscheidungen und für kommerzielle Zwecke auf Basis von Daten aus sozialen Netzwerken eingesetzt werden dürfen.

Sei es das Recht auf informationelle Selbstbestimmung, politikfeldspezifische Gesetzgebung oder auch die seit 2018 wirksame Datenschutz-Grundverordnung (DS-GVO) – bestehende Regulierung setzt dem Einsatz von Algorithmen in vielen Fällen schon wesentliche Grenzen. Deutlich wird das am Beispiel der algorithmenbasierten Studienberatung, die sich mit Programmen wie dem eAdvisor in den USA zunehmend verbreitet. Neben den Landeshochschulgesetzen regelt vor allem die DS-GVO den Umgang mit den personenbezogenen Daten der Studierenden. Der Zweckbindungsgrundsatz der Verordnung schützt vor einer unbegrenzten Verknüpfung und Auswertung der persönlichen Informationen. Auch verbietet die DS-GVO, dass auf eine algorithmische Analyse eine automatisierte Entscheidung folgt und Betroffene ohne menschliches Zutun bspw. zu Kursen zugelassen oder sanktioniert werden. Dennoch können ähnliche Softwaresysteme auch in Deutschland zur Anwendung kommen, wenn sie nicht voll-, sondern nur teilautomatisiert eingesetzt werden. Doch wo genau liegt die Grenze zwischen Entscheidungsfindung und Entscheidungsunterstützung? In der Betrachtung der fünf Fallstudien wird immer wieder deutlich, dass das Zusammenspiel maschineller mit menschlichen Entscheidungen rechtlich noch nicht ausreichend geklärt ist und in fast allen Anwendungsbeispielen eine Herausforderung darstellt.

Die Fallbeispiele gewähren uns interessante Einblicke in die Details der deutschen Rechtsordnung, doch eine simple, aber wichtige Erkenntnis ist allen fünf juristischen Tiefenbohrungen gemein: Die US-amerikanischen Anwendungsfälle, die mit personenbezogenen Daten gespeist vollautomatisierte Entscheidungen treffen, können nicht ohne Weiteres nach Deutschland übertragen werden. Statt über Negativszenarien zu diskutieren, die durch den bestehenden Rechtsrahmen von vorneherein ausgeschlossen sind, sollte sich die Debatte auf die Analyse

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf (Download 11.11.2019).

regulatorischer Lücken konzentrieren. Bei der Schließung dieser Leerstellen gilt es, stets dafür Sorge zu tragen, dass übergreifende Regelungen, bspw. der Datenschutz-Grundverordnung, mit politikfeldspezifischen Maßgaben, wie etwa dem jeweiligen Landeshochschulrecht, harmonisch ineinandergreifen. Das schließt auch nicht aus, bestehende Gesetze bei Bedarf so anzupassen, dass bislang rechtlich unzugängliche Potenziale algorithmischer Unterstützung, wie etwa bei der in einigen Bundesländern Professoren vorbehaltenden Studienberatung, gehoben werden können.

Diese Publikation ist Teil des Projekts „Ethik der Algorithmen“, in dem sich die Bertelsmann Stiftung mit den gesellschaftlichen Auswirkungen algorithmischer Entscheidungssysteme beschäftigt. Bislang erschienen 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), ein Papier zu Fehlerquellen und Verantwortlichkeiten in Prozessen algorithmischer Entscheidungsfindung (Zweig 2018), ein Gutachten zu den Potenzialen und Grenzen der europäischen Datenschutz-Grundverordnung für algorithmische Systeme (Dreyer und Schulz 2018), ein Lösungspanorama (Krüger und Lischka 2018), zwei Umfragen zur deutschen und europäischen Meinung über Algorithmen (Fischer und Petersen 2018; Grzymek und Puntschuh 2019), eine Analyse bestehender Gütekriterien für algorithmische Prozesse (Rohde 2018) sowie eine Untersuchung erfolgreicher Professionsethiken (Filipović, Koska und Paganini 2018). Darüber hinaus haben wir in einer Kooperation mit der Stiftung Neue Verantwortung mehrere Impulspapiere über konkrete Anwendungsbeispiele wie Predictive Policing (Knobloch 2018), Robo Recruiting (Knobloch und Hustedt 2019) oder Gesundheits-Apps (Klingel 2019) veröffentlicht, gemeinsam mit AlgorithmWatch einen Status-quo-Report über algorithmische Entscheidungsfindung in Europa herausgegeben (AlgorithmWatch 2019) und zuletzt das Sachbuch „Wir und die intelligenten Maschinen“ (Dräger und Müller-Eiselt 2019) veröffentlicht.

Um den Diskurs und die Debatte über die Ergebnisse dieser Studie zu erleichtern, veröffentlichen wir sie unter einer freien Lizenz (CC BY-SA 3.0 DE). Wir danken Professor Dr. Mario Martini und seinem Team für die produktive Zusammenarbeit und freuen uns mit ihm zusammen über Resonanz und natürlich auch jede Form konstruktiver Kritik an den Ergebnissen dieser Publikation.

Carla Hustedt
Projektleitung, Ethik der Algorithmen
Bertelsmann Stiftung

Ralph Müller-Eiselt
Direktor, Programm Megatrends
Bertelsmann Stiftung

ZUSAMMENFASSUNG

Automatisch erlaubt? Fünf Anwendungsfälle algorithmischer Systeme auf dem juristischen Prüfstand

Studienplatzvergabe

Studienplätze auf der Grundlage algorithmischer Systeme zu verteilen, ist im Grundsatz rechtlich zulässig („Ob"). Ein automatisiertes Verfahren muss aber so gestaltet sein, dass es den grundrechtlichen Teilhabeanspruch der Studienbewerber auf Zugang zu den verfügbaren Studienplätzen an staatlichen Hochschulen hinreichend achtet („Wie"). Das System darf einzelne Bewerber insbesondere nicht ungerechtfertigt gegenüber Mitbewerbern benachteiligen – etwa durch Vergabekriterien, die an den Wohnort oder das Geschlecht anknüpfen. Welche Kriterien für die Auswahl handlungsleitend sind, obliegt grundsätzlich allein dem Gesetzgeber – nicht den Hochschulen. Soll das System vollautomatische Entscheidungen über die Studienplatzbewerbungen treffen, muss der deutsche Gesetzgeber hierfür eine ausdrückliche Rechtsgrundlage aus der Taufe heben (Art. 22 Abs. 1, Abs. 2 lit. b DS-GVO).

Studienberatung

An US-amerikanischen Hochschulen kommen zunehmend algorithmenbasierte Studienberatungsprogramme zum Einsatz. Ein Beispiel ist eAdvisor. Ein solches System an deutschen Hochschulen einzusetzen, ist zum einen nur zulässig, wenn das einschlägige Landeshochschulgesetz nicht abschließend regelt, wer die Studien(fach)beratung durchzuführen hat (und den Hochschulen somit ein entsprechender Handlungsspielraum verbleibt). Zum anderen müsste eine datenschutzrechtliche Erlaubnis (im Sinne des Art. 6 DS-GVO bzw. des einschlägigen Landesrechts) die Datenverarbeitung decken. Insbesondere der Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO) verwehrt es den Hochschulen grundsätzlich, personenbezogene Daten der Studierenden unbegrenzt auszuwerten und neu miteinander zu verknüpfen.

Predictive Policing

Predictive Policing verheißt, durch eine automatisierte Auswertung unterschiedlicher Daten raum- oder personenbezogene Wahrscheinlichkeitsaussagen über Straftaten zu treffen und dadurch die Arbeit der Polizeibehörden zu optimieren. Auch die deutsche Polizei bedient sich zunehmend dieser Methode. Hierzulande ist ihr Einsatz (noch) auf Einbruchsdiebstähle begrenzt. Das System operiert nicht mit personenbezogenen, sondern mit raumbezogenen und aggregierten anonymisierten Daten. Es unterliegt daher grundsätzlich nicht den Regelungen des Datenschutzrechts. In anderen Ländern geht Predictive Policing deutlich weiter: In den USA kommen bspw. Listen zum Einsatz, die den Bürgern einer Stadt polizeitaktische Risikoscores zuordnen. Solche Listen wären in dieser Form in Deutschland nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar. Denn sie greifen in einer Tiefe in die Privatsphäre betroffener Bürger ein, die außer Verhältnis zu dem verfolgten staatlichen Gefahrenabwehrzweck stehen.

Gerichtsentscheidungen

(Straf-)richterliche Entscheidungen durch algorithmenbasierte Verfahren, z. B das Prognosesystem COMPAS, zu unterstützen, ist in Deutschland nur zulässig, sofern dies die richterliche Unabhängigkeit, das Prinzip des gesetzlichen Richters und die sonstigen Prozessgrundrechte (Recht auf ein faires Verfahren etc.) nicht verletzt. Automatisierte Systeme dürfen insbesondere keine faktische oder rechtliche Bindungswirkung entfalten (insbesondere müssen sie dem Automation Bias entgegenwirken) und müssen technisch und inhaltlich transparent sein. Die Systeme dürfen nicht an sachfremde oder besonders geschützte Merkmale i. S. d. Art. 3 Abs. 3 GG, wie Herkunft, Religion oder Geschlecht, anknüpfen.

Auswertung des Informationsstroms sozialer Netzwerke durch Unternehmen

Längst sind soziale Netzwerke aus dem Alltag vieler Menschen nicht mehr wegzudenken. Solche Netzwerke sind nicht nur ein Resonanzraum der Gesellschaft, sondern auch eine Fundgrube, um die Vorlieben und Eigenheiten potenzieller und aktueller Kunden besser zu verstehen. Das Vertragsverhältnis zwischen Nutzer und sozialem Netzwerk gestattet es Anbietern sozialer Plattformen grundsätzlich nicht, personenbezogene Daten an Dritte weiterzugeben. Will ein Unternehmen sich die Datenweitergabe an Dritte im Wege der Einwilligung einräumen lassen, muss diese für den Nutzer dann jedoch klar erkennbar sein. Auch ohne Einwilligung darf ein Unternehmen nutzergenerierte Daten eines (potenziellen) Kunden aus sozialen Netzwerken oder anderen Quellen grundsätzlich aber dann auswerten, wenn dieser die Informationen selbst „offensichtlich öffentlich gemacht“ hat (vgl. Art. 9 Abs. 2 lit. e DS-GVO). Unterhalb dieser Grenze ist eine Informationsanalyse sozialer Netzwerke ad personam nur dann zulässig, wenn das Interesse an der Auswertung die (insbes. grundrechtlich geschützten) Interessen des Betroffenen im Einzelfall überwiegt (Art. 6 Abs. 1 UAbs. 1 S. 1 lit. f DS-GVO).

! Reformbedarf der DS-GVO !

Seit die DS-GVO im Mai 2018 Geltung erlangt hat, sind den Mitgliedstaaten in großem Umfang die Hände gebunden, algorithmische Systeme in eigener Kraftanstrengung zu regulieren: Das EU-Datenschutzrecht reklamiert für sich den Anspruch, die rechtlichen Vorgaben für den Umgang mit personenbezogenen Daten im Grundsatz vollständig zu harmonisieren (Martini 2019a: 360). Auf die Eigenheiten algorithmenbasierter Entscheidungsverfahren und lernfähiger Systeme („Künstliche Intelligenz“) hat der EU-Gesetzgeber die DS-GVO bislang aber nicht ausreichend passgenau zugeschnitten. Für vollautomatisierte Verfahren ohne jegliche menschliche Beteiligung etabliert sie zwar bereits enge Schranken (siehe Art. 22 DS-GVO). Den praktisch sehr wichtigen Bereich entscheidungsunterstützender Softwareanwendungen hat er bislang aber nicht mit hinreichend klaren Regelungen adressiert. Die DS-GVO hinterlässt insoweit eine Regelungslücke, welche die Union zeitnah schließen sollte.

3 Einleitung

Schenkt man den Begeisterungsstürmen über technische Innovationen Glauben, entsteht der Eindruck: Die digitale Transformation ist eine Einbahnstraße in ein „kybernetisches Zeitalter“. Intelligente Maschinen nehmen den Menschen dort als steuernde Kraft allmählich das Zepter aus der Hand.

In diesem Prozess stellt sich Europa bisweilen wie das gallische Dorf der Digitalisierung auf: Die kantischen Werte der Freiheit beschwörend, bemühen sich die Europäer redlich, technologischer Übermacht aus Übersee Gegenwehr zu bieten. Zusehends beschleicht sie aber das dumpfe Gefühl, sich in dem eng geknüpften regulatorischen Netz selbst zu verfangen und eigenen digitalen Hoffnungsträgern den Weg an die digitale Spitze zu verstellen. Die Angst, mit seinem ethischen Rigorismus könnte das gute alte europäische Dorf schleichend den Anschluss an die technologische Zukunft verlieren und im Wettrennen um Daten sowie die besten Anwendungen Künstlicher Intelligenz auf der Strecke bleiben, greift um sich: Europa hat es weder vermocht, ein soziales Netzwerk aus der Taufe zu heben, das mit Facebook, Twitter, Instagram & Co. konkurrieren kann, noch hat es einen Smartphone-Hersteller hervorgebracht, der in der internationalen Liga auf Dauer mitspielen kann. Stattdessen teilen vor allem die Vereinigten Staaten und China den Weltmarkt unter sich auf.

Immerhin hat Deutschland mit seinen hoch qualifizierten Ingenieuren und leistungsfähigen Unternehmen für Elektrotechnik und Maschinenbau die Chance, in der Robotik und Industrie 4.0 mehr als nur Akzente zu setzen. Doch die Perfektion deutscher Ingenieurskunst, die sich in der analogen Welt als Exportweltmeister inkrementeller Verbesserungen profiliert hat, tut sich mit der Agilität und Experimentierfreude des neuen digitalen Kosmos schwer. Längst hat sich dort als Grundmodus durchgesetzt, Innovationen nicht mit letztem Feinschliff auf den Markt zu bringen, sondern Software sich stets im Praxistest vollenden zu lassen.

Im Wettbewerb um die besten Produkte tut sich der alte Kontinent trotz seiner exzellenten Talente und guten Infrastruktur nicht nur schwer damit, mit technologischen Neuschöpfungen den Sprung in den Markt zu wagen, sondern auch damit, diese dann konsequent kommerziell umzusetzen. Die digitalen Giganten aus Übersee und Fernost haben sich – auch aufgrund einer anderen, auf Risikokapital aufbauenden Unternehmenskultur – besser in Stellung gebracht: Sie folgen dem Leitmotiv „done is better than perfect“ und horten bereits einen reichen Datenschatz, den sie scheinbar hemmungslos ausbeuten. Denn sie wissen, dass Trainingsdaten aus der realen Welt das Lebenselixier maschinellen Lernens sind.

Diese technologische Vorrangstellung über digitale Informationsinfrastrukturen, die für das gesellschaftliche Miteinander von zentraler Bedeutung sind, erzeugt eine ethische Spannungslage: Das Silicon Valley exportiert mit lieblichem Pathos und dem Versprechen, das alles sei nur zu unserem Besten, auch seine eigenen Wertvorstellungen von Privatheit und Selbstbestimmung als Topographie des Morgen in die „alte“ Welt. Technische Innovationen, die den Markt erobern, durchlaufen in der Folge zunächst einen von europäischen Normen entkoppelten Entwicklungsprozess, um anschließend frontal auf die Wertvorstellungen der EU zu prallen. Viele dieser Schöpfungen beargwöhnt der *homo europeus* heute zwar noch mit einer Mischung aus ungläubigem Staunen und Verwunderung aus der Ferne. Vielfach stellt sich aber weniger die Frage, *ob*, sondern *wann* sie auch in das Abendland Einzug halten. In Gestalt der Datenschutz-Grundverordnung (DS-GVO) hat die EU einen Zaubertrank angerührt, den sie als Gegenmittel gegen neugierige Blicke lernfähiger Softwareanwendungen einsetzen will. Wie gut er der Union bekommt, ist noch nicht ausgemacht. Die einen erkennen in der DS-GVO eine „Magna Charta des Persönlichkeitsschutzes“, die anderen verspotten sie als „Regulierungsmonster“.

Fünf viel diskutierte Anwendungen aus dem Maschinenraum der digitalen Pioniere, die kritische Stimmen als Vorboten einer digitalen Invasion geißeln, legt die Studie paradigmatisch unter das analytische Mikroskop der Rechtswissenschaft und untersucht sie darauf, ob sie nach Maßgabe des nationalen sowie des unionalen Rechts zulässig wären. Der Fokus der Studie liegt dabei auf Anwendungen, die auf den öffentlichen Sektor zielen. Der Blick fällt zunächst auf Innovationen im Bildungssektor: Softwaresysteme, die im Rahmen der Studienplatzvergabe (Fallstudie 1) und der Studienberatung (Fallstudie 2) im Ausland für Aufsehen gesorgt haben. Es folgen zwei Analysen aus dem Polizei- und Gerichtswesen: Sie unterziehen die Phänomene „Predictive Policing“ (Fallstudie 3) und

softwareunterstützte Entscheidungen der Strafjustiz – am Beispiel des Systems COMPAS – (Fallstudie 4) einer rechtlichen Untersuchung am Maßstab des deutschen Rechts. Den Abschluss markiert eine Fallstudie zur Frage, inwiefern private Unternehmen auf den Datenschatz sozialer Netzwerke zugreifen dürfen, um daraus personalisierte Angebote für ihre Kunden zu stricken (Fallstudie 5).

Den ausländischen Anwendungsszenarien tritt die Studie dabei weder mit einem Obelix'schen „Die spinnen im Silicon Valley!" gegenüber noch verfolgt sie das Ziel, technische Innovationen aus dem akademischen Elfenbeinturm heraus moralisch-ethisch abzukanzeln. Vielmehr will sie die Entwicklungen mit wissenschaftlicher Neugier und juristischem Augenmaß an den Vorgaben unserer Rechts- und Gesellschaftsordnung messen: Mit dem Seziermesser der juristischen Methodik ergründet sie Schicht für Schicht, wie die technologischen Phänomene rechtsdogmatisch einzustufen sind. Dabei lässt sie sich von dem Bemühen leiten, nach gangbaren Wegen zu suchen, wie sich die Grundwerte der informationellen Selbstbestimmung, der freien Persönlichkeitsentfaltung und des demokratischen Rechtsstaats mit den Potenzialen der fortschreitenden Digitalisierung versöhnen lassen.

Für Europa liegt in einem solchen differenzierten Vorgehen womöglich eine Chance: Auch in anderen Ländern, insbesondere in den USA, wächst das Bedürfnis, in komplexen digitalen KI-Ökosystemen mehr Kontrolle über die eigenen Daten erlangen zu können. Dahinter steckt letztlich ein universales menschliches Anliegen: das Bedürfnis nach Vertrauen. Vertrauen in Produkte und Dienste herzustellen, gehört in Europa zur DNA der Marktfähigkeit. Diesen – womöglich auch wirtschaftlich zentralen – Startvorteil kann der alte Kontinent im Idealfall im weiteren Prozess der Digitalisierung auch international ausspielen.

Da Künstliche Intelligenz und Algorithmen eine gesellschaftliche Grundfrage adressieren, darf sich nach Überzeugung der Autoren auch die wissenschaftliche Auseinandersetzung nicht im disziplinären Fachdiskurs erschöpfen. Sie muss sich vielmehr anschlussfähig zeigen, insbesondere das Wissen der Rechtswissenschaft in – auch für Nichtjuristen – verständlicher, kurzer und eingängiger Form in die Gesellschaft hineintragen. Um diesem Ziel zu entsprechen, erklärt die Studie rechtliche Spezifika ausführlicher als einem rein juristischen Publikum. Umgekehrt verzichtet sie auf manche rechtliche Vertiefung sowie Breite der wissenschaftlichen Nachweise, die im Rahmen einer juristischen Fachpublikation angezeigt wären.

Das Werk ist auf dem Stand vom Januar 2020. Mein besonderer Dank gilt meinen Mitautoren Jonas Botta, Michael Kolain und David Nink sowie der sehr tatkräftigen inhaltlichen Unterstützung durch die Mitglieder meines Teams, allen voran Jan Mysegades, Jonathan Hain und Matthias Hohmann.

Speyer, Januar 2020 Prof. Dr. Mario Martini

4 Der Algorithmus als universitärer Pfortenwächter?

Zur rechtlichen Zulässigkeit einer Studienplatzvergabe durch Algorithmen

Prof. Dr. Mario Martini und Dr. Jonas Botta

Generationen von Abiturienten kennen es: das atemberaubende Gefühl, nach zermürbenden Tagen und Nächten – zwischen Hoffen und Bangen, Demut und Euphorie – das lang ersehnte Abschlusszeugnis in den Händen zu halten. Dem frischgebackenen Abiturienten öffnet es viele Türen: ein Studium der Medizin, der Psychologie oder der Rechtswissenschaft – und im Idealfall die Qual der Wahl. Wer die allgemeine Hochschulreife erreicht, empfindet einen Moment der Freiheit, dem ein ganz eigener Zauber innewohnt. Wollen jedoch zu viele Bewerber durch dieselbe Tür schreiten, kommt es unweigerlich zum Stau und zu ausgefahrenen Ellenbogen. Was also, wenn die Wunschuniversität Erstsemester in spe an ihren Toren abweist?

4.1 Per Algorithmus an die Universität – Vorbild Frankreich?

In Frankreich übernimmt ein Algorithmus die Aufgabe, die knappen Studienplätze als „Pfortenwächter“ zu verteilen. An dem Programm *Parcoursup* kommt kein Student vorbei. Seit der Gesetzgeber es zum Studienjahr 2018/2019 eingeführt hat, um die Studienplatzvergabe neu zu organisieren, regt sich in der Schülerschaft allerdings engagierter Protest: Das Programm beschneide die Studierfreiheit und etabliere undurchsichtige Verteilungsregeln (Pantel 2018).

Neu ist die automatisierte Verteilung nicht. Ihre ungelösten Probleme sind in Frankreich altbekannt. Denn schon seit zehn Jahren setzt Deutschlands Nachbarland algorithmengestützte Systeme ein, um die Mehrheit der Bachelorstudienplätze zentral zu vergeben. Bereits das Vorgängerprogramm *Admission Post Bac* sah sich einem Sturm der Kritik ausgesetzt – in erster Linie, weil es den Wohnort der Bewerber als relevantes Kriterium in seine Entscheidung einbezog.[2] Dadurch bevorzugte der Algorithmus Schüler aus den wohlhabenden Pariser Innenstadtbezirken gegenüber ihren Altersgenossen aus den *Banlieues* oder südlichen Küstendépartements, wenn sie sich für die französischen Spitzenuniversitäten bewarben, die vornehmlich in der Hauptstadt ansässig sind. Erst ein langwieriges Klageverfahren brachte das volle Ausmaß der Ungleichbehandlung ans Licht (Lischka und Klingel 2017: 25 f.; vgl. zu den informationsfreiheitsrechtlichen Implikationen auch Martini 2019a: 47, 342 f.).

Der diskriminierenden Praxis sollte das neue Programm *Parcoursup* ein Ende bereiten. Doch in einem Aspekt schreibt das neue französische Verteilungsregime eine unrühmliche Tradition der vorherigen Software fort: Die Vergabekriterien liegen nicht vollständig offen. Die Behörden haben zwar inzwischen den staatlichen Verteilungscode veröffentlicht (wenn auch ohne erläuternde Ausführungen, was ihn für den Laien gänzlich unbrauchbar macht).[3] Doch bei stark nachgefragten Studienfächern wie Medizin liegt es nicht allein in den Händen des Programms, sondern (auch) an den Hochschulen, die endgültige Auswahlentscheidung zu treffen – und diese schweigen sich über ihr Vorgehen aus (Boudinar-Zabaleta 2019).[4] Die Studienplatzvergabe nach französischem Modell erweist sich damit für die Betroffenen in weiten Teilen als Blackbox.

---

[2] Die französische Datenschutzbehörde *Commission Nationale de l'Informatique et des Libertés* (CNIL) hat in der Vergangenheit zudem weitere Datenschutzverstöße der *Admission Post Bac* gerügt (Entscheidung v. 30.8.2017, n° MED-2017-053). Sie bemängelte insbesondere, dass die französische Regierung die Studienplatzanwärter nicht auf die Verwendung und die Funktionsweise des Algorithmus hingewiesen habe und sie zudem im Unklaren darüber gelassen habe, wer ihre personenbezogenen Daten einsehen konnte. Eine Zusammenfassung der Entscheidung findet sich bei Debet 2017.

[3] Einzusehen unter: https://framagit.org/parcoursup/algorithmes-de-parcoursup (Download 11.11.2019).

[4] Betroffenen verheißt derzeit auch der Rechtsweg wenig Hoffnung. So hatte das Verwaltungsgericht Guadeloupe zwar die *Université des Antilles* angewiesen, die verwendeten Kriterien offenzulegen (Urteil vom 4.2.2019,

4.2 Das deutsche Hochschulzulassungssystem im Umbruch

Auch in Deutschland kann nicht jeder Schulabgänger auf den Studienplatz seiner Wahl zählen. Die Ausbildungskapazitäten, die der Staat zur Verfügung stellt, decken die Nachfrage nicht vollständig. Die Folge sind Mehrfachbewerbungen und -zulassungen, Überbuchungen, Absagen, lange Wartelisten und bisweilen einzelne verwaiste Studienplätze. Wie eine „Verwaltung des Mangels" am besten gelingt, d. h. wie die Studienplätze auf die Bewerber knappheitsgerecht zu verteilen sind, gehört zu den beständigen Grundrätseln der deutschen Hochschulpolitik. Ihren Handlungsrahmen stecken das Verfassungsrecht (Abschnitt 4.2.1) sowie – als einfachrechtliche Konkretisierungen der grundgesetzlichen Vorgaben – das Hochschulzulassungsrecht des Bundes (Abschnitt 4.2.2) und der Länder (Abschnitt 4.2.3) ab.

4.2.1 Verfassungsrechtlicher Rahmen

Das Grundgesetz (GG) stärkt dem Einzelnen gegenüber den Universitäten den Rücken: Es verbürgt grundsätzlich jedem Deutschen einen Anspruch auf Zulassung zum Hochschulstudium. Dieser Anspruch leitet sich aus der Berufsfreiheit (Art. 12 Abs. 1 GG) in Verbindung mit dem Gleichheitsgrundsatz (Art. 3 Abs. 1 GG) und dem Sozialstaatsprinzip (Art. 20 Abs. 1 GG) ab.[5]

Ein verfassungsrechtlich verbürgtes Recht auf einen spezifischen Studienplatz im Wunschfach an der eigenen Traumuniversität existiert jedoch nicht: Der Staat ist nicht verpflichtet (und wäre damit ohnedies überfordert), in unbegrenzter Höhe Ausbildungsangebote – bspw. Medizinstudienplätze für jedermann – vorzuhalten. Vielmehr genießt der einzelne Bewerber lediglich ein Recht darauf, nach Maßgabe objektiv sachgerechter und individuell zumutbarer Kriterien an den vorhandenen Studienplatzressourcen teilhaben zu können (sog. *derivatives Teilhaberecht* der Bewerber).[6] Die Verfassung gibt dem Staat auf, ein Verfahren der Studienplatzzulassung zu entwickeln, das diesem Gebot gerecht wird.

4.2.2 Bundesebene

Ursprünglich lag das Zulassungsrecht grundsätzlich in den Händen der Hochschulen selbst (Thieme 2004: Rn. 40).[7] Erst die Hochschulreformen der 1960er Jahre verrechtlichten und zentralisierten die Materie, als die Studierendenzahlen rapide anstiegen (Lindner 2017: 683 f. mit Rn. 98 f.). Im Jahr 1969 fiel dann nach einer Verfassungsänderung dem Bundesgesetzgeber die Rahmenkompetenz für das Hochschulwesen zu (Walter 2018: Rn. 1). Auf ihrer Grundlage (Art. 75 Abs. 1 Nr. 1a GG a. F.) konnte er die Grundzüge des Hochschulrechts festlegen; Detailregelungen blieben ihm hingegen versagt.[8]

Zum Erlass des Hochschulrahmengesetzes (HRG) des Bundes (1976) und eines Staatsvertrags der Länder (1972) kam es erst im Gefolge des ersten Grundsatzurteils des Bundesverfassungsgerichts zur Studienplatzvergabe im Jahr 1972.[9] Das Gericht hatte klare grundrechtliche Maßstäbe für die Verteilung der Studienplätze angemahnt.

Seit der Föderalismusreform des Jahres 2006 ist die spezielle Materie der Hochschulzulassung nun Teil der konkurrierenden Gesetzgebung (Art. 74 Abs. 1 Nr. 33 GG): Sowohl der Bund als auch die einzelnen Länder können

---

n° 1801094; dazu Chaltiel 2019). Der *Conseil d´État* hat dieses Urteil jedoch bereits aufgehoben (Urteil vom 12.6.2019, n° 427916).

[5] BVerfGE 33, 303 (332) – Numerus clausus I.; dazu bspw. Martini und Ziekow 2017: 44 ff.

[6] Vgl. BVerfGE 147, 253 (307) – Numerus clausus III. Private Hochschulen sind zudem nur mittelbar durch die Grundrechte ihrer Studienbewerber gebunden. Sie können sich zugleich selbst umfangreich auf Grundrechte berufen – neben der Wissenschaftsfreiheit (Art. 5 Abs. 3 S. 1 GG) vorrangig auf ihre unternehmerische Freiheit (Art. 12 Abs. 1 GG) und die Eigentumsgarantie (Art. 14 Abs. 1 GG).

[7] Weiterführend zur historischen Entwicklung des Hochschulzulassungsrechts Bode 2013: 349 ff.

[8] „Der Bund [war] im Hochschulbereich zu einer außerordentlich zurückhaltenden Gesetzgebung verpflichtet" (BVerfGE 112, 226 [243] – Studiengebühren).

[9] Vgl. BVerfGE 33, 303 – Numerus clausus I.

den Bereich im Grundsatz regulieren (vgl. dazu auch Martini und Ziekow 2017: 35 ff.).[10] Bis auf Weiteres behält das Hochschulrahmengesetz (HRG) des Bundes aber seine rechtliche Wirkung (Art. 125b Abs. 1 GG).[11] In seinen §§ 29 ff. hat es die Eckpfeiler der Hochschulzulassung (d. h. vornehmlich die Ermittlung und Festsetzung der Ausbildungskapazitäten) in das Regulierungsfundament des Hochschulrechts eingerammt.

4.2.3 Länderebene

Der „Staatsvertrag über die Hochschulzulassung“ (StV v. 2019) formt die §§ 29 ff. HRG näher aus.[12] Auf der Grundlage seines Vorgängers (des „Staatsvertrags der Länder über die Errichtung einer gemeinsamen Einrichtung für Hochschulzulassung v. 5.6.2008“) hatten die Länder die Stiftung für Hochschulzulassung errichtet (Art. 1 StV v. 5.6.2008). Sie führt zum einen die Platzvergabe für bestimmte Studiengänge (wie Medizin oder Pharmazie) eigenständig durch (*zentrales Vergabeverfahren*; Abschnitt 4.2.3.1). Zum anderen unterstützt sie die Hochschulen bei den örtlichen Zulassungsverfahren (*dialogorientiertes Serviceverfahren*; Abschnitt 4.2.3.2).

4.2.3.1 Zentrales Vergabeverfahren

Das zentrale Vergabeverfahren greift als Auswahlkriterien einerseits auf die Abiturnote (30 Prozent der Studienplätze; Art. 10 Abs. 1 S. 1 Nr. 1 StV v. 2019) sowie schulnotenunabhängige Kriterien, wie fachspezifische Studieneignungstests oder Auswahlgespräche, zurück (10 Prozent; Art. 10 Abs. 1 S. 1 Nr. 2 i. V. m. Abs. 2 StV v. 2019).[13] Andererseits verteilen die Hochschulen 60 Prozent der Studienplätze nach einem eigenen Auswahlverfahren („AdH“[14]). Sie müssen dabei aber die Vorgaben des Art. 10 Abs. 1 S. 1 Nr. 3 i. V. m. Abs. 3 StV v. 2019 beachten. Insbesondere müssen sie sich bei ihrer Zuteilungsentscheidung auf das Ergebnis in der Hochschulzugangsberechtigung und schulnotenunabhängige Kriterien im Sinne des Art. 10 Abs. 2 StV v. 2019 stützen.

Um gesamtgesellschaftlichen Bedürfnissen Rechnung zu tragen, hat der Bundesgesetzgeber auch Sonderquoten für bestimmte Bewerbergruppen gestattet (§ 32 Abs. 2 HRG). Deren Zulassungsspezifika dürfen die Länder näher ausgestalten,[15] insbesondere Härtefallregelungen für Bewerber mit lebensverkürzenden Erkrankungen vorsehen (vgl. § 32 Abs. 2 S. 1 Nr. 1 HRG), aber auch Sonderquoten für den besonderen öffentlichen Bedarf (§ 32 Abs. 2 S. 1 Nr. 2 HRG). Darunter fallen etwa Vorabquoten für Sanitätsoffiziersanwärter der Bundeswehr sowie die sog. *Landarztquote* (Bode 2018: Rn. 110 ff.; Martini und Ziekow 2017: 30 ff.). Sie gesteht Studienbewerbern, die sich bereit erklären, nach ihrer Approbation als Landarzt tätig zu werden, ein Sonderkontingent an Studienplätzen zu (vgl. § 2 Landarztgesetz NRW).[16]

---

[10] Macht der Bund von seiner Kompetenz Gebrauch, sind die Länder in ihrer Gesetzgebungskompetenz gesperrt (Art. 72 Abs. 1 GG).
[11] Auf ein neues „Bundeshochschulzulassungsgesetz“ hat der Bund bislang verzichtet. Von diesem könnten die Länder gleichwohl regulatorisch abweichen (Art. 72 Abs. 3 S. 1 Nr. 6 GG).
[12] Auf den neuen Staatsvertrag einigten sich im Frühjahr 2019 die Regierungen der Länder; vgl. https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMV17-1613.pdf (Download 11.11.2019). Dieser bedarf jedoch noch der Zustimmung der Landesparlamente. Die neuen Zulassungsregeln sollen ab dem Sommersemester 2020 gelten.
[13] Die Wartezeit ist hingegen kein Auswahlkriterium mehr (vgl. indes noch Art. 10 Abs. 1 Nr. 2 StV v. 5.6.2008). Selbiges gilt für die Ortspräferenz. Diese hatte ehemals eine wesentliche Rolle gespielt, da sich Bewerber nur für sechs von ihnen priorisierte Studienorte entscheiden konnten und die Mehrheit der Hochschulen verlangte, zumindest unter den ersten drei Ortswünschen zu sein. Dieser Praxis hatte das Bundesverfassungsgericht aber deutliche Grenzen gesetzt; BVerfGE 147, 253 (317 ff.) – Numerus clausus III.
[14] Das Akronym steht für „Auswahlverfahren der Hochschulen“.
[15] Insbesondere § 32 Abs. 1 S. 2, Abs. 2 S. 2, Abs. 3 Nr. 3 HRG; siehe auch Bode 2018: Rn. 81.
[16] Dazu Huster und Büscher 2019: 217 ff.

4.2.3.2 Dialogorientiertes Serviceverfahren

Das dezentrale dialogorientierte Serviceverfahren (DoSV) ermöglicht Hochschulen, auf das technische Know-how der Stiftung für Hochschulzulassung zurückzugreifen, wenn sie Plätze für grundständige Studiengänge[17] vergeben, die zwar einer örtlichen Zulassungsbeschränkung, aber nicht dem zentralen Vergabeverfahren unterliegen. Soweit die Hochschulen (wie im Regelfall) am DoSV teilnehmen, kann sich jeder Interessent über die Website https://hochschulstart.de nicht nur für Medizin oder Pharmazie, sondern bspw. auch für BWL, Jura oder Psychologie bundesweit bewerben.

Die Kriterien für das DoSV lehnen sich an das zentrale Vergabeverfahren an (vgl. Art. 10 Abs. 2 StV v. 2019). Die Landeshochschulzulassungsgesetze konkretisieren diese Vorgaben (Lindner 2017: 697 mit Rn. 141). Auch hier finden sich Vorabquoten für bestimmte Bewerbergruppen – etwa Spitzensportler oder Minderjährige (Bode 2018: Rn. 61 f.). Daneben ist der Numerus clausus maßgeblicher Türöffner. Beide Vergabeverfahren unterscheiden sich vornehmlich lediglich darin, dass die Teilnahme für die Hochschule im einen Fall (namentlich beim zentralen Vergabeverfahren) obligatorisch, im Falle des DoSV demgegenüber fakultativ ist.

Das System der Studienplatzvergabe im DoSV wie im AdH basiert auf dem sog. *Gale-Shapley-Algorithmus*. Er liegt auch dem französischen Programm *Parcoursup* zugrunde. Der Algorithmus ist so ausgerichtet, dass diejenigen Hochschulen und Bewerber zueinanderfinden, die sich in ihren individuellen Ranglisten gegenseitig präferiert haben (Bode und Reetz 2014: 412 mit Fn. 16).

4.3 Diskriminierungsfreie Auswahlkriterien

Neben den bekannten Auswahlparametern, allen voran der Abiturnote, haben die Länder auch immer wieder andere Auswahlmethoden erprobt – bspw. Landeskinder- (Abschnitt 4.3.1) oder Geschlechterquoten (Abschnitt 4.3.2). Vorstellbar ist es auch, andere Proxy-Variablen[18] bei der Entscheidung zu berücksichtigen (Abschnitt 4.3.3).

4.3.1 Wohnort

Den Wohnort der Bewerber zur Studienplatzvergabe heranzuziehen, wie es Frankreich lange Zeit praktiziert hat, ist auch dem deutschen System nicht gänzlich unvertraut. Unter dem Stichwort „Landeskinderregelung“ kursiert der Ansatz bereits seit mehreren Jahrzehnten in der Debatte.[19] Dem Konzept liegt ein landesväterlicher Fürsorgegedanke zugrunde: Die jeweiligen Landesgesetzgeber wollen ihre Abiturienten davor bewahren, ihre Heimat verlassen zu müssen und durch bundesweit ungleiche Notenvergaben bei der Bewerbung benachteiligt zu werden.

Landeskinderquoten hat die Rechtsprechung aber eine klare Absage erteilt[20] – und dies zu Recht: Sie widersprechen dem Grundverständnis der Verfassung. Denn „jeder Deutsche hat in jedem Lande die gleichen staatsbürgerlichen Rechte und Pflichten“ (Art. 33 Abs. 1 GG).

4.3.2 Geschlecht

Viele Studienfächer sind durch ein deutliches Geschlechtergefälle geprägt: Während medizinische Fächer bei Frauen in hoher Gunst stehen, sind es in den Ingenieurwissenschaften vorrangig Männer, die dieses Studium

[17] Grundständige Studiengänge führen zum Erwerb des ersten Hochschulabschlusses. Darunter fallen somit alle Bachelor- sowie Staatsexamensstudiengänge.
[18] Der Begriff steht für eine Variable, die an sich nicht direkt entscheidend ist, aber anstelle einer unmessbaren Variablen in die Berechnung einfließt.
[19] Vgl. BVerfGE 33, 303 (351 ff.) – Numerus clausus I.; Mehde 2019: 1028 ff.).
[20] Vgl. BVerfGE 33, 303 (348, 351 ff.) – Numerus clausus I.

aufnehmen.[21] In diesem Lichte hat als Korrektiv der Gedanke einer Studienplatz-Geschlechterquote – ähnlich wie im Fall der brandenburgischen Abgeordnetenquote[22] oder der Vorstandsquote in Aufsichtsräten – auf den ersten Blick Charme. Berlin hatte eine solche Quote in sein Auswahlregime implementiert (§ 8a Berliner Hochschulzulassungsgesetz).

Das Bundesverfassungsgericht hat diese Norm jedoch als verfassungswidrig verworfen[23] – nicht deshalb, weil es die Unterrepräsentation eines Geschlechts schlechthin als unzulässiges Kriterium einstuft. Vielmehr fehlte der Landesvorschrift eine Grundlage in § 32 Abs. 4 HRG. Dieser regelt die Auswahlregelungen für Fälle der Ranggleichheit in der Abiturbestenquote abschließend. Nur eine Gesetzesänderung auf Bundesebene könnte einer Geschlechterquote bei der Studienplatzvergabe daher den Weg ebnen.

4.3.3 Finanzielle Situation sowie sonstige Proxy-Variablen

Dass niemand durch Geldzahlungen bestehende Verteilungsregelungen umgehen darf, versteht sich. Weniger eindeutig ist, ob der zuteilende Hoheitsträger die finanzielle Situation der Bewerber oder sonstige Proxy-Variablen (wie z. B. Leistungsstipendien oder Auszeichnungen[24]) in die Studienplatzverteilung einbeziehen darf, um etwaigen Studienabbrüchen vorzubeugen. Wer auf Nebenverdienste angewiesen ist, dem fehlen womöglich die Zeit und Fokussierung, um sein Studium erfolgreich und zeitnah zum Abschluss zu bringen. Das könnte den Gesetzgeber zu dem Gedanken inspirieren, BAföG-Empfänger entweder bei der Studienplatzverteilung zu bevorzugen oder ihnen nur in Städten mit günstigen Lebenshaltungskosten einen Hochschulplatz zuzuweisen (nicht etwa in München oder Hamburg).[25]

Zwar sind Studienbeiträge verfassungsrechtlich grundsätzlich zulässig, „solange sie nicht prohibitiv wirken und sozial verträglich ausgestaltet sind“.[26] Bereits bei der Bewerberauswahl an die finanzielle Situation des Einzelnen anzuknüpfen, verstieße jedoch gegen den grundrechtlichen Anspruch auf Hochschulzulassung nach Maßgabe des Art. 12 Abs. 1 i. V. m. Art. 3 Abs. 1 GG. Denn die finanzielle Leistungskraft steht in keinem sachlichen Bezug zu dem zu verteilenden knappen Gut „Zugang zu Bildung“.

4.4 Grundrechtliche Zulässigkeit eines zentralen Vergabealgorithmus

Angestoßen durch das jüngste Numerus-clausus-Urteil des Bundesverfassungsgerichts[27] sind die deutschen Regelungen für die Hochschulzulassung im Umbruch begriffen. Diese hochschulrechtliche Epochenwende könnte der Gesetzgeber als Gelegenheit beim Schopf ergreifen, die Studienplatzvergabe nach französischem Vorbild auf der Grundlage eines algorithmenbasierten Verfahrens zentral und automatisiert neu zu organisieren. Dafür müsste die Stiftung für Hochschulzulassung für das gesamte Zulassungssystem – und nicht nur für das aktuelle, als „zentral“ bezeichnete Vergabeverfahren – hauptverantwortlich sein bzw. dem Bund die ausschließliche Regelungskompetenz für die Hochschulzulassung zustehen.

---

[21] Siehe hierzu https://www.bpb.de/nachschlagen/zahlen-und-fakten/soziale-situation-in-deutschland/61669/studierende (Download 11.11.2019).
[22] Wehner 2019.
[23] BVerfGE 147, 253 (356 ff.) – Numerus clausus III.
[24] Vgl. hierzu auch Bode 2018: Rn. 106.
[25] Überspitzt ließe sich so zumindest der Rat der aktuellen Bundesbildungsministerin *Anja Karliczek*, nicht in den „teuersten Städten“ zu leben, weiterdenken; vgl. auch Himmelrath 2019.
[26] BVerfGE 134, 1 (13 ff.); Kempen: Rn. 184.2; a. A. Deppner und Heck 2008: 46 ff., die sich u. a. auf Art. 13 Abs. 2 lit. c des Internationalen Paktes über wirtschaftliche, kulturelle und soziale Rechte und die Völkerrechtsfreundlichkeit des Grundgesetzes berufen.
[27] BVerfGE 147, 253 – Numerus clausus III.

Ein automatisiertes Entscheidungsverfahren kommt gegenwärtig bereits in einem ersten Auswahlschritt des zentralen Vergabeverfahrens zum Einsatz, um den Bewerberpool zu verkleinern. Eine Studienplatzvergabe via Algorithmus ist auch in den weiteren Stufen der Studienplatzvergabe denkbar – solange es nicht gegen das individuelle grundrechtliche Teilhaberecht auf Zulassung zum Hochschulstudium verstößt: Es muss gewährleisten, dass ausschließlich objektiv sachgerechte und individuell zumutbare[28] Kriterien zur Anwendung kommen.[29]

Zumindest einen segensreichen Vorzug hat ein algorithmengesteuertes Auswahlverfahren: Der Algorithmus entscheidet typischerweise frei von Flüchtigkeitsfehlern, „Vitamin B“ und Korruption. Blickt man in die Realität der Studienplatzvergabe, ist das ein kaum zu unterschätzender Vorzug. Jenseits des Atlantiks sind in den letzten Jahren bspw. über 25 Millionen US-Dollar Bestechungsgelder geflossen, um finanzstarken Bewerbern begehrte Studienplätze an US-amerikanischen Eliteuniversitäten zu verschaffen.[30] In diesem Lichte erstrahlen automatisierte Verfahren gleichsam als Inbegriff einer konsistenten und willkürfreien Entscheidung. Die Hoffnungen richten sich darauf, dass die algorithmengestützte Studienplatzvergabe zumindest perspektivisch für die Bewerber transparentere sowie gerechtere Verfahren und für die Hochschulverwaltungen weniger administrativen Aufwand mit sich bringt.

Der Reiz eines algorithmenbasierten Vergabesystems liegt nicht nur darin, Studienbewerber auf der Grundlage „harter“ Kriterien wie der Abiturbestenquote bundesweit effizient unterschiedlichen Studiengängen zuweisen zu können. Er gründet vielmehr auch darauf, dass ein lernfähiges System (eigenständig) entscheidungserhebliche Kriterien identifizieren kann: So ist es etwa denkbar, dass eine Software Studienerfolgsfaktoren erkennt, die der Gesetzgeber oder die Hochschulen selbst noch gar nicht antizipiert bzw. als relevant ausgemacht haben. Datenschätze aus beruflichen und privaten Onlineplattformen wie *LinkedIn* oder *Facebook* könnten es technisch ermöglichen, Indikatoren dafür zu bestimmen, welche Bewerber sich im Studium als besonders erfolgreich entpuppen und welche Bewerbergruppen bspw. für ein Medizinstudium später am ehesten dazu gewillt sind, in ländlichen Regionen zu arbeiten.

Doch das deutsche Recht zieht Hochschulen, die mit diesem Ansinnen liebäugeln, eine klare Grenze: Die Wissenschaftsfreiheit (Art. 5 Abs. 3 GG) gewährt den Hochschulen grundsätzlich zwar einen Spielraum, die Auswahlparameter festzulegen. Ihnen kommt gleichwohl kein „Kriterienerfindungsrecht“ zu. Es ist vielmehr dem Gesetzgeber vorbehalten, die wesentlichen Entscheidungen für die Hochschulzulassung zu treffen.[31] Bundes- bzw. Landesgesetzgeber sind verfassungsrechtlich gehalten, durch ein Parlamentsgesetz einen Kriterienkatalog zu beschließen, an den sich die Hochschulen – ebenso wie ein Algorithmus, den ihre Auswahlmechanismen implementieren – zu halten haben.

4.5 Grundsätzliches Verbot vollautomatisierter Entscheidungen (Art. 22 Abs. 1 DS-GVO)

Nicht nur das deutsche Verfassungsrecht, auch das Unionsrecht setzt dem Einsatz neuer Technologien im Interesse der Rechte und Freiheiten des Einzelnen Schranken: Seit dem 25.5.2018 formt die Datenschutz-Grundverordnung (DS-GVO) den Rahmen des Datenschutzrechts unionsweit neu. Auf den ersten Blick stellt sie dem Einsatz algorithmenbasierter Studienplatzvergabesysteme eine unumstößliche Hürde in den Weg: Art. 22 Abs. 1 DS-GVO verbietet vollautomatisierte Einzelfallentscheidungen, die auf personenbezogenen Daten

[28] Im Gegensatz etwa zu einer Wartezeitquote, die darin mündet, dass Studienbewerber de facto länger auf einen Studienplatz warten müssen, als sie später tatsächlich studieren.
[29] BVerfGE 147, 253 (330 f.) – Numerus clausus III.
[30] Weiterführend von Petersdorff 2019.
[31] BVerfGE 147, 253 (310 f.) – Numerus clausus III.

beruhen und eine rechtliche oder vergleichbare Wirkung mit sich bringen. Ein Computer-Algorithmus darf die Studienplatzauswahl also grundsätzlich nicht eigenständig steuern. Die Entscheidungsgewalt muss vielmehr einem Menschen vorbehalten bleiben.[32]

Art. 22 Abs. 1 DS-GVO gilt aber nicht vorbehaltlos. Der Unionsgesetzgeber lässt weitgehende Ausnahmen zu: Die Landesgesetzgeber können insbesondere durch eine gesetzliche Vorschrift den Weg für eine automatisierte Studienplatzvergabe freimachen (Art. 22 Abs. 2 lit. b DS-GVO).[33] Sie müssen dann aber sicherstellen, dass der Betroffene ggf. auch verlangen kann, dass ein Mensch das Entscheidungsergebnis überprüft und sich ausreichend Gehör verschaffen kann (Art. 22 Abs. 2 lit. b i. V. m. Art. 22 Abs. 3; ErwGrd[34] 71 Abs. 1 S. 4 DS-GVO; dazu bspw. Martini und Nink 2017: 3 f.). Zudem dürfen ausschließlich „geeignete mathematische oder statistische Verfahren" für die algorithmenbasierte Studienplatzvergabe zur Anwendung kommen (ErwGr 71 UAbs. 2 S. 1 DS-GVO). Die Algorithmen müssen also dem wissenschaftlichen Standard entsprechen und auf einer korrekten Datenlage basieren (vgl. Martini 2018: Rn. 39d).

4.6 Grenzen algorithmischen Auswahlermessens

So sehr Computer als zuverlässige und korruptionsfreie Entscheider gelten, so wenig überflügelt die Maschine den Menschen als Entscheidungsträger in toto. Denn die Technik stößt dort an ihre Grenzen, wo sie nicht nur nach „harten" Faktoren (wie der Abiturbestenquote) entscheiden soll, sondern auch „weiche" Kriterien (wie Empathie oder Kommunikationsgeschick) an den Tag legen müsste, um den „optimalen" Studienbewerber (bspw. den zukünftigen Unternehmenslenker, Richter oder Arzt) treffsicher aus der Bewerberschar herauszufiltern. Den lebensweltlichen Kontext, in welchem sie Entscheidungen zu treffen hat, kann Software (jedenfalls noch) nicht hinreichend zuverlässig erfassen.

Vor allem Vergabekriterien, die nicht auf die Schulnoten abstellen, sondern die Persönlichkeit eines Bewerbers analysieren sollen, können maschinelle Verfahren bislang nicht in einer Weise vollständig abbilden, die dem vielschichtigen grundrechtlichen Anforderungsprofil gerecht wird. Diese Risiken potenzierten sich, wenn lernfähige Systeme zum Einsatz kämen (vgl. Martini 2019a: 47 ff. u. 334 ff.). Denn eine fortentwickelte Künstliche Intelligenz entwickelt die Entscheidungsparameter, mit denen sie ihre Zielvorgaben erreicht, zum Teil selbsttätig. Sie könnte bspw. auf der Grundlage ihres Datenpools unerkannt den Wohnort als Korrelationskriterium für einen Studienabbruch erkennen und sodann als maßgeblich dafür ausmachen, ob die Bewerbung erfolgreich ist oder nicht. Dies verletzte aber den grundrechtlichen Anspruch auf gleichheitsgerechte Hochschulzulassung:[35] Den Wohnort indirekt als Korrelationskriterium eines lernfähigen Systems zu berücksichtigen, benachteiligt Studienbewerber auf der Grundlage eines unzulässigen Differenzierungskriteriums mittelbar. Ähnliches gilt, wenn ein lernfähiges System dank seines Datensatzes bspw. einen Zusammenhang zwischen der Vermögenssituation der Eltern und dem Studienerfolg erkennt. Es ist dann geneigt, auch dieses Kriterium als Gewichtungsfaktor in seine Auswahlentscheidung aufzunehmen, obgleich es sich um eine verfassungsrechtlich unzulässige soziale Differenzierung handelt.

---

[32] Vor Geltung der DS-GVO war es demgegenüber noch erforderlich, dass die Verarbeitung dazu diente, Persönlichkeitsmerkmale des Betroffenen zu bewerten (Art. 15 Abs. 1 Datenschutz-Richtlinie bzw. § 6a Abs. 1 S. 1 BDSG a. F.). Bloße „Wenn-dann-Entscheidungen", wie die Anknüpfung der Studienplatzvergabe an einen konkreten Abiturdurchschnitt, unterfielen demnach nicht dem Verbot; vgl. von Lewinski: Rn. 11. Diese Einschränkung kennt das neue unionale Datenschutzrecht nicht; Dammann 2016: 312.

[33] Daneben eröffnet der Unionsgesetzgeber grundsätzlich die Möglichkeit, das Verbot durch eine ausdrückliche Einwilligung zu überwinden (Art. 22 Abs. 1 lit. c DS-GVO). Diese muss jedoch freiwillig ergehen (Art. 4 Nr. 11; Art. 7 Abs. 4 DS-GVO). Mit Blick auf die Machtasymmetrie, die zwischen Bürger und Behörde regelmäßig besteht, unterliegt sie jedoch besonderen Anforderungen; vgl. hierzu auch bspw. unten Abschnitt 5.3.2.1 sowie Martini und Botta 2019: 248 ff.

[34] Die Abkürzung steht für „Erwägungsgrund".

[35] Dazu, dass das Kriterium „Wohnort" kein zulässiges Auswahlkriterium verkörpert; siehe bereits oben Abschnitt 4.3.1.

Die Entscheidungskriterien eines Zuteilungsverfahrens muss der Gesetzgeber nicht nur auf einer abstrakt normativen Ebene vorgeben. Er muss in diesem System auch sicherstellen, dass sie sich bis in die tatsächliche Entscheidungsebene hinein in kontrollierbarer Weise abbilden. Darin manifestiert sich ein Wesensmerkmal der verfassungsrechtlichen Ordnung: Das Gesetz ist gleichsam die Aorta der Demokratie. Es trägt die politischen Leitentscheidungen des Parlaments als Ausfluss der politischen Willensbildung in den Vollzug der Staatsgewalt hinein. Insbesondere bei diskriminierungsanfälligen Entscheidungen, die nachhaltig auf den Lebensplan der Grundrechtsträger ausstrahlen, muss der Entscheidungsvollzug daher gewährleisten, dass das System den normativen Vorgaben des Gesetzes in allen Facetten folgt.

Dafür muss der Staat die Auswahltechnologie hinreichend überwachen und steuern können. Insoweit genügt es noch nicht, dass die Stiftung für Hochschulzulassung die Auswahlentscheidungen bspw. stichprobenhaft untersucht oder bereits die Bewerbungsunterlagen Einzelner an menschliche Entscheider vorab aussteuert. Der Hoheitsträger muss vielmehr sicherstellen, dass das lernfähige System bei seiner Auswahlentscheidung nur rechtsstaatlich zulässige Kriterien anlegt, insbesondere weder direkt noch indirekt[36] diskriminiert. Dazu gehört jedenfalls, das System als Ganzes in regelmäßigen Rhythmen mit künstlich generierten Datensets zu testen. Nur durch solche Sicherungsmaßnahmen stellt der Gesetzgeber die staatliche Kontrolle sicher, die einen rechtmäßigen Vollzug seiner politischen Vorgaben verbürgt. Solange lernfähige Verfahren Diskriminierungen oder sonstige Abweichungen vom gesetzlich definierten Normprogramm nicht wirksam ausschließen können, dürfen allein Systeme zum Einsatz kommen, die ihre Entscheidungen nach einem festen linearen Schema treffen.

4.7 Transparenzpflichten

Staatliche Auswahlentscheidungen, die über Lebenspläne entscheiden, müssen rechtsstaatlich vollständig nachvollziehbar sein. Das erheischen nicht nur der Steuerungsvorbehalt der demokratischen Ordnung, sondern auch die Grundrechte und ihre Wehrfähigkeit (Art. 19 Abs. 4 GG).

Setzt der Gesetzgeber einen Algorithmus ein, um Studienplätze zu verteilen, darf er dessen Funktionsweise daher grundsätzlich nicht vor den Betroffenen geheim halten: Es ist ihm versagt, sich zu einem selbstherrlichen Türsteher aufzuschwingen, der die einen Bewerber annimmt und die anderen ablehnt, ohne ihnen zu offenbaren, welche Beweggründe zu seiner Entscheidung geführt haben. Eine Blackbox, deren Programmierer nicht mehr nachvollziehen können, nach welchen Maßstäben das Programm die Schulabgänger mithilfe Künstlicher Intelligenz bewertet und zuteilt, genügt diesen Maßstäben nicht (vgl. Martini 2019a: 70 f. und 227 f.).

Wo das gleißende Licht der Transparenz hinfällt, ist aber auch Schatten: Offene Systeme laden dazu ein, die Logik eines Systems gegen sich selbst zu richten, indem der Einzelne seine Angaben an die erwünschten Entscheidungskriterien des Systems anpasst. So verhalf bspw. die strategisch richtige Ortswahl Bewerbern um Medizinstudienplätze mitunter schneller zum Ziel als die Abiturnote und sonstige Qualifikationen (Brehm und Brehm-Kaiser 2018: 6 f.). Rechtsstaatliche Verfahren stellt das unausweichlich vor ein Dilemma: Einerseits soll der Einzelne nachvollziehen können, wie es zu einer Entscheidung kommt, die seine Lebensentfaltung nachhaltig steuert. Andererseits soll er die Logik des Systems nicht umgehen und sein Verhalten strategisch daran ausrichten dürfen. Auch die Transparenz des Datenschutz- und Informationsfreiheitsrechts gilt daher nicht grenzenlos.

Das Datenschutz- (Abschnitt 4.7.1) und das Informationsfreiheitsrecht (Abschnitt 4.7.2) lösen den Konflikt auf, indem sie den Staat – auch bei deterministischen Entscheidungsmustern – im Grundsatz dazu verpflichten, einen Einblick in die verwendeten Systeme zu gewähren.

---

[36] Indirekte Diskriminierung meint scheinbar neutrale Regelungen, die sich aber de facto auf eine bestimmte Personengruppe nachteilhaft auswirken.

4.7.1 Datenschutzrecht (Art. 13 Abs. 2 lit. f DS-GVO)

Die DS-GVO verlangt dem Verantwortlichen ab, Betroffenen zumindest die involvierte Logik einer vollautomatisierten Entscheidung im Sinne des Art. 22 Abs. 1 DS-GVO preiszugeben (Art. 13 Abs. 2 lit. f DS-GVO).[37] Er muss in allgemein verständlicher Sprache die Berechnungsgrundlagen und deren Methodik (nicht aber notwendigerweise den Algorithmus selbst) zugänglich machen (Eßer 2018: Rn. 40). Diese Verpflichtung besteht de lege lata aber nur, soweit das Auswahlsystem eine *vollständig automatisierte* Entscheidung trifft, in die kein menschlicher Amtsträger in nennenswerter Weise hineinwirkt.[38]

4.7.2 Informationsfreiheitsrecht

Der Staat ist nicht nur verpflichtet, *die Logik des Entscheidungsverfahrens* offenzulegen. Als amtliche Information unterliegt *der Programmcode* grundsätzlich auch den Informationsfreiheitsgesetzen des Bundes und der Länder (IFG). Der gesetzliche Anspruch erstreckt sich aber nur auf Informationen, die den Behörden tatsächlich vorliegen und keine Geschäftsgeheimnisse Dritter verletzen (§ 6 S. 2 IFG). Setzt der Staat Softwareanwendungen privater Unternehmen ein, kommt diesen daher de lege lata bundesrechtlich ein absolutes Vetorecht zu: Sie dürfen im Grundsatz frei darüber entscheiden, ob sie den Code freigeben wollen (Guckelberger 2018: Rn. 11; siehe aber zu grundrechtlich induzierten Ausnahmen und Regelungsvorschlägen de lege ferenda Martini 2019a: 69 ff. sowie 342 f.).

Da sich Informationsansprüche jeweils gegen die Hochschulen, d. h. typischerweise Landesbehörden, richten, ist freilich regelmäßig nicht das IFG des Bundes einschlägig, sondern die Informationsfreiheitsgesetze der Länder. Einige von ihnen sind weniger strikt als das Recht des Bundes. So gewährt der Freistaat Thüringen jedermann gegenüber öffentlichen Stellen des Landes einen Auskunftsanspruch, soweit das Informationsinteresse im Einzelfall den Schutz privater Betriebs- und Geschäftsgeheimnisse überwiegt (vgl. z. B. § 9 Abs. 1 Nr. 5 ThürIFG[39]; dazu auch Martini 2019a: 342). Der Antragsteller kann dann im Ergebnis unter Umständen auch eine Information über den konkreten Entscheidungsalgorithmus der Hochschulzulassungssoftware eines privaten Softwaredienstleisters verlangen.

4.8 Fazit

Studienplätze auf der Grundlage algorithmischer Systeme zu verteilen, ist im Grundsatz rechtlich zulässig („Ob“). Ein automatisiertes Verfahren muss aber so gestaltet sein, dass es den grundrechtlichen Teilhabeanspruch der Studienbewerber auf Zugang zu den verfügbaren staatlichen Studienplätzen hinreichend achtet („Wie“).

Das System darf einzelne Bewerber insbesondere nicht ungerechtfertigt gegenüber Mitbewerbern benachteiligen – etwa durch Vergabekriterien, die an den Wohnort oder das Geschlecht anknüpfen. Welche Kriterien für die Auswahl handlungsleitend sind, obliegt grundsätzlich allein dem Gesetzgeber – nicht den Hochschulen. Ihnen kommt kein „Kriterienerfindungsrecht“ zu – erst recht nicht den privaten IT-Unternehmen, die den Verteilungsalgorithmus entwickeln. Das ist Ausfluss des verfassungsrechtlichen Wesentlichkeitsvorbehalts: Als Gravitationszentrum der politischen Willensbildung hat das Parlament alle wesentlichen Entscheidungen selbst zu treffen.[40] Der Einsatz lernfähiger Systeme, die nicht nur für Betroffene, sondern auch für ihre Kontrolleure und Entwickler unerkannte

---

[37] Diese Pflicht besteht hingegen nicht, wenn die automatisierte Bewertung nur einem Menschen assistiert, der die Entscheidung über den Erfolg einer Bewerbung trifft. In einem solchen Fall liegt keine ausschließlich automatisierte Entscheidung im Sinne des Art. 22 Abs. 1 DS-GVO mehr vor. An eine solche knüpft die Informationspflicht des Art. 13 Abs. 2 lit. f DS-GVO aber an; Martini 2017a: 1020 mit Fn. 38.

[38] Martini 2018: Rn. 16 ff. zum Begriff der „ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung“ in Art. 22 Abs. 1 DS-GVO.

[39] Thüringer Informationsfreiheitsgesetz vom 14.12.2012. Ab dem 1.1.2020 findet sich die wortgleiche Regelung in § 13 Abs. 1 S. 1 Nr. 5 Thüringer Transparenzgesetz.

[40] Vgl. BVerfGE 147, 253 (310 f.) – Numerus clausus III.

(ggf. nur mittelbare) Kriterien, wie Geschlecht oder Herkunft, zur Berechnungsgrundlage erheben (könnten), verbietet sich daher im Grundsatz: Solange und soweit sie nicht wirksam sicherstellen, dass keine anderen als die normativen Leitvorgaben, insbesondere keine unzulässigen mittelbaren Diskriminierungskriterien Eingang in die Entscheidung finden, dürfen nur rein regelbasierte Systeme (sog. *deterministische Algorithmen*) Anwendung finden.[41] Rechtskonform eingesetzt können algorithmenbasierte Verteilungsprogramme jedoch der Schlüssel zu einem effizienten und gerechten Vergabesystem sein. Sie überwachen dann nicht allein die Hochschulpforte, sondern sichern zugleich den chancengleichen Hochschulzugang der Bewerber ab.

[41] Der Einsatz lernfähiger Systeme zur Studienplatzverteilung ist damit nicht per se unzulässig, sondern nur an hohe Anforderungen geknüpft.

5 Studienerfolg auf Kosten informationeller Selbstbestimmung?

Rechtliche Grenzen algorithmenbasierter Studienberatungsprogramme

Prof. Dr. Mario Martini und Dr. Jonas Botta

5.1 Massenphänomen Studienabbruch

Der zweitreichste Mensch der Welt, der saarländische Ministerpräsident und einer der bekanntesten Fernsehmoderatoren Deutschlands haben eines gemeinsam: *Bill Gates*, *Tobias Hans* und *Jan Böhmermann* haben allesamt ihr Studium abgebrochen. Ihre Entscheidung, die Studienzeit frühzeitig ohne Abschluss zu beenden, ist alles andere als eine Seltenheit: Fast jeder dritte Anfänger eines Bachelorstudiengangs bricht in Deutschland sein Studium ab.[42] In den Naturwissenschaften liegt die Abbrecherquote sogar spürbar höher: bei beinahe 40 Prozent. Die Beweggründe dafür, der Hochschule den Rücken zuzukehren, sind mannigfaltig. Wissenschaftliche Untersuchungen identifizieren vornehmlich Leistungsprobleme und mangelnde Selbstdisziplin der Studierenden als Ursachen: Nur 48 Prozent der Studienabbrecher gelingt es, ihr Studium selbstständig zu organisieren; bei denjenigen, die das Studium abschließen, schaffen das immerhin 81 Prozent (Heublein et al. 2017). Die Fähigkeit, die eigene universitäre Ausbildung selbstbestimmt zu gestalten, entpuppt sich damit als ein Schlüsselindikator für den Studienerfolg (ibid.).

Der Einzelne bleibt mit seinen individuellen Sorgen und Problemen an der (für die deutsche Hochschullandschaft typischen) „Massenuniversität“ aber oftmals auf der Strecke, statt auf dem Weg zum erhofften Abschluss sein Leistungspotenzial optimal zu entfalten. Sind es nicht nur die fachlichen Herausforderungen, denen sich Studierende ausgesetzt sehen, sondern auch und gerade die psychischen Belastungen, denen viele nicht standhalten, ist der Unterstützungsbedarf mit Händen zu greifen: Allein im Jahr 2017 suchten 108.000 Studierende die psychologische Studienberatung auf (Deutsches Studentenwerk 2019: 11). So verstehen es die hochschuleigenen Studienberatungen aus gutem Grund als ihre Kernaufgabe, einem Studienabbruch eines Studierenden durch gute Betreuungsangebote entgegenzuwirken. Studienberater wünschen sich, dass mehr Studierende von den bestehenden Beratungsmöglichkeiten erfahren.[43] Im Verhältnis zum Bedarf der Studierenden schätzen sie ihre derzeitige Ausstattung jedoch oft als prekär an.

5.2 Predictive-Analytics-Programme – Garanten für den individuellen Studienerfolg?

Klaffen Nachfrage und Ausstattung der Studienberatung auseinander, ohne dass Aussicht auf eine kurzfristige drastische Erhöhung der finanziellen Mittel besteht, liegt nichts näher, als die Effizienzressourcen algorithmischer Analysewerkzeuge anzuzapfen. Was die herkömmliche Studienberatung bislang nicht bietet und selbst mit mehr personellen wie finanziellen Ressourcen kaum vollständig gewährleisten könnte – individuell auf jeden Studierenden einzugehen –, das könnten in den Augen von Optimisten künftig algorithmenbasierte Beratungsprogramme leisten. Noch sind es vor allem die USA und Neuseeland, die solche Softwarelösungen erproben. Sie könnten die fachliche Studienberatung jedoch auch in Deutschland umwälzen.[44]

---

[42] Das hat eine Studie des *Deutschen Zentrums für Hochschul- und Wissenschaftsforschung* (DZHW) im Jahr 2017 aufgezeigt; Heublein et al. 2017: XV.

[43] Bislang nehmen Studienabbrecher die Beratungsangebote indes nicht merklich häufiger als die Gruppe der Hochschulabsolventen in Anspruch; Heublein et al. 2017: 181 ff. Die Hilfe erreicht damit nicht im ausreichenden Maße diejenigen, welche sie am stärksten benötigen.

[44] Neue Potenziale für die Studienberatung birgt auch der Einsatz von Chatbots wie an der *Erasmus Universität Rotterdam*. Dort berät ein Bot die Studierenden zu Studiengebühren. Weiterführend de Ruiter 2019: 16.

Am stärksten hat sich bislang das Beratungsprogramm der *Arizona State University*, der größten staatlichen Hochschule der USA, einen Namen gemacht: *eAdvisor* steht Studienanfängern zunächst bei der Wahl ihres Hauptfaches zur Seite und begleitet sie fortan durch ihr gesamtes Studium (Dräger 2016). Dafür weist die Software dem Nutzer aus, welche Kurse er zukünftig belegen sollte, um sein Studium nicht nur in der Regelstudienzeit, sondern auch mit größtmöglichem Erfolg abschließen zu können. Sie stützt sich dabei auf seinen bisherigen individuellen Studienverlauf und die Erfahrungen ehemaliger Teilnehmer.

Die Analyseverfahren, die auf der Grundlage vorhandener Datensammlungen zukünftige Ereignisse voraussagen sollen (sog. *Predictive Analytics*), nehmen den Studierenden nicht nur frühzeitig an die Hand. Sie verweisen ihn auch an den menschlichen Studienberater weiter, wenn er die Pflichtkurse nicht zeitgerecht absolviert oder bestanden hat (Phillips 2014). Das Programm beschränkt sich dabei nicht auf eine unverbindliche Gesprächsempfehlung: Ignoriert der Studierende die Analysevorschläge, bleibt er vorerst davon ausgeschlossen, weitere Kurse wählen zu können.

Predictive Analytics gleichen dem magischen Blick in die Kristallkugel. Doch statt Jahrmarktsfolklore verheißen die Algorithmen harte Fakten: Derzeit eingesetzte Beratungsprogramme nehmen für sich in Anspruch, den späteren Studienerfolg mit einer Wahrscheinlichkeit von bis zu 90 Prozent zu prognostizieren (Dräger und Müller-Eiselt 2015). Dafür greifen sie nicht nur auf die umfangreichen Vergleichsdaten früherer Kursabsolventen zu. Sie ziehen auch sensible Datenquellen zu Rate – etwa Einträge bei der Campus-Polizei, beim Studierendenwohnheim oder Informationen über die finanzielle Situation des Studierenden (Dräger 2016). Während ein Leistungsstipendium in dem Kaleidoskop der Gewichtungsfaktoren bspw. kontinuierlichen Studienerfolg indiziert, erschwert ein nicht studienbezogener Nebenjob ihn tendenziell. Teilweise tracken die Beratungsprogramme die Studierenden, wenn sie sich im WLAN ihrer Hochschule einloggen. Auf diese Weise gelingt es ihnen, die realen Präsenzzeiten einzubeziehen, wenn sie eine Prognose für den weiteren Studienerfolg errechnen (Fron 2018). Die *Arizona State University* wertet zudem (wenn auch bislang nur zu Forschungszwecken) die Nutzungsdaten des multifunktionalen Studierendenausweises aus, mit dessen Hilfe Studiosi Hochschulgebäude betreten, Mittagessen kaufen oder Bücher ausleihen können. Auf diese Weise soll die Catcard dazu beitragen, potenzielle Studienabbrecher bereits in den unteren Semestern zu identifizieren.

In Deutschland hat das *Karlsruher Institut für Technologie* ein Studienberatungsprogramm entwickelt, das den US-amerikanischen Anwendungen ähnelt (Weiß 2018). Für den Einsatz solcher Programme kommt das Phänomen der Massenuniversität einem Glücksfall gleich. Denn auf je mehr Daten die Beratungsprogramme potenziell zugreifen können, desto exakter kann die Prognose sein.[45]

Die algorithmengestützte Kursempfehlung mag durch präzise Erfolgsvorhersage die Wahrscheinlichkeit senken, dass jemand sein Studium aufgrund unzureichender Leistungen abbricht oder in die Länge zieht. Wenn aber die individuelle und kollektive Vergangenheit die universitäre Zukunft des Einzelnen determiniert, strahlt das auch auf die Lebensentfaltung und die Freiheit der Selbstfindung aus: Das Beratungsprogramm kann die Studierenden und ihr Schicksal zum Objekt einer panoptischen Dauerbeobachtung machen.[46] Die Analysesoftware setzt sie unter die gläserne Glocke eines Überwachungsinstruments, das jeden Fehltritt erfasst. Damit erhebt die Software (jedenfalls mittelbar) Assimilierung statt autonomer akademischer Selbstentfaltung zum Leitbild des universitären Bildungsauftrags.[47] Wer wird sich noch auf die Umwege einer wissenschaftlichen Entdeckungsreise einlassen, wenn ihm

---

[45] Ein reiches Datenreservoir hält auch die vor wenigen Jahren reformierte Studienverlaufsstatistik vor. Das Statistische Bundesamt und die statistischen Ämter der Länder sind kraft Gesetzes verpflichtet, sie zu erstellen (vgl. § 7 Hochschulstatistikgesetz). Ihre empirische Analyse soll dazu beitragen, Studienabbrüchen vorzubeugen. Den Studienabbruch selbst erfasst die Statistik jedoch nicht.

[46] Nicht nur der Hochschule offenbaren sich die Studierenden als Zielobjekte eines solchen Systems in einer sensiblen Weise. Sie setzen sich auch dem Risiko aus, dass Dritte (unberechtigterweise) auf diese Informationen zugreifen und damit ihre informationelle Selbstbestimmung verletzen.

[47] Die Lernfreiheit der Studierenden findet in Art. 5 Abs. 3 GG keine grundrechtliche Stütze. Er garantiert vielmehr die Lehrfreiheit der Hochschullehrer (Scholz 2019: 113 f.). Verfassungsrechtlichen Schutz erfahren Studierende

das Programm eine sichere Passage durch das Studium weist? Irrungen und Wirrungen eines von Neugier getriebenen Studiums gehören zum Humboldt'schen Bildungsideal. Es strebt nach einer „Mannigfaltigkeit der Situationen". Denn „[a]uch der freieste und unabhängigste Mensch, in einförmige Lagen versetzt, bildet sich minder aus."[48] Ein Verlust an akademischer Experimentierfreude durch stromlinienförmige Vorgaben eines Algorithmus schwört diesem Ideal ab.

Noch gravierender wären die Folgen, wenn das Programm nicht nur „beraten", sondern sogar entscheiden dürfte. Die Dystopie „Computer says no", die in der britischen Sketch-Show „Little Britain" den geneigten Zuschauer zum Schmunzeln bringt, hielte dann als libertärer Albtraum Einzug in die Seminarräume. Die gut gemeinte digitale Beratungsumgebung läuft dann Gefahr, zu einer Abrissbirne wissenschaftlicher Entfaltungsfreiheit zu mutieren, die das selbstbestimmte Streben nach neuem Wissen und Erkenntnis zermalmt.

5.3 Rechtliche Bewertung algorithmenbasierter Studienberatungsprogramme

Wollen deutsche Hochschulen nach dem Vorbild US-amerikanischer Predictive-Analytics-Programme die Anwendung *eAdvisor* einsetzen, um ihre Studienberatung zu optimieren, muss sich dieses Unterfangen rechtlich vornehmlich an den Vorgaben des Landeshochschulrechts (Abschnitt 5.3.1) und des Datenschutzrechts (Abschnitt 5.3.2) messen lassen.

5.3.1 Landeshochschulrecht

Das Hochschulrecht fällt in Deutschland grundsätzlich in die Hoheit der Länder. Der Bund gibt zwar die wesentlichen Grundzüge vor:[49] Das Hochschulrahmengesetz (HRG) verankert die Studienberatung als verpflichtende Aufgabe aller staatlichen bzw. staatlich anerkannten Hochschulen (§ 14 HRG). Bei ihrer Ausgestaltung breiten die unterschiedlichen Landesregelungen jedoch einen wahren Flickenteppich aus. Damit nicht genug: Den über 400 deutschen Hochschulen kommt als Teil ihrer Hochschulautonomie grundsätzlich auch das Recht zu, eigene Satzungen zu erlassen, mit deren Hilfe sie die Vorgaben für die Studienberatung noch weiter ausdifferenzieren können.

5.3.1.1 Allgemeine Studienberatung und Studienfachberatung

Die Hochschulgesetze der Länder unterscheiden regelmäßig zwischen der „allgemeinen Studienberatung" und der „Studienfachberatung".[50] Die *allgemeine* Studienberatung hat die Aufgabe, Studienbewerber und Studierende zu grundlegenden Fragen des Studiums – insbesondere pädagogisch und psychologisch – sowie zur Studienfinanzierung zu beraten. Demgegenüber zielt die *Studienfachberatung* darauf ab, die Studierenden bei ihrem *individuellen Studienverlauf* zu unterstützen. Studienfachberatung kann die Hochschule auch verbindlich anordnen[51] und den einzelnen Studierenden im Extremfall sogar exmatrikulieren, wenn er den Beratungstermin nicht wahrnimmt.[52]

---

vielmehr vorrangig aus der Berufsfreiheit (Art. 12 Abs. 1 GG): Sie kann bspw. verletzt sein, wenn das Beratungsprogramm den Studierenden von der weiteren Kursbelegung sperrt.

[48] Zitiert nach von Humboldt 1851: 10.

[49] Weiterführend Martini und Botta: Der Algorithmus als universitärer Pfortenwächter (Kapitel 4 dieser Studie).

[50] Vgl. § 2 Abs. 2 BW LHG; Art. 60 BayHSchG; § 28 BerlHG; § 20 BbgHG; § 51 BremHG; § 51 HmbHG; § 14 HHG HE; § 34 LHG M-V; § 58 Abs. 5 und 7 NRW HG; § 24 RLPHG; § 62 SHSG; § 5 Abs. 2 Nr. 6 und 7 Sächs-HSFG; § 11 HSG LSA; § 48 HSG SH.

[51] § 28 Abs. 3 BerlHG; § 20 Abs. 3 BbgHG; § 51 Abs. 2 HmbHG; § 34 S. 4 Hs. 2 LHG M-V.

[52] § 15 Abs. 2 Nr. 1 lit. a BerlHG; § 14 Abs. 5 Nr. 2 BbgHG; § 42 Abs. 2 Nr. 7 HmbHG.

5.3.1.2 Zuständigkeit für die Studien(fach)beratung

Wer für die Beratung der Studierenden zuständig ist, regeln die Landesgesetzgeber unterschiedlich. In manchen Ländern gehört die Studienberatung generell zu den Dienstaufgaben der *Hochschullehrer*;[53] teilweise sind sie nur für die Studienfachberatung zuständig.[54] Einige Landeshochschulgesetze verpflichten ergänzend ausdrücklich auch die *wissenschaftlichen Mitarbeiter* dazu, an der Studien(fach)beratung mitzuwirken.[55]

Ob neben dem akademischen Personal auch ein *Computerprogramm* die Studierenden beraten dürfte, hängt davon ab, inwieweit die jeweiligen Zuständigkeitsregelungen abschließend konzipiert sind. Solange die Landeshochschulgesetze nur eine Dienstaufgabe der Hochschullehrer (sowie des sonstigen wissenschaftlichen Personals) formulieren, folgt daraus nicht im Umkehrschluss, dass auch nur diese die Studienberatung durchführen dürfen. Anders verhält es sich hingegen, wenn der Landesgesetzgeber enumerativ geregelt hat, wer für die Beratung zuständig ist. Diesen Weg haben lediglich Berlin und Brandenburg eingeschlagen: In beiden Ländern geben die Hochschulgesetze vor, dass Hochschullehrer (in Berlin unterstützt durch mindestens eine studentische Hilfskraft) – und niemand sonst – die Studienfachberatung vornehmen.[56]

Überall dort, wo eine abschließende Zuständigkeitsregelung fehlt, könnten die Hochschulen im Grundsatz auch digitale Anwendungen wie *eAdvisor* in der Studienberatung einsetzen. Hierfür müssten sie gegebenenfalls lediglich ihre Satzungen anpassen (falls diese abschließend bestimmen sollten, wer die Studienberatung bislang durchzuführen hat).

5.3.2 Datenschutzrecht

Seit dem 25.5.2018 formt die Datenschutz-Grundverordnung (DS-GVO) in der Europäischen Union und ihren Mitgliedstaaten grundsätzlich einheitlich und unmittelbar aus, wer in welchem Umfang Daten der Studierenden verarbeiten darf. Sie setzt auch dem Einsatz eines Computerprogramms für eine (voll-)automatisierte Studienberatung nach US-amerikanischem Vorbild an deutschen Hochschulen datenschutzrechtliche Grenzen.

5.3.2.1 Verarbeitungsgrundlage

Programme wie *eAdvisor* sind i. d. R. auf Daten angewiesen, die sich auf eine identifizierte oder identifizierbare Person beziehen, um eine für den einzelnen Studierenden personalisierte Studienverlaufsprognose erstellen zu können.[57] Solche sog. *personenbezogenen Daten* (Art. 4 Nr. 1 DS-GVO) aktivieren den Verarbeitungsvorbehalt der DS-GVO: Die Hochschulen dürfen diese Daten nur verarbeiten, wenn entweder der Gesetzgeber das ausdrücklich zugelassen oder der Betroffene eingewilligt hat. Dieses grundsätzliche *Verbot mit Erlaubnisvorbehalt,* von dem die DS-GVO durchdrungen ist, strukturiert bereits das unionale Datenschutzgrundrecht (Art. 8 Abs. 2 S. 1

---

[53] § 46 Abs. 1 Nr. 2 BW LHG; § 35 Abs. 1 S. 1 NRW HG; § 24 Abs. 1 S. 2 NHG; § 48 Abs. 1 S. 2 RLPHG; § 39 Abs. 1 S. 2 SHSG; § 60 Abs. 1 S. 3 aE HSG SH; § 83 Abs. 2 Nr. 5 ThürHG.
[54] § 99 Abs. 4 Nr. 3 BerlHG; § 20 Abs. 3 S. 2 BbgHG; § 51 Abs. 2 S. 3 BremHG; § 12 Abs. 4 Nr. 2 HmbHG; § 61 Abs. 1 S. 2 Nr. 6 HHG HE; § 57 Abs. 3 Nr. 2 LHG M-V; § 67 Abs. 3 Nr. 4 SächsHSFG; § 34 Abs. 2 S. 1 Nr. 7 HSG LSA.
[55] § 27 Abs. 1 S. 4 HmbHG; § 44 Abs. 1 S. 3 NRW HG; § 68 Abs. 1 S. 2 HSG SH.
[56] § 28 Abs. 2 BerlHG; § 20 Abs. 3 S. 2 BbgHG.
[57] Sind die Daten anonymisiert, ist die DS-GVO nicht anwendbar. Ehemals personenbezogene Daten sind erfolgreich *anonymisiert*, wenn sie dauerhaft keiner natürlichen Person mehr zuordenbar sind. Das kann bspw. durch eine Datensynthese gelingen, indem das Beratungsprogramm aus den vorhandenen Daten ein Modell ableitet, auf dessen Grundlage es statistisch identische, aber nicht mehr personenbezogene Daten künstlich erzeugt und diese fortan ausschließlich verwendet, um die Studienprognosen zu erstellen; vgl. Steinebach et al. 2016: 443. *Pseudonymisierte* Daten fallen demgegenüber in den Anwendungsbereich der DS-GVO. Pseudonymisiert sind die Studierendendaten, wenn das Programm bspw. ihren Namen durch einen Code ersetzt hat und die Daten somit nur mithilfe eines Schlüssels der konkreten Person zuordenbar sind (Art. 4 Nr. 5 DS-GVO).

GRCh[58]) primärrechtlich vor („mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage"). Die denkbaren Erlaubnistatbestände konkretisiert und bündelt Art. 6 Abs. 1 UAbs. 1 DS-GVO sekundärrechtlich.

- **Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO)**
  In der Logik der DS-DVO ist die Einwilligung der vornehmste Ausdruck informationeller Selbstbestimmung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO). Damit sie als wirksam erklärt gilt, muss der Studierende sie freiwillig und informiert für einen bestimmten Verarbeitungszweck erteilen.[59]

  Der Hochschule ist daher aufgegeben, den Verarbeitungszweck so genau wie möglich zu bestimmen. Als datenschutzrechtlich Verantwortliche trifft sie die Pflicht, ihre Studierenden bestmöglich darüber zu informieren, welche Daten (Name, Alter, Hochschulnoten etc.) sie konkret verarbeitet. Der Studierende muss seine Einwilligung *bewusst* erklären (Art. 4 Nr. 11 DS-GVO). Im Regelfall heißt das, dass er während der Registrierung für das Beratungsprogramm aktiv ein Kästchen anklickt, um der Datenverarbeitung zuzustimmen (vgl. ErwGrd 32 S. 2 DS-GVO). Ein *Opt-out* genügt hingegen nicht – erst recht nicht der Umstand allein, dass ein Studierender das Programm tatsächlich nutzt (vgl. Ernst 2017: 114).

  Die Studierenden und ihre Hochschule stehen einander nicht in einem Gleichordnungsverhältnis gegenüber. Die Machtasymmetrie, die ihre Beziehung prägt, kann auf die Freiwilligkeit der Erklärung durchschlagen (ErwGrd 43 S. 1 DS-GVO; siehe hierzu bspw. auch Martini und Wenzel 2017: 753). Das gilt etwa dann, wenn die Hochschule faktischen Druck auf die Studierenden ausübt, bspw. ihren Studierenden die Kursteilnahme verweigert, solange diese nicht in die Datenverarbeitung zum Zweck der Studienberatung eingewilligt haben.[60] Einwilligungserklärungen gegenüber Behörden stuft die DS-GVO daher als (im Zweifel) nicht freiwillig und damit in der Folge unwirksam ein.

  Das heißt aber nicht, dass Studierende gegenüber ihrer Hochschule generell nicht wirksam einwilligen könnten. Dem Verdikt drohender Unwirksamkeit einer Einwilligungserklärung kann die Hochschule vorbeugen, indem sie das Beratungsprogramm rein fakultativ ausgestaltet (also an eine ablehnende Haltung der Studierenden keine negativen Konsequenzen knüpft). Haben sie eine echte Wahlfreiheit (ErwGrd 42 S. 5 DS-GVO), ist ihre Einwilligungserklärung im Zweifel freiwillig.

  Doch auch eine wirksam erteilte Einwilligung erweist sie sich nicht immer als verlässliche und praktikable Verarbeitungsgrundlage. Denn die Studierenden können sie *jederzeit widerrufen* (Art. 7 Abs. 3 S. 1 DS-GVO). Das Beratungsprogramm entfaltet als Hochschulinfrastrukturressource aber nur dann seine volle Effizienz, wenn es *alle* Studierenden erfasst. Mehr Planungssicherheit bieten den verarbeitenden Hochschulen insoweit gesetzliche Erlaubnistatbestände.

- **Gesetzliche Erlaubnistatbestände**
  Die DS-GVO gestattet den Hochschulen, personenbezogene Daten kraft Gesetzes zu verarbeiten, soweit dies erforderlich ist, um ihre öffentliche Aufgabe zu erfüllen (Art. 6 Abs. 1 UAbs. 1 lit. e,[61] Abs. 3

[58] Die Abkürzung steht für „Charta der Grundrechte der Europäischen Union".
[59] Ein Einwilligungsbeispiel findet sich beim Studienberatungsprogramm „PASST?!" der TU Dresden: https://tu-dresden.de/studium/im-studium/ressourcen/dateien/zentrale-studienberatung/passt/Einwilligungserklaerung_PASST.pdf?lang=de (Download 11.11.2019).
[60] Vgl. zu den Anforderungen an eine freiwillige Einwilligung im Hochschulkontext auch bspw. Martini und Botta 2019: 248 ff.
[61] Dieser Erlaubnistatbestand greift nicht aus sich selbst heraus. Die Union oder der Mitgliedstaat müssen dessen Voraussetzungen vielmehr in einer Norm konkretisiert haben (Art. 6 Abs. 3 S. 1 DS-GVO).

DS-GVO).[62] Die Landeshochschulgesetze füllen die unionsrechtliche Öffnungsklausel durch zahlreiche Verarbeitungsgrundlagen aus. Teilweise gestatten sie den Hochschulen explizit, Daten zum Zwecke der Studienberatung zu verarbeiten.[63] Fehlt es an spezifischen Vorschriften, können sich die notwendigen Rechtsgrundlagen aber auch aus den Generalklauseln der Landesdatenschutzgesetze ergeben, die zur Datenverarbeitung für öffentliche Aufgaben[64] ermächtigen.[65]

Einer universitären Datenverarbeitung, die sich auf Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO stützt, sind die Studierenden nicht vorbehaltlos ausgesetzt. Sie können der Verarbeitung grundsätzlich vielmehr nachträglich widersprechen (Art. 21 Abs. 1 S. 1 DS-GVO). Sie müssen dafür aber Gründe anführen können, die sich aus einer „besonderen Situation" ergeben. Ein Studierender könnte bspw. nach einem Cyberangriff auf die hochschuleigenen IT-Systeme erhebliche Datensicherheitsbedenken geltend machen. Bestehen solche besonderen Gründe tatsächlich, ist der Hochschule die weitere Verarbeitung grundsätzlich versagt. Etwas anderes gilt nur dann, wenn sie nachweisen kann, dass sie ihre Verarbeitung auf „zwingende schutzwürdige Gründe" stützen kann, welche die schutzwürdigen Belange des Studierenden überwiegen (Art. 21 Abs. 1 S. 2 DS-GVO).

5.3.2.2 Besondere personenbezogene Daten (Art. 9 DS-GVO)

Einige personenbezogene Daten, die nachhaltig auf die Persönlichkeitsentfaltung ausstrahlen können, stuft der Unionsgesetzgeber als besonders sensibel ein. Das gilt insbesondere für solche Informationen, aus denen die ethnische Herkunft oder die politische Meinung der Betroffenen hervorgehen oder die Aussagen über den Gesundheitszustand des Einzelnen treffen (Art. 9 Abs. 1 DS-GVO).

- **Anwendungsbereich des Art. 9 Abs. 1 DS-GVO**
  Besonders sensible Daten verarbeitet eine Beratungssoftware bspw. dann, wenn sie erfasst, wann und wie oft sich ein Studierender für Klausuren krankgemeldet hat. Gleiches gilt, wenn das Programm aus dem Namen sowie der Adresse des Studierenden Rückschlüsse auf seine Herkunft oder seinen Glauben zieht und auf dieser Grundlage Kurswahlempfehlungen trifft, die Kollisionen mit religiösen Festen des Studierenden vermeiden sollen. Name und Adresse eines Studierenden sind zwar isoliert betrachtet noch kein besonders sensibles Datum. Sie können aber im Verbund mit anderen Daten zu einem besonderen personenbezogenen Datum mutieren (sog. *doppelfunktionale Daten*). Dafür genügt nicht jeder entfernte Bezug zu einem besonders schutzbedürftigen Merkmal. Sonst verkehrte sich der Ausnahmetatbestand des Art. 9 DS-GVO zum Generalvorbehalt der Datenverarbeitung. Vielmehr ist für die Abgrenzung zwischen normalen und besonderen Daten auf den *objektivierten Verarbeitungskontext* abzustellen: Es ist aus Sicht eines objektiven Dritten zu ermitteln, ob das Beratungsprogramm ein Datum verarbeitet, das besonders schützenswerte Informationen über den Einzelnen zum Gegenstand haben wird.[66] In Zweifelsfällen schlägt der bewusste gesetzgeberische Kategorieschutz durch und ist der Anwendungsbereich des Art. 9 DS-GVO mit seinen verschärften Verarbeitungskautelen eröffnet.

---

[62] Es reicht nicht, dass die Hochschule berechtigte Interessen an der Datenverarbeitung anführen kann. Der Erlaubnistatbestand „Wahrung berechtigter Interessen" (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO) erweist sich zwar aufgrund seines weiten Anwendungsbereichs regelmäßig als einschlägige Verarbeitungsgrundlage für *Unternehmen und sonstige Private*. *Öffentliche Stellen* können sich hierauf jedoch nicht berufen (Art. 6 Abs. 1 UAbs. 2 DS-GVO).
[63] § 11 Abs. 1 Nr. 8 Alt. 2 BremHG oder § 55 Abs. 4 S. 1 i. V. m. § 14 S. 1 HHG HE.
[64] Dass die Datenverarbeitung eine öffentliche Aufgabe repräsentiert, ergibt sich aus den Aufgabenbestimmungen der Landeshochschulgesetze.
[65] Bspw. § 2 Abs. 2 LHG BW i. V. m. § 4 LDSG BW.
[66] Dazu bereits Martini und Botta 2019: 259 f.

- **Ausnahmetatbestand des Art. 9 Abs. 2 DS-GVO**
  Art. 9 Abs. 1 DS-GVO spricht kein absolutes Verarbeitungsverbot aus. Unter den eingeschränkten Voraussetzungen des Art. 9 Abs. 2 DS-GVO gestattet die DS-GVO dem Verantwortlichen vielmehr ausnahmsweise, auch besondere personenbezogene Daten zu verarbeiten. Im Falle eines Studienberatungsprogramms kommt als denkbare *gesetzliche Verarbeitungsgrundlage* allein Art. 9 Abs. 2 lit. g DS-GVO in Betracht.
  Die Vorschrift setzt ein erhebliches öffentliches Interesse an der Datenverarbeitung sowie eine spezielle Erlaubnis im Unionsrecht oder im nationalen Recht voraus. Eine Datenverarbeitung zu Zwecken der Studienberatung befriedigt aber schon kein *erhebliches* öffentliches Interesse. Denn dieses knüpft an eine besondere Bedeutung für die Allgemeinheit an, wie sie bspw. bei der Gefahrenabwehr oder beim Katastrophenschutz besteht (Kühling et al. 2016: 53 f.).
  Wollen Hochschulen im Rahmen einer algorithmenbasierten Studienberatung besonders sensible Daten ihrer Studierenden in zulässiger Weise verarbeiten dürfen, verbleibt ihnen als Verarbeitungsgrundlage daher in der Regel nur eine Einwilligung. Dafür muss die betroffene Person ihr Einverständnis aber „ausdrücklich“ (also nicht bloß durch schlüssiges Verhalten) erteilen (Art. 9 Abs. 2 lit. a DS-GVO).[67]

5.3.2.3 Verarbeitungsgrundsätze, insbesondere Speicherbegrenzung und Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO)

Hat die Beratungssoftware die Daten der Studierenden einmal erfasst, muss die Hochschule sicherstellen, dass sie im weiteren Verarbeitungsprozess die Grundsätze der *Speicherbegrenzung* und *Datenminimierung* wahrt (Art. 5 Abs. 1 lit. c bzw. lit. e Hs. 1 DS-GVO). Die Programme dürfen insbesondere nur solche Daten der Studierenden speichern, die tatsächlich erforderlich sind, um eine Prognose über den weiteren Studienverlauf zu erstellen. Sie dürfen die Informationen grundsätzlich auch nicht dauerhaft personenbezogen speichern. Vergleichsdaten der Alumni bspw., die als Grundlage für eine Kursempfehlung des Beratungsprogramms fungieren, müssen anonymisiert sein. Denn um den Verarbeitungszweck zu erreichen, müssen die Daten nicht notwendig zu einer einzelnen Person rückverfolgbar sein.

Wer Daten zu einem spezifischen Zweck erhoben hat, darf sie später grundsätzlich nicht für beliebige andere Zwecke weiterverwenden (sog. *Zweckbindungsgrundsatz*, Art. 5 Abs. 1 lit. b Hs. 1 DS-GVO). Big-Data-Anwendungen wie *eAdvisor* basieren aber regelmäßig darauf, personenbezogene Daten – unabhängig vom ursprünglichen Erhebungszweck (bspw. der Bewerbung für einen Wohnheimplatz oder einer Studienförderung) – zu immer neuen „Informationskokons“ zu verweben, um daraus neue Korrelationen und Empfehlungen zu generieren.

Der Gesetzgeber schließt eine Zweckänderung zugleich nicht kategorisch aus. Er knüpft sie aber an hohe Voraussetzungen: Ist die neue Verarbeitung nicht mit dem ursprünglichen Erhebungszweck vereinbar, ist sie nur dann zulässig, wenn der Studierende einwilligt oder eine besondere Rechtsvorschrift im Sinne des Art. 6 Abs. 4 DS-GVO sie ausdrücklich zulässt.

Datenverarbeitungen zu wissenschaftlichen Forschungszwecken gesteht der Unionsgesetzgeber ein besonderes Privileg zu, das sie dem Klammergriff des Zweckbindungsgebots vergleichsweise leicht entrinnen lässt: Er vermutet im Grundsatz, dass der Sekundär- mit dem Primärzweck kompatibel ist (Art. 5 Abs. 1 lit. b Hs. 2 DS-GVO). Von diesem Vorzug profitiert die Studienberatung jedoch nicht. Denn sie dient nicht der Forschung, d. h. dem Streben nach neuen Erkenntnissen.[68] Sie ist vielmehr der akademischen Lehre zuzuordnen. Diese hat die DS-GVO bewusst nicht privilegiert. Das Verarbeitungsprivileg lässt sie lediglich wissenschaftlichen Ausarbeitungen *über die* Studienberatung zukommen, nicht aber Datenverarbeitungen *der* Studienberatung.

---

[67] Ein späterer Widerruf ist ihr unbenommen (Art. 7 Abs. 3 S. 1 DS-GVO).
[68] Vgl. BVerfGE 35, 79 (113).

Konkret heißt das: Beratungsprogramme an deutschen Hochschulen dürfen die Daten ihrer Studierenden nicht im selben Maße wie ihre US-amerikanischen Vorbilder aus verschiedensten Quellen für ihre Prognosen zusammenführen und nutzen. So wäre es bspw. unzulässig, ohne Zustimmung des Studierenden bzw. ohne eine spezielle gesetzliche Rechtsgrundlage auf die personenbezogenen Daten beim BAföG-Amt oder beim hochschuleigenen Studierendenwohnheim zuzugreifen.

Daten aus allgemein zugänglichen Quellen weiterzuverarbeiten, die bspw. ein Studierender in einem öffentlichen Facebook-Post preisgegeben hat, gestattet die DS-GVO demgegenüber: Hat der Betroffene Informationen offensichtlich selbst veröffentlicht, erkennt sie fortwirkenden Privatheitsinteressen kein besonderes Schutzniveau zu (vgl. Art. 9 Abs. 2 lit. e DS-GVO),[69] sondern geht in diesen Fällen von einer Zweckkompatibilität im Sinne des Art. 6 Abs. 4 DS-GVO aus.

5.3.2.4 Automatisierte Einzelfallentscheidung, insbesondere Profiling (Art. 22 DS-GVO)

Algorithmenbasierte Beratungsprogramme wie *eAdvisor* operieren mit Persönlichkeitsprofilen der Studierenden. Dem setzt der Unionsgesetzgeber bewusst Grenzen: Verantwortliche dürfen Betroffene keiner Entscheidung unterwerfen, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling[70] – beruht und die dem Betroffenen gegenüber eine rechtliche Wirkung entfaltet oder ihn zumindest in ähnlicher Weise erheblich beeinträchtigt (Art. 22 Abs. 1 DS-GVO). Erkennt ein Beratungsprogramm bspw. einen Studierenden als „off track" und blockiert ihn anschließend automatisch bei der weiteren Kurswahl, bis er ein Beratungsgespräch wahrgenommen hat, dann setzt Art. 22 Abs. 1 DS-GVO dem grundsätzlich ein Verarbeitungsverbot entgegen.

Dieses Verbot gilt indes nicht absolut. Wie so viele andere Normen der DS-GVO steht es unter Ausnahmevorbehalt: Eine ausdrückliche Einwilligung der Studierenden (Art. 22 Abs. 2 lit. c DS-GVO) oder eine mitgliedstaatliche Rechtsgrundlage kann der automatisierten Verarbeitung den Weg zur Zulässigkeit ebnen (Art. 22 Abs. 2 lit. b DS-GVO). Zwingend sind dann aber angemessene Schutzmaßnahmen, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren" (Art. 22 Abs. 3 DS-GVO). Der betroffene Studierende muss insbesondere verlangen können, seinen Standpunkt darzulegen, aus besonderen Gründen einen Menschen in die Entscheidung einwirken zu lassen[71] sowie eine Neubewertung der Computerentscheidung zu erzwingen. Ein Recht, Einblick in den Programmcode der Beratungssoftware zu nehmen, verbürgt ihm die DS-GVO hingegen nicht (Martini 2018: Rn. 36).

Wenn letztlich *ein Mensch* die finale Entscheidung über ein Beratungsgespräch oder eine andere Maßnahme auf Grundlage des Beratungsprogramms trifft, ist Art. 22 DS-GVO demgegenüber nicht einschlägig. Denn die Vorschrift erfasst nur *vollautomatisierte* Entscheidungsverfahren (a. a. O.: Rn. 16 ff.). Profiling als Analyseverfahren, das eine menschliche Entscheidung lediglich *unterstützt*, unterliegt nur den allgemeinen Vorschriften der DS-GVO (ErwGrd 72 S. 1 DS-GVO). Hochschulen können den Anforderungen des Art. 22 DS-GVO also dadurch entrinnen, dass sie die Analyseprogramme lediglich als Assistenzsysteme ausgestalten: Eine Software bereitet die Entscheidungen der menschlichen Studienberater dann inhaltlich vor, ohne sie jedoch selbst zu treffen.

Welchen Weg der Einbindung eines Beratungsprogramms die Hochschule auch wählt: Eine *Totalerfassung* der Studierenden gestattet die DS-GVO einem Beratungsprogramm keinesfalls. Eine panoptische Überwachung der Studierenden verbietet sich schon allein deswegen, weil sie in ihre Menschenwürde eingreift (Art. 1 GRCh). Solche

---

[69] Weiterführend zu allgemein zugänglichen Daten in sozialen Medien: Martini und Kolain: Soziale Netzwerke – Daten-Eldorado für personalisierte Angebote? (Kapitel 8 dieser Studie, insbes. Abschnitt 8.5.3).

[70] „Profiling" definiert Art. 4 Nr. 4 DS-GVO als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, […] bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten […].

[71] Dazu und zur einschränkenden Auslegung der Norm Martini und Nink 2017: 4.

Maßnahmen sind keiner Rechtfertigung zugänglich.[72] Studierende diesseits des Atlantiks sind deshalb (jedenfalls grundsätzlich) davor geschützt, dass ihre Hochschulen sie zu „gläsernen Studierenden“ machen.

5.4 Fazit

Nicht jeder Studienabbrecher kann mit absoluter Gewissheit auf eine atemberaubende Karriere in der IT-Industrie, Politik oder Medienbranche hoffen. Auch deshalb besteht eine der vornehmsten und wichtigsten Aufgaben der Hochschulen darin, die Studierenden auf dem Weg zum ersehnten Abschluss nicht zu verlieren, sondern sie angemessen beratend zu begleiten. Der Blick auf die Realität der deutschen Hochschulen aber legt offen: Sollen die hohen Studienabbrecherzahlen sinken, führt kein Weg daran vorbei, die Betreuungsrelationen spürbar zu verbessern. Die Hochschulen sollten die Studienberatung so reformieren, dass sie auf die individuellen Bedürfnisse und Fragen der Studierenden möglichst frühzeitig eingeht.

Softwareanwendungen allein können das Problem jedenfalls nicht lösen. Sie stoßen insbesondere dort an ihre Grenzen, wo – wie in der psychologischen Studienberatung – zwischenmenschliche Kompetenzen, wie Einfühlungsvermögen und Lebenserfahrung, gefragt sind. Vollautomatisierte Verfahren können die Begleitung durch das Studium daher allenfalls unterstützen, nicht aber ersetzen. In dieser Funktion können sie sich als niedrigschwelliges und jederzeit verfügbares Zusatzangebot entpuppen, das Studierende bei ihrer Studienorganisation an die Hand nimmt – und nebenbei die Beratungsbüros der Universitäten entlastet, damit die Berater sich auf die individuelle Betreuung konzentrieren können.

Hochschulrechtlich sind solche Studienberatungsprogramme an deutschen Hochschulen im Grundsatz zulässig. Das gilt jedenfalls so lange, wie das einschlägige Landeshochschulgesetz nicht abschließend regelt, wer die Studien(fach)beratung durchzuführen hat (und den Hochschulen somit einen eigenen Handlungsspielraum belässt). Bis auf Berlin und Brandenburg haben die Landesgesetzgeber auf solch strikte Vorgaben in ihren Hochschulgesetzen verzichtet – wenn wohl auch nicht mit dem visionären Bestreben, automatisierte Beratungsmöglichkeiten explizit zuzulassen.

Algorithmenbasierte Studienberatungsprogramme sehen sich im Ergebnis weniger hochschul- als *datenschutzrechtlichen* Hürden ausgesetzt: Sie zu verwenden, setzt nicht nur eine Verarbeitungserlaubnis voraus (Art. 6 Abs. 1 UAbs. 1 DS-GVO). Vor allem der Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO) verwehrt es den Hochschulen grundsätzlich, personenbezogene Daten der Studierenden unbegrenzt auszuwerten und zu immer neuen Bewertungsschablonen miteinander zu verknüpfen. Keineswegs dürften deutsche Hochschulen daher US-amerikanische Beratungssoftware wie *eAdvisor* einfach unverändert einsetzen. Stattdessen müssten sie auf datenschutzkonforme Anwendungen zurückgreifen bzw. diese entwickeln (lassen).[73]

Dass ein Landesdatenschutzbeauftragter Bußgelder in Millionenhöhe gegen deutsche Hochschulen verhängt, wenn sie ein rechtswidriges Beratungsprogramm einsetzen, müssen diese zwar nicht fürchten. Denn sie genießen ein Behördenprivileg (Art. 83 Abs. 7 DS-GVO; dazu bspw. Martini, Wagner und Wenzel 2018: 177). Studierende könnten die Hochschulen jedoch zivilrechtlich auf Schadenersatz verklagen (Art. 82 Abs. 1 DS-GVO).

Im Informationsgeflecht der digitalen Welt lassen sich Daten immer einfacher mithilfe von Big-Data-Instrumenten zu umfangreichen Persönlichkeitsprofilen verweben. Für die informationelle Selbstbestimmung des Einzelnen gehen damit nachhaltige Risiken einher. Das Datenschutzrecht will dem ein schlagkräftiges Bollwerk der Kontrolle

---

[72] Siehe für das (insoweit praeter propter inhaltsgleiche) nationale Verfassungsrecht: BVerfGE 65, 1 (53). Allerdings sind solche Vollerfassungen der Persönlichkeit in einem reinen Studienberatungsprogramm, das viele Lebensbereiche außen vor lässt, technisch auch nur schwer vorstellbar. Denn sie beschränken sich regelmäßig jeweils auf Teilaspekte der Persönlichkeit.

[73] Zu den Gefahren eines internationalen Transfers personenbezogener Daten deutscher Studierenden in die USA siehe weiterführend Martini und Botta 2019: 260 ff.

über die eigenen Daten und damit der freien Persönlichkeitsentfaltung der Studierenden entgegensetzen. Privatsphäre alleine verbürgt dem Studienabbrecher zwar noch keinen beruflichen Erfolg. Ohne informationelle Selbstbestimmung fehlt dem beruflichen Erfolg aber womöglich die freiheitliche Grundlage der Persönlichkeitsbildung, die das wissenschaftliche Studium an deutschen Universitäten gerade beflügeln soll. Dass der eigene materielle Erfolg nicht alles ist, wusste schon der populäre Studienabbrecher *Bill Gates*: „Success is a lousy teacher. It seduces smart people into thinking they can't lose."

6 Mit der algorithmischen Kristallkugel auf Tätersuche?

Predictive Policing auf dem Prüfstand des deutschen Rechts

Prof. Dr. Mario Martini und David Nink

6.1 Predictive Policing – ein neues Instrument im staatlichen Handlungsbesteck

Zu den technischen Visionen der Sicherheitsforschung gehört eine uralte Idee: der Versuch, Straftaten bereits erkennen zu können, bevor sie ausgeführt werden. Big Data scheint diesen Gedanken Wirklichkeit werden zu lassen. Der Reigen der technischen Möglichkeiten ist unterdessen vielfältig. Er reicht von Gesichtserkennung über forensische Maßnahmen der Datenanalyse bis hin zum Gefährderdatenbankscoring.

So verwundert es kaum, dass auch die Polizei Bedarf verspürt, auf das Handlungsarsenal Künstlicher Intelligenz rechtssicher zurückgreifen zu können.[74] Dabei sieht sie sich einem grundrechtspolitischen Dilemma ausgesetzt: Je mehr Erkenntnisse algorithmenbasierte Systeme der Polizeibehörden generieren sollen, umso mehr Daten sind dafür nötig. Doch inwieweit rechtfertigt der Nutzen von Big Data die mit den Analysen verbundenen Risiken?

Am Beispiel von Predictive Policing ist darum eine lebhafte Diskussion entbrannt. Das Schlagwort beschreibt den Versuch, mithilfe datenbasierter Analysen vorausschauend orts- oder personenbezogene Wahrscheinlichkeitsaussagen über künftige Straftaten zu treffen, um dadurch die Arbeit der Polizeibehörden zu unterstützen. Polizeikräfte sollen auf diese Weise rechtzeitig am Ort des Geschehens eintreffen und Straftaten verhindern.

Der Grundgedanke des Ansatzes beruht darauf, tradierte kriminologische Hypothesen in die Welt der digitalen Möglichkeiten zu übersetzen. Das Konzept macht sich dabei Erkenntnisse der Statistik und der Kriminologie bzw. Sozialforschung zunutze, bspw. den *Near-repeats*-Ansatz. Ihm liegt die Vermutung zugrunde, dass bestimmte Delikte eine Indizfunktion für die Zukunft haben: Wo sie auftreten, erhöht sich die Wahrscheinlichkeit dafür, dass es in der räumlichen Nähe alsbald erneut zu einer vergleichbaren Straftat kommt. Für Wohnungseinbruchsdiebstähle gilt diese Hypothese als kriminologisch abgesichert – jedenfalls hinsichtlich professioneller Taten zur Tageszeit und der Lokalität (etwa Stadtviertel, Gebiet, Straße).[75] Für diese Delikte lassen sich dann nach Auswertung polizeilicher Daten – etwa der Tatschwerpunkte, angefertigter Täterprofile und des örtlichen Umfelds – zeitliche und räumliche Konzentrationen einzelner Straftaten prognostizieren. Das System markiert auf einer Karte Bereiche, in denen die Wahrscheinlichkeit für weitere Taten im Verhältnis zur Standardwahrscheinlichkeit signifikant erhöht ist. Der Blick in die Vergangenheit der Daten – so die Prämisse – offenbart dann ein Stück weit die Zukunft.

6.2 Nicht personenbezogene Anwendungen

6.2.1 Rechtsdogmatische Bewertung

6.2.1.1 Datenschutzrecht

Auch die deutsche Polizei bedient sich zunehmend der Methode des Predictive Policing. Hierzulande beschränkt sich ihr Einsatz gegenwärtig auf die Vorhersage professioneller bzw. bandenmäßiger (Wohnungseinbruchs- und

---

[74] Als Teil des Modernisierungsprojekts „Polizei 2020“ ist eine eigene KI-Strategie für die Polizei in Arbeit. Sie schreibt die „Nationale Strategie für Künstliche Intelligenz“ fort, die bereits im Sicherheitsbereich auf neue Technologien setzt. Vgl. BT-Drs. 19/5880, S. 32 f.

[75] Vgl. dazu Suckow 2018: 347 ff. sowie die Übersicht über die gängigen Kriminalitätstheorien bei Neubacher 2017: 87 ff.

Gewerbe- sowie Kfz-)Diebstähle.[76] Die Systeme arbeiten mit tat- und ortsbezogenen, nicht aber mit täter- oder tatverdächtigenbezogenen Analysen.[77] Sie bewegen sich damit außerhalb des Anwendungsradius des Datenschutzrechts: Sowohl die DS-GVO und die Datenschutzrichtlinie für (Straf-)Justiz und Inneres (Richtlinie [EU] 2016/680; „JI-RL“) der Europäischen Union als auch die deutschen Datenschutzgesetze erstrecken ihren normativen Geltungsanspruch lediglich auf personenbezogene Daten[78] (Art. 2 Abs. 1 DS-GVO, Art. 2 Abs. 1 JI-RL, § 1 Abs. 1 BDSG).

Allerdings kann auch ein Ortsbezug ausnahmsweise einen Personenbezug herstellen, also den Rückschluss auf Individuen ermöglichen – namentlich, wenn die Polizei den Datensatz (ggf. in Verbindung mit anderen Daten) auf kleinräumige Parzellen herunterbricht, die einzelne Personen (z. B. einzelne Bewohner eines Einfamilienhauses) identifizierbar machen.[79] So fließen bspw. in das nordrhein-westfälische Vorhersagesystem *SKALA* neben geographischen und infrastrukturellen auch soziodemographische Informationen (Kaufkraft, Einwohnerstruktur etc.) ein.[80] Zumindest unerwünschte räumliche Segregationseffekte lassen sich dann nicht gänzlich ausschließen.[81] Auf „parzellenscharfe“ Prognosen verzichten die deutschen Behörden jedoch bislang bewusst.

6.2.1.2 Polizeirecht

- **Abgrenzung zwischen Polizei- und Strafprozessrecht**
  Vorausschauende Polizeiarbeit bewegt sich zwischen Prävention und Repression, also zwischen Polizeirecht und Strafrecht. Denn sie nutzt die Daten bereits *begangener* Straftaten, um im Idealfall *bevorstehende* Delinquenz zu verhindern. Zwischen beiden Feldern verläuft ein rechtlicher Graben unterschiedlicher Kompetenzträgerschaft: Für die Gefahrenabwehr sind grundsätzlich[82] die Länder, für die Strafverfolgung ist grundsätzlich der Bund zuständig.[83] Die Länder haben das Gefahrenabwehrrecht in ihren Polizeigesetzen ausgestaltet, Instrumente der Strafverfolgung regelt der Bund in der Strafprozessordnung (StPO).

---

[76] Mediale Aufmerksamkeit erlangte insbesondere das System *PRECOBS* (Pre Crime Observation System); siehe etwa Hommel 2017: 10 f.; Petrick-Löhr 2017.
[77] Bayern, Hessen und Nordrhein-Westfalen nutzen das Werkzeug bereits im Dauerbetrieb; Baden-Württemberg, Niedersachsen und Berlin fahren die Systeme noch testweise bzw. als Piloten. Auch Hamburg und Schleswig-Holstein setzen auf algorithmische Unterstützung. Das Gros der Anwendungsfälle fällt in die Deliktsgruppe der Wohnungs- und Gewerbediebstähle bzw. -einbrüche; probeweise stoßen vereinzelt auch Anwendungen für Kfz-Delikte hinzu (so etwa im System *SKALA* – System zur Kriminalitätsauswertung und Lageantizipation – in Nordrhein-Westfalen). Zur Frage, ob und ggf. wann die Sicherheitsbehörden des Bundes Predictive Policing einsetzen, siehe die Antwort der Bundesregierung auf eine Kleine Anfrage der FDP-Fraktion (BT-Drs. 19/1513, S. 2).
[78] Personenbezogene Daten definieren Art. 4 Nr. 1 DS-GVO und Art. 3 Nr. 1 JI-RL als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen“.
[79] Eine rein theoretische Möglichkeit, einen Bezug zu einer Person herzustellen, reicht als solche nicht aus. Entscheidend ist der zeitliche und wirtschaftliche Aufwand, einzelne Personen zu identifizieren. Es kommt also darauf an, ob die konkrete und realistische Möglichkeit besteht, mit verhältnismäßigen Mitteln auf eine bestimmte Person direkt oder indirekt rückzuschließen. Dafür sind das tatsächlich und praktisch verfügbare Zusatzwissen sowie die sonstigen Mittel und Optionen des Verantwortlichen „oder einer anderen Person“ in Rechnung zu stellen, deren sich der Verantwortliche ohne unverhältnismäßigen Aufwand bedienen kann; siehe ErwGrd 26 S. 3 ff. DS-GVO; vgl. auch zur Abgrenzung zwischen Orts- (Geodaten) und Personenbezug, bereits Martini 2016a: 3 f.
[80] Landeskriminalamt Nordrhein-Westfalen 2018a: 22; Knobloch 2018: 23.
[81] So kann es bspw. zum sog. *Overpolicing* in „sozial schwächeren“, ggf. vermehrt von Minderheiten bewohnten Vierteln kommen. Die algorithmische Prognose kann dann (durch sog. *Feedbackschleifen*) zur selbsterfüllenden Prophezeiung mutieren.
[82] Etwas anderes gilt für die Aufgaben der Bundespolizei, insbesondere des Grenzschutzes (§ 1 f. BPolG).
[83] Die Strafverfolgung ist Teil des gerichtlichen Verfahrens. Für dieses weist das Grundgesetz Bund und Ländern eine konkurrierende Gesetzgebungskompetenz zu (Art. 74 Abs. 1 Nr. 1 GG). Die Länder dürfen dort also Regelungen treffen, solange und soweit der Bund von seiner Gesetzgebungszuständigkeit nicht gesetzlich Gebrauch gemacht hat (Art. 72 Abs. 1 GG).

Ob das Landespolizei- oder das Strafprozessrecht des Bundes einschlägig ist, hängt davon ab, welches Ziel die Maßnahme des handelnden Beamten jeweils verfolgt.[84] Predictive Policing ist regelmäßig darauf gerichtet, Straftaten vorbeugend abzuwehren, nicht aber sie zu verfolgen – es bewegt sich also im *Anwendungsbereich des Polizeirechts*.[85]

- **Abgrenzung zwischen der Prognoseentscheidung und dem Tätigwerden des Polizeibeamten**
  Nicht nur zwischen Polizeirecht und Strafprozessrecht verläuft aus juristischer Perspektive ein trennender Graben, sondern auch zwischen der *Prognose* eines Predictive-Policing-Systems und dem sich anschließenden *Tätigwerden der Polizeibeamten*: Algorithmische Prognosen als solche lösen grundsätzlich noch keinen Grundrechtseingriff aus (es sei denn, sie arbeiten mit personenbezogenen Daten). Ausführungsmaßnahmen gegenüber Bürgern – etwa eine Identitätsfeststellung (Personenkontrolle), ein Platzverweis oder die Überwachung der Telekommunikation –, die (zumindest auch) auf die algorithmische Prognose zurückgehen, muss die Polizei demgegenüber auf eine gesetzliche Befugnisnorm stützen können, die das Handeln legitimiert. Predictive Policing ersetzt insbesondere weder die Rechtsgrundlage noch das kriminalistische Gespür, geschweige denn die Berufserfahrung der Polizeibeamten. Prognosen, die auf der Grundlage von Big-Data-Analysen für bestimmte Gegenden erhöhte Deliktswahrscheinlichkeiten ausgeben, begründen daher als solche weder eine polizeirechtlich relevante Gefahr noch einen Tatverdacht.[86] Platzverweise etc. dürfte die Polizei mithin nicht ausschließlich auf eine (abstrakte) Softwareprognose stützen. Die handelnden Beamten kommen vielmehr nicht umhin, selbst eine Bewertung vorzunehmen und die vorliegenden *tatsächlichen* Anhaltspunkte auszuwerten.[87]

6.2.2 Rechtspolitische (Nutzen-)Bewertung

Ortsbezogenes Predictive Policing trägt im Idealfall dazu bei, Straftaten zu verhindern, statt sie erst nachträglich aufzuklären. Neben der Leistungsfähigkeit der eingesetzten Algorithmen und der kriminologischen Grundannahmen hängt dieser Ertrag des Systems entscheidend von der Datenbasis ab: Mit der Qualität, Verfügbarkeit und dem Umfang der Daten verbessern sich auch die Vorhersagen – bspw. wenn die Daten eines Wohnungseinbruchs schnell und vollständig vorliegen (etwa gestohlene Objekte, Beutehöhe, Tatort und -zeitpunkt sowie der Modus Operandi, also die Art und Weise der Tatbegehung). Unter diesen Prämissen kann Predictive Policing im Grundsatz erfolgreich zu einem ressourceneffizienten Einsatz der Polizeikräfte beitragen.

Besonders in Ländern wie den USA, in denen sich Polizeibeamte – bisweilen wohl auch nicht ganz ohne Grund – dem Vorwurf des Rassismus ausgesetzt sehen, tritt zur Tatprävention als Motivation und Nutzen des Predictive Policing hinzu, den Polizeieinsatz ein Stück weit nachvollziehbarer und rationaler zu machen, jedenfalls aber diskriminierende Vorannahmen und Tendenzen besser zu identifizieren (vgl. Capers 2017: 1254 f., 1268 ff.).[88]

---

[84] Schenke 2018: § 1 Rn. 11; Singelnstein 2018: 6.
[85] Steigt das Vertrauen der Polizei in (vermeintlich rationale) Prognosen, verändert das auch den Charakter des hoheitlichen Handelns insgesamt ein Stück weit: Der Blick verschiebt sich weg von der Aufklärung und Ahndung begangener Delikte hin zur Antizipation und Verhinderung bevorstehender Straftaten; Singelnstein 2018: 3, 5.
[86] Vgl. Meinicke 2015: 384; Singelnstein 2018: 7 f. Die *polizeirechtliche Gefahrendogmatik* unterscheidet insbesondere zwischen Anscheinsgefahr, Putativgefahr, Gefahrenverdacht, abstrakter Gefahr und erheblicher Gefahr. In der *Strafverfolgung* bildet hingegen der Tatverdacht (als sog. *Anfangsverdacht*) den Ausgangspunkt repressiv-polizeilichen Handelns: Es bedarf *konkreter* und *tatsächlicher* Anhaltspunkte dafür, dass ein Beschuldigter eine Straftat begangen hat. Eine bevorstehende Straftat begründet eine polizeirechtlich relevante Gefahr, die polizeiliches Tätigwerden legitimiert. Nachdem der bayerische Landesgesetzgeber den Anknüpfungspunkt der „drohenden Gefahr“ in das Sortiment der Eingriffsgrundlagen aufgenommen hat (vgl. Art. 11 Abs. 3 S. 1 BayPAG), sinkt zumindest dort auch die polizeiliche Eingriffsschwelle.
[87] Rademacher 2017: 384.
[88] Freilich sind algorithmenbasierte Systeme nicht per se diskriminierungsfrei, sondern abhängig von den Wertannahmen ihrer Programmierer sowie von der jeweiligen Datenbasis.

Ob die Methode allerdings im Ergebnis auch tatsächlich die gewünschten Wirkungen erzielt,[89] lässt sich nicht leicht messen. Kaum quantifizieren lässt sich bspw., inwieweit Predictive Policing das Sicherheitsgefühl der Bevölkerung steigert[90] – ebenso der Nutzen, der von einer verstärkten Kommunikation zwischen Bürgern und Polizei (etwa durch Bürgerdialoge oder Onlineinformationen zum polizeilichen Handeln) ausgeht. So verwundert es auch nicht, dass die Datenlage zu empirisch belegbaren Erfolgen des Predictive Policing ambivalent ist (dazu Knobloch 2018: 28 f.): Für Bayern scheinen die bisherigen Statistiken zumindest erste Erfolge zu dokumentieren;[91] für Karlsruhe und Stuttgart hingegen liegen die kriminalitätsmindernden Effekte der Prognosesoftware allenfalls in einem moderaten Bereich.[92]

Die Zahlen erlauben auch keinen validen Rückschluss auf Kausalzusammenhänge: Dass die Kriminalität in den untersuchten Gebieten zurückgegangen ist, kann auch auf andere Faktoren als den Predictive-Policing-Einsatz zurückzuführen sein. Sie kann insbesondere auf Zufallsschwankungen gründen. Ohnedies lassen sich hypothetische Entwicklungen (etwa „verhinderte Straftaten“) kaum erfassen und beweisen (vgl. dazu auch Egbert 2017: 21 ff.; Legnaro und Kretschmann 2015: 97; Rolfes 2017: 60 ff.). Nicht zuletzt können sinkende Kriminalitätszahlen in Predictive-Policing-Gebieten auch das Ergebnis von Verdrängungs- und Ausnutzungseffekten sein: Als „lernende Systeme“ nutzen die Täter im Zweifel vorausschauend den Umstand aus, dass die Polizei verstärkt solche Viertel „bestreift“, in denen bereits Einbrüche stattgefunden haben. Die Kriminalität verlagert sich dann in andere Ortslagen; ein Katz-und-Maus-Spiel der anderen Art nimmt seinen Lauf.

6.3 Personenbezogene Anwendungen

6.3.1 Ausländische Beispiele

Im englischsprachigen Ausland geht Predictive Policing deutlich weiter als in Deutschland. Etliche Behörden setzen dort auch personenbezogene Analysen ein: In den USA kommen bspw. Listen zum Einsatz, die den Bürgern einer Stadt polizeitaktische Risikoscores zuordnen.[93] Die Systeme umfassen zudem deutlich mehr Deliktsgruppen als in Deutschland (Ferguson 2017a: 1129 ff.; Gluba 2014: 7; Rademacher 2017: 369 f.).

Ein prominentes Beispiel für personenbezogenes Predictive Policing ist die sog. *Strategic Subject List* der Chicagoer Polizei (*Heatlist*; dazu auch Egbert 2017: 19). Die Liste erfasst jede Person, welche die Polizei einmal in Gewahrsam genommen oder erkennungsdienstlich (via Fingerabdruckregistrierung) behandelt hat – das sind immerhin fast 400.000 Menschen (Posadas 2017) und damit mehr als ein Siebtel der Einwohner. Seit 2013 berechnet ein Algorithmus täglich für jede der gelisteten Personen einen Wert zwischen 1 und 500. Je höher der Wert, desto größer ist – so die Hypothese – das Risiko, dass jemand als Täter oder Opfer (der Score unterscheidet insoweit

---

[89] Vgl. nur Landeskriminalamt Nordrhein-Westfalen 2018b: 4.

[90] Auch insoweit besteht eine gewisse Ambivalenz: Mehr Polizeipräsenz in einem Stadtviertel kann das Sicherheitsgefühl mancher Bürger erhöhen, umgekehrt aber auch dasjenige anderer senken.

[91] Das Bayerische Innenministerium führte gesunkene Kriminalitätsraten teilweise ausdrücklich auch auf den Einsatz von *PRECOBS* zurück: „Knapp 9 % weniger Wohnungseinbrüche, knapp 10 Millionen Euro weniger Schaden! Durch das Ineinandergreifen von Schwerpunktkontrollen, länderübergreifender Ermittlungsarbeit und dem Einsatz innovativer Technik, wie etwa der Prognosesoftware PRECOBS, konnten im vergangen Jahr 893 Wohnungseinbrecher festgenommen werden und damit 41,5 % mehr als 2014“; heißt es etwa in der Polizeilichen Kriminalstatistik Bayern 2015: 1 (Vorwort).

[92] Vgl. die Ergebnisse des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht bei Gerstner 2018: 115 ff.

[93] Auch in Großbritannien setzt die Polizei großflächig auf algorithmische Hilfe: Die Durham Police bspw. nutzt den „HART“-Algorithmus, der die Beamten u. a. bei der Entscheidung unterstützt, ob Verdächtige und Verurteilte in (Untersuchungs-)Haft verbleiben sollten. In vielen Dienststellen kommen auf Künstlicher Intelligenz basierende Systeme zum Einsatz, die aus historischen Kriminalitätsdaten Muster erlernen bzw. erkennen und die Beamten über sog. *Kriminalitäts-Hotspots* informieren, für die ein hohes Risiko für die Begehung von Straftaten besteht. Auch die Polizei in South Wales setzt auf moderne Ermittlungstechnologie: Sie nutzt eine Gesichtserkennungssoftware, um Delinquenten zu identifizieren – insbesondere bei großen (Sport-)Ereignissen.

nicht) in ein Gewaltdelikt, insbesondere eine Schießerei, verwickelt wird (Singelnstein 2018: 2; Sommerer 2017: 148). Ein hoher Risikoscore gestattet der Polizei besondere Überwachungsmaßnahmen oder individuelle Gefährderansprachen bzw. Hausbesuche (Ferguson 2017a: 1142 ff.).

Dass gerade Chicagos Polizei intensiv auf personenbezogenes Predictive Policing setzt, ist kein Zufall: Die Stadt leidet unter einer der höchsten Mordraten der Vereinigten Staaten.[94] Die *Heatlist* ist insofern nicht nur Ausdruck eines anderen Datenschutzverständnisses in Übersee, sondern auch eines als besonders hoch empfundenen Sicherheitsbedürfnisses.

Auch in der Schweiz verwenden die Behörden Gefährderdatenbanken und Scores für ihre Arbeit. Für mittlerweile über 3000 Einzelpersonen berechnet ein Algorithmus individuelle Gefährlichkeitsprognosen – etwa zur Wahrscheinlichkeit, dass ein vermeintlich oder tatsächlich gefährlicher Mann seine Partnerin schwer verletzt oder gar tötet. Das eingesetzte „Dynamische Risiko-Analyse-System“ (DyRiAS) des deutschen „Instituts Psychologie und Bedrohungsmanagement“ überschätzt jedoch im Schnitt die Gefährlichkeit der Eingetragenen: Es verdächtigt zwei von drei Personen zu Unrecht (Grossenbacher 2018).[95]

Die Mitgliedstaaten der Europäischen Union üben sich beim Einsatz personenbezogener Predictive-Policing-Anwendungen zwar bislang in Zurückhaltung. Aber auch hier ist der behördliche Einsatz automatisierter Mustererkennungssysteme keine Zukunftsmusik mehr. So kommen an den europäischen (Binnen- und Außen-) Grenzen bspw. bereits Technologien wie die „intelligente Videoüberwachung“ zum Einsatz: Sie sollen Einreisevorgänge durch automatische Gesichts- und Dialekterkennung sowie automatisierte Kontrollschleusen beschleunigen, Gefährder identifizieren und Verwaltungsressourcen einsparen (vgl. Jeandesboz, Rijpma und Bigo 2016:12 ff.; Lehtonen und Aalto 2017: 207 ff.). Die deutschen Behörden, insbesondere das Bundeskriminalamt (BKA) setzen vermehrt auf Scoring-Systeme, die Terrorverdächtige kategorisieren: Die Risikobewertungssoftware Radar-iTE bspw. soll die Gefahr einschätzen, die von islamistischen Gefährdern bzw. Terrorverdächtigen ausgeht, und mögliche Maßnahmen priorisieren.

Aus technischer Sicht ähneln derartige Anwendungen Predictive-Policing-Prognoseinstrumenten: Sie operieren jeweils mit (Verhaltens-, Bewegungs- und optischen) Mustern, um daraus Schlüsse für weitere Maßnahmen zu ziehen. Auch in Deutschland finden bereits Testläufe für Gesichts- und Mustererkennungssoftware im öffentlichen Raum statt, etwa in Berlin (am Bahnhof Südkreuz) und Mannheim. Die Systeme sollen Gewalttäter identifizieren sowie verdächtige, ungewöhnliche Handlungen möglichst frühzeitig detektieren. Ob sich dies auch datenschutzkonform umsetzen lässt, steht freilich auf einem anderen Blatt.[96]

6.3.2 Rechtsdogmatische Bewertung nach deutschem Recht

Personenbezogenes Predictive Policing gründet seine Leistungskraft auf Profiling-Methoden: Es analysiert personenbezogene Daten, um persönliche Aspekte einer natürlichen Person, z. B. ihr Verhalten, ihre Vorlieben oder Kriminalitätsneigungen, zu prognostizieren (vgl. auch Art. 3 Nr. 4 JI-RL).[97] In die Prognosedatenbanken fließen zahlreiche Faktoren ein: von Alter, Vorstrafen und sonstigen Polizeidaten über den Wohnort bis hin zum sozialen

[94] Allein im Jahre 2016 wurden 762 Morde in Chicago begangen, also im Schnitt mehr als zwei täglich; vgl. etwa Albes 2018.
[95] Der politisch gewollte Null-Risiko-Ansatz geht dort also mit einer starken Überschätzung des Risikos einher.
[96] Siehe dazu etwa Hornung und Schindler 2017: 205 ff.; Salzmann und Schindler 2018.
[97] Vgl. Art. 3 Nr. 4 JI-RL: „Profiling“ meint „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, […] personenbezogene Daten [zu verwenden], um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, wirtschaftlichen Lage oder Gesundheit sowie persönliche sowie Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“. Siehe auch Art. 11 Abs. 1 JI-RL: Wie stets ist eine Rechtsgrundlage notwendig, um die Maßnahme zu legitimieren.

Umfeld (etwa Daten über Mitinsassen in einer JVA oder eine Auswertung sozialer Medien)[98] – zusätzlich Lebensereignisse und Verhaltensmuster, welche die Polizei als kriminalitätsrelevant erachtet (Egbert 2017: 19 ff.).

Profilerstellung und individuelle Gefährlichkeitsprognosen sind zwar kein neues polizeitaktisches Phänomen der digitalen Welt. Vielmehr waren sie schon in der Vergangenheit Teil des Handlungsbestecks der Polizei (Rademacher 2017: 369). Personenbezogenes Predictive Policing dringt jedoch tiefer in die Privatsphäre Betroffener – auch unbeteiligter Dritter – ein als klassische analoge Ermittlungsmethoden.[99] Im schlimmsten Fall drohen eine Katalogisierung und Registrierung der Persönlichkeit (obgleich die kriminalstatistische Wirksamkeit bislang nicht belegt ist).[100]

6.3.2.1 Anwendbare Vorschriften

Für Systeme des Predictive Policing, die mit personenbezogenen Daten operieren, steckt seit Mai 2018 zuvorderst die Richtlinie (EU) 2016/680 (JI-RL) den zulässigen Handlungsrahmen ab.[101] Ihn füllen im Bereich *präventiven* polizeilichen Handelns die Vorschriften zur Datenerhebung und -verarbeitung der Landespolizeigesetze sowie ergänzend die Landesdatenschutzgesetze bzw. §§ 3 f., 48 ff. BDSG aus.[102] Für den *repressiven* Einsatz (also zur Strafverfolgung) sind demgegenüber die Regelungen der StPO einschlägig.

- **Verarbeitungsgrundsätze**
  Anders als das bisherige Datenschutzregime trennt das neue unionale Datenschutzrecht terminologisch nicht länger feingranular zwischen der Erhebung, Nutzung, Speicherung, Übermittlung, Verknüpfung etc. von Daten. Es fasst all diese Vorgänge nunmehr unter dem Begriffsdach „Verarbeitung“ zusammen.[103] Alle unterschiedlichen Spielarten der Verarbeitung bedürfen ausnahmslos einer datenschutzrechtlichen Erlaubnis (Art. 8 Abs. 1 JI-RL).

  Aber auch wenn eine Verarbeitungsgrundlage greift, gestattet sie der Polizei nicht jedes datenrelevante Handeln. Die Verarbeitung ist grundsätzlich nur zulässig, wenn sie einem festgelegten, eindeutigen, legitimen Zweck dient (Zweckbindung – Art. 4 Abs. 1 lit. b JI-RL)[104] und sich in ihrem Umfang auf das Maß beschränkt, das notwendig ist, um den Zweck zu erfüllen (Art. 4 Abs. 1 lit. c JI-RL[105] – „nicht übermäßig“[106]). Ein explizites allgemeines Gebot der Transparenz bzw. Nachvollziehbarkeit[107] kennen die Verarbeitungsgrundsätze des Art. 4 JI-RL demgegenüber (anders als Art. 5 Abs. 1 lit. a DS-GVO) nicht.

- **Spezielle Vorgaben im datenschutzrechtlichen Regelungsregime**
  Das unionsrechtliche Regime des Polizeidatenschutzes unterwirft vollständig automatisierte Einzelentscheidungen einer Sonderregelung (vgl. Art. 11 JI-RL; § 54 BDSG): Ein automatisiertes Profiling, das ohne menschliche Beteiligung in eine Entscheidung mit rechtlicher oder vergleichbarer Wirkung mündet, ist

---

[98] Vgl. zum sog. Social-Media-Monitoring öffentlicher Stellen bereits Martini 2016b: 308 ff.
[99] Daneben besteht die Gefahr, dass die Grenzen zwischen Gefahrenabwehr und Strafverfolgung bzw. -aufklärung verschwimmen, da die personenbezogenen Modelle auf Informationen aus „beiden Welten“ zugreifen.
[100] Vgl. zur Situation in Chicago die Analyse der *New York Times* (Asher und Arthur 2017): Die 1400 gelisteten Personen mit den höchsten Risikoscores (429 und höher) waren in weniger als 20 Prozent der Delikte mit Schusswaffen involviert (2016). Vgl. auch Saunders, Hunt und Hollywood 2016: 366: „The pilot effort does not appear to have been successful in reducing gun violence.”
[101] Vgl. Art. 2 Abs. 2 lit. d DS-GVO, Art. 1 Abs. 1 JI-RL.
[102] Für die Bundespolizei gilt das BPolG, subsidiär das BDSG (vgl. § 1 Abs. 1 BDSG).
[103] Die Rechtsgrundlagen in den Ländern und des Bundes unterscheiden demgegenüber (gegenwärtig noch) teilweise weiterhin begrifflich zwischen Datenerhebung (vgl. etwa §§ 21 ff. BPolG) und Datenverarbeitung bzw. -nutzung (vgl. etwa §§ 29 ff. BPolG). Erhebung und (Weiter-)Verarbeitung können zudem unterschiedliche Grundrechtseingriffe verkörpern, die jeweils gesonderter verfassungsrechtlicher Rechtfertigung bedürfen.
[104] Vgl. auch (für Anwendungsfälle jenseits der JI-RL) Art. 5 Abs. 1 lit. b DS-GVO.
[105] Vgl. auch Art. 5 Abs. 1 lit. c DS-GVO.
[106] Das ist Ausdruck des Verhältnismäßigkeitsprinzips, das alles staatliche Handeln überstrahlt.
[107] Siehe dazu auch unten Abschnitt 6.3.2.4.

grundsätzlich unzulässig. Die Mitgliedstaaten können eine solche Maßnahme aber durch gesonderte Rechtsvorschriften legitimieren (Art. 11 Abs. 1 JI-RL). Generell unzulässig sind allerdings Profiling-Maßnahmen, die an besonders geschützte Merkmale – etwa die ethnische Herkunft, die sexuelle Orientierung oder Gesundheitsdaten – anknüpfen und dadurch diskriminierend wirken (Art. 11 Abs. 3 i. V. m. Art. 10 JI-RL; § 54 Abs. 3 BDSG).

Jenseits solcher Entscheidungen, die *vollständig* automatisiert zustande kommen, setzen die JI-RL, die Landespolizei- und -datenschutzgesetze sowie §§ 45 ff. BDSG dem polizeilichen Profiling i. S. d. Art. 3 Nr. 4 JI-RL nur wenige *spezifische* normative Zulässigkeitsschranken entgegen. Eine konkrete Regelung treffen immerhin Art. 24 Abs. 1 S. 2 lit. e JI-RL und § 70 Abs. 1 S. 2 Nr. 5 BDSG: Setzen die Strafverfolgungsbehörden Profiling-Methoden ein, müssen sie dies in das datenschutzrechtliche *Verarbeitungsverzeichnis* aufnehmen. Neu ist auch die Pflicht, vor datenschutzrechtlich risikobehafteten Verarbeitungen, „insbesondere bei Verwendung neuer Technologien“ wie (personenbezogenem) Predictive Policing, eine *Datenschutz-Folgenabschätzung* durchzuführen (Art. 27 Abs. 1 JI-RL; § 67 Abs. 1 BDSG).

Im Übrigen finden die allgemeinen Verarbeitungsgrundlagen und -grundsätze des bereichsspezifischen Datenschutzrechts (insbesondere Art. 4 ff. JI-RL) sowie die konkretisierenden Regelungen des nationalen Rechts[108] Anwendung.

6.3.2.2 Anforderungen an eine zulässige Ausgestaltung

Soweit das (deutsche) Recht von den Regelungsspielräumen der JI-RL für eigene normative Gestaltungen Gebrauch macht, setzt das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)[109] der polizeilichen Datenerhebung die verfassungsrechtlichen Leitplanken.[110]

Erstellt die Polizei Risikolisten als Teil eines personenbezogenen Predictive Policing, verbietet (auch) das deutsche (Verfassungs-)Recht dies nicht a priori. Ein solches Vorgehen kann vielmehr dem Auftrag des Staates entsprechen, Leib und Leben der Bürger zu schützen (vgl. etwa Art. 2 Abs. 2 S. 1 GG): Zur Gefahrenabwehr und Strafverfolgung ist er kraft seines Gewaltmonopols nicht nur berechtigt. Er ist dazu auch verpflichtet. Greifen bspw. Erscheinungsformen der sog. *Organisierten Kriminalität*, etwa im Darknet, auf moderne Technologien zurück, um ihre Taten durchzuführen, müssen auch die Sicherheitsbehörden (selbstverständlich mit rechtsstaatlichem Augenmaß) handlungsfähig bleiben. So setzen nicht nur in den USA, sondern auch hierzulande die Behörden längst auf Gefährderdatenbanken und Risikoprognosen – etwa in europäischer Zusammenarbeit hinsichtlich islamistischer Gefährder oder bei der „Zentralen Informationsstelle Sporteinsätze“ (ZIS), die die bundesweite Datenbank „Gewalttäter Sport“ führt.

---

[108] Darunter fallen also die Vorschriften zur Datenerhebung und -verarbeitung in den Polizeigesetzen der Länder bzw. das BPolG für die Bundespolizei sowie ergänzend die Landesdatenschutzgesetze bzw. das BDSG.
[109] Grundlegend dazu BVerfGE 65, 1 (1 ff.) – Volkszählung.
[110] Der Grundrechtsschutz des Art. 8 der EU-Grundrechte-Charta greift nur insoweit, als zwingende Regelungsvorgaben des Unionsrechts und damit die Einheitlichkeit der Rechtsanwendung im Rechtskreis des Unionsrechts berührt sind. Denn der Anwendungsbereich der EU-Grundrechte-Charta ist kraft Art. 51 Abs. 1 S. 1 „ausschließlich bei der Durchführung des Rechts der Union“ eröffnet; der EuGH legt diesen Passus sehr weit aus; dazu insbesondere EuGH, NJW 2013, 1415 (1415 f.) – „Åkerberg Fransson“; restriktiver hingegen BVerfGE 133, 277 (315). Siehe zu dieser Abgrenzungsfrage auch Becker 2019: 469 ff.; Kirchhof 2014: 1537 f.; Martini 2019b: 735; sowie die Übersicht über die Rechtsprechung des EuGH und des BVerfG bei Kingreen 2016: Rn. 8 ff. Seit seinen jüngsten Entscheidungen zum Recht auf Vergessenwerden prüft das Bundesverfassungsgericht Verletzungen des Anwendungsvorrangs des Unionsrechts jedoch nicht nur am Maßstab der Vorschriften des Grundgesetzes, sondern auch am Maßstab der Grundrechte der Charta (BVerfG, Beschluss vom 6.11.2019, 1 BvR 276/17, Rn. 50 ff.; Beschluss vom 6.11.2019 – 1 BvR 16/13 –, Rn. 60 ff.). Betroffenen ebnet das zusätzliche Wege, unionalen Grundrechtsschutz gerichtlich sicherzustellen.

Inwieweit solche polizeilichen Maßnahmen zulässig sind, hängt jedoch stets von ihrer konkreten Ausgestaltung ab. Die Polizei muss vor ihrem Tätigwerden insbesondere kritisch prüfen: Ist die Rechtsgrundlage für die Datenerhebung hinreichend konkret, um die Maßnahme zu legitimieren? Sind die datenschutzrechtlichen Grundsätze eingehalten, bspw. die Zweckbindung (vgl. Art. 4 Abs. 1 lit. b und c JI-RL)? Bei ihren Verarbeitungsmaßnahmen hat die Polizei ferner – soweit möglich – zwischen den verschiedenen Kategorien betroffener Personen und dem staatlichen Handlungsziel zu unterscheiden (besteht der Verdacht, eine Straftat begangen zu haben/sie in Zukunft zu begehen; ist eine Person bereits in der Vergangenheit wegen einer Straftat verurteilt worden?) sowie zwischen Tatsachen und persönlichen Einschätzungen (vgl. etwa Art. 6, Art. 7 Abs. 1 JI-RL; § 72 f. BDSG).

Personenbezogene Daten, welche die Polizeibehörden bereits in zulässiger Weise erhoben und gespeichert haben (insbesondere Daten *Verurteilter*), dürfen die Polizeibehörden auf der Grundlage des gegenwärtigen deutschen Polizeidatenschutzrechts recht weitgehend zur vorbeugenden Kriminalitätsbekämpfung nutzen (vgl. für die Polizei Berlin etwa § 16 Abs. 3 ASOG Bln sowie § 21 S. 1, § 41 Abs. 1 Nr. 5, § 43a Abs. 1 BZRG[111]). Das müssen sie auch, um ihren Auftrag – Straftaten zu verhindern und aufzuklären – erfüllen zu können. Sofern unbedingt erforderlich, dürfen sie auch auf besondere Kategorien personenbezogener Daten, z. B. das Geschlecht oder genetische Daten, zurückgreifen, die grundsätzlich einen besonders hohen Schutz genießen (vgl. für die Bundespolizei etwa § 48 Abs. 1 BDSG; dann sind freilich geeignete Schutzgarantien geboten, vgl. § 48 Abs. 2 BDSG).

Maßgebliche Kriterien dafür, Personen rechtmäßig in ein Erfassungssystem einzubeziehen, sind – neben der Art der Daten – der Anlass sowie die Zweckbestimmung der Erhebung, insbesondere das Ausmaß der abzuwehrenden Gefahr (vgl. Singelnstein 2018: 7). Ein kriminaltaktisch sinnvoller Einsatz personenbezogener Vorhersagesysteme kann u. U. auch eine eingriffsintensive Nutzung in Gestalt maschineller, automatischer Datenabgleiche und Verarbeitungen sowie die Analyse großer Datenmengen erfordern.[112]

Zwar rechtfertigt das Ziel, einen Mord oder ein anderes schweres Verbrechen zu verhindern, deutlich intensivere Grundrechtseingriffe als bspw. ein Ladendiebstahl. Der gute Zweck heiligt aber nicht jedes Mittel. Die Eingriffstiefe muss vielmehr immer in einem grundrechtsschonenden, angemessenen Verhältnis zu dem erhofften Erfolg der Maßnahme, namentlich zur Schwere der drohenden Straftaten stehen. Solange nicht hinreichend valide erkennbar ist,[113] dass gerade der Personenbezug der Daten den Modellen die entscheidungserheblichen Ergebnisse abringt, ist die Verarbeitung datenschutzrechtlich nicht erforderlich und damit unzulässig. Daher ist es insbesondere grundsätzlich[114] nicht zulässig, Daten von Personen zu erheben und zu nutzen, die *keinerlei zurechenbaren Anlass zur polizeilichen Datenerhebun*g geliefert haben.[115] In dem System *SKALA* heißt das bspw. konkret: Daten über das Opfer (Name, Adresse) darf die Polizei zwar vorhalten, aber nicht in das Prognoseinstrument einfließen lassen. Denn sie stiften dem Systemerfolg keinen Nutzen und sind daher aus rechtlicher Sicht nicht erforderlich.[116] Konsequenterweise hat die Polizei *SKALA* in praxi auch so ausgestaltet: Das System verzichtet darauf, Opferdaten zu verarbeiten. Wo immer möglich, müssen die Systeme auch auf Anonymisierung, hilfsweise Pseudonymisierung

---

[111] Die Abkürzung steht für „Bundeszentralregistergesetz“.
[112] Wegen des Vorfeldcharakters des Predictive Policing ist die Nutzung personenbezogener Daten qua Natur der Sache sensibler als in der Strafverfolgung. Denn dort muss immerhin eine gewisse Wahrscheinlichkeit dafür bestehen, dass die Person bereits in strafrechtlich relevanter Weise in Erscheinung getreten ist.
[113] Vgl. zur Schwierigkeit, den tatsächlichen Nutzen und die Wirksamkeit von Predictive-Policing-Anwendungen nachzuweisen, bereits oben Abschnitt 6.2.2.
[114] Erlaubt ist die polizeiliche Inanspruchnahme nicht verantwortlicher und nicht verdächtiger Personen im Einzelfall immerhin, um eine gegenwärtige erhebliche Gefahr abzuwehren; vgl. für Berlin nur § 16 Abs. 1 ASOG Bln.
[115] Das wichtige Kriterium „Anlasslosigkeit“ brach sich in der Diskussion zur Chicagoer *Heatlist* Bahn: Darauf landeten höchstwahrscheinlich auch Personen, die dazu keinerlei Anlass gegeben hatten. Die Liste unterscheidet auch nicht zwischen Opfern und Tätern.
[116] Ein Vergleich mit der Rasterfahndung macht zudem deutlich: Auch für die verfassungsrechtliche Bewertung kommt es entscheidend darauf an, inwieweit die Methoden ihrer Zweckbestimmung entsprechend funktionieren; die Rasterfahndung brachte deutlich zu wenig „Ertrag“ bei zu viel „Datenbeifang“ ein.

setzen und angemessene Löschfristen vorsehen (vgl. etwa Art. 4 Abs. 1 lit. e, Art. 5 JI-RL), um dem Recht auf informationelle Selbstbestimmung der Betroffenen angemessen Rechnung zu tragen.

Mit Blick auf die intensiven Ausstrahlungswirkungen, die von *personenbezogenem* Predictive Policing auf die Grundrechte ausgehen (insbesondere das Risiko, dass sich auch Unbescholtene in einem solchen Netz der Überwachung verfangen), ist der Einsatz dieser Methode in Deutschland im Ergebnis allenfalls in engen Grenzen und nur für schwere Straftaten zulässig.[117] Bislang halten die Polizeigesetze der Länder dafür nicht die erforderlichen, hinreichend bestimmten Rechtsgrundlagen vor.[118]

Die Reichweite, in der US-Behörden Maßnahmen des personenbezogenen Predictive Policing zulassen, wäre mit den hiesigen verfassungsrechtlichen Vorstellungen von Verhältnismäßigkeit nicht vereinbar. Das Recht auf informationelle Selbstbestimmung und die Menschenwürdegarantie (vgl. Art. 1 Abs. 1 GG) verbieten eine anlasslose[119], rein prophylaktische „Rundum-Überwachung" der Bürger und eine vollständige Katalogisierung sowie Registrierung der Persönlichkeit des Einzelnen: Flächendeckend umfassende Persönlichkeitsprofile zu bilden, ist unzulässig.[120] Für Daten aus dem Kernbereich privater Lebensführung besteht ein absolutes verfassungsrechtliches Nutzungsverbot.[121]

6.3.2.3 Gefahr der Diskriminierung und Verfestigung

Predictive-Policing-Listen schreiben Vergangenes für die Zukunft fort. Wenn sich die Lebensumstände und das soziale Umfeld einer gelisteten Person ändern, spiegelt sich das daher nicht ohne Weiteres im Risikoscore wider. Soziale Zusammenhänge und Kausalbeziehungen in ihren ebenso facettenreichen wie komplexen lebensweltlichen Interdependenzen adäquat zu erfassen, sind algorithmische Systeme (jedenfalls noch) nicht imstande. Die Vielschichtigkeit delinquenten Verhaltens, Gruppendynamiken und Spontantaten lassen sich nur schwer in maschinelle Muster pressen.

Bereits die Einstufung als gefährdende oder gefährdete Person auf der Liste kann aber erhebliche stigmatisierende und ausgrenzende, schlimmstenfalls sich selbst verstärkende Effekte nach sich ziehen.[122] Predictive Policing avanciert dann auch unfreiwillig zu einem Instrument der Verhaltenssteuerung, etwa wenn Personen ihr eigenes (Alltags-)Verhalten bewusst oder unbewusst danach ausrichten, nicht in den Prüfradar polizeilicher Algorithmen zu geraten.[123]

---

[117] So auch Meinicke 2015: 382 f.; Rademacher 2017: 394 f.; Singelnstein 2018: 6. In diesem Sinne hat auch das BVerfG der (vergleichbaren) präventiven Rasterfahndung enge Grenzen gezogen; vgl. BVerfGE 115, 320.
[118] Die Vorschriften zur „drohenden Gefahr", die Bayern und Nordrhein-Westfalen in ihre Polizeigesetze aufgenommen haben, verlagern polizeiliche Datenerhebungsmaßnahmen noch weiter in das Vorfeld von Kriminalität (vgl. auch Fn. 86); den Einsatz personenbezogener Predictive-Policing-Methoden vermögen jedoch auch diese Normen nicht unmittelbar zu tragen; vgl. zu dieser neuen Rechtsfigur Leisner-Egensperger 2018: 677 ff.
[119] Allerdings erlauben die Polizeigesetze bereits jetzt anlassunabhängige Identitätsfeststellungen an sog. *kriminalitätsbelasteten Orten* sowie Informationsbeschaffungsmaßnahmen zur vorbeugenden Verbrechensbekämpfung; vgl. etwa § 21 Abs. 2, § 25 ASOG Bln.
[120] Vgl. dazu auch BVerfGE 6, 32 (41); 65, 1 (51); 109, 279 (323); 113, 348 (391 f.); 120, 274 (335 f.). Insbesondere ist es mit der Würde des Menschen nicht zu vereinbaren, ihn „zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren [...] und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist"; vgl. BVerfGE 27, 1 (6) – Mikrozensus.
[121] Dazu BVerfGE 120, 274 (335, Rn. 270).
[122] Zudem ist es maschineller Arbeitsweise eigen, nicht sauber zwischen Kausalität und Korrelation trennen zu können; vgl. zu diesen *Cum-hoc-ergo-propter-hoc*-Fehlschlüssen etwa Martini 2019a: 60.
[123] Martini 2019a: 50 ff.

6.3.2.4 Transparenz

Schlagzeilen machten Predictive-Policing-Gefährderlisten in der Vergangenheit besonders wegen ihrer Intransparenz. Die Chicagoer Polizei bspw. legt nicht lückenlos offen, wen das System bzw. die Polizeibehörden warum auf die Liste setzen. Neben den bereits einmal Inhaftierten und den erkennungsdienstlich Behandelten sollen auch vollkommen Unbescholtene den Weg in die *Heatlist* gefunden haben (Posadas 2017).[124]

Ein rechtsstaatlich tragfähiges System, das mit personenbezogenen Daten hantiert, bedürfte zweier Bausteine der Transparenz: der *Systemtransparenz*[125] und der *Ergebnistransparenz*.

- **Systemtransparenz**
  Solange Daten nicht im Ansatz nachvollziehbar sind, ist es weder Betroffenen möglich, ihre subjektiven Rechte zu verteidigen, noch können Richter die polizeilichen Maßnahmen in einer Weise wirksam gerichtlich kontrollieren, die ihnen Einblick in die algorithmischen Tiefen vermittelt. Die Funktionsweise des Systems muss technisch und polizeitaktisch in ihren wesentlichen Funktionselementen nachvollziehbar sein (ohne zugleich dadurch umgekehrt seine Sicherheitsfunktion einbüßen zu müssen). Das setzt im Grundsatz insbesondere allgemeine Erläuterungen voraus, die zumindest die genauen Aufgaben der Systeme und ihrer Methodiken offenlegen.

- **Ergebnistransparenz**
  Transparenz ist nicht nur nötig, um die prinzipielle Funktionsweise des algorithmischen Systems erfassen, sondern auch, um die Qualität der Prognoseinstrumente und ihrer Ergebnisse prüfen zu können.[126] Wichtige Bestandteile eines solchen Konzepts der Ergebnistransparenz sind neben passgenauen Kontrollmechanismen (etwa Kontrollschnittstellen der Aufsichtsbehörden, die bei Bedarf jederzeit einen Einblick in die Verarbeitungsmechanismen des Systems ermöglichen) auch (zu veröffentlichende) Projekt- und Testberichte (Singelnstein 2018: 7; Martini 2017a: 1021 f.).[127]

6.3.2.5 Zwischenergebnis

Listen wie die Chicagoer *Heatlist* wären in ihrer bisher praktizierten Form in Deutschland nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar. Ihre Eingriffstiefe in die Privatsphäre auch unbescholtener Bürger steht in keinem rechtsstaatlich verantwortbaren Verhältnis zum verfolgten staatlichen Zweck der Gefahrenabwehr. Das gilt umso stärker, je weniger valide der nachgewiesene Nutzen ist, den die Systeme hervorbringen.

---

[124] Im Unterschied dazu hat das Landeskriminalamt Nordrhein-Westfalen seine Evaluationsergebnisse vollständig offengelegt und so ein hohes Maß an Transparenz etabliert.

[125] Vgl. auch Zweig 2019: 9 ff.: Den Quellcode offenzulegen, ist nicht das Mittel der Wahl, sondern kann allenfalls in Ausnahmefällen bzw. als Ultima Ratio sinnstiftend sein, weil nicht „der Algorithmus“ transparent sein muss, sondern Gegenstand der Betrachtung das „sozioinformatische Gesamtsystem“ sein sollte. Der Algorithmus steht insbesondere selten isoliert vom „Faktor Mensch“.

[126] Mit dem Ziel, die Transparenz (auch staatlich eingesetzter) algorithmenbasierter Entscheidungssysteme zu erhöhen, ist bspw. im US-Bundesstaat New York kürzlich ein Gesetz in Kraft getreten („Automated decision systems used by agencies“, 2018/049). Es spricht u. a. Empfehlungen dafür aus, welche Informationen zu einem automatisierten Entscheidungssystem und zur jeweiligen Datengrundlage die datenschutzrechtlich Verantwortlichen öffentlich zugänglich machen sollten und wie sich Betroffene bei Rechtsverletzungen effektiv zur Wehr setzen können.

[127] Freilich lässt sich keine bedingungslose Transparenz garantieren: Besonders der Schutz der Geschäftsgeheimnisse des Herstellers (etwa ein privatwirtschaftlicher Vertragspartner der Polizeibehörde), aber rein tatsächlich auch die technische Komplexität der Prognoseinstrumente können dem Bemühen nach Transparenz Grenzen setzen. Bei Anwendungen, die für Hoheitsträger zum Einsatz kommen, genießt das Geschäftsinteresse der Programmhersteller aber nicht ohne Weiteres auch den Vorrang vor dem rechtsstaatlichen Gemeinwohlinteresse an Transparenz.

Eine algorithmische Prognose ersetzt nie eine konkrete Gefahr für die Eingriffsmaßnahmen des Einzelfalls (etwa eine Festnahme), welche die Polizei auf der Grundlage der Prädiktoren trifft – ebenso wenig diejenige des Tatverdachts (bei repressiven Maßnahmen). Die Datenanalyse eines Predictive-Policing-Systems versteht sich vielmehr immer lediglich als Ausgangspunkt, um polizeiliches Handeln einzuleiten (erste Stufe); ein anschließendes Tätigwerden der Polizeibeamten bedarf einer eigenständigen Gefahrenbewertung eines Akteurs aus Fleisch und Blut anhand konkreter Anhaltspunkte (zweite Stufe; ähnlich Rademacher 2017: 372 ff.; Singelnstein 2018: 2 ff., 7 f.).

6.4 Potenzial und Perspektiven – der Computer als kriminologischer Spürhund?

Predictive-Policing-Systeme der Kriminalgeographie, die bislang in Deutschland zum Einsatz kommen, basieren regelmäßig auf kriminologischen und kriminalistischen Annahmen, die der Mensch dem System vorgibt: Eine bestehende ätiologische[128] kriminologische Theorie verleiht der Prognosesoftware den analytischen Zielrahmen. Diese errechnet durch Datenauswertung Wahrscheinlichkeiten. In der Regel sind dazu einfache Entscheidungsbäume ausreichend.

Anders als solche „klassischen" Algorithmen sind lernfähige Systeme grundsätzlich in der Lage, weitgehend eigenständig Schlussfolgerungen zu ziehen – also etwa selbsttätig Muster von Delikten zu erkennen (vgl. auch Ferguson 2017b: 1 ff.). Das Zusammenspiel sehr großer verfügbarer Datenmengen[129] und maschineller Lernverfahren ermöglicht nunmehr, neue kriminologische Theorien bzw. neue ätiologische Annahmen zu entwickeln. Das eröffnet vertiefte Einblicke in Zusammenhänge, die der menschlichen und polizeilichen Erkenntnis bislang verborgen geblieben sind.[130]

Wenn die Systeme nicht mehr lediglich bereits bestehende (kriminologische und kriminalistische) Hypothesen anwenden und empirisch erhärten bzw. widerlegen, sondern selbst Muster und Zusammenhänge identifizieren, die sich dem menschlichen Betrachter verschließen, könnte sich das „Verhältnis zwischen Theorie und Daten sogar umkehren" (Singelnstein 2018: 3). So fußt bspw. die Software *HunchLab,* die in Philadelphia zum Einsatz kommt, nicht auf einer einzigen kriminologischen Theorie. Sie ist vielmehr theorieoffen, arbeitet also ohne vorgegebene kriminalistische Hypothesen. Mithilfe maschinellen Lernens erkennt sie sublime Muster in einem großen Datenpool und trifft im Idealfall passgenaue Vorhersagen (Azavea Inc. 2015: 10 ff.; Knobloch 2018: 17 f.; Shapiro 2017: 459 f.).

Derartige Risikoprognosen sind umso präziser, je leistungsfähiger die Algorithmen sind, die ihnen zugrunde liegen, und je breiter, also umfangreicher und aussagekräftiger, die Datengrundlage ist. Das impliziert allerdings auch, grundrechtlich sensible personenbezogene Daten einzubeziehen. Zudem lassen sich Prognosen, die auf lernfähigen Systemen basieren, einerseits noch schlechter als sonst nachvollziehen; für Betroffene und die Öffentlichkeit bleiben sie in der Regel eine Blackbox. Sie stellen andererseits nicht hinreichend sicher, dass ihre Entscheidungsparameter ausschließlich den Steuerungsvorgaben des demokratischen Gesetzgebers folgen, sich also nicht gleichsam verselbstständigen und neue, ggf. rechtswidrige Entscheidungskriterien entwickeln.[131] Verantwortbar

---

[128] Ätiologische Kriminalitätstheorien sind Theorien zur *Ursache* des Verbrechens. Dem stehen insbesondere die sog. *Etikettierungsansätze* (*labelling approach*) gegenüber. Sie erklären delinquentes Verhalten damit, dass die Abweichung sozial zugeschrieben und nicht objektiv vorhanden sei, vereinfacht gesagt also Kriminalität oftmals erst durch die Betrachtung als „kriminell" entsteht.

[129] Die global produzierte Datenmenge verdoppelt sich derzeit etwa alle zwei Jahre; vgl. Ferguson 2015: 354.

[130] Siehe dazu Berk 2013: 1 ff.; Chan und Bennett Moses 2016: 28 ff.; Ferguson 2015: 395 ff.; Singelnstein 2018: 3.

[131] Zu dem Problem der Transparenz bei lernenden Systemen ausführlich Martini 2019a: 28 ff., 176 ff.

sind solche Systeme nur, wenn sie auf einer – lückenlos zu gewährleistenden – demokratischen Legitimation aufbauen können und jedenfalls durch geeignete Kontrollmechanismen ihre vollständige Bindung an das Gesetz sicherstellen.[132]

6.5 Fazit

Predictive Policing eröffnet neue Chancen, um die Polizeiarbeit algorithmisch zu unterstützen und polizeiliche Ressourcen zielgerichtet einzusetzen. Die Symbiose großer Datenmengen und maschineller Lernverfahren, die für unterschiedliche kriminologische Theorien offen sind, verheißt für die Zukunft zusätzliche polizeitaktische und kriminologische Erkenntnisquellen. Die innovativen Methoden der maschinell-vorausschauenden Polizeiarbeit bergen umgekehrt aber auch das Risiko, Verdrängungseffekte auszulösen. Sie können ferner Fehler reproduzieren und auf diese Weise Verzerrungen institutionalisieren. Ihrer vermeintlichen Objektivität ist daher mit Obacht zu begegnen – ebenso der möglichen Kombination mehrerer Überwachungstechniken und dem Zusammenführen vieler Datenpunkte aus unterschiedlichen Quellen (etwa Videoüberwachung im öffentlichen Raum, Gefährderdatenbanken, automatische Kennzeichenerfassung etc.). Kriminalistisches Gespür, Berufserfahrung und Empathie können Algorithmen (jedenfalls noch) nicht bruchfrei abbilden.

Die Systeme eines *tatbezogenen* Predictive Policing, die in Deutschland Verwendung finden, sind mit den Bürgerrechten, insbesondere dem Recht auf informationelle Selbstbestimmung sowie der Unschuldsvermutung, vereinbar, verzichten sie doch darauf, mit personenbezogenen Daten zu operieren.

Die *personenbezogenen* Predictive-Policing-Anwendungen, die bspw. in der Schweiz und den USA zur Anwendung kommen, wären in Deutschland demgegenüber nicht ohne Weiteres zulässig. Um sie im Polizeialltag einzusetzen, bedürfte es nicht nur einer hinreichend bestimmten Rechtsgrundlage, welche die Datenerhebung und -nutzung legitimiert. Eine umfassende und großflächige, rein prophylaktische Profilerstellung lässt sich auch allenfalls bei schwersten Straftaten mit dem Recht auf informationelle Selbstbestimmung in Einklang bringen.

Bei allen Segnungen, die neue Technologien vorausschauender Polizeiarbeit verheißen: Eine Welt, die jede Form der Kriminalität im Keim erstickt, entpuppt sich bei genauerem Hinsehen als wenig erstrebenswert. Die *Möglichkeit*, Rechtsbruch zu begehen, ist gewissermaßen die Kehrseite der bürgerlichen Freiheit (Knobloch 2018: 7; Rademacher 2019: 702 ff.). Das chinesische Sozialkreditpunktesystem, das jeder Person einen sozialen Score zuordnet, um das Wohlverhalten der Bevölkerung zu optimieren, offenbart sich insoweit als dystopisch-düstere Kontrastfolie. Denn wer absolute Sicherheit um den Preis der bürgerlichen Freiheit anstrebt, wird auf Dauer weder das eine noch das andere erhalten.[133] Ein Recht, bei der Planung und Begehung schwerer Straftaten unbeobachtet zu bleiben, gibt es umgekehrt aber ebenso wenig. Einen mit Augenmaß ausgestalteten Kompromiss zwischen Sicherheit und Freiheit zu finden, wird Staat und Zivilgesellschaft in Zukunft mehr denn je einen anspruchsvollen Drahtseilakt abverlangen.

---

[132] Die Verfassung verlangt eine ununterbrochene Kette demokratischer Legitimation hin zu derjenigen Einheit, die die hoheitlichen Befugnisse im Einzelfall wahrnimmt. Auch der Einsatz neuer Technologien darf diesen Rückbezug staatlichen Handelns zum Volk als Souverän nicht unterbrechen; vgl. Art. 20 Abs. 2 S. 1 GG; BVerfGE 47, 253 (275); 83, 60 (72); 93, 37 (66); 107, 59 (87). Vgl. dazu ergänzend auch Abschnitt 4.6 in dieser Studie.

[133] In Anlehnung an *Benjamin Franklin*: „Those who would give up *essential* Liberty to purchase a little *temporary* Safety, deserve neither Liberty nor Safety.“ Das Zitat entstammt einem Schreiben *Franklins* vom 11.11.1755 und ist bspw. unter https://founders.archives.gov mit Beschreibung der Originalquelle zu finden.

7 Strafjustiz ex machina?

Zu den Grenzen algorithmenbasierter Assistenzsysteme bei Haftentscheidungen

Prof. Dr. Mario Martini und David Nink

7.1 Haftentscheidungen als das schärfste Schwert des Staates

Die Haft ist das schärfste Schwert des demokratischen Rechtsstaats. Als staatlich verordneter Freiheitsentzug ist sie daher nur unter strengen Voraussetzungen zulässig. Jeder kleine Fehler kann Lebensperspektiven zerstören. Paradigmatisch steht dafür das Schicksal des Syrers *Amad A.*: Er verlor im September 2018 sein Leben, als er zu Unrecht in einem nordrhein-westfälischen Gefängnis einsaß. Die Polizei hatte ihn aufgrund einer Verwechslung festgenommen. Einige Monate später starb er nach einem Brand in seiner Zelle (Stegemann 2018).

An solchen Einzelschicksalen arbeiten sich unzählige Bücher und Artikel über Justizirrtümer ab. Sie erfreuen sich nicht zuletzt deshalb hoher Aufmerksamkeit, weil sie ein psychologisches Urbedürfnis befriedigen: Sie führen dem Einzelnen vor Augen, dass auch die Autoritätsperson des Richters als „Halbgott in Schwarz“ nur ein Mensch mit Fehlern und Makeln ist. Tagesform,[134] Vorurteile, Grundeinstellungen und persönliche Sympathien beeinflussen sein Verhalten. Richter urteilen bspw. unterschiedlich „hart“ nach ihrem eigenen, persönlichen Rechtsempfinden. Je nach Region und Gerichtsbezirk unterscheidet sich die Strafzumessungspraxis substanziell: In Norddeutschland und Baden-Württemberg werfen die Strafrichter vergleichsweise eher milde Urteile aus; in (Ober-)Bayern und Südhessen sanktionieren sie tendenziell härter.[135] Sogar zwischen der Rechtsträgerschaft für Gefängnisse und der Höhe der ausgeworfenen Haftstrafe scheint es einen Zusammenhang zu geben. Empirische Untersuchungen aus den USA gelangen zu der Einschätzung: Je mehr Gefängnisse eines Landes in privatwirtschaftlicher Hand sind, desto höher sind die Gefängnisstrafen. Verdoppelt sich die Kapazität der privaten Gefängnisse, erhöht sich die Haftstrafe für den Verurteilten um durchschnittlich 18 Tage.[136] Ökonomen führen dies darauf zurück, dass die Kosten je Insasse in privaten Gefängnissen niedriger sind als in staatlichen und die Gerichte – unbewusst – Rücksicht auf die Finanzkraft ihres Landes und ihre Auslastung nehmen.[137] Aus Sicht der Verurteilten wirken derlei Einflussfaktoren in die gerichtliche Praxis willkürlich und ungerecht hinein: „Lokale Üblichkeit“ oder die Rechtsträgerschaft einer Gefängnisanstalt sind kein sachlicher Differenzierungsgrund (vgl. Art. 3 Abs. 1 GG).[138]

Da klingt der Gedanke verlockend, Inkonsistenzen und Schwächen menschlicher Entscheidungen durch rationale, fehlerfreie, jedenfalls konsistente Entitäten zu bändigen: Algorithmen berechnen ihre Ergebnisse unabhängig von Tagesform, persönlichen Sympathien und Entscheidungsverhalten der Kollegen im Gerichtsbezirk. Die Aussicht auf ein höheres Maß an Stringenz staatlicher Entscheidungen spielt im Idealfall dem Gedanken der Gleichheit vor dem Gesetz und der Rechtssicherheit in die Hände. Ganz nebenbei verheißt ein Algorithmeneinsatz auch, die Verfahrenseffizienz zu steigern, staatliche Entscheidungsressourcen zu entlasten und Verfahren insgesamt zu beschleunigen.

---

* Die Autoren danken besonders Herrn Forschungsreferenten *Jan Mysegades* für seine Mitwirkung.

[134] Vgl. zum – empirisch bislang nur schwach wissenschaftlich unterlegten – Zusammenhang zwischen der Tageszeit des Urteils und der Wahrscheinlichkeit einer Bewährungsstrafe Danziger, Levav und Avnaim-Pesso 2011: 6889 ff.; siehe zur Kritik an dieser Studie Chatziathanasiou 2019: 455 ff.; siehe auch Martini 2019a: 47 f.

[135] Grundies 2018: 297 ff.; ders. 2016: 514 ff.; Kaspar 2018: C 19 ff.

[136] Vgl. Dippel und Poyker 2019: 2, 13 f. Die empirischen Untersuchungen beziehen sich auf Entscheidungen in den USA.

[137] Dippel und Poyker 2019: 17 ff., 25 f.

[138] Dazu auch Deutscher Juristentag e. V. 2018: 20, 26.

7.2 Algorithmen auf dem Vormarsch in die Justiz – reale und denkbare Einsatzfelder

Automatisierte Systeme einzusetzen, um staatliche Entscheidungen zu unterstützen, liegt insbesondere in solchen Verfahren nahe, die einen hohen Grad an Schematisierung und Formalisierung aufweisen, in denen also eine Vielzahl der Fälle einem gleichen oder ähnlichen Prüfraster folgt. Das gilt auf Verwaltungsebene bspw. im Besteuerungsverfahren (ELSTER) oder für Entscheidungen über Gebühren (bspw. für die Abfallbeseitigung) – aber auch bei Massenentscheidungen im privatwirtschaftlichen Rechtsverkehr, etwa für gleich gelagerte Entschädigungsfälle bei Flug- oder Zugverspätungen.

E-Government-Vorreiter Estland experimentiert bereits mit einem System, das kleinere *Zivilrechtsstreitigkeiten* mit einer Schadenssumme bis zu 7000 Euro dem Schlichtungsverfahren einer Künstlichen Intelligenz anvertraut. Die Prozessparteien sollen dort relevante Dokumente in ein System einspeisen, das auf der Grundlage vergleichbarer Fälle zu einem Entscheidungsvorschlag gelangt.[139] Auch Kanada[140] und Großbritannien[141] haben für einfache Verfahren bereits onlinebasierte Schiedsverfahren eingerichtet. Dänemark[142] wickelt einige Zivilstreitigkeiten unterdessen schon über ein Onlineprozessportal ab. Die Bürger sind in unserem nördlichen Nachbarland sogar teilweise dazu verpflichtet, das Onlineportal zu nutzen. In Deutschland nimmt die Freie und Hansestadt Hamburg eine Vorreiterrolle ein: Das „Tor zur Welt" plant ein „Beschleunigtes Onlineverfahren" für bestimmte Massenverfahren mit einem Streitwert von bis zu 2000 Euro.[143] Dahinter verbirgt sich dann letztlich aber lediglich eine Eingabemaske für Onlineklagen. Nach Klageerhebung läuft das Verfahren in den bisherigen analogen Strukturen der Zivilprozessordnung (ZPO) ab.[144]

Neben rein metrischen Entscheidungselementen (wie der Höhe eines Schmerzensgeldes) sind pro futuro einem automatisierten Unterstützungssystem auf der Grundlage von Vergleichsdaten prinzipiell auch Entscheidungspro-

---

[139] Vgl. Niiler 2019.

[140] Die kanadische Provinz *British Columbia* hat eine staatliche Schiedsstelle eingerichtet, die vollständig onlinebasiert operiert. Bei dem „Civil Resolution Tribunal" handelt es sich nicht um ein Gericht, sondern um ein administratives Tribunal („administrative tribunal"), das in das System der öffentlichen Justiz eingebunden ist. Hat eine Partei dort eine Streitigkeit eingereicht, muss die beklagte Partei auf die „Klage" (ähnlich wie im deutschen Mahnverfahren) reagieren. Die Parteien können dann in eine Verhandlungsphase eintreten. Mündliche Verhandlungen finden nicht statt; die Parteien tauschen ihre Standpunkte vielmehr in Textform online aus. Auch Beweismittel lassen sich hochladen. Erzielen die Parteien keine Einigung, trifft das Tribunal als unabhängiger Dritter eine Entscheidung. Seine Entscheidung ist wie ein gerichtliches Urteil vollstreckbar. Eine eingeschränkte Berufung ist möglich. Mehr Informationen unter: https://civilresolutionbc.ca/faq/ (Download 11.11.2019).

[141] Das UK-Justizsystem kennt schon seit einigen Jahrzenten sog. *„Small Claims"-Gerichte*, die speziell für kleinere Bagatellstreitigkeiten zuständig sind; siehe dazu auch https://www.gov.uk/make-court-claim-for-money (Download 11.11.2019).

[142] Vgl. dazu vertiefend Justizministerkonferenz 2019: 75 ff. Das Schiedsverfahren zeichnet sich durch die Besonderheit aus, bereits existierende E-Government-Anwendungen (namentlich e-ID und elektronisches Postfach) eng miteinander zu verzahnen. Es soll die Parteien insbesondere via telefonischer Verhandlung zu einer gütlichen Einigung bewegen.

[143] Siehe zu den Einzelheiten den Abschlussbericht der Länderarbeitsgruppe, Justizministerkonferenz 2019 2019: 78 ff.

[144] Die Justizministerkonferenz 2019 stuft insbesondere einen gut funktionierenden elektronischen Rechtsverkehr als unverzichtbares Element des modernen Zivilprozesses ein. Sie hält es daher für erforderlich, allen potenziellen Verfahrensbeteiligten einfach zugängliche Korridore zu eröffnen, um elektronische Dokumente zu übermitteln und deren Empfang bestätigen zu lassen; vgl. 90. Konferenz der Justizministerinnen und Justizminister, Beschluss zu TOP I. 5.: Optimierung der zivilprozessualen Regelungen zum elektronischen Rechtsverkehr, S. 1, https://www.schleswig-holstein.de/DE/Schwerpunte/JUMIKO2019/Downloads/190605_beschluesse/TOPI_5.pdf?__blob=publicationFile&v=2 (Download 11.11.2019).

gnosen („Mit einer Wahrscheinlichkeit von 80 Prozent wird der Kläger den Prozess verlieren“) und Klassifikationsfragen zugänglich – bspw. als Instrument der Risikoprognose im personenbezogenen Predictive Policing[145] oder in der Strafrechtspflege.[146]

Jenseits der deutschen Grenzen sind Digitalisierung und Automatisierung auch in der Praxis der *Strafjustiz* bereits angekommen: In der Deutschschweiz ist bspw. das Programm „ROS“ (Risikoorientierter Sanktionenvollzug) im Einsatz.[147] Es berechnet das Rückfallrisiko verurteilter Straftäter und steuert auf dieser Grundlage die Bewährungshilfe: Ein „Fall-Screening-Tool“ teilt Verurteilte auf der Grundlage von Daten zur begangenen Tat, zu Vorstrafen sowie Persönlichkeitsmerkmalen binnen 20 Minuten in drei Risikokategorien ein: A (unbedenklich), B (begeht womöglich wieder leichte Straftaten) oder C (begeht womöglich erneut schwere Delikte). Die frühzeitige Kategorisierung einzelner Straftäter soll die Rückfallwahrscheinlichkeit nach dem Strafvollzug senken und diesen landesweit vereinheitlichen.[148]

Die USA haben mit solchen Systemen schon über einen längeren Zeitraum Erfahrungen gesammelt: In verschiedenen Bundesstaaten sind seit einigen Jahren sog. *Predictive-Analytics-Systeme* bei Haftentscheidungen im Einsatz. Das bekannteste und zugleich auch umstrittenste unter ihnen ist die Software *COMPAS*. Das Akronym steht für: *Correctional Offender Management Profiling for Alternative Sanctions*. Auf der Grundlage einer statistischen Analyse von Bestandsdaten berechnet die Software mithilfe lernender Algorithmen[149] die Wahrscheinlichkeit dafür, dass der Beschuldigte rückfällig wird. Für die Einzelfallauswertung zieht das Programm insbesondere polizeiliche Ermittlungsdaten und Informationen aus dem Strafregister sowie die Antworten eines detaillierten Fragebogens[150] heran. Der Risikowert, den die Software auf Grundlage der gesammelten Daten errechnet, soll nicht nur – wie in der Schweiz – die Bewährungshilfe unterstützen. Er bereitet vielmehr drei grundrechtssensible Teilentscheidungen vor: die Anordnung der Untersuchungshaft, die Festsetzung der Haftlänge und die vorzeitige Haftentlassung (Strafrestaussetzung).

Für deutsche Ohren klingt das COMPAS-System befremdlich. Nicht nur hierzulande, sondern auch in den USA stößt es auf Kritik: Amerikanische Datenjournalisten konnten nachweisen, dass der Algorithmus bei nicht weißen ethnischen Minderheiten häufiger als bei Menschen mit weißer Hautfarbe *false positives* – also Rückfallprognosen, mit denen tatsächlich kein Rückfall korrespondiert – auswirft (Angwin et al. 2016). Es liefert auch kaum bessere Entscheidungen als zufällig ausgewählte juristische Laien, die über weniger Informationen verfügen (Dressel und Farid 2018: 1 ff.). Der COMPAS-Hersteller hält dem entgegen, seinem Programm einen validen Fairnessmaßstab

---

[145] Siehe dazu Martini und Nink: Mit der algorithmischen Kristallkugel auf Tätersuche? (Kapitel 6 dieser Studie).
[146] Beispiele, aktuelle Entwicklungen in ganz Europa sowie Leitlinien für den Einsatz automatischer Systeme in der Justiz hat jüngst die (dem Europarat angegliederte) *Europäische Kommission für die Effizienz der Justiz* (European Commission for the Efficiency of Justice, CEPEJ) veröffentlicht (Europarat und Europäische Kommission für die Effizienz der Justiz [CEPEJ] 2018: 4 ff., 14 f.). Mit steigenden technischen Möglichkeiten wachsen auch die Anwendungsfelder: Während Big-Data-Auswertungen in den USA bereits als Beweismittel vor Gericht zum Einsatz kommen, diskutiert unterdessen auch die Fachwelt in Deutschland darüber (dazu mit Blick auf DNA-Analysen Mysegades 2018).
[147] Dazu auch Braun Binder 2019: 471; weiterführend: https://www.rosnet.ch/de-ch/ros-allgemein (Download 11.11.2019).
[148] Eine empirische Überprüfung des Tools liefern Treuthardt und Kröger 2019. Nur etwa 25 Prozent der Straftäter, die mit der höchsten Risikoklasse gelabelt waren, wurden anschließend tatsächlich rückfällig. Für den Einzelnen und dessen Resozialisierung kann sich eine hohe Risikoklasse indes zum Problem auswachsen. Denn die ursprüngliche Bewertung bleibt grundsätzlich über die gesamte Strafdauer – ungeachtet der persönlichen Entwicklung des Inhaftierten – erhalten.
[149] Darunter versteht die Informatik Handlungsvorschriften, die selbstständig Rückschlüsse zu ziehen in der Lage sind und dadurch auf der Grundlage statistischer Zusammenhänge von Vergangenheitsdaten Prognosen für die Zukunft entwickeln.
[150] Ein Originalfragebogen ist online einsehbar unter https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html (Download 11.11.2019).

zugrunde gelegt zu haben, der den Risikowert gerade unabhängig von der Ethnie des Angeklagten auswirft, sodass keine Diskriminierung vorliege (Dieterich, Mendoza und Brennan 2016: 3 ff., insbesondere 32).

Tatsächlich existieren für eine Prognosesoftware unterschiedliche statistische Fairnessmaßstäbe, die nicht vollständig miteinander harmonieren: Wann ein Algorithmus „fair" ist und wann nicht, ist stets auch eine Frage der Perspektive. Intrikat ist die Suche nach dem besten Maßstab insbesondere dann, wenn Gruppen gleichbehandelt werden sollen, die in der sozialen Realität unterschiedliches Verhalten (bspw. ein unterschiedliches durchschnittliches Maß der Straffälligkeit) an den Tag legen (Martini 2019a: 55 ff., 243 ff.).[151] Er steht dann vor der Herausforderung, wesensmäßig Ungleiches gleichzubehandeln. Algorithmische Analyseverfahren dürfen die normativen Aussagen, welche die Rechtsordnung für den Entscheidungsprozess der Justiz trifft, zugleich aber nicht unterwandern. Sie dürfen keine Merkmale berücksichtigen, die auch ein menschlicher Entscheider nicht einbeziehen dürfte.

7.3 Verfassungsrechtliche Vorgaben für algorithmenbasierte Entscheidungen in der (Straf-)Justiz

Das *Common Law*, das vor allem englischsprachige Staaten praktizieren, ähnelt im Grundsatz der Logik, der algorithmenbasierte Systeme folgen (Ashley 2017: 73 ff.). Sein korrelativer Rechtsfindungsprozess baut auf der Präjudizienwirkung vergangener Rechtsprechung („stare decisis"-Regel) auf. Dazu operiert es mit Analogien, die aus gemeinsamen Mustern in Fallkonstellationen wertende Schlüsse ziehen. Diese Mustererkennung ist das zentrale Kompetenzrevier algorithmischer Analyse: Ihr Wesenskern besteht darin, auf der Basis von Programmiervorgaben aus Eingabedaten konkrete Handlungsfolgen für den Einzelfall abzuleiten. Das fallorientierte *Common Law* ist daher für eine datenbasierte Entscheidungsunterstützung strukturell geradezu prädestiniert.

Das deutsche Rechtssystem fußt demgegenüber auf dem Prinzip, konkrete Rechtserkenntnisse ausschließlich aus abstrakt-generellen, aber im Grundsatz wertungsoffenen Vorgaben des Parlaments abzuleiten. Auch aus diesem Grund zieht die deutsche Rechtsordnung, insbesondere das Verfassungsrecht, dem Einsatz algorithmenbasierter Systeme in der Strafjustiz enge Grenzen.[152]

7.3.1 Der Roboter als Robenträger – vollautomatisierte Entscheidungen als verfassungsrechtliches Tabu

7.3.1.1 De constitutione lata

Das Grundgesetz geht in Art. 92 und 97 GG von unabhängigen und selbstständig verantwortlichen Richtern aus, die allein dem Gesetz und Recht unterworfen sind. Die „Richter", denen die Verfassung die Rechtsprechung „anvertraut" (Art. 92 Hs. 1 GG), versteht sie als besonders legitimierte und befähigte *menschliche* Entscheider. Das illustriert auch die Wortwahl des Art. 97 Abs. 2 GG: Er spricht – nicht zufällig – insbesondere vom „Willen", der

[151] Es kommt darauf an, auf welchen Prognosewert ein Klassifikationsalgorithmus hin *optimiert* werden soll (Sensitivität versus Spezifität). Technisch stehen beide Optimierungsstrategien gleichberechtigt nebeneinander. Intuitive Fairnessmaßstäbe, wie etwa „gleiche Auswirkungen auf alle Gruppen" oder „Nichtberücksichtigung sensitiver Merkmale wie Ethnie oder Geschlecht", springen daher zu kurz; siehe dazu etwa Corbett-Davies et al. 2016: 797 ff.; Kleinberg et al. 2018: 237 ff.; Zweig und Krafft 2018: 211 ff.

[152] Da justizielle Entscheidungs- bzw. Entscheidungsunterstützungssysteme mit personenbezogenen Daten operieren müssten, hält auch das (unionsrechtlich überformte) Datenschutzrecht normative Vorgaben bereit. In der Strafrechtspflege sind sowohl die DS-GVO als auch die zugleich erlassene Richtlinie 2016/680 (EU) für Polizei und Justiz zu beachten. Neben dem grundsätzlichen Verbot vollständig automatisierter Einzelentscheidungen (vgl. insbesondere Art. 22 DS-GVO) stellt das Unionsrecht vor allem die Verarbeitung besonders sensibler Daten, zu denen auch strafrechtliche Informationen zählen (vgl. etwa Art. 9 und 10 DS-GVO), vor hohe normative Hürden.

„Amtszeit“ bzw. „Lebenszeit“ und dem „Ruhestand“ des Richters. Das Grundgesetz verschließt sich damit algorithmischen Systemen als Letztentscheidungsinstanz – dies nicht so sehr deshalb, weil es aus einer anderen Zeit stammt, sondern als Teil eines festen normativen Bekenntnisses: Es hat bewusst den Menschen als Entscheider vor Augen. Denn Rechtsprechung erschöpft sich nicht darin, schematische Lösungsraster abzuspulen. Nur ein Mensch kann nach der Vorstellung der Mütter und Väter des Grundgesetzes die Gewähr dafür bieten, das Vorbringen der Prozessbeteiligten in all seinen Facetten zu hören, zu würdigen und in der Entscheidung zu berücksichtigen. Wer Adressat eines gerichtlichen Urteilsspruchs ist, muss insbesondere darauf vertrauen dürfen, dass der Richter den Sachverhalt in seinen gesamten lebensweltlichen Auswirkungen erfassen kann.[153] Das ist auch der Kerngedanke des Anspruchs auf rechtliches Gehör (Art. 103 Abs. 1 GG).[154] So ist es nur folgerichtig, dass kraft § 9 Nr. 4 Deutsches Richtergesetz (DRiG) in das Richterverhältnis nur berufen werden kann, wer über die *erforderliche soziale Kompetenz* verfügt.

Das Grundgesetz geht im Ergebnis implizit davon aus, dass *eine natürliche Person* sich des Rechtsstreits annimmt. Einen Richter-Automaten lässt es nicht zu: „Gesetzlicher Richter“ im Sinne des Art. 101 Abs. 1 S. 2 GG ist nur eine Person, die – aufgrund ihrer Befähigung zur Empathie – auch die sozialen und persönlichen Folgen für den Betroffenen in die Entscheidungsfindung einfließen lassen kann. Ihre streitentscheidende Tätigkeit erfordert stets eine Einzelfallbetrachtung aller – auch unvorhergesehener – Umstände (Martini und Nink 2018: 1136; so im Ergebnis auch Enders 2018: 723).

7.3.1.2 De constitutione ferenda?

Die Verfassung ist keine Heilige Schrift. Ebenso wie andere Rechtsregeln lassen sich auch ihre Rechtsgebote (mit Ausnahme der Prinzipien, welche die sog. *Ewigkeitsgarantie* des Art. 79 Abs. 3 GG absichert) pro futuro ändern. Zu den ehrgeizigen Zielen der Rechtsinformatik gehört es jedenfalls, Entscheidungssoftware zu befähigen, wie ein Richter auch solche Sachverhaltskonstellationen rechtlich zu beurteilen, die Programmierer nicht antizipiert bzw. bereits im Programmcode der Software einer juristischen Entscheidung zugeführt haben.

Text Mining und *Natural Language Processing* etwa erzielen derweil bemerkenswerte Fortschritte. Nicht nur Alltagsanwendungen, sondern auch Legal-Tech-Programme machen sich die neuen Möglichkeiten in der Rechtsberatung in wachsendem Umfang zunutze. So hat bspw. eine Künstliche Intelligenz der Plattform *LawGeex* 20 US-Anwälte bei der Analyse von Vertragsklauseln sowohl in der Genauigkeit als auch der Schnelligkeit klar hinter sich gelassen: Die Anwälte benötigten im Durchschnitt 92 Minuten und erkannten Fehler lediglich zu 85 Prozent; die Maschine benötigte 26 Sekunden mit einer Genauigkeit von 94 Prozent (Erxeben 2019).

Den menschlichen Akt der Rechts*anwendung* exakt nachzubilden, können die Softwaresysteme jedoch nicht für sich reklamieren: Sie sind (jedenfalls noch) nicht perfekt darin, natürliche Sprache fehlerfrei zu erfassen und in ihren Sinnzusammenhängen zu verstehen (vgl. etwa Herold 2018: 460 f.). Die Bemühungen der Automatisierung bescheiden sich in der Folge gegenwärtig damit, die Begründungen juristischer Entscheidungen (z. B. anhand Argumentationsschemata) möglichst ausdifferenziert zu klassifizieren, d. h. in Formalisierungsschemata einzuteilen. Eine Software kann dann im Idealfall einen ähnlich gelagerten Sachverhalt, der in dasselbe Logikschema gefasst ist, mit den eingespeicherten Entscheidungsbegründungen abgleichen, also Gemeinsamkeiten und Unterschiede feststellen, und auf Grundlage dieses Vergleichs eine – an den Besonderheiten des Einzelfalls ausgerichtete – Entscheidung treffen.

---

[153] Für Freiheitsentziehungen greift zudem der besondere Schutz des Art. 104 GG: Sie zu verhängen, bleibt grundsätzlich einem Richter vorbehalten und liegt in dessen voller Verantwortung.

[154] Das grundrechtsgleiche Recht (vgl. § 93 Abs. 1 Nr. 4a BVerfGG) folgt im Grundsatz der römisch-rechtlichen Rechtsregel „*audiatur et altera pars“* („Gehört werde auch die andere Seite“). Es verbürgt Beteiligten bzw. streitenden Parteien vor Gericht einen Anspruch darauf, dass ihre Aussagen nicht nur gehört, sondern auch inhaltlich gewürdigt und bei der Urteilsfindung gegebenenfalls berücksichtigt werden; vgl. dazu etwa BVerfGE 9, 89 (95); 84, 188 (190); 86, 133 (144 ff.).

Juristische Entscheidungssysteme können bislang aber weder Sachverhalte beurteilen, die sich zu weit von den jeweiligen Vergleichsfällen entfernen, noch ist eine Maschine (jedenfalls derzeit) fähig, rechtsdogmatische Prüfungsansätze selbst zu entwickeln. Das illustrieren auch die wenigen experimentellen Programme, die Entscheidungen prognostizieren. Ihnen gelingt es nur in sehr eng begrenzten Anwendungsbereichen, solche juristischen Entscheidungen zu automatisieren, die es erfordern, Rechtsfragen argumentativ zu beantworten.[155] Die gegenwärtig auf dem (deutschen) Markt erhältlichen Programme sind daher vor allem darauf angelegt, die Suchfunktion für die Rechtsprechung zu verbessern, Dokumente zu ordnen und zu visualisieren oder gleichartige Verträge vergleichen zu können, um die Zeit zu reduzieren, die ein Anwalt dafür benötigt.[156] Die Einsparpotenziale für Wirtschaftskanzleien, die etwa für Due-Diligence-Prüfungen bisher Horden an Referendaren und hoch bezahlten Anwälten einsetzen, um relevante Informationen aus den Dokumenten zu filtern, sind zwar immens. In die juristische, insbesondere richterliche Kerntätigkeit dringen sie aber (noch) nicht (mit hinreichender Qualität) vor.

Das hat seinen guten Grund: Juristische Analyse ist im Wesentlichen Sprachanalyse. Ihre Kunst verlangt mehr als eine klare Entscheidungssteuerung durch exakten Code. Sie setzt vielmehr insbesondere eine saubere lebensweltlich-argumentative Durchdringung des Einzelfalls und seines normativen Rahmens, ein wertgeprägtes, normatives Urteilsvermögen (das sog. *Judiz*) sowie die Kommunikation mit den Prozessbeteiligten voraus. Gerade bei der Priorisierung scheinbar gleichartiger Texte,[157] dem Lesen „zwischen den Zeilen“ sowie der Aufgabe, gesamtgesellschaftliche Folgen zu berücksichtigen, stoßen Maschinen jedoch an ihre Grenzen (Martini 2019a: 58 ff.). Einzelfälle zu schematisieren und sie samt und sonders in ein vorgefertigtes Prüfraster zu pressen, wird den Anforderungen des Rechts an Einzelfallgerechtigkeit nicht gerecht (Martini und Nink 2018: 1135 ff.). Diese lässt sich schon begrifflich nicht automatisieren. Vor allem Wertentscheidungen oder Entscheidungen mit Beurteilungs- oder Ermessensspielraum vollständig zu automatisieren, wird Maschinen auch auf absehbare Zeit nicht gelingen. *Machine learning*[158] kann zwar Korrelationen innerhalb von Datenbeständen erkennen, die Menschen bei einer händischen Auswertung verborgen blieben. Ob zwischen korrelierenden Faktoren innerhalb eines Datensatzes aber auch eine Kausalität besteht, vermögen algorithmische Systeme jedoch regelmäßig nicht zu erkennen. Von den vielgestaltigen Fähigkeiten des menschlichen Gehirns sind sie noch weit entfernt. Nicht zuletzt aufgrund ihrer eingeschränkten Sensorik, insbesondere der Abhängigkeit vom Dateninput, fehlt es Maschinen an einer vollständigen Wirklichkeitswahrnehmung; ihnen fehlt der *common sense*. Situationen in ihren lebensweltlichen Gesamtkontext fehlerfrei einzuordnen, zu verstehen und zu bewerten, gelingt ihnen daher nicht.

Da es Softwaresystemen nicht möglich ist, die richterliche *Entscheidungsfindung* bruchfrei abzubilden, ist einer vollständigen Automatisierung der Rechtsprechung im Ergebnis der Weg auch de lege ferenda versperrt. Die Demarkationslinien des Grundgesetzes und des Deutschen Richtergesetzes bilden die rein tatsächlichen, technischen Hürden, die eine Maschine nicht ohne Weiteres überspringen kann, daher treffend ab. Der Einsatzradius algorithmischer Systeme wird sich auch in Zukunft darauf beschränken, die richterliche Tätigkeit zu unterstützen.

7.3.2 Entscheidungsunterstützungssysteme und richterliche Unabhängigkeit

Nicht allein dem Versuch, Richter durch Algorithmen zu *ersetzen*, setzt die Verfassung Grenzen. Sie limitiert auch den Handlungsspielraum, Entscheidungs*unterstützungs*systeme in der Justiz einzusetzen.

---

[155] Vgl. etwa das „Value Judgment Argumentative Prediction“-Programm, das nur Entscheidungen im Bereich der Veruntreuung von Geschäftsgeheimnissen vorhersagen kann; Grabmair 2016: iv.

[156] Vgl. etwa die Übersicht der auf dem deutschen Markt erhältlichen Produkte bei Hartung und Zobel 2019.

[157] Während ein Mensch schon auf den ersten Blick den Unterschied zwischen einem online veröffentlichten Urteil des BGH oder einem anonym verfassten Blog-Beitrag erkennt, behandelt eine Software diese (ohne dazugehörige Regel oder Lernerfahrung) zunächst als gleichartig. Sie gewichtet beide Texte daher a priori im Grundsatz gleich; vgl. auch Herold 2018: 461.

[158] Als Teilbereich dessen, was Wissenschaft und Medien derzeit unter Künstlicher Intelligenz verstehen, befähigt maschinelles Lernen informationstechnische Systeme, auf Basis vorhandener Datenbestände und leistungsfähiger Algorithmen Gesetzmäßigkeiten sowie Muster zu erkennen. Die Systeme können sodann Aufgaben teilweise eigenständig lösen; siehe dazu bspw. Ashley 2017: 108 f.; Ertel 2016: 3.

Denkbar sind diese technisch nicht nur als intelligente Strukturierungstools, die den jeweiligen Verfahrensstoff aufbereiten, z. B. relevante Orte, Zeitpunkte und Personen zuordnen oder widerstreitende Aussagen von Zeugen und Argumentationen visuell gegenüberstellen. Vorstellbar sind auch juristische Vorauswertungen, die Rechtsdatenbanken auf Vergleichsfälle durchforsten und wertungsrelevante Sachverhaltsaspekte zusammenstellen, sowie konkrete Entscheidungsvorschläge nach dem Muster des Systems *COMPAS*.

7.3.2.1 Bindungswirkung?

Wie jedes Handeln, das dem Staat zurechenbar ist, unterfällt auch der Einsatz entscheidungsunterstützender Systeme in der Justiz dem Rechtsstaatsgebot aus Art. 20 Abs. 3 GG: Algorithmen, die Teil einer staatlichen Entscheidung sind, sind ebenso wie der Richter selbst an das Gesetz gebunden. Sie müssen sicherstellen, dass das System den Vorgaben der Rechtsordnung folgt.

Ebenso wenig dürfen sie die richterliche Unabhängigkeit (Art. 97 Abs. 1 GG) antasten. Sie dürfen daher für den Richter jedenfalls keine unzulässige faktische oder rechtliche Bindungswirkung entfalten. Der Richter muss immer die Möglichkeit haben, sich über einen Vorschlag hinwegzusetzen, den ihm eine entscheidungsunterstützende Software unterbreitet. Ein Gesetz, das Richter zwingt, algorithmisch generierte Entscheidungsvorschläge zu übernehmen, wäre verfassungswidrig.

Wo die Grenzlinie zwischen zulässigen dienstlichen Vorgaben, z. B. des Gerichtspräsidenten, und der sachlichen Unabhängigkeit des einzelnen Richters verläuft, haben obergerichtliche Entscheidungen bereits in vielen Verfahren auszuleuchten versucht. Der BGH hat bspw. entschieden, dass ein Richter sich nicht auf seine Unabhängigkeit berufen kann, um nach Einführung des elektronischen Handelsregisters statt am Computer nach wie vor mit Papierausdrucken zu arbeiten.[159] Umgekehrt verletzt es die richterliche Unabhängigkeit, wenn die Justizverwaltung Richter bspw. dazu verpflichten will, in den Entscheidungsgründen eines Urteils ausschließlich diejenigen vorgegebenen Textbausteine zu verwenden, welche die Software anbietet.[160]

Selbst wenn von einem algorithmischen System keine *rechtliche* Bindungswirkung ausgeht: Auch in rein *tatsächlicher* Hinsicht birgt jeglicher Einsatz automatisierter Entscheidungsunterstützungssysteme ein spezifisches rechtsstaatliches Risiko: Mit ihm geht die Gefahr einher, dass sich Menschen zu stark auf algorithmische Ergebnisse verlassen und in der Folge gegenläufige Informationen ignorieren oder ausblenden. Denn Menschen neigen dazu, Automatisierungssystemen Objektivität und Korrektheit in einem Maße zuzuschreiben, das diesen tatsächlich gar nicht innewohnt. Dieses Phänomen ist als *Automation Bias* (insbesondere im Bereich der Medizin sowie der Luft- und Raumfahrt) bekannt (vgl. etwa Goddard, Roudsari und Wyatt 2012: 121 ff.; Skitka, Mosier und Burdick 2000: 701 ff.). Einzelne Studien konnten den Effekt aber auch für die Arbeit an juristischen Fällen nachweisen (etwa Dijkstra 2001: 119 ff.). Dass empirische Forschungen auf eine solche faktische Bindungswirkung technischer Unterstützungsmittel hindeuten, überrascht nicht: Digitale Agenten sollen ihrem Wesen nach nicht nur die Entscheidungsqualität steigern, sondern auch den Justizapparat effizienter gestalten. Um diesen Nutzen zu erzielen, müssen sich Richter ein Stück weit auf die Systeme verlassen (können).

Im Extremfall kann der *Automation Bias* im justiziellen Einsatz jedoch darin münden, dass der Richter schwerwiegende strafrechtliche Entscheidungen gleichsam „durchwinkt“ und im Ergebnis einem phlegmatischen Qualitätskontrolleur am Fließband einer Fabrik gleicht. Hinzu kann sich ein „Pontius-Pilatus-Effekt“ gesellen: Das

---

[159] BGH, Urteil vom 21.10.2010, NJOZ 2011, 1461 ff.

[160] Pitschas 1998: 101; Voss 1998: 386 f. Daran knüpft sich zugleich auch die Frage, inwieweit der Richter *verpflichtet* werden kann, Entscheidungsunterstützungssysteme – vergleichbar einem Textverarbeitungsprogramm – als Hilfsmittel einzusetzen.

Entscheidungsunterstützungssystem vermittelt dem Richter einen Anreiz, unter Verweis auf die vordergründig unbestechliche Stringenz des automatisierten Vorschlags, gegenüber dem Angeklagten und der Öffentlichkeit „seine Hände in Unschuld zu waschen“ und dessen Prämissen nicht mehr infrage zu stellen.[161]

Die richterliche Amtspflicht verlangt dem Richter aber exakt das Gegenteil ab: Er ist *verpflichtet*, die Ergebnisse einer algorithmenbasierten Datenanalyse nicht als unumstößliche Feststellung in seine Entscheidungsfindung einfließen zu lassen. Vielmehr hat er sie kritisch zu prüfen. Er selbst zeichnet für den gesamten Entscheidungsprozess verantwortlich und muss die Entscheidung daher auch eigenverantwortlich treffen – nicht eine gleichsam im Inneren von Platinen verborgene Abfolge aus Einsen und Nullen. Einen Entscheidungsvorschlag unkritisch „abzunicken“, genügt mithin nicht den Vorgaben, welche die Verfassung an die richterliche Entscheidung stellt (Art. 92 Hs. 1, Art. 97 Abs. 1 GG).

7.3.2.2 Schutzmechanismen

Sollen entscheidungsunterstützende Systeme in der Rechtsprechung Einsatz finden, müssen sie die Friktionen, die ihr Einsatz für die richterliche Unabhängigkeit (Art. 97 Abs. 1 GG) und Verantwortungswahrnehmung auslösen kann, durch geeignete begleitende Maßnahmen antizipieren und auf ein vertretbares Niveau begrenzen. Mögliche Anknüpfungspunkte sind dabei zum einen die Richterschaft, zum anderen die Konzeption der Softwareanwendung selbst.

- **Nachvollziehbarkeit des Systems und seiner Entscheidungsvorschläge sowie möglicher Fehlerquellen**
  Damit Richter Entscheidungsunterstützungssysteme verantwortungsgerecht einsetzen können, müssen sie beurteilen können, wie deren Vorschläge zustande kommen. Ist es ihnen nicht möglich, sich bei Bedarf kritisch mit dem Entscheidungsvorschlag auseinanderzusetzen, sehen sie sich faktisch vor die Wahl gestellt, dem algorithmischen Ergebnis entweder blind zu vertrauen oder ihre Entscheidung ohne Rücksicht auf das System zu treffen.[162]

  Zugleich gilt auch wie sonst beim Einsatz technischer Systeme: Nicht jeder, der ein Auto fährt, muss die fachlichen Spezifika der Hydraulik oder der Einspritztechnik im Maschinenraum verstehen, um das Fahrzeug zu nutzen; auch wenn ein Richter bspw. einen Gerichtskostenrechner einsetzt, muss er keine Kenntnisse über die elektronischen Prozesse der einzelnen Bauelemente des Programms haben – genauso wenig wie er jede Einzelheit eines Recherchetools verstehen oder seinen genauen Quellcode kennen müsste. Entsprechend muss auch ein Richter kein Informatikstudium absolviert haben oder über tiefgehende technische Kenntnisse verfügen, um für seine Urteile einen Entscheidungsassistenten verwenden zu dürfen.

  Dass sich der Richter kritisch mit den Ergebnissen des Entscheidungsunterstützungssystems auseinandersetzen kann, ist allerdings nur gewährleistet, wenn er in der Lage ist, die wesentlichen Schritte des

---

[161] Ein Beispiel für die Versuchung, selbst erratische Ergebnisse eines Softwaresystems zu verteidigen, liefert ein US-amerikanischer Fall: Das *Department of Health* im US-Bundesstaat Idaho hatte mittels einer neuen Software die staatlichen Zuschüsse für Schwerstkranke neu berechnet. Der Computer halbierte kurzerhand die Zuschüsse zu ärztlichen Leistungen. Auf Anfragen, wie das denn sein könne, verwies die Behörde stets auf die Software und erklärte das Programm zum Geschäftsgeheimnis. Erst Jahre später förderte ein gerichtliches Verfahren die Ursache an das Tageslicht: Die der Berechnung zugrunde liegende Excel-Tabelle litt an einem einfachen Fehler.

[162] So auch der Beschluss zu TOP I. 11. der 90. Konferenz der Justizministerinnen und Justizminister, S. 1, abrufbar unter https://www.justiz.bayern.de/media/pdf/jumiko2019/fruehjahr2019/i-11_legal_tech.pdf (Download 11.11.2019): Der „Einsatz von digitalen Anwendungen in der gerichtlichen Praxis [ist] nur dann unbedenklich […], soweit es sich hierbei lediglich um die transparente und dadurch nachvollziehbare bloße Unterstützung der richterlichen Entscheidungsfindung handelt“.

algorithmenbasierten Entscheidungsprozesses gedanklich in Ansätzen zu rekonstruieren, welche die Entscheidung tragen. Er muss jedenfalls bei sensiblen Entscheidungen die Kriterien nachvollziehen können, nach denen ein algorithmisches System Prognosen für den justiziellen Einsatz trifft. Sowohl die grundlegende Methodik als auch die potenziellen Fehlerquellen solcher Systeme muss der Richter einschätzen und auf seinen Fall herunterbrechen können. Dazu muss er auch über die Fehlerquoten des Systems informiert sein. Dies ist Teil der Grundanforderungen an ein rechtsstaatliches Verfahren.[163]

Insoweit gilt im Kern nichts anderes als sonst, wenn der Richter als Teil der Beweiswürdigung technische Sachverhalte zu beurteilen hat, etwa Sachverständigengutachten einholt oder Beschuldigte wegen erhöhter Blutalkoholwerte verurteilt. Anders als in diesen Fällen können typischerweise aber weder das Gericht noch die Parteien ohne Weiteres einen menschlichen Sachverständigen konsultieren und zu seiner Methodik befragen. Die Entwickler des Entscheidungsunterstützungsprogramms stehen dem Richter nicht in jedem Einzelverfahren für Fragen zur Verfügung. Daher muss das System selbst dem Entscheider alle notwendigen Informationen zur Verfügung stellen. Soll der Richter die Wertungsentscheidungen valide treffen, die er seinem Urteil zugrunde legt, muss er im Grundsatz wissen, welche Kriterien der Algorithmus auswertet, welche Punkte unberücksichtigt bleiben und an welchen Punkten eine erhöhte Fehleranfälligkeit besteht. Er muss im Ernstfall Schritt für Schritt Einblick in den Entscheidungsmechanismus nehmen können, um transparent nachvollziehen zu können, warum das System eine bestimmte Entscheidung vorschlägt.

- **Begründung des Computerentscheidungsvorschlags**
  Nachvollziehbarkeit lässt sich zuvorderst durch die Begründung des Entscheidungsvorschlags herstellen, den der Algorithmus getroffen hat (vgl. auch Martini 2019a: 181 ff., 189 ff.). Das Entscheidungsunterstützungssystem sollte daher so konzipiert werden, dass es das Vertrauen in seine Leistungsfähigkeit ein Stück weit selbst infrage stellt. Es sollte also eine Einschätzung abgeben, wie hoch die statistische Sicherheit ist, die seinem Entscheidungsergebnis zugrunde liegt. Ein rechtsstaatlich vorbildliches System weist auf Mängel in der Datengrundlage hin und skizziert deren Auswirkungen auf das Entscheidungsergebnis. Das System sollte insbesondere Fehlerquellen (samt deren Wahrscheinlichkeit) und Risiken, die ihm inhärent sind, hinreichend klar ausweisen und den Entscheider ggf. zur ergänzenden Prüfung auffordern. Nur dann ist es dem Richter möglich, den algorithmischen Vorschlag auf seine Rechtmäßigkeit und Tauglichkeit hin gegenzuprüfen.

- **Begründungspflicht des Richters?**
  Wer Richtern ein Mindestmaß an methodischer Fachkenntnis im Umgang mit den Tücken und Spezifika des Entscheidungsassistenten vermittelt und abverlangt, legt die Grundlagen für eine sachgerechte Beweiswürdigung. Um die Gefahr eines *Automation Bias* zu verringern, kann es auch geboten sein, nicht nur dem *Assistenzsystem*, sondern auch *Richtern* – jedenfalls in spezifischen, sensiblen Entscheidungskontexten mit hoher Ausstrahlungswirkung auf Grundrechte – die Pflicht aufzuerlegen, ihre Entscheidung, das Ergebnis der Entscheidungsunterstützungssoftware zu übernehmen, zu begründen. Die Begründung sollte sich insbesondere darauf richten, ob Anhaltspunkte dafür bestehen, dass einzelne Aspekte des individuellen Sachverhalts in dem algorithmenbasierten Entscheidungsprozess womöglich unberücksichtigt geblieben sein könnten. Die richterliche Erläuterung sollte die Umstände benennen bzw. ergänzen, die das System (womöglich) nicht einbezogen hat bzw. nicht einbeziehen konnte, und aufzeigen, inwieweit der Entscheidungsvorschlag des Systems in diesem Lichte tauglich ist. Soweit konkrete Anhaltspunkte für Fehler bestehen, muss sich der Richter von der Zuverlässigkeit der Erhebung überzeugen.[164] Auf diese Weise lässt sich am ehesten der Spagat zwischen dem augenscheinlichen Widerspruch

[163] In diesem Sinne auch SaarlVerfGH, Urteil vom 5.7.2019 – Lv 7/17 – III. 1, NJW 2019, 2456 (2458, Rn. 45 ff. m. w. N.).
[164] Vgl. auch BGHSt 39, 291 (300 f.).

bewältigen, Richtern einerseits entscheidungsunterstützende Systeme an die Hand zu geben, deren technische Grenzen andererseits zum Teil unklar bleiben.

- **Zulassungsverfahren für die Anwendung in der gerichtlichen Praxis**
  Setzt der Richter Entscheidungsunterstützungssysteme ein, muss er sich – ähnlich wie bspw. bei Geschwindigkeitsmessgeräten – auf die basale technische Richtigkeit der Funktionsweise des Entscheidungsassistenten im Grundsatz verlassen dürfen, soweit Verfahrensbeteiligte keine substantiierten Einwände gegen ihre Validität vorbringen.[165] Das technische System sollte auch deshalb für seinen Einsatz im gerichtlichen Verfahren Prüfmechanismen durchlaufen, die sicherstellen, dass seine Aussagekraft valide ist. Im Idealfall durchleuchtet ein hoheitliches Zulassungsverfahren die Eignung eines Systems, valide Ergebnisse für eine Entscheidungsunterstützung zu liefern, auf Herz und Nieren. Solche Verfahren sind keineswegs vollständig neu. So nimmt die Physikalisch-Technische-Bundesanstalt (PTB) z. B. für Geschwindigkeitsmessgeräte eine obligatorische (vorherige) Bauartzulassung bzw. (seit 2015) eine Baumusterprüfbescheinigung vor.[166] Der Prüfmechanismus soll insbesondere sicherstellen, dass das System den Vorgaben gehorcht, welche die demokratische Ordnung an es stellt: Sie baut auf dem Gedanken auf, die Legitimationskette vom Volk bis in die letzten Verästelungen staatlichen Handelns sicherzustellen. Diesen grundlegenden Anforderungen müssen dann auch Algorithmen gerecht werden, die in der Justiz zum Einsatz kommen.

7.3.3 Fair Trial und Waffengleichheit (Art. 20 Abs. 3 GG i. V. m. Art. 6 Abs. 1 EMRK)

7.3.3.1 Diskriminierungsrisiken

Nicht ohne Weiteres gesichert ist die demokratische Legitimationszurechnung bei dynamischen lernfähigen Systemen, insbesondere neuronalen Netzen**.** Ihr Verhalten ist ex ante nur schwer prognostizierbar. Es kann sich von demokratischen Entscheidungsvorgaben entkoppeln.

Lernfähige Entscheidungsunterstützungssysteme sind insbesondere diskriminierungsanfällig. Denn datenbasierte Lernverfahren sind darauf abgerichtet, die soziale Realität, die ihnen ihre Trainingsdaten vermitteln, zu reproduzieren. Dass diese soziale Realität diskriminierend sein kann oder sozialpolitischen Bestrebungen bzw. normativen Zielvorstellungen zuwiderläuft, verschließt sich ihrem Erkenntnishorizont grundsätzlich.[167] Sie suchen schonungslos nach Korrelationen, die Aussagen über die erwünschten Erfolgsvariablen vermitteln. Dadurch spiegeln sie auch Ungleichbehandlungen der sozialen Realität, die ihrer Datengrundlage erwachsen, in ihren Entscheidungsvorschlägen.

---

[165] Vgl. auch zum sog. *standardisierten Messverfahren*, das der BGH für Geschwindigkeitsmessungen etc. entwickelt hat: Soweit die Voraussetzungen der Messung und die Verarbeitung ihrer Ergebnisse so gestaltet sind, dass die Messungen unter denselben oder gleichen Bedingungen nach wissenschaftlicher Erkenntnis reproduzierbar sind, sie also bei gleichen Geschehensabläufen zu gleichen Resultaten führen, dürfen die Gerichte die Ergebnisse dieser Verfahren nach Auffassung des BGH ihren Entscheidungen (vorbehaltlich substanziierter Einwände) ohne nähere Darlegung ihrer Voraussetzungen und ihrer Richtigkeit zugrunde legen. Siehe BGHSt 39, 291 (297); 43, 277 (277 ff.)

[166] Vgl. §§ 6, 7, 46 des Gesetzes über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz; MessEG) i. V. m. der entsprechenden Verordnung (MessEV) vom 11.12.2014, BGBl. I, 2010. Dazu bspw. Brück 2019: 393. Einen erfolgreichen Abschluss des Zulassungsverfahrens stuft die Rechtsprechung als antizipiertes Sachverständigengutachten ein; vgl. etwa OLG Frankfurt, Beschluss vom 4.12.2014 – 2 Ss OWi 1041/14 – juris, Rn. 15 f.; OLG Bamberg, Beschluss vom 22.10.2015 – 2 Ss OWi 641/15 – juris, Rn. 14 f.

[167] Zu den Diskriminierungsgefahren algorithmengestützter Entscheidungsfindung siehe auch bspw. Martini 2019a: 47 ff., Orwat 2019: 24 ff.

Algorithmen finden Korrelationen selbst dann, wenn sie für die primären Merkmale kraft verfassungsrechtlicher Diskriminierungsverbote blind gestellt sind bzw. sein sollten – etwa vermittelt über sekundäre Merkmale wie Wohnort oder sozioökonomischer Status, sog. *Proxy-Variablen* – und knüpfen hieran unversehens an (Martini 2019a: 239 ff.). Verfahren maschinellen Lernens können dadurch unzulässige Merkmale – wie die diskriminierungssensiblen Merkmale Geschlecht, Abstammung, Rasse, Sprache, Glauben oder religiöse oder politische Anschauungen des Art. 3 Abs. 3 GG – (zumindest mittelbar) in die Entscheidung hineintragen.

Mitunter erkennen sie auch Scheinrelationen: Ein Algorithmus ordnet einem Namensträger eine erhöhte Rückfallgefahr im Zweifel auch dann zu, wenn es lediglich der Namensvetter oder ein sonstiger Dritter ist, der als Teil eines gemeinsamen Gruppenkollektivs zufällig ähnliche (in concreto aber nicht entscheidungsrelevante) Merkmale wie der rückfällige Täter trägt. Ähnlich wird ein Algorithmus, der einen statistischen (wenn auch nicht realiter kausalen) Zusammenhang zwischen der Religionszugehörigkeit und der Rückfallgefahr erkennt, diese Erkenntnis seinen weiteren Entscheidungen zugrunde legen.

Gerade bei strafrechtlichen Entscheidungen können solche Fehleinschätzungen fatale Folgen für den Einzelnen, den Zusammenhalt der Gesellschaft und den sozialen Frieden zeitigen: Die Systeme laufen Gefahr, den (womöglich überholten) *Ist-* zu einem *Soll*zustand zu verklären – und dadurch existierende Alltagsdiskriminierung (z. B. zwischen Männern und Frauen oder zwischen Menschen unterschiedlicher Herkunft), die auch das Produkt gesellschaftlicher Entwicklung sind, zu perpetuieren.

Die Prognosekraft datenbasierter (lernfähiger) Systeme hängt daher entscheidend nicht nur von der Qualität ihrer Entscheidungsfindung, sondern vor allem auch von einer qualitativ ausreichend guten Datenbasis ab. Des Übels Wurzel liegt dann nicht im Algorithmus, sondern im System: Operiert dieses mit fehlerhaften, veralteten oder unpassenden Daten, produziert es unweigerlich fehlerhafte, veraltete oder unpassenden Ergebnisse. Im schlimmsten Fall laufen Systeme, in die sich rechtsstaatlich nicht verantwortbare Fehler einschleichen, Gefahr, gesellschaftliche Schieflagen zu verfestigen und eine aktive Resozialisierungspolitik zu erschweren. Sie müssen daher hinreichende Schutzmechanismen gegen Diskriminierung aufweisen und einem fortlaufenden Kontrollverfahren unterliegen, wenn sie in der Justiz zum Einsatz kommen sollen (dazu im Einzelnen Martini 2019a: 239 ff. und 248 ff.).

7.3.3.2 Recht auf ein faires Verfahren und Gebot prozessualer Waffengleichheit

Der Einsatz entscheidungsunterstützender Systeme darf Angeklagte nicht in ihrem Recht auf ein faires Verfahren (Art. 2 Abs. 1 i. V. m. Art. 20 Abs. 3 GG bzw. Art. 6 Abs. 1 EMRK[168]) verletzen. Aus dem Fair-Trial-Grundsatz erwächst ihnen u. a. das Recht auf prozessuale Waffengleichheit sowie ein Recht, mit den (Haupt-)Belastungszeugen konfrontiert zu werden.

Nutzt der Staat Werkzeuge im Rahmen eines rechtsstaatlichen Verfahrens, muss er daher durch die gesetzliche Ausgestaltung einer Validitätsprüfung sicherstellen, dass die Verfahrensbeteiligten nach den Vorgaben des gesetzlichen Verfahrensrechts eine Gleichbehandlung erfahren und sich gegen etwaige Fehler des Systems wirksam rechtlich verteidigen können. Das umschließt das Recht, die Validität eines algorithmisch ermittelten Entscheidungsvorschlags oder eines Messergebnisses – etwa einer Geschwindigkeitsübertretung, einer daktyloskopischen Untersuchung, einer DNA-Analyse oder eines Blutalkoholtests – überprüfen zu können. Nicht nur der Richter, sondern auch der Betroffene (sowie letztlich auch die Öffentlichkeit) müssen die Ergebnisse eines entscheidungsunterstützenden algorithmenbasierten Systems, auf das ein Urteil maßgeblich gründet, mithin kritisch hinterfragen können. Das impliziert korrespondierende Auskunftsrechte der Betroffenen – auch die

[168] Art. 6 EMRK (Europäische Menschenrechtskonvention) steht im Rang eines einfachen (Bundes-)Gesetzes. Das einfache Recht (etwa die StPO) ist aber aufgrund der Völkerrechtsfreundlichkeit des Grundgesetzes sowie dessen inhaltlicher Ausrichtung an dem Schutz der Menschenrechte (vgl. Art. 1 Abs. 2 GG) EMRK-konform auszulegen; vgl. etwa BVerfGE 128, 326 (367 ff.). In seinen einzelnen Komponenten etabliert Art. 6 Abs. 1 EMRK insbesondere ein Recht auf (prozessuale) Waffengleichheit; vgl. etwa BVerfGE 38, 105 (111); 110, 226 (253).

Herausgabe vorhandener Messdaten.[169] Anderenfalls wäre die Tatsachengrundlage einer Verurteilung gerichtlicher Überprüfung entzogen.[170] Der Einzelne wäre darauf verwiesen, der Zuverlässigkeit eines elektronischen Systems, das eine zentrale Lebensentscheidung über ihn fällen kann, bedingungslos ohne Verteidigungsmöglichkeit vertrauen zu müssen.

7.4 Referenzfall COMPAS – zu den Grenzen eines Risikoprognosesystems nach US-amerikanischem Vorbild

Auf das Feld entscheidungsunterstützender Systeme hat sich in der Strafjustiz das US-amerikanische System COMPAS bislang am weitesten vorgewagt. Seine Idee, computergesteuerte Entscheidungsunterstützung als strukturierende Ergänzung in den Prozess der Strafzumessung zu integrieren, klingt in den Ohren der Verfechter technischer Entscheidungsstringenz verlockend. Neu ist sie keineswegs (vgl. nur bspw. Philipps 1998: 263 ff.): Die Vision eines „Subsumtionsautomaten“ kam bereits im 19. Jahrhundert – weit vor Entwicklung des ersten Computers – auf.

Allen Unterschieden der Rechtssysteme zum Trotz sind Prognoseentscheidungen nicht nur dem US-amerikanischen, sondern auch dem deutschen Strafrecht keineswegs fremd: Jede Entscheidung darüber, ob die Freiheitsstrafe eines verurteilten Delinquenten zur Bewährung auszusetzen ist oder nicht, gründet auf einer Risikoprognose. Auch deshalb ist die Frage brisant, inwieweit ein System wie COMPAS unter den Bedingungen des deutschen Straf- und Strafprozessrechts zulässig wäre.

Das deutsche Recht fasst die Einschätzung der Rückfallgefahr unter dem Begriff „Sozialprognose“ zusammen: Entpuppt sie sich als günstig, setzt das Gericht die Vollstreckung einer Freiheitsstrafe zur Bewährung aus. Diese Entscheidung trifft das Gericht, wenn zu erwarten steht, dass der Verurteilte sich schon die Verurteilung als solche zur Warnung dienen lassen und künftig auch ohne die Einwirkung des Strafvollzugs keine Straftaten mehr begehen wird (§ 56 Abs. 1 S. 1 StGB).

Ähnliches gilt für die Entscheidung darüber, ob das Gericht den Strafrest einer bereits teilweise verbüßten Freiheitsstrafe zur Bewährung aussetzt (§§ 57, 57a StGB, § 454 StPO). Das Gericht darf dies nur verantworten, wenn sich das Ergebnis mit den Sicherheitsinteressen der Allgemeinheit, also dem Risiko einer erneuten Tat des Täters, vereinbaren lässt (§ 57 Abs. 1 S. 1 Nr. 2, S. 2 StGB). Auch die Entscheidung über die Anordnung von Untersuchungshaft i. S. d. § 112 Abs. 2 Nr. 2 und 3 StPO setzt eine Gefahren-, mithin eine Risikoprognose voraus.

7.4.1 Zulässige Entscheidungskriterien; strafprozessuales Gebot der Unmittelbarkeit

Bei der Risikoprognose sind dem Richter ebenso wie nach amerikanischem auch nach deutschem Recht Systeme zur Entscheidungsunterstützung als Hilfsmittel nicht a priori verwehrt. Sie in die richterliche Entscheidung einzubinden, ist grundsätzlich weniger eine Frage des „Ob“ als des „Wie“: Inwieweit sie zulässig sind, hängt stets von ihrer konkreten Ausgestaltung ab.

Das deutsche Recht legt die Messlatte dafür höher als das amerikanische: In den USA gibt der COMPAS-Algorithmus die Rückfallwahrscheinlichkeit für einen Täter auf der Grundlage seines Kriterienmix auf einer Skala von 1 bis 10 an. Die Befragung durch Polizeibeamte oder Bewährungshelfer, die eine wichtige Grundlage für den Risiko-Score des COMPAS-Systems bildet, dringt weit in die Privat- und Intimsphäre der Beschuldigten ein: Neben den bereits polizeilich erfassten Daten zu Vorstrafen etc. verlangt es Betroffenen insbesondere Informationen über die Kindheit, den Bildungs- und Berufsweg und die Familienverhältnisse ab. Auch Bekanntschaften und Nachbarschaft,

---

[169] SaarlVerfGH, Beschluss vom 27.4.2018 – Lv1/18, NZV 2018, 275 (275 ff.; dazu auch Wendt 2018: 441 ff.); BGHSt 39, 291 (291 ff.) = NJW 1993, 3081 (3081 ff.).
[170] SaarlVerfGH, Urteil vom 5.7.2019 – Lv 7/17 – III. 4, NJW 2019, 2456 (2458, Rn. 47 ff.).

Finanzen, Moralvorstellungen, eigene Gewalterfahrungen sowie Drogen- und Alkoholkonsum fließen in die Entscheidung ein.

In vielen seiner Aspekte knüpft der COMPAS-Fragebogen an Merkmale an, die hierzulande keine Entscheidungsrelevanz entfalten dürfen – etwa die Vorstrafen der Eltern, ob diese geschieden sind oder ob der Beschuldigte Geldprobleme hat. In Deutschland ist bei der Strafzumessung vielmehr das Schuldprinzip, also die persönliche Vorwerfbarkeit des Täterverhaltens, maßgebend. Es verlangt eine individuell auf Person und Tat zugeschnittene Strafe; „Sippenverantwortung" ist kein zulässiges Strafzumessungskriterium. Auch die wirtschaftlichen Verhältnisse bleiben hierzulande im Grundsatz ohne Auswirkung auf die Strafzumessung oder Bewährungsfähigkeit. Lediglich für die Bemessung der Geldstrafe (§ 40 Abs. 2 StGB) oder als Indikator für Fluchtmöglichkeiten bzw. soziale Integration können sie Relevanz entfalten. Auch für die Entscheidung über eine Straf(rest)aussetzung zur Bewährung (§ 56 Abs. 1 S. 2 bzw. § 57 Abs. 1 S. 2 StGB) sind rein korrelative Verknüpfungen keine tauglichen Indikatoren – erst recht nicht, wenn sie nicht in der Person des Beschuldigten liegen oder er sie nicht beeinflussen kann.

Dem deutschen Strafprozessrecht ist es überdies fremd, Aspekte, die nicht Teil der gerichtlichen Verhandlung waren, sondern auf einer Drittbefragung beruhen, in zentrale Erwägungen der richterlichen Entscheidung einfließen zu lassen: In die gerichtliche Entscheidung darf nur das Eingang finden, was Teil der mündlichen Verhandlung war (*Mündlichkeitsgrundsatz*; §§ 243, 264 StPO). Der Richter muss sein Urteil auf der Grundlage des unmittelbaren Eindrucks treffen, den er kraft einer Vernehmung in der Hauptverhandlung über den Angeklagten gewonnen hat (*Gebot der Unmittelbarkeit*; vgl. insbesondere §§ 261, 264, 250 StPO). Zumindest hat der Richter selbst zu bewerten, wie glaubhaft die Antworten sind, und die gerichtliche Entscheidung auf einer abwägenden Gesamtschau aufzubauen.

7.4.2 Nachvollziehbarkeit der Entscheidungskriterien

Zweifelhafte Prognosekraft und statistische Ungleichbehandlungen verschiedener Gruppen sind nicht der einzige Stein des Anstoßes am COMPAS-System. In der rechtlichen Bewertung hinterlässt auch seine mangelnde Nachvollziehbarkeit einen schalen Beigeschmack. Wie der Algorithmus zu seinem Entscheidungsvorschlag kommt, verliert sich grundsätzlich im Nebel der Spekulation (Angwin et al. 2016): Weder der Richter noch der Beschuldigte wissen, wie und nach welchen Maßstäben das Entscheidungsergebnis genau zustande kommt. Auch der Öffentlichkeit bleibt die Möglichkeit verwehrt, ihre Kontrollfunktion über die dritte Gewalt auszuüben, wenn die Entscheidungsgrundlagen nicht jedenfalls in ihren Grundzügen einsehbar sind.

Die exakte Funktionsweise des Systems – etwa wie es die verschiedenen Entscheidungskriterien und Einzelmerkmale gewichtet und berücksichtigt – ist einerseits als Geschäftsgeheimnis des Herstellers als privatwirtschaftliches Unternehmen geschützt (Martini 2019a: 37 ff.). Aus den grundgesetzlichen Verbürgungen des Demokratie- und Rechtsstaatsprinzips (Art. 20 Abs. 2 und 3 GG) entspringt jedoch andererseits zugleich die objektiv-rechtliche Verpflichtung des Staates, die Handlungen seiner Einrichtungen grundsätzlich öffentlich nachvollziehbar, vorhersehbar und rekonstruierbar auszugestalten.[171] Dem Maßstab dieses Transparenzgebots genügt ein Entscheidungsassistenzsystem, das zentrale Bestandteile der Urteilsfindung einer Nachvollziehbarkeit entzieht, nicht. Etwaige Geheimhaltungsinteressen der Softwarehersteller haben dahinter zurückzustehen, wenn diese ihre Software gezielt auf die justizielle Nutzung ausrichten.[172]

Der Grundsatz der Verfahrensöffentlichkeit (§ 169 Abs. 1 S. 1 GVG[173]) verleiht dem Verlangen, über die Aspekte, die in das Urteil Eingang finden, grundsätzlich Transparenz herzustellen, normativen Flankenschutz. Das impliziert nicht vollständige Transparenz, die das *gesamte* System für jedermann offenlegt und damit Umgehungsgefahren

[171] Vgl. etwa BVerfGE 123, 39 (68 ff.; Rn. 107 u. 110); 133, 143 (158).
[172] Siehe dazu auch oben Martini und Botta: Der Algorithmus als universitärer Pfortenwächter (Abschnitt 4.7.2 dieser Studie).
[173] Die Abkürzung steht für „Gerichtsverfassungsgesetz".

schafft: Wären alle Berechnungsfaktoren und ihre Ergebnisse jedermann bekannt, ließe sich das System (insbesondere durch eine strategisch-berechnende Beantwortung des Fragebogens) in einer Weise beeinflussen, die den ursprünglichen Prognosezweck torpediert.[174] Aus eben diesem guten Grund legt bspw. auch das Risikomanagementsystem, das die Finanzverwaltung im Steuerwesen einsetzt, nicht jeden Aspekt seiner Risikoschwellen offen (§ 88 Abs. 5 S. 4 AO). Mit dem Rechtsstaatsprinzip ist das vereinbar.[175]

Der Staat muss aber geeignete Verfahren vorhalten, mit denen der Einzelne bei zentralen grundrechtlichen Entscheidungen, wie der Entscheidung über die Haft oder die Studienplatzvergabe[176], eine wirksame Überprüfung auf alle entscheidungserheblichen Aspekte hin erreichen kann. Dazu gehören insbesondere wirksame behördeninterne Kontrollprozesse, gerichtlicher Rechtsschutz gegen algorithmenbasierte Einzelentscheidungen und hinreichende Information über die entscheidungsleitenden Kriterien, die diesen Rechtsschutz ermöglichen.

7.4.3 Einzelheiten der strafrechtlichen und strafprozessualen Entscheidungskaskade

Ebenso wie der Entscheidung über den Tatvorwurf und die Schuld des Täters ist den drei Entscheidungsschritten des COMPAS-Systems – Untersuchungshaft (§§ 112 ff. StPO), Strafhöhe (§ 46 StGB) und Strafrestaussetzung zur Bewährung (vgl. §§ 57, 57a StGB) – nach deutschem Recht das Gebot gemeinsam, dem Richter eine Gesamtwürdigung der Umstände des Einzelfalls abzuverlangen. Die Kriterien, die Rechtsprechung und Rechtspraxis dafür entwickelt haben, eignen sich aufgrund ihres objektiven Charakters im Ansatz auch für eine algorithmische Auswertung, um zu einer konsistenteren Entscheidungspraxis beizutragen. Denn Systeme maschinellen Lernens zeichnen sich durch die beeindruckende Fähigkeit aus, Entscheidungsparameter vergangener Entscheidungen kategorisiert aufzubereiten und Korrelationen mit vorherigen Entscheidungen aufzuzeigen.

Die Gesamtwürdigung einer Haftentscheidung möglichst objektiv und rational vorzunehmen, fordert die Strafjustiz zugleich in besonderer Weise heraus. Denn das Gesetz zeichnet nicht exakt vor, *wie* die einzelnen Kriterien und Anknüpfungspunkte zu gewichten und zu berücksichtigen sind und wie die Richter – ggf. geleitet von der algorithmischen Einschätzung – kraft eigener juristischer und kriminalistischer Erfahrung[177] zu ihren Entscheidungen gelangen (sollen).

Über das Ergebnis der Beweisaufnahme entscheidet der Strafrichter vielmehr nach Maßgabe seiner freien Überzeugung, die er aus dem Inbegriff der Verhandlung schöpft (§ 261 StPO). Er muss seine Entscheidung – nach Maßgabe des Gesetzes – auf der Grundlage seiner tatrichterlichen Überzeugung frei treffen und sie auf sein eigenes Judiz stützen. Die Entscheidung in eigener Verantwortung ist insbesondere essenzieller Teil der Freiheit der Beweiswürdigung (Miebach 2016: § 261 Rn. 54, 92). Der Richter ist daher weder verpflichtet noch berechtigt, ein algorithmisches Ergebnis zu berücksichtigen, wenn er hieran Zweifel hegt, noch schreibt die Rechtsordnung grundsätzlich fest, welche Schlussfolgerung er aus bestimmten Umständen zu ziehen oder welches Gewicht er einer Tatsache beizumessen hat.

Stark vereinfacht lässt sich ein algorithmenbasierter Vorschlag zur Untersuchungshaftanordnung (Abschnitt 7.4.3.1), zur Strafzumessung (Abschnitt 7.4.3.2) und zur Strafrestaussetzung (Abschnitt 7.4.3.3) mit der Einschätzung eines Kollegen oder Referendars vergleichen: Der Richter genießt die Freiheit, sich über den Vorschlag hinwegzusetzen. Als Ausfluss seiner richterlichen Unabhängigkeit ist er auch prinzipiell frei in der Wahl seiner

---

[174] Dazu auch bereits Abschnitt 4.7 dieser Studie.

[175] Andernfalls wäre insbesondere Steuerbetrügern Tür und Tor geöffnet, die in Kenntnis des Modus Operandi eines Systems ihre Angaben stets gerade unterhalb der Schwellenwerte ansetzen. Die partielle Intransparenz ist daher nicht nur gerechtfertigt, sondern ein Stück weit auch Voraussetzung für eine gleichmäßige und gesetzeskonforme Besteuerung (vgl. § 85 AO); ebenso Rätke 2018: Rn. 104 f.

[176] Dazu Martini und Botta: Der Algorithmus als universitärer Pfortenwächter (Kapitel 4 in dieser Studie).

[177] Für die richterliche Entscheidungsfindung gilt ohnehin der objektive Maßstab. Das kommt etwa in der Wendung „auf Grund bestimmter Tatsachen“ (§§ 112 Abs. 2 Satz 1; 112a Abs. 1 Satz 1 StPO) zum Ausdruck.

Hilfsmittel;[178] ihm steht es offen, die einzubeziehenden Umstände und Würdigungsfaktoren je nach Einzelfall zu erweitern. Er darf jedoch umgekehrt nicht blind auf einen Vorschlag vertrauen, sondern muss sich selbst mit der Lösung auseinandersetzen.

7.4.3.1 Untersuchungshaft

Untersuchungshaft anzuordnen, ist im deutschen Strafprozessrecht nur unter strengen Voraussetzungen zulässig: Es muss sowohl ein Haftgrund als auch ein dringender Tatverdacht bestehen. Wie jeder Grundrechtseingriff muss die Anordnung überdies verhältnismäßig sein.

- **Haftgrund**
  Als Haftgründe erkennt das Gesetz Flucht, Fluchtgefahr,[179] Verdunkelungsgefahr[180] und – bei besonders schweren Delikten wie bspw. Mord – Wiederholungsgefahr an (§§ 112 Abs. 2, 112a StPO).

  Um Haftgründe zu prüfen, stellt der Richter eine *faktenbasierte* Prognose über das zukünftige Verhalten des Verdächtigen auf. Die (nicht abschließenden) gesetzlichen Kriterien kann ein (lernender) Algorithmus grundsätzlich ähnlich wie ein Richter verwerten und vorbereiten, soweit er lebensweltliche Umstände adäquat zu erfassen in der Lage ist. Das Gesetz ist insoweit durchaus offen für softwareunterstützte Prognosen; sie könnten im Idealfall sogar eine Entscheidung konsistenter und nachvollziehbarer machen, wenn Richter dadurch die Kriterien, die sie für die Prognose herangezogen haben, sowie deren Gewichtung anhand einer objektiven Metrik entwickeln und offenlegen. Da die Letztentscheidung ohnedies dem Richter vorbehalten ist, kann er auch weitere Kriterien in Rechnung stellen und zu einem anderen Ergebnis als der Entscheidungsvorschlag[181] gelangen.

- **Dringender Tatverdacht**
  Während ein Computersystem bei der Feststellung des Haftgrundes hilfreiche Dienste leisten kann, stößt es bei der Feststellung des dringenden Tatverdachts schnell an seine Grenzen:

  Dringend einer Tat verdächtig ist ein Beschuldigter, wenn er nach den Erkenntnissen des jeweiligen Ermittlungsstandes mit hoher Wahrscheinlichkeit Täter oder Teilnehmer einer strafbaren Handlung ist. Dies

---

[178] Insoweit kritisch aber Justizministerkonferenz 2019: 57 f. Die Rechtsprechung steht dem Einsatz neuer Technologien traditionell skeptisch gegenüber. So waren bspw. Polygraphen („Lügendetektoren“) jahrzehntelang nicht als Beweismittel zulässig. Das Hauptargument des BGH (vgl. BGHSt 5, 332 [334]) war zunächst nicht die (fehlende) Funktionsfähigkeit oder die etwaige Intransparenz. Er hegte vielmehr vorrangig die Befürchtung, dass die indirekte Selbstbelastung des Angeklagten den sog. *Nemo-tenetur-Grundsatz* und damit letztlich die Menschenwürde beeinträchtigen könnte (vgl. Art. 1 Abs. 1 GG und § 136a StPO). Spätere Gerichtsentscheidungen hoben jedoch besonders auf die mangelnde Verlässlichkeit und die Fehleranfälligkeit der Systeme ab. Ihre rechtliche Bewertung bleibt im steten Wandel begriffen: In jüngeren Verfahren ließen Gerichte den Polygraphen (zur Entlastung des Angeklagten) teilweise zu; vgl. OLG Dresden, Beschluss vom 14.5.2013 – 21 UF 787/12 –, juris, Rn. 19 (Einsatz in Sorge- und Umgangsrechtsverfahren); AG Bautzen, Urteil vom 26.3.2013 – 40 Ls 330 Js 6351/12 –, juris, Rn. 38 ff.

[179] Bei einem Beschuldigten besteht *Fluchtgefahr,* wenn bei Würdigung der Umstände des Einzelfalls wahrscheinlicher ist, dass er sich dem Strafverfahren *entzieht,* als dass er sich ihm stellt; Graf 2013: § 112, Rn. 16; Krauß 2019: § 112, Rn. 23. Dafür ist eine Prognose anzustellen. Sie hat alle Kriterien einzubeziehen, die für und gegen eine wahrscheinliche Flucht sprechen. Zu berücksichtigen sind insbesondere die Lebensverhältnisse des Beschuldigten – ob ihm also auf der einen Seite durch Kontakte im Ausland oder seine wirtschaftlichen Verhältnisse eine Flucht leicht gelänge oder ob – auf der anderen Seite – sein Alter oder berufliche und familiäre Bindungen ihn von der Flucht abhalten werden. Einfließen können daneben auch die Art und Schwere der vorgeworfenen Tat, die Straferwartung sowie weitere Aspekte; Krauß 2019: § 112 Rn. 26.

[180] *Verdunkelungsgefahr* besteht, wenn das Verhalten des Beschuldigten den dringenden Verdacht begründet, er werde Handlungen vornehmen, die darauf zielen, Beweise zu vereiteln (vgl. § 112 Abs. 2 Nr. 3 StPO), und dadurch die Gefahr besteht, dass die Wahrheitsermittlung erschwert wird; vgl. Krauß 2019: § 112 Rn. 31; OLG Köln, Beschluss vom 10.9.1996 – 2 Ws 457/96 = StV 1997, 27.

[181] Zum Risiko eines *Automation Bias* siehe oben Abschnitt 7.3.2.1.

zu entscheiden, bewegt sich im Kernbereich strafrichterlicher Rechtsanwendung: Der Richter muss auf der Grundlage der vorhandenen Ermittlungsergebnisse eine vorläufige, jedoch zugleich umfassende Würdigung des Sachverhalts vornehmen. Einem Computersystem ist diese komplexe Entscheidung grundsätzlich verwehrt.

- **Verhältnismäßigkeit**
  Eine rechtsstaatlich bedenkliche Zone erreicht die algorithmische Unterstützung spätestens dort, wo die einzelfallbezogene Verhältnismäßigkeitsprüfung beginnt: Die Untersuchungshaft muss zur Straftat und Strafe in angemessenem Verhältnis stehen (§ 112 Abs. 1 S. 2 StPO).
  Diese Prüfung gelingt einem algorithmenbasierten System a priori nur eingeschränkt. Denn sie impliziert die Fähigkeit, alle Umstände des Einzelfalls zu gewichten und sachgerecht bewerten zu können. Die assistierende Funktion des Unterstützungssystems lässt sich daher insoweit in den Kernbereichen richterlicher Verhältnismäßigkeitsprüfung weniger gut als in Randbereichen richterlicher Entscheidungsgewalt entfalten – also etwa, um Sachverhaltsaspekte visuell aufzubereiten oder (vergangene) richterliche Entscheidungen bzw. Entscheidungsbegründungen vorbereitend zu identifizieren, die sich mit einer vergleichbaren Tatsachengrundlage auseinandersetzen.

7.4.3.2 Strafzumessung (insbesondere Haftlänge)

Im Rahmen der Strafzumessung im Hauptverfahren treffen Richter nicht in erster Linie eine *Prognose*entscheidung. Sie beurteilen vielmehr rückblickend das Unrecht, das der Täter verwirklicht hat: Grundlage für die Strafzumessung ist die Schuld des Täters (§ 46 Abs. 1 S. 1 StGB), die in der Tat zum Ausdruck kommt. Dies ist Ausfluss des verfassungsrechtlich verbürgten Schuldprinzips.[182]

Um Schuld zu beurteilen, müssen Richter insbesondere bewerten, ob und inwiefern einzelne Aspekte einer Tat strafschärfend oder -mildernd wirken. Das Gesetz gibt ihnen dafür lediglich abstrakte Kriterien vor, die den Entscheidungsraum steuern. Dazu gehören insbesondere die Beweggründe und die Ziele des Täters, die Art der Ausführung und die verschuldeten Auswirkungen der Tat – ferner das Vorleben des Täters, seine persönlichen und wirtschaftlichen Verhältnisse sowie sein Verhalten nach der Tat (§ 46 Abs. 2 StGB).[183]

Da die Faktoren der Entscheidung komplex und ihre Wirkungen einschneidend sind, sieht sich sachgerechte (algorithmenbasierte) Entscheidungsunterstützung in diesem Feld besonderen, praktischen Herausforderungen ausgesetzt. Denn sie setzt voraus, dass zumindest die Zielparameter konsentiert sind.

Wo genau die gerechte Strafe innerhalb des gesetzlichen richterlichen Spielraums anzusiedeln ist, darüber besteht jedoch weder in Wissenschaft noch Praxis Einigkeit (Hörnle 2005: 397 ff.). Das gründet insbesondere darauf, dass die Gewichtung der einzelnen Tataspekte auch von dem – umstrittenen – Zweck der Strafe abhängt.[184] Der Gesetzgeber hat diesen weder abschließend noch explizit determiniert. Er lässt sich dabei von der Idee leiten, dass es keine „richtige“, unmittelbar aus dem Gesetz folgende „Punktstrafe“ gibt. Er gibt dem Richter daher nur einen

---

[182] Zum Schuldprinzip siehe BVerfGE 133, 168 (Rn. 53, 55) m. w. N.
[183] Auch weitere, die Schuld indizierende Umstände können Richter in die Strafzumessung einfließen lassen; vgl. bspw. jüngst etwa die Diskussion zur „Lebensleistung“ eines Täters als Strafzumessungskriterium (Stadler 2017: 271 ff.). Die Aufzählung der Strafzumessungserwägungen in § 46 Abs. 2 StGB ist nicht abschließend. Über die Strafzumessung müssen Richter in voller eigener Überzeugung entscheiden (§§ 261, 264 StPO; vgl. auch von Heintschel-Heinegg: § 46, Rn. 1; Miebach und Maier 2016: § 46, Rn. 66). Im Einzelfall kann auch ein Strafbefehl ergehen – insbesondere dann, wenn ein Verteidiger bestimmt ist und die Freiheitsstrafe ein Jahr auf Bewährung nicht übersteigt (§ 407 Abs. 2 Satz 2 StPO). Diese Verfahrensart bildet eine Ausnahme zum Mündlichkeitsgrundsatz und dem Maßstab der „vollen Überzeugung“.
[184] Die deutsche Strafrechtslehre betrachtet die Spezialprävention und die Resozialisierung als die vorherrschenden Strafzwecke; vgl. nur Joecks und Miebach 2016: § 46 Rn. 45.

Entscheidungskorridor vor, damit er die für den Einzelfall passgenaue, gerechte Strafe auswerfen kann (sog. *Spielraumtheorie*).

Der Kompass der Strafzwecke weist dabei in unterschiedliche Richtungen: Wer den *Vergeltungs- und Sühnegedanken* des Strafrechts betont, wird in erster Linie auf die Begehungsweise und die Folgen der Tat schauen. Künftiges Verhalten des Täters nimmt dann eine untergeordnete Rolle ein. Folgt man demgegenüber einem *spezialpräventiven Ansatz*, liegt der Fokus eher auf den persönlichen Umständen des Täters. Dann kommt es vor allem darauf an, ob dieser voraussichtlich erneut straffällig werden wird. Unter *generalpräventiven Gesichtspunkten* sind demgegenüber die gesellschaftlichen Auswirkungen der Tat und der Strafe handlungsleitend: Die Strafe soll dann (negativ) vor allem andere davor abschrecken, eine ähnliche Tat zu begehen, sowie (positiv) das Vertrauen in die Rechtsordnung bestärken. Das insinuiert typischerweise eine hohe Strafe.

Ohne einen Konsens über die relevanten Kriterien der Strafzumessungslehre und deren Gewichtung steht ein algorithmenbasiertes Entscheidungssystem vor einem Dilemma: Entweder wird die Akzeptanz und Offenheit der Richter gegenüber Entscheidungsunterstützungssystemen ausbleiben oder die Richter setzen sie ein, beschwören aber die Gefahr herauf, Entscheidungsmacht in unzulässiger Weise an eine Software zu delegieren.

In praxi finden sich immerhin bereits erste konkrete Ansätze für Entscheidungsunterstützungssysteme, etwa ein auf der sog. *Fuzzy-Logik* basierendes System zur Strafzumessung für Vermögensdelikte.[185] Eigentums- und Vermögensdelikte eignen sich bereits wegen ihres objektiv quantifizierbaren Schadensausmaßes – als wichtiger Indikator des sog. *Erfolgsunrechts* und damit der Strafzumessungsschuld – für die algorithmische Abbildung tendenziell besser als Personendelikte wie Körperverletzung oder Vergewaltigung, bei denen sich das verwirklichte Unrecht vorrangig nicht durch einen materiellen, sondern einen immateriellen, nur durch einen Menschen nachempfindbaren Schaden definiert.

7.4.3.3 Prüfung der vorzeitigen Haftentlassung (insbesondere Strafrestaussetzung)

Die normativen Steuerungsvorgaben für die dritte gesetzliche Stufe der denkbaren Haftentscheidungen – die Aussetzung des Strafrests einer Freiheitsstrafe – formulieren materiell-rechtlich die Vorschriften des § 57 StGB (für die zeitige Freiheitsstrafe) bzw. § 57a StGB (für die lebenslange Freiheitsstrafe). In prozessualer Hinsicht setzt insbesondere § 454 StPO die normativen Leitplanken.

Den Strafrest zur Bewährung auszusetzen, lässt das Gesetz nur dann zu, wenn sich dies vor dem Angesicht des Sicherheitsinteresses der Allgemeinheit verantworten lässt (vgl. nur § 57 Abs. 1 Nr. 2 StGB). Dafür bedarf es keiner Gewissheit, sondern einer „naheliegenden Chance“, dass der Täter nicht in (vergleichbares) strafrechtliches Unrecht zurückfällt (von Heintschel-Heinegg: § 57 StGB, Rn. 7). Zu würdigen sind dabei insbesondere die Persönlichkeit der verurteilten Person, ihr Vorleben, die Umstände der Tat, ihr Verhalten im Vollzug – ebenso ihre Lebensverhältnisse sowie die Wirkungen, die von der Aussetzung zu erwarten sind (§ 57 Abs. 1 S. 2 StGB).

All diese Kriterien erfordern entweder zusätzliche Sachverhaltsermittlung, z. B. durch Psychologen, oder sind sehr breit gefasst. Bei dem Versuch, sie vollständig zu erfassen oder sie gar zueinander in Beziehung zu setzen, steht eine Software daher vor hohen Hürden. Sie lassen sich allenfalls dann überwinden, wenn der Gesetzgeber die einzelnen Kriterien stärker konturiert, z. B. welche Persönlichkeitsmerkmale negativ oder positiv zu werten sind. Auch die Wirkungen auf den einzelnen Beschuldigten kann die Software nicht zuverlässig schematisch beurteilen. Lediglich hinsichtlich der Umstände der Tat und der Lebensverhältnisse des Beschuldigten ist ein datengetriebener

[185] Giannoulis 2014: 315 ff. Mithilfe der Fuzzy-Logik kann ein System starren „Schwarzweiß“-Mustern entfliehen, weil sie für Aussagen auch den Modus „teilweise wahr“ kennt. Für die auf natürlicher Sprache aufbauenden verbalen Annäherungen an juristische Entscheidungen bietet die Fuzzy-Logik daher (ebenso wie künstliche neuronale Netze) mannigfaltige Möglichkeiten; siehe dazu etwa Munte 2001: 534 f.; Philipps 1994: 221 f.

Vergleich im Ansatz hilfreich, um damit auch bei Haftentlassungen zu einer konsistenteren und objektiveren Entscheidungspraxis beizutragen. Sie können das Bewusstsein der Richter für die einbezogenen Kriterien und deren Gewichtung schärfen.

7.4.4 Zwischenresümee

Die Strafzumessung algorithmisch zu steuern, sprengt den Korridor der juristisch-technischen Möglichkeiten. Denn Schuld ist nicht rein quantitativ beschreib- und metrisch erfassbar. Das System COMPAS wäre daher in Deutschland schon deshalb nicht in zulässiger Weise einsetzbar. Um einem System zur Entscheidungsunterstützung einen rechtsstaatlich tragbaren „Strafzumessungsalgorithmus“ einzupflanzen, bedürfte es zudem eines Mindestmaßes normativer Vorgaben.

Entscheidungen über die Untersuchungshaft und die Strafrestaussetzung eignen sich – jedenfalls teilweise – tendenziell besser als die Strafzumessung für eine Entscheidungsassistierung auf der Grundlage objektiver Kriterien. Sie sind zumindest im Hinblick auf einige Merkmale im Ansatz auch algorithmisch abbildbar. Dennoch verbietet sich auch hier jede Schematisierung, die den Einzelfall außer Acht lässt und einem *Automation Bias* Vorschub leistet; immer bleiben eine menschliche Zusammenschau, Bewertung und Gewichtung im Einzelfall geboten.

7.5 Fazit

Einer *vollständigen Automatisierung* gerichtlicher Entscheidungen zieht die Rechtsordnung klare verfassungsrechtliche Grenzen. Ob Strafzumessungskommissionen, verbindliche *Sentencing Guidelines* oder eben entscheidungsunterstützende Algorithmen: Kraft der verfassungsrechtlichen Vorgaben des Schuld- und Rechtsstaatsprinzips muss immer ein Richter aus Fleisch und Blut die Verantwortung für die gesamte Entscheidung in Kenntnis aller relevanten Umstände in den Händen halten. Nur er kann alle Aspekte berücksichtigen, die für die Einzelfallgerechtigkeit von Bedeutung sind.

Weniger klar umrissen sind die Grenzen, die das Verfassungsrecht algorithmenbasierten Systemen der *Entscheidungsunterstützung* setzt – insbesondere bei Risikoprognosen, die auch das deutsche Strafrecht kennt. Assistenzsysteme dürfen auch dort im Ergebnis nur zum Einsatz kommen, wenn die Prozessgrundrechte der Betroffenen gewahrt bleiben, das algorithmische System eine hinreichend valide Aussagekraft aufweist und der Richter seine Entscheidung nicht faktisch an eine Software delegiert. Denn die richterliche Gewalt ist dem Richter nicht nur anvertraut – sie ist ihm auch aufgegeben. Er muss seine Entscheidung auf eine eigene Gesamtwürdigung aller Umstände stützen, die für den Einzelfall relevant sind. Algorithmenbasierte Systeme können ihm dafür allenfalls einzelne Entscheidungsaspekte zuliefern.

Als Teil eines staatlichen Entscheidungssystems, das auf dem Gedanken beruht, dass sich staatliche Entscheidungsmacht von der Legitimation der demokratischen Organe ableiten muss, unterliegen algorithmenbasierte Assistenzsysteme dem Gebot der Nachvollziehbarkeit: Zumindest die Grundzüge der Funktionsweise, insbesondere die Entscheidungskriterien, müssen nicht nur für den Richter, sondern auch den Angeklagten und mittelbar die Öffentlichkeit, in deren Namen der Richter das Recht spricht, verständlich sein. Die Komplexität datenbasierter (lernfähiger) Systeme errichtet dafür eine technische Hürde. Umgekehrt sind algorithmenbasierte Entscheidungsvorschläge zugleich auch nicht unbedingt weniger transparent als menschliche: Computergenerierte Entscheidungen lassen sich dokumentieren und technisch – wenn auch bspw. bei neuronalen Netzen bisher nur sehr eingeschränkt – rekonstruieren. Ihre Ergebnisse lassen sich immerhin mithilfe von Kontrollalgorithmen überprüfen.

Demokratische Streitentscheidungslegitimation vertraut die Verfassung jedoch allein dem Richter an. Sollen algorithmische Systeme in seinen Entscheidungsprozess Eingang finden, muss die Rechtsordnung deren Kontrolle

sicherstellen. Jedenfalls in sensiblen Bereichen sollten Unterstützungssysteme aus diesem Grund einer vorherigen Zulassung unterworfen sein, die eine Eignungsprüfung „auf Herz und Nieren“ vornimmt.[186]

Entscheidungsunterstützungssysteme verheißen zwar, gerichtliche Entscheidungen durch die Verlässlichkeit der Einsen und Nullen abzusichern und eine gleichmäßigere, konsistentere Justizpraxis zu induzieren. Rechtlich verantwortbar sind sie aber nur sehr begrenzt und mit Augenmaß eingesetzt. So unerschütterlich und stringent ihre mathematische Logik auch sein mag: Dem Menschen als Individuum und dem Urbedürfnis des Rechtsstaats, (Individual-)Gerechtigkeit herzustellen, entsprechen sie (aus sich heraus) nicht.

[186] Als Entwicklungsakteure der Systeme sind neben privatwirtschaftlichen Unternehmen auch „behördliche Eigenproduktionen“ denkbar, wie bspw. das Landeskriminalamt Nordrhein-Westfalen für die dort eingesetzten Predictive-Policing-Systeme erfolgreich gezeigt hat. Dazu auch Martini und Nink: Mit der algorithmischen Kristallkugel auf Tätersuche? (Kapitel 6 dieser Studie, insbes. Abschnitte 6.2.1.1 und 6.3.2.2).

8 Soziale Netzwerke – Daten-Eldorado für personalisierte Angebote?

Rechtliche Rahmenbedingungen für die Auswertung nutzergenerierter Social-Media-Daten durch Private

Prof. Dr. Mario Martini und Michael Kolain

Im Jahr 2018 war der Aufschrei kaum zu überhören: Über Add-ons im sozialen Netzwerk *Facebook* gelang es dem britischen Datenanalyse-Unternehmen *Cambridge Analytica,* persönliche Daten mehrerer Millionen Menschen abzugreifen. Um Wähler zielgenau adressieren zu können, gab es Personenprofile an politische Akteure weiter (Dachwitz, Rudl und Rebinger 2018; Schindler 2018). *Facebook*-Nutzer, die den Persönlichkeitstest einer App mit dem vielsagenden Namen „thisisyourdigitallife" durchführten, hatten diese Daten unbewusst preisgegeben: Die App nahm über eine Schnittstelle Zugriff auf das jeweilige *Facebook*-Konto. Sie sammelte nicht nur Profilinformationen des Nutzers selbst, sondern auch seiner „Freunde" ein (Decker und Bernau 2018). Mithilfe der 270.000 Teilnehmer des Tests gelangte „thisisyourdigitallife" letztlich an die Daten von insgesamt 87 Millionen Personen (Dachwitz, Rudl und Rebinger 2018).[187]

8.1 Erkenntnispotenziale sozialer Netzwerke

Dass aus den Datenreservoirs sozialer Netzwerke wertvolle Erkenntnisse hervorsprudeln, haben nicht nur Wahlkämpfer und Behörden erkannt. Längst wecken die Informationen, die *Facebook, Twitter* und Co. über ihre Nutzer zusammentragen, auch bei marktwirtschaftlich agierenden Unternehmen Begehrlichkeiten: Wer die individuellen Neigungen, Lieblingsprodukte und Lebensgewohnheiten eines Menschen kennt, kann sein Angebot auf ihn maßschneidern.[188] So scheinen die Tage teurer Printprodukte, die mit langer Vorlaufzeit und hohen Streuverlusten zu kämpfen haben, unterdessen gezählt und ist die Onlinesparte zu einer der zentralen Säulen moderner Werbeagenturen avanciert (Martini 2016b: 315).

Vor allem für Wirtschaftsakteure, die Verbraucher auf ihre Kreditwürdigkeit durchleuchten wollen, sind die digitalen Fußspuren, die der Einzelne im Netz hinterlässt, eine Fundgrube der Erkenntnis. Nicht nur aus der präferierten Zahlungsweise beim Vertragsschluss, sondern bereits aus orthographischen Fehlern oder der Ausdrucksweise in Antragsformularen lassen sich Prognosen über die Zahlungsbereitschaft entnehmen (Carney 2013). So verspüren auch Banken, die mehr über einen Darlehensnehmer erfahren möchten, einen starken Anreiz, auf dessen Profile in sozialen Netzwerken zurückzugreifen. In der Vergangenheit erfolgten individuelle Auskünfte typischerweise via Fragebogen.[189] Nunmehr kommen verstärkt automatisierte Datenerhebungen und -analysen zum Einsatz. So greift bspw. das Schweizer Unternehmen *Creditgate24* bei der Kreditvergabe auf Informationen aus der Onlinewelt zurück.[190] In die Bonitätsprüfung des Hamburger FinTech-Startups *Kreditech* fließen Daten aus

---

* Die Autoren danken besonders dem Forschungsreferenten *Jan Mysegades* für seine sehr gute Mitwirkung an dem Beitrag.

[187] Im analogen Zeitalter lag diese Reichweite und das damit mögliche sog. *Mikrotargeting* noch völlig außerhalb der Vorstellungskraft: Die politische Kommunikation beschränkte sich vor allem auf repräsentative Umfragen unter potenziellen Wählern. Unterdessen hat *Facebook* im Gefolge des Skandals nicht nur eine Geldstrafe i. H. v. 5.000.000.000 US-Dollar zahlen müssen. Es hat auch zehntausende Apps überprüft, die auf seine Infrastruktur zugreifen. Mehrere hundert unter ihnen hat das soziale Netzwerk in der Folge gesperrt – bspw. die App „mai Persönlichkeit". Sie hatte Informationen ohne angemessene Schutzmechanismen an Forscher und Unternehmen weitergereicht.

[188] Zum politischen Microtargeting siehe Bodó, Helberger und de Vreese 2017: 3 ff.

[189] Etwa zu den Fragen, „wie viel ich verdiene, was meine Wohnung kostet, ob ich ein Auto oder ein Motorrad habe, wie viele Kreditkarten ich besitze und welche Kredite ich sonst noch so am Laufen habe" (Dörnfelder 2018).

[190] Vgl. „Was bedeutet Bonitätsprüfung?", https://www.creditgate24.ch/de/faq/ (Download 11.11.2019). Die Bank wählt die etwas kryptischen Worte „Betreibungsinformationen, Big Data Analysen, Social Media Internet", um die Datenquellen zu umreißen.

Onlinehandelsplattformen und sozialen Netzwerken, mobilen Endgeräten und sonstige Informationen ein, die im Internet verfügbar sind (Fuchs 2017).

Da in mobilen Daten wertvolle Erkenntnisse über individuelle Verhaltensmuster schlummern, setzen Unternehmen in jüngerer Zeit verstärkt darauf, das Smartphone als umfassendes Datenreservoir privater Lebensentfaltung anzuzapfen, um die Zahlungsbereitschaft ihrer Kunden zu analysieren.[191] So gewährt die App *Tala* Menschen in Kenia, die anderenfalls keinen Zugang zum Bankensystem hätten, Mikrokredite. Damit das Start-up potenziellen Kunden einen personalisierten Darlehensvertrag anbietet, muss der Nutzer der App Zugriff auf zahlreiche Bereiche seines Smartphones gewähren und Einblick in seine Nutzerhistorie beim beliebten mobilen Zahlungsanbieter *M-Pesa*[192] eröffnen (Siegrist 2016).[193]

Zu dem Erkenntnispotenzial sozialer Netzwerke gesellen sich immer häufiger Technologien der Quantified-Self-Bewegung hinzu, die das individuelle Verhalten der Verbraucher messen. Wearables, die als Fitness- oder Lifestyle-Produkt eine wachsende Konjunktur erfahren, sind bspw. sehr attraktive Datenquellen für Krankenkassen. So kooperiert etwa die *AOK Nordost* mit dem e-Health-Anbieter *dacadoo* (Friedrichs 2013). Zahlreiche Krankenversicherungen, wie die Schweizer *Helsana*, bieten ihren Versicherten für private Zusatzversicherungen Rabatte – auch Geldzahlungen – an, wenn sie ihren Gesundheitszustand mittels App und Schrittzähler überwachen lassen (Möckli 2017). Der amerikanische Lebensversicherer *John Hancock* verlangt als Bestandteil seiner Policen sogar, dass seine Kunden Fitness-Tracker benutzen (Krohn und Lindner 2018).

Überbordenden Auswüchsen im Umgang mit Gesundheitsdaten schiebt das deutsche System der gesetzlichen Krankenversicherung mit seinem Solidarprinzip zwar einen Riegel vor: Für Mitgliedschaftsbedingungen und Versicherungsleistungen statuiert es engmaschige Vorgaben.[194] Für Versicherungssegmente, die nicht solidarisch, sondern rein privatwirtschaftlich organisiert (und nicht dem Ideal einer Vollversorgung verschrieben) sind, weitet sich der Handlungskorridor jedoch. Tracker-Tarife sind dort auf dem Vormarsch.[195]

Dass es sich für beide Seiten monetär auszahlen kann, nutzergenerierte Daten zu personalisieren, illustrieren nicht zuletzt Telematik-Tarife von Kfz-Versicherungen. Sie erfreuen sich ebenfalls nicht ohne Grund wachsender Beliebtheit (Krempl 2017): Wer nachweisbar risikoarm Auto fährt, kann mit Beitragssenkungen rechnen – dafür erfasst die Versicherung das Fahrverhalten (z. B. die Beschleunigung und das Bremsverhalten) minutiös.

Wie detailscharf die Einblicke in das Privatleben der Nutzer sind, die eine Kombination verschiedener Datenquellen ermöglichen, machen sich viele Nutzer nicht bewusst: Soziale Netzwerke, Wearables und die Standortdaten des Smartphones begleiten den Nutzer in guten wie in schlechten Zeiten – bei der Arbeit, in der Freizeit und im Urlaub.[196] Aus dem digitalen Fußabdruck, den der Einzelne dort hinterlässt, können algorithmische Systeme vielfach

---

[191] Die Ergebnisse empirischer Untersuchungen legen bspw. nahe, dass Personen, die viele SMS schreiben, Schulden zuverlässiger zurückzahlen; Siegrist 2016.
[192] In Kenia nutzt mehr als die Hälfte der Bevölkerung die App. Hinter ihr steckt der marktmächtige Akteur *Safaricom*; Schlenk 2018.
[193] „*Loan decisions are based on many pieces of information, including income, repayment of other loans, M-Pesa usage, and other information. Users provide us this information by using the app and filling out our survey, and then our software builds a personal credit profile.*“, https://talasupport.zendesk.com/hc/en-us/articles/360022069711-How-do-you-decide-if-someone-is-approved-for-a-loan- (Download 11.11.2019).
[194] Namentlich im Fünften Buch des Sozialgesetzbuchs (Zweites Kapitel: Versicherter Personenkreis [§§ 5 ff. SGB V] sowie Drittes Kapitel: Leistungen der Krankenversicherung [§§ 11 ff. SGB V]). Die Regelungen sind vom Solidarprinzip durchdrungen; dazu bspw. Quaas et al. 2018: § 2 Verfassungs- und europarechtliche Vorgaben, Rn. 68 ff.
[195] Dass davon ein ökonomischer Druck ausgehen kann, Gesundheitsdaten preiszugeben, hat die hessische Justizministerin *Eva Kühne-Hörmann* gar jüngst zu dem Vorschlag veranlasst, Self-Tracking-Tarife zu verbieten (Kühne-Hörmann 2019).
[196] Sogar aus der Häuserfront von *Google-Street-View*-Aufnahmen lassen sich mithilfe moderner Technologien Rückschlüsse darauf ziehen, mit welcher Wahrscheinlichkeit die jeweiligen Bewohner in einen Autounfall verwickelt

ein präziseres Persönlichkeitsbild einer Person zeichnen, als dies nahestehenden Angehörigen möglich wäre – etwa mit Blick auf die Faktoren „politische Einstellung“, „Drogenkonsum“ oder „körperliche Gesundheit“ (Youyou, Kosinski und Stillwell 2015: 1038).

Dass es möglich ist, Menschen digital zu durchleuchten, weckt auch bei solchen Akteuren Neugierde, an die der Nutzer nicht unbedingt denkt, wenn er die Datensilos der digitalen Welt befüllt. So mancher Arbeitgeber würde sicher gerne in den privaten Instagram-Kanal seines Mitarbeiters hineinlugen oder dessen aktuelle GPS-Position überprüfen, um herauszufinden, ob er am Rosenmontag wirklich krank oder doch eher mit der Narrenkappe auf dem lokalen Fastnachtsumzug unterwegs war. Für eine Berufsunfähigkeitsversicherung könnten wiederum Äußerungen oder Bilder in sozialen Medien interessant sein, die auf nicht angegebene Vorerkrankungen schließen lassen.

Doch wer darf auf welche Social-Media-Daten zu welchen Zwecken zugreifen? Aus rechtlicher Perspektive entspinnen sich rund um die Daten(aus)lese in sozialen Netzwerken zahlreiche Fragen.

8.2 Methoden zur Analyse des Informationsstroms in sozialen Netzwerken

Ein zentrales technisches Werkzeug, um nutzergenerierte Inhalte sozialer Medien systematisch zu beobachten, zu filtern und auszuwerten, ist „Social Media Monitoring“: Die Methode leitet aus dem Echolot sozialer Netzwerke Signale ab und richtet daran den individuellen Handlungskurs ihres Nutzers aus (Martini 2016b: 311).[197] Social Media Monitoring macht sich dabei den Umstand zunutze, dass soziale Netzwerke den Drang des Einzelnen befriedigen, sich selbst zu inszenieren: Sie erweitern die Kommunikationsmöglichkeiten der Nutzer breitenwirksam und legen das digitale Verhalten zugleich unter eine Glocke der Beobachtung (a. a. O.: 357 f.). Unternehmen steht dafür eine Reihe professioneller Instrumente zur Verfügung.

8.3 Wie gelangt ein Unternehmen an Daten aus sozialen Medien?

Die Datenwälder sozialer Netzwerke systematisch zu durchforsten, gehört in vielen Firmen unterdessen zum Standardrepertoire der Marketingabteilung. Sie nutzen die Informationen zur Marktforschung und setzen das Kommunikationspotenzial sozialer Netzwerke als strategischen Rückkanal der Unternehmenskommunikation ein, um die Strahlkraft und Wirkmacht ihrer Marke durch ein virales Marketing zu stärken (Martini 2016b: 315).

Die unterschiedlichen Analyseelemente greifen vorrangig auf die Inhalte, Verbindungen und Präferenzen zu, die Nutzer im Netz teilen oder als Datenspuren hinterlassen. Hinzu kommen Merkmale wie Alter, Geschlecht, Wohnort, Qualifikation oder Arbeitgeber. Daraus lassen sich dann mittelbar Rückschlüsse auf persönliche Eigenschaften wie Offenheit, Lebenszufriedenheit, Neurotizismus, Glaube an Sternzeichen oder politische Einstellungen ziehen (Rosenberg, Confessore und Cadwalladr 2018).[198]

---

sein werden. Studien haben eine signifikante Korrelation zwischen dem Wohnsitz und der Unfallhäufigkeit ans Tageslicht befördert; Kita und Kidziński 2019. Auf dieser Grundlage lassen sich perspektivisch auch die Risikomodelle von Autoversicherern optimieren; Szentpetery-Kessler 2019.

[197] Geläufig ist auch der Begriff „Data Harvesting“ bzw. „Social Media Harvesting“. Auch er beschreibt im Grunde nichts anderes als das automatisierte (und unauffällige) Sammeln und Speichern personenbezogener Daten (in sozialen Netzwerken), um sie anschließend gezielt analysieren zu können; Liang und Zhu 2017: 1. Im Kontext von *Facebook* und *Cambridge Analytica* siehe Nic Lochlainn 2018.

[198] Vgl. auch ein Patent, mit dem *Facebook* seine Nutzer in sozioökonomische Klassen einteilt, https://www.freshpatents.com/-dt20180201ptan20180032883.php (Download 11.11.2019).

Die Wege, auf denen Unternehmen an Daten aus sozialen Netzwerken gelangen können, sind vielfältig. Möchte etwa eine Bank oder Versicherung auf nutzergenerierte Daten aus dem Web 2.0 zugreifen, um mit ihrer Hilfe personalisierte Angebote für ihre Kunden zu stricken, kann sie sich die Daten im Grundsatz auf zwei Wegen verschaffen: Sie kann diese entweder über allgemein zugängliche – also offene – Quellen recherchieren (Abschnitt 8.3.1) oder auf Schnittstellen und sonstige Servicekanäle der Anbieter zurückgreifen (Abschnitt 8.3.2).

8.3.1 Datenakquise über allgemein zugängliche Quellen

Für die Datenanalyse stehen verschiedene Web-Crawler bereit, die das Netz auf öffentlich verfügbare Informationen zu Personen, Marken und Suchbegriffen durchscannen. Die Computerprogramme können dabei auf die Indexierung in Suchmaschinen zurückgreifen oder die Web-Feeds sozialer Netzwerke nutzen, um im Informationsstrom des World Wide Web zu fischen.

8.3.2 Zugriff über Schnittstellen sozialer Netzwerke, Apps und sonstige Servicekanäle

Viele Unternehmen setzen ihre *Facebook*-Fanpage als Servicekanal ein, um Informationen über ihre Kunden zu gewinnen. Wer einer *Facebook*-Fanpage „folgt“, abonniert nicht nur die dort dargestellten Inhalte. Er gibt darüber hinaus Nutzerdaten preis, die *Facebook* den Betreibern anonymisiert zur Verfügung stellt (dazu bspw. Martini und Fritzsche 2015: 9). Auf dieser Grundlage können diese ihre Außendarstellung evaluieren, optimieren und personalisieren.

Innerhalb des Ökosystems der Plattformbetreiber können interessierte Unternehmen den Nutzern auch eigene Apps zur Verfügung stellen. Davon machen viele Drittanbieter rege Gebrauch (so geschehen bei „thisisyourdigitallife“, siehe Abschnitt S. 63). Sie nutzen *Facebook* als Distributionskanal für ihre Angebote. Persönlichkeitstests oder Spiele, die sie in das soziale Netzwerk integrieren, vermitteln ihnen im Gegenzug Erkenntnisse über abgefragte (und freiwillig angegebene) Eigenschaften der Nutzer. Zusätzlich können sie auch auf Profilinformationen der Teilnehmer sowie auf deren Verbindungen zu anderen Personen zugreifen. Plattformbetreibern wie *Facebook* spült das wiederum neue Daten in ihren Auswertungspool. Das größte soziale Netzwerk behält sich in seinen Plattformrichtlinien bspw. vor, die Datensätze, die Drittanbieter gesammelt bzw. weiter verfeinert haben, zu kommerziellen (insbesondere Werbe-)Zwecken zu nutzen[199] – und profitiert so mittelbar davon, dass es die Datenweitergabe zulässt.

Damit ein Unternehmen via *Facebook* an Nutzerdaten gelangt, um sie entweder selbst zu nutzen oder an Dritte weiterzugeben, stehen ihm zahlreiche weitere technische Instrumente offen. Sie reichen von der Methode, als Drittanbieter-App den *Facebook*-Login zur Authentifizierung („Single Sign On“) zu nutzen, über aktive Partnerschaften mit Unternehmen, an die *Facebook* Nutzerdaten weitergibt, bis hin zu Kooperationen mit Social-Media-Monitoring-Anbietern wie *brandwatch*. Auf diese Weise kann bspw. eine Bank technisch die Programmierschnittstelle eines sozialen Netzwerks dafür nutzen, relevante Informationen über (via Klarnamen registrierte) Nutzer zu erlangen, um sie in maßgeschneiderte Angebote einfließen zu lassen.

8.4 Grundrechtliche Rahmenbedingungen

Wer sich in die Öffentlichkeit eines sozialen Netzwerks begibt und dort persönliche Informationen preisgibt, gibt dadurch nicht seine verfassungsrechtlich verbürgte Freiheit auf, selbst zu bestimmen, innerhalb welcher Grenzen er persönliche Sachverhalte offenbart und (weiter-)verwendet (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bzw. Art. 8

[199] 7.1. und 7.8. der *Facebook* Plattformrichtlinien, https://developers.facebook.com/policy/?locale=de_DE (Download 11.11.2019).

Abs. 1 GRCh[200]; Art. 16 Abs. 1 AEUV[201]). Er macht von seinem Grundrecht[202] vielmehr in spezifischer Weise Gebrauch:[203] Er entfaltet seine Persönlichkeit nicht, indem er Dritte ausgrenzt, sondern indem er andere Personen bewusst an Informationen aus seiner Privatsphäre teilhaben lässt (Martini 2016b: 321; Schulz und Hoffmann 2010: 134). Das Grundrecht verbürgt gerade auch die Freiheit, die eigene Privatheit durch selbstbestimmtes Handeln zu gefährden.

Wer die allgemeine Öffentlichkeit sucht, gibt zu erkennen, dass er eine Information nicht für vollumfänglich vertraulich hält: Er ist mit dem Datenzugriff auf die Daten einverstanden und bereit, sie mit einem unbestimmten Personenkreis zu teilen.[204] Wer sich dann gegenüber Dritten auf die Privatheit der Information beruft, setzt sich zum eigenen Verhalten in Widerspruch (Martini 2016b: 322).

Umgekehrt gilt aber auch: Wo Selbstbestimmung zur Fiktion wird, weil der Betroffene bspw. uninformiert und unbewusst gehandelt hat oder weil Datenverarbeitungsprozesse für ihn nicht erkennbar sind, verlangt die grundrechtliche Schutzpflicht dem Staat angemessene regulatorische Maßnahmen ab (vgl. Art. 1 Abs. 1 S. 2 GG: „Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt"). Sie verdichtet sich umso stärker zu einem Handlungsgebot, je höher das Risiko und der zu erwartende Schaden für die Persönlichkeitsentfaltung des Betroffenen sind und je weniger er (z. B. als Jugendlicher) dieses Risiko und den möglichen Schaden einzuschätzen vermag.

8.5 Datenschutzrechtliche Zulässigkeit

Nicht jede Spielart der Informationsflussanalyse in sozialen Medien ist datenschutzrechtlich sensibel. Greift sie auf *anonymisiert-aggregierte Massendaten* zurück – stellt sie bspw. allgemeine Nutzungsstatistiken her, um die Beliebtheit eines Produktes im Kommunikationsstrom nachzuzeichnen –, setzt die Datenschutz-Grundverordnung (DS-GVO) dem keine Grenzen: Da anonymisierten Daten der Personenbezug fehlt, greift das normative Regime des EU-Datenschutzrechts nicht. Datenschutzrechtlich sensibel ist dort nur die vorgelagerte, personenbezogene Daten*erhebung* in sozialen Netzwerken (Martini 2016b: 353).[205]

Anonymisierung ist aber an hohe Voraussetzungen geknüpft. Sie setzt voraus, dass ein Datum nach allgemeinem Ermessen keinen direkten oder indirekten Rückschluss auf die natürliche Person mehr zulässt, die hinter ihm steht

[200] Die Abkürzung steht für „Charta der Grundrechte der Europäischen Union".
[201] „AEUV" ist der „Vertrag über die Arbeitsweise der Europäischen Union".
[202] Die Grundrechte verstehen sich in ihrer Grundfunktion in erster Linie als Instrument, den Einzelnen vor *staatlichen* Eingriffen in seine Freiheitssphäre abzuschirmen. Sie entfalten deshalb keine *unmittelbare Wirkung* zwischen Privaten – und damit auch nicht im Verhältnis zwischen dem Anbieter eines sozialen Netzwerks und dessen Nutzer. Das Wertesystem, das die Grundrechte etablieren, wirkt aber *mittelbar* (z. B. über zivilrechtliche Generalklauseln, wie § 242 BGB [„Treu und Glauben"]) in die gesamte Rechtsordnung hinein. Dadurch zeitigt es auch Auswirkungen im Verhältnis zwischen Unternehmen und Verbraucher. Zur mittelbaren Drittwirkung siehe insbesondere BVerfG, Beschluss vom 11.4.2018, NJW 2018, 1667 (1668, Rn. 33 ff.) – Stadionverbote (dazu Smets 2019: 34; Weinzierl 2018); jüngst explizit zu sozialen Netzwerken siehe BVerfG, Beschluss vom 22.5.2019, NJW 2019, 1935 (1936).
[203] BVerfG (1. Kammer des Ersten Senats), Beschluss vom 23.2.2007, NVwZ 2007, 688 (690) – Videoüberwachung öffentlicher Plätze; BVerfGE 120, 378 (399, Rn. 67) – automatisierte Kennzeichenerfassung.
[204] BVerfGE 120, 274 (344 f., Rn. 308) – Onlinedurchsuchungen.
[205] Der Europäische Gerichtshof (EuGH) sieht die Betreiber einer Fanpage ebenso wie eines Social Plug-ins (z. B. des „Facebook-Gefällt-mir-Buttons") jedoch in der Mitverantwortung (Art. 4 Nr. 7, Art. 26 Abs. 1 S. 1 DS-GVO) für die Datenverarbeitungsprozesse; vgl. EuGH, Urteil vom 5.6.2018, ECLI:EU:C:2018:388, Rn. 25 ff., 39 – Wirtschaftsakademie Schleswig-Holstein; EuGH, Urteil vom 29.7.2019, ECLI:EU:C:2019:629, Rn. 64 ff., 84 – Fashion ID. Zur gemeinsamen Verantwortlichkeit siehe auch Kunnert 2019: 257 ff.; Martini und Botta 2019: 251 f. sowie bereits Martini und Fritzsche 2015: 16.

(Art. 4 Nr. 1, ErwGrd 26 S. 3 ff. DS-GVO). In einer Welt ubiquitärer Datenverarbeitung genügen jedoch typischerweise bereits wenige Datenpunkte, um eine Person eindeutig reidentifizieren zu können. Eine wirksame Anonymisierung lässt sich unter diesen Bedingungen nur bedingt sicherstellen.

Erfolgt die Datenanalyse des Social-Media-Informationsstroms *ad personam* – will also ein Unternehmen insbesondere das persönliche Verhalten und die individuellen Präferenzen (bspw. eines *Influencers*) vermessen oder seine Erkenntnisse in ein personalisiertes Angebot einfließen lassen –, greift das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt des Art. 6 Abs. 1 DS-GVO. Wenn etwa der Social-Media-Crawler[206] eines Berufsunfähigkeitsversicherers auf den Eintrag eines Kunden stößt, der in einem Internetforum als „super_potato_83“ von seinen Depressionen berichtet, darf das Unternehmen diese Daten nur verarbeiten, wenn eine Verarbeitungsgrundlage seine Analyse deckt – sei es eine Einwilligung (Abschnitt 8.5.1), sei es ein gesetzlicher Erlaubnistatbestand (Abschnitte 8.5.2 und 8.5.3).

8.5.1 Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO)

Durch die Brille der informationellen Selbstbestimmung betrachtet, ist die Erlaubnis des Betroffenen die Goldrandlösung, um Dritten einen Zugriff auf seine Daten zu gestatten. Sie reicht aber nur so weit, wie die Entscheidung des Erklärenden auf informierter Grundlage erfolgt. Die betroffene Person muss dafür insbesondere wissen, „dass und in welchem Umfang sie ihre Einwilligung erteilt“ (ErwGrd 42 S. 2 DS-GVO). Eine Erklärung, die eine weitreichende Erlaubnis hinter unklaren Formulierungen oder im „Kleingedruckten“ versteckt, erfüllt diese Voraussetzungen nicht (Martini 2016b: 329; Schwartmann und Klein 2018: Rn. 17).

Ermächtigt der Diensteanbieter in seinen Allgemeinen Nutzungsbedingungen *Dritte* dazu, nutzergenerierte Kommunikationsinhalte auszulesen und sie aus dem spezifischen Verwendungskontext herauszulösen, muss er den Betroffenen darauf besonders aufmerksam machen. Denn wer eine Nachricht auf einer Plattform verbreitet, die nur nach Autorisierung zugänglich ist, geht in der Regel nicht davon aus, dass unbekannte Dritte, insbesondere Vertragspartner des sozialen Netzwerks, diese Inhalte analysieren und verwerten dürfen (Schreiber 2014: 35). Ein Nutzer willigt also nicht stillschweigend darin ein, dass unbekannte Dritte seine Kommunikation analysieren dürfen (dazu auch bspw. – insbesondere mit Blick auf das Kopplungsverbot – Martini und Botta 2019: 248 ff.).[207]

8.5.2 Für die Vertragserfüllung erforderlich (Art. 6 Abs. 1 UAbs 1 lit. b Var. 1 DS-GVO)

Auch ohne ausdrückliche Einwilligungserklärung darf ein soziales Netzwerk nutzergenerierte Daten an Unternehmen weitergeben, wenn dies erforderlich ist, um die Vertragspflichten zu erfüllen, die es gegenüber dem Nutzer eingegangen ist (Art. 6 Abs. 1 UAbs. 1 lit. b Var. 1 DS-GVO).

Die vertragliche Beziehung, die der Nutzer mit dem Anbieter eines sozialen Netzwerks eingeht, ist in erster Linie darauf gerichtet, an einer Plattform teilzuhaben, auf der die Mitglieder mit anderen Personen kommunizieren, sich informieren und sich selbst sowie Projekte, an denen sie beteiligt sind, darstellen können. Beide Seiten gehen dafür einen Servicevertrag des Geschäftsmodells „Dienste gegen Daten“ ein (vgl. Art. 3 Abs. 1 UAbs. 2 RL 2019/770): Um Werbetreibenden zu ermöglichen, ihre Angebote treffsicher an die gewünschte Zielgruppe zu adressieren, nutzt das soziale Netzwerk die personenbezogenen Daten seiner Nutzer auch dafür, ihre Interessen und Vorlieben zu vermessen. Im Gegenzug verzichtet es darauf, den Nutzern einen Geldbetrag dafür in Rechnung zu stellen, dass sie das soziale Netzwerk nutzen dürfen.

---

[206] Ein Social-Media-Crawler ist eine Software, die Daten sozialer Medien automatisiert auf Muster oder Inhalte durchsucht.

[207] Im Hinblick auf das *Urheberrecht* folgt die Rechtsprechung einer ähnlichen Linie: Das Landgericht Frankfurt hat jüngst entschieden, dass ein Nutzer, der ein Profilbild bei einer Plattform wie *Xing* einstellt, dadurch nicht darin einwilligt, dass Dritte das Bild per E-Mail in einem anderen Kontext (im Sinne des §§ 22, 23 Kunsturhebergesetz [KUG]) weiterverbreiten dürfen (LG Frankfurt, Urteil vom 26.9.2019, Az. 2-03 O 402/18).

Um einen solchen Vertrag – Zugang zu einem sozialen Netzwerk im Austausch für personalisierte Werbung, die das Angebot finanziert – zu erfüllen, ist es indes nicht erforderlich, dass das soziale Netzwerk zusätzliche Erkenntnisse über seine Nutzer an *Dritte* weitergibt (vgl. bspw. Martini und Botta 2019: 255) – weder nach einer typisierenden Betrachtung des Vertrags zwischen Plattformbetreiber und Nutzer noch bspw. nach *Facebooks*[208] konkreten Nutzungsbedingungen (vgl. zum Meinungsstand Engeler 2018: 57 f.). Ob die Verarbeitung „für die Erfüllung eines Vertrags […] erforderlich ist", bestimmt sich nämlich nicht danach, was der Anbieter des sozialen Netzwerks mit *Dritten* vereinbart hat. Entscheidend ist vielmehr ausschließlich, welche vertragliche Leistungspflicht ihn im Verhältnis zum *Nutzer* trifft.

Der Anbieter sozialer Netzwerke schuldet dem Nutzer, die Nachrichten anderer Mitglieder in der Kommunikationsinfrastruktur abzubilden und ihm Informationen aus seinem Freundes- und Interessenkreis anzuzeigen. Die Daten unbeteiligten *Dritten* zugänglich zu machen, gehört dazu gerade nicht – im Gegenteil: Ihn trifft vielmehr die Pflicht, diese Informationen vor dem Zugriff Dritter zu bewahren (vgl. § 13 Abs. 4 Nr. 3 TMG[209]: „Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass […] der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann").

8.5.3 Berechtigtes Interesse der privaten Stelle an einer Recherche in sozialen Netzwerken (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO)

Statt auf Schnittstellen oder Rahmenvereinbarungen mit Plattformanbietern zu setzen, um an die Daten potenzieller Kunden zu gelangen, kann sich ein Unternehmen auch selbst auf die Suche nach sprudelnden Informationsquellen begeben. Für neugierige Banken oder Versicherungen sind vor allem Informationen von Interesse, die sie via Suchmaschinen über Nutzer sozialer Netzwerke auffinden können oder die potenzielle Kunden innerhalb des Netzwerks selbst (etwa nur für *LinkedIn*-Nutzer) mit einem unbestimmten Personenkreis teilen. Unternehmen können technisch im Grundsatz zusätzlich auch dadurch an nutzergenerierte Kommunikationsinhalte gelangen, dass sie ihre Mitarbeiter mit ihren privaten Accounts (und ggf. der Hilfe eines Crawlers) als „Spürhunde" auf Plattformen entsenden.

Unternehmen, die „allgemein zugängliche Daten" verarbeiten, hatte das deutsche Datenschutzrecht bis zum Jahr 2018 noch mit klar formulierten Privilegien ausgestattet (Martini 2016b: 329 ff.): Ein Verantwortlicher durfte allgemein zugängliche personenbezogene Daten im Grundsatz uneingeschränkt verarbeiten.[210]

Die DS-GVO ist dagegen deutlich lakonischer. Sie kennt keine vergleichbar eindeutigen Vorschriften. Aus Art. 14 Abs. 2 lit. f DS-GVO lässt sich immerhin mittelbar eine Grundaussage ableiten: Die Vorschrift legt demjenigen, der Daten aus „öffentlich zugänglichen Quellen" verarbeitet, eine Unterrichtungspflicht auf. Das neue Datenschutzrecht schließt eine Verarbeitung solcher Daten mithin jedenfalls nicht kategorisch aus: Die Unterrichtungspflicht setzt denklogisch voraus, dass der Gesetzgeber es im Grundsatz für gestattungsfähig hält, öffentlich zugängliche Daten zu verarbeiten.

Obgleich der Unionsgesetzgeber für die Informationsauswertung sozialer Netzwerke keine spezifische Verarbeitungserlaubnis formuliert, hält er in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO immerhin eine Norm vor, an die Unternehmen insoweit normativ „andocken" können: Sie dürfen personenbezogene Daten verwerten, wenn dies erforderlich ist, um berechtigte – auch wirtschaftliche – Interessen zu verfolgen. Gegen diese Erlaubnis setzt sich das Privatheitsinteresse des Betroffenen nur dann durch, wenn es im Einzelfall schwerer als das unternehmerische Interesse wiegt, die Daten in ein personalisiertes Angebot einfließen zu lassen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO). Sind beide Interessen von gleichem Gewicht, darf der Verantwortliche die Daten verarbeiten (vgl. Martini und Kienle 2019: 240). Der Gesetzgeber gesteht dem Auswertungsinteresse des Unternehmens im Grundsatz also

---

[208] „Wir verkaufen keine deiner Informationen an irgendjemanden und werden das auch in Zukunft niemals tun.", https://www.facebook.com/privacy/explanation#sharing-partner-information (Download 11.11.2019).
[209] Die Abkürzung steht für „Telemediengesetz".
[210] § 14 Abs. 2 Nr. 5, § 28 Abs. 1 S. 1 Nr. 3, § 28 Abs. 3 S. 2 Nr. 1, § 29 Abs. 1 S. 1 Nr. 2, § 30 Abs. 2 Nr. 2, § 30a Abs. 1 S. 1 Nr. 2 BDSG a. F. Dazu Martini 2016b: 329 ff.

den Vorrang zu (Martini 2016b: 349). Das lässt sich aus dem Grundsatz-Ausnahme-Spiel der Vorschrift ableiten („sofern nicht […] überwiegen“).

Wie das Abwägungsergebnis im konkreten Fall ausfällt, hängt insbesondere davon ab, in welchem Zusammenhang die Daten ursprünglich erhoben wurden und wie eng die Verbindung zwischen der Informationsquelle und dem Auswertungszweck ist (vgl. Art. 6 Abs. 4 lit. a und b DS-GVO) – ebenso davon, wie schützenswert das Datum und derjenige ist, der es in ein Onlinemedium eingestellt hat.

Eine konkrete Wertentscheidung trifft insofern Art. 9 Abs. 2 lit. e DS-GVO: Er gestattet es den datenschutzrechtlich Verantwortlichen,[211] (sogar) besonders sensible personenbezogene Daten (z. B. Informationen über die Gesundheit, die ethnische Herkunft oder Religion) zu verarbeiten, wenn der Betroffene sie selbst „offensichtlich öffentlich gemacht“ hat. Daraus lässt sich *e contrario* eine generelle Wertaussage für die Analyse des Informationsstroms sozialer Netzwerke ableiten: Sind selbst besonders sensible Daten einer Verarbeitung zugänglich, sobald der Betroffene sie erkennbar eigenständig in das World Wide Web eingespeist hat, dann gilt dies *erst recht* bei weniger sensiblen Daten (also solchen, die nicht dem besonderen Schutz des Art. 9 DS-GVO, sondern dem allgemeinen Regime des Art. 6 DS-GVO unterfallen). An Daten, die der Betroffene offensichtlich selbst öffentlich macht, kann er deshalb generell kein überwiegendes Schutzinteresse für sich reklamieren. Er kann dann vernünftigerweise nicht erwarten und verlangen, dass Dritte diese Daten nicht zu anderen Zwecken weiterverarbeiten. Er muss mit einer Verarbeitung rechnen (vgl. auch ErwGrd 47 S. 1 und 4 DS-GVO). Denn wer öffentlich abrufbare Informationen eines *Facebook*-Profils oder *Twitter*-Accounts nutzt, macht von seiner grundrechtlich abgesicherten Informationsfreiheit (Art. 11 Abs. 1 S. 2 GRCh, Art. 5 Abs. 1 S. 1 Hs. 2 GG) Gebrauch. Er darf sich dann grundsätzlich auch durch Direktzugriff oder über Suchmaschinen ein Bild von relevanten Informationen machen (Martini 2016b: 337).

Für die Frage, ob Informationen „öffentlich“ sind, kommt es nicht darauf an, ob die Informationen dazu *bestimmt* sind, dass sie jedermann wahrnehmen kann. Entscheidend ist vielmehr, ob die Internetöffentlichkeit von der Kenntnisnahme der Inhalte (bei rechtmäßiger Nutzung) *tatsächlich* ausgeschlossen ist (dann sind die Daten nicht „öffentlich“) – oder ob jeder die Informationen ungehindert abrufen *kann*. Beschwert sich bspw. ein Tourist in einem öffentlichen *Facebook*-Post darüber, dass das *Hamam* (also das öffentliche Bad) seines Hotels während eines Türkeiurlaubs nicht benutzbar war, oder lobt er den Reiseveranstalter dafür, dass die Rennräder des Alpen-Hotels hervorragend gewartet waren, darf jedermann daraus Rückschlüsse auf die Urlaubspräferenzen und Hobbys dieser Person ziehen.[212]

8.5.3.1 Nicht autorisierte, d. h. nicht selbst öffentlich gemachte Informationen

Nicht alle personenbezogenen Daten, die jedermann zugänglich sind, will der Betroffene auch in jedem Fall dem Internetpublikum offenbaren. Das gilt etwa für Informationen, die Dritte über ihn ins Netz stellen, um sein Ansehen zu beschädigen (sog. *informationelle Gegenbilder*, vgl. Klas 2012: 57; Martini 2016b: 338). Man denke bspw. an das Nacktfoto, das der ehemalige Partner als Rache im Netz hochlädt, an ein Fake-Profil eines Prominenten, das ein notorischer Fan angelegt hat oder an die Veröffentlichung unautorisierter Gesprächsmitschnitte (Martini 2016b: 338). Liegen dem Verarbeitenden Anhaltspunkte dafür vor, dass ihm unautorisiert veröffentlichte Daten ins Schleppnetz gegangen sind, oder musste sich ihm dies aufgrund der Umstände aufdrängen, überwiegt regelmäßig das Privatheitsinteresse der betroffenen Person gegenüber dem Verarbeitungsinteresse des Unternehmens.

Gleiches gilt, soweit jemand von einer öffentlichen Information „mitbetroffen“ ist: Postet etwa eine Helferin der „Tafel“ ohne Rücksprache ein Selfie öffentlich auf Twitter, auf dem auch Personen erkennbar sind, die dort

---

[211] Nach dem Willen des Unionsgesetzgebers befreit die Vorschrift den Verantwortlichen nicht von den sonstigen Anforderungen an eine rechtmäßige Verarbeitung (ErwGrd 51 S. 5 DS-GVO). Er ist also insbesondere auch an das Erfordernis einer Verarbeitungsgrundlage in Art. 6 Abs. 1 DS-GVO rückgebunden. Art. 9 Abs. 2 lit. e DS-GVO ersetzt diese Voraussetzung also nicht.

[212] Dazu auch oben Abschnitt 5.3.2.3.

Lebensmittel abholen, kann sich eine Bank, die das Foto nutzen möchte, um die Kreditwürdigkeit einer Kundin zu beurteilen, für die Auswertung nicht ohne Weiteres darauf berufen, die abgebildete Person habe es (selbst) öffentlich gemacht.

8.5.3.2 Stufen der Vertraulichkeit: öffentliche, netzwerkinterne und auf einen bestimmten Personenkreis limitierte Informationen

So wie der Betroffene nicht jede Information, die sich im Internet findet, *selbst* öffentlich zugänglich gemacht hat, sind auch nicht alle im Internet abgelegten Daten *allgemein* zugänglich. Soziale Netzwerke und Internetforen schalten einem (unbegrenzten) Zugang zu ihren Seiten nämlich typischerweise ein Anmeldeerfordernis vor und beschränken den Zugang zu bestimmten Informationen auf individuell eingeladene Gruppenmitglieder.[213] Daten sozialer Netzwerke sind daher nur dann allgemein zugänglich, wenn ihre Abrufbarkeit *nicht* auf einen bestimmten Nutzerkreis, also eine individuell bestimmbare Personengruppe, beschränkt ist (Martini 2016b: 337 m. w. N.).[214] Macht jemand seine Paragliding-Bilder nur einer netzwerkinternen Teilöffentlichkeit, insbesondere seinen „Freunden", zugänglich, schlägt diese erkennbare Zugangsschranke auch auf die Abwägung zwischen Privatheits- und Auswertungsinteresse durch. Eine Versicherung, die an die Bilder des Gleitschirm-Abenteuers gelangt, darf die Information daher datenschutzrechtlich nicht verarbeiten, um etwa den Tarif einer Unfallversicherung zu erhöhen, weil der Kunde Extremsportarten ausübt. Weder sind die Daten allgemein zugänglich noch hat der Betroffene sie „öffentlich gemacht".

Das Einverständnis, dass Dritte im Internet veröffentlichte Informationen verwenden, reicht nach dem konzeptionellen Zuschnitt des Grundrechts auf Schutz personenbezogener Daten (Art. 8 Abs. 1 GRCh) nur so weit, wie der Grundrechtsträger es auch tatsächlich erteilt hat. Er kann es auch selektiv erteilen, insbesondere auf bestimmte Personen beschränken.[215] Nicht jeder, der auf eine veröffentlichte Information faktisch zugreifen *kann*, darf diese daher in rechtlich zulässiger Weise für eigene Zwecke verwenden. Er darf es jedenfalls dann nicht, wenn der Betroffene ein *schutzwürdiges Vertrauen in die Integrität seines Kommunikationspartners* genießt. Das Bundesverfassungsgericht vertritt für das nationale Recht insoweit jedoch eine restriktive Haltung: In Internetforen sei generell nicht zu erwarten, dass hinter einem Pseudonym wirklich die vorgebliche Privatperson steckt – und nicht etwa eine staatliche Ermittlungsbehörde. Ausgehend von der Annahme, dass man im Cyberspace „*die Identität seiner Partner nicht kennt oder deren Angaben über sie jedenfalls nicht überprüfen kann",*[216] hält das Gericht die Kommunikationspartner daher für nicht schutzwürdig. Überträgt man diese (zu staatlichen Ermittlungen ergangene) Rechtsprechung auch auf private Stellen im unionsrechtlichen Grundrechtsregime, ist das Recht auf Schutz personenbezogener Daten nicht beeinträchtigt, wenn ein Unternehmen ein Pseudonym nutzt, um an persönliche Daten zu gelangen, die ein Betroffener mit einem weit gesteckten Benutzerkreis teilt. Darunter fallen dann etwa

---

[213] Die – unterdessen obsolete – Legaldefinition des § 10 Abs. 5 Satz 2 BDSG a. F. („Allgemein zugänglich sind Daten, die jedermann […] nutzen kann") differenzierte nicht danach, ob eine Anmeldung erforderlich ist („sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts"). Die Vorschrift meinte damit in der Sache aber nur Konstellationen, in denen eine Anmeldung im Grundsatz jedermann offensteht. Erkennbare Zugangsbeschränkungen waren zu respektieren.

[214] Ein ähnliches Grundverständnis legt (wenn auch in ganz anderem Schutzkontext und mit völlig anderem normativen Hintergrund) § 19a Urheberrechtsgesetz (UrhG) mit seinem Topos der „öffentlichen Zugänglichmachung" an: Er versteht darunter jede Maßnahme, die den Mitgliedern der Öffentlichkeit, also jedem, der nicht mit dem Verwerter des Werkes durch persönliche Beziehungen verbunden ist, unabhängig von Ort und Zeit den Zugriff auf ein Werk eröffnet (BGH, Urteil vom 29.4.2010, GRUR 2010, 628 [629, Rn. 19] – Vorschaubilder Google).

[215] Die Reichweitenlimitierung muss dann allerdings hinreichend klar zum Ausdruck kommen. Denn ein Vertrauen darin, vor einem Zugriff Dritter geschützt zu sein, kann nur geltend machen, wer zu erkennen gibt, dass seine durch Verlautbarung gelebte öffentliche Privatheit ausschließlich darauf zielt, dass nur bestimmte oder in bestimmter Weise qualifizierte Dritte sie wahrnehmen – indem er etwa als Nutzer sozialer Netzwerke die Datenschutzvoreinstellung entsprechend konfiguriert oder Inhalte nur für einen bestimmten geschlossenen Benutzerkreis veröffentlicht. Bei *Facebook* kann der Nutzer etwa Nachrichten mit einer oder mehreren Personen austauschen, Informationen in Gruppen posten, die ihrerseits durch eigene Zugangshürden gesichert sein können; er kann im Profil oder der „Timeline" aber auch die Sichtbarkeit der jeweils geposteten Information individuell einstellen.

[216] BVerfG, Urteil vom 27.2.2008, BVerfGE 120, 274 (346, Rn. 311) – Onlinedurchsuchungen.

auch Informationen, die eine Person netzwerköffentlich (z. B. für alle *LinkedIn*-Nutzer) oder in einem Internetforum verbreitet, für das man sich vorher anmelden muss. Der Betroffene könnte sich dann jedenfalls nicht auf ein grundrechtlich geschütztes Vertrauen berufen, wenn ein Unternehmen solche Datenquellen für seine personalisierten Angebote nutzt.

In einer digitalisierten Kommunikationswelt überzeugt diese Einschätzung des Bundesverfassungsgerichts jedoch nicht vollständig. Selbst wenn die Identität des Gegenübers nicht überprüfbar ist, darf der Betroffene jedenfalls im Rahmen einer Individualkommunikation grundsätzlich darauf vertrauen, dass sein Kommunikationspartner (z. B. im Rahmen eines *Facebook*-Chats oder bei einer Kontaktaufnahme via *Tinder*) seine Vertrauenserwartung, mit einer Privatperson zu kommunizieren, nicht enttäuscht. Das Einverständnis zur Kommunikation bezieht sich bei personengebundener, etwa via Chat erfolgender, Kommunikation in der Regel ausschließlich auf diejenige natürliche Person, die vorgeblich hinter der Onlineidentität steckt – nicht auf jeden, der dieses Profil nutzt oder nutzen kann (Schulz und Hoffmann 2010: 12).

Bei genauerem Hinsehen zeigt sich also: Die Rechtsordnung erkennt im Rahmen der Abwägung zwischen dem Privatheitsinteresse und dem Auswertungsinteresse Dritter (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO) unterschiedliche Abstufungen in dem Vertraulichkeitsniveau der Internetkommunikation an. Das Datenschutzrecht trägt damit letztlich auch den veränderten Rahmenbedingungen Rechnung, unter denen Informationsverarbeitung im digitalen Zeitalter stattfindet: Anders als in der Ära gedruckter Zeitungen und öffentlicher Bekanntmachungen teilen Internetnutzer persönliche Informationen heute mit anderen Personen auf vielfältige Weise, zunehmend häufig und mit unterschiedlichen Vertrauensniveaus.

8.5.3.3 Grenzen der Neugier: Informationen, die ein Unternehmen unter Verstoß gegen die Nutzungsbedingungen oder unter einer Legende erlangt; Zweckbindung

Beschränkt nicht allein der *Nutzer*, sondern auch der *Diensteanbieter* in seinen Nutzungsbestimmungen den Kreis möglicher Teilnehmer, so spielt auch dieser Umstand in die Interessenabwägung hinein. Behält ein soziales Netzwerk die Anmeldung bspw. ausschließlich natürlichen Personen vor, die ein Klarnamenprofil verwenden, so steht demjenigen, der sich den Zugang regelwidrig – etwa durch ein Pseudonym, das die Identität einer natürlichen Person suggeriert – verschafft, kein überwiegendes Interesse daran zur Seite, die Daten für seine eigenen Zwecke zu verwerten.[217] Trotzt jemand einer anderen Person sensible Informationen nur dadurch ab, dass er ihr Vertrauen in den Kommunikationspartner ausnutzt, setzt sich sein Verwertungsinteresse in der Abwägung des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht durch. Die Rechtsordnung erkennt dieses Interesse regelmäßig nicht als „berechtigt“ an. Ein Nutzer, der eine Nachricht (nur) an die Gemeinschaft eines sozialen Netzwerks (Netzwerköffentlichkeit) kommuniziert, gibt dadurch insbesondere noch nicht zu erkennen, dass er mit *jeglicher* Weiterverarbeitung einverstanden ist: Er muss sich weder auf eine Kenntnisnahme der allgemeinen (Internet-)Öffentlichkeit bzw. eines jeden Dritten, insbesondere staatlicher Stellen, noch auf jede Form der Weiterverarbeitung und Verschneidung mit anderen Daten einstellen (Martini 2016b: 322; Schulz und Hoffmann 2010: 10).

Während *allgemein zugängliche Daten* für eine Vielzahl von Zwecken zur Verfügung stehen (schließlich hat der Betroffene ihnen bei der Veröffentlichung gerade keine Zweckbestimmung mit auf den Weg gegeben), greift für *sonstige Daten* der Zweckbindungsgrundsatz des Art. 5 Abs. 1 lit. b DS-GVO voll durch: Sie dürfen grundsätzlich nicht für solche Zwecke Verwendung finden, die mit der ursprünglichen Zweckbestimmung inkompatibel sind. Das gilt insbesondere für besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) sowie dann, wenn die Weiterverarbeitung nachteilige Folgen für die betroffene Person zeitigt oder wenn der Verarbeitende die Daten aus ihrem ursprünglichen Kontext herauslöst (Art. 6 Abs. 4 lit. b, c, d DS-GVO). Dann ist die Weiterverarbeitung nur zulässig, wenn eine spezielle Verarbeitungsgrundlage die Zweckänderung legitimiert (Art. 6 Abs. 4 DS-GVO).

---

[217] Ebenso für den Parallelfall des § 19a UrhG BGH, Urteil vom 29.4.2010, GRUR 2011, 56 (59, Rn. 30) – Session ID.

Eine Zweckänderung hat der Gesetzgeber indes nur für wenige Ausnahmetatbestände zugelassen (siehe § 24 BDSG). Social-Media-Daten, die sich hinter erkennbaren Zugangsbeschränkungen – insbesondere vor dem Zugriff durch einzelne Unternehmen – verbergen, welche nicht jedermann in rechtlich zulässiger Weise überwinden kann, sind einer Drittanalyse dadurch grundsätzlich entzogen. Stößt etwa der Sachbearbeiter einer Hausratsversicherung unter einem Pseudonym auf *Facebook* in der geschlossenen Gruppe „Grillfans Heppenheim" darauf, dass ein Kunde regelmäßig auf dem Balkon ausufernde Grillpartys veranstaltet, und setzt er deshalb die eigentlich anstehende Beitragssenkung aus, kann er die Datenverarbeitung nicht auf ein überwiegendes Nutzungsinteresse stützen.

8.5.4 Information des Betroffenen über die Datenquellen

Selbst wenn eine Versicherung sich nutzergenerierte Daten aus sozialen Netzwerken verschaffen *darf* (siehe Abschnitte 8.5.1 bis 8.5.3*)*, um daraus ein personalisiertes Angebot zu stricken, befreit sie das nicht von ihrer Pflicht, Transparenz über ihr Handeln herzustellen. Sie muss den potenziellen Kunden im Grundsatz aktiv darüber informieren, aus welcher Quelle sie seine Daten geschöpft hat und ob der Datensatz ggf. öffentlich zugänglichen Quellen entspringt (Art. 14 Abs. 1 i. V. m. Abs. 2 lit. f DS-GVO). Diese Unterrichtungspflicht formt den Transparenzgrundsatz des Art. 5 Abs. 1 lit. a DS-GVO aus. Er nimmt den Verantwortlichen in die Pflicht, Daten in einer Weise zu verarbeiten, die für die betroffene Person nachvollziehbar ist.

Auch das datenschutzrechtliche Gebot der Transparenz gilt jedoch nicht vorbehaltlos: Die Informationspflicht entfällt insbesondere dann, wenn es sich als unmöglich oder unverhältnismäßig erweist, die Information zu erteilen – etwa weil eine Vielzahl von Personen betroffen ist (Art. 14 Abs. 5 lit. b DS-GVO).[218] Aber auch dann hat der Einzelne das Recht, eine Auskunft darüber zu verlangen, ob und ggf. welche personenbezogenen Daten jemand über ihn verarbeitet hat (Art. 15 Abs. 1 DS-GVO). Davon wird der Nutzer freilich nur dann Gebrauch machen, wenn er einen Verdacht hegt, überhaupt von der Datenverarbeitung einer bestimmten Stelle betroffen zu sein.

8.6 Zusammenfassung des rechtlichen Status quo

„Zum ersten Mal haben wir ein Mikroskop, mit dem wir nicht nur das Sozialverhalten auf einem sehr feinen, bisher unerreichten Niveau untersuchen, sondern auch Experimente durchführen können, denen Millionen von Nutzern ausgesetzt sind" – mit diesen Worten beschrieb der Chef des *Data Science Teams* von *Facebook* die Potenziale des sozialen Netzwerks (Simonite 2012).

Dass sich ganze Wirtschaftszweige immer neugieriger auf die Suche nach den Datenspuren begeben, die jeder Nutzer in sozialen Netzwerken hinterlässt, verwundert deshalb nicht. Vor allem zwei Wege stehen Wirtschaftsakteuren offen, um an Informationen zu gelangen, die über eine reine Selbstauskunft potenzieller Kunden hinausgehen: Entweder fahnden sie selbst nach Informationen, die Nutzer bei *Twitter, Instagram* und Co. durch Veröffentlichung jedermann zugänglich gemacht haben – oder sie bedienen sich via Schnittstelle der Plattformanbieter und der Services von Drittanbietern direkt an der reichhaltigen Auswahl aus dem Datenreservoir sozialer Netzwerke.

Das Vertragsverhältnis zwischen Nutzer und sozialem Netzwerk gestattet es Plattformanbietern jedoch grundsätzlich nicht, personenbezogene Daten an Dritte weiterzugeben. Denn eine solche Form des Datenhandels ist in der Regel nicht erforderlich, um die Vertragspflichten gegenüber dem Nutzer einzulösen (Art. 6 Abs. 1 UAbs. 1 lit. b Var. 1 DS-GVO). Die Situation ändert sich, wenn sich das vertragliche Leistungsversprechen des Plattformanbieters gerade darauf richtet, Leistungen Dritter (z. B. Videodienste oder Arbeitsplatzangebote) einzubinden.

[218] Die Union und die Mitgliedstaaten dürfen darüber hinaus kraft Art. 14 Abs. 5 lit. c und Art. 23 DS-GVO durch gesetzliche Regelung Ausnahmen von der Informationspflicht etablieren.

Ein soziales Netzwerk kann sich die Datenweitergabe auch prinzipiell auf der Grundlage einer informierten und freiwilligen Einwilligung gestatten lassen. Dies muss für den Nutzer dann jedoch klar erkennbar sein, darf sich insbesondere nicht zwischen den Zeilen einer vorgefertigten Zustimmungserklärung verstecken. Andernfalls ist die Einwilligung nicht freiwillig im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. a i. V. m. Art. 4 Nr. 11 DS-GVO.

Auch ohne Einwilligung darf ein Unternehmen nutzergenerierte Daten eines potenziellen Kunden aus sozialen Netzwerken oder anderen Quellen dann verarbeiten, wenn es damit berechtigte (wirtschaftliche) Interessen verfolgt (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO). Es darf Informationen jedenfalls dann in ein personalisiertes Vertragsangebot einfließen lassen, wenn der Betroffene sie selbst „offensichtlich öffentlich gemacht" hat (i. V. m. Art. 9 Abs. 2 lit. e DS-GVO *a maiore ad minus*). Dabei kommt es nicht darauf an, ob die Information *dazu bestimmt* ist, dass sie jeder Internetnutzer wahrnehmen kann. Entscheidend ist also nicht, ob die Person, die ein Foto auf *Facebook* hochlädt, damit die Absicht verbindet, dass jeder das Bild mithilfe von Suchmaschinen auffinden und betrachten kann. Vielmehr ist maßgeblich, ob jeder die Informationen faktisch ungehindert abrufen *kann* – etwa weil die Sichtbarkeit aller Einträge auf der eigenen Pinnwand auf „öffentlich" gestellt ist. Verarbeitet ein Unternehmen solche Daten etwa für ein personalisiertes Angebot, muss es die betroffene Person dann aber grundsätzlich auch aktiv darüber informieren, aus welcher Quelle es seine Daten entnommen hat (Art. 14 Abs. 1 i. V. m. Abs. 2 lit. f DS-GVO).

Nicht für jedes Datum, das ein Nutzer in soziale Netzwerke eingespeist hat, überwiegt das unternehmerische Nutzungsinteresse aber das Privatheitsinteresse. Vielmehr kommt dem Schutzinteresse der betroffenen Person in der Regel dann ein höheres Gewicht zu, wenn eine Information für Dritte erst nach erfolgter Authentifizierung (etwa Eingabe eines Passworts) sichtbar oder nur für einen begrenzten Personenkreis (etwa die netzwerkinterne Teilöffentlichkeit oder eine geschlossene Gruppe) bestimmt ist. Auch wenn ein Nutzer seine Vertraulichkeitserwartung durch Voreinstellungen zur Privatsphäre zu erkennen gibt oder die Informationen von der Indexierung durch Suchmaschinen eindeutig ausschließt, will er üblicherweise nicht die Allgemeinheit adressieren (Martini 2016b: 355).

Darauf, dass ihr Interesse an der Datenverarbeitung schwerer wiegt als die Privatsphäre des Nutzers, können sich Unternehmen auch dann nicht berufen, wenn sie sich personenbezogene Daten im Datendschungel sozialer Netzwerke unter einer falschen Legende (d. h. etwa mit dem Profil einer anderen natürlichen Person) verschaffen oder indem sie Zugangsschranken umgehen. Ihr Interesse ist dann nicht mehr „berechtigt" im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Nicht alle Daten, die für denjenigen sichtbar sind, der sich bei einer Plattform „eingeloggt" hat, sind also im Ergebnis für Dritte auswertbar – sondern nur solche, die der Nutzer entweder einem bestimmten, abgrenzbaren Personenkreis (zu dem der Verarbeiter zählt) oder einem unbestimmten, nicht abgegrenzten Adressatenkreis zugänglich gemacht hat.

Das Grundrecht auf Schutz personenbezogener Daten (Art. 8 Abs. 1 GRCh) verwehrt es Verarbeitenden auch, Daten aus unterschiedlichen, allgemein zugänglichen Quellen systematisch zu einem *umfassenden Persönlichkeitsprofil* potenzieller Kunden zusammenzutragen.[219] Die Aussage des *Chief AI Scientist* bei *Facebook*, *Yann LeCun*, das Unternehmen treffe jeden Tag 200 Billionen Vorhersagen[220] (über das künftige Verhalten seiner Nutzer), präsentiert sich in diesem Lichte zwar als ein beeindruckender Beleg technischer Möglichkeiten. Er sollte der Gesellschaft aber vor allem ein Weckruf für einen effektiven Schutz der Grundrechte im Internet sein.

[219] Für das nationale Verfassungsrecht formulierte das BVerfG ein Verbot persönlichkeitsfeindlicher Katalogisierung (BVerfGE 65, 1 [48] – Volkszählung). Es gilt in ähnlicher Weise für das unionale Grundrechtsregime (Art. 8 i. V. m. Art. 1 GRCh).

[220] „That will help speed up the 200 trillion predictions and 6 billion translations Facebook does every day.", siehe https://twitter.com/ylecun/status/1115740807204679683?lang=en (Download 11.11.2019).

8.7 Rechtspolitischer Ausblick auf die Regulierung sozialer Netzwerke im Dienste des Schutzes der Privatsphäre

Die rechtlichen Fragen rund um den anschwellenden Informationsfluss in sozialen Netzwerken rufen nicht nur die Gerichte bei der Auslegung des geltenden Rechts auf den Plan. Sie treiben zusehends auch den Gesetzgeber um. Als Ausfluss seiner Schutzpflicht für die Grundrechte Betroffener und als Herzkammer der demokratischen Ordnung ist er dazu angehalten, nach maßgeschneiderten Lösungen zu suchen, welche die Rolle sozialer Netzwerke als Ort der Selbstinszenierung und öffentlicher Agora in der Demokratie gegen Missbrauch absichern.

8.7.1 Vorzüge einer (kostenpflichtigen) Alternative zu einem „Dienste gegen Daten"-Modell?

Je komplexer die technischen Abläufe und die ökonomischen Verflechtungen eines sozialen Netzwerks sind, desto weniger klar steht es dem durchschnittlichen Nutzer vor Augen, welche Konsequenzen sich damit verbinden, das Angebot in Anspruch zu nehmen. Einerseits wähnt er nicht ohne Weiteres, dass ein unterhaltsames Spiel oder ein lustiger Persönlichkeitstest als Vehikel dienen kann, um ihn auszuleuchten. Andererseits wird er sich durchaus fragen dürfen und müssen, warum das Angebot kostenlos ist und auf seine Profilinformationen zugreifen möchte. Bei nüchternem Blick auf das Geschäftsmodell sozialer Netzwerke verschließt sich dem Nutzer jedenfalls nicht die Erkenntnis, dass Werbung und Datenanalysen das Fundament dafür bilden, das Angebot wirtschaftlich betreiben zu können.

Birgt das Modell „Dienste gegen Daten" das Risiko, die Privatsphäre des Einzelnen zu gefährden, hat auf den ersten Blick eine Idee Charme: den Betreibern sozialer Netzwerke die Pflicht aufzuerlegen, Nutzern als Alternative ein (kostenpflichtiges) Dienstangebot anzubieten, das ohne Datensammlung und Werbung auskommt.[221] So konstruktiv und verlockend sich der Gedanke einer solchen persönlichkeitsschützenden Tarnkappe für *Facebook*-Nutzer auch präsentiert, so wenig ist jedoch gesichert, dass ein kostenpflichtiges Alternativangebot bei den Kunden auf hinreichende Resonanz stieße.[222] Denn das Konzept „Dienste gegen Daten" konnte sich gerade deshalb so gut im Markt entfalten, weil viele Menschen – nicht zuletzt die im internationalen Vergleich als besonders preisbewusst geltende „deutsche Seele" – lieber mit persönlichen Informationen als mit Geld zahlen. Wenn die Prämisse des sog. *Privacy Paradox* stimmt, dass die Preisbereitschaft für die eigene Privatsphäre im gelebten Alltag niedriger liegt als abstrakte Bekenntnisse zum Wert der Privatsphäre im Allgemeinen, steht nicht zu erwarten, dass Verbraucher ein zwar auswertungsfreies, dafür aber kostenpflichtiges Angebot besonders verlockend finden. Viele Menschen werden wahrscheinlich weiter mit Aufmerksamkeit statt mit Geld bezahlen wollen. Immerhin wäre es für datenschutzaffine Personen womöglich ein Gewinn, wenn sie eine Datenpreisgabe durch Geldleistung verhindern können. Ein solches monetär geprägtes Modell könnte aber auch eine soziale Spaltung begünstigen: Angemessener Privatsphärenschutz läuft dann im schlimmsten Fall Gefahr, zu einem Privileg finanziell besser gestellter Teile der Gesellschaft zu werden. Erforderlich wären deswegen (im Rahmen des wirtschaftlich Vertretbaren) zumindest Minderjährigen- und Sozialtarife.

8.7.2 Partizipation des Einzelnen an dem wirtschaftlichen Wert seiner Profildaten?

Immer mehr Menschen stellen sich die Frage, ob die ökonomische Rendite sozialer Netzwerke zwischen dem Betreiber und ihren Nutzern insgesamt fair verteilt ist. Immerhin hat jedes Profil eines sozialen Netzwerks einen substanziellen ökonomischen Wert, zu dem jeder Einzelne mit seinen Daten beiträgt. Grobe Schätzungen gehen für *Facebook*-Profile von einem Wert von etwa 50 Euro p.a. in Europa aus.[223]

---

[221] Manche lesen eine gesetzliche Pflicht zum datenschonenden Alternativangebot bereits jetzt aus Art. 7 Abs. 4 DS-GVO heraus (vgl. Ernst 2017: 112; Golland 2018: 133 f.). Diese Lesart überdehnt aber Wortlaut und Telos der Norm; siehe Martini und Botta 2019: 249 mit Fn. 63.

[222] Daneben wirft ein solches Abo-Modell einer zahlungspflichtigen Angebotsvariante die Frage auf, wie der *pretium iustum*, also der gerechte Preis, für die Nutzung eines sozialen Netzwerks zu ermitteln ist.

[223] Siehe https://de.statista.com/statistik/daten/studie/224878/umfrage/werbeumsaetze-von-facebook-pro-nutzer-nach-region/ (Download 11.11.2019).

Die Nutzer selbst an dem ökonomischen Wert ihrer Daten (z. B. durch eine „VG Soziale Netzwerke“) partizipieren zu lassen, mag als politischer Verteilungsmechanismus gerechtfertigt sein. Es setzt jedoch zugleich Anreize, die eigene Privatsphäre als ökonomisches Gut zu begreifen und auszubeuten. Das beschwört kontraproduktive Effekte herauf, die mit unserem gesellschaftlichen Modell der Privatsphäre nur bedingt kompatibel sind. Die eigenen personenbezogenen Daten als Wirtschaftsgut einzusetzen und dadurch zu kommerzialisieren, gerät namentlich in Konflikt mit unserer freiheitlich-egalitären Vorstellung davon, dass der freien Persönlichkeitsentfaltung ein Selbstwert (ohne wirtschaftliche Dimension) innewohnt.

Ein tauglicher Mittelweg kann darin bestehen, Werbetreibende, die von der digitalen Kommerzialisierung privater Daten profitieren, nicht nur *datenschutzrechtlich*, sondern *auch finanziell* stärker in die Mitverantwortung zu nehmen. Der Staat könnte und sollte die Erträge, die insbesondere Datenhändler aus der Weitergabe privater Daten erwirtschaften, mit Blick auf die gesellschaftlichen und individuellen Implikationen stärker abschöpfen, insbesondere höher als sonstige Geschäftsbeziehungen besteuern. Darüber hinaus sollte er alle Beteiligten noch stärker dazu verpflichten, Transparenz über Datenflüsse und Abschöpfungsprozesse herzustellen (Martini 2019a: 176 ff.). Die Nutzer sozialer Netzwerke sollten nicht nur im Grundsatz Einblick in die Profilbildungen und bereits vorgenommene Verhaltensvoraussagen über die eigene Person nehmen dürfen. Bewusste oder unbewusste Informations- und Kontrolllücken, die Firmen wie *Cambridge Analytica* ausnutzen können, gilt es zu schließen, insbesondere indem die Beteiligten ihre Vertragszwecke und Datenhandelsbeziehungen offenlegen.

8.7.3 Erweitertes Portabilitätsrecht

Der Wert sozialer Netzwerke bestimmt sich aus der Perspektive ihrer Nutzer zu einem maßgeblichen Anteil danach, wie viele *andere* User sich auf der Plattform tummeln. Soziale Netzwerke sind mit anderen Worten ökonomisch in besonderer Weise von Netzwerkexternalitäten geprägt (sog. *Lock-in-Effekte*). Das führt oftmals dazu, dass sehr gute Dienstangebote mit hervorragenden Privatsphäreeinstellungen solange verwaist und für den Einzelnen unattraktiv bleiben, wie sie nur eine geringe Resonanz in der Netzgemeinde erfahren.

Aus diesem Grund hat der Unionsgesetzgeber in Art. 20 DS-GVO ein besonderes Portabilitätsrecht aus der Taufe gehoben. Die rechtspolitisch erhofften Wanderungsbewegungen hin zu datenschutzfreundlichen Angeboten hat die Vorschrift aber noch nicht losgetreten. Das macht eine Zahl deutlich: Obwohl soziale Netzwerke wie *Pinterest, Youtube, Twitter* und *Snapchat* nennenswerte Marktanteile verbuchen können, hat der *Facebook*-Konzern mit einem weltweiten Marktanteil von 65,88 Prozent im Januar 2019 weiterhin eine beherrschende Stellung in dem relevanten Markt inne.[224] Womöglich ist die Zeit für eine abschließende Bewertung aber noch zu früh.

Ein denkbarer Anknüpfungspunkt, um die Markt-Macht-Spirale der großen sozialen Netzwerke zu entschleunigen, kann darin bestehen, das Portabilitätsrecht aus Art. 20 DS-GVO zu erweitern: Ebenso wie der Einzelne über verschiedene Netze hinweg mobil telefonieren kann, ist es prinzipiell vorstellbar (teilweise auch bereits in engen Grenzen technisch praktiziert)[225], aus jedem sozialen Netzwerk heraus andere soziale Netzwerke ansteuern zu können. Im Idealszenario kann der Bürger aus dem sozialen Netzwerk seines Vertrauens heraus mit Freunden und Bekannten, die sich auf anderen Plattformen bewegen, kommunizieren, ohne den Atem neugieriger Datenhändler im Nacken spüren zu müssen (vgl. auch Martini 2019a: 100).

Auch durch solche Maßnahmen sollte der Staat regulatorische Rahmenbedingungen dafür schaffen, dass die Nutzer ihre Persönlichkeit nicht kommerzialisieren, sondern effektiv schützen können. Sonst wird *Dave Eggers* dystopische Weissagung im Roman „The Circle“ eines Tages Realität: „Die Nachricht gehört dir nicht, selbst wenn sie über dich berichtet. [Sie] ist jetzt Teil der kollektiven Aufzeichnung“ (Eggers 2014: 178).

---

[224] Siehe https://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit/ (Download 11.11.2019).

[225] Für Messenger-Dienste ermöglicht etwa das Tool *Pidgin.im,* alle Nachrichten aus *Skype*, *ICQ*, *WhatsApp*, *WeChat*, *Signal* etc. in einer Oberfläche anzusteuern.

9 Literaturverzeichnis

Albes, Andreas (2018): Hunderte Gangs morden auf den Straßen: Chicago im Griff der Gewalt, Stern.de, 22.4.2018, https://www.stern.de/politik/ausland/chicago--eine-stadt-im-griff-der-gewalt---hunderte-gangs-morden-auf-den-strassen-7948800.html (Download 11.11.2019).

AlgorithmWatch gGmbH (2019): Automating Society. Taking Stock of Automated Decision-Making in the EU, Berlin.

Angwin, Julia, Jeff Larson, Surya Mattu und Lauren Kirchner (2016): Machine Bias, ProPublica, 23.5.2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (Download 11.11.2019).

Asher, Jeff, und Rob Arthur (2017): Inside the Algorithm That Tries to Predict Gun Violence in Chicago, The New York Times, 13.6.2017, https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html?searchResultPosition=1 (Download 11.11.2019).

Ashley, Kevin D. (2017): Artificial Intelligence and Legal Analytics. New Tools for Law Practice in the Digital Age, Cambridge.

Azavea Inc. (2015): HunchLab: Under the Hood. Whitepaper. https://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf (Download 11.11.2019).

Becker, Ulrich (2019): Grundrechte der Arbeit in Europa – zu Funktionen, Verschränkungen und Konfliktlinien vernetzter Grundrechtsordnungen, EuR Europarecht, S. 469–502.

Berk, Richard (2013): Algorithmic criminology, Security Informatics 2 (5), S. 1–14.

Bode, Matthias (2013): Hochschulzulassungsrecht im Spannungsfeld von gesamtstaatlicher Planung und lokaler Gerechtigkeit – Ein Beitrag zum ersten Numerus clausus-Urteil, WissR Wissenschaftsrecht 46, S. 348–385.

Bode, Matthias (2018): § 32 HRG. Hochschulrecht in Bund und Ländern. Kommentar, Losebl. (Stand: 50. Erg.-Lfg.), Heidelberger Kommentar, Heidelberg.

Bode, Matthias, und Christina Reetz (2014): Hochschulzulassung und partizipative Verwaltung. Das Verfahren von hochschulstart.de zur Unterstützung der Hochschulen bei der Vergabe von Studienplätzen in örtlich zulassungsbeschränkten Studiengängen, Recht der Jugend und des Bildungswesens (RdJB) (62) 14. S. 410–419.

Bodó, Balázs, Natali Helberger und Claes H. de Vreese (2017): Political micro-targeting: A Manchurian candidate or just a dark horse?, Internet Policy Review (6) 4, https://policyreview.info/articles/analysis/political-micro-targeting-manchurian-candidate-or-just-dark-horse (Download 11.11.2019).

Boudinar-Zabaleta, Ackiel (2019): Algorithmes et lignes directrices. Réflexions sur la codification automatisée des motifs des décisions administratives, Droit administratif 4, S. 13–18.

Braun Binder, Nadja (2019): Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, Schweizerische Juristen-Zeitung (SJZ)/Revue Suisse de Juris-prudence (RSJ), S. 467–476.

Brehm, Robert, und Alexandra Brehm-Kaiser (2018): Das Dritte Numerus-Clausus-Urteil des BVerfG, Neue Zeitschrift für Verwaltungsrecht – Extra (NVwZ-Extra) 8, S. 1–20.

Breustedt, Hannes (2015): Krankenversicherer sind begierig auf Fitnessdaten, Welt, 28.2.2015, https://www.welt.de/gesundheit/article137929788/Krankenversicherer-sind-begierig-auf-Fitnessdaten.html (Download 11.11.2019).

Brück, Christoph (2019): Abgeblitzt? Keine Geschwindigkeitsmessung ohne Datenspeicherung – zugleich eine Anmerkung zu VerfGH Saarbrücken, Urt. v. 5.7.2019 – Lv 7/17, juris Die Monatszeitschrift (jM) 10, S. 392–395.

Capers, Bennett (2017): Race, Policing, and Technology, North Carolina Law Review 95 (4), S. 1241–1292.

Carney, Michael (2013): Flush with $20M from Peter Thiel, ZestFinance is measuring credit risk through non-traditional big data, Pando, 31.07.2013, https://pando.com/2013/07/31/flush-with-20m-from-peter-thiel-zestfinance-is-measuring-credit-risk-through-non-traditional-big-data/ (Download 11.11.2019).

Chaltiel, Florence (2019): Parcoursup devant le juge administrative, Petites affiches, S. 6–15.

Chan, Janet, und Lyria Bennett Moses (2016): Is Big Data challenging criminology?, Theoretical Criminology 20 (1), S. 21–39.

Chatziathanasiou, Konstantin (2019): Der hungrige Richter, ein härterer Richter? Zur heiklen Rezeption einer vielzitierten Studie, JuristenZeitung (JZ), S. 455–458.

Corbett-Davies, Sam, Emma Pierson, Avi Feller und Sharad Goel (2016): A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear, The Washington Post, 17.10.2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/?utm_term=.6d23637b1ce1 (Download 11.11.2019).

Dachwitz, Ingo, Thomas Rudl und Simon Rebiger (2018): FAQ: Was wir über den Skandal um Facebook und Cambridge Analytica wissen (UPDATE), Netzpolitik, 21.3.2018, https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/ (Download 11.11.2019).

Dammann, Ulrich (2016): Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwarteter Fortschritt, Schwächen und überraschende Innovationen, Zeitschrift für Datenschutz (ZD), S. 307–314.

Danziger, Shai, Jonathan Levav und Liora Avnaim-Pesso (2011): Extraneous factors in judicial decisions, PNAS 108 (17), S. 6889–6892.

Debet, Anne (2017): APB enfin remis en cause par la CNIL!, Commerce électronique, S. 43–45.

Decker, Hanna, und Patrick Bernau (2018): Die wichtigsten Antworten zum Facebook-Skandal, Frankfurter Allgemeine Zeitung, 21.3.2018, https://www.faz.net/aktuell/wirtschaft/diginomics/fragen-und-antworten-zu-facebook-und-cambridge-analytica-15505321.html?printPagedArticle=true#pageIndex_0 (Download 11.11.2019).

Deppner, Thorsten, und Daniel Heck (2008): Studiengebühren vor dem Hintergrund der Umsetzung völkerrechtlicher Verpflichtungen im Bundesstaat und der Vorgaben materiellen Verfassungsrechts, Neue Zeitschrift für Verwaltungsrecht (NVwZ), S. 45–48.

Deutscher Juristentag e. V. (2018): Thesen der Gutachter und Referenten zum 72. Deutschen Juristentag. Leipzig: Deutscher Juristentag e.V., https://www.djt.de › fileadmin › downloads › 72 › 72_thesen_180728 (Download 11.11.2019).

Deutsches Studentenwerk (2019): Beratung im Profil. Die Sozialberatung und Psychologische Beratung der Studenten- und Studierendenwerke, Berlin.

Dieterich, William, Christina Mendoza und Tim Brennan (2016): COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity, Northpointe, http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf (Download 11.11.2019).

Dijkstra, Jaap J. (2001): Legal Knowledge-based Systems: The Blind Leading the Sheep?, International Review of Law, Computers & Technology 15 (2), S. 119–128.

Dippel, Christian, und Michael Poyker (2019): Do Private Prisons Affect Criminal Sentencing?, NBER, Working Paper No. 25715.

Dörnfelder, Andreas (2018): Was sich hinter den Kreditschnäppchen von Check 24 und Smava verbirgt, Handelsblatt 27.2.2018, https://www.handelsblatt.com/finanzen/banken-versicherungen/selbstversuch-was-sich-hinter-den-kreditschnaeppchen-von-check24-und-smava-verbirgt/21007016.html?ticket=ST-2124610-bivJwoA2fnReSYtItboa-ap6 (Download 11.11.2019).

Dräger, Jörg (2016): Orientierung für Orientierungslose – Wie Algorithmen durch den Bildungsdschungel weisen, Digitalisierung der Bildung, 11.1.2016, http://digitalisierung-bildung.de/2016/01/11/orientierung-fuer-orientierungslose-wie-algorithmen-durch-den-bildungsdschungel-weisen/ (Download 11.11.2019).

Dräger, Jörg, und Ralph Müller-Eiselt (2015): Humboldt gegen Orwell, Zeit Online, 8.10.2015, https://www.zeit.de/2015/39/digitalisierung-bildung-internet-computer-lehrplan (Download 11.11.2019).

Dräger, Jörg, und Ralph Müller-Eiselt (2019): Wir und die intelligenten Maschinen. Wie Algorithmen unser Leben bestimmen und wir sie für uns nutzen können, München.

Dressel, Julia, und Hany Farid (2018): The accuracy, fairness, and limits of predicting recidivism, Science Advances 4 (1), S. 1–5.

Dreyer, Stephan, und Wolfgang Schulz (2018): Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme? Potenziale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen, Gütersloh, https://doi.org/10.11586/2018011 (Download 11.11.2019).

Egbert, Simon (2017): Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum, Aus Politik und Zeitgeschichte 32–33, S. 17–23.

Eggers, Dave (2014): Der Circle, Köln.

Enders, Peter (2018): Einsatz künstlicher Intelligenz bei juristischer Entscheidungsfindung, Juristische Arbeitsblätter (JA), S. 721–727.

Engeler, Malte (2018): Das überschätzte Kopplungsverbot. Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen, Zeitschrift für Datenschutz (ZD) 2018, S. 55–62.

Ernst, Stefan (2017): Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO, Zeitschrift für Datenschutz (ZD) 3, S. 110–114.

Ertel, Wolfgang (2016): Grundkurs Künstliche Intelligenz. Eine praxisorientierte Einführung (Computational Intelligence, 4. Auflage, Wiesbaden.

Erxleben, Christian (2018): Facebook limitiert Zugriff auf Nutzerdaten, Internetworld, 29.4.2018, https://www.internetworld.de/technik/facebook/facebook-limitiert-zugriff-nutzerdaten-1533001.html (Download 11.11.2019).

Erxleben, Christian (2019): KI versus Anwalt: Wer gewinnt das Duell im Vertragsrecht? BASIC thinking, 3.1.2019, https://www.basicthinking.de/blog/2019/01/03/vertragsrecht-anwalt-ki/ (Download 11.11.2019).

Eßer, Martin (2018): Art. 13, DSGVO, DSGVO/BDSG. Datenschutz-Grundverordnung/Bundesdatenschutzgesetz und Nebengesetze, 6. Auflage, Köln.

Europarat, und Europäische Kommission für die Effizienz der Justiz (2018): European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, Straßburg.

Fanta, Alexander (2018): Ob Nutzer oder nicht: Facebook legt Schattenprofile über alle an, Netzpolitik, 29.3.2018, https://netzpolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/ (Download 11.11.2019).

Ferguson, Andrew Guthrie (2015): Big Data and Predictive Reasonable Suspicion, University of Pennsylvania Law Review 163 (2), S. 327–410.

Ferguson, Andrew Guthrie (2017a): Policing Predictive Policing, Washington University Law Review 94 (5), S. 1109–1189.

Ferguson, Andrew Guthrie (2017b): The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement, New York.

Filipović, Alexander, Christopher Koska und Claudia Paganini (2018): Ethik für Algorithmiker. Was wir von erfolgreichen Professionsethiken lernen können, Arbeitspapier, Gütersloh, https://doi.org/10.11586/2018033 (Download 11.11.2019).

Fischer, Sarah, und Thomas Petersen (2018): Was Deutschland über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage, Gütersloh, https://doi.org/10.11586/2018022 (Download 11.11.2019).

Friedrichs, Julia (2013): Das tollere Ich, Zeit Online, 8.8.2013, https://www.zeit.de/2013/33/selbstoptimierung-leistungssteigerung-apps (Download 11.11.2019).

Fron, Carina (2018): Berechnen, wer's nicht schafft, Deutschlandfunk, 31.5.2018, https://www.deutschlandfunk.de/studienabbruch-berechnen-wer-s-nicht-schafft.680.de.html?dram:article_id=419233 (Download 11.11.2019).

Fuchs, Jochen (2017): Kreditech: Bonitätsprüfung auf Social-Media-Basis, T3N 16.9.2017, https://t3n.de/news/kreditech-bonitaetspruefung-495150/ (Download 11.11.2019).

Gerstner, Dominik (2018): Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany, European Journal for Security Research 3 (2), S. 115–138, https://doi.org/10.1007/s41125-018-0033-0 (Download 11.11.2019).

Giannoulis, Georgios (2014): Studien zur Strafzumessung: Ein Beitrag zur Dogmatik, Rechtstheorie und Rechtsinformatik mit Vertiefung in den Eigentums- und Vermögensdelikten, Tübingen.

Gluba, Alexander (2014): Predictive Policing – eine Bestandsaufnahme: Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung, Hannover, https://netzpolitik.org/wp-upload/LKA_NRW_Predictive_Policing.pdf (Download 11.11.2019).

Goddard, Kate, Abdul Roudsari und Jeremy C. Wyatt (2012): Automation bias: a systematic review of frequency, effect mediators, and mitigators, Journal of the American Medical Informatics Association 19 (1), S. 121–127.

Golland, Alexander (2018): Das Kopplungsverbot in der Datenschutz-Grundverordnung. Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag, MultiMedia und Recht (MMR) 2018, S. 130–135.

Grabmair, Matthias (2016): Modeling Purposive Legal Argumentation and Case Outcome Prediction Using Argument Schemes in the Value Judgment Formalism, Pittsburgh.

Graf, Jürgen-Peter (2013): § 112, Karlsruher Kommentar zur Strafprozessordnung, GVG, EGGVG und EMRK, 7. Auflage, München.

Grossenbacher, Timo (2018): Polizei-Software verdächtigt zwei von drei Personen falsch, SRF, 5.4.2018, https://www.srf.ch/news/schweiz/predictive-policing-polizei-software-verdaechtigt-zwei-von-drei-personen-falsch (Download 11.11.2019).

Groß, Karl-Heinz (2016): § 56, Münchener Kommentar zum Strafgesetzbuch, Band 2: §§ 38–79b, 3. Auflage, München.

Grundies, Volker (2016): Gleiches Recht für alle? – Eine empirische Analyse lokaler Unterschiede in der Sanktionspraxis in der Bundesrepublik Deutschland, Krise – Kriminalität – Kriminologie, Mönchengladbach, S. 511–525.

Grundies, Volker (2018): Regionale Unterschiede in der gerichtlichen Sanktionspraxis in der Bundesrepublik Deutschland. Eine empirische Analyse, Kriminalsoziologie – Handbuch für Wissenschaft und Praxis, Baden-Baden, S. 295–315.

Grzymek, Viktoria, und Michael Puntschuh (2019): Was Europa über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage, Gütersloh, https://doi.org/10.11586/2019006 (Download 11.11.2019).

Guckelberger, Annette (2018): § 6 IFG, Beck'scher Online-Kommentar Informations- und Medienrecht, 24. Auflage, Stand: 1.5.2019, München.

Hartung, Markus, und Nicole Zobel (2019): Legal Tech 2019: 100 Angebote für Rechtsanwälte, https://legal-tech.de/Broschueren/FFI_Legal_Tech_2019-100_Angebote_f%C3%BCr_RAe.pdf (Download 11.11.2019).

von Heintschel-Heinegg, Bernd: § 46 StGB, Beck'scher Online Kommentar StGB, 42. Auflage, Stand: 1.5.2019, München.

von Heintschel-Heinegg, Bernd: § 57 StGB, Beck'scher Online Kommentar StGB, 42. Auflage, Stand: 1.5.2019, München.

Hermstrüwer, Yoan (2016): Informationelle Selbstgefährdung. Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, Grundlagen der Rechtswissenschaft Band 31, Tübingen.

Herold, Viktoria (2018): Algorithmisierung von Ermessensentscheidungen durch Machine Learning, Tagungsband DSRI-Herbstakademie 2018, Rechtsfragen digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht, S. 453–465.

Heublein, Ulrich, Julia Ebert, Christopher Hutzsch, Sören Isleib, Richard König, Johanna Richter und Andreas Woisch (2017): Zwischen Studienerwartungen und Studienwirklichkeit. Ursachen des Studienabbruchs, beruflicher Verbleib der Studienabbrecherinnen und Studienabbrecher und Entwicklung der Studienabbruchquote an deutschen Hochschulen (Forum Hochschule, 2017, 1), Hannover: DZHW Deutsches Zentrum für Hochschul- und Wissenschaftsforschung.

Himmelrath, Armin (2019): Die Unsichtbare, Spiegel Online 12.2.2019, http://www.spiegel.de/lebenundlernen/uni/anja-karliczek-bilanz-einer-unsichtbaren-bildungsministerin-a-1242275.html (Download 11.11.2019).

Hörnle, Tatjana (2005): Vorüberlegungen zu Decision-Support-Systemen aus der Sicht des Strafzumessungsrechts, Gerechtigkeitswissenschaft – Kolloquium aus Anlass des 70. Geburtstages von Lothar Philipps, Berlin, S. 393–410.

Hommel, Eva-Maria (2017): Entzauberte Vorhersage, Technology Review Deutschland (11), S. 10–11.

Hornung, Gerrit, und Stephan Schindler (2017): Das biometrische Auge der Polizei. Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung, Zeitschrift für Datenschutz (ZD), S. 203–209.

von Humboldt, Wolfgang (1851): Ideen zu einem Versuch, die Gränzen der Wirksamkeit des Staats zu bestimmen, Breslau.

Huster, Stefan, und Anna Büscher (2019): Das nordrhein-westfälische Landarztgesetz. Darstellung und verfassungsrechtliche Analyse, Vierteljahresschrift für Sozial- und Arbeitsrecht (VSSAR), S. 217–265.

Jeandesboz, Julien, Jorrit Rijpma und Didier Bigo (2016): Smart Borders Revisited: An Assessment of the Commission's Revised Smart Borders proposal, http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571381/IPOL_STU(2016)571381_EN.pdf (Download 11.11.2019).

Joecks, Wolfgang, und Klaus Miebach (2016): Münchener Kommentar zum Strafgesetzbuch. Band 2: §§ 38–79b, 3. Auflage, München.

Justizministerkonferenz 2019 (2019): Legal Tech: Herausforderungen für die Justiz. Abschlussbericht der Länderarbeitsgruppe, 1.7.2019, Travemünde.

Kaspar, Johannes (2018): Sentencing Guidelines versus freies tatrichterliches Ermessen – Brauchen wir ein neues Strafzumessungsrecht? Gutachten C zum 72. Deutschen Juristentag, Band 1, München.

Kempen, Bernhard (2019): Art. 5 Abs. 3, Beck'scher Online-Kommentar Grundgesetz, 41. Auflage, Stand: 15.5.2019, München.

Kingreen, Thorsten (2016): Art. 51 GRCh, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 5. Auflage, München.

Kirchhof, Ferdinand (2014): Nationale Grundrechte und Unionsgrundrechte. Die Wiederkehr der Frage eines Anwendungsvorrangs unter anderer Perspektive, Neue Zeitschrift für Verwaltungsrecht (NVwZ), S. 1537–1541.

Kita, Kinga, und Lukasz Kidziński (2019): Google Street View image of a house predicts car accident risk of its resident, arXiv, 10.4.2019, https://arxiv.org/abs/1904.05270 (Download 11.11.2019).

Klas, Benedikt (2012): Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, Edewecht.

Kleinberg, Jon, Himabindu Lakkaraju, Jure Leskovec, Jens Ludwig und Sendhil Mullainathan (2018): Human Decisions and Machine Predictions, The Quarterly Journal of Economics, 133 (1), S. 237–293.

Klement, Jan Henrik (2017): Öffentliches Interesse an Privatheit. Das europäische Datenschutzrecht zwischen Binnenmarkt, Freiheit und Gemeinwohl, JuristenZeitung (JZ), S. 161–170.

Klingel, Anita (2019): Gesund dank Algorithmen? Chancen und Herausforderungen von Gesundheits-Apps für Patient:innen, Gütersloh.

Knobloch, Tobias (2018): Vor die Lage kommen: Predictive Policing in Deutschland. Chancen und Gefahren datenanalytischer Prognosetechnik und Empfehlungen für den Einsatz in der Polizeiarbeit, Gütersloh.

Knobloch, Tobias, und Carla Hustedt (2019): Der maschinelle Weg zum passenden Personal. Zur Rolle algorithmischer Systeme in der Personalauswahl, Gütersloh.

Krauß, Markus (2019): § 112, Beck'scher Online-Kommentar OWiG, 32. Auflage, Stand: 1.1.2019, München.

Krempl, Stefan (2017): Mercedes-Benz-Bank startet Kfz-Versicherung mit überwachtem Fahrverhalten, Heise online, 12.9.2017, https://www.heise.de/newsticker/meldung/Mercedes-Benz-Bank-startet-Kfz-Versicherung-mit-ueberwachtem-Fahrverhalten-3828583.html (Download 11.11.2019).

Krohn, Philipp, und Roland Lindner (2018): Lebensversicherer verlangt, dass Kunden Fitness-Tracker nutzen, Frankfurter Allgemeine, 20.9.2018, https://www.faz.net/aktuell/wirtschaft/diginomics/lebensversicherung-bei-john-hancock-nur-mit-fitness-tracker-15798146.html (Download 11.11.2019).

Krüger, Julia, und Konrad Lischka (2018): Damit Maschinen den Menschen dienen. Lösungsansätze, um algorithmische Prozesse in den Dienst der Gesellschaft zu stellen. Hrsg. Bertelsmann Stiftung. Gütersloh, https://doi.org/10.11586/2018019 (Download 20.11.2019).

Kühling, Jürgen, Mario Martini, Johanna Heberlein, Benjamin Kühl, David Nink, Quirin Weinzierl und Michael Wenzel (2016): Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum nationalen Regelungsbedarf, Münster.

Kühne-Hörmann, Eva (2019): Kennen Sie Ihren Algorithmus?, Frankfurter Allgemeine Einspruch, 4.11.2019, https://www.faz.net/einspruch/hessen-will-self-tracking-tarife-verbieten-16468560.html (Download 11.11.2019).

Kunnert, Gerhard (2019): Das Aus für Social-/Media-Plug-ins?, Datenschutz und Datensicherheit (DuD) 2019. S. 257–264.

Landeskriminalamt Nordrhein-Westfalen (2018a): Projekt SKALA Abschlussbericht, 28.6.2018, Düsseldorf, https://polizei.nrw/sites/default/files/2018-07/180628_Abschlussbericht_SKALA.PDF (Download 11.11.2019).

Landeskriminalamt Nordrhein-Westfalen (2018b): Kooperative Evaluation des Projektes „SKALA“ (Kurzfassung des Endberichtes). Abschlussbericht der Zentralstelle Evaluation beim LKA NRW (ZEVA) und der Gesellschaft für innovative Sozialforschung und Sozialplanung e.V. Bremen (GISS), Kurzfassung des Endberichtes, 31.1.2018, Düsseldorf, https://lka.polizei.nrw/sites/default/files/2018-06/160131_Evaluationsbericht_SKALA_Kurzfassung.pdf (Download 11.11.2019).

Legnaro, Aldo, und Andrea Kretschmann (2015): Das Polizieren der Zukunft. The future of policing – policing the future, Kriminologisches Journal, S. 94–111.

Lehtonen, Pinja, und Pami Aalto (2017): Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States, European Security, 26 (2), S. 207–225, https://doi.org/10.1080/09662839.2016.1276057 (Download 11.11.2019).

Leisner-Egensperger, Anna (2018): Polizeirecht im Umbruch: Die drohende Gefahr, Die Öffentliche Verwaltung (DÖV), S. 677–688.

von Lewinski, Kai (2019): § 6a BDSG a. F., Beck'scher Online-Kommentar Datenschutzrecht, 28. Auflage, Stand: 1.5.2019, München.

Liang, Hai, und Jonathan Zhu (2017): Big Data, Collection of (Social Media, Harvesting), The International Encyclopedia of Communication Research 29.3.2019, DOI: 10.1002/9781118901731.iecrm0015.

Lindner, Josef Franz (2017): Rechtsfragen des Studiums, Hochschulrecht. Ein Handbuch für die Praxis, 3. Auflage, Heidelberg, S. 649–725.

Lischka, Konrad, und Anita Klingel (2017): Wenn Maschinen Menschen bewerten. Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung, Arbeitspapier, Gütersloh, https://doi.org/10.11586/2017025 (Download 11.11.2019).

Lischka, Konrad, und Christian Stöcker (2017): Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen, Arbeitspapier, Gütersloh, https://doi.org/10.11586/2017028 (Download 11.11.2019).

Lobe, Adrian (2019): Vorsicht, wachsamer Algorithmus!, Frankfurter Allgemeine Sonntagszeitung (FAS), 31.3.2019, S. 39.

Martini, Mario (2015): Wie viel ökonomische Rationalität verträgt der Gesundheitsschutz?, Jahrbuch des öffentlichen Rechts der Gegenwart, Band 63, Tübingen, S. 213–250.

Martini, Mario (2016a): Do it yourself im Datenschutzrecht. Der „Geo Business Code of Conduct“ als Erprobungsfeld regulierter Selbstregulierung, Neue Zeitschrift für Verwaltungsrecht – Extra (NVwZ-Extra) 35 (6), S. 1–13.

Martini, Mario (2016b): Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, Verwaltungsarchiv (VerwArch) 107, S. 307–358.

Martini, Mario (2017a): Algorithmen als Herausforderung für die Rechtsordnung, Juristen-Zeitung (JZ), S. 1017–1025.

Martini, Mario (2017b): Art. 26, Datenschutz-Grundverordnung, Kommentar, Beck'sche Kompakt-Kommentare, München.

Martini, Mario (2018): Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Auflage, München, S. 249–265.

Martini, Mario (2019a): Blackbox Algorithmus. Grundfragen einer Regulierung Künstlicher Intelligenz, Heidelberg.

Martini, Mario (2019b): Neue Freunde und Helfer? Drohnen als Mittel der Beobachtung von Großveranstaltungen und Versammlungen, Die Öffentliche Verwaltung (DÖV), S. 732–743.

Martini, Mario, und Jonas Botta (2019): Undurchsichtige Datentransfers – gläserne Studierende? Datenschutzrechtliche Schranken der Datenübermittlung in die USA am Beispiel von Massive Open Online Courses, Verwaltungsarchiv (VerwArch) 110, S. 235–279.

Martini, Mario, und Saskia Fritzsche (2015): Mitverantwortung in sozialen Netzwerken – Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, Neue Zeitschrift für Verwaltungsrecht – Extra (NVwZ-Extra) 3, S. 1–16.

Martini, Mario, und Thomas Kienle (2019): Facebook, die Lebenden und die Toten. Der digitale Nachlass aus telekommunikations- und datenschutzrechtlicher Sicht – zugleich Besprechung von BGH, Urteil v. 12.7.2018 – III ZR 183/17, JuristenZeitung (JZ), S. 235–241.

Martini, Mario, und David Nink (2017): Wenn Maschinen entscheiden … – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, Neue Zeitschrift für Verwaltungsrecht – Extra (NVwZ-Extra) 10, S. 1–14.

Martini, Mario, und David Nink (2018): Subsumtionsautomaten ante portas? – Zu den Grenzen der Automatisierung in verwaltungsrechtlichen (Rechtsbehelfs-)Verfahren, Deutsches Verwaltungsblatt (DVBl), S. 1128–1138.

Martini, Mario, David Wagner und Michael Wenzel (2018): Das neue Sanktionsregime der DSGVO – ein scharfes Schwert ohne legislativen Feinschliff, Teil 1, Verwaltungsarchiv (VerwArch) 108, S. 163–189.

Martini, Mario, und Michael Wenzel (2017): ‚Once only‘ versus ‚only once‘: Das Once-only-Prinzip zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, Deutsches Verwaltungsblatt (DVBl), S. 749–758.

Martini, Mario, und Jan Ziekow (2017): Die Landarztquote, Verfassungsrechtliche Zulässigkeit und rechtliche Ausgestaltung, Berlin.

Mehde, Veith (2019): Landeskinderklauseln in der Rechtsprechung, Deutsches Verwaltungsblatt (DVBl), S. 1025–1032.

Meinicke, Dirk (2015): Big Data und Data-Mining: Automatisierte Strafverfolgung als neue Wunderwaffe der Verbrechensbekämpfung?, Kommunikation & Recht (K&R), S. 377–384.

Miebach, Klaus (2016): § 261 StPO, Münchener Kommentar zum Strafgesetzbuch. Band 2: §§ 38–79b, 3. Auflage, München.

Miebach, Klaus, und Stefan Maier (2016): § 46 StGB, Münchener Kommentar zum Strafgesetzbuch, Band 2: §§ 38–79b, 3. Auflage, München.

Möckli, Andreas (2017): Datenschützer warnt vor Gesundheits-Apps – Untersuchung gegen Helsana, Aargauer Zeitung, 14.10.2017, https://www.aargauerzeitung.ch/leben/gesundheit/datenschuetzer-warnt-vor-gesundheits-apps-untersuchung-gegen-helsana-131805713 (Download 11.11.2019).

Munte, Oliver (2001): Fuzzylogik und Ausbildungsunterhalt, Rechtstheorie 32, S. 533–557.

Mysegades, Jan (2018): DNA-Auswertung in der Black Box? Gerichtliche Beweisführung durch statistische Computerprogramme, Computer und Recht (CR) (34) 4, S. 225–231.

Neubacher, Frank (2017): Kriminologie, 3. Auflage, Baden-Baden.

Newton, Casey (2018): Facebook gave Spotify and Netflix access to users' private messages, The Verge, 18.12.2018, https://www.theverge.com/2018/12/18/18147616/facebook-user-data-giveaway-nyt-apple-amazon-spotify-netflix (Download 11.11.2019).

Nic Lochlainn, Grainne Meadhbh (2018): Facebook data harvesting: what you need to know, The Conversation, 3.4.2019, https://theconversation.com/facebook-data-harvesting-what-you-need-to-know-93959 (Download 11.11.2019).

Niiler, Eric (2019): Can AI Be a Fair Judge in Court? Estonia Thinks So, WIRED, 25.3.2019, https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/?utm_source=instagram&utm_medium=social&utm_campaign=instagram_stories&utm_brand=wired&utm_social-type=owned (Download 11.11.2019).

Orwat, Carsten (2019): Diskriminierungsrisiken durch Verwendung von Algorithmen, Antidiskriminierungsstelle des Bundes, Baden-Baden, https://www.antidiskriminierungsstelle.de/SharedDocs/Downloads/DE/publikationen/Expertisen/Studie_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.html (Download 11.11.2019).

Pantel, Nadia (2018): Die Wut über den Algorithmus, Süddeutsche Zeitung, 3.6.2018, https://www.sueddeutsche.de/bildung/studienplatz-die-wut-ueber-den-algorithmus-1.3996243 (Download 11.11.2019).

von Petersdorff, Winand (2019): FBI ermittelt wegen Bestechung: Wie Amerikaner sich bei Elite-Unis einkauften, Frankfurter Allgemeine, 13.3.2013, https://www.faz.net/aktuell/wirtschaft/arm-und-reich/fbi-ermittelt-wie-us-amerikaner-sich-bei-elite-unis-einkauften-16086146.html (Download 11.11.2019).

Petrick-Löhr, Christina (2017): Entzauberte Vorhersage, Die Welt, 27.3.2017, https://www.welt.de/sonderthemen/wohnen/article162945232/Precobs-im-Einsatz-Minority-Report-laesst-gruessen.html (Download 11.11.2019).

Philipps, Lothar (1994): Ein bißchen Fuzzy Logic für Juristen, Institutionen und Einzelne im Zeitalter der Informationstechnik. Machtpositionen und Rechte (Sicherheit in der Informationstechnik 6, Neue Techniken und Recht, Band 2), München, S. 219–224.

Philipps, Lothar (1998): Iudex non calculat – jedenfalls nicht ohne Computer. Zugleich eine Besprechung von Wolfgang Köberer: Iudex non calculat. Über die Unmöglichkeit, Strafzumessung sozialwissenschaftlich-mathematisch zu rationalisieren. Monatsschrift für Kriminologie und Strafrechtsreform (MschrKrim) 263, Besprechungsaufsatz. S. 263 ff.

Phillips, Elizabeth D. Capaldi (2014): Revolutionizing Student Advising, Tracking and Intervention, The EvoLLLution, 28.7.2014, https://evolllution.com/opinions/revolutionizing-student-advising-tracking-intervention/ (Download 11.11.2019).

Pilling, David (2019): Are tech companies Africa's new colonialists?, Financial Times, 5.7.2019, https://www.ft.com/content/4625d9b8-9c16-11e9-b8ce-8b459ed04726 (Download 11.11.2019).

Pitschas, Rainer (1998): Der Kampf um Art. 19 IV GG, Funktionsgrenzen des „Neuen Steuerungssystems" in der Verwaltungsgerichtsbarkeit, Zeitschrift für Rechtspolitik (ZRP) 3, S. 96–103.

Posadas, Brianna (2017): How strategic is Chicago's „Strategic Subjects List"? Upturn investigates, Medium 22.6.2017, https://medium.com/equal-future/how-strategic-is-chicagos-strategic-subjects-list-upturn-investigates-9e5b4b235a7c (Download 11.11.2019).

Quaas, Michael, Rüdiger Zuck, Thomas Clemens und Julia Maria Gokel (2018): Medizinrecht, Öffentliches Medizinrecht – Pflegeversicherungsrecht – Arthaftpflichtrecht – Arztstrafrecht, 4. Auflage, München.

Rademacher, Timo (2017): Predictive Policing im deutschen Polizeirecht, Archiv des öffentlichen Rechts (AöR) 142 (3), S. 366–416.

Rademacher, Timo (2019): Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JuristenZeitung (JZ), S. 702–710.

Rätke, Bernd (2018): § 88, Abgabenordnung, 14. Auflage, München.

Rohde, Noëlle (2018): Gütekriterien für algorithmische Prozesse. Eine Stärken- und Schwächenanalyse ausgewählter Forderungskataloge, Arbeitspapier, Gütersloh, https://doi.org/10.11586/2018027 (Download 11.11.2019)

Rolfes, Manfred (2017): Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit, Potsdamer Geographische Praxis, S. 51–76.

Rosenberg, Matthew, Nicholas Confessore und Carole Cadwalladr (2018): How Trump Consultants Exploited the Facebook Data of Millions, The New York Times, 17.3.2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (Download 11.11.2019).

de Ruiter, Alexander (2019): Ein Chatbot an der Universität, eGoverment Computing, Heft 11, S. 6.

Salzmann, Miriam, und Stephan Schindler (2018): Polizeiliche Gesichtserkennung in Deutschland, ZD-Aktuell, 06344.

Sandfuchs, Barbara (2015): Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, Internet und Gesellschaft, Band 2, Tübingen.

Saunders, Jessica, Priscilla Hunt und John S. Hollywood (2016): Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot, Journal of Experimental Criminology, 12 (3), S. 347–371, https://doi.org/10.1007/s11292-016-9272-0 (Download 11.11.2019).

Schenke, Wolf-Rüdiger (2018): Polizei- und Ordnungsrecht, 10. Auflage, Heidelberg.

Schindler, Jörg (2018): Der Brexit – ein großer Betrug?, Spiegel Online, 26.3.2018, http://www.spiegel.de/politik/ausland/facebook-und-brexit-christopher-wylie-zu-cambridge-analytica-a-1199880.html (Download 11.11.2019).

Schlenk, Caspar Tobias (2018): Statt zur Bank einfach Cash von Mother Green, Die Welt, 6.4.2018, https://www.welt.de/sonderthemen/noahberlin/article176966702/Digitales-Banking-ist-in-Kenia-im-Massenmarkt-angekommen.html (Download 11.11.2019).

Scholz, Rupert (2019): Art. 5 Abs. 3, Grundgesetz, Stand 86, Erg.-Lfg., München.

Schreiber, Marlene (2014): Social Media Monitoring, Privacy in Germany (PinG), 2. Jahrgang, S. 34–36.

Schroepfer, Mike (2018): Unsere Pläne zur Einschränkung des Datenzugriffs auf Facebook, Facebook Newsroom 5.4.2018, https://de.newsroom.fb.com/news/2018/04/unsere-plaene-zur-einschraenkung-des-datenzugriffs/ (Download 11.11.2019).

Schulz, Sönke E., und Christian Hoffmann (2010): Grundrechtsrelevanz staatlicher Beobachtungen im Internet, Computer und Recht (CR), S. 131–136.

Schwartmann, Rolf, und David Klein (2018): Art. 6, DS-GVO/BDSG, Heidelberger Kommentar, Heidelberg.

Shapiro, Aaron (2017): Reform predictive policing, Nature 541, S. 458–460, https://doi.org/10.1038/541458a (Download 11.11.2019).

Siegrist, Patrice (2016): Wer viele SMS bekommt, ist kreditwürdiger, Tagesanzeiger.ch, 21.3.2016, https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/wer-viele-sms-bekommt-ist-kreditwuerdiger/story/25348702 (Download 11.11.2019).

Simonite, Tom (2012): What Facebook Knows, MIT Technology Review, 13.6.2012, https://www.technologyreview.com/s/428150/what-facebook-knows/ (Download 11.11.2019).

Singelnstein, Tobias (2018): Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, Neue Zeitschrift für Strafrecht (NStZ), S. 1–9.

Skitka, Linda J., Kathleen Mosier und Mark D. Burdick (2000): Accountability and automation bias, International Journal of Human-Computer Studies 52, S. 701–717.

Smets, Christoph (2019): Die Stadionverbotsentscheidung des BVerfG und die Umwälzung der Grundrechtssicherung auf Private, Neue Zeitschrift für Verwaltungsrecht (NVwZ), S. 34–37.

Sommerer, Lucia (2017): Geospatial predictive policing, Neue Kriminalpolitik (NK), S. 147–164.

Stadler, Tobias (2017): Die Lebensleistung des Täters als Strafzumessungserwägung, Studien und Beiträge zum Strafrecht Band 24, Tübingen.

Stegemann, Jana (2018): Er hätte niemals dort sein dürfen, Süddeutsche Zeitung, 5.10.2018, https://www.sueddeutsche.de/politik/verwechselter-haeftling-in-kleve-er-haette-niemals-dort-sein-duerfen-1.4158471 (Download 11.11.2019).

Steinebach, Martin, Erik Krempel, Christian Jung und Mario Hoffmann (2016): Datenschutz und Datenanalyse, Datenschutz und Datensicherheit (DuD), S. 440–445.

Suckow, Oliver (2018): Grundlagen des Predictive Policing. Near-Repeat-Victimisation im ländlichen Raum, Kriminalistik, S. 347–356.

Szentpetery-Kessler, Veronika (2019): Street View verrät Autounfall-Risiko, Heise online, 28.5.2019, https://www.heise.de/newsticker/meldung/Street-View-verraet-Autounfall-Risiko-4431756.html?wt_mc=nl_ho_top.2019-05-30 (Download 11.11.2019).

Thieme, Werner (2004): Deutsches Hochschulrecht. Das Recht der Universitäten sowie der künstlerischen und Fachhochschulen in der Bundesrepublik Deutschland, 3. Auflage, Köln.

Treuthardt, Daniel, und Melanie Kröger (2019): Der Risikoorientierte Sanktionenvollzug (ROS) – empirische Überprüfung des Fall-Screening-Tools (FaST), Schweizerische Juristen-Zeitung (SJZ)/Revue Suisse de Jurisprudence (RSJ) 1, S. 76–85.

Vieth, Kilian, und Ben Wagner (2017). Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können. Hrsg. Bertelsmann Stiftung. Gütersloh, https://doi.org/10.11586/2017027 (Download 20.11.2019).

Voss, Rainer (1998): Kostencontrolling und richterliche Unabhängigkeit oder Neues Steuerungsmodell contra unabhängige Rechtsprechung?, Deutsche Richterzeitung (DRiZ), S. 379–390.

Walter, Hannfried (2018): § 1 HRG, Hochschulrecht in Bund und Ländern, Kommentar, Stand 50. Erg.-Lfg., Heidelberg.

Wehner, Markus (2019): Gleichberechtigung per Gesetz, Frankfurter Allgemeine, 29.1.2019, https://www.faz.net/aktuell/politik/inland/frauenquote-in-brandenburg-gleichberechtigung-per-gesetz-16012751.html (Download 11.11.2019).

Weinzierl, Quirin (2018): Warum das Bundesverfassungsgericht Fußballstadion sagt und Soziale Plattformen trifft, JuWissBlog, 24.5.2018, https://www.juwiss.de/48-2018/ (Download 11.11.2019).

Weiß, Theresa (2018): Wie ein Algorithmus Studienabbrecher frühzeitig erkennt, Frankfurter Allgemeine, 19.6.2019, http://www.faz.net/aktuell/beruf-chance/campus/wie-ein-algorithmus-kuenftige-studienabbrecher-fruehzeitig-erkennt-15640650.html (Download 11.11.2019).

Wendt, Rudolf (2018): Das Recht auf Offenlegung der Messunterlagen im Bußgeldverfahren, Neue Zeitschrift für Verkehrsrecht (NZV), S. 441–446.

Youyou, Wu, Michal Kosinski und David Stillwell (2015): Computer-based personality judgements are more accurate than those made by humans, Proceedings of the National Academy of Sciences in the United States of America (PNAS) (112) 4, S. 1036–1040, http://www.pnas.org/content/112/4/1036.full (Download 11.11.2019).

Zweig, Katharina A. (2018): Wo Maschinen irren können. Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung, Gütersloh, https://doi.org/10.11586/2018006 (Download 11.11.2019).

Zweig, Katharina A. (2019): Algorithmische Entscheidungen: Transparenz und Kontrolle, Analysen und Argumente – Digitale Gesellschaft Nr. 338/Januar, Berlin.

Zweig, Katharina A., und Tobias D. Krafft (2018): Fairness und Qualität algorithmischer Entscheidungen, (Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, Berlin, S. 204–227.

10 Über die Autoren

Prof. Dr. Mario Martini ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer sowie Stellvertretender Direktor des Deutschen Forschungsinstituts für öffentliche Verwaltung, Fellow am CAIS und Mitglied der Datenethikkommission der Bundesregierung. Seit dem Jahr 2016 leitet er den Programmbereich „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung. Bis April 2010 hatte er eine Professur für Staats- und Verwaltungsrecht an der Ludwig-Maximilians-Universität München inne. Mario Martini hat sich an der Bucerius Law School habilitiert (2006) und wurde an der Johannes Gutenberg-Universität Mainz promoviert (2000). Seine Forschungsschwerpunkte liegen insbesondere im Internet-, Datenschutz-, Medien- und Telekommunikationsrecht, in der Verbindung von Recht und Ökonomik sowie in den Themenfeldern „Open Government“ sowie „Künstliche Intelligenz“.

Dr. Jonas Botta ist Forschungsreferent im Programmbereich „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer. Er beschäftigt sich vornehmlich mit den datenschutzrechtlichen Herausforderungen neuer Technologien und internationaler Datenströme. Im Kontext dieser Interessengebiete steht auch seine Dissertation „Datenschutz bei E-Learning-Plattformen“ (erscheint 2020), für die er Stipendien der Studienstiftung des deutschen Volkes und des Studienförderwerks Klaus Murmann erhielt. 2019 war Botta Visiting Scholar am Brussels Privacy Hub und verbrachte weitere Auslandsaufenthalte mit datenschutzrechtlichem Bezug in Florenz und Wien. Außerdem hat er einen Lehrauftrag für Grund- und Menschenrechte an der Hochschule für Wirtschaft und Recht Berlin inne.

David Nink ist Rechtsanwalt in der Praxisgruppe „Digital Business“ bei Noerr LLP in Frankfurt. Zuvor war er mehrere Jahre als Forschungsreferent und Doktorand im Programmbereich „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung in Speyer tätig, von 2017 bis 2018 war er dort auch Programmbereichskoordinator. Zuletzt absolvierte er von September bis November 2019 einen Forschungsaufenthalt in Estland. Sein Forschungsinteresse gilt insbesondere dem Datenschutzrecht, der Entscheidungsfindung und -steuerung sowie Fragen der Regulierung neuer Technologien. Seine Dissertation mit dem Titel „Justiz und Algorithmen“ erscheint 2020.

Michael Kolain ist Co-Koordinator des Programmbereichs „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung in Speyer, dem er von Beginn an als Forschungsreferent angehört. Seine Forschungsinteressen liegen im Bereich der Regulierung neuer Technologien, im Staats- und Datenschutzrecht und der Rechtsinformatik. Michael Kolain hat zahlreiche Vorträge zur Blockchain-Technologie im In- und Ausland gehalten. An der Monographie „Blackbox Algorithmus“ von Mario Martini hat er intensiv mitgewirkt. Als Visiting Scholar war er 2018 am Koreal Legislation Research Institute in Sejong-si zu Gast; 2019 lehrte er ein interdisziplinäres Seminar an der Université Catholique de Lyon. Neben seiner Tätigkeit in der rechtswissenschaftlichen Forschung verfasst er literarische und journalistische Texte.

11 Impulse Algorithmenethik

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

Impuls Algorithmenethik #1: Lischka, Konrad, und Anita Klingel (2017). *Wenn Maschinen Menschen bewerten. Internationale Fallbeispiele für Prozesse algorithmischer Entscheidungsfindung*. Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2017025).

Impuls Algorithmenethik #2: Vieth, Kilian, und Ben Wagner (2017). *Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können*. Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2017027).

Impuls Algorithmenethik #3: Lischka, Konrad, und Christian Stöcker (2017). *Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen*. Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2017028).

Impuls Algorithmenethik #4: Zweig, Katharina Anna (2018). *Wo Maschinen irren können. Verantwortlichkeiten und Fehlerquellen in Prozessen algorithmischer Entscheidungsfindung*. Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2018006).

Impuls Algorithmenethik #5: Dreyer, Stephan, und Wolfgang Schulz (2018). *Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme? Potenziale und Grenzen der Absicherung individueller, gruppenbezogener und gesellschaftlicher Interessen*. Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2018011).

Impuls Algorithmenethik #6: Krüger, Julia, und Konrad Lischka (2018). *Damit Maschinen den Menschen dienen. Lösungsansätze, um algorithmische Prozesse in den Dienst der Gesellschaft zu stellen*. Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2018019).

Impuls Algorithmenethik #7: Fischer, Sarah, und Thomas Petersen (2018). *Was Deutschland über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage.* Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2018022).

Impuls Algorithmenethik #8: Rohde, Noëlle (2018). *Gütekriterien für algorithmische Prozesse. Eine Stärken- und Schwächenanalyse ausgewählter Forderungskataloge.* Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2018027).

Impuls Algorithmenethik #9: Filipović, Alexander, Christopher Koska und Claudia Paganini (2018). *Ethik für Algorithmiker. Was wir von erfolgreichen Professionsethiken lernen können.* Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2018033).

Impuls Algorithmenethik #10: Grzymek, Viktoria, und Michael Puntschuh (2019): *Was Europa über Algorithmen weiß und denkt. Ergebnisse einer repräsentativen Bevölkerungsumfrage.* Hrsg. Bertelsmann Stiftung. Gütersloh (auch online unter https://doi.org/10.11586/2019006).

Adresse | Kontakt

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

Carla Hustedt
Ethik der Algorithmen
Telefon +49 5241 81-81156
Fax +49 5241 81-681156
carla.hustedt@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de

BertelsmannStiftung