
Kapitel 1

Das Optimierungsversprechen: neue Realisierungsstrukturen für Recht

Die individuelle, wirtschaftliche und gesellschaftliche Bedeutung, die als ‚intelligent‘¹ bezeichneten Systemen heute beigemessen wird, muss nicht mehr erläutert werden.¹ Dasselbe gilt für ihre historische Entwicklung, deren Beginn sich auf *Alan Turings* Beitrag „Computing Machinery and Intelligence“ und die mittlerweile berühmte *Dartmouth Conference* im Jahr 1956 datieren lässt.² Außerordentlich umfangreich ist die entsprechende, auch rechtsnahe Literatur hierzu mittlerweile, auf die hiermit verwiesen sei.³ Vergleichsweise jung sind hingegen systematische Überlegungen dazu, ob und wenn ja, unter welchen Umständen die aktuelle Generation künstlich-intelligenter Technologien dazu führen könnte, dass der Vollzug von Recht flächendeckend bis hin zu seinem „Vollvollzug“⁴ optimiert werden könnte. Um zu dieser Frage ausführen zu können, sind in diesem ersten Kapitel Erläuterungen dazu angezeigt, wie eine Optimierung der Realisierung von Recht durch KI technisch erfolgen kann. Dazu werden in einem ersten Schritt die Grundbegriffe knapp erläutert, die den immer noch schillernden Oberbegriff der künstlichen Intelligenz näher konturieren (sogleich, → § 1). In einem umfangreicheren → § 2 werden dann einzelne Anwendungsfelder künstlich-intelligenter Rechtserkenntnis und – noch avancierter – Rechtsrealisierung systematisiert und in insgesamt fünf große Gruppen unterteilt.

1 Für eine Übersicht über Chancen und Risiken von KI s. *Martini*, Blackbox Algorithmus, 2019, S. 14-66.

2 Eine anschauliche Zeittafel findet sich bei *Ertel*, Grundkurs KI, 2021, S. 7 ff.

3 Knapp und konzise *Wischmeyer*, AöR 143 (2018), 1 (9 f.), m. vielen weiteren Nachw.

4 Ebd., S. 42.

§ 1 Begriffe und Eigenschaften: künstliche Intelligenz in rechtswissenschaftlicher Betrachtung

- 1 Künstliche Intelligenz stellt einen Modebegriff dar. Ihn zu definieren, fällt aber immer noch schwer.
- 2 Besonders deutlich wird das an *relativen* Definitionen wie etwa der von *Elaine Rich* aus dem Jahr 1983: “Artificial Intelligence is the study of how to make computers do things at which, at the moment, people are better.”¹ Diese Definition wirft einerseits natürlich die Frage auf, ob die damit umstandslos nahegelegte Konvergenz von Mensch und Maschine überhaupt wünschenswert ist.² Aber auch dann, wenn man das beiseitelässt, überzeugt der Ansatz nicht: Computer sind praktisch seit ihrer Erfindung in vielen Bereichen Menschen überlegen, ohne dass der populäre oder der wissenschaftliche Diskurs dafür das Attribut ‚intelligent‘ verliehen hätte.³ Als einfaches Beispiel sei das Auswendiglernen und ‚Abrufen‘ von Gedichten genannt:⁴ für einen Menschen meist mühsam, während ein Computer den Text binnen Sekunden speichern, indexieren und wiederfinden kann. Die OECD weist darauf hin, dass eine solche Gewöhnung an – nach menschlichen Maßstäben: geradezu krasse – Maschinenleistungen voranschreite, sodass *mittlerweile* sogar maschinelle Schrifterkennung (*Optical Character Recognition* – OCR) “by the general public” nicht mehr als KI gewertet würde, obwohl die Technologie eindeutig “textbook AI methods” anwende⁵ (OCR wird mir daher im Folgenden auch weiterhin zur Illustration dienen; aber der Punkt, den die OECD machen will, leuchtet ein: *relative* Definitionen von KI sind letztlich nicht besonders nachhaltig).
- 3 Aber auch aus *nicht*-relativen Definitionsversuchen spricht eine gewisse Verlegenheit. Illustrieren lässt sich das an der Definition von „KI-System“ im finalen Text des AI Act. Die entsprechende Norm lautet:

1 E. Rich, Artificial intelligence, 1983, S. 1. Ähnl., noch im Jahr 2017, Finlay, Artificial Intelligence and Machine Learning for Business, S. 10: “Artificial Intelligence is the replication of human analytical and/or decision making capabilities.” Für eine krit. (“deeply flawed”) Auseinandersetzung mit diesen relativen Definitionsansätzen s. Kaplan, Artificial Intelligence, 2016, S. 1 ff. Im Kontrast zu diesen Ansätzen steht die Methode der *Integrative Social Robotics*, deren *Non Replacement*-Prinzip besagt, dass “social robots may only do what humans should but cannot do”. Dazu Seibt, in: Werthner et. al. (Hg.), Perspectives on Digital Humanism, 2022, S. 183 (186). Realistisch ist das freilich nicht.

2 Vgl. – neben Art. 1 Abs. 1 GG bzw. Art. 1 Abs. 1 GRC – noch deutlicher Art. 12 Abs. 1 der bremischen Landesverfassung: „Der Mensch steht höher als Technik und Maschine“; außerdem auf ethischer Basis die *Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz*, Leitlinien v. 8.4.2019, Rn. 9, 10 (Onlinequelle): „Die KI ist kein Selbstzweck, sondern [muss] auf den Menschen ausgerichtet sein.“

3 Vgl. auch die Schilderungen bei Ertel, Grundkurs KI, 2021, S. 1 ff., der freilich im Erg. doch häufig auf die Definition von Rich zurückgreift.

4 Mit diesem Bsp. Ertel, Grundkurs KI, 2021, S. 202.

5 s. <https://oecd.ai/en/wonk/definition>, besucht am 25.4.2025.

„KI-System‘ [bezeichnet] ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet,⁶ wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“ (Art. 3 Nr. 1 AI Act).

Offensichtlich problematisch an dieser und vergleichbaren⁷ Definitionen sind Begriffe wie „in unterschiedlichem Grade“, „anpassungsfähig sein kann“, „beeinflussen können“ (alles reichlich unbestimmt), und „autonom“ (unbestimmt, philosophisch aufgeladen und – wie der relative Definitionsansatz – mit Vermenschlichungstendenz); und trotz der Unbestimmtheit ist die Definition eventuell sogar zu eng geraten.⁸ Für einen Rechtsakt wie den AI Act, der sich ausdrücklich in den Dienst der „Rechtssicherheit“ stellt und daher eine „klare Definition“ von KI-System liefern will,⁹ ist diese Definition daher, vorsichtig gesagt, unbefriedigend.

Hier soll nun kein weiterer Definitionsversuch unternommen werden. Vielversprechender und, so scheint mir, im wissenschaftlichen und immer mehr auch populären Diskurs mittlerweile gebräuchlich, ist vielmehr ein phänomenologischer Ansatz, der ‚künstliche Intelligenz‘ aus den *technischen* Einzelementen bzw. -begriffen rekonstruiert, die die Grundlagen dessen bilden, was zusammenfassend eben als künstliche Intelligenz bezeichnet wird.¹⁰ Hier sind vor allem zu nennen: maschinelles Lernen (dazu sogleich → I.), angewandte Statistik (→ II.), und symbolische künstliche Intelligenz (→ III.). Im Kern bildet dieser technisch orientierte ‚Dreiklang‘ übrigens auch den Zugriff ab, den die EU-Kommission für ihren Vorschlag für den AI Act gewählt hatte,¹¹ den der Gesetzgeber dann aber, für seine regulatorischen Zwecke, als zu *weit* verwarf.¹² Für den folgenden, dezidiert rechtswissenschaftlichen

6 Zum zentralen Begriff der Ableitung/Inferenz s. *Steen*, KIR 2024, 7 ff.

7 s. bspw. die i. R. des Gesetzgebungsverfahrens einflussreiche Definition der *Unabhängigen Hochrangige Expertengruppe für Künstliche Intelligenz*, Definition v. 8.4.2019, S.1 (Onlinequelle); vgl. auch die der technischen Entwicklung angepasste Definition der OECD v. 5.3.2024, S. 4 (Onlinequelle), auf die ErwGr. 12 zum AI Act implizit verweist.

8 Nach Auffassung von *Roth-Isigkeit*, KIR 2024, 15 f., schließt die Def. des AI Act komplexe *regelbasierte* Systeme (dazu ab → S. 59) aus; dies offenlassend *Krönke*, NVwZ 2024, 529. Da ErwGr. 12, der die Def. in Art. 3 Nr. 1 AI Act näher konturiert, ausdrücklich auch „logik- und wissensgestützte Konzepte“ erfasst, scheint mit einer erweiternden, komplexe regelbasierte Systeme auch erfassende Auslegung mit *Krönke* a. a. O. durchaus möglich.

9 Vgl. bes. ErwGr. 12 S. 2 zum AI Act.

10 Ähnl. *Wischmeyer*, AöR 143 (2018), 1 (9): „Vor allem aber sind seit 2010 Fortschritte bei der Beherrschung und Integration jener drei Elemente zu verzeichnen, die das Herzstück aller lernfähigen Systeme ausmachen: Daten, lernfähige Algorithmen und menschliche Supervision.“ Noch deutlicher *Finlay*, *Artificial Intelligence and Machine Learning for Business*, 2017, S. 11: „It’s the combination of these individual components [data input, data (pre)processing, predictive models, decision rules (rule sets), response/output] that give us the ‘AI.’“ Knappe, konzise Begriffserläuterungen nun bei *Seckelmann*, *Die Verwaltung* 56 (2023), 1 (4 ff.).

11 s. Anhang I AI Act-Entwurf (*EU-Kommission*, COM[2021] 206 final v. 21.4.2021).

12 Zu weit, weil er mit dem *pauschalen* Verweis auf “logic- and knowledge based approaches” und “statistical approaches” (vgl. ebd., lit. b und c) wohl auch einfache regelbasierte und daher gut nachvollziehbare

Zugang zur Materie scheinen mir die drei genannten Grundbegriffe aber weiterhin tauglich und in jedem Fall deutlich greifbarer als die umständliche und eher unbestimmte Definition des finalen AI Act.

I. Maschinelles Lernen und verwandte Begriffe

- 6 Der fachwissenschaftliche wie auch der populäre Diskurs assoziiert mit KI heute vor allem die Technologien des sogenannten maschinellen Lernens (*Machine Learning*). Die EU-Kommission nannte das maschinelle Lernen ebenfalls als erstes unter den „Techniken und Konzepten“, auf die der AI Act nach ihrem Vorschlag Anwendung finden sollte.¹³ Zumindest in Erwägungsgrund 12 listet der verabschiedete AI Act maschinelles Lernen auch weiterhin als zentrale KI-Technologie.
- 7 Diese Technologien sollen in einem gegebenen Datenbestand mithilfe statistischer Methoden¹⁴ Datenpunkte identifizieren, denen in der Kombination nach menschlichen Maßstäben ein bestimmter Informationswert zukommt. Das sind z. B. bestimmte Bildpunkt-Muster, die den Schluss erlauben, bei der dem Computer vorgelegten Pixelmasse handele es sich um das Bild eines Menschen oder eines Pferdes. Gemeinhin ist hier die Rede davon, dass die Maschine in Anwendung einer vorgegebenen statistischen Methode aus den Daten selbstständig ‚lernt‘, welche Kombination aus Punkten phänotypisch für ein Pferd steht.¹⁵
- 8 Allerdings suggeriert ‚lernen‘ eine Verständnisebene, welche die Maschine im Fall des *Machine Learning* noch nicht erreicht. Dieser semantische Vorbehalt gilt jedenfalls dann, wenn man ‚lernen‘ nicht nur als einen Ablauf von *Wahrnehmung/Klassifikation der Welt* → *Verknüpfung mit Bekanntem* → *Mustererkennung* versteht, sondern

Software wie *Excel* etc. erfasst hätte. Bereits der Rat (s. Dok. 2021/0106[COD], S. 71) schlug daher vor, den Verweis auf statistische Methoden zu streichen. Am Ende wurde der phänomenologische Ansatz sogar ganz aus dem Normtext gestrichen. Ansätze dafür finden sich aber noch in ErwGr. 12. *Alternativ* hätte es sich angeboten, den Verweis auf die Techniken, die KI zugrunde liegen, beizubehalten, und eine *einschränkende* Bedingung anzufügen, dass vom AI Act nur solche Anwendungen der Technik erfasst sind, die aufgrund ihrer Architektur so komplex sind bzw. die in solche Entscheidungszusammenhängen eingesetzt werden, dass das die aufwändige Regulierung des AI Act rechtfertigen kann. Im Detail, nämlich bei der Def. dessen, was *Hochrisiko*-KI-Systeme sind, hat der Gesetzgeber diese Konstruktion auch gewählt (s. Art. 6 Abs. 3, 4, 6 AI Act), die m. E. eher geeignet gewesen wäre, die nun drohende *Over-regulation* zu vermeiden.

13 s. Anhang I lit. a AI Act-Entwurf (EU-Kommission, COM[2021] 2026 final).

14 Zu nennen sind hier ohne Anspruch auf Vollständigkeit künstliche neuronale Netze, lineare Regression, Naïve Bayes, *Support Vector Machines*, *Decision Trees*. Für eine gut lesbare Übersicht der je nach Anwendungsfeld unterschiedlich tauglichen Methoden s. Ertel, Grundkurs KI, 2021, Kapitel 8 f. Gut zugänglich auch Siegel, *Predictive Analytics*, 2016, bes. S. 168-173, der die Prinzipien v. a. am Bsp. von *Decision Trees* erläutert; sehr gut auch die Bsp. bei Burrell, *Big Data & Society* 3 (2016), 1, und Kaminski, in: Wieglering/Nerurkar/Wadephul (Hg.), *Datafizierung und Big Data*, 2020, S. 151 (157 ff.).

15 Z. B. Wischmeyer, AöR 143 (2018), 1 (3), unter Verweis auf technikwissenschaftliche Lit.

wenn man ‚lernen‘ anspruchsvoller versteht als Prozess der Konstruktion von Wissen,¹⁶

„das über unmittelbare Erfahrungen hinausgeht. Es [das Lernen] setzt auf Seiten des Lernenden die Überzeugung voraus, daß es in der Welt Regularien gibt, die sich zwar der unmittelbaren Beobachtung entziehen mögen, aber auf der Basis gehalterweiternder Schlußfolgerungen zu erschließen und zu ‚entdecken‘ sind.“¹⁷

Solche selbstständig schlussfolgernde KI wird sprachlich abgrenzend als *Artificial General Intelligence* (AGI)¹⁸ bezeichnet und in der Forschung zwar angestrebt,¹⁹ ist aber auch im Jahr 2024 noch nicht erreicht (dazu unten, → III., mehr).²⁰

Viel treffender als ‚lernen‘ erscheint für aktuelle Techniken des maschinellen Lernens der Begriff des *Beobachtens*: Die Maschine beobachtet und findet mittels einer vom Menschen vorgegebenen statistischen Methode²¹ in einem gegebenen Set an Trainingsdaten wiederkehrende Muster, die mit möglichst hoher Spezifizität (Genauigkeit) bei gleichzeitig hinreichend hoher Generalisierbarkeit Indikatoren (*Features*)²² für die Klassifikation ‚wahrscheinlich ein Pferd/wahrscheinlich kein Pferd‘ enthalten. Es handelt sich also um Induktion, nicht Deduktion, oder, wie *Eric Siegel* treffend schreibt: „Believing in such a rule is accepting *proof by example*“.²³

Ob Genauigkeit und Generalisierungskraft mit Blick auf die beabsichtigte Verwendung des Musters hoch genug sind, wird anhand von Validations- und Testdaten geprüft, die im Training nicht verwendet worden sind bzw. nicht verwendet worden sein dürfen. Mathematisch stark vereinfacht lässt sich das Resultat folgendermaßen illustrieren:

16 Für eine Übersicht über die rechtlich relevanten – also i. R. dieser Untersuchung im Vordergrund stehenden – Formen von Wissen *Hoffmann-Riem*, AöR 145 (2020), 1 (8 f.).

17 *Seel*, Psychologie des Lernens, 2003, S. 23.

18 Ein populärer Begriff ist auch der der „Superintelligenz“, geprägt v. a. vom Philosophen *Bostrom*, *Superintelligence*, 2014, passim. Krit. zu solch alarmistischen Prophezeiungen *Wischmeyer*, AöR 143 (2018), 1 (3, 15).

19 Vgl. bspw. die noch allzu euphorische Erfolgsmeldung von *Pei et al.*, *Nature* 572 (2019), 106 ff. Vorgestellt wird aber auch hier ‚nur‘ ein KI-Chip, der die Aufgabe ‚Fahrradfahren‘ besonders gut erfüllt. Zu AGI nochmals → § 1 Rn. 43 ff.

20 Vgl. etwa *Martini*, *Blackbox Algorithmus*, 2019, S. 59: „Inbesondere scheitern [Computer] daran, die Bedeutung von Inhalten jenseits der reinen Zeichenkette zu erfassen, den lebensweltlichen Kontext zu verstehen, in dem sie agieren, oder die gesellschaftlichen Folgen ihres Handelns in einen größeren Zusammenhang einzuordnen und sie selbstständig zu bewerten.“ Gegen die Antropomorphisierung, die mit bestimmten Begriffen wie „belief“, „knowledge“, „understanding“ oder „self“ einhergehen kann, *Shanahan*, arXiv:2212.03551v5 (16.2.2023), S. 2 f.

21 s. ausf. → § 1 Rn. 29 ff.

22 *Ertel*, *Grundkurs KI*, 2021, S. 202 ff.

23 *Siegel*, *Predictive Analytics*, 2016, S. 169.

Weil $x_1 \text{ Trainingsdatum} + x_2 \text{ Trainingsdatum} + x_3 \text{ Trainingsdatum} \dots + x_n \text{ Trainingsdatum} = y \text{ (Pferd)}$

sei $x_1 \text{ Realdatum} + x_2 \text{ Realdatum} + x_3 \text{ Realdatum} \dots + x_n \text{ Realdatum} = p_y \text{ (Pferd)}$ ²⁴

- 12 Wie gesagt ist das Ziel des Trainings die Erstellung von Mustern, die einerseits möglichst genau sind, also möglichst wenige Nicht-Pferde als Pferde auswerfen (Vermeidung von *False Positives* bzw. Reduzierung der Gefahr des *Underfitting*), andererseits aber hinreichend stark generalisieren (= robust²⁵ sind), d. h. in der Datengesamtmenge möglichst wenige Pferde übersehen; also etwa ein Pferd nicht nur deshalb als Nicht-Pferd klassifizieren, weil es im konkreten Fall eine andere Fellfarbe als die Tiere in den Trainingsdaten hat (Vermeidung von *False Negatives* bzw. Reduzierung der Gefahr des *Overfitting*).²⁶ Das Ergebnis sind Muster, die Näherungen akzeptieren *müssen*, um funktionieren zu können, es mit anderen Worten zulassen müssen, dass ein $x_1 \text{ Realdatum}$ in unterschiedlichen realen Anwendungen unterschiedlich stark an dem Ergebnis y_{Pferd} „beteiligt“²⁷ sein darf. Ich verwende im Buch statt des häufig verwandten Begriffs Algorithmus (= Handlungsvorschrift), der das Prozesshafte betont, den Begriff Muster, der das Ergebnis der algorithmisch durchgeführten Analyse/Suche bezeichnet;²⁸ er (der Begriff Muster) hat den Vorzug, dass er erstens anschaulicher umschreibt, um was es geht, und er zweitens nicht die sinistre Konnotation hat, die dem Begriff des Algorithmus mittlerweile anhaftet. Geläufiger – und deshalb auch im Titel des Buches beibehalten – ist freilich immer noch der Begriff Algorithmus.
- 13 Der Output, das y , stellt also stets ein Wahrscheinlichkeitsurteil (genauer daher p_y statt y) dar und ist damit in einem weiten technischen Sinn stets eine Prognose.²⁹ Sind diese Vorhersagen auf die Erkenntnis eines aktuellen Zustands gerichtet, also z. B. auf „Das Bild zeigt ein Pferd“ oder „Das BIP beträgt aktuell so und so viele Billionen“, lässt sich die gerade eingeführte Illustration folgendermaßen verallgemeinern:

Weil $x_1 \text{ gestern} + x_2 \text{ gestern} + x_3 \text{ gestern} \dots + x_n \text{ gestern} = y_{\text{gestern}}$

sei $x_1 \text{ heute} + x_2 \text{ heute} + x_3 \text{ heute} \dots + x_n \text{ heute} = p_y \text{ heute}$

24 Nicht y , sondern p_y , da das Verhalten nicht mit Gewissheit, sondern mit einer bestimmten Wahrscheinlichkeit vorhergesagt wird.

25 Zum Begriff, am Bsp. von Inhaltsfiltertechnologien für Online-Plattformen, *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 83 ff.

26 Dieses Dilemma aus Individualisierung und Generalisierung wird als *Bias-Variance-Trade-off* bezeichnet. Klärend zu den Begrifflichkeiten *Hermstrüwer*, AöR 145 (2020), 479 (488 f.) m. w. N.

27 So treffend *Wojciech Samek*, zitiert nach *Lenzen*, F.A.Z. v. 24.5.2017, S. N4.

28 Vgl. zum Algorithmenbegriff statt vieler *Datenethikkommission der Bundesregierung*, 2019, S. 54 und ff.

29 *Wischmeyer*, in: *Kulick/Goldhammer* (Hg.), *Der Terrorist als Feind?* 2020, S. 193 (201).

Ein vor allem in den Finanzwissenschaften eingeführter,³⁰ m. E. aber auch allgemein 14
 durchaus aussagekräftiger Begriff für solche Muster lautet *Nowcasting*. Abzugrenzen
 ist das *Nowcasting* vom *Forecasting*. Besonders große Erwartungen lagen zwischen-
 zeitlich gerade auch auf Prognosen künftiger Ereignisse:

Weil $x_1 \text{ gestern} + x_2 \text{ gestern} + x_3 \text{ gestern} \dots + x_n \text{ gestern} = y_{\text{heute}}$

sei $x_1 \text{ heute} + x_2 \text{ heute} + x_3 \text{ heute} \dots + x_n \text{ heute} = p_{\text{morgen}}$

Schließlich ließe sich in der Zeitdimension noch eine dritte Variante ergänzen: die 15
 der retrospektiven Analytik. Sie ist etwa im strafrechtlichen Bereich denkbar, wenn
 es darum geht, statt aktueller oder künftiger Rechtsverstöße gezielt nach bereits
 abgeschlossenen Taten zu fahnden.³¹

Bei der aktuellen Generation künstlicher Intelligenz müssen Trainings-, Validations- 16
 und Testdaten zuvor in der Regel noch von Menschen z. B. eben als Abbildun-
 gen von Pferden oder Nicht-Pferden gelabelt („klassifiziert“) werden. Die Rede ist
 deshalb von *Supervised Machine Learning*.³² Meist werden dafür gezielt und mit
 großem menschlich-personellem Aufwand Datensätze gelabelt. Eine wichtige, aber
 auch sehr spezifische Quelle des *Labeling* sind beispielsweise die Übersetzungen
 offizieller Texte aus Staaten und von Organisationen mit mehreren Amtssprachen.³³
 Jenseits der Spracherkennung erscheint freilich auch insoweit die Volksrepublik
 China im KI-Kontext besonders entschlossen. China ließ und lässt wohl weiterhin
 gezielt Trainingsdaten etwa auch für die dort immer flächendeckender eingesetzten
 Systeme zur Gesichtserkennung labeln.³⁴ Je nach Input-Daten – man denke an mehr
 oder weniger intime Fotoaufnahmen aus dem letzten Urlaub in der Cloud (für
 Bilderkennung) oder persönliche Gespräche etwa aus *Home-Assistent*-Systemen (für
 Spracherkennung) – liegen die datenschutzrechtlichen Fallstricke des *Labeling* in
 solchen Fällen offen zu Tage.

Teils entstehen die notwendigen Label auch durch die Nutzer von KI-Systemen 17
 selbst. Eine frühe Methode zum nutzergetriebenen *Labeling* sind die bekannten
 CAPTCHA-Verfahren, bei denen Internetnutzer Fotoaufnahmen klassifizieren müs-
 sen („Markiere von den gezeigten neun Bildern alle, die eine Ampel zeigen“), um
 den Zugang zu einer bestimmten Dienstleistung freizuschalten. Genutzt werden

30 Vgl. *Bánbura/Giannone/Reichlin*, ECB Working Paper No. 1275, Dez. 2010, S. 4: “We define nowcasting as the prediction of the present, the very near future and the very recent past.” Für Anwendungsbsp. außerhalb der Finanzwirtschaft *Lampos/Cristianini*, *ACM Transactions on Intelligent Systems and Technology* 3 (2012), 1 ff.

31 Sog. *Retrospective Policing*; dazu *Gless*, in: Herzog/Schlothauer/Wohlers (Hg.), *Rechtsstaatlicher Strafprozess und Bürgerrechte*, 2016, S. 165 (169 f.).

32 Vgl. *Ertel*, *Grundkurs KI*, 2021, Kapitel 8; zur Definition illustrativ a. a. O., S. 351.

33 So waren die Rechtstexte der EU eine wichtige – sozusagen ‚frei Haus‘ vorgelabelte – Lernquelle für das erfolgreiche Übersetzungsprogramm *deepl.com*.

34 s. *Böge*, *F.A.Z.* v. 9.4.2019, S. 3.

können diese Methoden nur in geringem Umfang, da sie für den Nutzer zeitaufwendig sind, eine Dienstleistung daher unattraktiver machen. Effizienter sind nutzerbasierte Lernsysteme dann, wenn sie die Labels gleichsam als „Beifang“ der ohnehin gewünschten Nutzung generieren. Ein datenschutzfreundliches Beispiel dafür sind Autokorrektur-Systeme, deren Vorschläge Nutzer annehmen oder verwerfen, d. h. unmittelbar lernrelevantes Feedback auf ihrem Mobiltelefon bereitstellen. Anhand solchen Feedbacks können die Muster direkt auf dem Gerät des Nutzers ‚lernen‘ und dann mit den Mustern anderer Nutzer geteilt und kombiniert werden, ohne dass personenbezogene Daten des konkreten Nutzers dessen Sphäre verlassen mussten. Diese Variante des maschinellen Lernens wird als *Federated Learning* bezeichnet und ist durch den Verzicht auf personenbezogene Trainingsdaten an zentraler Stelle (*Data Pools*) datenschutzfreundlich.³⁵

- 18 Zugleich passt hier der ansonsten viel zu häufig umfassend für *alle Machine-Learning*-trainierten Anwendungen genutzte³⁶ Begriff des *selbstlernenden Systems*; er besagt, dass das Verhältnis von $x_1 + x_2$ usw. zu y , also das Verhältnis des Inputs zum Output, *nicht* statisch oder „eingefroren“³⁷ ist (wie bei klassischer Technik, Beispiele: Lichtschalter oder Geschwindigkeitsmessgeräten³⁸), sondern dynamisch *neue Trainingsdaten* verarbeiten und das zugrundeliegende x -e-Muster *während der Nutzung* des Systems anpassen kann.³⁹ Es ergibt m. E. guten Sinn, den oftmals unpräzise, weil zu weitgehend verwendeten Begriff der technischen (!) Autonomie intelligenter Systeme (Stichwort Autonomierisiko⁴⁰) ebenso wie den Begriff des

35 Zum Ganzen *Leetaru*, Forbes v. 31.7.2019 (Onlinequelle). Eine andere datenschutzfreundliche Methode des *Machine Learning* stellt die sog. *Differential Privacy* dar. Dazu *Dwork/Roth*, *Foundations and Trends in Theoretical Computer Science* 9 (2014), 211 ff.; zu den durch *Differential Privacy* eintretenden Ungenauigkeiten *Steed et al.*, *Science* 377 (2022), 928 ff.

36 Vgl. etwa *Tischbirek*, in: Kahl/Ludwigs (Hg.), *HVwR V*, 2023, § 126 Rn. 14 ff.; *Guckelberger*, *Öffentliche Verwaltung im Zeitalter der Digitalisierung*, 2019, S. 497 f., bes. Rn. 574; ähnl. *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), *GVwR I*, 32022, § 26 Rn. 118 f.; auch *Hoffmann-Riem*, *AöR* 145 (2020), 1 (3), aber klarstellend in Fn. 54.

37 *Herbert Zech*, *ZfPW* 2019, 198 (203). Der Begriff „eingefroren“ passt grds. auch für *Large Language Models* (dazu ausf. ab → § 1 Rn. 44), bzw. er passt hier sogar besonders, weil deren Determiniertheit mit der sog. *Temperature* dieser Modelle/Muster korrespondiert, die gezielt „niedrig“ gesetzt werden kann, sodass die Determiniertheit zunimmt; dazu *Liu/Skrjanec/Demberg*, arXiv:2311.09325v2 (3.7.2024), *Renze/Guven*, arXiv:2402.05201v3 (2.10.2024), S. 4 sowie *Song et al.*, arXiv:2407.10457 (15.7.2024), S. 4 ff.; zur generellen Realisierbarkeit deterministischer KI-Systeme *Atil et al.*, arXiv:2408.04667v2 (12.9.2024). Allerdings können aufgrund der Architektur dieser Modelle auch bei niedriger *Temperature* Hardware-bedingte und Stand heute unvermeidbare Varianzen auftreten, die aber (wohl) so minimal ausfallen und nur in absoluten Grenzfällen Ergebnisrelevanz besitzen, sodass wir sie für unsere Zwecke (und zum gegenwärtigen Stand der Forschung) vernachlässigen können; zu diesen Varianzen, die ein Zufallselement ins Spiel bringen, *Goldberg*, *ACM Comput. Surv.* 23 (1991), 5; *Kaddour et al.*, arXiv:2307.10169 (19.7.2023), S. 33. Den Hinweis auf diese Restvarianz auch bei „eingefrorenen“ LLM-Systemen verdanke ich *Christoph Engel*, weiterführende, technisch anspruchsvolle Recherchen und Vorarbeiten hierzu *Michael Moghaddam*.

38 Vgl. dazu *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), *GVwR I*, 32022, § 26 Rn. 119.

39 Vgl. auch *Kaminski*, in: Wieglering/Nerurkar/Wadephul (Hg.), *Datafizierung und Big Data*, 2020, S. 151 (156 f.) m. w. N., der bei selbstlernenden Systemen von „transklassischer Technik“ spricht.

40 Hierzu ausf. *Teubner*, *AcP* 218 (2018), 155 (163 ff.).

selbstlernenden Systems auf dieses Szenario zu beschränken. Nach dem Training „eingefrorene“ Systeme *haben* hingegen selbst *gelernt*, was sprachlich z. B. dadurch angezeigt werden kann, dass von ML-trainierten Systemen zu sprechen wäre. Selbstlernende KI-Systeme im engen Sinn sind in sensiblen Anwendungsbereichen – also jenseits der Autokorrektur-Funktion von *Messenger*-Diensten oder *Chatbots* und vergleichbar harmlosen Szenarien – noch selten⁴¹ und nach teilweise vertretener Auffassung im staatlichen Einsatz sogar „kategorial ausgeschlossen“.⁴²

Wie das Beispiel der Autokorrektur-Systeme zeigt, lässt sich *Federated Learning* nur in solchen Szenarios einsetzen, in denen die Nutzenden ‚mitspielen‘. Die Überlegungen gehen daher dahin, den allgemeinen Trend zur sogenannten *Gamification* bei der Nutzung von *Smart Phones* und anderen *Smart Devices* zu nutzen, um auf spielerische Art – z. B. während längerer Pendelfahrten zur Arbeit – zum Labeln aufzufordern, es gegebenenfalls aktiv durch Services oder sogar monetäre Kompensation zu belohnen. Es wird sich erweisen, ob diese Methode zentrale, datenschutzrechtlich problematische Trainingspools⁴³ effektiv wird ablösen können.

Bislang nur für ausgewählte Aufgaben eignet sich demgegenüber das sogenannte *Unsupervised Machine Learning*, das ohne menschlich gelabelte Daten auskommt.⁴⁴ Diese Systeme suchen in der basalsten Version in den Trainingsdaten abstrakt nach Mustern, die besonders häufig oder besonders stark korreliert auftreten (*Clustering* oder Segmentierung). Es handelt sich dabei vor allem um Verfahren der explorativen Datenanalyse,⁴⁵ bei denen das Erkenntnisziel nicht feststeht, sondern bewusst nach unbekannten Zusammenhängen gesucht wird. Es handelt sich um echte Wissensmehrungs-Verfahren, die etwa im Marketing oder der Produktforschung Einsatz finden. *Unsupervised Learning* kann aber auch im Bereich von Gefahrenabwehr oder Strafverfolgung eingesetzt werden, indem der Fokus nicht auf die Cluster gerichtet wird, sondern auf ‚ausreißende‘ Datenmuster (sogenannte *Outliers*) – basierend auf der Annahme, dass das gefährliche oder deviante Verhalten in dem durchsuchten Datensatz eben die Ausnahme gegenüber dem ungefährlichen bzw. re-

41 So auch die Beobachtung von Zech, ZfPW 2019, 198 (203); s. auch Hilgendorf, JZ 2021, 444 (450) zum autonomen Fahren (§§ 1d ff. StVG), das vom autonomen Lernen derzeit noch weit entfernt ist.

42 So Britz/Eifert, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, 32022, § 26 Rn. 118: fehlende Bestreitbarkeit solcher Entscheidungen mangels Reproduzierbarkeit ihrer Ergebnisse. Anders nun BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 – Automatisierte Datenanalyse, Rn. 100, bes. a. E. Dazu auch nochmals ausf. unten, ab → § 2 Rn. 38.

43 Zu deren Notwendigkeit EU-Kommission, COM(2020) 66 final v. 19.2.2020, S. 4 f.

44 Ertel, Grundkurs KI, 2021, S. 351.

45 Zur Genese dieser Subdisziplin ursprünglich der Soziologie Diaz-Bone, Statistik für Soziologen, 2018, S. 300 m. w. N. Monographisch zu relevanten statistischen Methoden Cleff, Deskriptive Statistik und Explorative Datenanalyse, 2015, passim.

gelkonformen darstellt.⁴⁶ In der Theorie kann damit auch das sogenannte implizite Wissen sichtbar und technisch verarbeitbar gemacht werden.⁴⁷

- 21 In fortgeschrittenen Varianten kommt unüberwachtes Lernen als Lernen durch Verstärkung (*Reinforcement Learning*) zur Anwendung, insbesondere in der Robotik⁴⁸ oder beim Erlernen von Spielen. Das System lernt hier durch *Trial and Error* in einem anspruchsvolleren Sinne selbsttätig: Die Input-Daten müssen nicht gelabelt sein (was z. B. bei den Handlungsmöglichkeiten eines mehrdimensional-physisch agierenden Roboters nicht mehr denkbar erscheint). Allerdings muss eine Belohnungsfunktion definiert werden, die im Fall des Erfolgs ein positives Feedback-Signal auslöst und sich der namensgebende Verstärkungseffekt⁴⁹ somit in die richtige Richtung einstellen kann. Das Programmierungs- bzw. Klassifikationsproblem ist beim *Reinforcement Learning* daher auf diese Belohnungsfunktion verlagert: Der Erfolg muss definiert werden. Der menschliche Lehrer kommt damit doch wieder ins Spiel.⁵⁰ Beim Erlernen von Spielen mit klaren Erfolgsdefinitionen – z. B. beim Brettspiel Go durch die KI-Software *AlphaGo*⁵¹ – ist das noch vergleichsweise einfach, bei mehrdimensionalen robotischen Anwendungen schon nicht mehr, sodass hier an Schnittstellen für unmittelbar wertendes menschliches Feedback („Das war gut“/„Das war nicht gut“) gearbeitet wird.⁵²
- 22 Jedenfalls müssen die Trainings- bzw. Input-Datensätze und gegebenenfalls die menschlichen Feedback-Daten in möglichst großer Menge vorliegen oder etwa durch Sensoren unmittelbar generiert werden können. Denn die aktuellen Technologien benötigen noch sehr große Mengen an solchen Trainingsdaten, um Muster mit einer hinreichend starken Generalisierungskraft zu erstellen. Nicht anders sind die beeindruckenden Übersetzungssysteme wie *DeepL* entstanden, das auf umfangreiche Korpora übersetzter – also von Menschenhand gelabelter – Texte unter anderem der europäischen Institutionen aufbaute.⁵³ Werden solche Systeme hingegen auf Realdaten angewandt, die nicht wenigstens fragmentarisch das erlernte $x_1 + x_2 \dots$ etc. aufweisen (logisch aber dennoch eventuell y darstellen), muss ein solches System

46 s. Rademacher, AöR 142 (2017), 366 (373); für einen Anwendungsfall bei der US-amerikanischen *Securities and Exchange Commission* (SEC) s. Freeman Engstrom et al., 2020, S. 24: *Advanced Relational Trading Enforcement Metrics Investigation System* „ARTEMIS“.

47 Skeptisch hingegen Hoffmann-Riem, AöR 145 (2020), 1 (14): „Das für menschliches Handeln einschließlich der Auslegung und Anwendung von Recht so wichtige implizite Wissen scheidet daher für die Programmierung aus.“

48 Vgl. bspw. das Freiburger Verbundforschungsprojekt *reScale* (dazu www.brainlinks-braintools.uni-freiburg.de/de/rescale/; besucht am 22.8.2023).

49 Wischmeyer, AöR 143 (2018), 1 (13) spricht hier treffend von „responsiven Systemen“.

50 Mit einem *Legal-Tech*-Beispiel Yuan, RW 9 (2018), 477 (488).

51 Ausf. zur Struktur des Lernens durch AlphaGo und AlphaGoZero Ertel, Grundkurs KI, 2021, S. 370 ff.

52 Ertel, Grundkurs KI, 2021, S. 351 ff.

53 Merkert, heise online v. 29.8.2017 (Onlinequelle).

versagen. Anders ausgedrückt: Zu deduktiven Transferleistungen ist es nicht in der Lage.⁵⁴

Hinsichtlich der Trainings- bzw. Inputdaten verknüpfen die Technologien des maschinellen Lernens wegen des enormen Datenbedarfs mit dem mittlerweile schon wieder aus der Mode geratenen Begriff *Big Data*. Sinnvoll ist der Begriff immer noch. Denn erst die massenhafte Verfügbarkeit (*Volume*) und schnelle technische Auswertbarkeit (*Velocity*) auch unstrukturierter digitaler Datenbestände (*Variety*) als Lern- oder eben Such-Reservoir für Muster hat den Leistungssprung maschinellen Lernens ermöglicht,⁵⁵ der nun das Attribut von (einem Anschein von) ‚Intelligenz‘ rechtfertigt. Tatsächlich besteht zwischen den mittlerweile weniger häufig genannten Konzepten von *Big Data Analytics*⁵⁶ bzw. *Predictive Analytics*⁵⁷ – die ihre Wurzeln in der Big-Data-Diskussion der frühen 2010er Jahre noch im Namen tragen – und der *Machine-Learning*-getriebenen Variante künstlicher Intelligenz vor allem ein begrifflicher Unterschied. Der in den letzten Jahren vollzogene Begriffswandel verdankt sich wohl der gegenüber *Big Data* größeren Werbewirksamkeit von *künstlicher Intelligenz*. 23

Wichtig ist zuletzt noch ein anderer Aspekt des maschinellen Lernens: Die beschriebene lernende Beobachtung vergangener Vorgänge führt zwar – im *Erfolgsfall* – zu einem System, das verlässlich richtig Input zu Output ordnet („Das ist y_{Pferd} “), führt aber – je nach verwendeter Lern-Methode – nicht zugleich zu Mustern, die nach menschlichen Maßstäben noch verständlich sind. Damit ist das bekannte *Black-Box*-Phänomen aufgerufen, bei dem allerdings mindestens drei Dimensionen zu unterscheiden sind: 24

- Ein Muster kann *erstens* deshalb undurchschaubar sein, schlicht weil es ein Geschäfts- oder sonstwie staatlich geschütztes Geheimnis ist.
- Es kann *zweitens* undurchschaubar wirken, weil – Stichwort *Big Data* – das Training auf Massendaten zu Mustern führt, die so komplex sind (so viele x ’e enthalten), dass selbst diejenigen, die über eine grundsätzlich hinreichende technische Expertise verfügen, die Muster schlicht aufgrund ihrer Dimensionen nicht mehr durchdringen könnten (*Curse of Dimensionality*).

54 Vgl. *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17 m. w. N.

55 Die Idee, künstliche neuronale Netze zu entwickeln, findet sich bereit in dem 1943 veröffentlichten Artikel von *McCulloch/Pitts*, Bulletin of Mathematical Biophysics 5 (1943), 115 ff., ausgebaut dann von *Rosenblatt*, Cornell Aeronautical Laboratory, Report 85-460-1.

56 Prägend *Mayer-Schönberger/Cukier*, Big Data, 2013.

57 s. etwa – immer noch lesenswert – *Siegel*, Predictive Analytics, 2016.

- Schließlich – *drittens* – lässt sich noch eine spezifisch technische Form der *Black Box* ausmachen, nämlich die von *Andrew Selbst* und *Solon Barocas* sogenannten *Non-intuitive Models*.⁵⁸
- 25 Zwei sehr gute Beispiele, um diese Form der *Black Box* zu verstehen, lieferte *Jenna Burrell* in einer frühen Studie von 2016, in der sie zwei einfache maschinelle Lernanwendungen selbst nutzt – ein neuronales Netz zwecks Handschrifterkennung und eine *Support Vector Machine* zum Training eines Spam-Filters – und die ‚Maschine‘ dann zwingt zu zeigen, „How the machine ‘thinks’”.⁵⁹
- 26 Bei der Handschrifterkennung gelingt es ihr bildlich sichtbar zu machen, auf welche Bildpunkte das trainierte neuronale Netz ‚blickt‘, um zu dem Ergebnis zu gelangen, dass bzw. ob ein bestimmter Input eine 1, eine 2 oder eine andere Ziffer darstellt. Es handelt sich dabei um einen Unterfall der *explainable Artificial Intelligence* (xAI),⁶⁰ bei der durch *Feature Visualization*⁶¹ *Heat Maps* erzeugt werden, also „Wärmebilder“,⁶² die visualisieren können, welche Bildpunkte für das ‚Urteil‘ der Software erheblich waren, und die dem Menschen damit erlauben zu hinterfragen, ob diese Bildpunkte aus seiner Sicht plausibel und sinnvoll mit dem Ergebnis verknüpft sind. Das Ergebnis von *Burrell* ist erstaunlich: Das an dem handschriftlichen Input trainierte Programm ‚blickt‘ auf Stellen der zu identifizierenden Ziffern-Bilder, die aus menschlicher Sicht keineswegs phänotypisch für eine, sagen wir: 7 stehen – und gleichwohl liefert die Software verlässlich gute Ergebnisse bei der Erkennung handschriftlicher Ziffern.
- 27 Nicht viel besser verhält es sich im Fall des Spam-Filters. *Burrell* testet diesen an einer E-Mail aus den 2000ern, die für einen Menschen wohl ohne weiteres als Spam erkennbar gewesen ist (sogenannter Nigeria 419 Scam⁶³). Die verwendete Lernmethode (*Support Vector Machine*) erlaubt es anzuzeigen, mit welchem Gewicht bestimmte Begriffe in die Klassifizierungsentscheidung über „Spam ja/nein?“ einfließen. Das Ergebnis ist, dass aus menschlicher Sicht unverdächtige Begriff wie „our“ (0,500810 pro Spam), „click“ (0,464474 pro Spam) oder „visit“ (0,369730 pro Spam) maßgeblich sind. Interessanterweise⁶⁴ wies der von *Burrell* trainierte Algorithmus Ortsbezeichnungen wie „Nigeria“ nicht als entscheidungserheblich aus (0,001861).

58 Grundl. zur Unterscheidung *Pasquale*, *The Black Box Society*, 2015; zum dritten Aspekt ausf. *Selbst/Barocas*, *Fordham Law Rev.* 2018, 1085 (1096 ff.).

59 *Burrell*, *Big Data & Society* 3 (2016), 1.

60 Dazu ausf. unten, → § 1 Rn. 49 ff.

61 *Samek et al.*, *Explainable AI*, 2020.

62 *Lenzen*, *F.A.Z.* v. 24.5.2017, S. N4.

63 „My Dearest, Greetings to you my Dear Beloved, I am Mrs Alice Walton, a citizen of United State. I bring to you a proposal worth \$ 1,000,000,000.00 [...]”, s. *Burrell*, *Big Data & Society* 3 (2016), 1 (8).

64 Vgl. auch *Waltl/Vogl*, *DuD* 2018, 613 (617): „On the one hand this is valuable information to assess the trustworthiness of a classifier, and on the other hand this information could also be used to determine whether a classifier is discriminating on problematic attributes [...]”.

Als *Burrell* nun die pro-Spam-Begriffe aus ihrer Test-E-Mail entfernte, den Inhalt aber ansonsten – für einen Menschen unverkennbar ‚spamhaft‘ – unverändert ließ, klassifizierte sie die Software als Non-Spam. Sie hat händisch das vorgemacht, was zwischenzeitlich als „kontrafaktische Begründung“ besondere Aufmerksamkeit in der xAI-Forschung erlangt hatte: die Systeme derart auszugestalten, dass sie proto-kausal angeben können, dass y bejaht wurde, weil x_k war, y hingegen vereint worden wäre, wenn kontrafaktisch x_r gewesen wäre.⁶⁵

Vor allem zeigen die beiden Beispiele von *Burrell*, dass die Auswertungsergebnisse von KI-Technologien unter Umständen durchaus nachvollziehbar sein können in einem formellen, technischen Sinn – es kann je nach Lernmethode recht gut dargestellt werden, welche *Features* (welche x 'e) für y_{spam} usw. entscheidend oder zumindest erheblich waren. *Materiell* nachvollziehbar im Sinn von *sinnvoll* ist diese Darstellung damit aber noch lange nicht.⁶⁶ Mit *Jenna Burrell* gesprochen gilt: “When a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension.”⁶⁷

II. Angewandte Statistik und deren Probleme

Die beschriebenen Funktionsbedingungen des maschinellen Lernens lassen sich zu einer epistemischen Grundannahme verallgemeinern: *Es ist der rein beobachtende – nicht: der verstehende – Blick zurück in die Vergangenheit, der die Gegenwart oder sogar die Zukunft erkennen lässt.*⁶⁸ Weil mit einem gesuchten y in einem Set an Trainings- und Testdaten aus der Vergangenheit eine bestimmte Konstellation an *Features* (x 'en) verknüpft (‚gelabelt‘) wurde, gehen wir davon aus, dass diese Konstellation, erfasst sie eine Software heute erneut in den vorgegebenen Input-Daten, wieder den Schluss erlaubt, dass y vorliegt bzw. vorliegen wird. Welche der verschiedenen verfügbaren statistischen Methoden genutzt werden, bestimmt der

⁶⁵ Ausf. hierzu → § 1 Rn. 53.

⁶⁶ Nach der Klassifikation von *Burrell*, *Big Data & Society* 3 (2016), 1, bes. S. 4 ff., die auf der grundlegenden Unterscheidung von drei Arten von algorithmischer Opazität bei *Pasquale*, *The Black Box Society*, 2015, aufbaut, handelt es sich nur bei der fehlenden materiellen Nachvollziehbarkeit um diejenige *Black Box* bzw. Opazität, die „charakteristisch“ für maschinelles Lernen sei. Opazität qua Geschäfts- oder Staatsgeheimnisses (“Opacity as intentional corporate or state secrecy”, S. 3 f.), wegen der schieren Menge an Code und Muster-relevanten Input-Daten („Dimensionalität“), sowie wegen der fehlenden technischen Kompetenzen weiter Teile der Bevölkerung (“Opacity as technical illiteracy”, S. 4, 9), würden hingegen auch bei klassischen Algorithmen vorkommen, die gemeinhin nicht als KI qualifiziert werden würden.

⁶⁷ *Burrell*, *Big Data & Society* 3 (2016), 1 (10). An dieser Stelle noch ein Hinweis auf aktuellste Forschungen: Das Unternehmen *Anthropic* hat offenbar erste Erfolge dabei erzielt, auch in hochkomplexen LLM-Modellen (→ § 1 Rn. 44) *Features* zu identifizieren, die menschlich eben doch nachvollziehbar sind. Einsatzreif ist das energieintensive Verfahren, das erhebliche Chancen i. S. der *explainable AI* bieten dürfte, aber wohl noch lange nicht; s. hierzu *Templeton et. al*, *Transformer Circuits Thread* v. 21.5.2024 (Onlinequelle).

⁶⁸ Vgl. schon – dort noch auf den Begriff *Big Data* bezogen – *Rademacher*, AöR 142 (2017), 366 (367).

Mensch bzw. genauer gesagt: wird in der Praxis eine Gruppe von Menschen bestimmen, die den keineswegs trivialen Auswahl- und anschließenden Trainingsprozess organisiert.⁶⁹ Dabei fiele der staatliche Umgang mit maschinellem Lernen alias künstliche Intelligenz wahrscheinlich leichter, wenn ‚Statistik‘ bereits als Referenz- und Handlungsfeld erschlossen wäre.⁷⁰ Gleichwohl erscheint es mir etwas zu überspitzt formuliert, das Sich-Verlassen auf maschinelle vergangenheitsbasierte Schlüsse als „implizites Gottvertrauen [in die] Objektivität numerischer Kategorisierungen“ werten zu wollen.⁷¹

- 30 Dennoch rechtfertigen die statistischen Funktionsbedingungen von maschinellem Lernen die grundsätzliche Warnung vor Pfadabhängigkeiten, die dieser Form von KI in mehrfacher Weise zugrunde liegen können, und eben häufig auf diversen Auswahlentscheidungen der genannten Menschen(gruppe) beruhen – das Vertrauen in diese *Personen* und deren *Produkte* muss daher gleichermaßen problematisiert werden.⁷² Die folgenden sechs Schlaglichter stellen eine Auswahl an möglichen statistikbedingten Fehlerquellen dar, die für rechtserkenntnisfähige Technologien eine besondere Bedeutung haben; viele der Fehlerquellen werden nun vom neuen Art. 10 AI Act [Daten und Daten-Governance] adressiert.⁷³ Einen Anspruch auf Vollständigkeit, was die möglichen Probleme anbelangt, erhebe ich hier nicht.⁷⁴
- 31 *Sampling Bias*: Ein *Sampling Bias* oder *Selection Error* liegt vor, wenn eine bestimmte *Feature*-Konstellation, die in der Realität die Voraussetzungen von *y* erfüllt, in den Trainingsdaten unter- oder überrepräsentiert ist.⁷⁵ Das klassische Beispiel ist Software zur Auswahl von Bewerbern um Arbeits-⁷⁶ oder Studienplätze,⁷⁷ die – *prima facie* rational – anhand vergangener Leistungsdaten trainiert wurde. Problematisch wird das dann, wenn nicht überprüft wird, ob die Daten eventuell deshalb weiße Männer als besonders leistungsfähig ausweisen, weil der Arbeitgeber oder die

69 Hoffmann-Riem, AöR 145 (2020), 1 (12). Für eine differenzierende Darstellung der Vorgaben von menschlichen Programmierern (statistisch-mathematische Methode) und Trainern (Anwendung auf zu bestimmende Trainings- und Testdaten) Zech, in: Verhandlungen des 73. Deutschen Juristentages Hamburg 2020/ Bonn 2022 (Hg.), Bd. I: Gutachten (Gesamtband A - G + CD), 2020, S. A 34 ff.

70 Dazu Voßkuhle, in: ders./Eifert/Möllers (Hg.), GVwR I, ³2022, § 1 Rn. 45: „Weiter auf [seiner] Entdeckung warte[t] dagegen z. B. das [...] Statistikrecht.“ Der Vorschlag der Kommission für den AI Act, „statistische Ansätze“ neben maschinellem Lernen und regelbasierten Systemen als *eigenständige* dritte KI-Technikkategorie zu nennen (Anhang I lit. c AI Act-Entwurf), sie also ungeachtet davon zu erfassen, ob die statistischen Methoden im Rahmen maschineller Lernverfahren Anwendung finden oder nicht, wurde zutreffend als zu weitgehend kritisiert; der Unionsgesetzgeber ist ihm nicht gefolgt.

71 So Martini, Blackbox Algorithmus, 2019, S. 49. Zum sog. *Automation Bias* sogleich, → § 1 Rn. 35.

72 Ähnl. auch die Analyse von Burchard, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 553 (567).

73 Hierzu mehr unten, → § 4 Rn. 139 f.

74 Für eine Gesamtübersicht über mögliche *Biases* in KI-Systemen s. Richardson/Gilbert, arXiv:2112.05700v1 (10.12.2021); Ntoutsis et al., arXiv:2001.09762v1 (14.1.2020).

75 Vgl. ausf. Tischbirek, in: Wischmeyer/Rademacher (Hg.), Regulating Artificial Intelligence, 2020, S. 103 Rn. 3 ff.; Hermstrüwer, AöR 145 (2020), 479 (492 ff.).

76 Kim, William & Mary Law Rev. 58 (2017), 857 ff.; Martini, Blackbox Algorithmus, 2019, S. 53 f.

77 Das Bsp. wird ausf. beschrieben bei Hacker, CMLR 55 (2018), 1143 (1148).

Hochschule in der Vergangenheit schlicht nur weiße Männer beschäftigt bzw. immatrikuliert hat, sie also in den Trainingsdaten im Vergleich zur Gesamtheit leistungsfähiger Menschen zu häufig vorkommen. Ähnliches kann im verwaltungsrechtlichen Bereich passieren, wenn etwa gefahrenabwehrrechtliche Modelle ausschließlich am Inhalt von Polizeiakten trainiert werden, wenn und weil darin die *nicht*-pathologischen Fälle ebenso wie die (Devianz-)Daten sozial integrierter Gruppen unterhalb des üblichen polizeilichen Fahndungsspektrums fehlen.⁷⁸ Menschliche Vorurteile oder, neutraler formuliert: Auswahlentscheidungen werden hier durch die dann eben nur noch vermeintlich objektiv-neutrale Software fortgeschrieben (Fall des *Historical Sampling Bias*), jedenfalls bleibt das durch *Machine Learning* erzeugte Muster mit Blick auf bislang vernachlässigte Szenarien uninformatiert.⁷⁹ Philipp Hacker illustriert am mittlerweile berüchtigten *Google-Gorilla*-Fall anschaulich, welche krasse Konsequenzen *Sampling Bias* haben kann: Verkennt die Erkennungssoftware eines autonomen Kraftfahrzeugs einen Menschen mit dunkler Hautfarbe als Tier (wenn bzw. weil die Software in der Trainingsphase nur anhand der Bilder hellhäutiger Menschen auf y_{Mensch} trainiert wurde), dann wird sie in einer Unfallkonstellation im Zweifel Schaden an diesem ‚Objekt‘ deutlich geringer gewichten und daher eher verursachen.⁸⁰ In einem solchen Fall läge kein historisch bedingter *Sampling Bias* vor, sondern einer, der auf eine schlichte Fehltauswahl der Trainingsdaten zurückzuführen wäre. Eine Lösung dieses Problem dürfte darin liegen, eine möglichst umfassende Datensammlung zu generieren, wo nötig und möglich durch Zufallsstichproben, was je nach Sachbereich bis hin zu experimenteller/randomisierter Entscheidungsfindung etwa durch Los gehen kann.⁸¹

Proxy Discrimination: Idealerweise wäre künstliche Intelligenz ein Instrument, um 32 klassische Diskriminierungen zu bekämpfen.⁸² Denn immerhin können verpönte Merkmale oder zumindest starke Korrelationen von y etwa mit der Hautfarbe sichtbar gemacht und aktiv aus den Trainingsdaten oder sogar aus dem Modell selbst entfernt werden;⁸³ freilich gegebenenfalls zum Preis einer geringeren Genauigkeit des Modells.⁸⁴ Dieser Vorzug KI-gesteuerter Erkenntnisverfahren droht aber

78 Hermstrüwer, AöR 145 (2020), 479 (494); Rademacher, AöR 142 (2017), 366 (373).

79 Vgl., illustriert am Bsp. von Vergabeverfahren, in denen i. d. R. nur Daten über die Leistungen erfolgreicher Bieter genutzt werden können, Hermstrüwer, in: Wischmeyer/Rademacher (Hg.), *Regulating Artificial Intelligence*, 2020, S. 199 (206); ob andere Bieter, wären sie erfolgreich gewesen, bessere Leistungen erbracht hätten, lässt sich mit derartigen Modellen also kaum sagen.

80 Hacker, CMLR 55 (2018), 1143 (1147). Zum Stand von Bilderkennung und Diskriminierungsgefahren Fabbri et al., arXiv:2107.07919v2 (24.6.2022).

81 Dazu ausf. Hermstrüwer, AöR 145 (2020), 479 (497): „Vorübergehend suboptimale – weil lotterartige – Entscheidungen sind wohl unverzichtbar, um die Daten zu generieren, die langfristig für optimale Klassifikationen und Prognosen erforderlich sind (*Exploring*).“

82 Capers, North Carolina Law Rev. 95 (2017), 1241 ff.

83 Hermstrüwer, AöR 145 (2020), 479 (481, 501 ff.); s. auch Rademacher, AöR 142 (2017), 366 (376) m. w. N.

84 Insoweit besonders krit. Martini, *Blackbox Algorithmus*, 2019, S. 56–58.

durch das Phänomen der *Proxy Discrimination* verloren zu gehen.⁸⁵ *Proxies* sind Variablen ($x'e$), die zwar nicht selbst verpönt sind, aber stark mit einem verpönten Merkmal korrelieren; in der diskriminierungsrechtlichen Terminologie sind das die sogenannten indirekten Diskriminierungen.⁸⁶ KI-Verfahren sind geradezu darauf getrimmt, *prima facie* versteckte Korrelationen nutzbar zu machen, wenn ihnen zwar faktisch aussagekräftige Variablen fehlen oder ihnen, weil sie normativ unerwünscht sind, entzogen werden.⁸⁷ So ist der Geburtsort ein klassisches Proxy für die Hautfarbe (in den USA) bzw. den Migrationshintergrund (in Deutschland). Korreliert nun der Geburtsort – als vermeintlich nicht verpöntes *Feature* – mit einer statistisch signifikanten Kriminalitätsneigung, folgt daraus durch die Hintertüre *dunkle Hautfarbe/arabische Ethnie = kriminell*. Um solche *Proxies* erkennen und aus den Gleichungen eliminieren zu können, mehrten sich – im ersten Moment kontraintuitiv – die Forderungen, wonach die verpönten Kriterien gezielt erfasst und gespeichert werden sollten, um Modelle anhand von ihnen gezielt testen zu können (vgl. nun Art. 10 AI Act).⁸⁸ Zudem spielen hier Konzepte eine wichtige Rolle, wonach generell (veränderbaren) Verhaltens- anstelle von (statischen) Eigenschafts-bezogenen Prädiktoren der Vorzug eingeräumt werden sollte.⁸⁹

- 33 *Prima facie* gewollte Verstärkungseffekte: KI-Systeme sind in vielen Fällen Selektionsagenten, die dafür geschaffen sind, aus der Flut an Informationen solche auszuwählen, die – in der Regel aufgrund einer selbst oder von Dritten gewählten Voreinstellung – interessant oder relevant sein könnten. Nebenliegendes, eventuell Irritierendes bringen diese Agenten einem so Informierten ‚idealerweise‘ immer weniger zur Kenntnis. Besonders deutlich wird dieser Effekt erzeugt durch die Algorithmen mancher sozialer Netzwerke und News-Aggregatoren.⁹⁰ Dort wird er verhandelt unter den heute berühmten, wenn auch mittlerweile wegen der schwachen Empirie⁹¹ eher kritisch kommentierten Stichworten der „Echokammern“⁹² und „Filterblasen“.⁹³

85 s. Hacker, CMLR 55 (2018), 1143 (1148 ff.) m. w. N.; ausf. Schwarcz/Prince, Iowa Law Rev. 105 (2020), 1257 ff.

86 Vgl. hierzu, aber v. a. auch zu neueren Untersuchungen zu direkter Diskriminierung durch Algorithmen, Adams-Prassl/Binns/Kelly-Lyth, The Modern Law Rev. 86 (2023), 144 ff. m. w. N.

87 Schwarcz/Prince, Iowa Law Rev. 105 (2020), 1257 ff.

88 Tischbirek, in: Wischmeyer/Rademacher (Hg.), Regulating Artificial Intelligence, 2020, S. 103 Rn. 26 ff.; Hermstrüwer, AöR 145 (2020), 479 (501 ff.); s. aber auch Veale/Binns, Big Data & Society 4 (2017), 1. Mehr zu Art. 10 AI Act unten, → § 4 Rn. 139 f.

89 Vgl. dafür bes. EuGH, Gutachten 1/15 v. 26.7.2017 (Fluggastdatenabkommen EU/Kanada), Rn. 165: „Insofern ist festzustellen, dass jede Maßnahme, die auf dem Postulat beruht, dass eines oder mehrere der [grundrechtlich verpönten] Merkmale *als solche, unabhängig vom konkreten Verhalten* des betreffenden Fluggasts, für das in der Bekämpfung von Terrorismus und grenzübergreifender schwerer Kriminalität bestehende Ziel der Verarbeitung von PNR-Daten erheblich sein könnte, gegen die in den Art. 7 und 8 der Charta in Verbindung mit deren Art. 21 niedergelegten Rechte verstößt.“ Hervorhebung hier.

90 Für eine Übersicht über die Diskussion s. Martini, Blackbox Algorithmus, 2019, S. 99 ff.

91 Dazu die Übersicht bei Schemmel, Der Staat 57 (2018), 501 (509 ff.).

92 Hierzu *ibid.*, S. 507 f.

93 Begriffsprägend Pariser, Filter Bubble, 2017, *passim*.

Funktionieren diese Systeme gut, dann bewirken sie eine thematische Isolierung des Einzelnen am Maßstab seiner eigenen, immer weiter fokussierten und wiederholten *Präferenzen*, sozusagen ein immer weiter forciertes Zurückgeworfen-sein auf das ‚pure‘ Selbst (Echokammer) bzw. eine Gruppe, die dieses Selbst am genauesten spiegelt (Filterblase). Die potentiell negativen Konsequenzen für demokratische Gemeinwesen, die auf wechselseitigen Ausgleich und Kompromiss und das heißt zunächst: auf Konfrontation mit der jeweils anderen Auffassung angewiesen sind, werden intensiv diskutiert.⁹⁴ Ich gehe auf die rechtlichen Rahmenbedingungen dieser Effekte unten nochmals ausführlicher ein (→ S. 224 ff.). Jenseits individueller Präferenzen lassen sich Verstärkungstendenzen aber auch im Bereich der eigenen *Fähigkeiten* vermuten, nämlich dann, wenn zunehmend intelligente Lern- und Trainingshilfen darauf gerichtet sind, individuelle ‚Stärken zu stärken‘. Werden diese in größeren Lebenskontexten eingesetzt, wie etwa bei Auswahlsoftware im Rahmen der Studienwahl, ist das zwar kein Pfad in eine soziale Isolation. Allerdings droht eine stark deterministische Gesellschaft(sordnung), in der zumindest ungeplante Experimentierräume sukzessiv verschlossen werden könnten (dazu → S. 541 ff.).

Ungewollte Verstärkungseffekte: Eng damit verwandt ist schließlich die Gefahr eines ungewollten „Rückkoppelungseffekts“⁹⁵ für die Muster selbst, der eintreten kann, wenn Muster anhand zwar neuer realer Daten (nach)trainiert werden, diese neuen Daten allerdings aus Entscheidungen hervorgegangen sind, die unter Nutzung des ursprünglichen Musters getroffen wurden. Am Beispiel:⁹⁶ Werden aufgrund eines *Predictive-Policing*-Modells mehr Personendurchsuchungen in einem bestimmten Postleitzahl-Bezirk durchgeführt, dann werden in diesem Bezirk wahrscheinlich allein deshalb, also wegen des fokussierten Zugriffs, mehr Delikte aktenkundig und damit trainingsdatenfähig als zuvor. Das Modell wird daher für diesen Bezirk bzw. strukturell vergleichbare Bezirke potentiell immer präziser und erhöht damit die Wahrscheinlichkeit, dass ursprünglich in dem Modell enthaltene Verzerrungen immer stärkeres Gewicht erhalten.

Modelling Bias: Kein eigentliches Spezifikum von *Machine-Learning*-Technologien stellt der in diesem Kontext auch häufig genannte *Modelling Bias* dar.⁹⁷ Diagnostiziert wird er bei Prädiktions- oder Klassifikationssystemen, deren Zielvariable y nicht einfach und objektiv verifizierbar ist (wie das Alter), sondern selbst Wertungen enthält (z. B. die gute oder weniger gute Eignung für eine ausgeschriebene Stelle oder für ein Studium, insbesondere durch Anknüpfung an Schulnoten), also

94 Sunstein, #Republic, 2017, passim; Schemmel, Der Staat 57 (2018), 501 (505 ff.); Martini, Blackbox Algorithmus, 2019, S. 213; Wischmeyer, ELJ 2019, 169 ff.

95 Hermstrüwer, AöR 145 (2020), 479 (493).

96 Nach Hermstrüwer, AöR 145 (2020), 479 (493).

97 Für eine knappe Zusammenfassung s. Criado/Such, in: Yeung/Lodge (Hg.), Algorithmic Regulation, 2019, S. 82 (85 f.).

durch einen menschlichen Programmierer modelliert ist. Dass hier im Rahmen der menschlichen Definition dessen, was gute oder schlechte Eignung ausmacht, menschliche (Vor-)Urteile oder disparate sozioökonomische Bedingungen einfließen können – und letztlich wohl sogar in gewissem Umfang einfließen sollen und dürfen –,⁹⁸ versteht sich von selbst. Zu einem Themenfeld künstlicher Intelligenz wird der *Modelling Bias* also nur dann und deshalb, weil man Maschinen an menschlich beeinflusste Faktoren anknüpfen lässt und Menschen den maschinell erstellten Prognosen und Klassifikationen *dann dennoch* einen *per se* höheren Objektivitäts- oder gar Richtigkeitsgrad attestiert (sogenannter *Automation Bias*).⁹⁹

- 36 *Accuracy-Fairness-Trade-off*: Der viel diskutierte *Accuracy-Fairness-Trade-off* schließlich meint den Umstand, dass Fehlerraten (*False Positives* wie auch *False Negatives*) über Subpopulationen ungleich verteilt sein können, selbst dann, wenn die Trainingsdaten selbst keine Verzerrungen enthalten mögen. Ursache dafür ist, dass statistische Verfahren auf eine Gesamtfehlerminimierung abzielen, und damit die Reduzierung von Fehlern zugunsten der Mehrheit und nicht von Minderheitspopulationen betreiben. Ohne Modifikation würde das dazu führen, dass die „Fehlerrate für Minderheiten stets höher ist als für Mehrheiten.“¹⁰⁰
- 37 Zuletzt bleibt noch festzuhalten, dass statistische Methoden gegenwärtig keine Kausalitäten aufdecken können, sondern lediglich Korrelationen anzeigen.¹⁰¹ Die hintergründigen Kausalitätsmodelle, ohne die aus statistischen Erkenntnissen häufig keine sinnvollen Handlungsmaßgaben abgeleitet werden können, muss bislang der menschliche Auswerter beisteuern, da der Computer leicht sogenannte *cum-hoc-ergo-propter-hoc*-Schlüssen erliegt.¹⁰² Ein simples Beispiel liefert eine berühmt gewordene Studie von *Rich Caruana* et al. von 2015:¹⁰³ Die Autoren fanden heraus, dass ein Muster, das darauf trainiert war, mögliche Komplikationen im Zusammenhang mit Lungenentzündungen vorherzusagen, Asthma als risikoverringern den Faktor enthielt. Das ist nicht nur *non-intuitive*, sondern nach allen medizinischen Kenntnissen offensichtlich falsch. Ursache dieser Korrelation war (wohl), dass Patienten, die an Asthma leiden, ihre Atmung aufmerksamer beobachteten, daher rascher ärztliche Hilfe suchten und diese dann wegen der Vorerkrankung auch schneller und intensiver erhielten.¹⁰⁴ Oder man denke, um ein weiteres Beispiel zu nennen, noch simpler an Daten, die erkennen lassen, dass die Zahl von Bränden positiv

98 Etwa i. R. der ggf. einschlägigen Antidiskriminierungsvorgaben.

99 Hierzu nochmals → § 4 Rn. 77, 82, auch zu technischen Reaktionsmöglichkeiten.

100 *Hermstrüwer*, AöR 145 (2020), 479 (495). Zu Lösungen unten, → § 3 Rn. 102 ff.

101 Statt aller *Wischmeyer*, in: Ebers et al. (Hg.), *RechtsHdb, KI und Robotik*, 2020, § 21 Rn. 2, 47.

102 Dazu *Martini*, *Blackbox Algorithmus*, 2019, S. 60.

103 *Caruana* et al., in: Cao (Hg.), *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, S. 1721.

104 Vgl. auch *Selbst/Barocas*, *Fordham Law Rev.* 2018, 1085 (1123).

mit der Zahl der in einem Gebiet aufhältigen Feuerwehrleute korreliert.¹⁰⁵ Welches die falsche Schlussfolgerung hieraus wäre, liegt auch hier auf der Hand – für einen Menschen. Ein Computer, der ohne ein Bild der Welt im Ganzen vor diesen ‚Zahlen‘ stünde, könnte ohne menschliche Supervision eben diese falsche Reaktion anregen. Forschungen an *Kausalzusammenhänge* erschließender Statistik gibt es zwar,¹⁰⁶ aber sie stecken in den Anfängen.

III. Symbolische künstliche Intelligenz, General-purpose AI und explainable AI

Es fällt auf, dass rechtswissenschaftliche Abhandlungen zu KI seit Konstituierung dieses Rechtsgebiets – wir sprechen über einen Zeitraum von kaum zehn Jahren¹⁰⁷ – fast immer künstliche Intelligenz mit maschinellern Lernen gleichsetzen.¹⁰⁸ Dabei vertrauten Forschung und auch die wenigen praktischen Anwendungen in der ersten KI-Hochphase, die bis Ende der 1980er Jahre andauerte,¹⁰⁹ nicht auf das Konzept maschinellen Lernens.¹¹⁰ *State of the Art* waren lange Zeit sogenannte regelbasierte oder symbolische Systeme. Diese Systeme sind gemeint, wenn heute von klassischer KI¹¹¹ oder etwas despektierlich von *Good old-fashioned AI*¹¹² die Rede ist.

Bevor ich diese Technologie/Lern-Methode näher beschreibe (und auch darauf 39 eingehe, was sie mit *explainable AI* und *General-purpose AI* zu tun hat, die heute – Stand 2025 – für die Schlagzeilen sorgt), noch einmal ein Hinweis zum Vorgehen: In diesem § 1 möchte ich möglichst knapp mit den Grundbegriffen von KI vertraut machen, soweit sie für die rechtswissenschaftliche Analyse hilfreich sind. Fragen der konkreten rechtlichen Leistungsfähigkeit von KI, z. B. als rechtserkenntnisfähige Technologien, behandle ich ausführlicher beim Mensch-Maschine-Vergleich in → § 3 (= S. 271 ff.).

105 Vgl. mit dieser Illustration schon Rademacher, AöR 142 (2017), 366 (375).

106 Barocas/Hardt/Narayanan, Fairness and Machine Learning, 2021, S. 77 ff.; Pearl/Mackenzie, The Book of Why, 2019; Mooij et al., Journal of Machine Learning Research 17 (2016), 1 ff.

107 Erst seit 2015 finden sich bei beck-online Aufsätze zum Stichwort „künstliche Intelligenz“ im zweistelligen Bereich; mittlerweile nähern wir uns langsam dem vierstelligen Bereich.

108 Bes. deutlich, weil sogar ohne Hinweis auf die Alternativen, Martini, Blackbox Algorithmus, 2019, S. 17 ff., bes. S. 20, dort Fn. 86; vgl. aber auch Wischmeyer, AöR 143 (2018), 1, in und bei Fn. 38, mit knapper Darstellung auch des „symbolischen Ansatzes“; außerdem Rademacher/Wischmeyer, in: Wischmeyer/Rademacher (Hg.), Regulating Artificial Intelligence, 2020, S. V Rn. 5 und die einzelnen Arbeitsdefinitionen von *Artificial Intelligence* im gesamten Band.

109 Garnelo/Shanahan, Current Opinion in Behavioral Sciences 29 (2019), 17.

110 Einflussreich das Buch von Minsky/Papert, Perceptrons, 1969, über das die beiden Autoren in der 3. Aufl. von 1990 (Prolouge, S. xii) mutmaßen, dass ihr Buch mit seinen kritischen Erkenntnissen dafür verantwortlich gewesen sein könnte, dass die schon in den 1940er Jahren begonnenen Forschungen an neuronalen Netzwerken (damals sog. „Perceptrons“, vgl. dazu die Nachw. in → § 1 Fn. 55) bis in die 1990er Jahre unterbrochen wurden.

111 Garnelo/Shanahan, Current Opinion in Behavioral Sciences 29 (2019), 17.

112 Kaplan, Artificial Intelligence, 2016, S. 27.

- 40 Nun zur symbolischen KI. Eine gut nachvollziehbare Definition davon liefern *Marta Garnelo* und *Murray Shanahan*:

“A symbolic AI system works by carrying out a series of logic-like reasoning steps over language-like representations. The representations are typically propositional in character, and assert that certain relations hold between certain objects [knowledge base¹¹³], while each reasoning step computes a further set of relations that follow from those already established, according to a formally specified set of inference rules [inference engine¹¹⁴].”¹¹⁵

- 41 Sprachlich eher verunglückt,¹¹⁶ aber in der Sache ähnlich, nennt nun auch der einschlägige Erwägungsgrund 12 des AI Act symbolische KI als von der Regulierung erfasste Technologie:

„Ein wesentliches Merkmal von KI-Systemen ist ihre Fähigkeit, abzuleiten. [...] Zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, gehören Ansätze für maschinelles Lernen [...] sowie *logik- und wissensgestützte Konzepte*, wobei aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe abgeleitet wird.“
ErwGr. 12, S. 3 und 5, Hervorhebung hier.

- 42 Aussagen symbolischer KI entstehen also aus Kombinationen von für sich selbst bereits aussagekräftigen Teilaussagen, denen durch eine regelgeleitete Komposition zusätzliche Aussagekraft zukommt (in der Linguistik/Logik: Kompositionalitätsprinzip).¹¹⁷ Um in der oben verwendeten Formel zu sprechen: Die *x*'e einer maschinell trainierten KI sind nur in der jeweiligen konkreten Verknüpfung sinntragend (*entangled*), weshalb diese Lernmethode auch als *konnektionistisch* bezeichnet wird.¹¹⁸ Im Gegensatz dazu sind die *x*'e einer symbolischen KI jeweils selbst sinntragend (*disentangled*)¹¹⁹ und sind vor allem relational, verfügen also über Informationen über ihr hierarchisches (also z. B. kausales, zeitliches oder örtliches¹²⁰) Verhältnis¹²¹ zu weiteren Sinneinheiten. *Gary Marcus* und *Ernest Davis* sprechen von

113 Ibid., S. 23.

114 Ibid.

115 *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17. Vgl. auch ausf. *Harnad*, Physica D: Nonlinear Phenomena 42 (1990), 335 (336).

116 Besser gelungen *insoweit* der AI Act-Entwurf, wo in Anhang I lit. b zu KI gerechnet werden sollten: „Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme“.

117 *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17 f.

118 *Harnad*, Physica D: Nonlinear Phenomena 42 (1990), 335 (337): “connectionism”; *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17: “connectionist paradigm”, jeweils als alternativer Ausdruck für neuronale Netze. Auf die kurz vor Drucklegung dieser Arbeit erschienen Forschungen dazu, auch in maschinell trainierten Algorithmen sinntragende Informationszusammenhänge zu identifizieren, sei nochmals hingewiesen, s. Details in → § 1 Fn. 67.

119 *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17 (18).

120 Mit diesen Bsp. für Relationen, zurückgeführt auf *Kants* Kritik der reinen Vernunft, *Marcus/Davis*, Rebooting AI, 2019, S. 161 und ff.

121 *Y. Bengio/Courville/P. Vincent*, IEEE Transactions on Pattern Analysis and Machine Intelligence 35 (2013), 1798, 3.4.

Knowledge Frameworks,¹²² gebräuchlich ist auch der Begriff der *Knowledge Base*.¹²³ Man könnte auch sagen, dass symbolische KI ‚plastisch‘ ist, gegenüber der ‚flachen‘ KI, die aus maschinellern Lernen resultiert. Um ein konkreteres Beispiel anhand des obigen Feuerwehrfalls zu bilden:¹²⁴ Symbolische KI ‚wüsste‘, dass offenes Feuer am Haus unerwünscht ist, dass Feuerwehrleute Feuer bekämpfen und deshalb *als Folge* des Feuers gerufen werden; und die Zahlen Feuer / Feuerwehrleute *deswegen* positiv korrelieren. Diese KI sollte den korrelationsbasierten Fehlschluss ausschließen, dass es häufiger brennt, weil mehr Feuerwehrleute vor Ort sind.¹²⁵ Kompositionelle Systeme erlauben damit Rekombinationen von Sinneinheiten, die das System zuvor nicht in den Trainingsdaten ‚gefunden‘, also nicht ‚gelernt‘ hatte.

Symbolische KI ist daher ihrem Grundgedanken nach nicht nur menschlich nachvollziehbar (eben weil aus je für sich sinntragenden x'en zusammengesetzt), sondern *idealerweise* auch zu starken Generalisierungen fähig (deshalb auch der gerade in diesem Zusammenhang häufig anzutreffende Begriff der *Artificial General Intelligence* – AGI – oder *General Artificial Intelligence*), was sie wiederum vergleichsweise datensparsam macht.¹²⁶ Dass sich konnektionistische KI (also maschinelles Lernen) als aktuell dominante Methode und damit als Synonym für KI insgesamt durchsetzen konnte, liegt an der bisherigen (menschlichen)¹²⁷ Unfähigkeit, die auf reale Sachverhalte anzuwendenden Regeln und Relationen in hinreichender Zahl und Genauigkeit darzustellen, d. h. händisch zu programmieren. Versuche, zumindest bereichsspezifisch brauchbare Systeme (sogenannte Expertensysteme) zu schaffen, scheiterten in der Vergangenheit meist dann, sobald Regeln, Ausnahmen und Gegenausnahmen zu komplex wurden, wie es z. B. bei der menschlichen Kommunikation und Sprache der Fall ist.¹²⁸ Die Rede ist vom *Knowledge Acquisition Bottleneck*¹²⁹ oder *Symbolic Grounding Problem*.¹³⁰ Erfolgreich waren regelbasierte KI-Systeme nur, aber immerhin in Konstellationen mit klar abgrenzbaren, perfekt

122 Marcus/Davis, Rebooting AI, 2019, S. 161 f.

123 Zhou/Zafarani, ACM Comput. Surv. 53 (2020), 1 (11) m. w. N.

124 s. oben, → § 1 Rn. 37.

125 Für ein weiteres anschauliches Bsp. (Regenschirm/Regen) s. Mosa, Explainable AI vs Explaining AI – Part 2, Medium v. 7.1.2019 (Onlinequelle).

126 Garnelo/Shanahan, Current Opinion in Behavioral Sciences 29 (2019), 17.

127 Ein Plädoyer für eine Rückbesinnung auf symbolische Techniken, u. a. mit dem Ziel, bei der Entwicklung von *Artificial General Intelligence* Fortschritte zu machen, findet sich bei Marcus/Davis, Rebooting AI, 2019, bes. S. 155 ff.; s. auch Brachman/Levesque, Machines like Us, 2023, passim; lesenswert dazu Brachman/Levesque, F.A.Z. v. 25.7.2022, S. 18.

128 Vgl. ausf. Kaplan, Artificial Intelligence, 2016, S. 22 ff.; s. auch das Zitat von Andrew Ng bei Burrell, Big Data & Society 3 (2016), 1 (6): "[M]achine learning [is] the domain of '[applications] we cannot program 'by hand'.'" Eine frühe jur. Einschätzung von Expertensystemen liefert Susskind, The Modern Law Rev. 1986, 168 ff.

129 Rubin et al., in: Kwasny (Hg.), Proceedings of the 1993 ACM Conference on Computer Science, 1993, S. 522.

130 s. ausf. Harnad, Physica D: Nonlinear Phenomena 42 (1990), 335 ff.; anschauliche Bsp. für teils unterhaltsam fehlgeschlagene Versuche finden sich bei Marcus/Davis, Rebooting AI, 2019, S. 149 ff.

regelhaft bearbeitbaren Inputs, wie sie etwa auch bei Rechenprogrammen oder bestimmten Spielen vorkommen (z. B. Schach). Sobald aber der Gegenstand der künstlich-intelligenten Erfassung unsicher, wertungs offen und/oder ambig ist, sind regelbasierte, also streng logische Exaktheit voraussetzende Systeme wenig leistungsfähig.¹³¹

- 44 Hinzuweisen ist in diesem Zusammenhang nun freilich auf die aktuellen, für viele immer noch überraschenden Fortschritte im Bereich des *Natural Language Processing* (NLP). Sie wurden mit der im Winter 2022 veröffentlichten Anwendung ChatGPT¹³² auch einer breiten Öffentlichkeit bekannt.¹³³ ChatGPT und vergleichbare Anwendungen¹³⁴ sind Stand Frühsommer 2025 bereits extrem leistungsfähig, unter anderem, weil sie in der Lage sind, aufeinander aufbauende Frage-Antwort-Dialoge¹³⁵ in ganz unterschiedlichen Anwendungsdomänen¹³⁶ zu führen. Auch bei ChatGPT & Cie handelt es sich zwar letztlich um *Machine-Learning*-trainierte Modelle der *Mustererkennung* und vor allem der *Musterreproduktion* in bzw. zu Texten. Die Anwendungen setzen Texte so zusammen, dass die *wahrscheinlichste* Antwort auf die vom Nutzer gestellte Frage (*Prompt* genannt) aus dem vom Anbieter bzw. Nutzer vergebenen Quellenmaterial (z. B. dem Internet, beck-online, einem *Open-access*-verfügbaren Buch oder einer hochgeladenen PDF) generiert wird (sogenannte *Retrieval-augmented Generation* – RAG).¹³⁷ Wegen dieser Fähigkeit zur Textproduktion werden die Anwendungen häufig als LLMs bezeichnet, als *Large*

131 Marcus/Davis, Rebooting AI, 2019, S. 176.

132 Basierend auf der NLP-Anwendung GPT-3 (für *Generative Pre-trained Transformer*); dazu aus der technischen Lit. T. B. Brown et al., in: Larochelle et al. (Hg.), *Advances in Neural Information Processing Systems* 33, 2020, S. 1877; zur Technologie der *Transformer* grundlegend Vaswani et al., in: Guyon et al. (Hg.), *Advances in Neural Information Processing Systems* 30, 2017, S. 6000; informativ/zugänglich Ertel, Grundkurs KI, 2021, S. 338 ff. Zum im Frühjahr 2025 aktuellen Stand der Technik s. Maslej et al., *The AI Index 2025 Annual Report*. Stanford University, April 2025.

133 Dazu aus der Presse nur Armbruster, F.A.Z. v. 28.6.2021, S. 18; Wulfers, F.A.S. v. 11.12.2022, S. 26; Pretschner et al., F.A.Z. v. 9.1.2023, S. 18.

134 Einen Überblick über die aktuell "notable AI Models" liefern Maslej et al., *The AI Index 2025 Annual Report*. Stanford University, April 2025, S. 46 ff.

135 Dazu, dass bestimmte Fragetechniken, die die Anwendung dazu zwingen können, "[to] think step-by-step", die Antwortqualität erhöhen, Shanahan, arXiv:2212.03551v5 (16.2.2023), S. 8 f. Mittlerweile bieten fast alle großen Anwendungen diese *Step-by-step-reasoning*-Methode an.

136 Auf diese Fähigkeit der generellen Nutzung, d. h. ohne sog. "fine-tuning" für konkrete Anwendungskontexte (z. B. Tierbild- statt Gesichtserkennung), weisen hin T. B. Brown et al., in: Larochelle et al. (Hg.), *Advances in Neural Information Processing Systems* 33, 2020, S. 1877: "NLP has shifted from learning task-specific representations and designing task-specific architectures to using task-agnostic pre-training and task-agnostic architectures."

137 Die erstaunliche, vielleicht auch für manche erschütternde Einsicht, die dem zugrunde liegt, hat Shanahan, arXiv:2212.03551v5 (16.2.2023) auf den Punkt gebracht: "[A] great many tasks that demand intelligence in humans can be reduced to next token prediction with a sufficiently performant model." Hervorhebung im Original.

*Language Models*¹³⁸ oder *Large Generative AI Models* (unschön in der Abkürzung: LGAIMs).¹³⁹

Was LLMs leisten, klingt und ist *technisch-methodisch* also zunächst vertraut: Es ist und bleibt *Machine Learning* und damit letztlich Statistik.¹⁴⁰ Was sie aber hervorhebt und so bedeutsam macht, ist, dass der Korpus an – mehr oder weniger ‚gut/richtig‘ gelabelten – Daten, anhand derer sie trainiert wurden, so massiv ist, dass

“they are models of the distribution of token sequences produced *collectively* by an enormous population of humans. Accordingly, they exhibit wisdom-of-the-crowd effects, while being able to draw on expertise in multiple domains.”¹⁴¹

Da moderne Anwendungen zunehmend Text-, Bild- und Tonerkennung und -erstellung miteinander verkoppeln (sogenannte multimodale Systeme¹⁴²), ist auch der Begriff LLM für solche Anwendungen freilich schon wieder zu eng. Der Europäische Rat hat sich erfolgreich dafür eingesetzt, diese Technologien im AI Act gesondert zu regulieren, und dafür den neuen, durchaus aussagekräftigen Begriff der “General-purpose AI Systems/Models” eingebracht (jetzt Artt. 51 bis 56 AI Act).¹⁴³

Lässt man sich auf den Begriff der *General-purpose AI* ein, dann kommt man damit der *Artificial General Intelligence* (rechts-)begrifflich schon sehr nahe. Und man berücksichtigt mit dem Begriff, dass Sprach- und Texterkennung – zumal dann, wenn sie wie mit Bild- und Audioerkennung und -erstellung zu multimodalen Systemen kombiniert wird – letztlich die methodische Grundlage für praktisch

138 *Large Language Model* lässt begrifflich erkennen, dass es sich hierbei *eigentlich* lediglich um einen – freilich sehr leistungsfähigen – Fall von *Natural Language Processing* handelt; vgl. z. B. Shanahan, arXiv:2212.03551v5 (16.2.2023), bes. seine Def. auf S. 2: “LLMs are generative mathematical models of the statistical distribution of tokens in the vast public corpus of humangenerated text, where the tokens in question include words, parts of words, or individual characters including punctuation marks. They are *generative* because we can sample from them, which means we can ask them questions. But the questions are of the following very specific kind. ‘Here’s a fragment of text. Tell me how this fragment might go on. According to your model of the statistics of human language, what words are likely to come next?’ [...] Suppose we give an LLM the prompt [= input/question] ‘The first person to walk on the Moon was’, and suppose it responds with ‘Neil Armstrong’. What are we really asking here? In an important sense, we are not really asking who was the first person to walk on the Moon. What we are really asking the model is the following question: Given the statistical distribution of words in the vast public corpus of (English) text, what words are most likely to follow the sequence ‘The first person to walk on the Moon was’? A good reply to this question is ‘Neil Armstrong’.” Hervorhebung im Original.

139 Dazu eine gute Einordnung von Hacker/A. Engel/Mauer, arXiv:2302.02337 (5.2.2023).

140 s. gut lesbar Shanahan, arXiv:2212.03551v5 (16.2.2023), S. 2 ff. m. w. N.

141 Ibid., S. 9. Deshalb auch sog. Basismodelle/*Foundation Models*, grundl. hierzu Bommasani et al., arXiv:2108.07258 (12.7.2022).

142 Ibid., S. 6 f.; ausf. Alayrac et al., in: Koyejo et al. (Hg.), *Advances in Neural Information Processing Systems* 35, 2022, S. 23716; s. auch T. B. Brown et al., in: Larochelle et al. (Hg.), *Advances in Neural Information Processing Systems* 33, 2020, S. 1877.

143 s. *Council of the European Union*, 2021/0106(COD), dort Art. 3 Abs. 1b, für den ersten Aufschlag. Die rechtsverbindliche Def. von „KI-Modell mit allgemeinem Verwendungszweck“ findet sich nun in Art. 3 Nr. 63 AI Act. Für eine gute Übersicht zu den materiell-rechtlichen Bestimmungen s. A. Engel, KIR 2024, 21 ff.

alle menschlichen Handlungen und damit *strukturell* eine Domänen-unspezifische, eben *generalistische* Anwendung bildet.¹⁴⁴ Es gibt auch schon Forschungen, wie *General-purpose AI* genutzt werden kann, um Roboter, namentlich Haushaltsroboter, mit ihren Nutzern in natürlicher Sprache interaktionsfähig zu machen.¹⁴⁵ Dieses Anwendungsbeispiel wird im Verlauf des Buches noch wichtig werden.¹⁴⁶

- 48 Fehlerfrei arbeiten die Systeme Stand 2025 noch (lange?) nicht; in Öffentlichkeit und Wissenschaft wechseln sich aktuell das Erstaunen über die Leistungsfähigkeit der Systeme und die Sorge/der Hinweis auf weiterhin bestehende Fehler (Halluzinationen) in kurzer zeitlicher Folge geradezu wellenartig ab.¹⁴⁷
- 49 Während die KI-Vergangenheit (bis gegen Ende der 1980er Jahre) also von symbolischen Methoden geprägt war, und in der Gegenwart der konnektionistische Ansatz dominiert, könnte die Zukunft kombinatorischen Lösungen gehören.¹⁴⁸ Über die Frage, ob und wie maschinelles Lernen dabei helfen kann, das *Knowledge Acquisition Problem* zu lösen, wird schon seit 1993 diskutiert.¹⁴⁹ Die unter anderem unter dem Stichwort *Representation Learning* firmierenden Forschungsvorhaben versuchen, die besondere Beobachtungskraft maschinellen Lernens (Mustererkennung, flexible Gewichtung) zu nutzen, um die spezifische Herausforderung symbolischer KI zu lösen (das *Symbolic Grounding Problem*). Eine Forschungsrichtung versucht dafür, *Machine-Learning*-Software zu zwingen, selbst symbolisch zu lernen, also x_1 bis x_n in selbstständig sinntragende Einheiten (z. B. Katze, Tier) aufzuspalten und deren relationale Struktur (auch „Kanten“ genannt) zueinander zu erkennen¹⁵⁰ und auf zuvor nicht beobachtete (gelernte) Konstellationen anwendbar zu machen (Generalisierung). Vor allem sollen sie auch optisch für einen Nutzer in Form

144 Etwas voreilig hat DeepMind seine Anwendung Gato (beherrschte immerhin schon 604 unterschiedliche Aufgaben) bereits 2022 als „generalist AI“ bezeichnet, dazu *Heikkilä*, MIT Technology Rev. v. 23.5.2022 (Onlinequelle).

145 Ahn et al., arXiv:2204.01691v2 (4.4.2022).

146 s. unten, ab → S. 150.

147 Krit. namentlich zur jur. Leistungsfähigkeit von ChatGPT & Cie *Ouellette* et al., Stanford Public Law Working Paper et al. v. 4.2.2025 (Onlinequelle). Scharf aus der Presse z. B. *Wiele*, F.A.Z. v. 17.5.2025, S. 9: „Alles falsch“.

148 *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17 ff.; *Garnelo/Arulku-maran/Shanahan*, arXiv:1609.05518 (1.10.2016).

149 Vgl. *Rubin* et al., in: Kwasny (Hg.), Proceedings of the 1993 ACM Conference on Computer Science, 1993, S. 522, S. 522 ff.

150 *Garnelo/Shanahan*, Current Opinion in Behavioral Sciences 29 (2019), 17 (20); *Niederée/Nejdl*, in: Ebers et al. (Hg.), RechtsHdb. KI und Robotik, 2020, § 2 Rn. 112, sprechen von „hybriden Systemen“. Ausf. und sehr gut lesbar die skeptische Darstellung von *Perkowski*, Desinformationsregulierung (Manuskript 2024), Kap. 3, A.II.2.b, am Bsp. der bes. anspruchsvollen, weil auf möglichst vollständiges und aktuelles Wissen angewiesenen automatisierten Erkennung von Desinformation. Eine aktuelle, für uns bes. relevante, vorsichtig optimistische Studie zur Realisierbarkeit von medizin-ethischen Ratgebersystemen, die einem hybriden Ansatz folgen (sog. *Fuzzy Cognitive Maps*), liefern *Meier* et al., The American Journal of Bioethics 2022, 1, bes. S. 3 ff. (zur Relevanz für die Rechtserkenntnisfähigkeit von Technologie unten, → § 3 Rn. 39).

sogenannter *Knowledge Graphs*¹⁵¹ aus Knoten (z. B. Katze, Tier) und Kanten (also Relationen, z. B. *ist*) dargestellt werden. Das Ziel ist es, dadurch dem menschlichen Nutzer der Technologie ein menschlich nachvollziehbares *Explanation Interface* bieten zu können,¹⁵² das Ergebnisse hinterfragbar macht. Erfolgreich getestet wurden solche Ansätze etwa schon bei einfachen 2D-Spielen wie BoxWorld und vor allem im Bereich der Bilderkennung, wo mit Technologien, die auf *explainable AI* zielen, der Output von „Pferd“ hin zu „Pferd, weil lange Nase und vier Beine“ ausdifferenziert werden kann.¹⁵³

Diese Art von *Representation Learning* ist allerdings anspruchsvoll und fehleranfällig.¹⁵⁴ Zwar klingen die Zahlen zunächst beeindruckend: Stand März 2024 enthielt der Google *Knowledge Graph*¹⁵⁵ 54 Milliarden Entitäten (Personen, Orte, Tiere usw.) mit 1,6 Billionen Milliarden relationalen Verknüpfungen (Kanten). Das klingt nach viel, reicht aber natürlich bei weitem nicht aus, um eine auch nur in Ansätzen vollständige Realitätserfassung zu liefern, die für eine wirklich generalistische künstliche Intelligenz erforderlich wäre (einfaches Beispiel: Statt *ist* mag eine automatisiert erstellte Kante *stellt dar* lauten, meint aber dasselbe, ohne dass die Technologie das ohne Weiteres erkennen könnte¹⁵⁶).

Allerdings ist das für viele Anwendungsszenarien möglicherweise auch gar nicht erforderlich. Mit einfacheren und gegenwärtig auch schon erfolgreichen Anwendungen von *explainable AI*¹⁵⁷ (xAI) oder auch seltener sogenanntem *Interpretable Machine Learning*¹⁵⁸ gelingt es, etwa bei graphischem Input darzustellen, warum ein

151 Zhou/Zafarani, ACM Comput. Surv. 53 (2020), 1 (11) m. w. N.

152 Garnelo/Shanahan, Current Opinion in Behavioral Sciences 29 (2019), 17 (18 ff.); Chen et al., arXiv:1806.10574 (28.12.2019); s. auch Knight, MIT Technology Rev. v. 9.8.2016 (Onlinequelle), der beschreibt, wie Trainingsdaten zunehmend mit auch relationalen Tags gelabelt werden (allg. zum *Labeling* → § 1 Rn. 16), z. B.: „A dog riding a skateboard“. Skeptisch zu dem auch als „crowdsourcing“ bezeichneten Vorgehen (falls das *Labeln* durch Laien geschieht) Marcus/Davis, Rebooting AI, 2019, S. 151 ff.

153 Am Bsp. eines Bildes einer Fahl-Ammer (einer Spatzenart) Chen et al., arXiv:1806.10574 (28.12.2019); s. dort auch zur Unterscheidung von *post hoc* arbeitenden „Erklärern“ von solchen Systemen, deren Erkennungsprozesses („reasoning processes“) tatsächlich auch technisch auf je für sich selbst sinntragenden Einheiten aufbauen.

154 Ausf. Perkowski, Desinformationsregulierung (Manuskript 2024), Kap. 3, A.II.2. m. w. N.; s. auch Garnelo/Shanahan, Current Opinion in Behavioral Sciences 29 (2019), 17 (21), denen zufolge zwar viele Forschungsprojekte zu *Representation Learning* gestartet worden seien, mit bislang (2019) aber noch geringen Fortschritten; eine „truly satisfying synthesis of symbolic AI with [machine] learning“ sei ein Fernziel.

155 Diese *Knowledge Base* wird von Google v. a. genutzt, um neben Suchanfragen die sog. *Knowledge Panels* mit spezifischen Informationen zu der Suchanfrage anzuzeigen, s. Sullivan, Google Blog v. 20.5.2020 (Onlinequelle).

156 Perkowski, Desinformationsregulierung (Manuskript 2024), Kap. 3, A.II.2.a.

157 Die Lit. zur xAI ist uferlos. Nur als Auswahl: Molnar, Interpretable Machine Learning, 2023 (Onlinequelle), bes. Abschnitt 3.1; Gunning et al., Applied AI Letters 2 (2021); ausf. die Beiträge in Samek et al., Explainable AI, 2020, mit einem übersichtlichen Einführungsbeitrag S. 5 ff.; einführend Waitl/Vogl, DuD 2018, 613 ff.

158 Zu den diversen Begriffen D. S. Watson/Florida, <https://ssrn.com/abstract=3509737> besucht am 17.3.2020, m. w. N.

Objekt als ‚Pferd‘, nicht als ‚Hund‘ gelabelt wurde, und welche Bildpunkte für und welche gegen die Klassifizierung als ‚Pferd‘ sprechen. Das ist immerhin auch schon eine Form relationalen ‚Wissens‘,¹⁵⁹ wenn auch eine sehr einfache. Es handelt sich hierbei um die sogenannten *Heat Maps*, *Saliency Maps*¹⁶⁰ oder *Attention Maps*,¹⁶¹ die im Bereich der xAI eine große Rolle spielen, die noch steigen dürfte.

- 52 So hat das Team um den KI-Entwickler *Aleph Alpha* und das DFKI schon vor einiger Zeit eine Anwendung vorgestellt, welche die *Heat Maps* nicht mehr nur – aber *auch* (Stichwort Intermodalität/*Multimodal Prompt*)¹⁶² – für graphischen Input zur Verfügung stellt (= das Bilderkennungsbeispiel von soeben), sondern auch für die gerade so erfolgreichen LLM-Modelle. Soll heißen: Gibt man dem Modell von *Aleph Alpha* die Aufgabe, Text auszuwerten, dann ist dieses Modell in der Lage, diejenigen Worte oder Sätze farblich zu markieren, auf denen die Antwort basiert;¹⁶³ auch widersprechende Textstellen können als solche gekennzeichnet werden. Erweitert werden könnten solche Systeme noch dadurch, dass sie Konfidenzen (= Wahrscheinlichkeiten, die dem Output zugrunde liegen) anzeigen, farblich markieren, oder auch die sogenannten *Next Best Results* darstellen. Gerade vor dem Hintergrund der hiesigen Erkenntnis- und Anwendungsinteressen – also KI-basierte und -assistierte Rechtserkenntnis und -durchsetzung – ist diese Forschungsrichtung von xAI besonders wichtig: die Fähigkeit der Systeme, zuverlässig die Quellen für die von ihnen produzierten Texte, eventuell/perspektivisch auch Graphiken und Audioteile zu liefern. Mittlerweile (Stand 2025) sind alle gängigen Systeme mal mehr, mal weniger zuverlässig in der Lage, ihre Textproduktion mit relevanten und vor allem echten Quellen zu referenzieren (bei unseren am Lehrstuhl durchgeführten Versuchen halluzinierte die KI fast nur noch dann, wenn die wahrscheinlichste Antwort auf eine juristische Frage mit einer Quelle = Zitation verknüpft ist, die hinter eine Bezahlschranke verborgen ist, z. B. der beck-online-Datenbank).
- 53 Ebenfalls zu den Methoden von *explainable AI* gehört die längere Zeit vielbesprochene sogenannte kontrafaktische Begründung.¹⁶⁴ Sie soll nicht die positiv für die Entscheidung maßgeblichen Kriterien sichtbar machen, sondern anzeigen, welche Kriterien hätten erfüllt sein müssen, damit der Output *anders* ausgefallen wäre; da-

159 s. Samek/K.-R. Müller, in: Samek et al. (Hg.), *Explainable AI*, 2020, S. 5 (11). Dabei kommen teils erstaunliche Erkenntnisse zu Tage, vgl. etwa *Gless/Weigend*, JZ 2021, 612 (613), mit dem Bsp. einer KI, die Wolfs- und Husky-Darstellungen unterscheiden lernen sollte; da aber alle mit ‚Wolf‘ gelabelten Trainingsdaten Schnee zeigten, lernte sie, Schnee zu erkennen.

160 *Niederée/Nejdl*, in: Ebers et al. (Hg.), *RechtsHdb. KI und Robotik*, 2020, § 2 Rn. 129.

161 So *Deb* et al., arXiv:2301.08110 (23.1.2019), Abschnitt 1.

162 s. *ibid.*, Abb. 1: Auf die Frage nach „What am I looking at?“ liefert die xAI-Anwendung in dem multimodalen System von *Aleph Alpha* die Antwort „a lonely cabin“ [mit entsprechender farblicher Markierung im Bild] „on the edge of a lake“ [mit farblicher Markierung der Bildteile, die die Anwendung mit „lake“ korreliert] usw. Zur Multimodalität auch schon soeben, → § 1 Rn. 46.

163 *Deb* et al., arXiv:2301.08110 (23.1.2019), Abschnitt 3, bes. 3.3 mit Abb. 6.

164 Bes. *Wachter/Mittelstadt/Russell*, *Harvard Journal of Law & Technology* 31 (2018), 842 ff.

mit also z. B. statt eines Pferdes ein Hund erkannt oder statt ‚Genehmigung-zu-ver-sagen‘ ein ‚Genehmigung-zu-erteilen‘ ausgeworfen worden wäre. Ein anschauliches Beispiel für eine Kombinationslösung findet sich bei *Hermstrüwer*: „Die Genehmigung wurde Ihnen versagt, weil Sie die Eigenschaft x_r aufweisen. Hätten Sie die Eigenschaft x_k aufgewiesen, wäre Ihnen die Genehmigung erteilt worden.“¹⁶⁵ Die Idee kontrafaktischer Begründungen hat in den vergangenen Jahren zunächst viel Aufmerksamkeit erhalten, weil sie einen Weg aufzeigen sollte, „Transparenz“ zu schaffen, ohne die unter Umständen geschäftsschädliche oder das sogenannte *Gaming* von KI-Anwendungen ermöglichende Offenlegung des Quellcodes der jeweiligen Anwendung vorauszusetzen. Das Anliegen ist sicher sinnvoll, das eigentliche *technische Black-Box-Problem* wird durch kontrafaktische Begründungen aber nicht unbedingt gelöst: Denn wenn x_r und x_k usw. keine *menschlich plausiblen* Gründe bzw. Gegengründe für y darstellen,¹⁶⁶ dann weiß der Adressat der ‚Erklärung‘ zwar möglicherweise, wie er einen anderen Output generieren kann („explanation as enabling action“¹⁶⁷). Er weiß aber in einem anspruchsvollen Sinn nicht, warum ein Output so und nicht anders ausgeworfen wurde/wird,¹⁶⁸ und ob diese Kriterien jenseits ihrer statistischen Verlässlichkeit kausale Zusammenhänge haben oder *Proxies* anderer, nicht beobachteter Hintergrundvariablen sind.

Festzuhalten ist jedenfalls schon an dieser Stelle, dass der Druck auf die Entwickler von KI, ihre Systeme in für den konkreten Anwendungskontext hinreichendem Maße *explainable* zu machen, durch die jüngste Rechtsprechung des EuGH zu Art. 22 Abs. 3 DSGVO und durch Art. 86 AI Act (Stichwort: *Recht* auf Erklärung) massiv steigen wird.¹⁶⁹ 54

Von den soeben beschriebenen, *lokalen* Ansätzen von xAI, die eine *konkrete* Entscheidung erklären soll, sind zu guter Letzt *globale* Erklärungen zu unterscheiden, die auf das Verständnis des gesamten Musters abzielen.¹⁷⁰ Besonders für Plausibilitätsanalysen interessant sind *reverse* xAI-Anwendungen, im Rahmen derer ein KI-System offenlegt, was es unter dem Label y = Pferd ‚gelernt‘ hat, also ein nach seinem ‚Wissen‘ prototypisches Pferd darstellt.¹⁷¹ 55

165 *Hermstrüwer*, AöR 145 (2020), 479 (499).

166 Vgl. die Bsp. hierfür in → § 1 Rn. 25 ff.

167 *Selbst/Barocas*, Fordham Law Rev. 2018, 1085 (1120).

168 Mit diesem Einwand auch schon *Wachter/Mittelstadt/Russell*, Harvard Journal of Law & Technology 31 (2018), 842 (883) selbst. Krit. auch *Wischmeyer*, in: ders./Rademacher (Hg.), *Regulating Artificial Intelligence*, 2020, S. 75 Rn. 34 f. m. w. N. Der EuGH hat sich mittlerweile vorsichtig dahingehend geäußert, dass kontrafaktische Begründungen den Anspruch aus Art. 15 Abs. 1 lit. h DSGVO auf Erläuterung der Logik einer automatisierten Entscheidung erfüllen *könnten*, s. Urt. v. 27.2.2025, Rs. C-203/22 (Dun & Bradstreet Austria) Rn. 62; m. E. zutreffend zurückhaltend hierzu *Hense/Niekrenz*, KIR 2025, 240 (243).

169 Ausf. unten, → § 4 Rn. 148.

170 s. *Niederée/Nejdl*, in: Ebers et al. (Hg.), *RechtsHdb. KI und Robotik*, 2020, § 2 Rn. 128 m. w. N.

171 *Samek/K.-R. Müller*, in: Samek et al. (Hg.), *Explainable AI*, 2020, S. 5 (10).

IV. Legal Tech und hier sog. Law-abiding Technology

- 56 Nicht unerwähnt bleiben soll schließlich in diesem Abschnitt über die Terminologie der Begriff *Legal Technology*, kurz *Legal Tech*. Namentlich *Wolfgang Hoffmann-Riem* verwendet den Begriff weit im Sinn von „Nutzung digitaler Techniken bei der Rechtsanwendung“.¹⁷² Darunter fallen dann *thematisch* zivilrechtliche, öffentlich-rechtliche und sanktionen-/vollstreckungsrechtliche Anwendungsfälle gleichermaßen.¹⁷³ *Methodisch* sind einfache regelbasierte Systeme ebenso wie komplexe maschinell trainierte Systeme erfasst, und – im Verhältnis zum menschlichen Beitrag, also sozusagen *architektonisch* – wird das gesamte Spektrum von algorithmenbasierten, -getriebenen und -determinierten Entscheidungen abgedeckt.¹⁷⁴
- 57 Mit dieser Weite würde sich der Begriff grundsätzlich auch zur Abdeckung des in diesem Buch verfolgten Erkenntnisinteresses eignen.¹⁷⁵ Ich werde ihn gleichwohl nicht verwenden. Denn mir scheint, dass der Begriff *Legal Tech* in der KI- und Recht-Diskussion insgesamt zunehmend spezifischer und enger gebraucht wird, nämlich zur Beschreibung der „Umgestaltung v. a. der Rechtsdienstleistungsbranche durch die Digitalisierung“.¹⁷⁶ Die besondere, auf die realweltliche Durchsetzung von staatlichem und supranationalem Recht fokussierte Perspektive, die in dieser Arbeit eingenommen wird, soll hinter dieser eher wirtschaftlich ausgerichteten Begriffsprägung nicht unsichtbar werden.
- 58 Deshalb werde ich gleich in → § 2 spezifischere Begrifflichkeiten für die Beschreibung und Systematisierung von Technologien vorschlagen, die Menschen bzw. genauer: *die jeweiligen (Erst-)Adressaten*¹⁷⁷ bei der Realisierung von an sie gerichteten Normen in unterschiedlichem Maße unterstützen können: von der rechtsrelevanten Information (*Compliance Assistance Technologies*) bis hin zum Zwang (*Impossibility Structures*), mit graduellen Abstufungen dazwischen (*Justification Structures*). Einige der Begrifflichkeiten sind mittlerweile in die Diskussion schon gut eingeführt (das gilt besonders für Begriff der *Impossibility Structure*), andere sind hier erstmals

172 *Hoffmann-Riem*, AöR 145 (2020), 1 (2); *ders.*, Recht im Sog der digitalen Transformation, 2022, S. 244 ff.

173 Vgl. *Hoffmann-Riem*, AöR 145 (2020), 1 (17 ff.).

174 *Ibid.*, S. 4.

175 Wegen der damit nach Auffassung der Autoren einhergehenden „Simplifizierung“ einer komplexen Idee krit. zum Begriff *Hähnchen/Bommel*, JZ 2018, 334 (335).

176 So *Steinrötter/Warmuth*, in: Hoeren/Sieber/Holznapel (Hg.), Handbuch Multimedia-Recht, 56. EL Stand Mai 2021, Teil 30 Rn. 1 m. w. N. Mit dem Hinweis, dass der Begriff den Einsatz digitaler Technologien „insbesondere bei der Erbringung (vor allem anwaltlicher) Rechtsdienstleistungen“ meine, auch *Hoffmann-Riem*, AöR 145 (2020), 1 (2) selbst. Jedenfalls ist der Sprachgebrauch nicht einheitlich, deshalb krit. *Werthmann*, in: Ebers et al. (Hg.), RechtsHdb. KI und Robotik, 2020, § 22 Rn. 1 ff.

177 Diese etwas mühsame Umschreibung bedeutet kurz gesagt: Es wird fast durchweg um die Rechtsanwendung durch juristische Laien gehen, denn diese sind – freilich mit Ausnahmen, vgl. die ab → S. 191 beschriebenen Anwendungen im Verbraucherschutz- und Studienrecht – die Erstadressaten von Recht (dazu nochmals ausf. unten, ab → S. 328). Die Perspektive professioneller Rechtsanwender wird in anderen Arbeiten fokussiert.

vorgeschlagene Wortneuschöpfungen (das gilt namentlich für die *Justification Structures*). Ich gehe in → § 2 ausführlich auf die Konzepte ein und liefere Beispiele für einschlägige Anwendungen.

Ein weiteres Konzept liegt quer zu diesen Kategorien und soll deshalb bereits hier kurz vorab eingeführt werden: Die Idee von der Notwendigkeit der hier sogenannten *Law-abiding Technology*.¹⁷⁸ Während die in → § 2 beschriebenen Anwendungen grundsätzlich vom Menschen ausgehen – wie wird er gezwungen bzw. dabei unterstützt, Recht zu realisieren, dessen Erstadressat er wäre? – beschreibe ich mit *Law-abiding Technology* künstliche Aktanten mit großem Aktionsradius in einem weiten Sinn: Maschinen, Roboter, bestimmte Programme wie avancierte *Digital Personal Assistants*, die selbst (Erst-)Adressaten von Recht sein können *müssen*, um ihre eigentliche Funktionalität ausüben zu können. Ich komme an den für meine Überlegungen entscheidenden Stellen auf diesen Begriff bzw. solche Aktanten zurück;¹⁷⁹ hier soll nur als Illustration des Gemeinten das geläufige Beispiel autonomer Fahrzeuge dienen: Jedenfalls wenn diese in gemischten Verkehren ‚agieren‘ (können) sollen, werden sie mit einem wachsenden Aktionsradius in der Lage sein müssen, sich an die für menschliche Akteure im gleichen Raum geltenden Regeln in analoger Weise halten zu können; sie werden eben, in diesem Sinne, *law-abiding* sein müssen.¹⁸⁰ Ich werde auf diese Kategorie, wie gesagt, noch zu sprechen kommen.

178 Soweit ersichtlich ist der Begriff auch im anglo-amerikanischen Schrifttum noch nicht etabliert. Er findet sich in der hier vorgeschlagenen Verwendung nur bei *Perritt/Sprague*, *Columbia Science & Technology Law Rev.* 16 (2015), 385, bes. S. 421 ff., die freilich (2015!) noch sehr einfache Methoden beschreiben, um Kleinst-Drohnen „automatically law abiding“ zu machen. *Prakken*, *Artificial Intelligence and Law* 25 (2017), 341 (342) rechnet die hier aufgeworfene Frage zum Forschungsfeld *AI & Law*.

179 Bes. unten, → S. 247 ff.

180 Das ist auch bereits die in Deutschland geltende Rechtslage, s. unten, → S. 146 ff.

§ 2 Anwendungen, Konzepte und Status quo der Dogmatik(en): künstlich-intelligente Strukturen zur Optimierung der Realisierungschancen des Rechts

- 1 Dass das demokratisch gesetzte und grundrechtlich konturierte Recht *nicht* auf seine flächendeckende Befolgung¹ und damit Durchsetzung abzielen könnte, wird erst jüngst wieder² in Erwägung gezogen. Bezeichnenderweise geschieht das gerade im Zusammenhang mit dem Auftreten künstlicher Intelligenz.³ Jenseits dieser noch vereinzelter Stimmen wurde und wird bislang aber doch eher auf die teils erheblichen Defizite fokussiert, die bei Befolgung und/oder Vollzug des Rechts bestehen;⁴ *hierfür*, also für die Beseitigung der Realisierungsdefizite, wird gemeinhin nach Instrumenten gesucht. Gerade in den jüngeren, unional geprägten Rechtsgebieten wie dem Daten- und Verbraucherschutzrecht und dem Recht der Plattformregulierung zielen die Rechtsakte mit ihren extrem hohen Bußgeldern auf starke Abschreckungseffekte und damit einen hohen *Compliance*-Druck ab. Aber auch in klassischen Feldern wie dem Steuerrecht oder der Terrorabwehr wird seit jeher nach Möglichkeiten der *Compliance*-Optimierung gesucht. Darum – also die Steigerung der Rechtsbefolgung/-durchsetzung durch neue Technologien – geht es in diesem § 2. Die Auswahl der folgenden Anwendungsbeispiele erfolgte nach drei Kriterien:
- 2 *Erstens* handelt es sich um Lebensbereiche, in denen KI besondere, *rechtlich* relevante Optimierungserfolge bereits hervorgebracht hat oder alsbald hervorzubringen verspricht (bzw. hervorbringen muss, Stichwort autonomes Fahren).
- 3 Das Ziel ist *zweitens*, mit der Auswahl das Potential technologiebasierter Wirkungsstrukturen in der Breite veranschaulichen und systematisieren zu können. Vollständigkeit innerhalb der einzelnen Kategorien wird nicht angestrebt. Sie ist auch gar nicht nötig, denn das Optimierungspotential von KI ist methodisch „allgemein

1 Die Pflicht zum Rechtsgehorsam scheint – neben der Steuer- und Wehrpflicht – die eine Grundpflicht der Bürger zu sein, auf die sich die Staatsrechtslehrertagung 1982 bei aller sonstigen Zurückhaltung einigen konnte, vgl. den Bericht von *Schuppert*, AöR 107 (1982), 614 (615 ff.). Vgl. auch *Schieder*, Ethisch motivierter Rechtsungehorsam, 2018, S. 258.

2 Vgl. die ältere Diskussion rund um die Möglichkeit zum zivilen Ungehorsam, z. B. bei *Raz*, in: ders. (Hg.), *The Authority of Law*, 2009, S. 262 ff.; *Habermas*, *Merkur* 38 (1984), 15 ff.; *R. Dreier*, *Recht – Staat – Vernunft*, 2016, S. 39 ff., 73 ff.

3 Bes. *Möllers*, Die Möglichkeit der Normen, 2018, S. 478; s. außerdem *Burchard*, JRE 27 (2019), 527 (547 ff.); *Wischmeyer*, in: Ebers et al. (Hg.), *RechtsHdb. KI und Robotik*, 2020, § 20 Rn. 61; *Bernzen/Kehrberger*, RW 10 (2019), 374 ff.; *Becker*, ZUM 2019, 636 ff.; *Rademacher*, JZ 2019, 702 ff.; *Rostalski*, GA 166 (2019), 481 ff.; knapp *Rademacher*, AöR 142 (2017), 366 (398).

4 Jüngst etwa *Kube*, AöR 146 (2021), 494 (502 f.). Dazu, dass die Forderung nach einem besseren, bzw. neutralen: nach *mehr* Vollzug von Recht auf einer verzerrten Wahrnehmung nur der extremen und damit meist schädlichen Regelabweichungen in der/durch die Öffentlichkeit liegen könnte, *Kühl*, *Brauchbare Illegalität*, 2020, S. 12: „Allein der Blick auf diese Beispiele [Enrons Bilanzfälschung, VWs Diesel-Betrug] zeigt, wie sehr unsere Perspektive auf Regelabweichungen durch das öffentlich sichtbare Scheitern dieser Organisationen verzerrt wird.“ s. zudem die Nachw. a. a. O., S. 23.

angelegt und durchwirkt alle Lebensbereiche“.⁵ Es geht darum, Anschaulichkeit im Sinn einer *Strukturierung* der technologiebasierten Optimierungsmöglichkeiten für die Realisierung des Rechts zu entwickeln. Maßstab dafür ist die durch die jeweilige Technologie bewirkte *Unmittelbarkeit* des angestrebten Steuerungserfolgs.

Aus diesem Fokus auf den demokratisch gesetzten Steuerungszweck von Recht 4 erklärt sich auch, warum die Beispiele zuvorderst aus dem deutschen und europäischen öffentlichen Recht stammen, dessen „Domäne [die] Verhaltenssteuerung im Allgemeinwohlinteresse“ ist,⁶ und die Beispiele zu einem kleinen Teil auch aus dem Strafrecht stammen, dem es zumindest nach der herrschenden, die präventiven Straftheorien betonenden Meinung (jedenfalls auch) um hoheitliche Verhaltenssteuerung⁷ geht.⁸ Privatautonom gesetztes Recht und insbesondere das große Thema der sogenannten *Smart Contracts*⁹ bleibt wegen der Fokussierung auf den demokratischen Steuerungsanspruch hingegen grundsätzlich außerhalb der Betrachtung.¹⁰ Nur soweit es um zivilrechtliche Rechtspositionen geht, die strafrechtlich oder sonst wie durch öffentlich-rechtliche Verhaltensgebote abgesichert sind, sind auch Regelungen aus dem Zivilrecht von Interesse. Das gilt zuvorderst für das Urheberrecht, in dem automatisierte Rechtsdurchsetzung derzeit schon ins Werk gesetzt wird und wo die entsprechenden Technologien ohnehin nicht auf rein privatrechtliche Einsatzszenarien beschränkt sind. Vereinzelt nehme ich auch Bezug auf Beispiele aus Drittstaaten wie den USA, weil dort die Bereitschaft, rechtsrealisierende Techno-

⁵ Burchard, JRE 27 (2019), 527 (534).

⁶ Bruns, Umsetzung der EU-Verbandsklagerichtlinie in deutsches Recht, 2022, S. 2; und weiter: „Zivilrecht und Zivilprozess haben hingegen für die Verhaltenssteuerung eher eine flankierende und unterstützende Bedeutung, und zwar insbesondere dort, wo das Instrumentarium des öffentlichen Rechts keine zufriedenstellenden Ergebnisse zeitigt.“ Ähnl. Bunz, CCZ 14 (2021), 81 (85): „Das Zivilrecht (etwa [...] § 138 Abs. 1 BGB) verbietet nicht ein bestimmtes Handeln. Dies stünde dem Zivilrecht auch gar nicht zu. Es ordnet lediglich zivilrechtliche Ansprüche an für den Fall, dass auf bestimmte Art und Weise gehandelt wird – etwa unter Verwendung sittenwidriger oder aus anderem Grunde unwirksamer Vertragsklauseln. Das Zivilrecht regelt also keine Verbote, sondern Rechtsverhältnisse und ordnet Rechtsfolgen an.“

⁷ Vgl. Renzikowski, in: Dölling (Hg.), FS Gössel, 2002, S. 1 (12) m. w. N.

⁸ In § 2 interessiert also nicht die „sekundäre Normordnung“ der Sanktionen, sondern es interessieren die primären Verhaltenspflichten, die den eigentlichen Strafnormen als im Kern öffentliches Recht vorausgehen. Prägnant dazu Haffke, in: Schünemann (Hg.), FS Roxin, 2001, S. 955 (957): „zufällige Platzierung [...] der Verhaltensnorm im Strafrecht“. Zur Unterscheidung ausf. Renzikowski, in: Dölling (Hg.), FS Gössel, 2002, S. 1 ff. Vgl. auch BVerfG, Urt. v. 25.2.1975 = BVerfGE 39, 1 – Schwangerschaftsabbruch I = NJW 1975, 573 (580): „[Das Strafgesetz] soll sagen, was für den Einzelnen Recht und Unrecht ist.“ Dort allerdings auch eine *prima facie* verwirrende, scharfe Gegenüberstellung einer „sozialethische[n] und – ihr folgend [sic!] – rechtliche[n] Bewertung menschlicher Handlungen“ als Ziel demokratischen Rechts einerseits und einer „sozialtechnischen Verwendung des Gesetzes“ i. S. der Steuerungsperspektive andererseits. Die Gegenüberstellung verdunkelt, dass das eine das andere nicht ausschließt. Plausibel wird die Aussage des BVerfG, wenn man beachtet, dass das konkret geprüfte Gesetz (über den Schwangerschaftsabbruch den Schutz des *einzelnen* Lebens zugunsten einer „Gesamtrechnung“ (so die Gesetzesbegründung, zitiert a. a. O.) an Schwangerschaftsabbrüchen hinstellen wollte. Das hielt das BVerfG damals für unzulässig.

⁹ Dazu nach wie vor hervorragend der Band von Fries/Paal, *Smart Contracts*, 2019.

¹⁰ s. hierzu, auch zu den Grenzen privatiniziativer automatisierter Rechtsdurchsetzung, die Nachw. unten, in → § 2 Fn. 486.

logien zu erproben, höher als im europäischen Rechtskreis ist. Der Dominanz englischsprachiger Literatur sowie der diskursiven Anschlussfähigkeit ist es dann auch geschuldet, dass für die folgende Strukturierung englische Begriffe genutzt werden. Völkerrecht bleibt als solches außen vor. Auf die im völkerrechtlichen Schrifttum jüngst ebenfalls intensiver untersuchten Funktionen von Rechtsbrüchen¹¹ wird aber an passender Stelle¹² eingegangen werden.

- 5 *Drittens* war für die Auswahl der Anwendungsbeispiele auch ausschlaggebend, dass dem KI-bedingten Optimierungspotential in den beschriebenen Rechtsgebieten bereits jetzt – teils versteckt, teils offensiv – Zufallsarrangements oder zumindest ‚Beimischungen‘ von Zufälligkeit entgegengesetzt werden. Hierauf wird aber nicht in diesem § 2, sondern abschließend in → § 6 eingegangen.
- 6 Was nun die Strukturierung angeht, so schlage ich vor, zwischen *Intelligent Surveillance* (→ I.), *Impossibility Structures* (→ II.), *Compliance Assistance Technologies* (→ III.), *Justification Structures* (→ IV.) und *Preference Assistance Technologies* (→ V.) zu unterscheiden.
- 7 Innerhalb dieser Kategorien liefere ich zunächst jeweils eine knappe begriffliche Einordnung, bevor kleine Berichte über beispielhafte Anwendungen folgen, die ihrerseits in der Regel grob nach Rechtsgebieten sortiert sind (z. B. *Intelligent Surveillance* ... im Sicherheitsrecht, ... im Steuerrecht, ... im Recht der Online-Kommunikation usw.). Rechtsdogmatische und -theoretische Zwischenbemerkungen zum Stand der Diskussion um die jeweiligen Technologien stehen jeweils am Ende einer Kategorie. Mit diesen Zwischenbemerkungen verfolge ich das Anliegen, die ‚großen Linien‘ in den jeweiligen Debatten (soweit schon vorhanden) herauszuarbeiten, und strebe weniger danach, die (verfassungs-)rechtliche Zulässigkeit einer *konkreten* Anwendung im Detail zu beurteilen. Insofern verweise ich auf die knappen Hinweise direkt in den Berichten. Ein größeres erstes Zwischenfazit zu den konzeptionellen Verschiebungen bei der Durchsetzung staatlichen Rechts durch und mithilfe von künstlicher Intelligenz schließt diesen § 2 ab (→ VI.).

I. Intelligent Surveillance

- 8 *Elizabeth Joh* hat die bisherige Diskussion um „smarte“ – also KI-gestützte – staatliche Rechtsdurchsetzung in den USA vor einiger Zeit treffend als „Echo“ der Überwachungsstaatsdiskussionen der Vor-KI-Zeit bezeichnet.¹³ Diese pointier-

11 *Marxsen*, Völkerrechtsordnung und Völkerrechtsbruch, 2021, passim und bes. S. 195 ff.

12 s. unten, → § 5 Rn. 39.

13 *Joh*, Int. J. Law in Context 26 (2019), 177 f.

te Wertung beschreibt nach meiner Einschätzung auch die deutsche Debatte gut: Im Mittelpunkt der Diskussion um neue Technologien zwecks Rechtsdurchsetzung stehen nach wie vor die durch KI potentiell erheblich verbesserten *Erkenntnismöglichkeiten* der staatlichen Rechtsdurchsetzungsorgane, die präventiv wie repressiv genutzt werden können, um einen Gefahr- oder Straftatverdacht zu gewinnen. Auch wenn Überwachung natürlich streng genommen *selbst* noch keine Realisierungswirkung erzielen kann, können und sollen entsprechende ‚intelligente‘ Technologien hier folglich nicht außen vor bleiben. Im Gegenteil: Da sich auch im deutschen Rechtsdiskurs eine Art von ‚überwachungsakzessorischer‘ Bewältigung auch der auf *physische Realisierung* gerichteten Technologien abzeichnet,¹⁴ ergibt es guten Sinn, die hier sogenannte *Intelligent Surveillance* an den Beginn der Untersuchung zu stellen.

1. Begriff (zugleich Einordnung in die Kategorien des AI Act)

Mit nicht immer ganz klarer Definition/Abgrenzung verläuft die Diskussion unter den Stichworten *Predictive Policing*,¹⁵ *Smart Law Enforcement*,¹⁶ *Intelligent Surveillance*,¹⁷ automatisierte Verdachtsgewinnung¹⁸ bzw. *Automated Suspicion Algorithms*,¹⁹ oder *Intelligence Augmentation* (IA).²⁰ Es geht darum, dass neue Technologien, also aktuell besonders *Machine-Learning*-gestützte KI-Anwendungen, genutzt werden sollen, um Gefahren oder Straftaten staatlicherseits *maschinell* gezielt erkennen und dann *menschlich* verhindern oder sanktionieren zu können. Hierfür hat der Begriff der *Intelligent Surveillance* m. E. den größten deskriptiven Wert: Er kombiniert die maschinelle ‚Erkenntnis‘, das maschinell ‚Gesehene‘, ‚Gehörte‘ oder eventuell sogar ‚Gerochene‘ könne gefährlich oder verboten sein (= ‚Intelligenz‘), mit der noch fehlenden physischen Durchsetzung durch das KI-System selbst (= ‚nur‘ Überwachung). Wir haben es daher – in der klassischen Terminologie des Sicherheitsrechts gesprochen – mit Verdachtsgewinnungsverfahren zu tun,²¹ die durch den Einsatz

14 Details hierzu dann unten, ab → S. 166.

15 Hierzu u. a. Koch, *Predictive Policing und Gefahrenkategorien*, 2023; Trute/S. Kuhlmann, GSZ 2021, 103 ff.; He. Hofmann, *Predictive Policing*, 2020; Sommerer, *Personenbezogenes Predictive Policing*, 2020; Wischmeyer, in: Kulick/Goldhammer (Hg.), *Der Terrorist als Feind?* 2020, S. 193; Rademacher, AöR 142 (2017), 366 ff.

16 Wischmeyer, in: Kulick/Goldhammer (Hg.), *Der Terrorist als Feind?* 2020, S. 193 ff.; Rademacher, in: Wischmeyer/Rademacher (Hg.), *Regulating Artificial Intelligence*, 2020, S. 225 ff.; zivilrechtlich N. Kuhlmann, in: Fries/Paal (Hg.), *Smart Contracts*, 2019, S. 117 ff.

17 Rademacher, JZ 2019, 702 (703).

18 Rademacher, in: Eifert (Hg.), *Digitale Disruption und Recht*, 2020, S. 45 ff.

19 M. L. Rich, *Penn Law Rev.* 164 (2016), 871 (876). Monographisch mit/zu diesem Begriff jüngst Leffer, *Automated Suspicion Algorithms*, 2025, passim, zur Def. und Abgrenzung S. 39.

20 Pasquale, *George Washington Law Rev.* 87 (2019), 1 (47).

21 Grundlegend Bull, in: Osterloh/Schmidt/Weber (Hg.), *Staat, Wirtschaft, Finanzverfassung*, 2004, S. 29 ff.

,intelligenter‘ Technologie besonders effizient gemacht werden sollen.²² Um diesen Aspekt – also: Einsatz neuer Technologien – noch hervorzuheben, könnte man auch etwas umständlicher von *Automated Intelligent Surveillance* sprechen. Aber mir scheint, dass jedenfalls hier, in diesem Buch, der Kontext ausreichend klarstellt, dass es um maschinelle ‚Intelligenz‘ geht, nicht um menschliche. Es folgen sogleich (→ Rn. 20 ff.) einige Beispiele für entsprechende Anwendungen in unterschiedlichen Referenzfeldern des deutschen Rechts.

- 10 Zuvor ist allerdings noch eine terminologische Selbstkorrektur, vielleicht ja auch nur eine Klarstellung angezeigt: Soweit ich früher²³ den Begriff *Predictive Policing* zur Beschreibung auch der nun folgenden Anwendungen vorgeschlagen habe (*technisch* ist jede automatische Bewertung eine Prognose²⁴), scheint es mir angezeigt, von dieser weiten Verwendung von *Predictive Policing* in Zukunft abzugehen. Der Grund dafür ist, dass der Begriff zunehmend exklusiv für *Risk (!) Assessments* weit im Vorfeld von tatsächlichem deviantem Verhalten genutzt wird/werden soll, die also *künftiges* Verhalten vorhersagen und nicht aktuelles Verhalten erkennen sollen. Ein solch stark zukunftsbezogenes Verständnis von *Predictive Policing* hat sich nach meinem Eindruck vor allem im Europäische Parlament durchgesetzt; nach dem Willen der beiden Berichterstatter des EP zum AI Act²⁵ sollten als „Predictive Policing“ nämlich folgende KI-Anwendungen definiert werden:

“the placing on the market, putting into service or use of an AI system for making individual *risk* assessments of natural persons in order to assess the *risk* of a natural person for offending or reoffending or for *predicting* the occurrence or reoccurrence of an actual or potential criminal offence *based on profiling* of a natural person or on assessing personality traits and characteristics or past criminal behavior of natural persons or groups of natural persons.”
Hervorhebungen hier.

- 11 Und wichtig: Solchermaßen definiertes *Predictive Policing* sollte nach dem Willen der Berichterstatter *vollständig verboten* werden. Der finale Text des AI Act übernimmt das Verbot mit nur kleinen Modifikationen am Wortlaut in seinem Art. 5 Abs. 1 lit. d Hs. 1. Die entscheidende Frage ist nun, ob das für uns eine Rolle spielt, also ob nun einige oder alle oder viele Anwendungen, die im Folgenden als *Intelligent Surveillance* vorgestellt werden, nunmehr pauschal verboten sind. Die Antwort ist ein klares ‚Nein‘ (sogleich, → Rn. 17 f.). Aber: Der sprachlich und systematisch – zumindest an dieser Stelle – wirklich grob misslungene AI Act lädt zu Missverständnissen geradezu ein; ganz offensichtlich war sich der Unionsgesetzgeber selbst nicht ganz sicher, was er hier eigentlich regeln bzw. verbieten wollte bzw. sollte. Zur

22 Zur Einordnung auch schon Rademacher, in: Zimmer (Hg.), Regulierung für Algorithmen und KI, 2021, S. 229 ff., auf dem die folgenden Überlegungen auch teilweise aufbauen.

23 Vgl. Rademacher, AöR 142 (2017), 366 ff.

24 Dazu schon oben, → § 1 Rn. 13 sowie unten, → S. 290 ff.

25 s. Benifei/Tudorache, 2021/0106(COD) v. 20.4.2022, S. 54.

Illustration dieser scharfen Behauptung drucke ich im Folgenden den Wortlaut der einschlägigen Passagen im AI Act ab.

Verboten ist jetzt also folgende Art von KI-gestützter Überwachung: 12

„das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von *Risikobewertungen* in Bezug auf natürliche Personen, um die *Wahrscheinlichkeit*, dass eine natürliche Person eine Straftat begeht, *ausschließlich auf der Grundlage des Profiling* einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen“. Hervorhebung hier.

Halbsatz 2 schwächt das Verbot freilich sofort wieder ab: 13

„[D]ieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität zu unterstützen, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen.“

Diese Systeme sind dann grundsätzlich ‚nur‘ Hochrisiko-Anwendungen i. S. von Artt. 6 ff. AI Act (siehe Anhang III lit. d AI Act) und müssen daher besondere Anforderungen erfüllen (zu Ausnahmen *hiervon* siehe aber Art. 6 Abs. 3 AI Act). Verboten sind sie jedenfalls nicht, zumindest nicht von Unionsrechts wegen. 14

Erwägungsgrund 42 S. 3 zum AI Act ergänzt noch, dass das Verbot in Art. 5 Abs. 1 lit. d AI Act 15

„nicht Risikoanalysen [betrifft], die nicht auf dem Profiling von Einzelpersonen oder auf Persönlichkeitsmerkmalen und -eigenschaften von Einzelpersonen beruhen, wie etwa KI-Systeme, die Risikoanalysen zur Bewertung des Risikos eines Finanzbetrugs durch Unternehmen auf der Grundlage verdächtiger Transaktionen durchführen, oder Risikoanalyseinstrumente einsetzen, um die Wahrscheinlichkeit vorherzusagen, dass Betäubungsmittel oder illegale Waren durch Zollbehörden, beispielsweise auf der Grundlage bekannter Schmuggelrouten, aufgespürt werden.“

Auch dem Unionsgesetzgeber war also klar, dass es dieser Klarstellung bedürfe, weil der Wortlaut von Art. 5 Abs. 1 lit. d AI Act sehr leicht zu weit verstanden werden könnte.²⁶ Das zentrale oder zumindest ein zentrales Problem scheint mir zu sein, dass die Schwierigkeiten, die bei der Bestimmung des Begriffs des *Profiling* i. S. von Art. 4 Nr. 4 DSGVO/Art. 3 Abs. 4 JI-Richtlinie bestehen, vom Gesetzgeber in den AI Act importiert werden (Art. 3 Nr. 52 AI Act). Profiling *selbst* wird übrigens vom AI Act nicht verboten; soweit es „im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten“ eingesetzt wird, wird es vom AI Act ‚nur‘ als Hochrisiko-Technologie klassifiziert.²⁷ 16

²⁶ Krit. auch Busche, AöR 149 (2024), 207 (246).

²⁷ s. Anhang III Nr. 6 lit. e AI Act. Interessant ist, dass das ursprünglich ebenfalls als *High-Risk*-Anwendung eingeklassifizierte polizeilich-strafrechtliche *Data Mining* im Trilog aus dem entsprechenden Katalog heraus-

- 17 Hier ist noch unerfreulich viel Auslegungsarbeit zu leisten;²⁸ für uns spielt das aber glücklicherweise keine entscheidende Rolle: Die für uns wichtige Klarstellung, was der Unionsgesetzgeber hier im Kern eigentlich gemeint und verboten hat, findet sich versteckt in Satz 1 von Erwägungsgrund 42. Anliegen des Unionsgesetzgebers war es, dass „natürliche Personen in der EU stets nach ihrem tatsächlichen Verhalten beurteilt werden“, und

„natürliche Personen in der EU stets nach ihrem tatsächlichen Verhalten beurteilt werden [und] niemals allein nach dem Verhalten, das von einer KI auf der Grundlage ihres Profiling, ihrer Persönlichkeitsmerkmale oder -eigenschaften wie Staatsangehörigkeit, Geburtsort, Wohnort, Anzahl der Kinder, Schulden oder Art ihres Fahrzeugs vorhergesagt wird, ohne dass ein begründeter Verdacht besteht, dass diese Person an einer kriminellen Tätigkeit auf der Grundlage objektiver nachprüfbarer Tatsachen beteiligt ist, und ohne dass eine menschliche Überprüfung stattfindet“.

- 18 Also: Sobald eine Technologie zumindest auch an konkretes *tatsächliches Verhalten* einer Person anknüpft, greift das Verbot von Art. 5 Abs. 1 lit. d AI Act schon nicht mehr.²⁹ Man fragt sich aufrichtig verwundert, was den Unionsgesetzgeber davon abgehalten hat, diese reichlich simple Bedingung im verbindlichen Normtext auszuformulieren, statt den notorisch auf- und überladenen *Profiling*-Begriff zu verwenden.
- 19 Bei den im Folgenden vorgestellten Anwendungen geht es gerade darum, objektive, nachprüfbare Tatsachen im *aktuellen* Verhalten einer überwachten Person mithilfe künstlicher Intelligenz aufzuspüren. Um es am Beispiel konkret zu machen: Der sogleich vorgestellten smarten Videoüberwachung etwa geht es um die Auswertung von Verhaltensdaten, die auf die konkrete und gegenwärtige „*Begehung* einer Straftat hindeuten“ (vgl. etwa § 44 Abs. 4 S. 2 PolG BW, auf den ich später ausführlicher eingehe), nicht darum festzustellen, ob ein solches *Risiko* – also in Zukunft – besteht.

2. ... im Polizeirecht

- 20 Das Polizeirecht liefert mittlerweile eine Vielzahl an Ermächtigungsgrundlagen für Überwachungsmaßnahmen, die im weiteren Sinn auf künstlicher Intelligenz basieren. Eine grobe Vorab-Kategorisierung kann danach vorgenommen werden, ob die

gefallen ist, vgl. Annex III lit. g AI Act-Entwurf (dort wurden als *High-Risk*-Anwendung definiert “AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data”). Ausdrücklich *keine High-Risk*-Anwendungen sind nach ErwGr. 59 S. 6 „KI-Systeme, die speziell für Verwaltungsverfahren in Steuer- und Zollbehörden sowie in Zentralstellen für Geldwäsche-Verdachtsanzeigen, die Verwaltungsaufgaben zur Analyse von Informationen gemäß dem Unionsrecht zur Bekämpfung der Geldwäsche durchführen, bestimmt sind [...]“.

28 Krit. (auch zur fehlenden Kompetenz der EU) und wie hier für ein enges Verständnis des Art. 5 AI Act insgesamt plädierend Krönke, NVwZ 2024, 529 (531 f.).

29 So jetzt auch Busche, AöR 149 (2024), 207 (246 f.).

mit der Überwachung betrauten Behörden Daten neu erheben oder vorhandene Daten zweckändernd nutzen, oder ob die Erhebung durch oder unter Mitwirkung von Privaten erfolgt. Interessant ist, das sei vorneweg gesagt, dass die mögliche „reflexive Dimension“³⁰ von KI-basierter oder -unterstützter staatlicher Überwachung bislang – soweit ersichtlich – ungenutzt bleibt: also KI zur Überwachung der Überwacher zu nutzen.

a. *Intelligente Videoüberwachung.* Paradigmatisch für staatliche *Intelligent Surveillance* steht die ‚intelligente‘ Videoüberwachung.³¹ Sie soll in der Lage sein, automatisch zu erkennen, ob in ihrem Erfassungsbereich etwas Gefährliches oder Verbotenes geschieht und soll zumindest³² Alarm schlagen können. In den USA sind vergleichbare Systeme schon flächendeckend ausgerollt,³³ in Deutschland wurden und werden sie getestet unter anderem von der Bundespolizei am Bahnhof Berlin-Südkreuz, von der baden-württembergischen Landespolizei³⁴ und der in Rheinland-Pfalz.³⁵ Die Bundespolizei kann sich dafür bislang lediglich auf die polizeiliche Datenschutz-Generalklausel in § 29 Abs. 1 S. 1 i. V. mit § 27 BPolG³⁶ stützen, die es der Bundespolizei erlaubt, Videoaufnahmen an bestimmten Orten zwecks Gefahrererkennung anzufertigen und sodann „personenbezogene Daten [zu] nutzen, soweit dies zur Erfüllung ihrer jeweiligen Aufgaben erforderlich ist“.³⁷ Ob dieses „Nutzen“ angesichts der strengen Bestimmtheitsanforderungen des Bundesverfassungsgerichts

30 Begriff von Ralf Poscher, Diskussionsbeitrag auf der Tagung Fachdialog Sicherheitsforschung „(Selbst)Überwachung: Zur Relevanz von neuen Techniken und Nutzungspraktiken für die zivile Sicherheit“, am 29.1.2021, via Webex.

31 Für Volkmann, NVwZ 2009, 216 f. steht schon die sozusagen klassische Videoüberwachung „paradigmatisch“ für das Sicherheitsbedürfnis der modernen Gesellschaft und den damit verbundenen sozialen Steuerungsanspruch des Staates.

32 Denkbar sind natürlich auch Erkennungssysteme, die im Gefahren(verdachts)fall bzw. im Fall von Regelverstößen automatisiert Sanktionen auf den Weg bringen. In China offenbar schon seit geraumer Zeit im Einsatz sind Überwachungssysteme, die Fußgänger, die rote Ampeln übertreten, per Gesichtserkennung identifizieren und automatisiert Bußgeldbescheide ausstellen, s. Nachw. bei Joh, Int. J. Law in Context 26 (2019), 177 (180).

33 Ferguson, The Rise of Big Data Policing, 2017, S. 86 ff., beschreibt das 9.000 Kameras umfassende System *Domain Awareness System* (DAS) in New York.

34 Vgl. Sprenger, in: Ebers et al. (Hg.), RechtsHdb. KI und Robotik, 2020, § 31 Rn. 45 ff.

35 Hier geht es um sog. „Handy-Blitzer“, d. h. Videoauswertungen, die Verstöße gegen § 23 Abs. 1a StVO automatisiert erkennen können sollen. Dazu rechtspolitisch befürwortend (wegen der erheblichen Gefährdung durch die Handynutzung am Steuer), rechtlich mangels Rechtsgrundlage aber abl., Roggan, NZV 2023, 145. So nun auch AG Trier, Urt. v. 2.3.2023, Az. 27c OWi 8041 Js 2838/23; keine taugliche Rechtsgrundlage.

36 Das BPolG sollte zwar umfassend reformiert werden, bis Stand Mai 2025 ist das allerdings nicht erfolgt. Dezidierte KI-Klauseln enthält die Novelle freilich nicht bzw. kaum.

37 Hinzuweisen ist i. d. Zusammenhang auf § 27 BPolG, der der Bundespolizei u. a. an Bahnhöfen den „Einsatz [von] selbsttätige[n] Bildaufnahme- und Bildaufzeichnungsgeräte[n]“ erlaubt, aber selbst nicht die Ermächtigung zur Nutzung, insb. nicht zur automatisierten Auswertung enthält. Dafür steht derzeit, wie gesagt, nur § 29 BPolG zur Verfügung.

an Eingriffsermächtigungen im Sicherheitsrecht auch den Einsatz ‚intelligenter‘ *Auswertungstechniken* umfasst, ist im Schrifttum umstritten.³⁸

- 22 Eindeutiger ist die Rechtslage in Baden-Württemberg. Im dortigen Polizeigesetz findet sich in § 44 PolG BW eine ausdrückliche Ermächtigung zum Einsatz solcher Systeme. Die Norm nennt zuerst in gewohnter Manier die Orte und Gelegenheiten, wo bzw. bei denen Video- und Tonaufnahmen³⁹ zulässig sind. Das sind nach Absätzen 1 bis 3 der Norm „öffentlichen Veranstaltungen und Ansammlungen, die ein besonderes Gefährdungsrisiko aufweisen“, besonders schützenswerte Objekte⁴⁰ oder öffentliche Orte, an denen „sich die Kriminalitätsbelastung [...] von der des übrigen Gemeindegebiets deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist.“ Die intelligente Komponente der Überwachung folgt dann ganz unscheinbar in Absatz 4 der Norm:

„¹Der Polizeivollzugsdienst kann die nach Absatz 1 Satz 2 Nummer 1 sowie Absatz 2 und 3 angefertigten Bildaufzeichnungen auch automatisch auswerten. ²Die automatische Auswertung darf nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein, die auf die Begehung einer Straftat hindeuten.“

- 23 § 44 Abs. 4 S. 2 PolG BW fordert damit neben der möglichst gezielten Sachverhaltsermittlung von der ‚Maschine‘ zugleich eine rechtliche Klassifikation und/oder Prognose. Hier zeigt sich, dass eine scharfe analytische Trennung zwischen reiner Sachverhaltsermittlung und rechtlicher Beurteilung/Bewertung angesichts der „Verwobenheit von Fakten und Normen“⁴¹ oftmals nicht möglich sein wird.⁴²
- 24 *b. Automatisierte Kennzeichenkontrollen.* Während die von § 44 PolG BW zugelassenen Verhaltensanalysen technisch komplex sind, ist eine andere ‚intelligente‘ Form der staatlichen Videoüberwachung bereits im Einsatz und technisch auch deutlich einfacher gelagert: die Nutzung von Kennzeichenerfassungssystemen im Straßenverkehr, die auf vergleichsweise simplen Bilderkennungs-technologien aufbauen. Sie sollen schlicht Kennzeichen von Kraftfahrzeugen richtig auslesen.
- 25 Im Anschluss an den *Kennzeichenkontrollen-II*-Beschluss des Bundesverfassungsgerichts und die *Section-Control*-Entscheidungen der (Ober-)Verwaltungsgerichte in

38 Schenke, in: Schenke/Graulich/Ruthig (Hg.), *Sicherheitsrecht des Bundes*, 2019, § 27 BPoG Rn.18 m. w. N. zum Streitstand. Hierzu Details unten, → § 2 Rn. 87.

39 Die Möglichkeit automatisierter Auswertung von Tonaufnahmen wird hier nicht weiter vertieft, da sie in Deutschland m. W. bislang ungebräuchlich ist. Das liegt einerseits an der besonderen Grundrechtsrelevanz wegen des möglichen Eingriffs in das Recht am nicht-öffentlich gesprochenen Wort, andererseits daran, dass die Technologien wohl noch nicht ausgereift sind. Für einige Bsp. und zur US-amerikanischen Diskussion unten, in → § 2 Fn. 830.

40 s. für Details § 27 Abs. 1 Nr. 4 PolG BW.

41 Vgl. Möllers, *Die Möglichkeit der Normen*, 2018, ab S. 194, Zitat S. 197.

42 s. für das allg. VerwR ausf. J.-P. Schneider, in: Schoch/Schneider (Hg.), *VwVfG*, Stand Grundwerk Juli 2020, § 24 Rn. 29 ff. m. w. N.

Hannover bzw. Lüneburg hat beispielsweise der niedersächsische Polizeigesetzgeber ein ganzes Arsenal an Ermächtigungen zum Einsatz solcher Technologien geschaffen. Einschlägig sind – systematisch etwas unglücklich verteilt – § 32 Abs. 6 NPOG und § 32a NPOG.⁴³ Es geht dabei um so unterschiedliche Zwecke wie streckenbezogene Geschwindigkeitskontrollen anhand der Nummernschilder (§ 32 Abs. 6 NPOG);⁴⁴ um deren Identifikation „zur Verhinderung des weiteren Gebrauchs von Kraftfahrzeugen ohne ausreichenden Versicherungsschutz“⁴⁵ (diese und alle folgenden Bsp.: § 32a Abs. 1 NPOG) sowie – klassischer – um die Identifikation zur „Abwehr erheblicher Gefahren“; außerdem um die Nutzung von Kennzeichenkontrollen zur „Verhütung von Straftaten von erheblicher Bedeutung mit Grenzbezug aufgrund polizeilicher Lageerkenntnisse“ und an bestimmten Orten (im Kern ist das die sogenannte Schleierfahndung); ferner: automatisierte Kennzeichenkontrollen zur „Verhütung von Straftaten“ an Orten, wo „Tatsachen die Annahme rechtfertigen, dass dort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben“ werden und in der unmittelbaren Nähe bestimmter anderer Orte wie Versorgungseinrichtungen und Amtsgebäuden, wenn „Tatsachen die Annahme rechtfertigen“, dass bestimmte Straftaten dort begangen werden sollen. Oder es geht um Kennzeichenkontrollen an „Kontrollstellen“, die eingerichtet werden dürfen, wenn „Tatsachen die Annahme rechtfertigen“, dass z. B. Straftaten von erheblicher Bedeutung (irgendwo) begangen werden sollen und die Kontrollstelle (konkret hier) für deren Verhütung erforderlich ist.

Die Normen enthalten außerdem zahlreiche Vorkehrungen im Sinne des Grundrechtsschutzes durch Verfahren, die das Bundesverfassungsgericht in *Kennzeichenkontrollen II* vorgegeben hat: Dazu zählen z. B. die Pflicht zur sofortigen Löschung der Daten im Nicht-Trefferfall;⁴⁶ zum grundsätzlich *offenen* Einsatz der Kennzeichenlesesysteme;⁴⁷ oder zur besonderen schriftlichen Anordnung ihres Einsatzes.⁴⁸ Grundsätzlich verboten ist die Erstellung von „Bewegungsbildern“⁴⁹ und der flä-

43 Jeweils i. d. F. vom 17.12.2019, gültig seit 28.12.2019 (Nds. GVBl., S. 428).

44 Das ist das sog. *Section Control*, weil die Durchschnittsgeschwindigkeit auf einer längeren Wegstrecke durch Erkennung und Speicherung eines Kennzeichens bei Einfahrt in den kontrollierten Bereich und bei Ausfahrt ermittelt wird, dazu – die Verfassungskonformität der Norm bejahend – OVG Lüneburg, Urt. v. 13.11.2019, Az. 12 LC 79/19 = NZV 2020, 145 – Section Control (mit zust. Anm. Müller) m. w. N. zur Rspr.- und Normhistorie, und BVerwG, Beschl. v. 31.7.2020, Az. 3 B 4/20 = NZV 2021, 99, zur Zurückweisung der Nichtzulassungsbeschwerde gegen das Urteil des OVG.

45 § 32a Abs. 1 S. 1 Nr. 6 NPOG, zurückgehend (wohl) auf die ausdr. Nennung eines solchen Einsatzzweckes in BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 94. Interessant ist insofern § 58 des neuen Sächsischen Polizeivollzugsdienstgesetzes, der anlasslose Stichprobenkontrollen nicht nur zum Auffinden von Kfz ohne ausreichenden Pflichtversicherungsschutz zulässt, sondern auch „mit dem Ziel der Sicherstellung gestohlener oder sonst abhanden gekommener Kraftfahrzeuge oder Kraftfahrzeugkennzeichen“ (§ 58 Abs. 1 Nr. 2 SächsPVDG).

46 Vgl. § 32 Abs. 6 S. 3, § 32a Abs. 3 S. 1 NPOG.

47 Vgl. § 32 Abs. 6 S. 1, 4, § 32a Abs. 4 NPOG.

48 Vgl. § 32a Abs. 5 NPOG.

49 Vgl. § 32a Abs. 3 S. 2 NPOG.

chendeckende Einsatz der Technologien.⁵⁰ Auszuschließen ist, dass die „Insassen“ der Fahrzeuge „zu sehen sind oder sichtbar gemacht werden können“.⁵¹ Schließlich ist speziell der Einsatz zum Zweck der Ermittlung von fehlendem Versicherungsschutz „auf Stichproben zu begrenzen“.⁵²

- 27 Andere Bundesländer⁵³ und auch der Bund⁵⁴ haben strukturell vergleichbare Vorschriften erlassen. Der extreme Spezifizitäts- und Detailgrad der Normen ist dem im Sicherheitsrecht besonders scharf gestellten Bestimmtheitsgebot geschuldet, worauf ich im Rahmen der systematischen Zusammenschau näher eingehen werde (→ S. 104 ff.).
- 28 c. *„Intelligente“ Verdachtsgewinnung unter Einsatz von Radar- und LiDAR-Technologien.* Verdachtsgewinnungsverfahren unter Einsatz von Radar- und LiDAR-Technologien befinden sich meines Wissens noch im experimentellen Stadium. Ihre Besonderheit könnte darin liegen, dass sie in der Lage sein könnten, einen verhaltensbezogenen Gefahren- oder Anfangsverdacht zu generieren, ohne dafür auf die Auswertung personenbezogener Daten angewiesen zu sein. Das wäre einigermaßen revolutionär, weshalb ein erster Anwendungsfall von LiDAR-Technologie hier näher analysiert werden soll.
- 29 Es handelt sich um den Probeeinsatz eines Systems durch die Stadt Rüsselsheim am Main, das dazu dienen soll, Verstöße gegen ein immissionsschutzrechtlich motiviertes Durchfahrverbot für Lastkraftwagen von mehr als 7,5 Tonnen Gewicht zu detektieren.⁵⁵ Theoretisch könnten dafür Kennzeichenlesegeräte genutzt werden, wenn und weil das Kennzeichen in den Datenbanken der Zulassungsbehörden mit dem zulässigen Gesamtgewicht des Fahrzeugs verknüpft ist. Die LiDAR-Technologie kommt jedoch im ersten Schritt ohne Kennzeichenerfassung aus: LiDAR arbeitet mit Laserstrahlen, die für das menschliche Auge ungefährlich sind. Im Unterschied zu Radar, das methodisch an sich vergleichbar mit Strahlen arbeiten, erlaubt es die LiDAR-Technologie, die Tiefe von Objekten zu erfassen, erlaubt also mit anderen Worten dreidimensionale Modellierung. An einem Kontrollpunkt A wird nun

50 Vgl. § 32a Abs. 1 S. 3. Speziell für die Geschwindigkeitskontrolle fehlt die Einschränkung des „Nicht-Flächendeckenden“, s. dazu aber OVG Lüneburg, Urt. v. 13.11.2019, Az. 12 LC 79/19 = NZV 2020, 145 (146): „Dem Kläger kann [...] nicht in der Annahme gefolgt werden, von Verfassungen wegen müsse die in § 32 [Abs. 6] NPOG enthaltene Ermächtigung zur Kennzeichenerfassung [...] gesetzlich weiter gehend eingegrenzt werden, etwa auf Strecken mit besonderer Unfallträchtigkeit oder einer überdurchschnittlich hohen Quote von Geschwindigkeitsverstößen [...]“. Im Übrigen besteht jedenfalls gegenwärtig auch deshalb kein Anlass für den Landesgesetzgeber, den Anwendungsbereich des § 32 [Abs. 6] NPOG zu beschränken, weil [...] jegliche Anzeichen für eine flächendeckende Ausdehnung in Niedersachsen als Massenerscheinung fehlen; dies liegt auch angesichts des [...] Aufwands fern.“

51 § 32 Abs. 6 S. 2, § 32a Abs. 1 S. 2 NPOG.

52 § 32a Abs. 1 S. 6 NPOG.

53 Z. B. § 51 i. V. m. § 27 PolG Baden-Württemberg.

54 Z. B. § 63c StVG, § 163g StPO.

55 s. ausf. D. Müller, SVR 2022, 41 ff.

mithilfe dieser Technologie bzw. der damit verknüpften Mustererkennungssoftware ein Profil der einfahrenden Fahrzeuge nach Größe und anderen Formmerkmalen erstellt und zusammen mit einem Zeitstempel zwischengespeichert. Ergänzt wird die Erfassung durch eine Bildaufnahme, die allerdings so niedrigauflösend sein soll, dass Details des Fahrzeugs und insbesondere seiner Fahrerin nicht erkennbar sind. LiDAR-Aufnahmen, die nicht in das Profil ‚Lkw‘ passen, werden sofort gelöscht. Die zwischengespeicherten Daten sollen nun so individuell sein, dass sie eine Wiedererkennung des Fahrzeugs an Kontrollpunkt B ermöglichen. Ist der zeitliche Abstand zwischen A und B so kurz, dass es den Rückschluss erlaubt, dass tatsächlich nur eine Durchfahrt vorliegt (eine Anfahrt z. B. an einen Supermarkt wäre ja erlaubt), dann löst das System an Kontrollpunkt B eine hochauflösende Bildaufnahme aus, die dann von der Bußgeldbehörde weiter bearbeitet wird.

Dieter Müller hat sich in einem Gutachten-Aufsatz⁵⁶ als einer der ersten ausführlich mit den juristischen Implikationen dieser Konstruktion befasst; in Auseinandersetzung gerade auch mit der Entscheidung des Bundesverfassungsgerichts in *Kennzeichenkontrollen II*.⁵⁷ Müller geht davon aus, dass das Rüsselsheimer Modell nach deren Maßstäben *keinen* Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt, weil

„am Kontrollpunkt A mittels LiDAR und Kamera für sich genommen, d. h. ohne Hinzuziehen der am Kontrollpunkt B gewonnenen Zusatzinformationen, keine Identifizierung von Kfz und Fahrenden möglich ist[. Weil damit] an Kontrollpunkt A ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung [also] vollständig ausgeschlossen ist“⁵⁸

erfolge auch der Abgleich an Kontrollpunkt B seinerseits nicht mit personenbezogenen Daten (im Fall von *Kennzeichenkontrollen II*: mit dem Fahndungsregister; im Fall von *Section Control*:⁵⁹ mit dem bei Einfahrt in die Kontrollstrecke gespeicherten Kennzeichen).⁶⁰ Folge: Es bedürfe, so Müller, keiner eigenständigen Rechtsgrundlage für die Erfassung des Fahrzeugprofils an Kontrollstelle A und des Abgleichs/der Zeitauswertung an Kontrollstelle B; vielmehr reiche vorliegend *insgesamt* die ordnungswidrigkeitsrechtliche Dokumentationserlaubnis von *schon als solchen erkannten* Verdachtsfällen aus.⁶¹

Wenn diese Lesart zuträfe, dann könnte das erhebliche Folgen haben: Es wäre einerseits ein technologiebasiertes Verdachtsgewinnungsverfahren geschaffen, das mangels Eingriffs in ein Grundrecht keiner gesetzlichen Ermächtigungsgrundlage

56 Ausweislich der *-Fußnote wurde das dem Aufsatz zugrundeliegende Gutachten im Auftrag des Unternehmens erstellt, das die in Rüsselsheim eingesetzte Technologie entwickelt hat.

57 Dazu schon oben, → § 2 Rn. 25 f.

58 D. Müller, SVR 2022, 41 (48).

59 Dazu schon oben, in/bei → § 2 Fn. 44.

60 D. Müller, SVR 2022, 41 (48).

61 § 100h Abs. 1 S. 1 StPO i. V. m. § 46 Abs. 1 OWiG.

bedürfte, und das andererseits in seinem Anwendungsbereich zumindest potentiell weit über die Typenkontrolle von Fahrzeugen ausgeweitet werden könnte: *Müller* selbst weist auf Technologien in der Erprobungsphase hin, die das Gewicht von Fahrzeugen mittels LiDAR erfassen können sollen.⁶² Zudem finden sich Berichte darüber, das Forschergruppen an Verfahren der Verhaltens- und Gestenerkennung durch immer weiter „miniaturisiertes“ Radar arbeiten,⁶³ das es erlauben soll, z. B. riskantes Verhalten im Straßenverkehr⁶⁴ und im Haushalt⁶⁵ als solches zu erkennen. Auch hierbei handelt es sich – das ist der zentrale Unterschied zur intelligenten Videoüberwachung – zunächst wohl um die Verarbeitung von *nicht* personenbezogenen Daten,⁶⁶ die erst im Fall eines Treffers z. B. einen Alarm oder eine Videoaufnahme auslösen könnten. Auch hierzu folgt die rechtliche Wertung an späterer Stelle (→ § 2 Rn. 128 ff.).

- 32 *d. Data Mining.* Ein rechtlich erneut kategorial anders gelagertes, weil nicht mit Datenneuerhebungen verbundenes Beispiel intelligenter Überwachung bieten die diversen Ermächtigungsgrundlagen für das, was mittlerweile unter dem Oberbegriff des polizeilichen *Data Mining* Bekanntheit erlangt hat.⁶⁷ Normbeispiele liefern § 6a Antiterrordateigesetz [ATDG], § 7 Rechtsextremismus-Datei-Gesetz [RED-G], § 25a des hessischen Gesetzes über die öffentliche Sicherheit und Ordnung [HSOG] und § 49 des hamburgischen Gesetzes über die Datenverarbeitung der Polizei [PolDVG]. Bei allen Unterschieden im Detail geht es diesen Ermächtigungsgrundlagen durchgängig darum, die automatisierte Auswertung von bereits beim Staat *vorhandenen* Daten zu erlauben, um Verhaltens- oder Beziehungsmuster zu erkennen, die für bestimmte Straftaten oder Gefahren indikativ sind. Es geht also, in der datenschutzrechtlichen Terminologie gesprochen, oftmals um zweckändernde Datenweiterverarbeitungen.
- 33 ‚Gemustert‘ werden dürfen (bzw. durften – siehe sogleich) im Fall der beiden Landesgesetze undifferenziert die „polizeilichen Datensysteme“ (§ 49 Abs.1 PolDVG) oder die von Polizeibehörden „gespeicherten personenbezogenen Daten“ (§ 25a Abs.1 HSOG). Bei ATDG und RED-G geht es um die jeweils namensgebenden Verbunddateien, die sowohl von polizeilichen wie auch nachrichtendienstlich tätigen Bundes- und Landesbehörden beschickt werden müssen. Das Mustern selbst

62 *D. Müller*, SVR 2022, 41 (47 f.).

63 *s. Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik FHR*, Radar: Für Mensch und Umwelt, www.fhr.fraunhofer.de/de/geschaeftsfelder/mensch_und_umwelt.html, besucht am 26.4.2023.

64 *s. Weiffenfels/Wilking*, technikjournal v. 20.5.2021 (Onlinequelle).

65 Sog. „Präsenzsensoren“, hierzu nur *Spehr*, F.A.Z. v. 11.7.2023, S. T 4.

66 Es handelt sich nicht um biometrische Daten i. S. v. Art. 4 Nr. 14 DSGVO, da es nicht um die eindeutige Identifikation einer bestimmten Person geht, sondern um die Suche nach verallgemeinerbaren Handlungsmustern, die gerade *nicht* typisch für eine konkrete Person sein dürfen, damit der Ansatz funktioniert.

67 Hierzu ausf. *Sprenger*, in: Ebers et al. (Hg.), RechtsHdb. KI und Robotik, 2020, § 31 Rn. 30 ff. m. w. N.

fasst § 6a Abs. 5 ATDG – wenig anschaulich – unter dem Begriff der „erweiterten Datennutzung“, und definiert diese folgendermaßen:

„(5) ¹Eine erweiterte Nutzung sind das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. ²Hierzu dürfen die beteiligten Behörden des Bundes Daten auch mittels

1. phonetischer oder unvollständiger Daten,
2. der Suche über eine Mehrzahl von Datenfeldern,
3. der Verknüpfung von Personen, Institutionen, Organisationen, Sachen oder
4. der zeitlichen Eingrenzung der Suchkriterien

aus der Datei abfragen sowie räumliche und sonstige Beziehungen zwischen Personen und Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen darstellen sowie die Suchkriterien gewichten.“

Ähnliche Definitionen enthalten alle der oben genannten Gesetze, wobei die beiden Landesgesetze anschaulicher von einer „automatisierten Anwendung zur Datenanalyse“ (§ 49 PolDVG) oder „automatisierten Anwendung zur Auswertung vorhandener Daten“ sprechen (§ 25a HSOG). Welche Techniken eingesetzt werden dürfen, spezifiziert(e) keine der genannten Normen,⁶⁸ sodass gerade auch Muster miterfasst sind, die aus künstlicher Intelligenz im oben beschriebenen Sinn resultieren.⁶⁹ 34

Alle Normen zum *Data Mining* sehen sich erheblicher verfassungsrechtlich begründeter Kritik ausgesetzt. Sie entzündet sich vor allem an der partiellen Durchbrechung des datenschutzrechtlichen Zweckbindungsgrundsatzes und des informationellen Trennungsprinzips zwischen unterschiedlichen Behörden, die beide die sicherheitsrechtliche Struktur der Bundesrepublik prägen. Eingeführt werde durch die jeweiligen „Datenpools“ ein übergreifendes „informationelles Verfügbarkeitsprinzip“. ⁷⁰ Konkret wird gerügt, dass die für die Durchbrechung bislang legislativ vorgesehenen Eingriffsschwellen zu niedrig⁷¹ und/oder zu unbestimmt seien.⁷² Vereinfacht gesagt geht es stets um die Frage, was bei der ermittelnden Stelle eventuell schon bekannt sein muss, bevor sie mithilfe des *Data Mining* unter Einbeziehung von *für andere Zwecke* bzw. *von anderen Behörden* angelegten staatlichen Datenbanken nach neuen Zusammenhängen und Erkenntnissen suchen darf.⁷³ 35

68 Dazu krit. Arzt, in: Schenke/Graulich/Ruthig (Hg.), *Sicherheitsrecht des Bundes*, ²2019, § 6a ATDG Rn. 26.

69 I. d. S. auch Golla, NJW 2021, 667 (671 ff.); andeutungsweise auch BVerfG, Beschl. v. 10.11.2020, Az. 1 BvR 3214/15 = BVerfGE 156, 11 – Antiterrordateigesetz II, Rn. 73: „mit praktisch allen informationstechnisch möglichen Methoden“.

70 Arzt, in: Schenke/Graulich/Ruthig (Hg.), *Sicherheitsrecht des Bundes*, ²2019, § 6a ATDG Rn. 7 f.

71 Z. B. *ibid.*, Rn. 7 ff.

72 *Ibid.*, Rn. 22.

73 Zur erfolgreichen Verfassungsbeschwerde gegen § 6a Abs. 2 ATDG (zu niedrige Eingriffsschwelle für das Mustern zu strafrechtlichen Zwecken) s. Golla, NJW 2021, 667 ff.

- 36 Besonders offen gehalten waren insofern die landesrechtlichen Normen, die das *Data Mining* auf Anordnung (immerhin!) des Behördenleiters bzw. seines Vertreters „in begründeten Einzelfällen“ zulassen wollten. Das RED-G (§ 7) und das ATDG (§ 6a) sind spezifischer abgefasst und sehen konkrete und differenzierte Eingriffsschwellen für straf- und gefahrenabwehrrechtliche sowie nachrichtendienstliche Datenauswertungen vor. In der gefahrenabwehrrechtlichen Dimension, die uns vorliegend besonders interessieren soll, weil sie unmittelbar auf die Durchsetzung von Verhaltenspflichten bezogen ist, sind das beispielsweise „Tatsachen[, welche] die Annahme rechtfertigen, dass eine [qualifizierte] Straftat [des internationalen Terrorismus]⁷⁴ begangen werden soll“. Das *Data Mining* muss „für die Verhinderung [dieser] Straftat erforderlich [sein], um weitere Zusammenhänge des Einzelfalls aufzuklären“. In seiner ersten *Data-Mining*-Entscheidung hat das Bundesverfassungsgericht diese Schwelle im Wege verfassungskonformer Auslegung dahingehend spezifiziert, dass zumindest eine „hinreichend konkretisierte Gefahr“⁷⁵ der Begehung einer qualifizierten Straftat bestehen muss.⁷⁶
- 37 In der im Jahr 2023 ergangenen Entscheidung zu den beiden *landesrechtlichen* Vorschriften war eine solche verfassungskonforme Auslegung schwerlich möglich; dafür waren die Vorschriften zu unbestimmt. Nicht überraschend hat das Bundesverfassungsgericht sie deshalb für verfassungswidrig erklärt, dabei allerdings detailliert aufgezeigt, unter welchen Voraussetzungen, d. h. vor allem ab welchen

74 Definiert in § 6a Abs. 3 S. 2, Abs. 2 S. 2 ATDG: „Qualifizierte Straftaten des internationalen Terrorismus sind Taten des internationalen Terrorismus, die einen Straftatbestand nach den §§ 89a, 89b, 91, 102, 129a, 129b, 211 oder 212 des Strafgesetzbuchs erfüllen.“

75 Das BVerfG definiert die im 141. Band (S. 220 [271] – BKA-Gesetz) erfundene Kategorie so: Es müssen „zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. [...] Eine hinreichend konkretisierte Gefahr [i. d. S.] kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen.“ Nach bis dato g. h. M. handelte es sich beim Beschriebenen freilich um einen Fall der *konkreten* Gefahr. Hier muss bzw. musste die auf Tatsachen gestützte, hinreichende Wahrscheinlichkeit eines Schadenseintritts bestehen. In Anwendung der sog. je-desto-Formel durften aber (traditionell selbstverständlich) Abstriche bei der Vorhersehbarkeit des *exakten* Kausalverlaufs gemacht werden, u. a. abhängig davon, wie gewichtig die potentiell geschädigten Güter sind. Die *konkretisierte* Gefahr spaltet also nun den bisher einheitlichen, aber flexiblen Begriff der konkreten Gefahr in zwei Kategorien auf, verengt daher potentiell massiv den Erfassungsbereich der traditionellen, auf die konkrete Gefahr bezogenen Generalklauseln und sonstigen Eingriffsermächtigungen der Polizeigesetze. Zum Ganzen *Möstl*, GSZ 2021, 89 (90 f.) m. w. N. sowie zu den von BVerfGE 141, 220 angestoßenen Reformen der Landespolizeigesetze. Bes. krit. zur Rspr. *M. Thiel*, Die Verwaltung 53 (2020), 1 (2 f.). Das BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 58, geht nunmehr davon aus, dass es sich bei der „hinreichend konkretisierte[n] Gefahrenlage“ um die „traditionelle“ Eingriffsschwelle im Bereich der Gefahrenabwehr“ handele, definiert aber a. a. O., Rn. 106, gleichwohl weiterhin i. S. des gespaltenen Begriffs: „Eine hinreichend konkretisierte Gefahr setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr [...] bestehen.“

76 BVerfG, Beschl. v. 10.11.2020, Az. 1 BvR 3214/15 = BVerfGE 156, 11 – Antiterrordeutgesetz II, Rn. 118.

Eingriffsschwellen „deterministische“⁷⁷ und sogar „selbstlernende“ Systeme alias „Künstliche[] Intelligenz“⁷⁸ zu präventivpolizeilichen Zwecken eingesetzt werden dürfen. Kurz: Der Einsatz selbstlernender Systeme soll ab Vorliegen einer zumindest „konkretisierten Gefahr“ möglich sein,⁷⁹ der von deterministischen Systemen ist unter stark reduzierten⁸⁰ Voraussetzungen zulässig.

Auf die wichtige Schwellenfrage gehe ich in der Zusammenschau von staatlicher *Intelligent Surveillance* ausführlicher ein, weil sich hier verallgemeinerbare und konsolidierte ‚große Linien‘ der verfassungsgerichtlichen Rechtsprechung herausarbeiten lassen (ab → S. 102). Zunächst sei hier in eher technischer Perspektive die vom Bundesverfassungsgericht zentral gestellte Unterscheidung zwischen deterministischen und selbstlernenden Systemen aufgegriffen; und *hier* ist zum gegenwärtigen Zeitpunkt noch Vorsicht geboten, was Verallgemeinerungen anbelangt. Die Unterscheidung klingt zwar einfach, ist aber bei genauerem Hinsehen problematisch. Kurz gesagt ist unklar, ob das Gericht einen engen Begriff des selbstlernenden Systems verwendet (= dynamische *Weiterentwicklung* des Systems während der *Nutzungsphase*), oder den zu weiten Begriff des selbstlernenden Systems, der schlicht alle *ML-trainierten* Systeme erfasst, unabhängig davon, ob sie nach dem Training „eingefroren“ wurden oder eben auch danach noch weiterlernen.⁸¹

Bei schnellem Lesen scheint es so, als meine das Gericht mit „lernfähige[n] Systeme[n], also Künstlicher Intelligenz“ alle Systeme, die auf einem „maschinellen Lernprozess“ *aufbauen*, in dessen Verlauf sich „komplexe algorithmische Systeme [...] immer mehr von der ursprünglichen menschlichen Programmierung lösen [könnten]“.⁸² Daraus folgten sodann *möglicherweise* („könnten“, „droht“, „besteht [...] eine Gefahr“) die ML-typischen *Black-Box*-⁸³ und Diskriminierungsrisiken.⁸⁴ Deretwegen

„dürften [sic?] selbstlernende Systeme in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern.“⁸⁵

77 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 101.

78 Ibid., Rn. 100.

79 s. hierzu in Zusammenschau die Rn. 106, 110, 120 f. i. V. m. Rn. 100 f. in BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse.

80 s. bes. *ibid.*, Rn. 108. Zu dieser potentiell folgenreichen Randnummer ausf. unten, → § 2 Rn. 108 ff.

81 Zu diesen Begrifflichkeiten oben, → § 1 Rn. 18.

82 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 100.

83 s. hierzu oben, → § 1 Rn. 24 ff.

84 Hierzu → S. 53 ff.

85 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 100.

- 40 Schon dieser letzte Satz weckt freilich Zweifel daran, ob das Bundesverfassungsgericht wirklich einen weiten Begriff des selbstlernenden Systems (also unter Einschluss auch „eingefrorener“ Systeme⁸⁶) nutzen wollte. Diese Zweifel werden durch die Gegenüberstellung zu den vom Bundesverfassungsgericht sogenannten „deterministischen Systemen“ erhärtet. Deterministisch – und hinsichtlich der grundrechtlichen Eingriffstiefe weniger gravierend⁸⁷ – seien „Systeme, deren Analysefunktion sich [...] nicht eigenständig verändern kann, sondern [die] in der Software unveränderlich vorprogrammiert ist“; freilich „können [auch] diese komplex und für die Anwendenden und Betroffenen schwer nachvollziehbar sein“, weshalb „der Gesetzgeber [auch] dann für schützende Regelungen“ sorgen müsse.⁸⁸ Diese Definition von *deterministischem* System würde es auch erlauben, ein maschinell trainiertes und sodann „eingefrorenes“ KI-Modell als deterministisches System zu fassen.
- 41 Im Ergebnis denke ich, dass das Bundesverfassungsgericht sprachlich wenig glücklich, aber in der Sache klug spezifisch für seine Zwecke *ein relatives* Verständnis des selbstlernenden Systems vorgibt, das folgendermaßen zu verstehen ist: Grundsätzlich fallen darunter alle ML-trainierten Systeme. Wenn diese allerdings für die Nutzung eingefroren sind (d. h. technisch-formal deterministisch sind), *und* wenn Testverfahren gegen diskriminierende Ergebnisse sowie Verfahren der *explainable AI* umgesetzt werden, die die beschriebenen abstrakten *Black-Box*- und Diskriminierungsgefahren *in concreto* auflösen oder doch zumindest erheblich reduzieren, dann liegt ein im Sinn des Bundesverfassungsgerichts deterministisches System vor, das von Grundrechts wegen weniger restriktiven Voraussetzungen unterliegt.
- 42 Zwei zusätzliche Überlegungen bzw. Aspekte im Urteil sprechen für einen solchen relativen Begriff des Selbstlernens:
- *Erstens* leitet das Gericht seine Überlegungen zur Verwendung selbstlernender Systeme mit der unscheinbaren, aber wichtigen Bemerkung ein, dass ein „lernfähige[s] System[],^[89] also künstliche[] Intelligenz (KI)“ ein „[b]esonderes Eingriffsgewicht [...] haben“ „kann“, und zwar: „je nach Einsatzart“.⁹⁰ Damit vermeidet das Gericht, dass schon der Einsatz von heutzutage relativ banaler Bilderkennungssoftware z. B. für die Zwecke automatisierter Kennzeichenkontrollen – technisch immer noch ein Parade-Anwendungsfall für KI-Systeme –, dass also *allein schon* der Einsatz einer solchen Software zu einem besonders hohen Eingriffsgewicht

86 Zu diesen Begrifflichkeiten oben, bei/ab → § 1 Rn. 18.

87 Vgl. BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 120 f. i. V. m. Rn. 101, 100.

88 Ibid., Rn. 101.

89 Ich verstehe „lernfähig“ hier als Synonym für „selbstlernend“. Aber auch das ist eine sprachliche Diskrepanz, welche Rn. 100 in BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, schwer interpretierbar macht.

90 Ibid., Rn. 100. Hervorhebung hier.

führen würde. Das wäre angesichts des Stands der Technik und vor allem der relativ einfachen menschlichen Überprüfbarkeit im Einzelfall (= Bilder nebeneinander halten!) keine sinnvolle Wertung.

- Für das relative, d. h. vom konkreten Einsatzfeld und dem Stand der Technik abhängige Verständnis dessen, was im Sinne des Gerichts *selbstlernend* ist, spricht *zweitens*, dass das Gericht die selbstlernenden Systeme in einem Atemzug mit einem *anspruchsvollen* Verständnis von *Predictive Policing* nennt; anspruchsvoll in dem Sinn, dass *Predictive Policing* theoretisch auch zwar statistisch signifikante und polizeilich gut brauchbare, aber menschlich *nicht mehr (oder noch nicht) nachvollziehbare Ergebnisse* liefern könnte, die sich also – in den Worten des Gerichts – als *selbstständige* „maschinell[e] Gefährlichkeitsaussagen“ über Personen erweisen könnten.⁹¹ Aber genau das, also die menschlich fehlende Nachvollziehbarkeit, ist eine Frage des konkreten Einsatzfeldes und kann durch allerlei Instrumente der *Explainability* soweit reduziert und durch Test-, Evaluations- und Sicherungssysteme flankiert werden, dass im konkreten Fall keine relevanten Unterschiede zu einer menschlichen Arbeitsteilung mit ebenfalls gestuften Wissensbildungsprozessen und den damit verbundenen menschlichen *Black-Box*-Effekten mehr bestehen müssen.

Es bleiben letztlich bedauerliche und angesichts des Standes der Debatte überflüssige Zweifel, was genau mit dem entscheidenden Begriffspaar des selbstlernenden und des deterministischen Systems gemeint sein soll. Diese Uneindeutigkeit an dieser doch recht zentralen Stelle teilt das Bundesverfassungsgericht freilich mit dem Europäischen Gerichtshof, auf den das Verfassungsgericht auch ausdrücklich, aber leider auch wieder unklar („vgl.“⁹²) verweist.⁹³ Der EuGH hat sich zwar noch nicht zum *Data Mining* im soeben beschriebenen Sinn äußern können, dafür aber zum sogenannten Fluggastdatenabgleich und dem auch dort möglichen Einsatz von KI. Darum wird es jetzt gehen.

e. Fluggastdatenabgleich. Alle drei bisherigen Beispiele – also die intelligente Videoüberwachung, die Kennzeichenerfassung und die diversen Formen des *Data Mining* – haben gemeinsam, dass die Polizeien/Strafverfolgungsbehörden die Überwachungs- und Auswertungsarbeit selbst leisten, freilich gegebenenfalls unter Nutzung meist ‚zugekaufter‘ Software.⁹⁴ Der Zugriff erfolgt über polizeilich installierte Kameras bzw. auf staatliche Datenbanken. Anders verhält es sich in den folgenden

91 Vgl. – unter Verweis auf Rademacher, AöR 142 (2017), 366 ff., wo es dezidiert um solche *nicht* nachvollziehbaren Anwendungen geht – BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 97, 99.

92 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 100.

93 Krit. zur missverständlichen Wortwahl des EuGH, die sich *mutatis mutandis* auf das BVerfG-Urteil übertragen lässt, Kostov, GSZ 2023, 14 (15 f.), und → § 2 Rn. 56.

94 Zu dieser Wissens- und Herrschaftsproblematik → § 2 Rn. 418 und → § 4 Rn. 160 ff.

drei Anwendungsfeldern, in denen in unterschiedlicher Intensität *Private* in die Überwachung eingebunden sind: als Überwachungsdaten-Beschaffer über Dritte (sogleich, hier unter e.), als Daten-Beschaffer über sich selbst (Steuerrecht, dazu ab → S. 94), und als Daten-Auswerter über Dritte (Finanzaufsichtsrecht, namentlich Geldwäschebekämpfung, dazu ab → S. 95).

- 45 aa. *Grundzüge der gesetzlichen Regelungen und deren praktischer Einsatz.* Das erste Anwendungsbeispiel, das auf private Datenbeschaffung über Dritte baut, zählt noch zum Sicherheitsrecht im klassischen Sinn. Es geht um den sogenannten Fluggastdatenabgleich, den der Bundesgesetzgeber in Umsetzung der entsprechenden EU-Richtlinie (EU) 2016/681 [PNR-Richtlinie] im Fluggastdatengesetz [FlugDaG] vorgesehen hat. Gemustert werden diejenigen Daten, die eine Fluggesellschaft über die von ihr beförderten Personen erhebt und die sie dann an die beim BKA eingerichtete Fluggastdatenzentralstelle liefern muss (§§ 2, 1 Abs. 1 FlugDaG). Ziel des Verfahrens ist einmal ein Abgleich der Daten mit Fahndungsdateien, also die Suche nach zur Suche ausgeschriebenen Personen.⁹⁵ Das soll uns hier nicht weiter interessieren. Interessant ist vielmehr der sogenannte vorzeitige⁹⁶ Musterabgleich. Ziel hierbei ist es gem. § 4 Abs. 1 Hs. 1 FlugDaG, bislang nicht gesuchte/bekannte

„Personen zu identifizieren, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie eine [in Hs. 2 näher bezeichnete terroristische Straftat oder schwere grenzüberschreitende Delikte] begangen haben oder innerhalb eines übersehbaren Zeitraumes begehen werden“.

- 46 Entsprechende „Treffer, die aus einem vorzeitigen [Muster-]Abgleich resultieren, werden von der Fluggastdatenzentralstelle individuell überprüft“⁹⁷ bevor diese Stelle die Daten an die für Folgemaßnahmen zuständigen Ermittlungsbehörden⁹⁸ weiterleiten darf. Eine irgendwie konkretisierte Eingriffsschwelle ist nach dem Richtlinien-, wie auch nach dem Gesetzeswortlaut nicht zu überschreiten, das Verfahren *scheint* – siehe sogleich – vielmehr auf alle das Bundesgebiet verlassenden bzw. alle einreisenden Fluggäste anzuwenden zu sein.⁹⁹ Eine Differenzierung nach präventiven und repressiven Zwecken erfolgt auf der Ebene des Musterabgleichs nicht, vielmehr stehen beide gleichberechtigt nebeneinander.
- 47 Die bislang verfügbaren bzw. genutzten Muster sind nach den öffentlich zugänglichen Informationen wenig komplex, basieren (wohl) noch nicht auf maschinell

95 s. hierzu *Ruthig*, in: Schenke/Graulich/Ruthig (Hg.), *Sicherheitsrecht des Bundes*, ²2019, § 4 FlugDaG Rn. 3 m. w. N.

96 „Vorzeitig“ meint *vor Abflug* eines Passagiers von oder *vor Ankunft* auf einem deutschen Flughafen, s. § 4 Abs. 2 S. 1 FlugDaG.

97 § 4 Abs. 2 S. 2 FlugDaG.

98 s. §§ 6 ff. FlugDaG.

99 § 4 Abs. 2 S. 1 FlugDaG.

Lernen, sondern auf leicht erfassbaren symbolischen Elementen¹⁰⁰ und werfen daher viele der in → § 3 beschriebenen KI-spezifischen Fragen noch nicht auf. Zudem scheint die Zahl der *False Positives* außerordentlich hoch zu sein,¹⁰¹ sodass die ‚Intelligenz‘ des Verfahrens noch stark angezweifelt werden kann. Allerdings *kann* § 4 FlugDaG mit seinen offenen Formulierungen („Muster“) ohne Weiteres auch den Einsatz von maschinell trainierten Mustern gestatten, sodass der Fluggastdaten-abgleich mittlerweile eines der zentralen Referenzfehler für Verdachtsgewinnungsverfahren unter Nutzung moderner Technologien geworden ist.¹⁰² Zudem hat der Gesetzgeber hier die Gefahren algorithmischer Diskriminierung ausdrücklich erkannt und mit § 4 Abs. 3 S. 7 FlugDaG eine lange Liste von Merkmalen (z. B. Ethnie, Religion, Sexualleben) aufgestellt, die *nicht* Bestandteil („Prüfungsmerkmal“) der Muster sein dürfen.

bb. Einschränkungen durch den EuGH. In diese richtlinienrechtlichen bzw. gesetzlichen Vorgaben hat der EuGH mit seinem Urteil zur PNR-Richtlinie im Frühsommer 2022 allerdings erheblich eingegriffen. Einige der darin im Wege primärrechtskonformer, insbesondere Artt. 7, 8 GRC verpflichteter Interpretation der Richtlinie¹⁰³ vorgenommenen Modifikationen und Klarstellungen sind im Weiteren relevant:

Hinsichtlich der geschützten Güter bzw. verfolgten Straftaten (also bezüglich der *Zwecke* der Ermittlungsmaßnahme) müssten, so der EuGH, die Mitgliedstaaten bei der Umsetzung sicherstellen, dass die Taten *erstens* tatsächlich zur schweren Kriminalität gehören, und nicht Taten der „gewöhnlichen Kriminalität“ erfassen¹⁰⁴ – was aufgrund der reichlich komplizierten Verweisteknik ins nationale Strafrecht, mit der die Richtlinie die Delikte bestimmt, nach denen geforscht werden muss,¹⁰⁵ durchaus denkbar ist.

100 Vgl. hierzu bereits Rademacher, AöR 142 (2017), 366 (371); das BKA selbst gibt zumindest öffentlich keine informative Auskunft über die verwendeten Muster, vgl. www.bka.de/DE/UnsereAufgaben/Aufgabenbereiche/Zentralstellen/Fluggastdatenspeicherung/FAQ/faq_node.html, besucht am 20.4.2023.

101 Vgl. BT-Drs. 19/9536 v. 17.4.2019, S. 5: Nach Auskunft der Bundesregierung wurden von 94.098 sog. „technischen Treffern“ von der Fluggastdatenzentralstelle 277 „fachlich positiv“ überprüft und anschließend zur weiteren Verwendung an die Bundespolizei übermittelt.

102 Vgl. Trute/S. Kuhlmann, GSZ 2021, 103 (108 ff.); Sprenger, in: Ebers et al. (Hg.), RechtsHdb. KI und Robotik, 2020, § 31 Rn. 28 f.; Rademacher, AöR 142 (2017), 366 (410 ff.).

103 Zum Gebot einer geltungserhaltenden Auslegung von Unionssekundärrecht EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 86. Der EuGH kam damit ohne eine (teilweise) Nichtigerklärung der Richtlinie aus.

104 Ibid., Rn. 149 ff.

105 s. Art. 3 Rn. 9 RL (EUR) 2016/681, der „schwere“ Kriminalität definiert durch Verweis auf „die in Anhang II [der Richtlinie] aufgeführten strafbaren Handlungen, die nach dem nationalen Recht eines Mitgliedstaats mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind“. Hervorhebung hier. Diese Technik führt dazu, dass z. B. ein einfacher Betrug (§ 263 StGB) schwere Kriminalität wäre. Zur Kritik daran schon Rademacher, AöR 142 (2017), 366 (413).

- 50 Wichtig ist sodann *zweitens*, was der EuGH unter Verhältnismäßigkeitsgesichtspunkten als „*Zusammenhang* zwischen [Fluggast-]Daten und den Zielsetzungen der Verarbeitung dieser Daten“¹⁰⁶ verlangt: Insoweit würden es Artt. 7, 8 GRC

„von den Mitgliedstaaten [verlangen], u. a. [?] bei der [...] vorgesehenen individuellen Überprüfung auf nicht automatisierte Art dafür zu sorgen, dass die Anwendung des durch die Richtlinie geschaffenen Systems auf terroristische Straftaten und auf schwere Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen beschränkt wird.“¹⁰⁷

- 51 Diese Beschränkung *kann* also, *muss* aber offenbar nicht schon zwingend in das Design der Muster einfließen. Zudem ist der geforderte Zusammenhang relativ lose:

„[A]uch strafbare Handlungen, die keinen [...] unmittelbaren Zusammenhang mit der Beförderung von Fluggästen aufweisen,¹⁰⁸ können] je nach den Umständen des Einzelfalls einen mittelbaren Zusammenhang mit der Beförderung der Fluggäste aufweisen [was dem EuGH ausreicht]. Dies gilt insbesondere dann, wenn die Beförderung auf dem Luftweg als Mittel zur Vorbereitung solcher strafbaren Handlungen dient oder dazu, sich nach deren Begehung der strafrechtlichen Verfolgung zu entziehen.“¹⁰⁹

- 52 Was es hingegen nach Auffassung des Gerichtshofs ausdrücklich *nicht* braucht, um den notwendigen Zusammenhang zwischen Ziel und Mittel herzustellen, ist ein *konkreter Anlass* für die Maßnahme etwa in Form von „irgendwelche[n] objektive[n] Anhaltspunkte[n] dafür[,] dass die betreffenden Fluggäste in terroristische Straftaten oder schwere Kriminalität verwickelt sein könnten“. *Vorausgesetzt*, die Kontrolle findet aus Anlass der Überschreitung einer EU-Außengrenze statt.¹¹⁰ Die angebotene Ratio dafür (also für den Verzicht auf einen konkreten Anlass) ist – vorsichtig gesagt – kryptisch:

„Die Übermittlung und Vorabüberprüfung der PNR-Daten von Fluggästen, die in die Union ein- oder aus der Union ausreisen, können nämlich angesichts der Art der Bedrohungen für die öffentliche Sicherheit, die sich aus terroristischen Straftaten und schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen zwischen der Union und Drittstaaten ergeben können, nicht auf einen bestimmten Kreis von Fluggästen beschränkt werden. Somit ist davon auszugehen, dass es den erforderlichen Zusammenhang zwischen diesen Daten und dem Ziel der Bekämpfung solcher strafbaren Handlungen gibt, so dass die PNR-Richtlinie nicht allein deshalb über das absolut Notwendige

106 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Überschrift vor Rn. 153. Hervorhebung hier.

107 Ibid., Rn. 157. Dazu, dass die Richtlinie diesen Konnex nicht schon von sich aus sicherstellen kann, s. a. a. O., Rn. 154 und bereits Rademacher, AöR 142 (2017), 366 (412 f.).

108 Als Bsp. für einen unmittelbaren Zusammenhang nennt EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 155 Anschläge mit Flugzeugen und auf Flugzeuge oder bestimmte Formen des Menschen- und Drogenhandels.

109 Ibid., Rn. 156. Auch Kostov, GSZ 2022, 267 (271) geht davon aus, dass die einschränkende Wirkung dieser Anforderung im Erg. eher „fraglich“ erscheint.

110 Zu der besonderen völkerrechtlich-diplomatischen Genese des Fluggastdatenabgleichs Kostov, GSZ 2022, 267 f.

hinausgeht, weil sie den Mitgliedstaaten vorschreibt, die PNR-Daten aller dieser Fluggäste systematisch zu übermitteln und vorab zu überprüfen.“¹¹¹

Anders sei es hingegen bei Flugbewegungen innerhalb der EU (EU-Flüge). Hier 53
fordern Artt. 7, 8 GRC nach Auffassung des Gerichtshofs Zurückhaltung: Lediglich
im Fall „einer als real und aktuell oder vorhersehbar einzustufenden terroristischen
Bedrohung“ dürfe ein Mitgliedstaat eine Auswertung *aller* Ein- und Ausreisen an-
ordnen.¹¹² Ansonsten dürfe nur selektiv ausgewertet werden, d. h. die Fluggastdaten-
kontrollen durch Muster müssten sich auf

„die Übermittlung und Verarbeitung der PNR-Daten von Flügen beschränken, die etwa be-
stimmte Flugverbindungen, bestimmte Reisemuster oder bestimmte Flughäfen betreffen, für die
es Anhaltspunkte gibt, die eine solche Anwendung rechtfertigen können.“¹¹³

Insoweit brauche es dann also doch eines mehr oder weniger zu konkretisierenden 54
Anlasses, um die Verarbeitung verhältnismäßig erscheinen zu lassen.¹¹⁴

cc. Insbesondere: direkte Aussagen zur Nutzbarkeit von KI-Systemen. Schließlich ist 55
der Fokus auf diejenigen Ausführungen zu lenken, die der EuGH, gemeinsam mit
Generalanwalt Giovanni Pitruzzella, zum Einsatz von künstlicher Intelligenz macht.
Beide haben erkannt, dass die Ermächtigung zum Einsatz von „Mustern“ in diese
Richtung genutzt werden kann, einschließlich der Nutzung maschineller Lernver-
fahren. Auf den ersten Blick erteilt der EuGH dem Einsatz spezifisch von *Machine*
Learning eine klare Absage:

„Zu den Kriterien, die die [Fluggastdaten]-Zentralstelle [für den Musterabgleich] heranziehen
kann, ist zunächst festzustellen, dass sie nach dem Wortlaut von Art. 6 Abs. 3 Buchst. b der
PNR-Richtlinie ‚im Voraus festgelegt‘ worden sein müssen. Wie der Generalanwalt in Nr. 228
seiner Schlussanträge^[115] ausgeführt hat, steht dieses Erfordernis der Heranziehung von Tech-

111 EuGH, Urt. v. 21.6.2022, Az. C-817/19 (Ligue des droits humains), Rn. 162.

112 Ibid., Rn. 171.

113 Ibid., Rn. 174.

114 Vgl. hierzu auch Kostov, GSZ 2022, 267 (271): „zwar nicht personenbezogene, jedoch lagebezogene Anhaltspunkte“ als Eingriffsschwelle gefordert.

115 s. GA Pitruzzella, Schlussanträge v. 27.1.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 228: Es gehe „sowohl aus dem Wortlaut von Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie als auch aus dem [darin] vorgesehenen System von Garantien, die mit der automatisierten Verarbeitung von PNR-Daten einhergehen, hervor, dass die Funktionsweise der Algorithmen, die im Rahmen der in Art. 6 Abs. 3 Buchst. b vorgesehenen Analyse verwendet werden, transparent und das Ergebnis ihrer Anwendung nachvollziehbar sein muss. Dieses Transparenzerfordernis bedeutet natürlich nicht, dass die verwendeten ‚Profile‘ veröffentlicht werden müssen. Es verlangt jedoch, dass die Erkennbarkeit der algorithmischen Entscheidungsfindung gewährleistet ist. Zum einen schließt das Erfordernis, wonach die Kriterien, anhand deren die Analyse zu erfolgen hat, ‚im Voraus festgelegt‘ werden müssen, nämlich aus, dass sich die Kriterien ohne menschlichen Eingriff ändern lassen, und steht daher der Nutzung von KI-Technologien, die auch als ‚machine learning‘ bezeichnet werden und einen höheren Detaillierungsgrad aufweisen können, aber selbst für Betreiber, die eine automatisierte Verarbeitung vorgenommen haben, schwer zu interpretieren sind, entgegen. [Anm. TR: Der GA vermischt hier die Frage des dynamisch-selbstlernenden Charakters und der Interpretationsfähigkeit von Machine-learning-Systemen bzw. ihres Outputs.] Zum anderen muss [...] gemäß der in Art. 6 Abs. 5 und 6 [...] beschriebenen Garantie, wonach jeder einzelne Treffer

nologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme („machine learning“) entgegen, die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können.“¹¹⁶

56 Dieser Passus klingt nach einer Absage an die Nutzung von *Machine-Learning*-Technologien insgesamt, doch ist die Position des EuGH *bei genauem Lesen*¹¹⁷ differenzierter:

- *Erstens* ist zu berücksichtigen, dass der EuGH – in dieser Nuance übrigens differenzierter als der Generalanwalt – nicht pauschal *Machine-Learning*-basierte Muster ausschließt, sondern dies durch den angefügten Relativsatz qualifiziert: „[...] die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien [...] sowie die Gewichtung der Kriterien ändern können.“ Der EuGH rekurriert also auf das, was hier als selbstlernendes System im engeren Sinn bezeichnet wurde,¹¹⁸ d. h. auf Systeme, die aufgrund dynamischer Feedback-Responsivität während der Nutzung sich derart weiterentwickeln können, dass eine „menschliche Einwirkung und Kontrolle“ durch Test und Evaluation – anders als bei einem erlernten und dann „eingefrorenen“ Muster¹¹⁹ – tatsächlich unmöglich oder doch zumindest erheblich erschwert ist.
- *Zweitens* ist damit auch klar, dass die *explorative* Nutzung von *Machine Learning*,¹²⁰ also die Suche nach bislang unbekannten relevanten Kriterien und Zusammenhängen von und für grenzüberschreitende Kriminalität und Terrorismus in den vorhandenen Trainingsdaten, zulässig bleibt.

57 Ich verstehe den EuGH an der genannten Stelle also nicht kategorisch im Sinn eines: *Machine-Learning*-trainierte Muster sind unbedingt verboten; sondern sie müssen bestimmten Bedingungen entsprechen (wie gesagt insbesondere: „eingefro-

bei der automatisierten Verarbeitung von PNR-Daten nach Maßgabe von Art. 6 Abs. 2 Buchst. a auf andere, nicht automatisierte Art individuell überprüft wird, nachvollzogen werden können, weshalb das Programm zu einem solchen Treffer gelangt ist, was sich u. a. dann nicht gewährleisten lässt, wenn Selbstlernsysteme verwendet werden. [Anm. TR: *explainable AI* ignoriert der GA.] Gleiches gilt für die Kontrolle der Rechtmäßigkeit dieser Analyse, auch in Bezug auf den nicht diskriminierenden Charakter der erzielten Ergebnisse, mit der der Datenschutzbeauftragte und die nationale Kontrollstelle [...] betraut sind. Die Transparenz der Funktionsweise der verwendeten Algorithmen ist auch eine notwendige Bedingung, um den Betroffenen die Ausübung ihrer Beschwerderechte und ihres Rechts auf effektiven gerichtlichen Rechtsschutz zu ermöglichen.“

116 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 194.

117 Plausibel daher leider die Befürchtung von Kostov, GSZ 2023, 14 (16), dass die missverständliche Ausdruckweise des EuGH „für Polemik und Fehlinterpretationen anfällig [ist], etwa [dahingehend,] dass der EuGH den Einsatz von maschinellern Lernen im Kontext der Fluggastdatenverarbeitung per se verboten habe.“ Unzutreffend – jedenfalls nach hier vertretener Auffassung – bspw. die Auslegung bei Eisele, NJW 2022, 2886 Rn. II: „Der EuGH teilt insoweit der Heranziehung von Technologien der Künstlichen Intelligenz in Form von selbstlernenden Systemen zur Aufstellung von Kriterien eine Absage.“

118 s. oben, → § 1 Rn. 18.

119 Zum Begriff → § 1 Rn. 18.

120 Dazu oben, → § 1 Rn. 20.

rene“ Muster sein), um nutzbar zu sein.¹²¹ In diese Richtung geht auch folgende Aussage des EuGH, die unmittelbar an die dem *Machine Learning* gewidmeten Ausführungen anschließt:

„Darüber hinaus brächte der Rückgriff auf solche Technologien die Gefahr mit sich, dass der nach den Bestimmungen der PNR-Richtlinie erforderlichen individuellen Überprüfung der Treffer und der Rechtmäßigkeitsprüfung die praktische Wirksamkeit genommen wird. Wie der Generalanwalt in Nr. 228 seiner Schlussanträge im Wesentlichen ausgeführt hat, kann es sich nämlich angesichts der für die Funktionsweise von Technologien der künstlichen Intelligenz kennzeichnenden mangelnden Nachvollziehbarkeit als unmöglich erweisen, den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat. Unter diesen Umständen könnte die Nutzung solcher Technologien den Betroffenen auch ihr in Art. 47 der Charta verankertes Recht auf einen wirksamen gerichtlichen Rechtsbehelf nehmen, [...] damit insbesondere gerügt werden kann, dass die erzielten Ergebnisse nicht frei von Diskriminierung seien.“¹²²

Der EuGH stellt damit über die Statik der Muster hinaus (= eingefrorene Muster) 58 Anforderungen an das, was als Erklärbarkeit oder Plausibilität der Muster bezeichnet werden kann (*explainable AI*¹²³), und er verlangt – wenn auch verklausuliert – Absicherungen gegen potentiell diskriminierende Effekte. Bei alledem erkennt der EuGH übrigens mit zu begrüßender Klarheit an, dass der Einsatz automatisierter Verfahren zu einer „erheblichen Zahl ‚falsch positiver‘ Ergebnisse“ führen wird, was freilich deren Nutzung nicht ausschließen soll, sondern ‚nur‘ dazu zwingt, strenge Anforderungen an die menschliche Überprüfung des Ergebnisses zu formulieren.¹²⁴ Interessant ist in diesem Zusammenhang, dass der EuGH nicht nur ausdrücklich die sozusagen ‚händische‘ Prüfung der Daten durch einen Menschen verlangt, sondern zusätzlich – wie sich aus der vorstehend abgedruckten Passage ergibt – verlangt, dass das automatisierte Ergebnis *selbst* auf für den *menschlichen* Prüfer nachvollziehbaren Kriterien beruht. Das ist bei genauem Hinsehen sogar eine doppelte Absicherung, die insbesondere dem *Automation Bias*¹²⁵ entgegenwirken kann und vermutlich (der EuGH nutzt diesen Begriff nicht) auch soll.

Umfassende Dokumentationspflichten runden das Sicherungsregime des EuGH mit 59 Blick auf die Nutzung von „Mustern“ wie auch deren „individuelle Überprüfung“ durch einen menschlichen Beamten ab:

„In diesem Kontext [= große Zahl an *False Positives*] haben die Mitgliedstaaten dafür zu sorgen, dass die [Fluggastdaten]-Zentralstelle [...] jede Verarbeitung von PNR-Daten, die im Rahmen der Vorabüberprüfung, einschließlich der individuellen Überprüfung auf nicht automatisierte

121 So auch das Verständnis des Urteils von *Kostov*, GSZ 2023, 14 (15 f.).

122 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 195.

123 Dazu oben, → § 1 Rn. 51 ff.

124 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 206 und ff.

125 s. dazu unten, bei → § 4 Rn. 77.

Art, vorgenommen wird, zum Zweck der Überprüfung ihrer Rechtmäßigkeit und zur Selbstkontrolle dokumentiert.“¹²⁶

3. ... im Steuerrecht

- 60 Ein weiteres Beispiel für potentiell KI-gestützte Überwachung liefert der 2016 neugefasste § 88 Abs. 5 AO.¹²⁷ Die Norm ermächtigt die Finanzbehörden im Rahmen der ihnen aufgetragenen Amtsermittlung (§ 88 Abs. 1 AO) zur ergänzenden Nutzung von sogenannten Risikomanagementsystemen

„zur Beurteilung der Notwendigkeit weiterer Ermittlungen und Prüfungen für eine gleichmäßige und gesetzmäßige Festsetzung von Steuern und Steuervergütungen sowie Anrechnung von Steuerabzugsbeträgen und Vorauszahlungen automationsgestützte Systeme [...] (Risikomanagementsysteme)“ (§ 88 Abs. 5 S. 1 AO).

- 61 Entsprechend der im Steuerrecht besonders weitreichenden Mitwirkungspflichten der Bürger (§ 90 AO) ist der Gegenstand der ‚Überwachung‘ vor allem das vom Bürger *selbst* vorgelegte Material, also seine Steuererklärung. Das Risikomanagementsystem dient dazu, diejenigen Steuererklärungen „herauszufiltern“, die einer *menschlichen* Prüfung bedürfen.¹²⁸ Alle nicht vom System ausgesteuerten Steuererklärungen können und sollen hingegen grundsätzlich unmittelbar Grundlage der nach § 155 Abs. 4 AO vorgesehenen vollautomatisierten Steuerfestsetzung werden und so die mit der Automatisierung des Steuerverfahrens verbundenen Effizienzerwartungen realisieren helfen.¹²⁹ Einer zwingenden Überprüfung durch menschliche Amtsträger, wie sie bei den zuvor genannten Anwendungsbeispielen entweder implizit oder ausdrücklich vorgesehen ist, soll es hier also gerade möglichst nicht geben.
- 62 Allerdings war sich der AO-Gesetzgeber der Defizite aktueller KI- oder auch nur algorithmenbasierter Erkennungstechnologien bewusst. In den Sätzen 3 bis 4 von § 88 Abs. 5 AO finden sich deshalb recht ausführliche Regelungen zur Sicherstellung bzw. Prüfung der Leistungsfähigkeit und der Einheitlichkeit/Gleichmäßigkeit der Prüfung und damit Besteuerung:

„³Das Risikomanagementsystem muss mindestens folgende Anforderungen erfüllen:

1. die Gewährleistung, dass durch Zufallsauswahl eine hinreichende Anzahl von Fällen zur umfassenden Prüfung durch Amtsträger ausgewählt wird,

126 EuGH, Urt. v. 21.6.2022, Az. C-817/19 (Ligue des droits humains), Rn. 207.

127 Dazu allg. *Braun Binder*, in: Wischmeyer/Rademacher (Hg.), *Regulating Artificial Intelligence*, 2020, S. 295 ff. m. w. N.

128 *Rätke*, in: Klein (Hg.), *Abgabenordnung*, 2024, § 88 Rn. 91 m. w. N.

129 Vgl. auch S. 2 von § 88 Abs. 5 AO: „Dabei [also beim Einsatz der Risikomanagementsysteme] soll auch der Grundsatz der Wirtschaftlichkeit der Verwaltung berücksichtigt werden.“ Das bedeutet nach *Rätke*, in: Klein (Hg.), *Abgabenordnung*, 2024, § 88 Rn. 95, dass „Bagatellfälle“ nicht zur menschlichen Prüfung vorgeschlagen werden sollten.

2. die Prüfung der als prüfungsbedürftig ausgesteuerten Sachverhalte durch Amtsträger,
3. die Gewährleistung, dass Amtsträger Fälle für eine umfassende Prüfung auswählen können,
4. die regelmäßige Überprüfung der Risikomanagementsysteme auf ihre Zielerfüllung.

⁴Einzelheiten der Risikomanagementsysteme dürfen nicht veröffentlicht werden, soweit dies die Gleichmäßigkeit und Gesetzmäßigkeit der Besteuerung gefährden könnte. ⁵Auf dem Gebiet der von den Landesfinanzbehörden im Auftrag des Bundes verwalteten Steuern legen die obersten Finanzbehörden der Länder die Einzelheiten der Risikomanagementsysteme zur Gewährleistung eines bundeseinheitlichen Vollzugs der Steuergesetze im Einvernehmen mit dem Bundesministerium der Finanzen fest.“

Einer wie auch immer gearteten Eingriffsschwelle bedarf es für den Einsatz des Risikomanagementsystems konsequenterweise nicht. Vielmehr können und sollen ja gerade alle Steuererklärungen entsprechend kontrolliert werden, sofern sich das System als zweckmäßig im Sinn eines guten ‚Ersatzes‘ für die bisher angeordnete menschliche Prüfung durch Mitarbeiter der Finanzämter erweist. 63

Wichtig ist, dass das Risikomanagement i. S. von § 88 Abs. 5 AO nach im steuerrechtlichen Schrifttum vertretener Ansicht bezüglich der Datenquellen *nicht* auf die Steuererklärung selbst beschränkt ist; andere Datenquellen wie „z. B. Daten von Kapitalanlegern aus Liechtenstein“ oder sonstiges „Kontrollmaterial“ sollen ebenfalls in die Musterung nach Auffälligkeiten und Anlässen für eine menschliche Überprüfung mit einbezogen werden dürfen.¹³⁰ Zu den Einzelheiten, insbesondere zur Leistungsfähigkeit des Systems, ist entsprechend der Geheimhaltungsanordnung in § 88 Abs. 5 S. 4 AO wenig bekannt.¹³¹ 64

4. ... im Finanzaufsichtsrecht

Ein in seinen Dimensionen ganz erstaunliches Überwachungsregime verlangen die EU-Geldwäscherichtlinien, von denen es mittlerweile die fünfte gibt.¹³² Umgesetzt sind sie in Deutschland im Geldwäschegesetz [GwG]. Dessen Anliegen ist es, die vom GwG „Verpflichteten“ – Kreditinstitute, Versicherungsunternehmen, Rechtsanwältinnen und Notare, Wirtschaftsprüfer und viele andere¹³³ – dafür zu ‚nutzen‘, 65

¹³⁰ Vgl. für die Bsp. *Rätke*, in: Klein (Hg.), Abgabenordnung, 2024, § 88 Rn. 95.

¹³¹ Zur im Schrifttum geäußerten Kritik an der Geheimhaltungspflicht (diese im Erg. allerdings zurückweisend) *Rätke*, in: Klein (Hg.), Abgabenordnung, 2024, § 88 Rn. 105 m. w. N.

¹³² s. nur RL (EU) 2018/843 v. 30.5.2018 – 5. Geldwäsche-Richtlinie. Hierzu nun ausf. *Leffe*, Automated Suspicion Algorithms, 2024, passim, zu den so langsam bewusster werdenden verfassungsrechtlichen Bedenken – jedenfalls wenn man die Rspr. des BVerfG undifferenziert anwendet – bes. S. 188 ff.; *Schindler*, Geldwäschegesetzgebung und Steuerrecht, 2021, ebenso passim, bes. S. 44 ff. Spezifisch zur Nutzung von KI bei der Geldwäsche-Überwachung auch *Bertrand/Maxwell/Vamparys*, 10.11.2020 (Onlinequelle).

¹³³ Die Zahl der Verpflichteten ist immens, mittlerweile sind sogar „Kunstlagerhalter“ grds. nach dem GwG verpflichtet, vgl. § 2 Abs. 1 GwG, konkret Nr. 16.

Verdachtsfälle von Geldwäsche und Terrorismusfinanzierung¹³⁴ durch ihre jeweiligen Auftraggeber möglichst effektiv *aufzuspüren* (§§ 10 ff. GwG), deren Umsetzung zumindest vorläufig *zu verhindern* (§ 46 GwG) und der Zentralstelle für Finanztransaktionenuntersuchungen¹³⁵ solche Verdachtsfälle „unverzüglich“¹³⁶ zu *melden* (§ 43 GwG).¹³⁷ Rechtstechnisch handelt es sich damit also um eine Überwachung von Privaten durch Private auf gesetzliche Anordnung.¹³⁸

- 66 Für uns konkret interessant sind zuvorderst die „Sorgfaltspflichten“, die den Verpflichteten auferlegt sind, um Verdachtsfälle zunächst einmal aufspüren zu können. Diese Sorgfaltspflichten umfassen zunächst mehr oder weniger selbstverständlich Anmutendes wie die Identifikation der Vertragspartner,¹³⁹ was insbesondere anonyme und reine Nummernkonten und Ähnliches verbietet. Zudem müssen die Verpflichteten auch Verfahren etablieren, um feststellen zu können, ob es sich bei einem Kunden um eine „politisch exponierte Person“ (eine sogenannte PEP¹⁴⁰) oder einen ihrer Familienangehörigen oder eine ihr „bekanntermaßen nahestehende Person“ handelt.¹⁴¹
- 67 Zum Ort für KI-Anwendungen werden die Sorgfaltspflichten mit § 10 Abs.1 Nr.5 GwG. Denn demnach zählt zur allgemeinen Sorgfalt, die jeder Verpflichtete im Umgang mit seinen Kunden zu gewährleisten hat,

„die *kontinuierliche Überwachung der Geschäftsbeziehung* einschließlich der Transaktionen, die in ihrem Verlauf durchgeführt werden, zur Sicherstellung, dass diese Transaktionen übereinstimmen

a) mit den beim Verpflichteten vorhandenen Dokumenten und Informationen über den Vertragspartner und gegebenenfalls über den wirtschaftlich Berechtigten, über deren Geschäftstätigkeit und Kundenprofil und,

134 Mit Geldwäsche meint das GwG Geldwäsche i. S. des § 261 StGB, vgl. den Verweis in § 1 Abs.1 GwG. Terrorismusfinanzierung definiert § 1 Abs.2 GwG, ebenfalls unter Verweis auf das StGB.

135 Die Zentralstelle wird in §§ 27 ff. GwG näher ausgestaltet und stellt eine als *Financial Intelligence Unit* firmierende Einheit im Zollkriminalamt dar; dazu *Da Rosa*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 27 Rn. 6 ff. Die Zentralstelle untersteht gleichwohl direkt der Aufsicht des BMF, die teilweise auf Rechtsaufsicht beschränkt ist, s. § 28 Abs. 2 GwG.

136 Zur Unverzüglichkeit sehr streng OLG Frankfurt, Beschl. v. 10.4.2018, Az. 2 Ss-Owi 1059/17 = NStZ 2020, 173 (174 ff.).

137 Bei den Meldungen handelt es sich nicht um Strafanzeigen i. S. v. § 158 Abs.1 StPO, sondern um Meldungen *sui generis*, s. *Da Rosa*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 43 Rn. 5 ff. Ein Verdacht i. S. v. § 43 GwG ist auch nicht mit einem – anspruchsvolleren – strafprozessualen Anfangsverdacht gleichzusetzen, s. BVerfG(K), Beschl. v. 31.1.2020, Az. 2 BvR 2992/14 = NJW 2020, 1351 Rn. 43. Zur Frage, ob eine Strafanzeige zur örtlich zuständigen Polizei oder Strafverfolgungsbehörde eine Meldung nach § 43 GwG ersetzen kann, s. *Da Rosa*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 43 Rn. 9 ff.

138 Zur Kritik an der Inpflichtnahme Privater *Brian/Pelz*, in: *Brian/Pelz* (Hg.), BeckOK GwG, Einführung, 21. Ed. 1.3.2025, Rn. 1 m. w. N.

139 Vgl. § 10 Abs.1 Nr.1 i. V. m. § 11 GwG.

140 Vgl. OLG Frankfurt, Beschl. v. 10.4.2018, Az. 2 Ss-Owi 1059/17 = NStZ 2020, 173 (174).

141 § 10 Abs.1 Nr. 4 GwG.

b) soweit erforderlich, mit den beim Verpflichteten vorhandenen Informationen über die Herkunft der Vermögenswerte“ (Hervorhebung hier).

Anlass für die „kontinuierliche Überwachung“ ist allein die Geschäftsbegründung an sich (§ 10 Abs. 3 Nr. 3 GwG).¹⁴² Auch soweit Verpflichtete im Fall bestimmter Kunden, Transaktionen oder Dienstleistungen nur die „vereinfachten Sorgfaltspflichten“ nach § 14 GwG beachten müssen (wenn bzw. weil die allfällige Risikoanalyse nach § 5 GwG ergibt, dass insoweit „nur ein geringes Risiko der Geldwäsche oder der Terrorismusfinanzierung besteht“) müssen

„[d]ie Verpflichteten in jedem Fall die Überprüfung von Transaktionen und die Überwachung von Geschäftsbeziehungen in einem Umfang sicherstellen, der es ihnen ermöglicht, ungewöhnliche oder verdächtige Transaktionen zu erkennen und zu melden.“ (§ 14 Abs. 2 S. 2 GwG)

Zumindest die kontinuierliche Überwachung von Geschäftsbeziehungen, die Massengeschäfte darstellen (wie etwa Banktransaktionen), ist ihrem Umfang nach immens und kann deswegen nicht menschlich, sondern nur noch im Wege der automatisierten Mustererkennung geleistet bzw. muss maschinell vorstrukturiert und -sortiert werden.¹⁴³ Zu beachten ist hier zusätzlich, dass der *Gegenstand* der Überwachung mit der Expansion des Geldwäschetatbestands in § 261 StGB in den vergangenen Jahren erheblich ausgedehnt wurde: Als Tatobjekt der Geldwäsche qualifiziert mittlerweile *jeder* Gegenstand, der aus einer *jeden* beliebigen rechtswidrigen Tat stammen kann.¹⁴⁴ Entsprechend bezeichnet auch *Europol* „Financial intelligence“ als „a clear example of big data“, „requiring computational analysis to reveal patterns, trends, and associations“.¹⁴⁵ Schon 2013/14 gingen immerhin 20 % der von *Europol* erfassten *Suspicious Transaction Reports* (STRs ~ Verdachtsmeldungen) auf die Rasterung nach *Suspicious Transaction Patterns* zurück.¹⁴⁶ In der einschlägigen Kommentarliteratur heißt es dann etwa, speziell mit Blick auf die Überwachungspflicht nach § 10 Abs. 1 Nr. 5 GwG:

„Aufgrund der sachlichen Verbindung zu den Überwachungspflichten nach § 6 GwG, § 25g Abs. 2 KWG empfiehlt sich eine Einbindung in die von den Verpflichteten vorzuhaltenden allgemeinen EDV-Überwachungsmaßnahmen, etwa in Form eines Abgleiches mit eingesetzten Parametern im Rahmen automatisierter Researchprogramme, mit den Typologiepapieren des Bundeskriminalamtes, etc.“¹⁴⁷

142 Klarstellend, dass sich die „kontinuierliche Überwachung“ natürlich nicht im Moment der Begründung erschöpft, sondern ihrem Wortlaut und Zweck nach auf die Dauer der gesamten Geschäftsbeziehung angelegt ist, *Krais*, in: Brian/Pelz (Hg.), BeckOK GwG, 21. Ed. 1.3.2025, § 10 Rn. 53.

143 Vgl. *Da Rosa*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 43 Rn. 29 f.; *Europol – Financial Intelligence Group*, 2017, S. 22, 37.

144 Die nach § 261 Abs. 1 S. 1 StGB a. F. vorgesehene Begrenzung der tauglichen Vortaten auf Verbrechen und einen (freilich umfangreichen) Katalog an bestimmten Vergehen, ist mit der zum 18.3.2021 in Kraft getretenen Neufassung der Norm aufgehoben geworden.

145 *Europol – Financial Intelligence Group*, 2017, S. 37.

146 *Ibid.*, 2017, S. 22.

147 *Figura*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 10 Rn. 30.

- 70 Freilich sind die (öffentlich bekannten!) maschinellen Muster, die derzeit genutzt werden, um das interne Geldwäschemonitoring der verpflichteten Stellen zu ermöglichen bzw. vorzustrukturieren, relativ simpel. Dazu zählen etwa auch einfache Bar-Umsatzschwellen im Fall von Kreditinstituten.¹⁴⁸ Daher dürfte eine manuelle menschliche Überprüfung von automatisch generierten Überwachungshinweisen unumgänglich sein,¹⁴⁹ bevor bzw. damit ein Verpflichteter der Pflicht nachkommen kann, tatsächlich *Verdachtsfälle* von Geldwäsche und Terrorismusfinanzierung an die Zentralstelle zu melden (definiert als „Tatsachen, die darauf hindeuten, dass [...]“, vgl. § 43 Abs. 1 GwG). Dabei finden sich in der Rechtsprechung zum GwG erstaunlich strenge Maßstäbe dafür, wann von einer Meldung *abgesehen* werden darf. Beispielfhaft:

„Eine in jeder Hinsicht gesetzeskonforme Herkunft des in dieser Höhe eingezahlten Bargeldes war für die Bank mit den ihr zur Verfügung stehenden Mitteln vorliegend | *nicht sicher* belegbar, so dass bereits bei den Bareinzahlungen, erst Recht aber bei der Überweisung unter Zugrundelegung der [verstärkten] Sorgfaltspflichten nach [§ 15 GWG n. F. – da die Kundin im konkreten Fall Ehefrau einer PEP war] die Voraussetzungen der Verdachtsmeldung gegeben waren.“¹⁵⁰

- 71 Wichtig ist schließlich in Bezug auf die *Folgen* der Verdachtsmeldung nach § 43 GwG, dass die Verpflichteten die zugrundeliegende Transaktion auch vorläufig zu *blockieren* haben, entweder bis die Zentralstelle oder eine Staatsanwaltschaft sie freigibt oder bis der dritte Werktag nach dem Tag der Meldung verstrichen ist, je nachdem, welches dieser beiden Ereignisse früher eintritt. Mit dieser heute in § 46 GwG näher geregelten Blockadepflicht unterstreicht der Gesetzgeber seine primär *präventive* Intention, die darauf aus ist, „Geldwäscheverdachtshandlungen möglichst noch vor der Durchführung unterbinden zu können.“¹⁵¹ Wir haben es also mit einem Arrangement zu tun, das bei genauem Hinsehen bereits auf der Schwelle zur hier sogenannten *Impossibility Structure* steht¹⁵² (dazu ausführlich → S. 126 ff.).

148 Vgl. die aufschlussreiche Darstellung in OLG Frankfurt, Beschl. v. 10.4.2018, Az. 2 Ss-Owi 1059/17 = NStZ 2020, 173 (174): „Bei Privatkunden ohne PEP-Status wurde bei ‚Hohen Bargeldeinzahlung/Fresh Money‘ erst bei einer Transaktion über 200.000,- € eine Meldung generiert. Zu Kunden mit PEP-Status wurde eine solche Meldung bereits bei Bargeldeinzahlungen in Höhe von 40.000,- € generiert.“

149 Vgl. i. d. S. auch *Da Rosa*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 43 Rn. 29: „Bloße Warnmeldungen durch ein eingesetztes technisches Monitoring-System (*systemgenerierte Regeltreffer*) sind dabei aufgrund der Breite und Fehleranfälligkeit der verwendeten Parameter und ‚Scores‘ ohne weitere Abklärung des Fachpersonals des Instituts noch nicht per se auffällig oder ungewöhnlich.“ Hervorhebung im Original.

150 So OLG Frankfurt, Beschl. v. 10.4.2018, Az. 2 Ss-Owi 1059/17 = NStZ 2020, 173 (174 f.). Positiv – und damit restriktiver – allerdings die Definition der h. M., vgl. dafür statt vieler *Da Rosa*, in: Herzog/Achtelik (Hg.), GwG, ⁴2020, § 43 Rn. 38 m. w. N.

151 OLG Frankfurt, Beschl. v. 10.4.2018, Az. 2 Ss-Owi 1059/17 = NStZ 2020, 173 Ls. 1, bezogen noch auf die Pflicht zur „unverzüglichen“ Meldung von Verdachtsfällen in § 11 GwG a. F. (heute § 43 GwG).

152 Zumindest theoretisch. Rein praktisch handelt es sich wohl v. a. um eine Verzögerungsstruktur, weil die zuständige *Financial Intelligence Unit* mit der Bearbeitung der unzähligen Verdachtsmeldungen völlig überfordert ist; s. für Nachw. und Zahlen *El-Ghazi/Jansen*, NZWiSt 2022, 465 (466 f.).

5. ... im Online-Kommunikationsrecht

Das abschließende, in seinen Dimensionen durchaus mit dem Geldwäschemonitoring vergleichbare Anwendungsbeispiel für *Intelligent Surveillance* finden wir im Medienaufsichtsrecht. Es handelt sich dabei um ein seit Februar 2021 zunächst von der Landesanstalt für Medien Nordrhein-Westfalen (LfM) erprobtes und sodann¹⁵³ von allen Bundesländern übernommenes System, das der Überwachung von Internetkommunikation dient. Das KIVI¹⁵⁴ genannte Programm stellt nach Auskunft der LfM ein „Werkzeug basierend auf künstlicher Intelligenz“ dar (wohl eine Art *Webcrawler* zur Bild-, Text-, Quellen- und Netzwerkanalyse¹⁵⁵), das „automatisch nach potenziellen Rechtsverstößen im Netz suchen und unseren Mitarbeiterinnen und Mitarbeitern vorarbeiten“ soll.¹⁵⁶ Das System wurde auf bestimmte „Verstoßkategorien“ trainiert, kann Feedback der Mitarbeiter der LfM verarbeiten (und scheint damit selbstlernend zu sein) und analysierte Stand 2022 „täglich 10.000 Seiten“ auf den Kanälen Twitter, YouTube, VKontakte und Telegram.¹⁵⁷ Nach Medienberichten war eine Ausweitung auf TikTok geplant.¹⁵⁸ Die LfM beschreibt als Ziel ihrer Bemühung eine „flächendeckend bessere Erkennbarkeit von Verstößen“. Es kann davon ausgegangen werden, dass die Überwachung sich bislang nur auf öffentlich zugängliche Kommunikationsforen¹⁵⁹ bezieht. Ansonsten läge ein Eingriff in Art. 10 Abs.1 GG¹⁶⁰ oder in das Computer-Grundrecht vor, wofür dann ersichtlich die Voraussetzungen fehlen würden (zur Rechtsgrundlage sogleich). Genutzt wird das Werkzeug von der LfM selbst, entwickelt wurde es privatwirtschaftlich.¹⁶¹

153 Vgl. *Sagatz*, Tagesspiegel Background Digitalisierung & KI v. 24.5.2022 (Onlinequelle).

154 Für „Künstliche Intelligenz und Vigilante“, vgl. *ibid.*

155 Vgl. die Beschreibung bei *Tieschky*, Süddeutsche Zeitung v. 24.8.2021 (Onlinequelle); *Sagatz*, Tagesspiegel Background Digitalisierung & KI v. 24.5.2022 (Onlinequelle).

156 Grundlegend zu solchen Technologien immer noch *Rückert*, ZStW 129 (2017), 302 ff., der allerdings gerade das „dauerhafte Monitoring des Internet“ ausklammert und nur knapp – wegen Vergleichbarkeit mit einer Vorratsdatenspeicherung (zweifelhaft) – als „äußerst bedenklich“ qualifiziert, s. a. a. O., S. 308.

157 Im Mai 2025 schreibt die LfM auf ihrer Website, dass ein „automatisierte[s] Monitoring von über 10.000 öffentlichen Social-Media-Profilen und Websites“ stattfindet.

158 *Tieschky*, Süddeutsche Zeitung v. 24.8.2021 (Onlinequelle).

159 Zum Begriff der *öffentlich zugänglichen* Daten speziell in Online-Kommunikationsräumen ausf. *Rückert*, ZStW 129 (2017), 302 (310 ff.).

160 Vgl. grundlegend BVerfG, Urt. v. 27.2.2008, Az. 1 BvR 370/07 = BVerfGE 120, 274 – Online-Durchsuchung, Rn. 292 f.: „Das heimliche Aufklären des Internet greift danach dann in Art. 10 Abs. 1 GG ein, wenn die [im konkreten Fall:] Verfassungsschutzbehörde Zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. So liegt es etwa, wenn ein mittels Keylogging erhobenes Passwort eingesetzt wird, um Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat zu erlangen. | Dagegen ist ein Eingriff in Art. 10 Abs. 1 GG zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt. Erst recht scheidet ein Eingriff in das Telekommunikationsgeheimnis aus, wenn die Behörde allgemein zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht Zugangsgesicherte Webseiten einsieht.“

161 *Tieschky*, Süddeutsche Zeitung v. 24.8.2021 (Onlinequelle).

- 73 Die LfM beschrieb die „Trefferquote des KI-Tools“ schon 2022 als hoch. Im Bereich Pornographie habe sie bei 94 % gelegen. Insgesamt habe man bei 20.000 Treffern binnen eines Jahres nach menschlicher Durchsicht 6.700 als *True Positives* eingestuft.¹⁶² Eine *Whitelist* vertrauenswürdiger Websites soll helfen, die Zahl der *False Positives* zu reduzieren.¹⁶³
- 74 Besonders stellt die Landesanstalt die Schutzmechanismen für die eigenen Mitarbeiter heraus: Denen melde das System die Treffer zur weiteren Kontrolle und gegebenenfalls Weiterleitung an die Strafverfolgungsbehörden, allerdings in einer Weise, die „möglicherweise verstörende Inhalte zunächst unscharf [darstelle] – was gerade bei Gewaltdarstellungen wie Tötungsvideos die psychische Belastung [der Mitarbeiter] mindern“ könne.¹⁶⁴ Zuständig für die Erst-Sichtung der Treffer sind zunächst juristische Laien (nach Medienberichten studentische Hilfskräfte), eine Zweitkontrolle vor Weiterleitung an die Strafverfolgungsbehörden erfolge durch Juristen der Anstalt.¹⁶⁵ Die LfM setzt dabei bewusst vorrangig auf Strafverfahren und nur hilfsweise auf Primärrechtsschutz (Slogan: „Viel mehr als nur Löschen“¹⁶⁶); eine Löschungsaufforderung an die jeweilige Plattform/den jeweiligen Telemediendienst ergehe nur, falls die Strafverfolgungsbehörden nicht in der Lage seien, einen Verantwortlichen zu ermitteln.¹⁶⁷
- 75 Eine Rechtsgrundlage für den Einsatz des Tools ist nicht ganz einfach zu finden. Erforderlich ist sie wohl jedenfalls, wenn und weil durch die umfassenden Auswertungstechniken unweigerlich personenbezogene Daten verarbeitet werden. Damit sind die Grundrechte auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG bzw. – im Anwendungsbereich des Unionsrechts – von Art. 8 GRC aktiviert.¹⁶⁸ Erwägenswert ist zwar, ob eine Form der vom Bundesverfassungsgericht grundsätzlich ohne Gesetzesvorbehalt zugelassenen „Online-Streife“ vorliegt. In der Literatur werden die Ausführungen des Gerichts speziell zu Art. 10 Abs. 1 GG ganz überwiegend dahingehend verallgemeinert,¹⁶⁹ dass auch ein Eingriff in das Recht auf

162 Meineck, netzpolitik.org v. 8.4.2022 (Onlinequelle).

163 Ibid.

164 Alle Zitate in diesem Abschnitt stammen von der Website *Landesanstalt für Medien NRW*, Viel mehr als nur löschen, www.medienanstalt-nrw.de/imagebroschuere/viel-mehr-als-nur-loeschen.html, besucht am 11.3.2022. Heute (Stand Mai 2025) nicht mehr abrufbar.

165 Tieschky, *Süddeutsche Zeitung* v. 24.8.2021 (Onlinequelle).

166 *Landesanstalt für Medien NRW*, Viel mehr als nur löschen, www.medienanstalt-nrw.de/imagebroschuere/viel-mehr-als-nur-loeschen.html, besucht am 11.3.2022.

167 Tieschky, *Süddeutsche Zeitung* v. 24.8.2021 (Onlinequelle).

168 So auch Golla, *DSRITB* 9 (2018), 871 f.

169 s., aufbauend auf BVerfG, Urt. v. 27.2.2008, Az. 1 BvR 370/07 = BVerfGE 120, 274 – Online-Durchsuchung, Rn. 293 zum Eingriff in Art. 10 Abs. 1 GG, für das Polizeirecht *Roggenkamp*, in: Specht/Mantz (Hg.), *Hdb. DatenschutzR*, 2019, § 21 Rn. 32 f. m. w. N.; strafprozessrechtl. Griesbaum, in: Hannich (Hg.), *Karlsruher Kommentar zur StPO*, 2019, § 161 Rn. 12a: „Die Online-Streife in allgemein zugänglichen Bereichen ohne gezielte Datenerhebung ist ohne weiteres zulässig. [Erst die] gezielte Suche nach Informationen über eine Person bedarf hingegen einer Rechtsgrundlage“.

informationelle Selbstbestimmung dann nicht vorliege, wenn eine Behörde ungezielt „allgemein zugängliche Inhalte erhebt, etwa indem sie offene Diskussionsforen oder nicht Zugangsgesicherte Webseiten einsieht“.¹⁷⁰ So dürften die Dinge hier, wie gesagt, liegen. Allerdings hat das Gericht damals (2008) sicherlich nicht bedacht, dass dieser Streifengang hochautomatisiert mit dem Ziel einer „flächendeckenden“ Überwachung des Kommunikationsverkehrs erfolgen könnte.¹⁷¹

Die LfM beruft sich in einer Antwort auf eine IFG-Anfrage von Netzpolitik.org auf die „Wahrnehmung [ihrer] öffentlich-rechtlichen Aufgaben i. S. von Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit dem Jugendmedienschutz-Staatsvertrag [JMStV] sowie dem Landesmediengesetz NRW“.¹⁷² Das könnte ein Verweis auf die Aufgabengeneralklausel in § 88 Abs. 1 LMG NRW sein, wonach

„[d]ie LfM [...] im Interesse der Allgemeinheit die nach den Vorschriften dieses Gesetzes und den aufgrund dieses Gesetzes erlassenen Rechtsvorschriften sowie die ihr nach dem Medienstaatsvertrag und anderen Rechtsvorschriften übertragenen erforderlichen Entscheidungen und Maßnahmen [trifft].“

Der Medienstaatsvertrag erscheint mit Blick auf die hier vorliegende Maßnahme allerdings wenig ergiebig, es findet sich lediglich in § 104 Abs. 1 S. 1 über die „Organisation“ der Medienaufsicht die sehr allgemeine Bestimmung, dass, „[s]oweit nichts anderes bestimmt ist, [...] die zuständige Landesmedienanstalt [siehe dafür § 106] die Einhaltung der Bestimmungen nach diesem Staatsvertrag [überprüft].“ Ähnlich offen formuliert ist § 14 Abs. 1 S. 1 JMStV, wonach „[d]ie zuständige Landesmedienanstalt die Einhaltung der für die Anbieter geltenden Bestimmungen nach diesem Staatsvertrag und der Bestimmungen der §§ 10a und 10b des Telemediengesetzes [überprüft].“ Nach § 20 JMStV kann sie *dann*, wenn sie einen Verstoß festgestellt hat, die „erforderlichen Maßnahmen gegenüber dem Anbieter“ treffen.

Ergiebiger ist das LMG NRW in § 88 Abs. 4: Danach ist die LfM „[i]m Rahmen ihrer Aufsichtsfunktion [...] kontinuierlich zur *Beobachtung* von Rundfunkprogrammen und Telemedienangeboten verpflichtet“ (Hervorhebung hier). Bei dem von der LfM eingesetzten „Tool“ handelt es sich definitiv um eine Beobachtung. Der Wortlaut von § 88 Abs. 4 LMG NRW „trägt“ daher grundsätzlich; und i. V. mit Art. 6 Abs. 1 lit. e DSGVO ist dies auch datenschutzrechtlich anknüpfungsfähig. Allerdings handelt es

170 BVerfG, Urt. v. 27.2.2008, Az. 1 BvR 370/07 = BVerfGE 120, 274 – Online-Durchsuchung Rn. 293.

171 Eine eigene Rechtsgrundlage fordert daher auch Rückert, ZStW 129 (2017), 302 (306, 314 f.). Zur Vertiefung auch sogleich, bei → § 2 Rn. 87.

172 Meineck, netzpolitik.org v. 25.5.2022 (Onlinequelle). Noch offener die Angaben auf der Website der LfM (Landesanstalt für Medien NRW, Viel mehr als nur löschen, www.medienanstalt-nrw.de/imagebroschue/viel-mehr-als-nur-loeschen.html, besucht am 11.3.2022): „Das Internet ist kein rechtsfreier Raum – und hier aktiv zu sein, ist ein zentraler gesetzlicher Auftrag der Landesanstalt für Medien NRW. Wir kontrollieren, verfolgen, bringen Verstöße zur Strafanzeige, arbeiten eng mit der Staatsanwaltschaft und Polizei zusammen.“ Heute (Mai 2025) nicht mehr aufrufbar.

sich zugleich um eine durch automatisierte Mittel massiv verstärkte Beobachtung, die darüber hinaus auch ausdrücklich auf eine flächendeckende Überwachung zu-
mindest bestimmter digitaler Kommunikationskanäle angelegt ist. Zweifel an der
hinreichenden Bestimmtheit der gegenwärtig verfügbaren Rechtsgrundlagen sind
daher angezeigt.¹⁷³

- 79 Die Lücke soll übrigens durch den Digitale-Medien-Staatsvertrag (DMStV) ge-
schlossen werden, dessen Entwurf wenige Tage vor Abschluss des Manuskripts
veröffentlicht wurde. § 109a MStV würde dann eine – umzusetzende – Ermächtigung
zur „Nutzung technischer Mittel in der Aufsicht“ vorsehen.¹⁷⁴ Eine Eingriffsschwe-
le/Anlassbindung sieht die neue Vorschrift nicht vor.

6. Zum Stand der Diskussion: die Rechtsprechung zum Einsatz neuer
Verdachtsgewinnungstechnologien in der dogmatischen Konsolidierungsphase

- 80 Unterstellen wir nun, dass die genannten Verfahren hinreichend gut funktionieren;
also derart wenige *False Positives* und *False Negatives* liefern, dass von einer gleicher-
maßen effektiven wie effizienten Überwachung auszugehen ist. Diese Überwachung
würde das ‚Ressourcenproblem‘ Mensch bei der Rechtsdurchsetzung zwar nicht lö-
sen; denn wie gesagt: Es geht ‚nur‘ um *Überwachung*, die definitionsgemäß mensche-
liche Folgehandlungen erfordert, um Effekte in der Realität zu erzielen. Eine derart
effektivisierte Überwachung würde aber immerhin zu einem erheblich gesteigerten
Durchsetzungs- und damit Befolungsdruck für Recht insgesamt führen.
- 81 Folgerichtig sind mit den hier sogenannten *Intelligent-Surveillance*-Technologien
vielfältige Ängste vor dem diktatorischen Überwachungsstaat verbunden. Sie erhal-
ten mit dem chinesischen *Social-Credit*-System ein reales Anschauungsobjekt. Wäh-
rend somit die *faktischen* Grenzen einer staatlichen, flächendeckenden Massenüber-
wachung schwächer werden, gewinnen *normative* Grenzziehungen umso größere
Bedeutung. Insbesondere das Bundesverfassungsgericht ist hier mittlerweile aktiv
geworden und hat in mehreren Urteilen elastische, aber gleichwohl starke Grenzen
für automatisierte staatliche Überwachung gezogen. Um dieses ‚Bollwerk‘ gegen den
Überwachungsstaat soll es hier zunächst gehen, seine grundsätzlichen Konturen
und zentralen Aussagen werden aufgezeigt (→ a.). Die noch weniger ausgebaute

173 A. A. Kühling, ZUM 2023, 566 (572): „Noch weniger problematisch (als der Einsatz von KI zu Detekti-
ons- und Löschungszwecken durch *Unternehmen*) ist der bisherige Einsatz von KI durch die Aufsichts-
behörden. Dabei besteht allgemein Einigkeit darin, dass die Verwaltung Zugriff auf KI-Technologien
benötigt, um ihre Aufgaben auch künftig zu bewältigen. Das gilt schon aus Effektivitäts- und Effizi-
enzgesichtspunkten und nicht zuletzt vor dem Hintergrund des Personalmangels. Diese allgemeinen
Erwägungen greifen auch für die Medienaufsicht insbesondere bei[m] Jugendschutz[e].“ Zum Bestimm-
theitsgrundsatz beim Einsatz automatisierter Überwachungstechnologien → § 2 Rn. 87 ff.

174 Der Entwurf ist hier abrufbar: <https://rundfunkkommission.rlp.de/digitale-medien-staatsvertrag>,
besucht am 23.6.2025.

Rechtsprechung des EuGH wird an passender Stelle mit in die Betrachtung einbezogen (→ b.). Es folgen sodann zwei kritische Anmerkungen zur Tragfähigkeit des verfassungsgerichtlichen Konzepts zur Regulierung von *Intelligent Surveillance*: Zwar liefert die gegenwärtige Dogmatik durchaus brauchbare Ergebnisse und ist praktisch handhabbar. Aber sowohl dogmatisch-konzeptionell (→ c.) wie auch grundrechtstheoretisch (→ d.) hat sie Lücken, die in einigen Fällen zu wenig überzeugenden argumentativen ‚Verrenkungen‘ führen. Die relativ ausführliche Darstellung und Kritik der Überwachungsdogmatiken in Deutschland und auf Unionsebene erscheint mir hier sinnvoll und geboten, weil darauf aufbauend dann im nächsten Abschnitt (→ II.) diejenigen Anwendungsszenarien von Technologien beschrieben und dogmatisch eingeordnet werden können, die dann eben doch *selbst* die physische Rechtsdurchsetzung leisten können. Hingewiesen sei vorneweg darauf, dass die hier folgenden Ausführungen insbesondere unter a., c. und d. eine ergänzte und aktualisierte Fassung eines bereits vorab veröffentlichten Beitrags von mir darstellen.¹⁷⁵

a. *Das Konzept des Bundesverfassungsgerichts: Rechtschaffenheitsvermutung und Anlassdogmatik.* Das Bundesverfassungsgericht hat sich mittlerweile in fünf großen Entscheidungen mit Technologien befasst, die *Intelligent Surveillance* oder – im klassischen Sprachgebrauch – automatisierte Verdachtsgewinnung leisten können, wie sie hier soeben illustriert wurde. Es handelt sich dabei um die Entscheidung zur Rasterfahndung (2006),¹⁷⁶ die beiden Entscheidungen zu automatisierten Kennzeichenkontrollen (2008¹⁷⁷ bzw. 2018¹⁷⁸) und um die noch recht jungen Entscheidungen zum sogenannten *Data Mining* (2020¹⁷⁹ bzw. 2023¹⁸⁰). Einige der speziell für den Einsatz von KI-Systemen relevanten Aussagen des Gerichts wurden schon im Rahmen der soeben präsentierten Fallstudien dargestellt, wo sie jeweils relevant waren. Hier geht es nun um eine grundsätzlichen ‚Linie‘ des Gerichts; die gibt es m. E. und sie hat sich mittlerweile konsolidiert:

Die gemeinsame Kernaussage der genannten Entscheidungen ist, dass die anlasslos-automatisierte Verdachtsgewinnung von Verfassungen wegen erheblichen Restriktionen unterliegt. Der rechtsdogmatische Aufhänger dafür ist das Recht auf informationelle Selbstbestimmung. In dieses Grundrecht greifen fast alle Verfahren der *Intelligent Surveillance* ein, wenn und weil sie personenbezogene Daten ‚mustern‘. Nach einer zwischenzeitlichen Rechtsprechungsänderung des Gerichts ist nunmehr

175 Vgl. Rademacher, in: Zimmer (Hg.), *Regulierung für Algorithmen und Künstliche Intelligenz*, 2021, S. 229 (252 ff.).

176 BVerfG, Beschl. v. 4.4.2006, Az. 1 BvR 518/02 = BVerfGE 115, 320 – Rasterfahndung.

177 BVerfG, Urt. v. 11.3.2008, Az. 1 BvR 2074/05 = BVerfGE 120, 378 – Kennzeichenkontrollen I.

178 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II. Für eine ausf. Anm. s. Bull, AöR 145 (2020), 291 ff.

179 BVerfG, Beschl. v. 10.11.2020, Az. 1 BvR 3214/15 = BVerfGE 156, 11 – Antiterrordateigesetz II.

180 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse.

jede Musterung als solche als Eingriff zu werten, unabhängig davon, ob sie als Trefferfall einer menschlichen Polizistin zur weiteren Verwendung weitergeleitet oder als Nicht-Treffer sofort wieder gelöscht wird.¹⁸¹ *Intelligent Surveillance* bedarf daher grundsätzlich (wie gesagt: sobald sie personenbezogene Daten verarbeitet) einer gesetzlichen Eingriffsermächtigung, ohne Bagatellvorbehalt;¹⁸² und sie muss sich der grundrechtlichen Bestimmtheits- und Verhältnismäßigkeitsprüfung stellen.

- 84 Bekanntlich ist bei Verallgemeinerungen aus einzelnen Entscheidungen besondere Vorsicht angezeigt, wenn sie aus der Verhältnismäßigkeitsprüfung hervorgehen sollen. Wenngleich das Verfassungsgericht mit seinem Maßstäbeteil gerade selbst auf Verallgemeinerungsfähigkeit abzielt,¹⁸³ bildet spezifisch der Grundsatz der Verhältnismäßigkeit einen stark vom Kontext der im jeweiligen Verfahren angegriffenen polizeilichen Maßnahmen geprägten Maßstab; für die damit aufs Engste verknüpften, herausgehobenen Bestimmtheitsanforderungen des Rechts auf informationelle Selbstbestimmung¹⁸⁴ gilt notwendigerweise dasselbe. Nichtsdestotrotz können aus den genannten Entscheidungen des Verfassungsgerichts m. E. vier allgemeine Anforderungen herausdestilliert werden, die für den Einsatz von *Intelligent Surveillance* zentral sind.¹⁸⁵ Sie lassen sich unter den folgenden vier Schlagworten zusammenfassen: *scharfe Bestimmtheitsanforderungen*, *Katalog-Gebot*, *„Quellen“-Schutz*, und *Eingriffsschwellen*.

- 85 *aa. Scharfe Bestimmtheitsanforderungen.* In allen Entscheidungen hat das Gericht eine erhöhte grundrechtliche Eingriffstiefe damit begründet, dass die Automatisierung gegenüber menschlicher Auswertung sowohl in der Breite (Zahl der kontrollierbaren Personen) wie auch in der Tiefe (individuelle Perspektive) eine deutlich erhöhte Effektivität der Überwachung bewirke.¹⁸⁶ Der Konformitätsdruck steigt durch den Einsatz von intelligenter Technologie gegenüber dem klassisch-menschli-

181 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 45. Zu der hochrelevanten Frage, ob die reine Umgebungserfassung, die z. B. von autonomen Fahrzeugen in großem Umfang durchgeführt werden muss, nach diesen und den europäischen datenschutzrechtlichen Maßstäben einen Eingriff darstellt, s. – überzeugend verneinend – K. Hofmann, ZD 2023, 18 ff.

182 Grundlegend immer noch BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83 u.a. = BVerfGE 65, 1 (45) – Volkszählungsurteil; angesichts der modernen „Informationstechnologie[n] eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten“ gäbe „es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr.“

183 Dazu Lepsius, in: Jestaedt et al. (Hg.), Das entgrenzte Gericht, 2011, S. 159 (168 ff.), ausf. auch zu den Problemen, die diese „Methode“ bereitet.

184 Vgl. Marsch/Rademacher, Die Verwaltung 54 (2021), 1 (21 ff.).

185 s. hierzu schon Rademacher, in: Zimmer (Hg.), Regulierung für Algorithmen und Künstliche Intelligenz, 2021, S. 229 (252 ff.).

186 Vgl. bes. deutlich BVerfG, Urt. v. 11.3.2008, Az. 1 BvR 2074/05 = BVerfGE 120, 378 (406 f.) – Kennzeichenkontrollen I; BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 98; ähnl. BVerfG, Beschl. v. 10.11.2020, Az. 1 BvR 3214/15 = BVerfGE 156, 11 – Antiterrordateigesetz II, Rn. 54; BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 78. Aus der Lit. Golla, DSRITB 9 (2018), 871 (880); Rückert, ZStW 129 (2017), 302 (326 ff.).

chen Überwachen daher potentiell massiv an. Hinzu kommt, dass die Verfahren als Verdachtsgewinnungsverfahren (bzw. Verdachtsergänzungsverfahren im Fall des *Data Mining*), um bestimmungsgemäß zu funktionieren, gerade solche Personen massenhaft betreffen müssen – d. h.: deren Daten verarbeiten müssen –, die keinen Anlass für die staatliche Maßnahme gegeben haben: „Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind *grundsätzlich* von höherer Eingriffsintensität als anlassbezogene.“¹⁸⁷ Das ist die sogenannte große Streubreite¹⁸⁸ der hier einschlägigen Überwachungsarrangements.

Die eingriffsabmildernden Rahmenbedingungen der Verfahren, insbesondere die *Spezifizität* der Überwachung¹⁸⁹ oder den Umstand der gegebenenfalls *öffentlichen* Datenerhebung (im Fall der Kennzeichenkontrollen) benennt das Gericht zwar in der Regel ausdrücklich als mildernde Faktoren.¹⁹⁰ Aber daraus folgt letztlich nie etwas Greifbares:¹⁹¹ Es bleibt bzw. blieb in den Entscheidungen angesichts des auf breite Wirkung angelegten Verdachtsgewinnungs- bzw. -ergänzungszwecks der Maßnahmen und/oder der besonderer Effektivität der Überwachung bei einem Eingriff von erheblichem Gewicht.

Daraus folgen nach überkommener Dogmatik zunächst erhöhte – nach Ansicht vieler: allerdings zu hohe – Anforderungen an die gebotene *Bestimmtheit* der gesetz-

187 So bes. deutlich BVerfG, Urt. v. 11.3.2008, Az. 1 BvR 2074/05 = BVerfGE 120, 378 (402) – Kennzeichenkontrollen I, Hervorhebung hier; s. für das *Data Mining* auch BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 77, für die konkret in Rede stehenden Normen sodann Rn. 126, 136, 140.

188 s. zur Definition bes. BVerfG, Beschl. v. 4.4.2006, Az. 1 BvR 518/02 = BVerfGE 115, 320 (354) – Rasterfahndung: „Grundrechtseingriffe, [sind] durch eine hohe Streubreite gekennzeichnet [wenn] zahlreiche Personen in den Wirkungsbereich der Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben [. . .].“ Zu Missverständnissen hinsichtlich des Begriffs s. die Nachw. bei Rademacher, JZ 2019, 702 (706 f.), dort bes. in Fn. 45.

189 Gemeint ist damit der Umstand, dass dann, wenn technologische Verdachtsgewinnungsmaßnahmen gut funktionieren, die Trefferfälle und somit die belastende Wirkung etwaiger *menschlicher* Kenntnisnahme und insb. von Folgemaßnahmen auf diejenigen Personen beschränkt wäre, bei denen tatsächlich ein Verdacht vorliegt. Das hat potentiell erhebliche Auswirkungen auf das Eingriffsgewicht, s. dazu ausf. Rademacher, AöR 142 (2017), 366 (396 ff.); schon zuvor Spiecker gen. Döhmman, K&R 2014, 549 (551). Ob sich Menschen weniger „überwacht fühlen, wenn sie davon ausgehen, dass ihre Daten rein maschinell ausgewertet werden[,] ist empirisch ungeklärt“, so Moll/F. Schneider, Monatsschrift für Kriminologie und Strafrechtsreform 104 (2021), 92 (11).

190 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 96.

191 Das übersieht m. E. Golla, DSRITB 9 (2018), 871 (874 f.), wenn er maßgeblich aus der Öffentlichkeit von verarbeiteten Daten auf eine geringe Intensität des Grundrechtseingriffs schließt. Auch die von ihm vorgeschlagene Verringerung der Eingriffsintensität dadurch, dass die „Datenverarbeitung auf Gruppen, Seiten oder Ereignisse anstelle von Individuen“ konzentriert werden könne bzw. müsse, überzeugt mich nicht, weil dadurch die Streubreite letztlich ja sogar vergrößert, die Spezifität der Treffermeldungen also verringert und das dadurch ausgelöste menschliche Interesse an den Inhalten potentiell häufiger fehlgeleitet würde; zur bes. belastenden Wirkung von zu vielen *False Positives*, die dann *menschlich* geprüft werden müssen, schon BVerfG, Beschl. v. 4.4.2006, Az. 1 BvR 518/02 = BVerfGE 115, 320 (356 f.) – Rasterfahndung, und Rademacher, AöR 142 (2017), 366 (394 ff.).

lichen Eingriffsermächtigungen.¹⁹² Wenn das Verfassungsgericht nicht grundsätzlich bereit ist, von seinen sehr hohen Bestimmtheitsanforderungen abzurücken, dann lässt es die bisherige Rechtsprechung jedenfalls unwahrscheinlich erscheinen, dass das Gericht automatisierte Auswertungen in Zukunft auf Basis allein der polizeilichen Datenverarbeitungsgeneralklauseln gestatten wird; jedenfalls solange, wie diese keine ausdrücklichen Verweise auf derartige Verfahren enthalten.

- 88 Am Beispiel: Die allgemeine Erlaubnis zur „Nutzung“ von Videoaufnahmen zum Zweck der Gefahrenerkennung im Bundespolizeigesetz¹⁹³ dürfte – eben wegen der Unschärfe des Begriffs *Nutzung* – den Anforderungen des sicherheitsrechtlichen, streng verstandenen Bestimmtheitsgebots schwerlich genügen, um darauf auch automatisierte Auswertungen stützen zu können.¹⁹⁴ Auch die Ermächtigung der Landesanstalt für Medien zur „Beobachtung“ von Telemediendiensten erscheint mir vor dem Hintergrund der Streubreite der Maßnahme zu wenig bestimmt, um den Maßstäben des Verfassungsgerichts aktuell zu genügen.¹⁹⁵
- 89 Hinzu tritt – immer noch in Sachen Bestimmtheit –, dass das Bundesverfassungsgericht in *Kennzeichenkontrollen II* besonders deutlich gemacht hat, dass automatisierte Kontrollen ebenfalls *gesetzlich* hinreichend bestimmte „übergreifende Anforderungen“ erfüllen müssen, zu denen das Gericht „Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle“ zählt.¹⁹⁶ KI-basierte Verfahren stellen insoweit besondere Herausforderungen dar, etwa in Sachen statistischer Diskriminierungsschutz¹⁹⁷ oder der Notwendigkeit, den Einsatz zu protokollieren und Feedback-Daten zum fortlaufenden Training zu generieren, zu speichern und zu nutzen.

192 Mit Nachdruck nun BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 112-122.

193 § 29 Abs. 1 S. 1 i. V. m. § 27 Abs. 1 BPolG; dazu Näheres oben, bei → § 2 Rn. 21.

194 So wohl auch, allg. zur Frage der Tragfähigkeit der Generalklauseln, der *BfDI* v. 23.3.2022 (Onlinequelle), S. 7 ff.; möglich sei aber immerhin, ohne gesonderte Rechtsgrundlage, der Einsatz von Texterkennungsssoftware. Grundlegend a. A. *Trute/S. Kuhlmann*, GSZ 2021, 103 (109 f.): „Einer [neuen, über die Datenverarbeitungsgeneralklauseln hinausgehenden Rechtsgrundlage] wird es aber jedenfalls dann nicht bedürfen, wenn die Polizei [...] ausschließlich auf ohnehin zum Zwecke der Gefahrenabwehr bereits erhobene Daten zurückgreift. Insofern tritt die durch ein PP-System anhand dieser Daten generierte Prognose lediglich an die Stelle, die ansonsten ein Polizeibeamter anhand eben dieser Erkenntnisse getroffen hätte.“ Allerdings scheint mir die Argumentation unvollständig: Bei auf Breitenwirkung angelegten Verdachtsgewinnungsverfahren (= Verdachtslosigkeit + Streubreite) tritt die automatisierte Prognose ja gerade nicht an die Stelle einer *ohnehin* von einem menschlichen Polizeibeamten getroffenen Prognose, weil es so viele Polizeibeamte schlicht nicht gibt. Der Sinn und Zweck der hier behandelten Verfahren ist es ja gerade, das *Fehlen* menschlicher Ressourcen durch die Leistungsfähigkeit der Technologie zu kompensieren. Der Überwachungsdruck wird damit in der Summe größer.

195 A. A. aber wohl *Kühling*, ZUM 2023, 566 (572), s. schon in → § 2 Fn. 173. Großzügiger auch *Golla*, DSRITB 9 (2018), 871 (876 f.), der aber wenigstens „diffuse Anhaltspunkte“ für eine situationsgebundene Schadensprognose fordert, damit die polizeilichen Generalklauseln Verdachtsgewinnungseingriffe im offenen Online-Verkehr tragen können sollen.

196 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 101, 153.

197 s. oben, → § 1 Rn. 30 ff.

Solange die Polizei- und andere einschlägige Gesetze keine *verfahrensrechtlichen Automatisierungsgeneralklauseln* enthalten, die entsprechende Anforderungen übergreifend als Rahmenvorgaben enthalten,¹⁹⁸ muss dem Bestimmtheitsgebot für automatisierte Verdachtsgewinnung wohl in jedem einzelnen Ermächtigungsfall Rechnung getragen werden.

bb. Nur für gewichtige Schutzgüter (Katalog-Gebot). Zweitens erlauben die verfassungsgerichtlichen Entscheidungen in der Zusammenschau die Schlussfolgerung, dass der mit *Intelligent Surveillance* verbundene Verdachtsgewinnungs-/ergänzungseingriff eben wegen des „grundsätzlich erheblichen Gewichts“ nur dann als verhältnismäßig anerkannt wird, wenn er *zum Schutz von hinreichend gewichtigen Rechtsgütern* erfolgt (konkretisierte Zweckbestimmung). Der jeweils zuständige Gesetzgeber ist demnach gefordert, einen Katalog an mehr oder weniger spezifizierten Schutzgütern zu erstellen. Es kommen dafür konkrete Straftaten in Frage, aber auch – allgemeiner – die klassische Liste aus Leib, Leben, Freiheit und Bestand des Bundes und der Länder. Vor diesem Hintergrund hat sich etwa an der baden-württembergischen Regelung des § 44 Abs. 4 S. 2 PolG BW Kritik entzündet, weil darin die intelligente Videoüberwachung ganz allgemein zum „Erkennen solcher Verhaltensmuster“ erlaubt wird, „die auf die Begehung [irgend]einer Straftat hindeuten“.¹⁹⁹

cc. Grundsätzlich unzulässige Datenquellen, Verbot der Rundumüberwachung. Umgekehrt sind bestimmte *Datenquellen* und *Datentypen* tabu bzw. nur unter nochmals verschärften Anforderungen auswert- bzw. nutzbar: beispielsweise Daten aus der eigenen Wohnung bzw. solche, die den Kernbereich privater Lebensgestaltung betreffen; oder solche, die die Datenanalyse auf in Art. 3 Abs. 3 GG genannte Kriterien stützen könnten; das hat das Bundesverfassungsgericht in seinem Urteil *Automatisierte Datenanalyse* besonders betont.²⁰⁰

Ebenfalls unzulässig sollen nach ständiger Rechtsprechung „additive Überwachungsmaßnahmen“ sein für den Fall, dass sie derart umfassend ausfallen, dass räumlich und zeitlich eine „Rundumüberwachung“ vorliegt.²⁰¹ Das Bundesverfassungsgericht will durch dieses aus der Menschenwürde abgeleitete und daher unbedingte (!) Verbot vermeiden, dass der Staat die seit dem *Volkszählungsurteil*

198 Zur Möglichkeit, im Stil von Generalklauseln auf „Vorschriften des allgemeinen oder des polizeilichen Datenschutzrechts“ zurückgreifen zu können, eher zurückhaltend BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 114.

199 s. oben, → § 2 Rn. 22. Zur Kritik *Wendt*, ZD-Aktuell 2018, 6122.

200 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 77 (für Art. 3 Abs. 3 GG), Rn. 59, 81 (für aus Online-Durchsuchungen und Wohnraum-Überwachung erlangte Daten); vgl. hierzu auch schon *Rademacher*, AöR 142 (2017), 366 (406, 408 f.).

201 Hierzu ausf. und aktuell *Benz*, Additive Überwachungsmaßnahmen, 2024, S. 266 ff.

immer wieder beschworenen „Persönlichkeitsprofile“²⁰² erstellen kann.²⁰³ Die Hürden für das Verbot liegen damit freilich hoch: Neben einer Datenerhebung und -verknüpfung aus vielen verschiedenen Quellen müssten die Daten auch für erhebliche Zeit²⁰⁴ gespeichert werden, damit wirklich aussagekräftige Persönlichkeitsbilder erstellt werden können. Diese Rechtsprechungslinie taucht daher bislang nur im Rahmen von sehr langfristigen oder Dauerüberwachungsmaßnahmen auf sowie bei der Online-Durchsuchung;²⁰⁵ sie dürfte im Fall der *per definitionem* gezielten *Intelligent Surveillance*²⁰⁶ also nicht greifen (jedenfalls wenn keine anschließende Datenspeicherung auf Vorrat erfolgt).

- 93 Im Hinterkopf behalten sollte man zudem, dass gar nicht mehr so sicher erscheint, dass das Gericht Persönlichkeitsprofile (oder gar die *bloße Möglichkeit* ihrer Erstellung) weiterhin *per se* als Würdeverstoß werten will; jedenfalls hat es diese ohnehin problematische Figur²⁰⁷ kürzlich stark relativiert: In der Entscheidung *Automatisierte Datenanalyse* hat das Gericht genau gesehen, dass *Data Mining* in der Tat die *faktische* Möglichkeit schafft, „mit einem Klick umfassende Profile von Personen, Gruppen und Milieus zu erstellen“. Das führte das Gericht aber gerade nicht zur Annahme der Verfassungswidrigkeit *per se*, sondern ‚nur‘ dazu, dass eben „dieselben verfassungsrechtlichen Anforderungen“ gelten sollen, „wie sie auch an andere tief in die Privatsphäre eingreifende Überwachungsmaßnahmen der Gefahrenabwehrbehörden gestellt werden.“²⁰⁸ Dass die Behörden Persönlichkeitsprofile erstellen *können*, ist damit offenbar nicht mehr das Problem; sie *dürfen* es freilich nicht tun, wenn und weil ein Persönlichkeitsprofil so, wie das Bundesverfassungsgericht es seit dem Volkszählungsurteil als grundrechtsstaatliches *No-Go* beschrieben hat, wohl nie eine erforderliche staatliche Maßnahme darstellen wird.
- 94 *dd. Konkretisierte Eingriffsschwellen (hier sog. Anlassdogmatik).* Die vierte Anforderung stellt schließlich die wohl größte Hürde auf: Das Gebot der Verhältnismäßigkeit – so das Bundesverfassungsgericht in *Kennzeichenkontrollen II* in besonderer Deutlichkeit und Allgemeinheit – verlange, dass staatliche Überwachungsmaßnah-

202 Grundl. zu dieser Angst des Gerichts BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83 u.a. = BVerfGE 65, 1 – Volkszählungsurteil, S. 42 f. Die Definition von „Persönlichkeitsbild“ fällt notorisch schwer. Einen neueren, bedenkenswerten Vorschlag liefern Bode, Verdeckte strafprozessuale Ermittlungsmaßnahmen, 2012, S. 458, und, darauf auf- und ausbauend, Benz, Additive Überwachungsmaßnahmen, 2024, S. 269 f., 291.

203 Zuletzt wieder diskutiert, aber im Erg. wie stets verneint, von BVerfG, Beschl. v. 1.12.2020, Az. 2 BvR 916/11, 2 BvR 636/12 = BVerfGE 156, 63 – Elektronische Fußfessel, Rn. 250 f.

204 Für deren Bestimmung kommt es auf den Einzelfall an, s. Benz, Additive Überwachungsmaßnahmen, 2024, S. 273 f.

205 Für eine Rspr.-Übersicht aktuell Benz, Additive Überwachungsmaßnahmen, 2024, S. 265 f.

206 Dazu oben, → § 2 Rn. 9.

207 Zur grds. Kritik Hahne, Die datenschutzrechtliche Zulässigkeit der Registermodernisierung, Manuskript 2024, Abschnitt E.II.5.e und ff. Zur Krit. auch schon die Nachw. in → Fn. 75 (Einleitung).

208 Beide Zitate von BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 150 f.

men an einen konkreten „Anlass“ gebunden sein müssten, der die staatliche Datenverarbeitung vorhersehbar mache und begrenze und deshalb auch gesetzlich präzise normiert werden müsse (sogenannte Eingriffsschwelle).²⁰⁹

Das Gebot der Anlassbindung von staatlichen Kontrollen stützt das Bundesverfassungsgericht einerseits auf die aus der Rechtsprechung mittlerweile gut bekannten *Chilling Effects*, die das „Gefühl eines ständigen Überwachtwerdens“ auf die freie und *erlaubte*²¹⁰ Grundrechtsausübung der Bürger haben könnte²¹¹ – und die es folglich grundsätzlich zu *vermeiden* gelte. Das Gericht gibt damit einem in der Bevölkerung latent vorhandenen Misstrauen gegen den Staat juristischen Raum, dass sich dessen einzelne Repräsentanten ihrerseits womöglich (oder häufig? Oder zu oft? Oder nicht oft genug?) nicht an das geltende Recht halten oder der Staat insgesamt ins Totalitäre ableiten könnte.²¹²

In der Entscheidung *Kennzeichenkontrollen II* tritt zu dieser empirisch-soziologischen Begründung der Anlassdogmatik des Gerichts noch ein zweiter, stärker normativ bzw. wohl sogar rechtsphilosophisch fundierter Strang hinzu, der auch eine Reaktion auf die mitunter heftige Kritik an der Figur der *Chilling Effects*²¹³ sein könnte. So gehöre „[z]ur Freiheitlichkeit des Gemeinwesens“,

209 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 93; dazu auch *Löffelmann*, GSZ 2023, 92 ff., krit. dazu, dass Anlass und Rechtsgut vom BVerfG „als zwei verschiedene Größen“ behandelt werden (a. a. O., S. 94).

210 Dass das Gericht *Chilling Effects* auf *erlaubte* Verhaltensweisen befürchtet, lässt sich v. a. daran ablesen, dass es in den hier näher untersuchten Entscheidungen auf die Gefahr des *Missbrauchs* der verarbeiteten Daten durch die staatlichen Stellen hinweist, vgl. etwa BVerfG, Beschl. v. 10.11.2020, Az. 1 BvR 3214/15 = BVerfGE 156, II – Antiterrordateigesetz II, Rn. 96.

211 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51, 98; BVerfG, Urt. v. 11.3.2008, Az. 1 BvR 2074/05 = BVerfGE 120, 378 (402) – Kennzeichenkontrollen I; BVerfG, Beschl. v. 4.4.2006, Az. 1 BvR 518/02 = BVerfGE 115, 320 (355) – Rasterfahndung. In BVerfG, Beschl. v. 10.11.2020, Az. 1 BvR 3214/15 = BVerfGE 156, II – Antiterrordateigesetz II taucht das Gefühl des Überwachtwerdens zwar nicht auf, doch recurriert das BVerfG hier auf die „Gefahr des Missbrauchs“ bei der Verarbeitung von Daten, s. a. a. O., Rn. 96.

212 Hierzu schon *Rademacher*, AöR 142 (2017), 366 (400 f.).

213 BVerfG, Urt. v. 2.3.2010, Az. 1 BvR 256/08 = BVerfGE 125, 260 – Vorratsdatenspeicherung, Sondervotum Eichberger, S. 380 f.; harsch *Dreier*, in: ders. (Hg.), GG Bd. I, ³2013 Art. 2 I Rn. 87 m. w. N. Monographisch *Staben*, Der Abschreckungseffekt auf die Grundrechtsausübung, 2016, passim. Eine Übersicht über aktuelle empirische Forschungen liefern *Moll/F. Schneider*, Monatsschrift für Kriminologie und Strafrechtsreform 104 (2021), 92 ff., bes. S. 6 f. Es gebe sich „verdichtende Hinweise“ auf *Chilling Effects* in der Bevölkerung, ausgelöst durch staatliche Überwachung, aber weitere Forschung sei notwendig. Ähnl. *Büscher* et al., DuD 2023, 503 ff., dort S. 509 f. zum nachbarwissenschaftlichen Forschungsstand. Gegen die Kritik am BVerfG grundlegend *Eifert*, in: Herdegen et al. (Hg.), VerfassungsR-HdB, 2021, § 18 Rn. 119, der das Gefühl des Überwachtwerdens bzw. dessen Vermeidung als von vornherein „*normativen* Bezugspunkt einer mit dem grundgesetzlichen Freiheitsverständnis unvereinbaren anlasslosen oder vollständigen Überwachung“ versteht (Hervorhebung hier). Hiergegen lässt sich freilich einwenden, dass das Gericht das dann auch so sagen müsse, denn: „Bei allem Respekt vor der Rechtsprechung des Verfassungsgerichts muss auch festgestellt werden, dass diese sich nicht als Stimulans für neues Vertrauen erwiesen, sondern im Gegenteil das Misstrauen eines Teils der kritischen Öffentlichkeit noch verstärkt hat. Man kann irrationaler Angst eben nicht dadurch ihre Wirkung nehmen, dass man sie für berechtigt erklärt“; so treffend *Bull*, AöR 145 (2020), 291 (307).

„dass sich Bürgerinnen und Bürger fortbewegen können, ohne dabei *beliebig* staatlich registriert zu werden, *hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen* und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein (vgl. BVerfGE 107, 299 [328]; BVerfGE 115, 320 [354 f.]; BVerfGE 120, 378 [402]; BVerfGE 122, 342 [370 f.]; BVerfGE 125, 260 [335]).“²¹⁴

- 97 Das freiheitliche Gemeinwesen, so kann man diesen Gedanken noch etwas weiter entfalten, basiere folglich auf einem grundsätzlichen *Vertrauen*,²¹⁵ dass seine Mitglieder auch ohne ständige Kontrolle ihrer Rechtschaffenheit eben das *sind*:²¹⁶ wenigstens so *hinreichend* rechtschaffen, dass das soziale Gefüge, dessen Ermöglichung und Erhaltung staatliche Gewalt als Vorbedingung *sowohl* von Freiheit *wie* von Gemeinwesen verpflichtet ist, ohne präventiv-staatliche Intervention Bestand hat (hier sogenannte Rechtschaffenheitsvermutung).²¹⁷ Der damit gewährte Vertrauensvorschuss ist natürlich widerleglich. Aber dafür muss der Bürger *etwas tun* (= im Sinn der überkommenen polizeirechtlichen Störerdogmatik irgendeinen Anlass liefern bzw. – als Nicht-Störer – in einem Anlass verfangen sein²¹⁸), *nicht* umgekehrt.
- 98 Unklar bleibt aus dieser Perspektive, die eine Verhaltenstransparenz *der Bürger* gegenüber Staat und Gesellschaft ganz bewusst ausschließt, ob der Bestand des sozialen Gefüges dadurch gewährleistet wird, dass die Bürger sich eben im Großen und Ganzen an das Recht halten. Oder ob Ursache hierfür ist, dass zwar rechtliche „Verhaltensabweichung die Regel und nicht die Ausnahme ist“²¹⁹ dass aber die Regeleinhaltung in großem Umfang schlicht nicht erforderlich ist, um ein geordnetes Gemeinwesen zu erhalten. *Thomas Wischmeyer* etwa neigt Letzterem zu und folgert

214 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51. Hervorhebung hier. Notabene: Die in der Klammer genannten Rechtsprechungsnachweise enthalten zwar die Argumentation mit den *Chilling Effects*, nicht jedoch die grundsätzliche Rechtfertigungsfreiheit des Bürgers. Diese erscheint m. W. in BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51 tatsächlich erstmals.

215 Auf die Rolle von Vertrauen zur Erhaltung von Devianz gehe ich ausf. ab → S. 422 ein.

216 Vgl. in d. S. etwa *Rostalski*, GA 166 (2019), 481 (487 f.); a. A. *Kube*, AöR 146 (2021), 494 (506): „[D]ie Rechtsbefolgung durch die Bürger ist zwar staatlich erwünscht und erwartet, aber nicht Gegenstand staatlichen Vertrauens. Denn es bleibt – im Rahmen der zur Verfügung stehenden Ressourcen – stets die Option der zwangsweisen Rechtsdurchsetzung.“ Mit Blick auf die referierte Rspr. des BVerfG, die die Beschränkung staatlicher Überwachung und damit verbundener Rechtsdurchsetzungsmöglichkeiten gerade von der Ressourcenfrage abgekoppelt hat, scheint mir diese Einschätzung nicht mehr ganz zutreffend. Umgekehrt geht aber auch *Rostalski* sehr weit, wenn sie (scheinbar?) argumentiert, dass es einem freiheitlichen Gemeinwesen entspreche, auf eine „*bloße* Ansprache [des] Bürgers durch Vernunftgründe“ zu setzen (Hervorhebung hier).

217 s. hierfür schon *Rademacher*, in: Zimmer (Hg.), *Regulierung für Algorithmen und K Künstliche Intelligenz*, 2021, S. 229 (252 und ff.).

218 *Bäcker*, *Kriminalpräventionsrecht*, 2015, S. 272 f., weist zutreffend nach, dass nur im ersten Fall klassische Zurechnungsgesichtspunkte tragen; im zweiten Fall geht es hingegen richtigerweise um „Aufopferungserwägungen“.

219 So eine Einschätzung von *Wischmeyer*, in: Baumgärtel/Hoppen (Hg.), *Informationstechnik und Recht*, 2021, S. 9 (22), anschließend an die soziologischen Thesen von *Heinrich Popitz*: „Kein System sozialer Normen könnte einer perfekten Verhaltenstransparenz ausgesetzt werden, ohne sich zu Tode zu blamieren. Eine Gesellschaft, die jede Verhaltensabweichung aufdeckte, würde zugleich die Geltung ihrer Normen ruinieren.“

daraus, dass erst das bewusste Nicht-Wissen(-Wollen) um die *tatsächliche* Rechtsbefolgung das Recht vor weitreichenden „Glaubwürdigkeitsverlusten“²²⁰ und zugleich die zur Durchsetzung bzw. zur Behebung von Rechtsverstößen berufenen offiziellen Stellen vor einer Überlastung schütze.²²¹

Zwangsläufig unterbelichtet bleiben in dieser Dogmatik die *Chilling Effects* fehlender 99
Rechtsdurchsetzung. Diesen Aspekt macht *Hans Peter Bull* stark, wenn er darauf hinweist, dass die

„Schwächung der Sicherheitsorgane im Namen der Freiheit [...] auch zu schwächerem Schutz der Bürger vor Straftätern, zugespißt also zu größeren Entfaltungsmöglichkeiten für Störer und Rechtsbrecher führen [kann], und darüber hinaus allenfalls [zu] mehr Freiheit, sich selbst zu schützen, also eine Teilprivatisierung der Staatsaufgabe Sicherheit.“²²²

Dass diese Sorge keine theoretische ist, zeigen zwei Beispiele, einmal aus dem analo- 100
gen, einmal aus dem digitalen Bereich. Hier ist zum einen die mittlerweile vielfach beobachtete Wirkung von *Hate Speech* im Rahmen von Onlinekommunikation zu nennen. Sie kann zum Phänomen des *Silencing* führen: Diskursteilnehmer, die ruhiger und interessiert an einer sachlichen Debatte sind, werden durch rechtswidrige oder grenzwertige Äußerungen anderer Teilnehmer aus dem Diskurs gedrängt.²²³ Davon sind besonders, aber nicht nur, vulnerable Gruppen betroffen.

Als krasses Beispiel aus dem analogen Bereich kann eine Entscheidung des Verwal- 101
tungsgerichts Ansbach dienen, zur verneinten Rechtmäßigkeit einer Überwachungs-kamera in einem Fitnessstudio:

„Zwar mag die Videoüberwachung für manche eher ein willkommenes Gefühl der Sicherheit als einen unangenehmen Anpassungsdruck auslösen. Die Risiken der Aufklärbarkeit eines Diebstahls oder Übergriffs liegen aber primär im Verantwortungsbereich der Trainierenden selbst [...]. Wer das Smartphone nicht in den Spind sperrt, ist sich regelmäßig der so erleichterten Möglichkeit eines Diebstahls im Trainingsraum im Fitnessstudio bewusst. Auch dass die Aufklärung von Straftaten in einem verhältnismäßig engen Raum unter vielen sich fremden Menschen erschwert ist, dürfte den Trainierenden als Teil des allgemeinen Lebensrisikos be-

220 Es erscheint mir allerdings zweifelhaft, ob man dem auf der verfassungsrechtlichen Judikatur aufbauen-
den Datenschutzrecht deshalb wirklich die *rechtlich relevante* Funktion zuschreiben darf, den Staat vor
der Blamage zu schützen, dass der Umfang der tatsächlichen Devianz ‚ans Licht‘ kommen könnte; in
diese Richtung *Wismeyer*, in: Baumgärtel/Hoppen (Hg.), *Informationstechnik und Recht*, 2021, S. 9
(21 f.): „Praktisch wird eine Überlastung des Sanktionensystems insbesondere dadurch verhindert, dass
den Trägern und Trägerinnen des Sanktionensystems großflächig Verhaltensinformationen vorenthalten
werden. Damit sind wir wieder beim Datenschutzrecht, dem auf diese Weise eine weitere, bisher kaum
beachtete Funktion für die Stabilisierung des Rechtssystems zukommt.“

221 *Wismeyer*, in: Baumgärtel/Hoppen (Hg.), *Informationstechnik und Recht*, 2021, S. 9 (21).

222 *Bull*, AöR 145 (2020), 291 (311).

223 Vgl. *Morath*, Tagesspiegel Background Digitalisierung & KI v. 8.7.2021: „Die Folge ist, dass sich immer
mehr Menschen aus Netz-Diskursen zurückziehen. Eine Umfrage des Marktforschungsinstituts ‚For-
schungsgruppe g/d/p‘ im Juni 2020 ergab, dass 42 Prozent aller Befragten aufgrund von Hassreden
vorsichtiger eigene Beiträge im Internet formulieren oder darauf verzichten, etwas zu posten.“

wusst sein. Es liegt in der Hand der Trainierenden selbst, dieses Risiko bei Bedarf zu minimieren, indem beispielsweise Trainingsgeräte in der Nähe der Empfangstheke gewählt werden oder zu zweit oder zu einer ‚risikoärmeren‘ Uhrzeit trainiert wird.“²²⁴

- 102 Es dürfte sich hierbei zwar um einen außergewöhnlich üblen Fall des *Victim Blaming* handeln, der hoffentlich Seltenheitswert hat. Aber er zeigt wie unter dem Brennglas die von *Bull* beschriebene Privatisierungsgefahr.
- 103 *ee. Konsequenzen der Rechtsprechung für den Einsatz von KI zu Überwachungszwecken.* Was sind nun die *dogmatischen* Konsequenzen dieser doppelt²²⁵ fundierten *grundsätzlichen* Freiheit vor Überwachung? Unstreitig dürfte aus der Anlassbindung zunächst folgen, dass Überwachungsmaßnahmen nicht „flächendeckend“ eingesetzt werden dürfen;²²⁶ und es bietet die Anlassbindung bzw. das dahinterstehende Verbot einer „ständigen“ Überwachung zudem einen Ansatzpunkt für die ebenfalls quantitativ arbeitende sogenannte Überwachungsgesamtrechnung, für die mittlerweile Vorschläge vorliegen, wie sie operationalisiert werden könnte.²²⁷
- 104 Jenseits dessen wird das Bild diffuser: Es gibt Autoren, die das Gebot der Anlassbindung so konsequent durchsetzen wollen, dass *automatisierte* Verdachtsgewinnung grundsätzlich nur noch aus Anlass einer konkreten Gefahr im engen Sinn zulässig sein soll.²²⁸ Die Technologie bzw. ihr Einsatz wäre damit weitgehend unzulässig und unsinnig. Eine Verdachtsgewinnungsmaßnahme ergibt wenig Sinn, wenn eine konkrete oder doch eine zumindest konkretisierte Gefahr²²⁹ bereits mit anderen, *nicht* automatisierten Mitteln erkannt wäre. *Intelligent Surveillance* würde dann lediglich einer Verdachtsbestätigung oder (immerhin) einer weiteren Eingrenzung eines bereits mehr oder weniger stark verdächtigen Personenkreises bzw. Raumes/Umfeldes dienen können (Stichwort *Data Mining*).
- 105 Das Bundesverfassungsgericht selbst ist hier jedenfalls heute²³⁰ deutlich weniger restriktiv. Dahinter mag Realismus stecken: Es hat besonders deutlich in *Kennzeichenkontrollen II* (an)erkannt, dass es eine Vielzahl an Verdachtsgewinnungsarran-

224 VG Ansbach, Urt. v. 23.2.2022, Az. AN 14 K 20.00083 = BeckRS 2022, 7643 – Keine Videoüberwachung im Fitnessstudio, Rn. 41. Hier geht es natürlich um privates Datenschutzrecht. Allerdings wird dem Sicherheitsrecht (sdatenschutzrecht) mittlerweile häufig *allgemein* maßstabsbildende Kraft zugewiesen; gegen diesen Kurzschluss *Marsch/Rademacher*, Die Verwaltung 54 (2021), 1 (12 ff.).

225 D. h. durch die Figur der *Chilling Effects* sowie die hier sog. Rechtschaffenheitsvermutung.

226 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 100.

227 *Poscher/Kilchling/Landerer*, Überwachungsbarometer für Deutschland, Januar 2022; für die Grundzüge immer noch *Roßnagel*, NJW 2010, 1238 ff. Vertiefend, im Erg. gut begründet skeptisch zur Überwachungsgesamtrechnung *Busche*, AöR 149 (2024), 207 (250 ff.).

228 So bes. prononciert *Sommerer*, Personenbezogenes Predictive Policing, 2020, S. 167 f.

229 Zum feinen Unterschied zwischen konkreter und konkretisierter Gefahr in → § 2 Fn. 75.

230 In BVerfG, Beschl. v. 4.4.2006, Az. 1 BvR 518/02 = BVerfGE 115, 320 – Rasterfahndung hat das Gericht als Eingriffsschwelle noch eine konkrete (oder zumindest konkretisierte) Gefahr gefordert, was ihm erhebliche Kritik eingebracht hat, s. bspw. *Schoch*, in: ders. (Hg.), Besonderes Verwaltungsrecht, 2018, S. 12, Rn. 81 ff., 775; krit. auch *Trute*, Die Verwaltung 42 (2009), 85 (98 ff.).

gements gibt – analoge und in vielen Bereichen auch schon jetzt digitale – die dem Bürger eben doch eine mehr oder weniger spezifische Rechenschaftslegung abverlangen, *ohne* dass zuvor ein polizei- oder strafrechtlicher Anlass in Form der klassischen konkreten Gefahr, des Gefahrenverdachts, der typisierten Gefahrenlage z. B. an bekannten Schwerepunkttorten bzw. eines Straftatverdachts vorliegen würde. Erinnert sei nur an die beschriebenen Arrangements aus dem Geldwäschegesetz²³¹ und der Abgabenordnung.²³²

Das Verfassungsgericht sah sich daher offensichtlich gedrängt, den Grundsatz der 106
Anlassbindung staatlicher Überwachung zugleich mit breiten *Ausnahmen* zu versehen, d. h. Maßstäbe für die Zulässigkeit von vom Gericht auch ausdrücklich sogenannten „anlasslosen Kontrollen“ spezifisch im Zusammenhang mit automatisierten Verdachtsgewinnungstechnologien aufzustellen.²³³ Sie sind nach der Würdigung in *Kennzeichenkontrollen II* zulässig, wenn sie „an ein gefährliches oder risikobehaftetes Tun beziehungsweise an die Beherrschung besonderer Gefahrenquellen anknüpfen“; schon darin könne „ein dem Verhältnismäßigkeitsgrundsatz genügender Grund liegen.“²³⁴ Als Beispiel für eine solche Gefahrenquelle nennt das Gericht den Betrieb eines Kfz:

„Die Rechtfertigung für [automatisierte Kennzeichen-]Kontrollen [etwa zur Durchsetzung der Versicherungspflicht²³⁵ oder auch von Geschwindigkeitsbegrenzungen²³⁶] kann dort bereits an der besonderen Verantwortung der Betroffenen gegenüber der Allgemeinheit anknüpfen und bedarf deshalb eines darüberhinausgehenden Anlasses grundsätzlich nicht.“²³⁷

Ausdrücklich erlaubt bleiben auch Kontrollen, die „anlasslos stichprobenhaft“ im 107
Straßenverkehr oder, ebenfalls anlasslos, „in weiten Bereichen etwa des Umwelt- oder Wirtschaftsverwaltungsrechts“ durchgeführt werden.²³⁸ Insoweit ist allerdings nicht ganz klar, ob das Gericht damit auch *automatisiert*-anlasslose Kontrollen gemeint und damit grundsätzlich erlaubt hat.

231 s. oben, → § 2 Rn. 65 ff. Wobei insoweit natürlich zu beachten ist, dass das GWG teils unionsrechtlich vorgegeben ist. Für eine gründliche Prüfung am – nach dortiger Auffassung gleichwohl anwendbaren – Grundgesetz *Schindler*, Geldwäschegesetzgebung und Steuerrecht, 2021, S. 308 ff., bes. S. 339 ff., mit bes. Fokus auf das Steuerrecht.

232 s. oben, → § 2 Rn. 60 ff.

233 Es sei nur nebenbei erwähnt, dass das BVerfG hier sprachlich unglücklich operiert: Rn. 93 von BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, beginnt apodiktisch: „Verhältnismäßig ist eine Ermächtigung zu einer Kontrolle nur [sic!], wenn hierfür ein Anlass bestimmt ist [...]“. Das passt nicht zur nächsten Rn. 94: „Anlasslose Kontrollen sind damit nicht generell ausgeschlossen.“

234 s. BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 94.

235 So ausdr. *ibid.*

236 So, unter Rückgriff auf die Maßstäbe in BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 94, das OVG Lüneburg, Beschl. v. 3.7.2019, Az. 12 MC 93/19 = NJW 2019, 2951 – Section Control, Rn. 24 ff.

237 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 94.

238 *Ibid.*

- 108 ff. *Sonderfall Data Mining innerhalb einer Behörde*. Eine Besonderheit dürfte zudem für das *Data Mining* gelten, wo das Bundesverfassungsgericht die Anlassbindung für Übermittlungen zwischen Behörden und vor allem bei Zweckänderungen *verschärft* hat, für Auswertungen innerhalb „derselben Behörde“ und innerhalb der „ursprünglichen Aufgabenbestimmung“²³⁹ allerdings stark *gelockert* hat.²⁴⁰ Hier, also im zuletzt genannten Fall, gilt nun, dass vernetzte Auswertungen zulässig sind, wenn entweder

„[i.] die einbeziehbaren Daten gesetzlich nach Art und Umfang in einer Weise reduziert und die möglichen Methoden der automatisierten Analyse oder Auswertung von vornherein so eingeschränkt [sind], dass eine auf die Befugnis gestützte Maßnahme *nicht zu tieferen Einsichten in die persönliche Lebensgestaltung der Betroffenen führt* [das BVerfG sieht diese Möglichkeit als Proprium des sogenannten *Predictive Policing* an²⁴¹] *als sie die Behörde, wenngleich aufwendiger und langsamer, auch ohne automatisierte Anwendung realistisch erlangen könnte*, oder [wenn] die Befugnis [ii.] von vornherein nur darauf [zielt], gefährliche oder gefährdete Orte zu identifizieren, ohne dabei personenbezogene Informationen zu generieren[.]“²⁴²

- 109 Dann, so das Gericht weiter, könne

„sogar die Einhaltung des Grundsatzes der Zweckbindung ausreichen, um die weitere Verarbeitung der Daten in einer automatisierten Anwendung [zur Verwendung als Spurenansatz²⁴³] zu rechtfertigen [...]. Eine gänzlich anlasslose automatisierte Auswertung personenbezogener Daten durch Polizeibehörden zur vorbeugenden Bekämpfung von Straftaten wäre zwar verfassungsrechtlich unzulässig; die Einhaltung des verfassungsrechtlichen Grundsatzes der Zweckbindung [der ursprünglichen Datenerhebung] sichert dann jedoch, dass es einen Eingriffsanlass gibt.“²⁴⁴

- 110 Lassen wir einmal die Befugnis zur Ermittlung gefährdeter Räume (= soeben, ii.) als – zu begrüßende – Erleichterung der Polizeiarbeit in einer organisatorisch-strategischen, d. h. nicht unmittelbar personenbezogenen Dimension einmal beiseite; interessanter ist die Justierung, die das Gericht unter i. vorgenommen hat. Etwas weniger umständlich formuliert besagt dieser Passus nichts anderes, als dass sich eine *Behörde mit ihren Datenbanken als Wissenseinheit* begreifen darf, die sich –

239 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 57.

240 Die Neujustierung kann schon auf das BKAG-Urteil des BVerfG zurückgeführt werden, s. *Schwabenbauer*, in: Bäcker/Denninger/Graulich (Hg.), PolR-HdB, 72021, Abschnitt G Rn. 27 ff.; a. a. O., Rn. 30, auch zu den schwierigen Folgefragen, die diese fein differenzierende Rspr. bewirkt (z. B.: was ist „dieselbe Behörde?“).

241 Vgl. für dieses anspruchsvolle Begriffsverständnis von *Predictive Policing* BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 98, 100, sowie schon → § 2 Rn. 42, dort 2. Bulletpoint.

242 BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 108 (Hervorhebung hier).

243 Ibid., Rn. 58.

244 Ibid., Rn. 108; lies dazu Rn. 57 f. (der Binnenverweis a. a. O. in Rn. 108 ist leider ungenau). Für Daten, die aus Wohnraumüberwachungen und Online-Durchsuchungen stammen, gelten allerdings *per se* verschärfte Anforderungen, s. a. a. O., Rn. 59.

plakativ formuliert – nicht unwissender stellen muss, als sie *auch unter Einsatz technischer Hilfsmittel* ist.²⁴⁵

Beispielhaft: Liegen in zwei verschiedenen Datenbanken derselben Behörde Datensätze, die kombiniert einen polizeilich-*menschlich* unproblematisch erkennbaren Hinweis auf eine Gefahr darstellen, dann muss die Behörde nicht auf diese Erkenntnis verzichten, nur weil ihre *menschlich*-personellen Kapazitäten nicht ausreichen, um diesen Hinweis rechtzeitig zu erkennen. Sie darf dafür automatisierte Datenauswertung einsetzen, und dann sogar unter Zuhilfenahme selbstlernender Systeme,²⁴⁶ vorausgesetzt eben, diese leisten keine höhere „Einsichts“-Tiefe als auch durch eine menschliche Auswertung, die mit der entsprechenden personellen bzw. zeitlichen Ausstattung möglich wäre. Damit ist in kluger Weise eine Option eröffnet, Behörden vor dem oft unfairen Vorwurf zu bewahren, sie hätten Ereignis X verhindern müssen, weil ‚der Staat‘ – allerdings eben in bewusst fragmentierter Form – schon über alle Informationen verfügt hätte, um dies zu tun. Freilich: Diese fast voraussetzungslose Befugnis zur Datenauswertung ist nachdrücklich auf dieselbe Behörde im selben Aufgabenkreis beschränkt. Von der alten Idee der Verwaltung bzw. des Staats *insgesamt* als (Wissens-)Einheit sind wir also nach wie vor weit entfernt.

b. Konvergenzen in der Rechtsprechung des EuGH. Es wird sich herausstellen, soviel sei hier vorweggenommen, dass die Anlassdogmatik des Bundesverfassungsgerichts eine dogmatisch brauchbare, aber an den Rändern und vor allem theoretisch nicht überzeugende Behelfskonstruktion ist (zu meiner Kritik sogleich, → S. 106 ff.). Bevor aber die Kernaussagen der Anlassdogmatik kritisch hinterfragt werden, soll an dieser Stelle ein kurzer Blick auf die unionsrechtliche (Grundrechts-)Rechtsprechung geworfen werden.²⁴⁷ Diese wird voraussichtlich auch im sicherheitsrechtlichen Bereich immer wichtiger werden, wenn und weil der unionsrechtlich determinierte Bereich auch hier weiter anwächst, in dem die Grundrechte des deutschen Grundgesetzes folglich grundsätzlich keine Anwendung mehr finden können.²⁴⁸

Dafür ist das Urteil des EuGH zum Fluggastdatenabgleich wiederaufzugreifen, das vorhin schon ausführlicher geschildert wurde.²⁴⁹ Legt man dieses Urteil und die soeben in groben Strichen gezeichnete Dogmatik des Bundesverfassungsgerichts nebeneinander, fällt zunächst auf, dass sich mittlerweile beide Gerichte zum maschinellen Lernen als aktuell dominanter Form von KI geäußert,²⁵⁰ dass beide das

245 Vgl. hierzu auch Rademacher, AöR 142 (2017), 366 (406 f., 410).

246 Zum im Urteil *Automatisierte Datenanalyse* nicht ganz klaren Begriff → § 2 Rn. 38 ff.

247 Vgl. zur „Vision“ der EU für die Regulierung von Big Data und KI im polizeilichen Einsatz auch Bäuerle, CR 2023, 64 ff.

248 Vgl. für die Unterscheidung von unionsrechtlich determinierten und nicht-determinierten Feldern nationalen Handelns nun aufschlussreich EuGH, Urt. v. 19.II.2019, Rs. C-609/17 (TSN), Rn. 41 ff.

249 s. oben, → § 2 Rn. 48 ff.

250 s. oben ausf., → § 2 Rn. 56 ff.

aber angesichts der fortgeschrittenen Debatte in erstaunlich unklarer Form getan haben.²⁵¹ Noch bemerkenswerter erscheint mir allerdings, dass bzw. in welcher Entscheidung sich das Bundesverfassungsgericht noch *nicht* zum Einsatz von maschinell trainierter Mustererkennung geäußert hatte: nämlich gerade in *Kennzeichenkontrollen II*, obwohl doch Kennzeichenlesegeräte (= Bilderkennung) einen Standardanwendungsfall eben von maschinellern Lernen darstellen. Wie das Urteil zur *Automatisierten Datenanalyse* zeigt, heißt das freilich nicht, dass das Bundesverfassungsgericht hierdurch wirklich permissiver sein wollte als sein unionales Pendant – permissiver in dem Sinn, dass es keine vergleichbar restriktiv-skeptischen Hürden für den Technologieeinsatz formuliert hätte. Hier ist eine vorsichtige Kontextualisierung sowohl der Urteile wie auch – für uns noch wichtiger – der konstitutionellen Determinanten anhand der konkreten Anwendungsszenarien der KI angezeigt:

- 114 In *Kennzeichenkontrollen II* stand eine Technologie zur Diskussion, deren Treffer von einem menschlichen Beamten anhand eines einfachen Sichtabgleichs von Klar-Bild (= Fotoaufnahme) und Fahndungsdatei verifiziert oder falsifiziert werden können. Anders als bei einer solchen simplen Bildprüfung ist es bei den unter Umständen viel komplexeren Mustern, die zum Fluggastdatenabgleich oder eben bei der *Automatisierten Datenanalyse* genutzt werden könnten,²⁵² deutlich weniger gesichert, dass ein flüchtiger menschlicher Blick ausreichen würde, um einen falsch-positiven Treffer auch als solchen zu erkennen, bevor gegebenenfalls belastende Folgemaßnahmen eingeleitet würden. Vor diesem Hintergrund erscheint es daher viel naheliegender und jedenfalls nachvollziehbarer, dass EuGH und Generalanwalt schon an die *Plausibilität* der Muster höhere Anforderungen stellen und damit das Thema der *explainable AI* auf die Agenda rufen,²⁵³ welches in *Kennzeichenkontrollen II* keine Rolle gespielt hat.
- 115 Diese kleine Gegenüberstellung mahnt zur Vorsicht dabei, technologiebezogene verfassungsrechtliche Aussagen und Vorgaben, die hinsichtlich eines spezifischen Anwendungsszenarios sinnvoll oder gar geboten erscheinen können, undifferenziert auf alle Anwendungen derselben oder gar nur ähnlicher Technologien (gar: *Machine Learning* pauschal) zu übertragen.
- 116 Daneben gibt es weitere, für uns relevante Konvergenzen in der Rechtsprechung: Zum einen ist das die Forderung des EuGH, den Einsatz automatisierter Verdachtsgewinnungstechnologien aus Gründen der Verhältnismäßigkeit auf den Schutz be-

251 s. oben, → § 2 Rn. 38 ff./bzw. → § 2 Rn. 56 ff.

252 Dazu, dass das derzeit offenbar kaum der Fall ist, → § 2 Rn. 47.

253 Wenn auch nicht ausdr., vgl. dazu die Überlegungen oben, → § 2 Rn. 57 f.

stimmter hochrangiger Rechtsgüter zu beschränken und „gewöhnliche Kriminalität“²⁵⁴ nicht einfach als ‚Beifang‘ mitzunehmen.²⁵⁵

Hinsichtlich der grundsätzlichen Anlassbindung ist der EuGH zurückhaltender als 117
das Bundesverfassungsgericht, aber ‚Spuren‘ davon finden sich auch bei ihm: So ist zwar der bloße Grenzübertritt an der EU-*Außengrenze* Anlass genug, um alle ein- und ausreisenden Passagiere zu ‚mustern‘, was natürlich darauf hinausläuft, auf einen wirklichen Anlass, der diesen Namen verdient, zu verzichten. Aber auch insoweit stellt der EuGH unter dem Gesichtspunkt des „Zusammenhangs zwischen den [Fluggast-]Daten und den Zielsetzungen der Verarbeitung dieser Daten“ eine freilich niedrige Hürde auf, indem er fordert, dass die Handlungen, nach denen gefahndet wird, einen wenigstens „mittelbaren Zusammenhang mit der Beförderung der Fluggäste aufweisen“ müssen.²⁵⁶ Der EuGH geht also nicht so weit wie das Bundesverfassungsgericht, das für eine anlasslose Kontrolle ein „gefährliches“ Verhalten fordert, das eine besondere Verantwortung des Handelnden gegenüber der Allgemeinheit begründen kann (z. B. Autofahren),²⁵⁷ aber er verlangt doch immerhin, dass Verdachtsgewinnung und Bürgerhandeln eine gewisse innere *Konnexität* aufweisen,²⁵⁸ die es dem Bürger plausibel machen kann, warum er nun genau bei diesem Handeln einer gesteigerten Aufmerksamkeit staatlicher Stellen ausgesetzt ist, er also ein Mehr an Rechenschaftslegung schuldet als Personen, die diese Verhalten nicht an den Tag legen.

Was demgegenüber die Inner-EU-Flüge angeht, ist der EuGH deutlich stärker auf 118
der Linie des Bundesverfassungsgerichts. Im Grunde fordert auch das Unionsgericht hier einen vergleichsweise konkreten Anlass für die Maßnahme: entweder „hinreichend konkrete Umstände für die Annahme“, dass ein Mitgliedstaat „mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist“, um *alle* ein- und ausreisenden Fluggäste zu mustern;²⁵⁹ oder, wenn es nicht um Terror mit seinen potentiell „die tragenden Strukturen eines Landes“ destabilisierenden Wirkungen geht,²⁶⁰ muss es gehen um „bestimmte Flugverbindungen, bestimmte Reisemuster oder bestimmte Flughäfen [...], für die es Anhaltspunkte gibt, die eine solche [Verdachtsgewinnungsmaßnahme] rechtfertigen können“,²⁶¹ um eben zumindest diese bestimmten Strecken und Flughäfen zu mustern.

254 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 148.

255 Dazu soeben, → § 2 Rn. 49.

256 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 156.

257 s. soeben, → § 2 Rn. 106.

258 Vgl. dazu auch schon *Rademacher*, AöR 142 (2017), 366 (404 ff.).

259 EuGH, Urt. v. 21.6.2022, Rs. C-817/19 (Ligue des droits humains), Rn. 171.

260 Ibid., Rn. 170.

261 Ibid., Rn. 174.

- 119 Die Maßstäbe, die in der Rechtsprechung des EuGH und der des Bundesverfassungsgerichts angelegt sind, sind daher zwar nicht identisch, für unsere, auf grundsätzliche Fragen bezogenen Überlegungen aber doch hinreichend konvergent, so dass im Folgenden vor allem wieder die – nicht nur zahlenmäßig – ausgereifere Rechtsprechung des Bundesverfassungsgerichts in den Fokus genommen werden kann und soll; zumal sie solange dominant bleiben wird, solange im Sicherheitsrecht die nicht unional determinierten Bereiche noch überwiegen.
- 120 *c. Dogmatisch-konzeptionelle Zweifel: Wäre es konzeptionell stimmiger, nach Gründen statt nach Anlässen zu fragen?* Tritt man einen Schritt zurück, dann ergibt sich aus dem Gesagten ein zweigleisiges Konzept, das hinter der Anlassdogmatik des Bundesverfassungsgerichts steht:
- Einmal ist Kontrolle dann und nach *Kennzeichenkontrollen II* auf den ersten Blick sogar „nur“²⁶² dann gerechtfertigt, wenn es einen Grund in Form eines äußerlich erkennbaren Anlasses gibt, d. h. der Bürger die Kontrolle aufgrund seines eigenen gefährlichen/strafbaren Verhaltens oder zumindest aufgrund des eigenen Agierens z. B. in einem besonders gefahrgeneigten Raum (Bahnhof, Kriminalitätsschwerpunkt etc.) *tatsächlich vorhersehen* konnte. Er ist hier, frei nach *Dieter Grimm*, tatsächlich in der Lage, den über „die eigene Rechtschaffenheit Rechtfertigung“ verlangenden Staat durch rechtmäßiges oder zumindest *bewusstes* Verhalten mehr oder weniger zuverlässig auf Distanz zu halten.²⁶³ Auch die auf ihn einwirkenden *Chilling Effects* staatlicher Überwachung kann der Bürger in diesem Szenario quasi selbst unter Kontrolle behalten, d. h. vermeiden.
 - Im anderen, ausdrücklich „anlasslos“ genannten Szenario, liegen die Dinge anders: Mit der Zulassung von Stichprobenkontrollen „in weiten Bereichen“ des Wirtschafts-, Umwelt-, aber eben auch des Verkehrs- und – unionsrechtlich bedingt – des Datenschutzrechts²⁶⁴ bleibt ein Instrument im Spiel, das seine Funktionalität gerade daraus gewinnt, dass die staatliche Kontrolle jedenfalls für den Kontrollierten möglichst *unvorhersehbar* erfolgt. Durch *einzelne*, unvorhersehbare Kontrollen werden hier bewusst *allgemeine Chilling Effects* erzeugt, um eine *Breitenwirkung* in Richtung einer möglichst flächendeckenden Rechtsbefolgung

262 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 93.

263 Vgl. *Grimm*, Die Zukunft der Verfassung, 1991, S. 418. Zu diesem rechtsstaatlichen Ideal auch *Barczak*, Der nervöse Staat, 2021, S. 518 ff. m. w. N. zu aktuellem Schrifttum.

264 Soweit ersichtlich unbestr. soll Art. 58 Abs. 1 lit. b, e und f DSGVO den Datenschutzaufsichtsbehörden Datenschutzüberprüfungen, Zugang zu Akten sowie das Betreten von Räumlichkeiten, einschließlich Wohnungen, anlasslos erlauben, s. statt vieler *Boehm*, in: Kühling/Buchner (Hg.), DSGVO, BDSG, 2024, Art. 58 DSGVO Rn. 15, 18 f. Wie das mit Artt. 7, 16 GRC vereinbar sein soll, erschließt sich mir allerdings in keiner Weise. Ob auch automatisierte Kontrollen etwa im offen zugänglichen Internet erlaubt sind, wird, soweit ersichtlich, noch nicht diskutiert.

der Bürger erzeugen zu können,²⁶⁵ da diese nie wissen können, ob ein konkreter Regelverstoß nicht doch ausnahmsweise hoheitlich erkannt werden wird.²⁶⁶ Gebannt ist mit dem Konzept ‚Stichprobe‘ – das quasi als Ausnahmekonzept ein Teil des Regelkonzepts ‚Anlassbindung‘ ist – beim Bürger also tatsächlich nur die Gewissheit eines ständigen Überwachtwerdens. Gezielt erzeugt und genutzt wird hingegen das Bewusstsein eines ständigen Überwachtwerden-Könnens. Die Begründung dafür, warum das Bundesverfassungsgericht den Bürger insoweit den durch automatisierte Kontrollen erzeugten *Chilling Effects* aussetzt, ist, wie in *Kennzeichenkontrollen II* ausdrücklich hervorgehoben, die besondere Verantwortung, die aus einem zwar erlaubten, aber gleichwohl gefahrgeneigten Verhalten des Bürgers folgt. Die Überwachung, so könnte man knapp formulieren, muss auf eine einleuchtende ‚Betriebsgefahr‘ einer bestimmten Betätigung, Nutzung, oder Handlung bezogen sein, was zumindest für ein gewisses Maß an Vorhersehbarkeit und Nachvollziehbarkeit sorgt.

Das alles klingt zunächst schlüssig und im Sinn einer effektiven Rechtsdurchsetzung 121 – nämlich im Fall *hoher* Betriebsgefahren (z. B. Kraftfahrzeuge, Kernkraftwerke) – aus einer Schutzpflichtenperspektive sogar geboten. Allerdings ist der Grad zu einer allgemeinen Bürgerverantwortung für rechtmäßiges Verhalten schmal: Das zeigen die Beispiele aus dem Steuer-, Geldwäsche- oder Online-Kommunikationsrecht, in denen automatisierte Legalitätskontrollen eben doch anlasslos und sogar flächendeckend ausgerollt sind. Soll das Konzept des Bundesverfassungsgerichts hier tragen, dann müsste *jeder* Steuererklärung, *jeder* Banktransaktion und *jeder* Äußerung im Internet eine eigene, spezifische Gefährlichkeit beigemessen werden, um eine erhöhte Bürgerverantwortung und damit eine Durchbrechung der grundsätzlichen Anlassbindung staatlicher Überwachung zu rechtfertigen.²⁶⁷ Oder es müsste eingeräumt werden, dass hier weder konkreter Anlass noch bürgerliche Verantwortung die (automatisierte) Überwachung rechtfertigen.

Es gäbe eine Alternative: Wie an anderer Stelle schon vorgeschlagen,²⁶⁸ wäre es 122 überlegenswert, das Postulat einer grundsätzlichen, allerdings schon jetzt verdünnten Anlassbindung mit ihrer Fokussierung auf *äußere* Handlungsgründe (Verhalten, Orte etc.) aufzugeben, und stattdessen allgemeiner nach *Gründen* oder *Konzepten*

265 s. ganz i. d. S. *Huber*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR II, 32022, § 43 Rn. 252: „das mit der [staatlichen] Überwachung angestrebte Ziel [ist das] einer flächendeckenden Erfüllung öffentlich-rechtlicher Pflichten“.

266 So auch noch BVerfG, Beschl. v. 28.6.1994, Az. 1 BvL 14/88 = BVerfGE 91, 118 (124) – Bezirksrevisor zur Legitimität des in Stichprobenkontrollen definitionsgemäß enthaltenen Zufallselements: Es sei „dem Gleichbehandlungsgebot in besonderer Weise Rechnung [ge]tragen, da das Kontrollrisiko gleichmäßig verteilt“ sei. Die Instanzgerichte waren im konkreten Verfahren noch anderer Auffassung (Willkür).

267 Vgl. mit diesen Überlegungen auch schon *Rademacher*, in: Zimmer (Hg.), Regulierung für Algorithmen und Künstliche Intelligenz, 2021, S. 229 (257 ff.).

268 Zum Folgenden ebenfalls bereits *ibid.*, S. 258 ff.

zu fragen, warum eine bestimmte Norm mit einem höheren, d. h. gegebenenfalls eben auch automatisiertem Überwachungsdruck verbunden werden könnte/dürfte. Für die genannten Szenarien der anlasslosen Geldwäsche- und Steuer-Kontrolle lassen sich solche Gründe jenseits von Anlässen und besonderer Verantwortung durchaus finden: Es handelt sich schlicht um Konstellationen, die keine unmittelbar Geschädigten kennen, die – plakativ gesprochen – angesichts eines Rechtsverstoßes um Hilfe rufen und damit die klassischen staatlichen Rechtsdurchsetzungs- und -verfolgungsmechanismen aktivieren können. Würde sich das Gemeinwesen hier allein auf anlassbasierte Verfahren (also z. B. Hinweise durch *Whistleblower* etc.) beschränken, dann wäre der Realisierungsdruck vorsichtig gesagt gering. Oder es könnte eine kategoriale Unterscheidung zwischen Überwachung versucht werden, die das Privatleben betrifft, und solcher, die berufliche Tätigkeiten betreffen.²⁶⁹ Auch die vom Bundesverfassungsgericht in der Entscheidung *Automatisierte Datenanalyse* ausgeführte Ermächtigung zum *Data Mining* in solchen Datenbeständen, die der Behörde selbst bereits vorliegen, lässt sich nicht mit einem Anlass, sondern nur mit einem Grund erklären; schlicht: Die Daten = Verdachtsmomente sind schon da.²⁷⁰

- 123 Ins Allgemeine gewendet: Ließe man sich auf die Suche nach Gründen statt nach Anlässen (als Grundsatz) und spezifischen bürgerlichen Verantwortungen (als *vermeintliche* Ausnahme) ein, dann könnten die *Spezifika* einer konkreten Norm stärker in den Blick kommen: beispielsweise das *spezifische* Fehlen klassischer (also anlassbasierter) Rechtsdurchsetzungschancen oder empirische Rechtsdurchsetzungsdefizite. Ein besonders sichtbares Beispiel für eine solche Rücksichtnahme auf (das Fehlen von) Rechtsdurchsetzungschancen in der digitalen Sphäre lieferte vor einigen Jahren die Entscheidung des EuGH zur ausnahmsweise nun doch auch anlasslos zulässigen Vorratsdatenspeicherung von IP-Adressen, wenn und weil

„im Fall von im Internet begangenen Straftaten die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht, die Identität der Person zu ermitteln, der diese Adresse zugewiesen war, als die Tat begangen wurde.“²⁷¹

- 124 Man könnte sogar überlegen, eine Erhöhung des Verfolgungsdrucks schlicht aufgrund politischer Prioritätensetzung zuzulassen, wenn etwa – wie im Fall der Serie von Wohnungseinbruchsdiebstählen, die den erstmaligen Einsatz von *Predictive-Po-*

269 So erwägenswert N. Kuhlmann, in: Fries/Paal (Hg.), *Smart Contracts*, 2019, S. 117 (123).

270 Hierzu ausf. → § 2 Rn. 109 ff.

271 EuGH, Urt. v. 6.10.2020, Rs. C-511/18 u.a. (*La Quadrature du Net*) = NJW 2021, 531, Rn. 154. Zusätzlich musste die Vorratsdatenspeicherung nach diesem Urteil auch noch auf die Verhütung oder Verfolgung schwerer Kriminalität oder Bedrohungen der öffentlichen Sicherheit gerichtet sein (a. a. O., Rn. 156); beispielhaft verwies der EuGH auf Kinderpornographie (a. a. O., Rn. 154). 2024 folgte allerdings schon die nächste Lockerung der ursprünglich restriktiven Linie: Auch zur Bekämpfung von „Straftaten im Allgemeinen“ darf eine Vorratsdatenspeicherung dann angeordnet werden, wenn andernfalls „eine echte Gefahr der systemischen Straflosigkeit“ drohen würde, weil nur so die Identität von Straftätern feststellbar ist; s. EuGH, Urt. v. 30.4.2024, Rs. C-470/21 (*La Quadrature du Net*), Rn. 82 f., 117 ff.

licing-Anwendung in Deutschland (mit)motivierte²⁷² – aus der Bevölkerung ein Vertrauensverlust in die reale Bewirkungsleistung bestimmter Rechtssätze artikuliert wird. Das mag im ersten Augenblick rechtsstaatlich bedenklich klingen. Aber letztlich wäre damit nur anerkannt, dass sich solche Prioritätensetzungen nicht nur im materiellen Recht abbilden können, sondern – damit das materielle Recht realisiert werden kann – notwendig auch das eben dieser Realisierung geltende Recht miterfassen und mit rechtfertigen können.

Ob damit tatsächlich eine Gefahr der Ausweitung staatlicher Überwachungsbefugnisse entstünde,²⁷³ müsste sich dann zeigen. Auf materieller Ebene hinge das davon ab, welche Anforderungen an die innere Kohärenz der Begründung gestellt werden würden, warum gerade *dieser* Rechtssatz einem verschärften, über das normale (anlassbezogene, stichprobenhafte) Maß hinausgehenden Durchsetzungsdruck ausgesetzt werden soll. Das ist, darauf sei hier nochmals hingewiesen, etwas anderes als nur zu fragen, ob das Rechtsgut, dessen Schutz die Norm dient, besonders wichtig ist. Sodann kann der Gefahr einer übermäßigen Überwachung mit einer Mischung aus prozedural-systemischen Maßnahmen begegnet werden. Und zwar dadurch,

- dass *erstens* automatisiert auswertende Überwachungsbefugnisse tatsächlich einem strengen Bestimmtheitsgebot unterworfen werden, sodass die datenschutzrechtlichen Generalklauseln oder sonstige allgemeine Aufgabenzuweisungen nicht als Eingriffsermächtigung ausreichen;
- dass *zweitens* solche Ermächtigungen mit *Sunset Clauses* versehen und damit zwingend regelmäßig demokratisch neu legitimiert und – mehr oder weniger scharf/stringent – begründet werden müssten;
- dass *drittens* an die bereits ausgebaute Diskussion um die Vorsteuerung der Verwaltung durch administrative Konzepte angeknüpft wird, die in solchen Bereichen, in denen eine gesetzgeberische Steuerung nicht sinnvoll ist (weil zu schwerfällig, zu grob, zu unflexibel etc.), eine verstärkte Selbststeuerung der Verwaltung bewirken;²⁷⁴ und eventuell auch dadurch,
- dass – *viertens* – das Konzept einer Überwachungsgesamtrechnung tatsächlich operationalisiert wird (ich habe meine Zweifel, dass das wirklich geht).

Dem *Orwell'schen* Überwachungsstaat, der den Bürger auf Schritt und Tritt zur Rechtfertigung über die eigene Rechtschaffenheit auffordert, wäre mittels einer Kombination aus qualitativen (= besonderer Gesetzesvorbehalt und besondere Begründungspflicht) und quantitativen Elementen (= *Sunset Clauses*, Überwachungs-

272 Vgl. hierzu Rademacher, AöR 142 (2017), 366 ff., bes. S. 415.

273 So noch meine Befürchtung in Rademacher, in: Zimmer (Hg.), Regulierung für Algorithmen und Künstliche Intelligenz, 2021, S. 229 (259 f.).

274 Angerissen habe ich dies bereits in Rademacher, AöR 142 (2017), 366 (409); s. auch Möllers, NVwZ 2000, 382 (387). Ausf. zur Steuerung der Verwaltung durch Konzepte Herzmann, VerwArch 2013, 429 ff.

gesamtrechnung) gewehrt. Die konstruktiven Schwächen der aktuellen Anlassdogmatik würden vermieden.

- 127 *d. Grundrechtstheoretische Zweifel: Bildet das Recht auf informationelle Selbstbestimmung das falsche Schutzgut aus?* Die soeben genannte Kritik bzw. die aus der Kritik entwickelten Vorschläge betreffen letztlich nur die Feinjustierung einer durchaus brauchbaren Rechtsprechungsline, ²⁷⁵ die konsequent auf der empirisch-normativen Doppel(hypo)these von *Chilling Effects* und Rechtschaffenheitsvermutung aufbaut und davon ausgehend zu einer wirksamen, zugleich praktisch handhabbaren Einhegung staatlicher Überwachungstätigkeit führen kann. Sie vermeidet zudem den mancherorts sichtbaren Impuls, ²⁷⁶ den Einsatz neuer, breitenwirksamer Verdachtsgewinnungstechnologien durch zu hohe Eingriffsschwellen vollständig an die überkommene gefahrenabwehrrechtliche Dogmatik zu binden und damit weitestgehend zu verhindern. ²⁷⁷ Aus einer solchen pragmatischen Sicht wäre lediglich wünschenswert, dass die Gerichte die allzu scharfen Bestimmtheitsanforderungen zurückfahren, die das Sicherheitsrecht mittlerweile allzu unübersichtlich gemacht haben. ²⁷⁸
- 128 Es gibt allerdings eine konzeptionelle Lücke zwischen Grund (bzw. Gründen) und Mittel. Die Lücke wird greifbar, wenn wir den Fokus auf *Intelligent Surveillance* lenken, die *keine* personenbezogenen Daten verarbeitet, und auch nicht in den Anwendungsbereich eines spezielleren Grundrechts fällt. Ist sie dann und deshalb wirklich ohne gesetzliche Ermächtigung und damit eben doch „beliebig“ möglich?
- 129 Kehren wir an dieser Stelle noch einmal zu dem Beispiel der LiDAR-gestützten Verkehrsüberwachung zurück. ²⁷⁹ Zur Erinnerung: LiDAR-Technologie soll im aufgeführten Rüsselsheimer Pilotprojekt die Erfassung (an Kontrollpunkt A) und Wiedererkennung von Kraftfahrzeugen (an Kontrollpunkt B) ermöglichen, ohne dass dabei personenbezogene Daten verarbeitet werden. Erst im als Verdachtsfall definierten Trefferfall = Wiedererkennungsfall wird an Kontrollpunkt B ein hochauflösendes Lichtbild angefertigt, das das Kennzeichen erkennen lässt und damit eine Identifikation erlaubt. Nach der oben referierten Ansicht von *Dieter Müller* braucht diese Art der Überwachung keine eigenständige Ermächtigungsgrundlage, eben weil zur Verdachtsgewinnung keine personenbezogenen Daten verarbeitet werden; es gibt mit anderen Worten keinen Eingriff in das Recht auf informationelle Selbstbestimmung oder ein sonstiges Grundrecht. *Konkret* zu diesem Beispiel nur so viel: Die Auslegung/Subsumtion von *Müller* ist plausibel. Sie deckt sich auf den ersten Blick zudem mit der in *Kennzeichenkontrollen II* gegebenen Begründung

²⁷⁵ So auch – trotz ebenfalls starker dogmatischer Kritik – *Mösl*, GSZ 2021, 89 (109 f.).

²⁷⁶ Vgl. Nachw. in → § 2 Fn. 228.

²⁷⁷ Vgl. auch *Trute/S. Kuhlmann*, GSZ 2021, 103 (107).

²⁷⁸ Einschließlich der noch unerfreulicheren *Spill-Over*-Effekte dieser Rspr. in die nicht-sicherheitsrechtlichen Bereiche, vgl. *Marsch/Rademacher*, Die Verwaltung 54 (2021), 1 (16 ff.).

²⁷⁹ s. zum Fallbeispiel ausf. oben, → § 2 Rn. 29.

dafür, warum *klassische* Rotlicht- und sonstige Verkehrskontrollen in der Tat keinen Grundrechtseingriff darstellen:

„Indem sich die Kennzeichenkontrolle mit den Kraftfahrzeugkennzeichen auf personenbezogene Daten erstreckt, unterscheidet sie sich von Kontrollen, die gegenüber einer unbestimmten Vielzahl von Personen ohne Erfassung personenbezogener Daten durchgeführt werden und erst im Fall eines Treffers Daten zu einzelnen Personen erfassen. Dies ist etwa bei Geschwindigkeits- oder Rotlichtkontrollen im Straßenverkehr der Fall. Dort wird das Fahrverhalten zunächst ohne Erfassen des Kennzeichens und damit unabhängig von einer persönlichen Zuordenbarkeit der Kraftfahrzeuge kontrolliert. Personenbezogene Daten werden erst dann erhoben, wenn eine Übertretung gemessen und hierdurch ausgelöst ein Lichtbild erstellt wird. Dass dort ein Grundrechtseingriff nur im Trefferfall anzunehmen ist, lässt sich auf die Kennzeichenkontrolle nicht übertragen. Im Übrigen lassen sich Verkehrskontrollen auch deshalb nicht mit Kennzeichenkontrollen vergleichen, weil sie an risikobehaftetes Tun anknüpfen und damit materiell in anderem Umfang gerechtfertigt sind.“²⁸⁰

Zwingend ist die Auslegung von *Müller* gleichwohl nicht; und ich habe gewisse 130 Zweifel, ob sich das Bundesverfassungsgericht, konfrontiert mit den Potentialen von LiDAR- und Radar-Technologien, der Argumentation anschließen würde. Auch im LiDAR-Beispiel könnte man argumentieren, dass schon an Kontrollpunkt A dem jeweiligen Kraftfahrzeug sozusagen ein Identitätsmarker zugewiesen wird, der dafür sorgt, dass er an Kontrollpunkt B im Trefferfall identifizierbar sein *wird* (vgl. Art. 4 Nr. 1 DSGVO: „Zuordnung zu einer Kennung“). Mit was wir es im LiDAR-Beispiel zu tun haben, ist also eine *zunächst* nicht-personenbezogen arbeitende Verhaltenskontrolle, die aber mit einem System der temporär eng begrenzten Identifizierbarkeitsvorsorge arbeitet.

Freilich, legt man die Definition von „personenbezogen“ zugrunde, wie sie das Uni- 131 onsrecht in Art. 4 Nr. 1 DSGVO liefert, dann bleibt es dabei, dass *Müller* formal recht hat: Zwischen den Kontrollpunkten A und B und bevor ein Treffer die Anfertigung eines *dann* verdachtsbasierten Lichtbildes auslöst, werden Daten verarbeitet, die tatsächlich *noch nicht* identifizierbar sind.²⁸¹ Art. 4 Nr. 1 DSGVO scheint genau diese *aktuelle* Identifizierbarkeit zu fordern,²⁸² wenn man die Norm genau liest:

280 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 52. Zur Rechtfertigung von Überwachung aufgrund eines „risikobehafteten Tuns“ oben, bei → § 2 Rn. 106.

281 Die Konstellation ist abzugrenzen von dem – häufigen – Fall, dass die Identifizierbarkeit schon vorliegt, das Mittel zur Identifikation aber noch nicht genutzt wurde. Bsp.: eine Telefonnummer ist auch schon personenbezogenes Datum, bevor der Verantwortliche sie mit einem Namen verknüpft hat, vgl. für dieses und weitere Bsp. zum maßgeblichen Zeitpunkt der Bewertung *Klar/Kühling*, in: Kühling/Buchner (Hg.), DSGVO, BDSG, ³2020, Art. 4 Nr. 1 DSGVO Rn. 24 m. w. N.

282 Vgl. aber auch Opinion 4/2007 v. 20.6.2007 der Article-29-WP „on the concept of personal data“, die einen extrem weiten Begriff des Personenbezugs vorgeben wollte, der auch jede Verarbeitung von Daten erfasst hätte, deren „use is likely to have an impact on a certain person’s rights and interests“ (ibid., S. 11). *Purtova*, Law, Innovation and Technology 10 (2018), 40 (56 ff.) zeigt, zu welch absurden Ergebnissen ein *derart* weiter Begriff des personenbezogenen Datums führt: „weather is personal data“ (ibid., S. 57).

„Im Sinne [der DSGVO] bezeichnet der Ausdruck: [...] ‚personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte [hier sicher nein] oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“;

– identifiziert werden *kann*; nicht: identifiziert werden können *wird*, nachdem noch weitere Verfahrensschritte durchlaufen wurden.

- 132 Verallgemeinern wir nun von dieser Erkenntnis ausgehend, dann legt das eine Vermutung und eine Beobachtung nahe. *Erstens* die Vermutung: Die hier soeben nachvollzogene Auslegung, wie von Dieter Müller vorgeschlagen, ist zu formalistisch (was den Begriff des Personenbezugs anbelangt) und zu eindeutig eine Umgehung des Schutzanliegens (was das Recht auf informationelle Selbstbestimmung angeht); die Gerichte werden sich ihr nicht anschließen. Wie gesagt, das ist eine Vermutung. Entscheidender scheint mir – *zweitens* – die Beobachtung: Das Recht auf informationelle Selbstbestimmung scheint den falschen Schutzgegenstand zu haben, falls es wirklich darum gehen soll zu verhindern, dass Bürger „beliebig [...] hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen [...] müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt [sind].“²⁸³ Wenn das Grundrecht gegen ständige Rechtfertigungsabfragen und den *dadurch* ausgelösten, möglicherweise in den Bereich des *rechtlich* Erlaubten übergreifenden, d. h. überschießenden Konformitätsdruck schützen soll,²⁸⁴ dann dürfte es *nicht* darauf ankommen, dass bzw. ob es mehr oder weniger mühsam gelingt, ein personenbezogenes Datum zu kreieren, sondern darauf, ob eben ein *solcher* Konformitätsdruck entsteht. Es macht dann keinen Unterschied, ob ein Streckenradar eingesetzt wird, das zufällig mit personenbezogenen Daten arbeitet, oder ein klassischer ‚Blitzer‘, der erst im Moment des Rechtsverstoßes auslöst. In beiden Fällen zielt die staatliche Maßnahme „auf die Gewinnung von Erkenntnissen über Verdachtsmomente [...]“ und bringt „Personen in das Visier staatlicher Überwachungstätigkeit“²⁸⁵
- 133 In gewisser Weise lässt sich eine Unsicherheit darüber, ob es tatsächlich nachhaltig ist, *nicht* personenbezogene Überwachungsregimes vom grundrechtlichen Schutz und damit Rechtfertigungsdruck auszunehmen, schon beim Bundesverfassungsgericht selbst ausmachen: Denn es sieht sich gehalten, die – offenbar? – unbegrenz-

283 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51; vgl. dazu auch schon → § 2 Rn. 96.

284 Grundlegend BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83 u.a. = BVerfGE 65, 1 (43) – Volkszählungsurteil.

285 Albers, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hg.), GVwR II, ²2012, § 22 Rn. 65; Binnenzitat nach BVerfG, Beschl. v. 4.4.2006, Az. 1 BvR 518/02 = BVerfGE 115, 320 (344) – Rasterfahndung.

te, jedenfalls grundrechtlich nicht greifbare Zulässigkeit von klassischen Rotlichtkontrollen nicht nur mit dem fehlenden Eingriffscharakter zu begründen, sondern schiebt materiell nach, dass die Überwachung auch materiell rechtfertigungsfähig wäre, weil sie an ein „risikobehaftetes Tun“ anknüpft.²⁸⁶ Was *Kennzeichenkontrollen II* mit seiner Doppel(hypo)these von *Chilling Effects* und Rechtschaffenheitsvermutung²⁸⁷ also *eigentlich* einfordern würde, wäre eine Ausprägung des Allgemeinen Persönlichkeitsrechts, die spezifisch gegen staatlich angeordnete Verhaltensabfragen schützt (Achtung: nicht *Verhaltenslenkung* im engeren Sinn, dafür wäre entweder die *Nudging*-²⁸⁸ oder ist die sogleich anschließende Debatte um *Impossibility Structures* zuständig).²⁸⁹

Das Recht auf informationelle Selbstbestimmung erweist sich damit als zwar *im* 134
Allgemeinen wirkungsvolles, aber in Randbereichen – wie das LiDAR-Beispiel zeigt – doch ungenaues *Proxy* (also Hilfskriterium) für das, worum es aus einer verfassungsdogmatischen Kontrollperspektive eigentlich geht bzw. zu gehen scheint: erwünschte von nicht erwünschten/übermäßigen Verhaltensabfragen abgrenzen zu können. Indem im grundlegenden *Volkszählungsurteil* von 1983 grundrechtlich an die damals absehbaren *technischen* Formen der Verhaltensabfrage angeknüpft wurde (automatisierte Verarbeitung und vor allem Speicherung *personenbezogener* Daten), wurde in nach meinem Dafürhalten durchaus kluger Weise vermieden, pauschal alle verhaltensbeeinflussenden staatlichen Maßnahmen (paradigmatisch: die Streife gehende Polizistin) zu erfassen. Mit der doppelten Erfahrung totalitärer Staatlichkeit im Hinterkopf war 1983 ja auch weniger die Sorge vor derart flüchtigen Verhaltenskontrollen Motiv der Entwicklung des neuen Grundrechts, sondern vielmehr die Missbrauchsmöglichkeiten, die sich aus langfristigen, umfassenden *Persönlichkeitsprofilen* ergeben sollten. *Personenbezogene* Daten waren hier der sozusagen natürliche Schutzgegenstand.

286 s. Zitat soeben, → § 2 Rn. 129.

287 s. oben, bei → § 2 Rn. 96.

288 Dazu noch einmal unten, → § 3 Rn. 478.

289 Sozusagen ein Seitengleis dieser Einsicht ist es, dass mittlerweile mehrere Zivilgerichte einen Eingriff in das (bürgerlich-rechtliche) Allgemeine Persönlichkeitsrecht im Fall von *Kameraattrappen* bejaht haben. Entwickelt wird dafür die Figur des „Überwachungsdrucks“, der bejaht wird, „sofern eine Überwachung durch eine Kamera auf Grund von Verdachtsmomenten ernsthaft zu befürchten ist“ (so LG Berlin, Urt. v. 14.8.2018, Az. 67 S 73/18 = ZD 2019, 129 – Überwachungsdruck durch Kamera-Attrappe; a. A. OLG Frankfurt am Main, Beschl. v. 12.10.2017, Az. 3 U 195/16 = ZD 2018, 313 – Keine Persönlichkeitsrechtsverletzung durch Kameraattrappe). Die Logik dieses Schutzes bleibt aber letztlich den Begrenzungen des Rechts auf informationelle Selbstbestimmung verhaftet, weil sie eben darauf aufsetzt, dass scheinbar oder eventuell *personenbezogene* Daten verarbeitet werden. Davon heben sich solche Überlegungen in Lit. und Rspr. ab, die bereits den *Chilling Effect* als solchen als Grundrechtseingriff werten wollen, ohne dass es auf die Verarbeitung personenbezogener Daten ankommen soll; für Nachw. *Büscher* et al., DuD 2023, 503 (506). Damit handelt man sich allerdings das Problem der empirischen Ungewissheit über das tatsächliche Ausmaß dieser Effekte (wieder) ein. Vgl. hierzu schon die Nachw. in → § 2 Fn. 213.

- 135 Die Frage ist, ob dieser Zuschnitt des Schutzbereichs heute noch genauso gut passt wie damals; jedenfalls muss sie aus doppeltem Grund neu gestellt werden: *erstens* natürlich mit Blick auf veränderte technische Möglichkeiten der Überwachung (= reicht der Schutzzumfang noch aus?). Und *zweitens* in Bezug auf den veränderten Umfang automatisierter Verarbeitung von personenbezogenen Daten insgesamt. Denn wenn diese schon längst zum Alltag geworden bzw. mittlerweile sogar eine Alltagserwartung in weiten Teilen der Bevölkerung ist, die sich einen vernetzten Staat wünscht, verliert sie ihre Unterscheidungskraft, um Grundrechtseingriffe von Alltagsverhalten wirksam abgrenzen zu können (= greift der Schutz zu *weit*?). Die beiden Fragen können und sollen hier nicht beantwortet werden, ist dies doch nicht der eigentliche Schwerpunkt dieses Buches.²⁹⁰ Allerdings war dieser ‚Ausflug‘ in die Tiefen des Grundrechts auf informationelle Selbstbestimmung wichtig, weil – wenn es sogleich um *Impossibility Structures* geht – die zunehmend fehlende Passgenauigkeit des Rechts auf informationelle Selbstbestimmung zum Umgang mit neuen rechtserkenntnis- und rechtsdurchsetzungsfähigen Technologien noch einmal eine Rolle spielen wird.²⁹¹

II. *Impossibility Structures*

- 136 Wenden wir uns nun dem – von *Intelligent Surveillance* kommend – anderen Extrem der KI-unterstützten Rechtsdurchsetzung zu: der präventiv wirksamen *Verhinderung* von Rechtsverstößen durch physisch wirkende KI-Systeme. Ich schlage zur Kategorisierung dieser Systeme den aus der frühen US-amerikanischen Diskussion übernommenen Begriff der *Impossibility Structures* vor.

1. Begriff

- 137 Der Begriff *Impossibility Structures* wurde von Michael L. Rich im Jahr 2012 in die Diskussion um strukturell-physisch wirkende Instrumente der Rechtsdurchsetzung eingebracht.²⁹² Er will *per se* technologie-neutral Instrumente oder Vorkehrungen im weitesten Sinn bezeichnen, die es den Rechtsunterworfenen physisch unmöglich machen sollen, sich rechtswidrig zu verhalten.²⁹³ Recht und Vollzug fallen damit

290 Für eine krit. Bestandsaufnahme zum Recht auf informationelle Selbstbestimmung Behrendt, Entzauberung des Rechts auf informationelle Selbstbestimmung, 2023, passim.

291 s. unten, ab → S. 173 ff.

292 M. L. Rich, Harvard Journal of Law & Public Policy 36 (2013), 795 (802 ff.); s. dort auch Fn. 2, wonach der Begriff ursprünglich von Edward Cheng stammt.

293 Für die Übertragung des Konzepts in den deutschen Diskurs s. Rademacher, JZ 2019, 702 ff.; aufgegriffen u. a. von Britz/Eifert, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, 3202, § 26 Rn. 143 ff.; Bernzen/Kehrberger, RW 10 (2019), 374 (382 ff.), die ansonsten allerdings meist weniger verschlagwortet von „Rechtsdurchsetzung durch Informationstechnik“ sprechen; Fateh-Moghadam, ZStW 131 (2019), 863 (871 f.);

auf den ersten Blick in eins, ohne dazwischenliegenden Normbefolgungswillen bzw. dessen Betätigung durch den Normadressaten.²⁹⁴ Reine Rechtsfolgen – wie beispielsweise die Formnichtigkeit von Testamenten – gehören für mich nicht hierher, eben weil hier nichts Physisches geschieht und sich damit von vornherein keine vergleichbaren (Rechts-)Fragen stellen.²⁹⁵

Alternativbegriffe mit einem zumindest ähnlichen (wenn auch nicht immer identischen) Bedeutungsgehalt gibt es mittlerweile viele: *Embedded Law*,²⁹⁶ *Self-executing Law*,²⁹⁷ *Preemptive Technologies*,²⁹⁸ *Techno-Regulation*²⁹⁹ oder schlicht: automatisierte Rechtsdurchsetzung.³⁰⁰ Häufig verwendet werden neuerdings auch: *Law by Design*³⁰¹, *Compliance by Design*, oder – bewusst positiv konnotiert – *Legal Protection by Design*.³⁰² Einen interessanten Vorschlag unterbreitet Alexander Baur, der von „digitalen Interventionsagenten“ spricht.³⁰³ (Nennen mag man hier auch noch *Les-sigs Code is Law*, wobei dieser Ausspruch die spezifische Botschaft trägt bzw. tragen sollte, dass *Code* wie oder sogar besser *als* Recht *steuert*).

Alle Begriffe meinen mit mehr oder weniger großen Abweichungen im Detail Strukturen, die rechtlich deviantes Verhalten und *möglichst nur* und „trennscharf“ das deviante Verhalten³⁰⁴ faktisch verunmöglichen oder – wo Handlungspflichten bestehen – das rechtmäßige Tun erzwingen sollen.³⁰⁵ (*Predictive Policing* im Sinn einer nicht aus dem konkreten Verhalten, sondern aus vergangenen Handlungen und/oder allein aus Persönlichkeitsmerkmalen der betroffenen Person deduzierten Risikoprognose,³⁰⁶ liegt damit im Vorfeld der hier betrachteten Mechanismen bzw. kann/darf aufgrund des Vorfeldcharakters also gerade nicht Wissensgrundlage für eine *Impossibility Structure* sein.)

übersetzt ins Deutsche nun bei Rauber, JZ 79 (2024), 174 ff.: „Unmöglichkeitsstrukturen“. Ausf. zum Begriff, in Abgrenzung zum älteren Diskurs um physische Methoden der Kriminalprävention, Hastedt, MMR 2021, 696 ff.

294 Vgl. an dieser Stelle nur Möllers, Die Möglichkeit der Normen, 2018, S. 471: „Eine wichtige Besonderheit von Algorithmen liegt darin, dass ihre Anwendung keinen Raum für Entscheidung kennt.“

295 Anders Rauber, JZ 79 (2024), 174 (178): „zumindest verwandt“.

296 Becker, ZUM 2019, 636 (637); Breidenbach, REthinking:Law 1 (2018), 38 ff.

297 Hoffmann-Riem, AöR 145 (2020), 1 (33); Pasquale, George Washington Law Rev. 87 (2019), 1 (6).

298 Vgl. für den Unterschied zwischen Prädiktion und Präemption Burchard, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 553 (569).

299 Brownsword, Rights, regulation, and the technological revolution, 2008, S. 242 ff.

300 Beaucamp, Rechtsdurchsetzung durch Technologie, 2022, S. 11 f.; Paschke, MMR 2019, 563 (566). Ähnl. Eisenberger, in: Kahl/Ludwigs (Hg.), VII, 2025, § 191 Rn. 38. Unscharf G. Wagner, AcP 222 (2022), 56 (61), der als Bsp. für „Smart Enforcement“ auch Anwendungen wie Webcrawler zur Detektion von illegalen Inhalten anführt, die phänomenologisch Überwachung sind.

301 Raji, Künstliche Intelligenz, 2023, S. 145 ff.; Djeflal, ZaöRV 80 (2020), 847 (849).

302 Hildebrandt, Smart Technologies and the End(s) of Law, 2016, S. 218 ff.

303 Baur, ZIS 15 (2020), 275 (284).

304 Vgl. i. d. S. auch Bäcker, Vereitelungssysteme, Antrittsvorlesung in Mainz am 14.7.2022.

305 *Impossibility Structures* können also auch genutzt werden, um rechtlich verbürgte „Möglichkeitsräume“ (Hoffmann-Riem, Innovation und Recht, 2016, S. 145) offen zu halten.

306 Diesen Anwendungen setzt der AI Act nun sehr enge Grenzen, → § 2 Rn. 10 ff.

- 140 *Impossibility Structure* hat als Begrifflichkeit neben seiner internationalen Anschlussfähigkeit den zentralen Vorzug, dass er auf den Punkt bringt, worum es im Kern geht: die physisch-äußerliche *Verunmöglichung* von rechtlicher Devianz. Damit ist dann auch zugleich zum – freilich benachbarten – Phänomen des sogenannten *Nudging* abgegrenzt, das Verhaltenssteuerung beschreibt, die auf *psychische*, manipulativ-*unbewusst* erzeugte Reaktionen (in) der Zielperson setzt.³⁰⁷ Um *Nudging* soll es hier – wie die nachfolgenden Anwendungsbeispiele illustrieren werden – *nicht* gehen. Allerdings, und das mag man für den Untersuchungsfokus dieser Studie als (inkaufgenommenen) Nachteil begreifen, erfasst der Begriff der *Impossibility Structure* *prima facie* auch rein analoge Strukturen, etwa bauliche Vorkehrungen: Ein mit Stacheldraht bewehrter Zaun realisiert das Verbot von Eigentums- oder Besitzstörungen im Zweifel effektiver als der kommunikative Effekt der sanktionsbewehrten Verbotsnorm alleine. Als *Impossibility Structures* wurden schon von *Rich* selbst auch chemische oder physiologische Einwirkungen auf Körper und Psyche von Menschen beschrieben, wie etwa eine Kastration, die in den USA gegen Sexualstraftäter eingesetzt wird.³⁰⁸ Auch um diese Methoden soll es nicht gehen.
- 141 In den Blick genommen werden stattdessen solche *digitalen* Systeme, die mithilfe von im weiten Sinn künstlicher Intelligenz das Geschehen in der ihnen sensorisch zugänglichen ‚Umgebung‘ (einschließlich des Internets) in dem Sinn ‚wahrnehmen‘ und als rechtlich relevant ‚bewerten‘ können, dass sie *situativ angepasst* auf menschliches Verhalten reagieren können und dadurch insbesondere in der Lage sind, einen begonnenen menschlichen Handlungsablauf zu verunmöglichen. Deshalb hat der Begriff der Interventionsagenten von *Baur* durchaus seine Vorzüge. Bei einem analogen Banktresor würde hingegen wohl niemand von einem Agenten sprechen.
- 142 Noch eine weitere terminologische Fokussierung ist an dieser Stelle notwendig: Es geht bei den hier sogleich untersuchten ‚intelligenten‘ *Impossibility Structures* nicht um bloße Automatisierung. Der Kern des Phänomens ist nämlich nicht darin zu sehen, dass ein mit automatisierten oder autonomen Fahrfunktionen³⁰⁹ ausgestattetes Kfz „gänzlich ohne Zutun des Adressaten“ automatisiert abbremst, um eine Geschwindigkeitsbegrenzung zu ‚befolgen‘.³¹⁰ Das wäre einfach nur Automatisierung und ist eine Selbstverständlichkeit: Wenn selbstfahrende Fahrzeuge je eine Chance im regulären (also gemischten) Straßenverkehr haben sollen, müssen sie *law abiding* sein können.³¹¹ Zur *Impossibility Structure* wird ein solches System erst dann, wenn es sich dem Steuerungsbefehl des Fahrers, an dieser Stelle schneller zu fahren, wi-

307 s. statt vieler die konzise Begriffsbestimmung bei *O'Hara*, AöR 145 (2020), 133 (140) m. w. N., sowie nochmals unten, → § 2 Rn. 478.

308 Vgl. *M. L. Rich*, Harvard Journal of Law & Public Policy 36 (2013), 795 (798).

309 Zur Unterscheidung unten, → § 2 Rn. 191.

310 So *Günther*, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (544).

311 s. dazu nochmals ausf. unten, → § 2 Rn. 454 ff.

dersetzt; obwohl es *grundsätzlich* dazu in der Lage wäre, den Befehl zu verarbeiten und das Auto weiter zu beschleunigen. Es ist also sehr wohl so, dass „Faktizität [...] normativ imprägniert“ wird, die Norm bleibt hinter der bzw. durch die *Impossibility Structure* weiterhin „latent“ erkennbar, nämlich als *erkennbar situativ angepasster, physischer* Widerstand.³¹² Sonstiges Produktrecht mit Lenkungscharakter ist hingegen nicht per se *Impossibility Structure* im hier gemeinten und hier interessierenden Sinn, wenngleich seine Relevanz für die Gestaltung der Gesellschaft damit natürlich nicht in Abrede gestellt werden soll.

In diesem Sinn intelligente *Impossibility Structures* lassen sich zunächst im staatlichen Einsatz denken, etwa in Form von automatisierten Abrechnungssystemen im kommunalen Nahverkehr. Diese würden Nutzende selbsttätig etwa anhand eines *Bluetooth*-Signals ihres Mobiltelefons oder mithilfe von Gesichtserkennungssoftware identifizieren und entsprechend der zurückgelegten Wegstrecke digital „abkassieren“ können. Der vielfach kritisierte Tatbestand der Leistungserschleichung in § 265a StGB wäre damit in weitem Umfang überflüssig, schlicht deshalb, weil er zunehmend nicht mehr realisierbar wäre.³¹³ Das kleine Beispiel zeigt auch, dass die Verunmöglichung sich nicht zwingend auf rechtswidriges aktives Tun beziehen muss, sondern auch gegen rechtswidriges Unterlassen gerichtet werden kann.

Wahrscheinlicher ist aber, dass der Staat zunächst privaten Akteuren den Einsatz digitaler *Impossibility Structures* zur Wahrung eigener oder fremder Rechte erlaubt oder zum Schutz der Rechte und Interessen Dritter oder der Allgemeinheit sogar vorschreibt. Auf diese letzte Gruppe konzentrieren sich die folgenden Anwendungs- und Regelungsbeispiele.

2. ... im Online-Kommunikationsrecht

Impossibility Structures finden sich zunächst im Feld der Online-Kommunikation: Die zwischenzeitlich vieldiskutierten *Upload*-Filter sind eine Form KI-getriebener *Impossibility Structures*.

a. *Ursprung: Freiwilliges Filtern der Inhalte durch die Diensteanbieter.* Eingesetzt wurden diese Systeme schon früh von öffentlich zugänglichen Online-Plattformen, um deren eigene *Content Policies* physisch und präventiv wirksam durchzusetzen. Es ging und geht hier etwa um das Verbot pornographischer Darstellungen bei *Facebook* oder *YouTube*. Das für die Durchsetzung der *Content Policies* erforderliche Filtern der von den Nutzern hochgeladenen Inhalte geschah dabei von Seiten der

312 A. A. Günther, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (544 f.), dort auch das Zitat, freilich in verneinender Form. Ähnl. wie hier hingegen Burchard, a. a. O., S. 568: „Faktizitätsverheißungen normativ unterfüttert“.

313 Vgl. die Forderung von Pergande, F.A.Z. v. 11.11.2018, S. 10.

Unternehmen zunächst rein freiwillig. Die Klarstellung, dass das Unionsrecht einer solchen freiwilligen Kontrolle nicht entgegensteht, findet sich heute in Art. 7 DSA. Eine staatliche Anweisung zur Nutzung von Filtertechnologien lag hingegen nicht vor, *durfte* wegen des Verbots der Auferlegung allgemeiner Überwachungspflichten auf die Diensteanbieter gemäß Art. 15 der E-Commerce-RL 2000/31/EG, jetzt Art. 8 DSA, auch grundsätzlich nicht vorliegen; und auch die straf- oder zivilrechtliche Haftung der Diensteanbieter für rechtswidrigen Upload ihrer Nutzer, den sie nicht proaktiv herausfiltern, war bislang nach Art. 14 E-Commerce-RL, jetzt Art. 6 DSA, ausgeschlossen.

- 147 Im Allgemeinen gelten diese recht umfassenden Haftungs- und Kontrollfreistellungen auch heute noch (zum ‚aber‘ sogleich); Voraussetzung dafür ist, dass es sich bei dem Diensteanbieter um einen Anbieter von Hosting-Diensten im Sinn der Richtlinie bzw. des DSA handelt, er rechtswidrigen Inhalt nicht positiv kennt und er – vor allem – auf Hinweis oder sonstige Kenntniserlangung hin tätig wird, d. h. den *konkreten* Inhalt löscht oder sperrt (Art. 14 Abs. 1 E-Commerce-RL/Art. 6 Abs. 1 lit. b DSA). Somit gilt für die Bekämpfung rechtswidriger Web-2.0-Inhalte in Europa weiterhin der Grundsatz *Notice-and-take-down*, greift also *im Grundsatz* ein *ex-post*-Verfahren, das gerade *nicht* zur Errichtung von *Impossibility Structures* zwingt.
- 148 Seinen Ursprung hat dieser – sehr Plattform-freundliche – Grundsatz im Ende der 1990er Jahre vorherrschenden rechtspolitischen Wunsch, die gerade erst entstehende, noch relativ kleine Internet-Ökonomie vor scharfen nationalen Haftungsregelungen zu schützen.³¹⁴ Die mit der niedrigschwelligen Jedermann-Kommunikation im Web 2.0 verbundenen Gefahren wurden noch nicht gesehen. Beides hat sich mittlerweile geändert, sodass vielen die sektoriell und größenmäßig undifferenzierten Haftungsprivilegien der E-Commerce-RL und nun auch des DSA als „Überprivilegierung [jedenfalls] bestimmter Geschäftsmodelle“³¹⁵ erscheint. *Daniel Holznapel* hebt insofern – unter Verweis auf die Korrekturbemühungen der deutschen Zivilgerichte – solche Hosting-Anbieter besonders hervor, die „strukturell gefahrgeneigte Geschäftsmodelle“ betreiben oder die sich die Inhalte ihrer Nutzer „strukturell zu eigen machen.“³¹⁶ Der Grundsatz des (nur) *Notice-and-take-down* gerät daher von vielen Seiten – legislativ wie judikativ – unter Druck, wie die nachfolgenden Beispiele

314 s. *Schiff*, Informationsintermediäre, 2021, S. 58 ff. Für die Anbieter großer Plattformen etc. noch heute *Roßnapel*, in: Ehlers/Fehling/Pünder (Hg.), Bes. VerwR., ⁴2020, § 61 Rn. 66.

315 Überzeugend *D. Holznapel*, CR 2021, 123 Rn. 10, auch zur Rspr. des BGH vor dem DSA.

316 *Ibid.*, Rn. 10 ff. m. w. N. zur dt. Rspr. sowie krit. zu den Korrekturbemühungen des EuGH, der danach differenziert, ob der Anbieter eine „aktive Rolle“ einnimmt (dann Verlust des Haftungsprivilegs) oder eine „passive“ oder „neutrale Rolle“ (nur dann greift das Haftungsprivileg). Ausf. und ebenfalls krit. zur (Un)Tauglichkeit des Neutralitäts-/Passivitätskriteriums *Schiff*, Informationsintermediäre, 2021, S. 165.

le ohne Anspruch auf Vollständigkeit³¹⁷ illustrieren sollen. Zunehmend verlangen Gesetzgeber und Gerichte *ex ante* wirksame, d. h. Online-Inhalte filternde und gegebenenfalls deren Upload *hindernde* Mechanismen des Rechts(widrigkeits)schutzes im digitalen Raum,³¹⁸ die sich konzeptionell als *Impossibility Structures* kategorisieren lassen.

Bevor diese Beispiele untersucht werden, vorab noch ein aktueller Hinweis: Hier 149 nicht näher untersucht werden kann die Frage, ab welchem Punkt die derzeit diskutierte Dynamik³¹⁹ oder Emergenz-Regulierung³²⁰ insbesondere von bzw. gegen Desinformationen³²¹ als *Impossibility Structure* gewertet werden kann. Hierbei würde – wenn sich entsprechende Vorschläge durchsetzen sollten – Kommunikation, die Muster von Desinformation aufweist, nicht verhindert werden, aber auf den Plattformen so sehr verlangsamt, dass deren Gefährlichkeit, insbesondere Demokratieschädlichkeit, gemindert werden soll. Hier wäre vielleicht etwas treffender von einer *Mitigation Structure* zu sprechen.

b. Filterpflichten aus dem neuen digitalen Urheberrecht? Angesichts der medialen 150 wie auch rechtswissenschaftlichen Diskussion läge es nahe, die Diskussion um digitale Kommunikationsfilter-Technologien mit dem berichtigten Art. 17 der 2019 verabschiedeten Richtlinie über das Urheberrecht im digitalen Binnenmarkt (DSM-RL)³²² zu eröffnen. Zwar schreibt auch dessen zuletzt besonders kontrovers diskutierter³²³ Absatz 4 den Einsatz von Upload-Filtern zum Schutz von Urheberrechten im Internet gerade *nicht* ausdrücklich vor. Allerdings verlangt Art. 17 Abs. 3, 4 DSM-RL die Aufhebung des Haftungsprivilegs des Art. 14 E-Commerce-RL/jetzt Art. 6 DSA für den Fall, dass ein Host-Provider es versäumt hat, „nach Maßgabe hoher branchenüblicher Standards für die berufliche Sorgfalt alle Anstrengungen“ zu unternehmen, damit urheberrechtlich geschütztes Material, zu dem „die Rechteinhaber den Anbietern dieser Dienste einschlägige und notwendige Informationen bereitgestellt haben, nicht [öffentlich] verfügbar“ ist (Art. 17 Abs. 4 lit. b DSM-RL).

317 Insbes. das vom BGH als Teil der Störerhaftung entwickelte *Notice-and-stay-down*-Konzept kann hier nicht ausf. vorgestellt werden. Vgl. hierzu *D. Holznapel*, CR 2021, 123 ff., schon mit Blick auf die durch den DSA festgeschriebenen Änderungen; ausf. außerdem *Schiff*, Informationsintermediäre, 2021, S. 193 ff.

318 Soweit ersichtlich wird ein solcher Trend zu „preventive monitoring [...] as long as the adequate technology exists“ von den meisten, wenn nicht allen Beobachtern diagnostiziert, wenn auch nicht allseits gutgeheißen, vgl. schon *Arroyo Amayuelas*, in: Schulze/Staudenmayer/Watson (Hg.), EU Digital Law, 2020, Art. 14 E-Commerce-Directive Rn. 13, mit den Zitaten und w. Nachw.

319 *Eifert*, in: Hermstrüwer/Lüdemann (Hg.), Der Schutz der Meinungsbildung im digitalen Zeitalter, 2020, S. 189 ff. Vgl. auch schon *Raz*, in: ders. (Hg.), The Authority of Law, 2009, S. 279 (285 f.).

320 Ausf. *Perkowski*, Desinformationsregulierung (Manuskript 2024), passim, bes. Kap. 2.C.II.

321 Zu den Regulierungsbemühungen *ibid.*, Kap. 1.E. Außerdem *Peukert*, JZ 2023, 278.

322 RL (EU) 2019/790 v. 17.4.2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der RL 96/9/EG und 2001/29/EG, kurz DSM-Richtlinie, abgeleitet von der englischen Kurzform für *Directive on Copyright in the Digital Single Market*.

323 Für eine positive Bewertung s. *F. Hofmann*, GRUR 2019, 1219 (1221 ff.): „vermittelt ausgewogen zwischen der Durchsetzung des Urheberrechts im Internet und Plattform- sowie Nutzerinteressen“.

Mittelbar, nämlich um der eigenen Haftung für die ihm nunmehr *als eigene*³²⁴ zugerechnete Rechtsverletzung seiner Nutzer zu entgehen, folgt daraus eben doch, dass die vom Anwendungsbereich des Art. 17 DSM-RL erfassten Diensteanbieter ihre Filtertechnologien nunmehr im Sinne eines *Notice-and-prevent*-Modells³²⁵ auf den Schutz von Urheberrechten einstellen müssen. Dass das Ziel von Art. 17 Abs. 4 DSM-Richtlinie *ohne* automatisierte Filter erreicht werden könnte bzw. dass ein Verzicht auf solche Technologien heute noch den „branchenüblichen Standards“ entspräche, wird soweit ersichtlich nicht ernsthaft vertreten.³²⁶ Technisch geht es in der Regel um Bild- und Texterkennung, auf Plattformen wie YouTube spielt auch die Erkennung von geschützten Toninhalten eine wichtige Rolle.³²⁷

- 151 Aber: Auch wenn es daher so scheint, als schreibe Art. 17 DSM-RL den EU-Mitgliedstaaten die Schaffung eines Haftungsregimes vor, das Private (= Host-Provider) zum Einsatz von *Impossibility Structures* gegen Private (= Nutzer) zum Schutz anderer Privater (= Urheberinnen) vorschreibt, zeigt das deutsche Umsetzungsgesetz (das Urheberrechts-Diensteanbieter-Gesetz [UrhDaG]), dass es einen Mittelweg zwischen dem alten Modell des erst auf eine erfolgte Rechtsverletzung reagierenden *ex-post*-Schutzes (*Notice-and-take-down*) und dem *ex ante* wirksamen Filtern gibt. Dieser für den Ausgleich der widerstreitenden Interessen vielversprechende Mittelweg³²⁸ soll an späterer Stelle als eigene Kategorie der *Justification Structures* vorgestellt werden. Wir wollen Art. 17 DSM-RL daher fürs Erste zurückstellen, um die Diskussion später gemeinsam mit dem deutschen Umsetzungsgesetz wiederaufzugreifen (siehe unten, → S. 204 ff.).
- 152 Im nun Folgenden soll der Blick zunächst noch einmal zurückgehen zum in Artt. 14 f. E-Commerce-R/Artt. 6, 8 DSA geregelten Grundsätzlichen. Auch der EuGH scheint mittlerweile – nach zahlreichen, zunächst sehr Plattform-freundlichen Urteilen – realisiert zu haben, dass das in den genannten Normen vorgesehene undifferenzierte Haftungsprivileg mit Schuld daran ist, dass der digitale Kommunikationsraum vielfach zum ‚rechtsfreien Raum‘ geworden ist; der von der Richtlinie vorgesehene *ex-post*-Rechtsschutz (*Notice-and-take-down*) kommt angesichts der

324 Zum darin liegenden „Epochenwechsel“ Lennartz/Möllers, GRUR 2021, 1109 m. w. N.

325 Pravemann, GRUR 2019, 783 (786): *Notice* deshalb, weil die Plattformen nicht verpflichtet sind, von sich aus nachzuforschen, ob ein Urheberrecht an einem bestimmten Upload besteht oder nicht. Allerdings ist zu beachten, dass die *Notice* nun einen anderen Bezugsgegenstand hat: Nicht mehr auf eine (konkrete) Rechtsverletzung, sondern (nur noch) auf ein zu schützendes Rechtsgut muss hingewiesen werden.

326 Soweit ersichtlich einhellige Meinung, vgl. etwa GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 62 ff.; Lennartz/Möllers, GRUR 2021, 1109; F. Hofmann, GRUR 2019, 1219 (1220) m. w. N. in Fn. 15.

327 Eine knappe Übersicht und Einordnung der verfügbaren Verfahren der automatisierten Inhalteerkennung speziell für den Bereich von Art. 17 DSM-RL (Stichworte: *Hashing*, *Watermarking*, *Fingerprinting*) findet sich bei GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 57 ff. Ausf. Beaucamp, Rechtsdurchsetzung durch Technologie, 2022, S. 81 ff.

328 Ähnl. F. Hofmann, NJW 2021, 1905 (1910): „handwerklich durchaus beeindruckend“.

Verbreitungsdynamiken des Internet³²⁹ oftmals schlicht zu spät. Zwei Urteile sind in diesem Zusammenhang von zentraler Bedeutung: die Rechtssache *Glawischnig-Piesczek* (2019) sowie die Rechtssache *Cyando* (2021).

c. *Filterpflichten im Ehrschutzrecht: die Rechtssache Glawischnig-Piesczek*³³⁰ ging es nicht um den Schutz von Urheberrechten, sondern um den Ehrschutz in Facebook-Foren. Zur Überraschung vieler³³¹ urteilte der EuGH, dass es mit dem Unionsrecht, speziell Artt. 14 und 15 E-Commerce-RL vereinbar sei, wenn ein Internetdiensteanbieter (Facebook) von einem nationalen Gericht dazu verurteilt wird, automatisiert solche Meinungsäußerungen zu erkennen und zu verhindern, die zuvor von dem nationalen Gericht als ehrverletzend und deshalb als unzulässig bewertet wurden; und zwar unter Einschluss „wortgleicher“ sowie „sinngleicher“ Inhalte³³² und ungeachtet dessen, ob die Äußerung von dem ursprünglichen Beleidiger oder von anderen Nutzern des Dienstes stammen.³³³ Der EuGH hat sich insoweit zu einem relativ umfassenden *Notice-and-stay-down*-Modell³³⁴ bekannt.

Begründet hat der Gerichtshof die Zulässigkeit der vergleichsweise weiten präventiven Filterauflagen mit dem Schutzbedarf der beleidigten Personen, was angesichts der Verbreitungsdynamiken rechtsverletzender Inhalte im Internet auch sofort einschichtig ist. Diesen Schutzbedarf erkennt die einschlägige E-Commerce-RL auch explizit an, in ihren Artt. 14 Abs. 3, 18 Abs. 1. Darin heißt es, dass dann, wenn ein Gericht oder eine Verwaltungsbehörde eine Rechtsverletzung festgestellt hat, es zulässig ist, von den Diensteanbietern über deren Beseitigung (Sperrung/Löschung) hinausgehend zu verlangen, dass sie weitere Rechtsverletzungen „verhindern“.³³⁵ Unter Berücksichtigung dieser Vorschriften, so der EuGH, könne daher bei der präventiven Filteranordnung auch nicht von einer nach Art. 15 E-Commerce-RL verbotenen „allgemeinen“ Überwachungspflicht die Rede sein, da wegen des engen Bezugs (= wort- oder zumindest sinngleich) zu einer konkreten, bereits erfolgten Verletzungshandlung eine ausweislich der genannten Vorschriften zulässige, weil „spezifische Überwachungspflicht“ vorliege.³³⁶

Wohlgemerkt haben sich mit dieser Entscheidung des EuGH die Bezugspunkte dafür verschoben, was „allgemein“ (= unzulässig) und was „spezifisch“ (= zulässig) ist. Die Rechtsprechung des EuGH habe sich, so Generalanwalt Saugmandsgaard

329 s. dazu bes. *Eifert*, in: Hermstrüwer/Lüdemann (Hg.), *Der Schutz der Meinungsbildung im digitalen Zeitalter*, 2020, S. 189 ff.

330 EuGH, Urt. v. 3.10.2019, Rs. C-18/18 (*Glawischnig-Piesczek*).

331 Das Urteil wurde meist krit. aufgenommen, vgl. bspw. *Janal*, ZEuP 2021, 227 (250 f.).

332 EuGH, Urt. v. 3.10.2019 – Rs. C-18/18 (*Glawischnig-Piesczek*), Rn. 33 ff. bzw. 38 ff.

333 *Ibid.*, Rn. 37.

334 *F. Hofmann*, GRUR 2019, 1219 (1220).

335 EuGH, Urt. v. 3.10.2019 – Rs. C-18/18 (*Glawischnig-Piesczek*), bes. Rn. 40 f.

336 *Ibid.*, Rn. 34 und ff., 47.

Øe in seinen Schlussanträgen zur Rs. C-401/19 befürwortend, mit *Glawischnig* „weiterentwickelt“.³³⁷ Früher wurde „allgemein“ vom EuGH (und wird in Teilen der Literatur noch heute³³⁸) mit Blick auf die *Menge* der vom Anbieter zu filternden Inhalte/Daten interpretiert. Wenn ein Anbieter *sämtliche* Uploads auf seine Speicher filtern muss, lag eine allgemeine Überwachung vor. Heute, so stellt *Saugmandsgaard Øe* fest, „scheint der Gerichtshof auf die Präzision der Nachforschung abzustellen[,] da es darum gehe, eine ‚konkrete‘ [= wort- und sinngleiche] diffamierende Information aufzuspüren und zu sperren“.³³⁹ Dass er das kann, d. h., dass der Gerichtshof diesen Trend hin zum „preventive monitoring“³⁴⁰ schon unter Geltung der E-Commerce-RL in Gang setzen konnte, liegt *erstens* daran, dass Artt. 14 Abs. 3, 18 Abs. 1 E-Commerce-RL den *Verhinderungs*aspekt bereits ausdrücklich benennen, und dürfte *zweitens* darauf zurückzuführen sein, dass der *freiwillige* Einsatz von wirksamen Filtertechnologien durch die Diensteanbieter gezeigt hat, dass sie mit einer präventiven Kontrolle der hochgeladenen Inhalte trotz der teils gewaltigen Mengen dank des „technischen Fortschritts“ nicht mehr überfordert sind.³⁴¹ Damit das so bleibt, also damit der mit der Filterpflicht verbundene Aufwand für die Diensteanbieter wirtschaftlich zumutbar ist (Stichwort Verhältnismäßigkeit), fordert der EuGH ausdrücklich, dass das zuständige nationale Gericht „wortgleich“ und vor allem „sinngleich“ derart genau ausdefinieren müsse, dass der Anbieter der Verpflichtung durch „automatisierte Techniken und Mittel zur Nachforschung“ nachkommen könne, also ohne „autonome Beurteilung“ der Rechtswidrigkeit einer neuerlichen Äußerung.³⁴² Anders ausgedrückt: Nur im Fall der *Möglichkeit* des Rückgriffs auf das, was hier als *Impossibility Structures* bezeichnet wird, sei Diensteanbietern im Anwendungsbereich von Artt. 12 ff. E-Commerce-RL die Durchsetzung des Ehrschutzes nach dem *Notice-and-stay-down*-Modell zumutbar.

- 156 Die Meinungsfreiheit der Nutzer taucht in der Abwägung des EuGH als eigenständiger Gesichtspunkt übrigens erstaunlicherweise nicht auf.³⁴³ Der Gerichtshof

337 Vgl., auch zu den nachfolgenden Zitaten, GA *Saugmandsgaard Øe*, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 110 ff.

338 Krit. deshalb *Janal*, ZEuP 2021, 227 (250 f.): *Glawischnig* führe zu einer – zu „revidierenden“ (S. 251) – allg. Überwachungspflicht, die „der Konzeption freiheitlicher Gesellschaften“ widerspreche (S. 272). A. A. *Lennartz/Möllers*, GRUR 2021, 1109 (1112): „Ihr Pflichtenprogramm [= das der Diensteanbieter, Inhalte zu filtern] ist insofern ein reaktives, als dass sie auf [...] Blockadeaufforderungen reagieren, aber nicht proaktiv und anlasslos die gesamte Nutzung überwachen müssen.“ Ähnl. GA *Saugmandsgaard Øe*, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 114.

339 Ibid., Rn. 112.

340 *Arroyo Amayuelas*, in: Schulze/Staudenmayer/Watson (Hg.), EU Digital Law, 2020, Art. 14 E-Commerce-Directive Rn. 13.

341 Vgl. i. d. S. auch GA *Saugmandsgaard Øe*, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 113.

342 EuGH, Urt. v. 3.10.2019 – Rs. C-18/18 (*Glawischnig-Piesczek*), Rn. 45 f.

343 Hierin zeigt sich für *Schiff*, Informationsintermediäre, 2021, S. 81 eine „grundrechtliche Leerstelle“ der Entscheidung.

entwickelt die *Notice-and-stay-down*-Verpflichtung vielmehr konsequent aus dem Schutzinteresse der Hosting-Provider, das dank der Verfügbarkeit automatisierter Inhaltserkennungstechnologien nun nicht mehr in gleichem Maße wie früher relevant ist.³⁴⁴ Auch der Datenschutz der Nutzerinnen wird in dem Urteil nicht als Abwägungsgut herangezogen.

d. *Filterpflichten im bisherigen Urheberrecht: die Rechtssachen YouTube und Cyando.* 157
In den verbundenen Rechtssachen C-682/18 und C-683/18 (*YouTube und Cyando* – im Folgenden kurz *Cyando*) geht der EuGH einen weiteren Schritt in Richtung präventiver Maßnahmen.³⁴⁵ Auf den ersten Blick scheint freilich das Gegenteil der Fall zu sein: Die wieder im Urheberrecht, allerdings noch unter alter Rechtslage vor In-Kraft-Treten des Umsetzungsrechts zu Art. 17 DSM-Richtlinie spielenden Urteile werden etwa in der GRUR überschrieben mit „Keine Haftung für Internetplattformbetreiber bei Urheberrechtsverstößen in Unkenntnis der hochgeladenen Inhalte“.³⁴⁶ Das klingt wie eine simple Bestätigung dessen, was in Art. 14 Abs. 1 E-Commerce-RL ohnehin geregelt ist, also grundsätzlich keine Haftung vor entsprechender *Notice*.

Tatsächlich ist die Überschrift aber missverständlich, denn in einer komplexen Auslegungskonstruktion drängt der EuGH das allgemeine Haftungsprivileg in Art. 14, 15 E-Commerce-RL zurück und verlangt zur Gewährung des Privilegs auch *ex ante* ansetzende Maßnahmen. Der EuGH gelangt dorthin, indem er die Voraussetzungen schärfer definiert, unter denen sich ein Host-Provider überhaupt darauf berufen kann, im Anwendungsbereich des Art. 14 E-Commerce-RL zu agieren. Dafür muss etwas weiter ausgeholt werden, da die Auslegung verschachtelt ist. Es lohnt sich, die entscheidenden Passagen im Wortlaut wiederzugeben. Der EuGH beginnt mit dem allgemeinen Maßstab: 158

„Um zu ermitteln, ob der Betreiber einer Video-Sharing- oder Sharehosting-Plattform nach Art. 14 [Abs. 1 E-Commerce-RL] von seiner Verantwortung für die geschützten Inhalte befreit werden kann, die Nutzer rechtswidrig über seine Plattform öffentlich wiedergeben, ist daher zu prüfen, ob die Rolle dieses Betreibers *neutral* ist, d. h., ob sein Verhalten rein technisch, automatisch und passiv ist, was bedeutet, dass keine Kenntnis oder Kontrolle über die von ihm gespeicherten Inhalte besteht, oder ob der Betreiber im Gegenteil eine *aktive* Rolle spielt, die ihm eine Kenntnis dieser Inhalte oder eine Kontrolle über sie zu verschaffen vermag [...]“³⁴⁷

344 Vgl. bes. EuGH, Urt. v. 3.10.2019 – Rs. C-18/18 (Glawischnig-Piesczek), Rn. 44, 46. Die Meinungsfreiheit der Nutzer wird nur implizit als mitgedacht angedeutet, vgl. Rn. 43 i. V. m. ErwGr. 41 und 9 der E-Commerce-RL (im Urteil abgedruckt unter Rn. 3). Ähnl. die Einschätzung von *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 173 f.: „mittelbar [auch] ein Schutz für die Nutzer“.

345 Ähnl. die Einschätzung von H. Frey, MMR 2022, 97: „deutliche Tendenz [...] Rechtsverletzungen im Internet stärker an der ‚Quelle‘ zu unterbinden.“

346 GRUR 2021, 1054.

347 EuGH, Urt. v. 22.6.2021, verb. Rs. C-682/18 und C-683/18 (Peterson/Google und Elsevier/Cyando) = GRUR 2021, 1054, Rn. 106. Hervorhebungen hier.

159 Eine *neutrale* oder passive Rolle, so der EuGH weiter, habe ein Diensteanbieter im urheberrechtlichen Zusammenhang dann *nicht*, wenn er „über die bloße Bereitstellung [seiner] Plattform hinaus dazu beiträgt, der Öffentlichkeit unter Verletzung des Urheberrechts geschützte Inhalte *zugänglich* zu machen.“³⁴⁸

160 Für den Begriff des Zugänglichmachens zieht der EuGH den Begriff der „Wiedergabe“ nach Art. 3 der Urheberrechtsrichtlinie heran.³⁴⁹ Eine Wiedergabe in diesem Sinn liege vor,

„wenn [der Diensteanbieter] in voller Kenntnis der Folgen seines Verhaltens tätig wird, um seinen Kunden Zugang zu einem geschützten Werk zu verschaffen, und zwar insbesondere dann, wenn ohne dieses Tätigwerden die Kunden das verbreitete Werk grundsätzlich nicht abrufen könnten [...].³⁵⁰ Um festzustellen, ob der Betreiber einer Video-Sharing- oder Sharehosting-Plattform in voller Kenntnis der Folgen seines Verhaltens bei der unerlaubten Wiedergabe geschützter Inhalte durch Nutzer seiner Plattform tätig wird, [...] sind alle Gesichtspunkte zu berücksichtigen, die die betreffende Situation kennzeichnen und es ermöglichen, direkt oder indirekt Schlussfolgerungen hinsichtlich der Frage zu ziehen, ob der Betreiber bei der unerlaubten Wiedergabe dieser Inhalte vorsätzlich tätig wird oder nicht.“³⁵¹

161 Zentral ist sodann, worauf sich der Vorsatz – die „volle Kenntnis“ – beziehen muss: Nicht etwa auf die konkrete, einzelne Rechtsverletzung, sondern darauf, dass *im Allgemeinen* Urheberrechtsverstöße auf der fraglichen Plattform erfolgen; und es reicht, konträr zur Rede von der „vollen Kenntnis“, sogar *Dolus eventualis*. Im Wortlaut:

„Zu den insoweit maßgeblichen Gesichtspunkten zählen namentlich die Tatsache, dass ein solcher Betreiber, obwohl er weiß *oder wissen müsste*, dass über seine Plattform *im Allgemeinen* durch Nutzer derselben geschützte Inhalte rechtswidrig öffentlich zugänglich gemacht werden, nicht *die geeigneten technischen Maßnahmen* ergreift, die von einem die übliche Sorgfalt beachtenden Wirtschaftsteilnehmer in seiner Situation erwartet werden können, um Urheberrechtsverletzungen auf dieser Plattform glaubwürdig und wirksam zu bekämpfen [...]“³⁵²

162 Abschließend gibt der EuGH dem vorlegenden Bundesgerichtshof auch Hinweise, was unter „geeigneten technischen Maßnahmen“ in Übereinstimmung mit der „üblichen Sorgfalt“ zu verstehen ist:

„Weiter heißt es [im Vorlagebeschluss], YouTube habe verschiedene technische Vorkehrungen getroffen, um Urheberrechtsverletzungen [...] zu unterbinden und zu beenden, wie etwa einen Meldebutton und ein spezielles Benachrichtigungsverfahren, um rechtsverletzende Inhalte zu melden und entfernen zu lassen, sowie ein *Programm zur Inhaltsprüfung und Inhaltserkennungsprogramme, die die Identifizierung und die Bezeichnung solcher Inhalte erleichterten*. Somit

348 Ibid., Rn. 107. Hervorhebung hier.

349 Ibid., Rn. 108.

350 Ibid., Rn. 68.

351 Ibid., Rn. 83.

352 Ibid., Rn. 84. Hervorhebung hier.

ist davon auszugehen, dass dieser Betreiber technische Maßnahmen ergriffen hat, um Urheberrechtsverletzungen auf seiner Plattform glaubwürdig und wirksam zu bekämpfen.“³⁵³

Der EuGH hat mit dieser Rechtsprechung einen Weg gefunden, im Sinn des Verhältnismäßigkeitsgrundsatzes nach der Leistungsfähigkeit des konkreten Diensteanbieters *und* der Verfügbarkeit geeigneter Technologien („übliche Sorgfalt“) justierbare Verkehrspflichten, einschließlich „proaktiver Filterpflichten“,³⁵⁴ einzuführen, die – mehr oder weniger elegant – an den *prima facie* entgegenstehenden Artt. 14, 15 E-Commerce-RL vorbei die übermäßige Privilegierung der Dienstanbieter und das damit verbundene defizitäre Schutzniveau der Rechteinhaber korrigieren.

Festzuhalten ist allerdings, dass – soweit ersichtlich – Einigkeit besteht, dass der EuGH nicht dahingehend zu verstehen ist, dass Plattform- und andere Diensteanbieter von vornherein nach *jeder* Form von Rechtsverletzung filtern/suchen müssen. Das wäre letztlich mit Art. 15 E-Commerce-RL/Art. 8 DSA unvereinbar. Wohl aber müssen sie Verfahren bereithalten, um *gleichartige Wiederholungen* von einmal konkret bezeichneten Rechtsverletzungen zu verhindern (*Notice-and-stay-down*).³⁵⁵ Dadurch würde dann ein Gleichlauf mit den Maßstäben von *Glawischnig* bestehen, mit dem Unterschied freilich, dass in *Glawischnig* eine *gerichtliche* Feststellung der Initial-Rechtsverletzung vorlag, worauf es im urheberrechtlichen Bereich nicht ankommen scheint.

Negativ fällt freilich insgesamt auf, wie unsicher der Maßstab erforderlicher Maßnahmen im Detail geraten ist. Denn die von den Diensteanbietern zu erfüllenden (*ex-ante*)-Pflichten erscheinen angesichts des Katalogs an *möglichen* Maßnahmen, den der Gerichtshof im Wege einer unstrukturierten Gesamtschau präsentiert hat, extrem einzelfallabhängig geraten.³⁵⁶ In systematischer Hinsicht fällt auf, wie nah die in *Cyando* entwickelten allgemeinen Maßstäbe („die übliche Sorgfalt beachtenden Wirtschaftsteilnehmer“ hinsichtlich der Bekämpfung von Urheberrechtsverstößen) an den speziellen Verschärfungen der Provider-Verantwortlichkeit liegen, die der Unionsgesetzgeber in Art. 17 Abs. 4 lit. b DSM-Richtlinie aufgestellt hat („nach Maßgabe hoher branchenüblicher Standards für die berufliche Sorgfalt alle Anstrengungen [zu unternehmen], um sicherzustellen, dass bestimmte Werke und sonstige Schutzgegenstände [...] nicht verfügbar sind“).³⁵⁷ Dieser Quervergleich verweist nun

353 Ibid., Rn. 94. Hervorhebung hier.

354 Vgl. *Specht-Riemenschneider*, GRUR 2021, 1066 f.

355 In diese Richtung *Zurth*, ZUM 2021, 829 (833); vgl. auch *H. Frey*, MMR 2022, 97 (99 f.), der im Erg. allerdings davon ausgeht, dass sich das *Stay-down* nur auf den „konkreten Inhalt“ beziehen kann (a. a. O. in Fn. 30). Das würde allerdings der Rechtsprechungslinie in *Glawischnig* zuwiderlaufen, wo der Rechtsschutz auf *Notice* hin gerade auch „sinngleiche“ Rechtsverletzungen erfassen sollte.

356 Das gilt gerade auch für den Einsatz von Inhaltserkennungstechnologien, vgl. beispielhaft die Unsicherheiten bei *H. Frey*, MMR 2022, 97 (99 f.).

357 So auch *Specht-Riemenschneider*, GRUR 2021, 1066; s. auch *H. Frey*, MMR 2022, 97 (98): „Gleichlauf zu Art. 17 Abs. 4 DSM-RL“.

doch noch einmal zurück zu den *gesetzgeberischen* Bemühungen, die Kontrolle der Online-Kommunikation von einem *ex-post*- auf ein präventives Konzept umzustellen. Zwei weitere Beispiele aus diesem inkrementellen Prozess seien hier noch vorgestellt:

- 166 *e. Ausdrückliche proaktive Filterpflichten aus dem Unionsrecht: Anti-Terror-Gesetzgebung.* Hier ist der Blick auf die Verordnung (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte zu richten [TCO-VO³⁵⁸]. Sie wurde am 29. April 2021 verabschiedet und gilt seit dem 7. Juli 2022.³⁵⁹ Auch hier geht es darum, die Anbieter von Hosting-Diensten in die Kontrolle von Online-Kommunikation einzubinden, diesmal mit dem Ziel, „deren Missbrauch [...] zur Verbreitung terroristischer Online-Inhalte“ zu bekämpfen.³⁶⁰ In diesem Fall interessiert uns auch die Gesetzgebungsgeschichte. Denn in ihrem schon 2018 vorgelegten Verordnungsvorschlag³⁶¹ wollte die Kommission die Hosting-Anbieter noch auf ein umfassendes Set an ausdrücklich sogenannten „proaktiven Maßnahmen“ festlegen; einmal in Form des schon bekannten *Notice-and-stay-down*-Verfahrens. Dafür hieß es in Art. 6 Abs. 2 des Vorschlags:

„Im Fall einer Unterrichtung [eines Hostingdiensteanbieters über einen zu entfernenden Inhalt fordert die] zuständige Behörde den Hostingdiensteanbieter auf, innerhalb von drei Monaten nach Eingang der Aufforderung und danach mindestens einmal jährlich einen Bericht über die von ihm ergriffenen spezifischen proaktiven Maßnahmen, *einschließlich der Verwendung automatisierter Werkzeuge*, vorzulegen, um (a) ein *erneutes Hochladen von Inhalten, die zuvor entfernt oder gesperrt wurden*, weil sie als terroristische Inhalte erachtet werden, *zu verhindern* [...]“.³⁶²

- 167 Soweit, so klassisch. Diese konkrete *Notice* sollte allerdings zugleich der Anlass für eine umfassende Pflicht zur proaktiven Filterung der auf der konkreten Plattform stattfindenden Kommunikation/des dortigen Uploads insgesamt sein. Dafür sollte es unmittelbar folgend in lit. b von Art. 6 Abs. 2 heißen: „(b) terroristische Inhalte zu erkennen, zu ermitteln und unverzüglich zu entfernen oder zu sperren.“
- 168 Das ging dem Europäischen Parlament zu weit. Es sorgte sich um die Meinungs- und Äußerungsfreiheit der Nutzenden des so in die Pflicht genommenen Diensteanbieters.³⁶³ Am Ende des Trilogs steht nun als Kompromiss Art. 5 TCO-VO über „spezifische [nicht mehr: proaktive] Maßnahmen“. Die finale Norm erstreckt sich über acht Absätze, zahlreiche Unterabsätze und Aufzählungen, und ist damit außerordentlich kompliziert geraten. Im Grunde ist das zu etablierende System aber

358 TCO steht für *Terrorist Content Online*.

359 Art. 24 UAbs. 2 TCO-VO (EU) 2021/784.

360 Vgl. Art. 1 Abs. 1 TCO-VO (EU) 2021/784.

361 s. COM(2018) 640 final v. 12.9.2018.

362 Hervorhebung hier.

363 Vgl. Art. 6 Abs. 4 S. 2, 3 der Stellungnahme des EP in Dok. P8_TA-PROV(2019)0421.

relativ simpel; insbesondere das präventive Grundkonzept bleibt erhalten: Sobald ein Diensteanbieter zwei behördliche Anordnungen erhalten hat, terroristische Inhalte zu entfernen, kann er in der Regel von der zuständigen Behörde „als terroristischen Inhalten ausgesetzt“ verbeschrieben werden.³⁶⁴ Diese förmliche Feststellung verpflichtet ihn dann dazu, „spezifische Maßnahmen [zu ergreifen], um zu verhindern, dass über seine Dienste terroristische Inhalte öffentlich verbreitet werden.“³⁶⁵ Für uns relevant ist das, weil zu diesen spezifischen Maßnahmen ausdrücklich auch „technische Mittel [zählen], um terroristische Inhalte zu *ermitteln* und *unverzüglich zu entfernen* oder den Zugang dazu zu sperren.“³⁶⁶ Allerdings „entscheidet [der Hostinganbieter] selbst über die zu treffenden spezifischen Maßnahmen“³⁶⁷ und es ist der zuständigen Behörde, welche die Geeignetheit und Adäquanz der ergriffenen Maßnahmen beurteilen darf und muss, *verwehrt*, spezifisch die Verwendung „automatisierter Verfahren“ anzuordnen.³⁶⁸ Kurz: der Diensteanbieter darf,³⁶⁹ muss aber nicht automatisierte Verfahren der Inhalterkennung und -löschung/-sperrung nutzen, *sofern* er eben andere geeignete „spezifische Maßnahmen“ ergreifen kann. Hierzu zählt die Verordnung *Flagging*-Mechanismen für Nutzer der Dienste, „weitere Mechanismen zur stärkeren Sensibilisierung für terroristische Inhalte“, und „jedwede andere Maßnahme, die der Hostingdiensteanbieter für geeignet hält, um gegen die Verfügbarkeit terroristischer Inhalte“ vorzugehen.³⁷⁰

Ob diese Maßnahmen ausreichen, um die Terror-Kommunikation „wirksam einzudämmen“³⁷¹, *ohne* auf die „automatisierten Verfahren“ zurückzugreifen, wird die Praxis erweisen müssen. Zu erinnern ist freilich daran, dass der EuGH in seiner *Cyando*-Entscheidung den Einsatz von Inhaltserkennungstechnologien zum Schutz von Urheberrechten bereits als Teil der „üblichen Sorgfalt von Wirtschaftsteilnehmern“ qualifiziert hat.³⁷² 169

Bei aller scheinbaren Gemeinsamkeit oder zumindest Konsequenz der genannten Urteile und Gesetzgebungsvorhaben – Konsequenz im Sinne von: vorsichtige Verschiebung von der *ex-post*-Kommunikationskontrolle in Richtung *präventiv-verhindernder* Verfahren –, bei all dieser *verfahrensmäßigen* Konsequenz also ist auf einen wichtigen *qualitativen* Unterschied hinzuweisen: Während der EuGH in *Glawisch-nig* großen Wert darauf legte, dass die Filterpflichten der Hosting-Anbieter diese nicht in die Position bringen dürfen, eine „autonome Beurteilung“ über die Ehr- 170

364 Vgl. Art. 5 Abs. 4 TCO-VO (EU) 2021/784.

365 Art. 5 Abs. 2 UAbs. 1 TCO-VO (EU) 2021/784.

366 Art. 5 Abs. 2 UAbs. 2 S. 2 lit. a TCO-VO (EU) 2021/784. Hervorhebungen hier.

367 Art. 5 Abs. 2 UAbs. 2 S. 1, auch Abs. 6 UAbs. 2 TCO-VO (EU) 2021/784.

368 Art. 5 Abs. 8 UAbs. 2 TCO-VO (EU) 2021/784.

369 Vgl. i. d. S. auch nochmals nachdrücklich ErwGr. 25 zur TCO-VO (EU) 2021/784.

370 Art. 5 Abs. 2 UAbs. 2 S. 2 lit. b bis d TCO-VO (EU) 2021/784.

371 So die Maßgabe von Art. 5 Abs. 3 lit. a TCO-VO (EU) 2021/784.

372 s. soeben, → § 2 Rn. 162.

widrigkeit einer Aussage vornehmen zu müssen,³⁷³ und während im Urheberrecht immerhin der Schutzgegenstand noch relativ klar umrissen ist,³⁷⁴ beziehen sich die durch die TCO-VO aufgestellten proaktiven Filter-„Obliegenheiten“ gegen „terroristische Inhalte“³⁷⁵ auf hochgradig auslegungs- und kontextualisierungsbedürftige Informationen/Daten. Ohne eine aktiv abwägende Rolle der Diensteanbieter wird es hier nicht gehen. Das erklärt, warum die Verordnung die Diensteanbieter (!) außerordentlich wortreich auf die Berücksichtigung der Meinungsfreiheit und sonstigen „Grundrechte der Nutzer“ festlegt,³⁷⁶ und warum sie eine „menschliche Beaufsichtigung und Überprüfung“ der automatisierten Verfahren fordert, „um für Genauigkeit zu sorgen und zu verhindern, dass Materialien entfernt werden, bei denen es sich nicht um terroristische Inhalte handelt.“³⁷⁷ Konsequenterweise sieht die Verordnung dann auch nicht nur die Möglichkeit von gerichtlichem Rechtsschutz gegen Löscho- und Sperrentscheidungen vor,³⁷⁸ sondern verlangt den Diensteanbietern die Einrichtung interner Beschwerdemechanismen ab.³⁷⁹

- 171 f. *Perspektive Digital Services Act: weitere Impulse in Richtung präventiver Rechtskontrolle mit allgemeiner Reichweite.* Abschließend soll die Betrachtung noch einmal vom Speziellen zurück ins Allgemeine/Horizontale geweitet werden. Damit kommt die Nachfolgeregelung für Art. 14 E-Commerce-RL im *Digital Services Act* in den Blick. Wie schon gesagt greift der DSA mit seinem zentralen Art. 6 [Hosting] das *Notice-and-take-down*-Konzept von Art. 14 E-Commerce-RL *prima facie* erneut auf:³⁸⁰

„(1) Bei der Durchführung eines Dienstes der Informationsgesellschaft, der in der Speicherung der von einem Nutzer bereitgestellten Informationen besteht, haftet der Diensteanbieter nicht für die im Auftrag eines Nutzers gespeicherten Informationen, sofern er

373 Vgl. oben, → § 2 Rn. 155.

374 Die Urheber müssen diese Information selbst bereitstellen, die Hostingdiensteanbieter m. a. W. insofern nicht aktiv suchen, vgl. Art. 17 Abs. 4 lit. b DSM-RL (EU) 2019/790. Damit ist nicht in Abrede gestellt, dass die urheberrechtlichen Ausnahmetatbestände (Satire etc.) dann wiederum sehr wohl kontextsensibel sind.

375 s. zur Legaldefinition – unter Rückgriff auf diverse Straftatbestände, was immerhin der Rechtssicherheit dient – Art. 2 Nr. 7 TCO-VO (EU) 2021/784.

376 Art. 5 Abs. 1 UAbs. 2 TCO-VO (EU) 2021/784.

377 Art. 5 Abs. 3 UAbs. 2 TCO-VO (EU) 2021/784. Dieser letzte Unterabsatz enthält natürlich eine gewisse Auslegungsunsicherheit: Ich gehe hier mit Blick auf den Wortlaut von Art. 5 Abs. 2 lit. a TCO-VO (EU) 2021/784 davon aus („technische Mittel, um zu ermitteln und unverzüglich zu entfernen“), dass diese „menschliche Überprüfung“ nicht in jedem Einzelfall gefordert wird, sondern sich auf die verwendete Technologie bezieht, z. B. durch Stichprobenkontrollen. Das kann man im Interesse des Grundrechtsschutzes auch anders auslegen, d. h. unter Verweis auf das nur „Unverzüglich“ eine menschliche Überprüfung in jedem Einzelfall fordern. Dass das praktikabel wäre, bezweifle ich. Folgt man dennoch der restriktiven Auslegung, dann wäre Art. 5 TCO-VO (EU) 2021/784 kein Bsp. für eine rein KI-basierte *Impossibility Structure*, sondern für staatlich angeregte *Intelligent Surveillance* (= „ermitteln“), mit menschlicher Freigabe des anschließenden Einsatzes einer Verhinderungsstruktur.

378 Art. 9 TCO-VO (EU) 2021/784.

379 Art. 10 TCO-VO (EU) 2021/784.

380 Statt vieler dazu Janal, ZEuP 2021, 227 (244 ff.) m. w. N.

a) keine tatsächliche Kenntnis von einer rechtswidrigen Tätigkeit oder illegalen Inhalten hat und sich in Bezug auf Schadensersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder illegale Inhalte offensichtlich werden, oder

b) sobald er diese Kenntnis oder dieses Bewusstsein erlangt, zügig tätig wird, um den Zugang zu den illegalen Inhalten zu sperren oder diese zu entfernen.“

Wie wir gesehen haben, hat die jüngere Rechtsprechung des EuGH die ganz ähnlich lautende Vorgängervorschrift im Bereich der öffentlichen Online-Kommunikation Stück für Stück ins Präventiv-Hindernde gewendet – also hin zu *Impossibility Structures* nach hiesiger Konzeption. Bei genauem Hinsehen konsolidiert der DSA diesen Trend und hebt ihn vor allem über die sektoriellen Ausprägungen im Ehrschutz, Urheberrecht und der Terrorismus-Bekämpfung hinaus auf die horizontale regulatorische Ebene:

Erstens verweist der Kommissionsvorschlag ausdrücklich auf die Rechtssache *Glawischnig*,³⁸¹ und damit auf das Modell des *Notice-and-stay-down*, das die Anordnung einer Filterpflicht auch für *sinngleiche* Rechtsverletzungen erlaubt, *sobald* die ‚Initi-
altat‘ behördlich oder gerichtlich festgestellt ist.³⁸² Die damit in der Rechtsprechung begonnene Verschiebung der Dogmatik ins Präventiv-Hindernde wird somit *allgemein* konsolidiert, selbst wenn Art. 8 DSA in der Nachfolge von Art. 15 E-Commerce-RL weiterhin behauptet,³⁸³ dass eine „allgemeine Verpflichtung zur Überwachung oder aktiven Nachforschung“ den Diensteanbietern nicht auferlegt werden dürfe.

Zweitens spricht einiges dafür, dass der DSA auch die in *Cyando* entwickelte Definition der „aktiven Rolle“ eines Diensteanbieters verfestigen könnte. Zur Erinnerung: eine aktive Rolle führt zum *Wegfall* des Haftungsprivilegs. Und eine aktive Rolle kann, so lässt sich die verschachtelte Argumentation des EuGH deuten,³⁸⁴ dann vorliegen, wenn ein Anbieter *keine* „geeigneten technischen Maßnahmen“ zur Erkennung rechtswidriger Inhalte einsetzt, obwohl das der „üblichen Sorgfalt“ der konkreten Branche entspricht. Der EuGH hat damit für die Frage der „aktiven Rolle“ also ein wertend festzustellendes Kennen-Müssen von im *Allgemeinen* (!) durch die Nutzer begangenen Rechtsverletzungen der Kenntnis von konkreten Rechtsverletzungen gleichgesetzt.³⁸⁵ Der DSA benennt die für die Plattform negati-

381 Dazu soeben, → § 2 Rn. 153.

382 s. COM(2020) 825 final v. 15.12.2020, S. 4, in/bei Fn. 8: „Solche Anordnungen [an Diensteanbieter, gegen ‚bestimmte spezifische Inhalte‘ vorzugehen], insbesondere wenn sie den Anbieter verpflichten, das erneute Auftreten illegaler Inhalte zu verhindern, müssen im Einklang mit dem Unionsrecht, insbesondere mit dem Verbot der Auferlegung allgemeiner Überwachungspflichten, in der Auslegung durch den Gerichtshof der Europäischen Union [z. B. Urt. v. 3. Oktober 2019, Glawischnig-Piesczek (C-18/18)], erlassen werden.“

383 Dazu, dass *Glawischnig* durchaus als Zulassung der Auferlegung einer allg. Überwachungspflicht verstanden werden könnte, s. soeben, bei/in → § 2 Fn. 338.

384 s. oben, → § 2 Rn. 162.

385 Vgl. nochmals oben, → § 2 Rn. 161.

ven Folgen einer „aktiven Rolle“ in Erwägungsgrund 18³⁸⁶, indem er für die Geltung des Haftungsprivilegs ausdrücklich eine „neutrale“ Rolle verlangt. Nachdem der DSA in der finalen Fassung *nach* dem Urteil in *Cyando* verabschiedet wurde, ist davon auszugehen, dass die Rechtsprechung des EuGH bekannt war und damit als legislativ bestätigt gelten kann.

- 175 Noch nicht abschließend beurteilt werden kann hier *drittens* die Frage, ob der DSA über den *indirekten* haftungsrechtlichen Weg hinausgehend sogar eine *direkte* Rechtspflicht zum Einsatz von Filter- oder ähnlichen Technologien enthalten könnte. Auf den ersten Blick tut er das nicht; er privilegiert lediglich deren *freiwilligen* Einsatz (siehe sogleich). Allerdings wird insoweit noch der praktische und anschließend auch aufsichtsbehördliche Umgang mit Art. 20 DSA genau zu beobachten sein. Die Norm verpflichtet solche Hosting-Diensteanbieter, die „Online-Plattformen“ im Sinn der Verordnung sind,³⁸⁷ ein internes Beschwerdeverfahren einerseits *gegen* (vermeintlich) unberechtigte *Sperrungen* vorzuhalten. Andererseits – umgekehrt – werden die Anbieter nach Art. 20 Abs. 4 aber auch verpflichtet, *rechtswidrige* Inhalte *zu sperren*, und zwar „in dem Umfang, der angesichts des gemeldeten Inhalts angemessen ist (vgl. ErwG 58 S. 4)“³⁸⁸ Bedenkt man, was der Gerichtshof im Rahmen seiner *Glawischnig*-Rechtsprechung für angemessen hielt (= auch proaktive Sperrung von *sinngleichen* Inhalten),³⁸⁹ könnte sich hier ein weiterer, rechtsverbindlicher und vor allem durch die Aufsichtsbehörden durchsetzbarer Motor für den Einsatz von *Impossibility Structures* verborgen halten.
- 176 Keinerlei Unsicherheiten lässt der DSA *viertens* daran aufkommen, dass „freiwillige Untersuchungen oder andere Tätigkeiten zur Erkennung, Feststellung und Entfernung illegaler Inhalte oder zur Sperrung des Zugangs zu illegalen Inhalten“ von Seiten der Hosting-Diensteanbieter (auch sogenannte *Content Moderation*) *nicht* zum Wegfall des Haftungsprivilegs führen sollen, sie also *keine* (für die Plattformen unerfreuliche) „aktive Rolle“ begründen (Art. 7 DSA). Die Frage war in der Literatur längere Zeit umstritten,³⁹⁰ wurde vom EuGH in *Cyando* dann aber nega-

386 Der ErwGr. lautet: „¹Die in dieser Verordnung festgelegten Haftungsausschlüsse sollten nicht gelten, wenn der Anbieter sich nicht darauf beschränkt, die Dienstleistungen auf neutrale Weise und durch die bloße technische und automatische Verarbeitung der vom Nutzer bereitgestellten Informationen zu erbringen, sondern dahingehend eine aktive Rolle einnimmt, dass er Wissen oder Kontrolle über diese Informationen erhält. ²Diese Ausschlüsse sollten dementsprechend nicht für die Haftung im Zusammenhang mit Informationen gelten, die nicht vom Nutzer bereitgestellt werden, sondern vom Anbieter des Vermittlungsdienstes selbst, auch wenn diese Informationen im Rahmen der redaktionellen Verantwortung dieses Anbieters entwickelt wurden.“

387 Art. 3 lit. i DSA; und sofern nicht die Bereichsausnahme für Kleinst- und Kleinunternehmen in Art. 19 greift.

388 *Raue*, in: Hofmann/Raue (Hg.), NK-DSA, 2023, Art. 20 Rn. 70.

389 Letztlich maßgeblich ist hier die materielle nationale (!) Haftungsnorm, s. *Raue*, in: Hofmann/Raue (Hg.), NK-DSA, 2023, Art. 20 Rn. 69. Viele Fragen zum Zusammenspiel von DSA und nationalem Recht sind noch offen, vgl. dazu *Rademacher*, a. a. O., Art. 56 Rn. 5.

390 s. *Hofmann*, in: ders./Raue (Hg.), NK-DSA, 2023, Art. 7 Rn. 1, 4 f. m. w. N.

tiv beantwortet – also im Sinn der haftungsrechtlich *unschädlichen* Zulässigkeit eigeninitiativer Filterung der Diensteanbieter nach rechtswidrigen Inhalten unter Art. 14 E-Commerce-RL.³⁹¹ Die sogenannte „Gute-Samariter“-Klausel des Art. 7 DSA schreibt dies nunmehr auch positiv-rechtlich eindeutig fest.

Der DSA geht in der Hinwendung zu Filtertechnologien also nicht so weit voran wie 177 die TCO-VO zur Bekämpfung von terroristischen Online-Inhalten. Aber dennoch enthält er Einzelelemente, die den Eindruck einer vorsichtig-tastenden, aber kontinuierlichen Bewegung hin zum Präventiv-Hindernden bei der Bekämpfung rechtswidriger Online-Kommunikation auch auf einer allgemeinen Ebene bestätigen.³⁹²

3. ... im Datenschutzrecht

Eine ausdrückliche gesetzgeberische Einforderung von *Impossibility Structures* findet sich an einer in diesem Zusammenhang bislang weitgehend übersehenen Stelle, die aber potentiell extrem wirkmächtig sein kann. Gemeint ist Art. 25 Abs. 1 DSGVO mit seiner Forderung nach „Datenschutz durch Technikgestaltung“, oder, dem hiesigen Sprachgebrauch nahekommend: nach *Data Protection by Design* in der englischen Fassung.³⁹³ Datenverarbeiter müssen demnach – unter dem Vorbehalt des technisch Möglichen und ökonomisch Zumutbaren³⁹⁴ –

„geeignete technische und organisatorische Maßnahmen [treffen], die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung *wirksam umzusetzen* und die notwendigen Garantien in die Verarbeitung aufzunehmen, *um den Anforderungen dieser Verordnung zu genügen* und die Rechte der betroffenen Personen zu schützen“ (Hervorhebung hier).

Marit Hansen stellt zutreffend fest, dass „Art. 25 [damit] *unter einer gestalterischen und operativen Perspektive zu der umfassendsten Norm der DSGVO* [wird], denn sie verweist auf die zentralen Datenschutzgrundsätze in Art. 5 und auf die Verordnung 179

391 EuGH, Urt. v. 22.6.2021, verb. Rs. C-682/18 und C-683/18 (Peterson/Google und Elsevier/Cyando) = GRUR 2021, 1054 Rn.109.

392 Hierzu, mit weiteren Anhaltspunkten aus dem DSA, weiterführend J.-P. Schneider, in: Ruffert (Hg.), Die Regulierung digitaler Plattformen, 2023, S. 105 (128 ff., bes. 134 ff.).

393 Vgl. auch, für das Recht auf Vergessenwerden, Art. 17 Abs. 2 DSGVO: „Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.“ Freilich beschränkt sich Art. 17 Abs. 2 DSGVO auf die technische Umsetzung einer Informationspflicht, geht also in Richtung der hier sog. *Compliance Assistance Technologies*, → S. 182 ff.

394 s. Hs. 1 von Art. 25 Abs. 1 DSGVO: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche [...] Maßnahmen [...]“

selbst³⁹⁵ und verlangt technische Vorrichtungen, die „den Verantwortlichen in der Erfüllung seiner Pflichten [unterstützen] und [...] Verstöße oder Fehler bezüglich der Verarbeitung [erschweren].“³⁹⁶ Kurz: Art. 25 Abs. 1 verlangt, die DSGVO insgesamt *self-executing* zu machen.³⁹⁷

- 180 Eine Umsetzung dieses Gebots³⁹⁸ wäre etwa denkbar in Form von möglichst manipulationssicher getaggtten Datensätzen, sodass diese nicht mehr zweckwidrig verwendet werden könnten (= Datenschutzgrundsatz der Zweckbindung, Art. 5 Abs. 1 lit. b DSGVO), oder in Form von automatisierten Meldungen von Datenschutz- und Persönlichkeitsrechtsverletzungen an Betroffene ohne eigenständige Veranlassung durch den Meldepflichtigen (Art. 34 DSGVO), dem dadurch eine Unterlassungsmöglichkeit entzogen werden würde.³⁹⁹ Mit diesen Beispielen sind beide Dimensionen von *Impossibility Structures* abgedeckt: die Verunmöglichung, rechtswidrig zu handeln, wie auch die Verunmöglichung, rechtswidrig *nicht* zu handeln.
- 181 Die Aufgabe von KI wäre es dabei, gesetzeskonforme Verwendungszwecke von unzulässigen zu unterscheiden: „The infrastructure will have to be engineered and organized in a way that is conducive to actions and behaviors that are compatible with the law.“⁴⁰⁰ Die Rede ist treffend von einer „Datenschutz-KI“,⁴⁰¹ die perspektivisch sogar in Form dezidierter Datenschutz-KI-Agenten denkbar wäre, die systemweit (in einem Unternehmen, einer Behörde, ‚dem Staat‘) kontinuierlich nach Datenschutzverstößen suchen und diese sogar verhindern können müssten. Datenleaks, wie sie 2020 bei der hessischen Polizei im Zusammenhang mit den NSU-2.0-Drohbriefen vorkamen, könnten auf diese Weise technisch verunmöglicht werden. Das wäre etwa auch ein Einsatzszenario, das der von *Ralf Poscher* geforderten reflexiven Dimension

395 Hansen, in: Simitis/Hornung/Spiecker gen. Döhmman (Hg.), Datenschutzrecht, ²2025, Art. 25 DSGVO Rn. 15, Hervorhebung im Original.

396 Ibid., Rn. 17.

397 Bygrave, in: Yeung/Lodge (Hg.), Algorithmic Regulation, 2019, S. 248 (256 f.).

398 Dazu allg. Hansen, in: Simitis/Hornung/Spiecker gen. Döhmman (Hg.), Datenschutzrecht, ²2025, Art. 25 DSGVO Rn. 16 m. w. N. Ein vernichtendes Urteil über den Stand der Umsetzung, zurückzuführen auf fehlende Kommunikation zwischen Juristen und Technikern, findet sich bei Denga/Pohle/Hölzel, RW 11 (2020), 420 (434 ff.).

399 Beide Bsp. nach Martini, in: Paal/Pauly (Hg.), DS-GVO, ³2021, Art. 25 Rn. 30 bzw. 33 m. w. N. Die beschriebene Kombination aus Meldepflicht + *by-design*-Anordnung führt nach hiesiger Konzeption zu einer Form von *Intelligent Surveillance*, die *by-design*-Anordnung ist hinsichtlich der Meldepflicht selbst *Impossibility Structure*.

400 Hildebrandt, Smart Technologies and the End(s) of Law, 2016, S. 219; zustimmend Unger, in: ders./Ungern-Sternberg (Hg.), Demokratie und künstliche Intelligenz, 2019, S. 113 (127 f.). Auf den ersten Blick irritierend folgt bei Hildebrandt a. a. O. dann die Einschätzung, "[t]his is not a matter of nudging people into compliance; it is not a matter of techno-regulation." Die Aussage ergibt nur dann und deshalb Sinn, wenn man klar zwischen *Law by Design* und *Nudging/Techno Regulation* unterscheidet; s. dazu auch → § 2 Rn. 478.

401 So Rost, DuD 2018, 558 (560). Vgl. auch Guckelberger, Öffentliche Verwaltung im Zeitalter der Digitalisierung, 2019, Rn. 591. Für eine – allerdings alte – Studie (2006) zur Automatisierung des Gesundheitsdatenschutts in den USA s. Pasquale, George Washington Law Rev. 87 (2019), 1 (19 ff.).

von Überwachung⁴⁰² entspräche (freilich sogar in verschärfter, weil physisch wirksamer Form).

Von den Verfechtern wird die Verpflichtung des Datenschutzrechts auf *Law by Design* (i. e. *Impossibility Structures*) vor allem als Lösung für bzw. besser: gegen die wahrgenommene „*technological regulation*“ durch privatwirtschaftlich genutzte KI-Agenten angesehen.⁴⁰³ Zu bedenken ist hier freilich, wie weitgreifend das europäische Datenschutzrecht ist:⁴⁰⁴ Es wurde nicht zu Unrecht bereits angemerkt, dass es mit seinem weiten Anwendungsbereich zum *Law of Everything* zu werden drohe,⁴⁰⁵ und kürzlich hat auch der Generalanwalt *Michal Bobek* zur Reichweite der DSGVO festgestellt:

„[1] Die [DSGVO] ist kein Rechtsakt im Kleinform. Ihr weit gefasster Anwendungsbereich, das faktische Aushöhlen jeglicher Ausnahmeregelungen durch die Rechtsprechung sowie der definitionsbasierte, abstrakte und daher eher radikale Auslegungsansatz haben ihren Teil dazu beigetragen, dass die DSGVO eine nahezu grenzenlose Geltung hat. *Heutzutage ist es insoweit mit Schwierigkeiten verbunden, einen Lebenssachverhalt zu nennen, in dem nicht irgendjemand zu irgendeinem Zeitpunkt personenbezogene Daten verarbeitet*“.⁴⁰⁶

Kombiniert man diese Erkenntnis mit Art. 25 Abs. 1 DSGVO wird klar, in welchem weitem Umfang die Norm den Einzug datenschutzrechtserzwingender *Impossibility Structures* im Alltag vorantreiben könnte, *sobald* die entsprechende Technologie verfügbar ist. Gebremst werden dürfte der Einsatz der Technik durch die Entscheidung des DSGVO-Gesetzgebers, als Adressaten von Art. 25 Abs. 1 DSGVO die Datenverarbeiter („Verantwortliche“), nicht hingegen die Anbieter und Hersteller datenverarbeitender Technologien zu bestimmen. Die Norm spielt sozusagen über Bande,⁴⁰⁷ wohl vom Wunsch getrieben, mit der DSGVO kein Produktrecht zu schaffen.⁴⁰⁸

Aber diese Detailfrage einmal außer Acht gelassen: Unterstellt man für den Moment, dass das Datenschutzrecht *sinnvoll* ist, also zwar weit, aber *nicht zu weit* ausgreift, wie *Bobek* annimmt, dann erscheint der Einsatz von *Impossibility Structures* als nachgerade zwingend: Wegen seiner Weite und des fast vollständigen Verzichts auf einigermaßen klare Ausnahmen von seinem Anwendungsbereich, liefert das Datenschutzrecht ein Beispiel für Recht ab, dass zwar eindeutig auf Befolgung angelegt

⁴⁰² s. oben, → § 2 Rn. 20.

⁴⁰³ Vgl. z. B. *Hildebrandt*, *Smart Technologies and the End(s) of Law*, 2016, S. 10 ff.

⁴⁰⁴ Vgl. auch *ibid.*, S. 221.

⁴⁰⁵ s. krit. zu dieser Entwicklung *Purtova*, *Law, Innovation and Technology* 10 (2018), 40.

⁴⁰⁶ Schlussanträge von GA *Bobek* zu Rs. C-175/20 (SIA „SS“/Valsts ierēnēmumu dienests), Rn. 1. Hervorhebung hier.

⁴⁰⁷ Vgl. ErwGr. 78 S. 4 zur DSGVO: „Ermutigung“ der Hersteller, Datenschutz durch Technikgestaltung zu ermöglichen; hierzu *Hansen*, in: *Simitis/Hornung/Spiecker gen. Döhmman* (Hg.), *Datenschutzrecht*, 2025, Art. 25 DSGVO Rn. 20 f. Weitergehend *Specht-Riemenschneider*, *MMR* 2020, 73 ff.: schon *de lege lata* Sachmängel- und Produkthaftung für nicht datenschutzkonform nutzbare IT-Produkte.

⁴⁰⁸ Zur unglücklichen Adressatenwahl näher *Mantz*, in: *Sydow/Marsch* (Hg.), *DS-GVO – BDSG*, 32022, Art. 25 DSGVO Rn. 16 f., 79 ff. m. w. N.

ist (siehe die Sanktionsdrohungen), aber mit menschlich-*individuellem* Können und Begreifen kaum befolgt werden kann (mit Ausnahme von starken Wirtschaftsakteuren vielleicht). Die DSGVO-eigene Forderung nach *Impossibility Structures* in Art. 25 Abs. 1 ist vor diesem Hintergrund der konsequente Schritt, der eine enorme Entlastungsfunktion im Bereich *fahrlässiger Non-Compliance* und im Bereich von Verbotsirrtümern haben kann.

- 185 Hinzuweisen ist abschließend noch darauf, dass sich die Durchschlagskraft von Art. 25 Abs. 1 DSGVO bald massiv erhöhen dürfte. Seine *direkten* Adressaten sind, wie gesagt, bislang nur die für eine Datenverarbeitung *Verantwortlichen*. Das wird sich allerdings ein gutes Stück weit ändern, sobald der *Cyber Resilience Act* der EU ab 11. Dezember 2027 vollständig gilt. Er verpflichtet die Hersteller von Produkten, sobald sie eine digitale Komponente enthalten,

„die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß [zu] beschränken („Datenminimierung“)“⁴⁰⁹

4. ... im Straßenverkehrsrecht

- 186 Wechseln wir nun vom Bereich der digitalen Kommunikation und des ebenfalls vorwiegend digitalen Datenaustauschs in den Bereich der physischen Bewegungen. Damit gerät erneut das selbstfahrende Auto in den Blick. Ein solches wird selbstverständlich in der Lage sein müssen, sich rechtskonform im Straßenverkehr zu bewegen, wird also dazu in der Lage sein müssen, rechtmäßiges von rechtswidrigem Verhalten zu unterscheiden.⁴¹⁰ Es muss, um die oben schon eingeführte Terminologie aufzugreifen, selbst *law abiding* sein können.⁴¹¹

- 187 a. *Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion*. Davon geht auch der Gesetzgeber aus. Zunächst hat dieser mit § 1a Abs. 2 Nr. 2 StVG „Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion“ wie folgt an das geltende Straßenverkehrsrecht gebunden:

„¹Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion im Sinne dieses Gesetzes sind solche, die über eine technische Ausrüstung verfügen, [...] 2. die in der Lage ist, während der hoch- oder vollautomatisierten Fahrzeugsteuerung den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen, [...]“

409 Anhang I, Teil I, Abs. 2 lit. g VO (EU) 2024/2847 des Europäischen Parlaments und des Rates v. 23.10.2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (*Cyber Resilience Act*).

410 Dazu, vor dem Hintergrund des technisch bald Möglichen, auch ausf. *Prakken*, Artificial Intelligence and Law 25 (2017), 341 ff. Zum Umfang der Befolgungspflicht zudem *Will*, NZV 2020, 163 (171), speziell für Spurhaltesysteme. Zum Verhältnis der nationalen, unionalen und völkerrechtlichen Zulassungsregeln ausf. *Weise*, Hochautomatisiertes Fahren in Deutschland und Kalifornien, 2022, S. 56 ff.

411 Zu diesem Querschnittsbegriff schon oben, → § 1 Rn. 59.

Hier, so könnte man annehmen, spricht wenig dafür, dass der Gesetzgeber es den Automobilherstellern erlauben könnte, Software einzusetzen, die sich vom Nutzer auch dann übersteuern lässt, wenn sie erkennt, dass sich dieser regelwidrig verhalten, also etwa eine rote Ampel 'überfahren' will. Die Überlegung lässt sich freilich noch verschärfen: Was, wenn das Fahrzeug erkennt, dass die Fahrerin mit dem Fahrzeug nicht nur eine rote Ampel, sondern eine Gruppe Passanten am Wegesrand überfahren will?

Gegenwärtig scheint freilich genau das erlaubt bzw. sogar geboten zu sein: Nach § 1a Abs. 2 Nr. 3 StVG muss auch ein „Kraftfahrzeug mit hoch- oder vollautomatisierter Fahrfunktion“ jederzeit von der Fahrerin übersteuerbar sein:

„Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion im Sinne dieses Gesetzes sind solche, die über eine technische Ausrüstung verfügen, [...] 3. die jederzeit durch den Fahrzeugführer manuell übersteuerbar oder deaktivierbar ist [...]“.

Die Software solcher Kraftfahrzeuge darf diese also gegenwärtig gerade *nicht* zu einer *Impossibility Structure* für die Fahrerin machen. Nach § 63a Abs. 1 S. 1 StVG muss ein Kfz mit hochautomatisierter Fahrfunktion lediglich „Positions- und Zeitangaben“ speichern, „wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt“. Auf diese Daten haben die Verkehrsbehörden der Länder sowie eventuell geschädigte Dritte auch ausdrücklich Zugriff, um diese in eventuellen Buß- oder Strafverfahren bzw. Rechtsstreitigkeiten gegen den Halter/Fahrer zu verwenden (siehe § 63a Abs. 2, 3 StVG); allerdings nur auf ihr Verlangen, sodass hier auch keine Form einer *Intelligent Surveillance* vorliegt.

b. Kraftfahrzeuge mit autonomer Fahrfunktion. Nochmal anders verhält es sich nun mit den noch relativ frisch eingeführten §§ 1d bis 1l StVG, die das *autonome* Fahren als Regelverkehr regeln und zulassen, zunächst für bestimmte und von den zuständigen Landesbehörden zu genehmigende Betriebsbereiche.⁴¹² Das autonome Fahren ist dadurch definiert, dass es eine „fahrzeugführende Person“ nicht mehr zu geben braucht (§ 1a Abs. 1 Nr. 1 StVG). Dementsprechend muss erst recht das autonome Fahrzeug „in der Lage [sein], [...] selbständig die an die Fahrzeugführung gerichteten Verkehrsvorschriften einzuhalten“ (§ 1e Abs. 2 Nr. 2 StVG) und muss sich „selbständig in einen risikominimalen Zustand⁴¹³ [...] versetzen [können], wenn die

412 s. § 1d Abs. 2 StVG. Wegen dieses nur beschränkten Einsatzgebiets ordnet der Gesetzesentwurf das mit § 1d ff. StVG geschaffene Regelwerk „nur“ der Stufe 4 der SAE-Klassifikation zu (s. BR-Drs. 155/21 v. 12.2.2021, S. 1). Hilgendorf, JZ 2021, 444 (445) spricht von „beschränkt autonomen“ Fahrfunktionen.

413 Definiert in § 1d Abs. 4 StVG als „ein Zustand, in den sich das Kraftfahrzeug mit autonomer Fahrfunktion auf eigene Veranlassung oder auf Veranlassung der Technischen Aufsicht selbständig versetzt, um unter angemessener Beachtung der Verkehrssituation die größtmögliche Verkehrssicherheit für andere Verkehrsteilnehmende und Dritte zu gewährleisten.“

Fortsetzung der Fahrt nur durch eine Verletzung des Straßenverkehrsrechts möglich wäre“ (§ 1e Abs. 2 Nr. 3 StVG).

- 192 Ganz ohne menschliche Interventionsmöglichkeit bleibt das Fahrzeug aber nicht: Vorgesehen ist eine natürliche (!) Person als „Technische Aufsicht“ (§ 1d Abs. 3, § 1e Abs. 2 Nr. 4 StVG),⁴¹⁴ die das Fahrzeug, wenn es sich in den risikominimalen Zustand versetzt hat, wieder in Betrieb setzen und die Fahrmanöver freigeben bzw. anweisen kann, gerade auch für den Fall, dass ein Fahrmanöver gegen Recht verstoßen sollte.⁴¹⁵ Das ist zunächst einmal eine technisch, organisatorisch und haftungsrechtlich⁴¹⁶ anspruchsvolle, aber dennoch *konzeptionell* simple telematische Struktur: Es handelt sich um eine Möglichkeit der Fernsteuerung, wie sie z. B. von Drohnen oder Schienenfahrzeugen bekannt ist.⁴¹⁷
- 193 Für uns interessant ist die sozusagen als doppelter Boden eingebaute *Impossibility Structure*, die mit der Technischen Aufsicht verknüpft ist: Denn wenngleich also eine Übersteuerungsmöglichkeit gegen das Straßenverkehrsrecht ausdrücklich vorgesehen ist, so sieht § 1e Abs. 2 Nr. 5 StVG wiederum einschränkend vor, dass das Fahrzeug „ein von der Technischen Aufsicht vorgegebenes Fahrmanöver zu überprüfen und dieses nicht auszuführen [hat], [...] wenn das Fahrmanöver am Verkehr teilnehmende oder unbeteiligte Personen gefährden würde“. Hierzu die Feststellung von *Eric Hilgendorf*:

„Auch wenn davon auszugehen ist, dass bei der Formulierung der Vorgaben des § 1e Abs. 2 [StVG] technischer Sachverstand aus den Laboren der Hersteller eingeflossen ist, erscheinen doch die Anforderungen, die [das Gesetz] an die Ingenieurskunst stellt, gewaltig. [...] | [D]as gestufte Entscheidungsmodell [des § 1e Abs. 2 Nr. 5 StVG] setzt voraus, dass die technische Ausrüstung des Fahrzeugs die konkrete Gefahrenlage relativ genau einschätzen kann.“⁴¹⁸

- 194 *c. Inkurs: Überwachungsleistungen solcher Kraftfahrzeuge.* Gerade im Zusammenhang mit den bestehenden Unsicherheiten über die technische Leistungsfähigkeit der Systeme ist auf § 1g StVG hinzuweisen. Er verpflichtet die Halter von Kfz mit autonomen Funktionen zu umfangreichen Datensammlungen (und verpflichtet die

414 *Hilgendorf*, JZ 2021, 444 (453), weist zutreffend darauf hin, dass eine nat. Person mit den telematischen Aufgaben als Technische Aufsicht überfordert sein dürfte, ohne *ihrerseits* auf KI-Unterstützung zurückzugreifen. Das Gesetz geht zwar davon aus, dass den Menschen die alleinige Verantwortung trifft (*Hilgendorf*, a. a. O.), lässt aber mit § 1e Abs. 2 Nr. 5 StVG – dem hier sog. doppelten Boden – durchaus Zweifel daran erkennen, ob auf die Technische Aufsicht allein Verlass sein soll. Sorgfaltsmaßstäbe, die das hybride Arrangement fair erfassen können, werden sich erst entwickeln müssen.

415 s. § 1e Nr. 4 i. V. m. § 1d Abs. 3 StVG, wonach die Technische Aufsicht spezifisch für den Fall der Nicht-Weiterfahrt wegen drohenden Verstoßes gegen Straßenverkehrsrecht (Fall des § 1e Abs. 2 Nr. 3 StVG) „Fahrmanöver freigeben kann“ bzw. können muss. Als Bsp. nennt *Hilgendorf*, JZ 2021, 444 (448), das Überfahren einer wegen eines Defekts dauerhaft auf „rot“ gestellten Ampel. Zu weiteren Pflichten der Technischen Aufsicht a. a. O., S. 451.

416 Hierzu in einem ersten Ansatz *Hilgendorf*, JZ 2021, 444, (452 ff.).

417 s. dazu ausf. *ibid.*, S. 446.

418 *Ibid.*, S. 447 f.

Hersteller dazu, solche zu ermöglichen⁴¹⁹). Dazu zählen neben Identifikationsdaten unter anderem Positions- und Umweltdaten, vor allem aber die Daten über „Anzahl und Zeiten der Freigabe von alternativen Fahrmanövern“ durch die Technische Aufsicht (vgl. § 1g Abs. 1 StVG). Gespeichert werden muss⁴²⁰ „bei Eingriffen durch die Technische Aufsicht“, „bei Konfliktszenarien, insbesondere bei Unfällen und Fast-Unfall-Szenarien“, „bei nicht planmäßigem Spurwechsel und Ausweichen“, sowie ganz allgemein „bei Störungen im Betriebsablauf“ (§ 1g Abs. 2 StVG). Gerade bei *prima-facie*-Rechtsverstößen, wie dem von der Technischen Aufsicht anzuordnenden Überfahren einer ununterbrochenen Linie, wird folglich zu speichern sein.⁴²¹

Zugriff auf diese Daten haben

195

- das Kraftfahrt-Bundesamt, unter anderem zu Aufsichts-, aber auch zu Forschungszwecken (einschließlich Weitergabe der Daten in anonymisierter Form an Universitäten und Forschungsstellen, vgl. § 1g Abs. 4, 5 StVG),
- die nach Landes- oder Bundesrecht zur Ausweisung von Gebieten, in denen autonome Fahrzeuge verkehren dürfen, zuständige Behörde (§ 1g Abs. 6 StVG), und
- „Dritte“, soweit das zur Durchsetzung von Rechtsansprüchen erforderlich ist, die im Zusammenhang mit dem Betrieb des Kfz mit autonomen Fahrfunktionen stehen (§ 1g Abs. 7 StVG).

d. *Freiwilliger Einbau von Impossibility Structures durch die Kfz-Hersteller und der Einsatz jenseits von Kraftfahrzeugen.* Zu bedenken ist noch, dass die Vorgaben von § 1a und §§ 1d f. StVG nur hinsichtlich der hoch- oder vollautomatisierten bzw. autonomen Fahrfunktionen gelten; nichts ist hier darüber ausgesagt, ob Fahrzeughersteller nicht punktuell noch zusätzlich *Impossibility Structures* verbauen dürfen. So hat etwa der Hersteller *Volvo* schon sehr früh angekündigt, dass seine Fahrzeuge die Fahrzeugführer künftig per Gesichtserkennung daraufhin überprüfen sollen, ob sie Alkohol getrunken haben. Die Folge wäre, dass der Motor gegebenenfalls nicht anspringt.⁴²² Auch sollen die Autos künftig vor Kindergärten automatisch und ohne Möglichkeit der Übersteuerung auf die zulässige Schrittgeschwindigkeit abbremesen. *Volvo* sieht den Einsatz solcher *Impossibility Structures* dabei nicht nur als sein

196

419 s. ausdr. § 1g Abs. 3 StVG.

420 Ganz eindeutig ist die Norm hier nicht: Nach § 1g Abs. 1 StVG muss anscheinend stets gespeichert werden, nach Absatz 2 nur in den sogleich genannten Fällen; vgl. zu dieser Unsicherheit auch Hilgendorf, JZ 2021, 444 (454), dort Fn. 101: „noch zu klären [...], ob die in § 1g StVG-E angesprochenen Daten fortlaufend oder nur ereignisbezogen abgespeichert werden müssen.“

421 Mit diesem Bsp. BR-Drs. 155/21 v. 12.2.2021, S. 28.

422 Dafür, dass eine solche *Impossibility Structure* bald vorgeschrieben werden könnte, spricht Art. 6 Abs. 1 lit. b VO (EU) 2019/2144, dazu auch unten, → § 2 Rn. 287.

„Recht“, sondern sogar als seine – wohl moralisch verstandene – „Verpflichtung“ an.⁴²³

- 197 Im Einsatz, wenn auch in kleinerem Maßstab, finden sich *Impossibility Structures* schon bei den sogenannten E-Scootern, die seit 2019 auch in Deutschland genutzt werden dürfen und sich rasch zu einer Gefahrenquelle im Straßenverkehr entwickelt haben. Die Stadt Frankfurt wies die privaten Anbieter der Scooter deshalb an, die Geschwindigkeit der Roller von den grundsätzlich möglichen 20 km/h automatisch auf maximal 5 km/h zu drosseln, sobald diese in städtische Parks einfahren (*Geofencing*⁴²⁴).⁴²⁵ Im Ausland finden sich noch umfangreichere Vorgaben: So plant Melbourne (Australien), wo die Nutzung von E-Scootern besonders hoch ist, nicht nur die auch aus Frankfurt bekannten Langsamfahrzonen automatisiert durchzusetzen. Man will zudem technisch dafür Sorge tragen, dass eine Fahrt (bzw. die Miete des Scooters) abrechnungstechnisch nur beendet werden kann, wenn der E-Scooter regelkonform abgestellt ist. Auch ein Alkohol-Erkennungssystem ist geplant und Nutzer sollen von dem E-Scooter „angeschrien“ werden (vornehmer ausgedrückt: sie sollen den Nutzer im Wortsinn zurechtweisen), falls sie ihn fehlerhaft nutzen.⁴²⁶

5. ... im Technikrecht allgemein? Ein futuristisches Gedankenexperiment um robotische Haushalts- und Servicehilfen

- 198 Die Entwicklung von humanoiden Haushalts- und Servicerobotern („Robobutlern“) hatte in den vergangenen Jahren zunächst einige Rückschläge erlitten,⁴²⁷ bevor sie nun – Stand 2025 – wieder deutlich an Fahrt aufzunehmen scheint. Unabhängig davon, wie lange die Entwicklung noch tatsächlich dauern wird, dürfte es jedenfalls nicht utopisch, sondern „nur“ futuristisch sein anzunehmen, dass robotische Haushalts- und Servicehilfen in den kommenden Jahren vielerorts Einzug halten werden.

423 Zitiert nach Maak, F.A.Z. v. 10.3.2019, S. 38.

424 *Geofencing* liegt auch den elektronischen Fußfesseln für entlassene, aber besonders rückfallgefährdete Straftäter zugrunde, s. § 68b Abs. 1 S. 1 Nr. 12 StGB, § 463a Abs. 4 StPO, dazu Baur, ZIS 15 (2020), 275. Freilich schlägt dieses System nur Alarm, wenn eine kontrollierte Person einen unzulässigen Bereich betritt, eine *Impossibility Structure* ist das noch nicht. V. a. setzt sein Einsatz einen bereits stark verdichteten Verdacht gegenüber einer konkreten Person voraus, was diese Form der intelligenten staatlichen Überwachung von den bisher genannten Beispielen deutlich unterscheidet.

425 s. dazu den Bericht von Heunmann, F.A.Z. v. 30.12.2019 (Onlinequelle). Die Stadt habe die Anordnung demnach zwischenzeitlich zurückgenommen. Jedenfalls forderte der *Deutsche Städtetag* eine bundesgesetzliche Grundlage dafür, E-Scooter an „besonders stark besuchten Orte[n] in Städten [...] auf Schrittgeschwindigkeit“ begrenzen zu können, vgl. Pressemitteilung v. 15.6.2020, abrufbar unter <http://www.staedtetag.de/presse/statements/092858/index.html>, besucht am 27.8.2020.

426 s. Barkhausen, H.A.Z. v. 15.8.2023 (Onlinequelle).

427 Zur Ankündigung von Elon Musk, schon 2022 einen Prototypen für einen industriell nutzbaren humanoiden Roboter fertigzustellen, dpa, F.A.Z. v. 23.8.2021, S. 20. Das Unternehmen iRobot ging 2021 ebenfalls davon aus, alsbald „Haushaltsroboter mit Armen“ auf den Markt bringen zu können, vgl. dpa, F.A.Z. v. 10.9.2021, S. 21. Bislang ist es bei Ankündigungen geblieben. Zudem hat das Unternehmen Alphabet seine Forschungsabteilung *Everyday Robots* – deren dezidiertes Ziel die Entwicklung von Haushaltsrobotern mit Armen war – Anfang 2023 geschlossen, vgl. J. Vincent, *The Verge* v. 24.2.2023 (Onlinequelle).

Allein die Bedürfnisse einer alternden Gesellschaft bei gleichzeitigem Mangel an menschlichen Arbeitskräften werden dafür sorgen, dass wir es zumindest in den Industrieländern vermehrt mit ‚Robobutlern‘, Pflege- und Gastrorobotern usw. zu tun haben werden.

Umso mehr fällt auf, dass es im Gegensatz zum Straßenverkehrsrecht bislang keine 199 vergleichbaren Vorschriften für den Haushalts- und Servicebereich gibt. Zumindest in Deutschland ist der Stand des Rechts nach wie vor derjenige des allgemeinen Produktsicherheitsrechts, das im Zuge der Neufassung und Hochstufung der EU-Produkthaftungsrichtlinie und der Maschinenrichtlinie zu Verordnungen immerhin an KI-basierte Produkte und neue Anforderungen an die Cybersicherheit angepasst wurde. Es bleibt hier aber beim eher passiv formulierten Grundsatz des überkommenen Produktsicherheitsrechts, wonach „Wirtschaftsakteure [...] nur sichere Produkte in den Verkehr bringen oder auf dem Markt bereitstellen“ dürfen (so Art. 5 der neuen *General Product Safety Regulation*⁴²⁸).

Die Frage, die mich im Folgenden leiten wird und die ich im Ergebnis vorsichtig 200 bejahen möchte, ist, ob es daneben weitere, versteckte, man könnte vielleicht sagen: tieferliegende Anhaltspunkte dafür gibt, dass das Technikrecht *allgemein* oder doch zumindest für Haushalts- und Serviceroboter *im Speziellen* absehbar Vorgaben enthalten wird, die diese Systeme in großem Umfang zu *Impossibility Structures* machen könnten. Auf die weitere Stärkung der entsprechenden Vorschriften des Datenschutzrechts durch den *Cyber Resilience Act* wurde bereits hingewiesen;⁴²⁹ aber das betrifft eben nur die Einkleidung spezifisch des Datenschutzrechts mit *Impossibility Structures*. Ich möchte hier an zwei andere existierende Normkomplexe anknüpfen, anhand derer ich meine soeben aufgestellte, breiter ansetzende These glaube begründen zu können:

Das sind zum einen die soeben behandelten §§ 1a, 1e StVG. Sie betreffen mit dem 201 Straßenverkehr ein zwar spezielles Feld des Technikrechts, aber immerhin eines, das in der alltäglichen Bedeutung an die Relevanz von Haushalt und Servicebereichen heranreichen dürfte (hierzu sogleich, → a.). Die zweite Norm, die – wahrscheinlich etwas überraschend – auf ihre Aussagekraft für eine mögliche künftige Einführung von *Impossibility Structures* untersucht werden soll, ist § 323c StGB. Dabei geht es freilich nicht um den originär strafrechtlichen, d. h. sanktionenrechtlichen Teil der Norm (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe), sondern um die davor liegende Pflicht zur allgemeinen Hilfeleistung im Unglücksfall (dazu → b.).

428 Die VO (EU) 2023/988 v. 10.5.2023 über die allgemeine Produktsicherheit, zur Änderung der VO (EU) 1025/2012 und der RL (EU) 2020/1828 sowie zur Aufhebung der RL 2001/95/EG und der RL 87/357/EWG [General Product Safety Regulation] gilt gem. Art. 52 Abs. 2 ab dem 13.12.2024.

429 Dazu oben, bei → § 2 Rn. 185.

- 202 a. *Orientierung am Straßenverkehrsrecht*. Es liegt nahe, für das Gedankenexperiment zunächst existierendes Technikrecht heranzuziehen, das bereits Rechtsbefolgungspflichten für robotische Systeme enthält. Das sind die soeben im Detail vorgestellten §§ 1a, 1e StVG aus dem Straßenverkehrsrecht. Hier soll nun hinterfragt werden, ob und inwieweit ihre normativen Gehalte verallgemeinerungsfähig und auf den Kontext von Haushalts- und Servicerobotern übertragbar sind.
- 203 aa. *Pflicht zur allgemeinen Befolgung des situativ geltenden Rechts (hier sog. Law-abiding Technology)*. Zunächst sei daran erinnert, dass der jeweilige Absatz 2 Nr. 2 von §§ 1a und 1e StVG verlangt, dass die hoch- oder vollautomatisierten bzw. autonomen Kraftfahrzeuge allen „an die Fahrzeugführung gerichteten Verkehrsvorschriften“ entsprechen können müssen.⁴³⁰ Das lässt sich dahingehend verallgemeinern, dass auch Haushalts- und Serviceroboter, sobald sie über ein vergleichbar weites Handlungsspektrum verfügen wie autonome Kraftfahrzeuge, zunächst einmal allen Vorschriften entsprechen können müssen, die für *menschliche* Haushalts- und Servicehilfen in der entsprechenden Situation gelten.⁴³¹ Sie müssen *law-abiding* sein.⁴³² Gefordert sind damit *situativ angepasste* Programmierungen. Ohne hier Nachforschungen im Detail anstellen zu können, wird man fest davon ausgehen dürfen, dass für Haushaltshilfen andere Vorschriften und andere Maßstäbe gelten als für Mitarbeiter in Pflegeheimen (z. B. besondere Sorgfaltspflichten bei medizinischen Handlungen) oder für solche im gastronomischen Bereich (z. B. gesteigerte Hygieneanforderungen).
- 204 bb. *Verbot, zum Werkzeug für Gefährdungen zu werden*. Aus § 1e StVG ist sodann dessen Absatz 2 Nrn. 3 bis 5 i. V. mit § 1d Abs. 3 StVG für uns von weiterem Interesse. Die Normen enthalten ein ausdrückliches, zwar etwas kompliziert arrangiertes, aber im Ergebnis einleuchtendes dreistufiges Interaktionsregime für das autonome Kraftfahrzeug mit seiner Umwelt *speziell im Feld der Rechtsbefolgung*.⁴³³ Zur Erinnerung: Die Normen verlangen
- erstens, dass das Fahrzeug sich selbst in „einen risikominimalen Zustand [versetzt], wenn die Fortsetzung der Fahrt nur durch eine Verletzung des Straßenverkehrsrechts möglich wäre“ (§ 1e Abs. 2 Nr. 3 StVG); sie verlangen also, dass das Fahrzeug nicht *selbst* gegen geltendes Recht verstößt;
 - zweitens, dass die „Technische Aufsicht“ (ein Mensch) Fahrmanöver gerade auch dann „freigeben“ können muss, wenn diese vom Fahrzeug gemäß § 1e Abs. 2 Nr. 3

430 s. soeben, → § 2 Rn. 186 ff.

431 Diese Einschätzung mag zunächst selbstverständlich und damit beinahe trivial klingen, hat aber für die Verbreitung von *Impossibility Structures* womöglich weitreichende Konsequenzen; darauf wird unten, ab → S. 256, eingegangen.

432 s. zum Begriff schon oben, → § 1 Rn. 59.

433 s. soeben, ab → S. 146.

StVG wegen drohenden Rechtsverstoßes unterlassen wurden (§ 1d Abs. 3 i. V. mit § 1e Abs. 2 Nr. 4 StVG).

- schließlich, drittens, dass das Fahrzeug „ein von der Technischen Aufsicht vorgegebenes Fahrmanöver zu überprüfen [hat] und dieses nicht aus[]führen [darf], [...] wenn das Fahrmanöver am Verkehr teilnehmende oder unbeteiligte Personen gefährden würde“ (§ 1e Abs. 2 Nr. 5 StVG).

Was lässt sich aus diesem Arrangement für eine mögliche Regulierung von Haushalts- und Servicerobotern lernen?

Im Kern folgt daraus die allgemeine Aussage, dass sich ein ‚intelligentes‘ robotisches System auch im Moment der Übernahme der ‚Fernsteuerung‘ durch einen Menschen nicht *ganz* ‚dumm‘ stellen und damit – wertungsmäßig – zum bloßen Werkzeug herabstufen lassen darf, sondern sich vielmehr fortdauernd weigern muss, zum Instrument einer unbewussten und erst recht einer bewussten Gefährdung von Personen zu werden, die durch den Verstoß gegen das Straßenverkehrsrecht womöglich ausgelöst werden würde. Allgemeiner formuliert: Soweit es um Gefahren für Leib oder Leben anderer Menschen geht, muss das System für seinen ‚Herrn‘ zur *Impossibility Structure* werden und darf kein bedingungsloser gehorsamer ‚Diener‘ sein. Sachschäden und andere Rechtsgutverletzungen scheint § 1e StVG von der Wirkung der *Impossibility Structure* ausnehmen zu wollen. Auf den zweiten Blick zeigt sich aber, dass das Gesetz auch hier schon differenzierter vorgeht:

cc. Überwachungsleistungen auch von robotischen Haushalts- und Servicehilfen? Es sei insofern nämlich noch einmal an § 1g StVG erinnert⁴³⁴ und daraus vor allem an dessen Absatz 7. Demzufolge können

„[...] Dritte vom Halter [des Kraftfahrzeugs] Auskunft über die gemäß Absatz 1 und 2 gespeicherten Daten verlangen, soweit diese Daten zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit einem in § 7 Abs. 1 geregelten Ereignis [hier sind neben Personen- auch Sachschäden erfasst] erforderlich sind und das entsprechende Kraftfahrzeug mit autonomer Fahrfunktion an diesem Ereignis beteiligt war. [...] ³Eine Verwendung dieser Daten durch die Dritten ist nur zu den in Satz 1 genannten Zwecken zulässig.“

Bei den in Absätzen 1 und 2 gespeicherten Daten handelt es sich unter anderem um solche, bei denen die Technische Aufsicht ein Fahrmanöver anordnet, welches das Fahrzeug wegen eines Verstoßes gegen die straßenverkehrsrechtlichen Vorschriften selbst unterlassen hat (siehe § 1g Abs. 2 Nr. 2 StVG). Bezieht man § 1g StVG in die Analyse mit ein, dann haben wir es folglich mit einem System von kombinierter *Impossibility Structure* (für Personengefährdungen) und Ansätzen einer *Intelligent Surveillance* (für Personen- und Sachschäden) zu tun, welches die Durchsetzbarkeit

434 Dazu ausf. oben, → § 2 Rn. 194 f.

des Straßenverkehrsrechts in gestufter Form deutlich erhöhen könnte, sobald eine erhebliche Zahl an autonomen Kraftfahrzeugen auf den Straßen unterwegs ist.

- 208 *dd. Synthese und verallgemeinerungsfähige Gehalte.* Falls nun ein dem StVG angelehntes Arrangement auch für robotische Haushalts- und Servicehilfen geschaffen werden sollte, würde sich natürlich sogleich die Frage nach Differenzierungen stellen: Bei dem Einsatz in professionellen Kontexten wie der Pflege oder der Gastronomie erscheint es geradezu selbstverständlich, dass sich die robotischen Systeme von vornherein nicht zu bloßen Werkzeugen für Rechtsverstöße machen lassen dürfen (siehe schon *soeben*). Auch die Überwachungsleistung, die gegebenenfalls nachlaufenden Rechtsgüterschutz in Form von Kompensationen ermöglicht, dürfte im professionellen Bereich intuitiv wenigen Bedenken begegnen. Auch auf den zweiten (dogmatischen) Blick lässt die Rechtsprechung des Bundesverfassungsgerichts in *Kennzeichenkontrollen II* den Schluss zu, dass in solchen Bereichen optimierte Rechtsverfolgungsmöglichkeiten vergleichsweise leicht zu rechtfertigen wären.⁴³⁵
- 209 Anders verhält es sich mit Haushaltshilfen und vergleichbaren avancierten Assistenzsystemen, die in Bereichen eingesetzt werden, die von Art. 12 GG, vielleicht auch von Art. 10 GG erfasst sind.⁴³⁶ Das StVG kann hier keinen vollständigen Vorbildcharakter haben, weil sich der Straßenverkehr nicht in solchen rechtlich besonders geschützten Räumen abspielt, um die es hier geht.
- 210 Deshalb soll nun auf eine *prima facie* wohl überraschende und aus öffentlich-rechtlicher Sicht gut versteckte Vorschrift aus dem StGB eingegangen werden. Gemeint ist, wie schon angedeutet, § 323c StGB und die darin enthaltene allgemeine, sehr weitreichende Pflicht zur Hilfeleistung. Sie ist zwar kein Technikrecht, aber die dahinterstehenden Rechtsgedanken könnten auch für eine zukünftige technikrechtliche Regulierung bedenkenswert sein.
- 211 *b. Orientierung an der allgemeinen Hilfeleistungspflicht gemäß § 323c StGB?* Ich werde versuchen zu zeigen, dass, denkt man die Logik der Norm bis an ihr Ende durch, sie den Einsatz von *Impossibility Structures* weit über die bislang genannten Beispiele aus dem Verkehrs-, Datenschutz- und digitalen Kommunikationsrecht hinaus nahelegt. Diese sind zwar gesellschaftlich wichtig und rechtspolitisch umstritten, aber im Grunde doch relativ speziell.⁴³⁷ Der sogenannte „Samariter-Paragraph“⁴³⁸ des § 323c Abs. 1 StGB hingegen ‚durchschneidet‘ alle Lebens- und Gesellschaftsbereiche.

435 Vgl. hierzu oben, → § 2 Rn. 105 ff.

436 Zum bes. Schutz vor Überwachung in diesen Bereichen schon oben, → § 2 Rn. 91.

437 Auch wenn man das speziell mit Blick auf Art. 25 DSGVO wie gesagt mit guten Gründen anders sehen kann, vgl. oben, → § 2 Rn. 182.

438 *Heintschel-Heinegg*, in: *ders. (Hg.), BeckOK StGB*, 64. Ed. 1.2.2025, § 323c StGB Rn. 1.

aa. *Vorneweg: Tendenzen zu ‚freiwillig‘ hilfsbereiter KI.* Bevor wir uns mit der *Pflicht* 212 zur Hilfeleistung beschäftigen, ist vorneweg darauf hinzuweisen, dass viele Anbieter von digitalen Systemen (es muss nicht zwangsläufig schon um KI im engeren Sinn gehen) diese Systeme *freiwillig* um Funktionen ergänzen, die in einem Notfall Hilfe leisten können. Als frühes und bekanntes Beispiel einer auf Vermeidung von Schadensereignissen ausgerichteten Umwelterfassung ist die *Watch* von *Apple* zu nennen: Sie verfügt über Sensoren, die einen Unglücksfall ihres Träger erkennen und zwar noch nicht physisch eingreifen, aber immerhin schon autonom den Notruf betätigen können soll.⁴³⁹ Auch der in jedem iPhone aktivierbare *Personal Assistant Siri* kann mittlerweile auf Zuruf den Notruf wählen, wobei das Programm bis drei runterzählt und schon zu diesem Zeitpunkt Raum-Lautsprecher und -mikrofon aktiviert. Wenn wir ausgehend davon noch etwas weiter in die Zukunft schauen, gelangen wir eben zu humanoiden Haushaltsrobotern oder noch avancierteren *Personal Assistants* und KI-Agenten, die sicherlich in der Lage sein werden bzw. sein sollen, *jedenfalls* ihrem Eigentümer/Nutzer drohende Unglücksfälle zu erkennen oder, hilfsweise, zumindest auf dessen Hilferufe zu reagieren. Von dieser *wahrscheinlichen* Verbreitung einer Hilfeleistungsfunktion avancierter KI-Systeme ausgehend kann zur Frage nach einer allgemeinen Hilfeleistungspflicht weitergegangen werden. Für Menschen ist eine solche im deutschen Recht in § 323c StGB normiert:

bb. *Grundzüge von § 323c StGB.* Die Norm verpflichtet zur Leistung von Hilfe in 213 „Unglücksfällen, gemeiner Gefahr oder Not“. Ich konzentriere mich im Folgenden auf das Merkmal des Unglücksfalls, mit dem die beiden anderen Merkmalen weite Überschneidungsbereiche haben.⁴⁴⁰ Unglücksfälle sind nicht nur, aber vor allem auch Straftaten durch Dritte, also Rechtsverletzungen, deren Verwirklichung zulasten des Opfers der zur Hilfe Verpflichtete möglichst und soweit zumutbar zu verhindern hat. Ein denkbar eingängiges Anschauungsbeispiel liefert *Georg Freund*: „Wenn A im Begriff ist, auf B zu schießen, und C das ohne weiteres verhindern kann, muss er das im Güterschutzinteresse tun.“⁴⁴¹ C muss für den A also zur *menschlichen Impossibility Structure* werden.

439 s. support.apple.com/de-de/HT208944: „Wenn die Apple Watch Series 4 oder neuer einen schweren Sturz erkennt, während du die Watch trägst, tippt sie dir auf das Handgelenk, lässt einen Alarm ertönen und gibt eine Meldung aus. [...] Sollte die Apple Watch erkennen, dass du dich ungefähr eine Minute lang nicht bewegt hast, tätigt sie den Anruf [beim Rettungsdienst] automatisch. [...] Wenn du dein Alter beim Einrichten deiner Apple Watch oder in der Health-App eingegeben hast und mindestens 55 Jahre alt bist, wird diese Funktion automatisch aktiviert.“ Unzutreffend war ein Medienbericht, wonach Amazons *Alexa* bereits im Jahr 2017 das Leben einer jungen Frau gegen deren gewalttätigen Lebenspartner gerettet habe, indem es die Polizei rief.

440 Freund, in: Hefendehl/Hohman (Hg.), *MüKo StGB*, 32019, § 323c StGB Rn. 67 (zur „Gefahr“) bzw. Rn. 73 (zur „Not“).

441 Ibid., Rn. 65.

- 214 Umstritten ist dabei die Frage, ob jede, auch die „lapidarste“ Straftat⁴⁴² oder doch nur eine Straftat „von einigem Gewicht“ die Verpflichtung auslöst.⁴⁴³ „Ein drohendes Verbrechen stellt – wohl weitgehend unbestritten – einen Unglücksfall dar.“⁴⁴⁴ Nach wohl herrschender Meinung sollen auch drohende Sachschäden zur Hilfeleistung verpflichten.⁴⁴⁵ Hier soll die Erkenntnis ausreichen, dass der Umfang der von § 323c StGB ausgelösten Pflicht zur fremdnützigen privaten Verhinderung von Rechtsverstößen bzw., positiv gewendet, zur Rechtsdurchsetzung zugunsten Dritter *weit* ist.⁴⁴⁶
- 215 Zentral für uns ist nun die Frage, ob z. B. ein humanoider Haushaltsroboter – nennen wir ihn iC – im genannten Beispiel der ‚C‘ sein könnte, also von Rechts wegen gegen A einschreiten und damit zur *Impossibility Structure* werden müsste. Oder, falls die Technologie noch nicht physisch aktionsfähig und damit zum Verhindern in der Lage wäre, zumindest im Sinn von §§ 138 f. StGB Hilfe rufen müsste, was sie dann zu einer sehr spezifischen Form der *Intelligent Surveillance* machen würde.⁴⁴⁷
- 216 cc. § 323c StGB ist kein Technikrecht. Im ersten, positiv-rechtlichen Zugriff ist die Frage mit Nein zu beantworten. Die Verhaltenspflicht, die vor der Sanktionsregelung des § 323c StGB steht,⁴⁴⁸ richtet sich nur an *Menschen*, die einer *konkreten* Unglückssituation in vorsatzbegründender Weise gewahr werden. An Maschinen richtet sie sich nicht. Ob Menschen *als Hersteller* von Maschinen verpflichtet werden könnten oder werden sollten, Maschinen – *sobald und falls* diese die Fähigkeit zur Unterscheidung von Recht und Unrecht und zur physischen Hilfeleistung im Sinn von § 323c StGB haben – auf Hilfeleistung zu programmieren und damit für einen Angreifer zu einer *Impossibility Structure* zu machen, wird, soweit ersichtlich, im strafrechtlichen Schrifttum noch nicht diskutiert. Mir scheint, dass die Frage –

442 So Pawlik, GA 142 (1995), 360 (366): „Da die Hilfspflicht des § 323c StGB von ihrem Ausgangspunkt her der staatlichen Schutzpflicht umfangmäßig akzessorisch ist, ist somit auch der lapidarste Ladendiebstahl als ‚Unglücksfall‘ im Sinne des § 323c anzusehen.“ Weitgehend wohl auch Heger, in: Lackner/Kühl/Heger (Hg.), StGB, ³⁰2023, § 323c Rn. 2.

443 So die h. M., vgl. Freund, in: Hefendehl/Hohman (Hg.), MüKo StGB, ³2019, § 323c Rn. 65.

444 A. Koch, GA 165 (2018), 323 (335) m. w. N.

445 Str., s. Heger, in: Lackner/Kühl/Heger (Hg.), StGB, ³⁰2023, § 323c Rn. 2 m. w. N.

446 Bes. weit sollte die Hilfeleistungspflicht im Nationalsozialismus ausgedehnt werden; hierzu und zur Fortgeltung der Norm/ihrer Rechtsgedanken im demokratischen Staat ausf. BGH, Beschl. v. 10.3.1954, Az. GSSt 4/53 = BGHSt 6, 147 – Hilfeleistung nach Selbstmordversuch. Dort auch zur heute immer noch referenzierten Definition des Unglücksfalls, die als in Rspr. und Lit. herrschend geltend kann: „Unglücksfall ist demnach jedes mit einer gewissen Plötzlichkeit eintretende, eine erhebliche Gefahr bringende oder zu bringen drohende Ereignis, gleichgültig, ob die Gefahrenlage dem Gefährdeten von außen zugestoßen oder ob sie, wie beim Selbstmörder, von seinem Willen hervorgerufen ist.“

447 Es hätte sich angeboten, §§ 138, 139 StGB bereits i. R. der Vorstellung des Konzepts der *Intelligent Surveillance* anzusprechen und die hier für § 323c StGB angestellten Überlegungen zur Übertragbarkeit *mutatis mutandis* schon dort vorzunehmen. Dass das nicht erfolgt ist, liegt nicht an inhaltlichen Erwägungen, sondern schlicht darin, dass §§ 138, 139 StGB – soweit mir ersichtlich – in der Strafrechtswissenschaft so unterdogmatisiert sind, dass ich sie im hier gegebenen Rahmen nicht sinnvoll aufgreifen konnte. Mit dieser Einschätzung (unterdogmatisiert) auch Rojas, GA 147 (2017), 147: „Stiefkind der Dogmatik“.

448 Zur Unterscheidung von Verhaltenspflicht und Sanktionsnorm Freund, in: Erb/Schäfer (Hg.), MüKo StGB, ⁴2020, Vor § 13 Rn. 69 ff.; Gärditz, Staat und Strafrechtspflege, 2015, S. 13 m. w. N.

sozusagen im zweiten Zugriff auf die Materie – grundsätzlich und *de lege ferenda* mit einem Ja beantwortet werden kann (*de lege lata* scheitert eine strafrechtliche Verantwortlichkeit wohl schon daran, dass nur die Fahrlässigkeitsvariante in Betracht käme, und § 323c StGB ist ein Vorsatzdelikt; außerdem wäre die Garantenstellung des Herstellers recht zweifelhaft):

dd. Aber Übertragbarkeit des Rechtsgedankens von § 323c StGB auf ‚intelligente‘ Maschinen de lege ferenda? Dafür, dass § 323c StGB zu den Rechtsvorschriften gehört, die – ähnlich den schon genannten straßenverkehrsrechtlichen Vorschriften – jedenfalls grundsätzlich auf autonom agierende Maschinen übertragen werden können, spricht dessen Telos. Allerdings ist hier genau zu differenzieren: Schon jetzt wird zwar ernsthaft diskutiert, ob KI als Subjekt strafrechtlicher Verantwortlichkeit taugt, d. h. sinnvoll bestraft werden kann.⁴⁴⁹ Hiergegen spricht vieles, denn die verschiedenen Strafzwecklehren passen nicht oder doch nur mehr schlecht als recht auf Software. Insbesondere der zumindest in Teilen der Strafrechtslehre und in der Judikatur immer noch (oder wieder⁴⁵⁰) hochgehaltene Vergeltungsgedanke lässt sich kaum auf KI übertragen.⁴⁵¹ Diese Bedenken gelten aber nur für die *Sanktionsdrohung* in den Strafnormen. Die davorliegenden Verhaltenspflichten, die in den Strafnormen mitnormiert sind, können hingegen – vorbehaltlich einer entsprechenden Fähigkeit der KI – je nach konkreter Pflicht sehr wohl ‚passen‘. Für das in §§ 211 ff. StGB mitnormierte Tötungsverbot etwa dürfte sich das von selbst verstehen. Für die Verhaltenspflichten aus dem Verkehrsstrafrecht der §§ 315 Abs. 1 Nr. 2, 315d StGB folgt die Übertragung jetzt – wie gesagt – aus §§ 1a, 1e StVG, dort jeweils Absatz 2 Nr. 2.

Passt nun also der in § 323c StGB enthaltende Befehl auf eine ‚Befolgung‘ durch Maschinen? Folgt man einer im älteren Schrifttum zum Strafgrund von § 323c StGB vertretenen Auffassung, passt die Norm auf den *ersten Blick* überhaupt nicht. Demnach sollte der Strafgrund der Norm im Schutz bzw. in der Stabilisierung eines allgemeinen Rechtsgebots „mitmenschlicher Solidarität“ und „Nächstenliebe“ liegen, das sich aus der sozialen Verbundenheit der Menschen untereinander und ihrem Angewiesensein aufeinander ergeben soll.⁴⁵² Als aus menschlicher Sozialität

449 Ausf. Gaede, Künstliche Intelligenz – Rechte und Strafen für Roboter? 2019, S. 57 ff.

450 Weigend, RW 1 (2010), 39 ff.

451 s. die Nachw. bei Gaede, Künstliche Intelligenz – Rechte und Strafen für Roboter? 2019, S. 66 f.; dort auch zu Bedenken gegen die Durchsetzbarkeit von Strafen. Aus deontologischer Perspektive ähnl. Talbot/Jenkins/Purves, in: Lin/Jenkins/Abney (Hg.), Robot Ethics, 2017, S. 258 (260): "[R]obots cannot be right or wrong; they cannot be blameworthy or praiseworthy."

452 Vgl. Pawlik, GA 142 (1995), 360 (363) für die Zitate und Frisch, GA 163 (2016), 121 (123) für akt. Nachw. sowie krit. zur Tragfähigkeit von Solidarität als Begründung für allgemeine Hilfeleistungs- und notstandsbedingte Duldungspflichten (a. a. O., S. 124 ff.). Vgl. auch Gärditz, Staat und Strafrechtspflege, 2015, S. 53; ihm zufolge gehört „[d]ie Begründung von Solidaritätspflichten in einer auf individueller Selbstbestimmung gründenden Rechtsordnung [...] zu den schwierigsten Aufgaben einer Theorie gesellschaftlicher Institutionen.“

abgeleitete Pflicht ließe sich die Hilfspflicht des § 323c StGB auf Maschinen solange nicht übertragen, wie sich ein Solidaritätsempfinden zwischen Maschinen und Menschen nicht sinnvoll behaupten lässt.⁴⁵³ Ein solches ist zwar nicht undenkbar, aber unwahrscheinlich, solange sich Spekulationen über ein Bewusstsein von Maschinen nicht wenigstens halbwegs plausibel begründen lassen.

- 219 Auf einen genauen *zweiten Blick* sollte man freilich auch das Schutzgut ‚Solidarität‘ nicht zu schnell beiseite schieben. Der folgende Gedanke soll in Frageform formuliert werden: Verweigern wir uns nicht selbst Solidarität *untereinander*, wenn wir Entitäten schaffen, die wir uns in wesentlichen Zügen angleichen, und die wir im Fall von Haushalts- und Servicehilfen auch tief in unser Sozial- und Privatleben integrieren, diesen allerdings dennoch *nicht* vergleichbare Wertemuster sozialer Interaktion mit auf den Weg geben, die wir uns *untereinander* an *vergleichbarer* Stelle abverlangt hätten? Kurz gesagt: Wäre es nicht denkbar, dass der Rechtsgrund bzw. das Schutzgut ‚Solidarität‘ dann und deshalb passt, sobald bzw. weil wir *uns* in und hinter einer Technik⁴⁵⁴ *selbst* wiedererkennen werden, die zunehmend vermenschlicht?⁴⁵⁵ Diese sicherlich etwas anspruchsvolle These soll hier wie gesagt in Frageform stehen bleiben.
- 220 Tatsächlich lässt sich die Frage nach der Passung der in § 323c StGB enthaltenen Verhaltenspflichten zur allgemeinen Hilfeleistung auf ‚intelligente‘ Maschinen viel einfacher und ohne Überhöhungen von Mensch-Maschine-Mensch-Beziehungen beantworten, wenn man sich den aktuellen Thesen über den Strafgrund unterlassener Hilfeleistung zuwendet.⁴⁵⁶ Nach heute herrschender Meinung dient § 323c

453 Dazu, dass auch das *zwischenmenschliche* Gefühl der Verbundenheit, eben weil es *Gefühl*, „Motivation“, oder „Einstellung“ ist, streng genommen nicht Regelungsgegenstand modernen Rechts sein kann, sondern lediglich das nach außen tretende, als solidarisch beschreibbare Verhalten, *Frisch*, GA 163 (2016), 121 (125 f.).

454 Zur rechtlichen Relevanz der Vermenschlichungstendenzen ausf. → § 2 Rn. 454 ff.

455 Die Frage führt über *Immanuel Kants* bekannte ethische These zum Schutz von Tieren hinaus; s. für die Übertragbarkeit auf ‚intelligente Maschinen‘ *Anderson*, AI & Society 22 (2008), 477 (490 ff.): „Immanuel Kant considered a parallel situation and argued that humans should not mistreat the entity in question, even though it lacked rights itself. [...] Consider, then, the reaction Kant most likely would have had to the scene involving the bullies and Andrew [der humanoide Haushaltsroboter aus *Isaac Asimovs* ‚The Bicentennial Man‘ von 1976]. He would have abhorred the way they treated Andrew, fearing that it could lead to the bullies treating human beings badly at some future time. [...] As applied to the machine ethics project, Kant’s argument becomes stronger, therefore, the more the robot/machine that is created resembles a human being in its functioning and/or appearance.“

456 Für eine Übersicht *Hecker*, in: Schönke/Schröder (Hg.), StGB, ³⁰2019, § 323c Rn. 1.

StGB schlicht dem Rechtsgüterschutz⁴⁵⁷ des vom Unglücksfall Betroffenen.⁴⁵⁸ Ihre Rechtfertigung findet die Hilfspflicht zugunsten Dritter dabei nicht in einem Grundsatz zwischenmenschlicher Solidarität, sondern – ganz im Sinn *Hobbes'scher* Gesellschaftskonstruktion⁴⁵⁹ – darin, dass der Staat seiner grundrechtlichen Schutzpflicht durch eine Inanspruchnahme von Bürgern „gleichsam als Verwaltungshelfer[n]“⁴⁶⁰ auch dann und dort nachkommen kann, will und darf, wo es ihm durch eigene staatliche Bedienstete nicht möglich oder nicht erlaubt wäre.⁴⁶¹ Zum Beispiel in den schon erwähnten, von Artt. 10, 12 GG erfassten Bereichen. *Michael Pawlik* verwarft sich zwar dagegen, dass darin eine „Instrumentalisierung“ von Bürgern liege, weil der zur Dritt-Hilfe Verpflichtete sich durch die Stabilisierung des staatlichen Schutzanspruchs,⁴⁶² von dem er auch selbst profitiert, perspektivisch ja selbst helfe.⁴⁶³

457 Womit nicht gemeint ist, dass § 323c StGB bzw. die sogleich zitierten Autoren zwingend i. S. der sog. strafrechtlichen ‚Rechtsgutslehre‘ argumentieren, die eine *vorpositive* Bestimmung der Legitimität (und damit wohl auch Legalität?) von Strafgesetzen annimmt/annahm. Zur verfassungsrechtlichen Irrelevanz einer den Gesetzgeber bindenden Rechtsgutslehre s. die Nachw. zur Judikatur des BVerfG oben, in → Fn. 51 (Einleitung) und s. *Stuckenberg*, GA 158 (2011), 653 ff., krit. zur in der Strafrechtslehre immer noch anhaltenden „Phase der Verfassungsferne“ (a. a. O., S. 654) sowie zur Uneindeutigkeit der strafrechtswissenschaftlichen Kritik-Kategorien („unzulässig“, „illegitim“ u. ä., a. a. O., S. 660).

458 *Hecker*, in: *Schönke/Schröder* (Hg.), StGB, ³⁰2019, § 323c Rn. 1; *Freund*, in: *Hefendehl/Hohman* (Hg.), MüKo StGB, ³2019, § 323c Rn. 2 ff., jeweils m. w. N. Differenzierend nun die Neuaufl.: *Freund/Koch*, in: *Hohmann* (Hg.), MüKo StGB, ²2022, § 323c Rn. 2: „§ 323c StGB erfasst Verstöße gegen Verhaltensnormen, die dem Schutz der bedrohten Individualrechtsgüter des in Not Geratenen dienen. Gemeint sind also insbesondere Verstöße gegen Normen, die Leben und Gesundheit anderer Menschen schützen. Jedenfalls insoweit erfasst die Vorschrift die Verletzung einer im Interesse des Verunglückten bestehenden Solidaritätspflicht.“ Ähnl. *A. Koch*, GA 165 (2018), 323 (335).

459 Vgl. i. d. S. auch *Frisch*, GA 163 (2016), 121 (128).

460 *Pawlik* dürfte den Begriff im älteren, weiten Sinn meinen, der als Oberbegriff alle Formen privater Mitwirkung an Verwaltungsaufgaben umfassen sollte. Heute ist der Begriff verwaltungsrechtlich schärfer konturiert, s. *Vofskuhle*, VVDStRL 62 (2002), 266 (299), dort in Fn. 138, m. w. N.; für eine monographische Aufarbeitung s. immer noch *Burgi*, Funktionale Privatisierung und Verwaltungshilfe, 1999, passim, zu den Begriffen bes. S. 151 ff.

461 *Pawlik*, GA 142 (1995), 360 (364); in der Sache ähnl. *Frisch*, GA 163 (2016), 121 (129). Für eine Übertragung des Gedankens auf den Fall des rechtfertigenden Aggressivnotstandes s. *Pawlik*, JRE 22 (2014), 137 (154 ff.). Wohl a. *A. Rojas*, GA 147 (2017), 147 (155), dort Fn. 35: „Insofern ist die von *Pawlik* GA 1995, 360 [364 f.], formulierte These, die den Bürger als *Verwaltungshelfer* ansieht, sicherlich für die unterlassene Verbrechensanzeige richtig; in Bezug auf die unterlassene Hilfeleistung ist der These nicht unbedingt beizupflichten, denn es ist nicht evident, vor einem Unglücksfall, einer gemeinen Gefahr oder Not Aufgaben des Staates auf den Bürger abzuwälzen, ohne eine allgemeine Pflicht gegenüber dem Opfer selbst anzunehmen [...]“ Sowie im Fließtext a. a. O.: „Zunächst einmal ist der Staat zur Inanspruchnahme der Bürger nur legitimiert, wenn es sich um gravierende rechtswidrige Taten handelt, genauer um ganz bestimmte *Verbrechen*.“ Hervorhebung im Original. Wie (ob?) diese Auffassung mit § 323c StGB vereinbar sein soll, erschließt sich nicht recht.

462 Das ist nach *Pawlik* der eigentliche Legitimationsgrund von § 323c StGB, den er – insofern selbst auch von der h. M. absetzend – nicht mit dem Rechtsgüterschutz des individuell Betroffenen gleichsetzt, vgl. nachdrücklich *Pawlik*, GA 142 (1995), 360 (365 f.). Für die hier gestellte Frage nach der grds. Übertragbarkeit der Hilfeleistungspflicht auf Maschinen macht diese feinsinnige Unterscheidung aber m. E. keinen relevanten Unterschied zwischen der heute h. M. und der Argumentation von *Pawlik* aus.

463 *Pawlik*, GA 142 (1995), 360 (365, 371 ebd. (364)). Ähnl. *Frisch*, GA 163 (2016), 121: „Zur Rechtspflicht wird das im Verhältnis zum anderen ethisch Richtige in einer Solidargemeinschaft autonomer Personen nur, wenn und soweit man davon ausgehen kann, dass eine solche Pflicht der Autonomie der Mitglieder dieser Gemeinschaft entspricht“ Vgl. a. a. O. S. 129 f., 132 f. für die allerdings nur bedingt überzeugende Begründung, der es insb. an einer klaren Herausarbeitung der (verfassungsrechtlichen?) Maßstäbe fehlt.

Doch selbst wenn man milder bloß von einer „Inanspruchnahme des Bürgers“⁴⁶⁴ als „Verwaltungshelfer“ bei der Durchsetzung des staatlichen garantierten Friedens spricht, bleibt der utilitaristische und funktionelle Charakter der in § 323c StGB normierten Hilfspflicht dominant.⁴⁶⁵ Damit wiederum könnte der Rechtsgedanke und die damit bewirkte Rechtsdurchsetzungspflicht auf Technologie übertragen werden, *sofern* diese eben zur Hilfe im Sinn der Norm in der Lage und – nach Maßgabe ihrer sensorischen Leistungsfähigkeit – am Ort des Unglücksfalls präsent ist.

- 221 In letzterem – also der Notwendigkeit der Präsenz einer zur Hilfe fähigen Maschine am Ort des Unglücksfalls – liegt freilich eine erhebliche Beschränkung des Wirkungsradius einer auf Maschinen übertragenen Variation von § 323c StGB. Ich komme am Ende des Abschnitts wieder darauf zurück.⁴⁶⁶
- 222 *ee. Irrelevanz des pflichtbeschränkenden Zumutbarkeitskriteriums für Maschinen.* Der Vollständigkeit halber ist zuvor noch festzuhalten, dass das pflichtbeschränkende Tatbestandsmerkmal⁴⁶⁷ der individuellen Zumutbarkeit der Hilfeleistung für den Verpflichteten einer Übertragung der Handlungspflicht auf Maschinen nicht entgegensteht bzw. deren Handlungspflichten nicht einschränken könnte. Das Kriterium der Zumutbarkeit ist in § 323c StGB wertungsoffen und damit ausfüllungsbedürftig formuliert, d. h. kann und soll die individuelle Situation des Normadressaten und die ihm im Fall der Hilfeleistung drohenden Schäden berücksichtigen. Im Fall der Übertragung der ‚Adressatenstellung‘ auf eine Maschine wird sich – wenn überhaupt – der drohende Eigenschaden einer Intervention in der Regel auf Sachschäden an der Maschine selbst und damit einer Beeinträchtigung ihres Eigentümers bzw. Besitzers beziehen. Da solche „Beeinträchtigungen an Eigentum und Vermögen typischerweise später ausgeglichen werden können“, dürften sie nur dann zur sozusagen ‚egoistisch‘ motivierten Unzumutbarkeit einer Hilfeleistung führen, wenn sich die Hilfeleistung selbst nur auf monetäre Interessen richtet.⁴⁶⁸ Warnungen und die Verständigung von Hilfe dürften zudem in keinem Fall zu nennenswerten Eigenschäden führen.
- 223 Für uns interessanter sind daher die Fälle der Unzumutbarkeit, die quasi ‚altruistisch‘ begründet ist. Das Gemeinte lässt sich am besten am Beispiel erläutern: Nehmen wir an, der humanoide und entsprechend aktionsfähige Haushaltsroboter iC erkennt, dass seine Eigentümerin A unmittelbar angesetzt hat, den Besucher B mit

Krit. zu dieser „Konzeption einer ‚Solidarität des gegenseitigen Vorteils‘“ daher später auch Pawlik, JRE 22 (2014), 137 (149 ff.).

464 Pawlik, GA 142 (1995), 360 (364).

465 Heute h. M., vgl. Hecker, in: Schönke/Schröder (Hg.), StGB, ³⁰2019, § 323c Rn. 1 m. w. N.

466 → § 2 Rn. 232 ff.

467 Zur dogmatischen Einordnung der Zumutbarkeit statt vieler Freund, in: Hefendehl/Hohman (Hg.), MüKo StGB, ³2019, § 323c Rn. 90, dort Fn. 132 m. w. N. zu Gegenauffassungen.

468 Vgl. *ibid.*, Rn. 95.

dem Messer zu erstechen. Würde der auf Gefahrerkennung programmierte iC im Sinn von § 323c StGB intervenieren – also der A buchstäblich in den Arm fallen –, würde das B retten, aber gleichzeitig A der Gefahr einer Strafverfolgung aussetzen. Führt das zu einer relevanten Unzumutbarkeit?

Unter zwei Gesichtspunkten ist das zumindest diskutabel: Einmal „scheint [die strafrechtliche Judikatur] der Ansicht zuzuneigen, dass die *Gefahr der Strafverfolgung für einen Angehörigen* zu genereller Unzumutbarkeit der Hilfeleistung führt.“⁴⁶⁹ Nun ist iC im Beispiel kein Angehöriger (§ 11 Abs. 1 StGB erfasst ausschließlich Menschen). Er ist aber immerhin Eigentum von A und damit – so könnte man sagen – Angehöriger ‚analog‘. Der Analogieschluss trägt aber nicht: Denn die zu § 323c StGB referierte Rechtsprechung will unter dem Kriterium der Zumutbarkeit ja nicht den Angreifer schützen, sondern den Hilfspflichtigen:

„Ihm soll der Gewissenskonflikt erspart werden, in den er geraten würde, wenn seine Verpflichtungen gegenüber der Allgemeinheit seinem persönlichen Interesse, seine Familienangehörigen vor Strafe zu bewahren, widerstreiten.“⁴⁷⁰

Zu einem solchen „Gewissenskonflikt“ ist eine Maschine nicht fähig. Sie könnte ihn nur simulieren, d. h. könnte es – abhängig von ihrer Programmierung – eben auch ‚lassen‘, womit die Unzumutbarkeit aus diesem Grund schon entfiel. Es bliebe nur das wirtschaftliche Interesse des *Herstellers* von iC, der A versprechen zu können (gleichsam als Produktbeschaffenheit), dass sich iC keinem Wunsch der A widersetzen oder sie doch zumindest nicht der Gefahr der Strafverfolgung aussetzen werde. Das ist allerdings ein Interesse, das so pauschal formuliert wohl eher gering zu veranschlagen wäre.⁴⁷¹

Naheliegender ist es allerdings ohnehin, in Fällen wie dem beschriebenen (also Eigentum der A an iC) nicht auf die hier sogenannte ‚altruistische‘ Unzumutbarkeit abzustellen (die sich vor dem Hintergrund des Gewissenskonflikts letztlich doch auch als egoistisch motiviert entpuppt), sondern die Frage hin zur *Selbstbelastungsfreiheit* der A durch ihr Eigentum zu wenden. Und hier ist das Ergebnis für § 323c StGB einigermaßen erstaunlich bzw. bleibt konsequent dem Denken in der Schutzpflichtenerfüllung verhaftet: Der BGH geht in Übereinstimmung mit zumindest Teilen des Schrifttums⁴⁷² davon aus, dass die Gefahr der *eigenen* Strafverfolgung

469 Heintschel-Heinegg, in: ders. (Hg.), BeckOK StGB, 64. Ed. 1.2.2025, § 323c Rn. 24, Hervorhebung im Original.

470 BGHSt 11, 135 = NJW 1958, 390, noch zu § 330c StGB a. F.

471 Vgl. zu den Abstufungen der Wertigkeit der Grundrechte und damit verbundener Schutzpflichten Lepsius, Der Staat 52 (2013), 157 (183), bes. in und bei Fn. 99, dort auch weitere Nachw. zur Judikatur des BVerfG.

472 s. die Nachw. bei Freund/Koch, in: Hohmann (Hg.), MüKo StGB, 42022, § 323c Rn. 98 ff.

grundsätzlich nicht zur Unzumutbarkeit der Hilfeleistung nach § 323c StGB führt.⁴⁷³ Differenzierende Stimmen wollen danach unterscheiden,

„ob die in Frage stehende Straftat sich gerade in der schuldhaften Verursachung der Gefahrenlage erschöpft – dann soll keinesfalls von Unzumutbarkeit auszugehen sein – oder ob die Straftat in keinerlei Zusammenhang mit der Gefahrenlage steht – dann soll sich daraus die Unzumutbarkeit ergeben können.“⁴⁷⁴

Auch nach diesem differenzierenden Maßstab könnte also A in unserem Beispiel *nicht* unter Berufung auf den Grundsatz der Selbstbelastungsfreiheit verlangen, dass ‚ihr‘ iC sie gewähren lässt.⁴⁷⁵

- 227 c. *Ergebnis: keine analoge Anwendung der Normen de lege lata, aber dreifache Orientierung de lege ferenda.* Weder §§ 1a, 1e StVG noch § 323c StGB können ohne Weiteres Eins-zu-eins auf ‚intelligente‘ Maschinen übertragen werden. In dem einen Fall handelt es sich um *spezifisches* Technikrecht und in dem anderen Fall handelt es sich um zwar denkbar allgemeines Recht, aber eben *Menschen-Recht*.
- 228 Gerade die besonders weitgehend auf die Verhinderung von Rechtsgutverletzungen gerichtete allgemeine Hilfeleistungspflicht hat als Erfüllung staatlicher Schutzpflichten ein Regelungsziel, bei dessen Verfolgung der Gesetzgeber bekanntlich einen weiten Gestaltungsspielraum hat. Wenn man mit dem älteren Schrifttum § 323c StGB als – dann freilich freiheitsrechtlich problematischen⁴⁷⁶ – gesetzgeberischen Versuch ansehen will, zwischenmenschliche Solidarität zu erzwingen, gilt das natürlich erst recht. Die vorangehenden Überlegungen stellen folglich auch nicht den Versuch dar, eine Hilfeleistungs-*Programmier*-Pflicht *de lege lata* aus § 323c StGB ableiten zu wollen. Es bleibt dabei, dass sich § 323c StGB an Menschen als Normadressaten richtet, und zwar in einer konkreten Unglückssituation. Unglücksfall*vorsorge* (die mit der soeben benannten Programmierpflicht aufgerufen wäre) ist – soweit ersichtlich – vom Regelungszweck des § 323c StGB nicht umfasst und wird im strafrechtswissenschaftlichen Schrifttum auch nicht diskutiert.
- 229 Gleichwohl lassen sich den in diesem Abschnitt 5. angestellten Überlegungen verallgemeinerungsfähige Aussagen entnehmen, die bei einer technikrechtlichen Regulierung im Allgemeinen und einer Regulierung von Haushalts- und Servicerobotern im Besonderen Beachtung finden sollten:
- 230 *Erstens* ist klar geworden, dass der technikrechtliche Gesetzgeber davon ausgeht, dass sich ‚intelligente‘ Maschinen mit großem Aktionsradius (vulgo ‚Autonomie‘)

473 BGH, Urt. v. 23.3.1999, Az. 1 StR 21/93 = BGHSt 39, 164 = NJW 1993, 1871 (1872).

474 Vgl. Freund, in: Hefendehl/Hohman (Hg.), MüKo StGB, 73. 2019, § 323c Rn. 98 ff. m. w. N.

475 Zur am *Nemo-Tenetur*-Prinzip zu messenden Verwertbarkeit von durch „intelligente Agenten“ generierten Daten als Beweismittel im Strafprozess Gless/Weigend, JZ 2021, 612 (615 f.).

476 Hierzu Nachw. in → § 2 Fn. 453.

grundsätzlich an das einem Menschen in einer vergleichbaren Situation geltende Recht halten können müssen. Dafür stehen exemplarisch die §§ 1a, 1e StVG.

Mit § 1e StVG geht der Gesetzgeber *zweitens* einen Schritt weiter. Er verlangt von der rechtsfolgsamen Maschine, ihrerseits das Verhalten des Menschen beurteilen zu können, an den sie im Fall nur noch rechtswidrig möglicher Aktionen zunächst die Kontrolle über das Fahrzeug abgeben musste. § 1e Abs. 2 Nr. 5 StVG verlangt hier von dem autonomen Fahrzeug, die Gefährlichkeit der menschlichen Aktion für die Umwelt vor Ort zu erfassen und es gegebenenfalls besser zu wissen als der Mensch, also dessen Befehl zurückzuweisen, wenn anderen durch dessen Befolgung Gefahren drohen würden. Verallgemeinernd lässt sich sagen, dass sich das intelligente Fahrzeug nicht zum Werkzeug von gefährlichen menschlichen Handlungen machen lassen darf, und zwar selbst dann nicht, wenn es die Handlungskontrolle eigentlich bereits an den Menschen abgegeben hat. Hier ist also eine erste *Impossibility Structure* eingezogen, die m. E. durchaus *insgesamt* verallgemeinert werden kann bzw. sogar muss. Wichtig ist dabei festzuhalten, dass nach dem StVG die dem System abverlangte, fortdauernde Umgebungssensibilität zwar noch auf die Auswirkungen der menschlich veranlassten Aktion *des Fahrzeugs selbst* beschränkt ist. Aber eine Technologie, die Gefahren erkennen kann, die *vom Fahrzeug* für andere Objekte ausgehen, ist nicht weit davon entfernt, schlicht *Gefahren* zu erkennen, die *in seinem Umfeld* für andere Objekte bestehen – egal von welchem Objekt sie dann ausgehen. Nochmals sei an Systeme wie avancierte *Personal Assistants* und Haushaltsroboter erinnert, die diese Funktionen für ihre Eigentümer/Nutzer wohl schon als Teil der vom Hersteller offerierten Produktleistung werden erbringen können.⁴⁷⁷

Damit ist *drittens* der Bogen zur Frage nach einer allgemeinen Hilfeleistungspflicht auch für Maschinen geschlagen. Die vorstehenden Überlegungen sollten zeigen, dass es in der auf Rechtsgüterschutz gerichteten Logik der Hilfeleistungspflicht des § 323c StGB liegt, diese irgendwann auch auf entsprechend aktionsfähige KI-Systeme zu erstrecken. Andernfalls, so würde ich argumentieren, entstünde eine mit Blick auf die Schutzpflichten-Wahrnehmung begründungsbedürftige, letztlich sogar gleichheitsrechtlich erklärungsbedürftige Unwucht. Denn der Staat würde zur Erfüllung seiner Schutzpflichten „Bürger [also Menschen] über den Bereich des dem organisierten Staat Möglichen hinaus“⁴⁷⁸ in Anspruch nehmen, obwohl sich Bürger damit eventuell selbst in Konflikte und sogar Gefahr begeben könn(t)en. Er würde diese Zumutung aber ausgerechnet ‚intelligenten‘ Maschinen (bzw. deren Herstellern) ersparen. Die wichtige Einschränkung, die ich soeben schon angedeutet habe, liegt in dieser Gleichsetzung begründet: Die *geltende* allgemeine Hilfeleistungspflicht für Menschen ist wohl vor allem deshalb ohne grundrechtliche Störgefühle erträglich,

477 s. für konkrete Bsp. oben, → § 2 Rn. 212.

478 Pawlik, GA 142 (1995), 360 (364).

weil die Pflicht auf *Anwesende* beschränkt ist, die den Unfall (im weiten Sinn) in vorsatzbegründender Weise mehr oder weniger zufällig wahrnehmen. Auch die von § 323c StGB vermittelte Rechtsdurchsetzung nimmt somit an der jeder menschlichen Rechtsdurchsetzung eigenen Kontingenz teil.

- 233 Die *Übertragung* der Hilfeleistungslogik auf Maschinen würde daher auch *nicht* fordern, einen jeden ‚smarten‘ Kühlschrank in einen off- und online aktions- und damit hilfefähigen Aktanten zu verwandeln, wenn das für seine designierte Funktionalität nicht erforderlich ist. Aber es fordert diejenigen Systeme heraus, Hilfe zu leisten (bzw. von ihren Programmierern zur Hilfeleistung eingerichtet zu sein), die *zum Zwecke ihres bestimmungsgemäßen Gebrauchs* über Sensorik, Software und Aktuatoren verfügen (müssen), die sie zugleich technisch in die Lage versetzen, Unglücksfälle wahrzunehmen und/oder zu verhindern. Ein übertragener § 323c StGB würde daher nur, aber immerhin fordern, dass die genannten Systeme in zeitlicher und/oder räumlicher Weise *äquivalente* ‚Unglücksfälle‘ erkennen und verhindern können müssen, die von Dritten oder sogar vom Eigentümer/Nutzer des Systems selbst einem Dritten zugefügt werden. Oder kürzer: Das, was das intelligente System für den einen (= Eigentümer) an Hilfe leisten kann, darf es dem anderen (= Dritten, gegebenenfalls ‚Opfer‘ des Eigentümers) nicht verwehren.
- 234 Lässt man sich darauf ein, die Logik von § 323c StGB auf intelligente und aktionsfähige Maschinen zu projizieren, dann bildet diese vordergründig unscheinbare, im Strafrecht ‚versteckte‘ Verhaltenspflicht angesichts der absehbaren Ubiquität intelligenter Maschinen den Ausgangspunkt für ein immens wirkmächtiges Rechtsdurchsetzungsarrangement. Oder, frei nach *Pawlik*: Es würde den Ausgangspunkt für ein sehr weitgespanntes „Verwaltungshelfer“-Arrangement zur Durchsetzung staatlichen Rechts bilden. Der oben offen gelassenen Definition dessen, was als zum Einschreiten verpflichtender Unglücksfall oder als gemeine Gefahr oder Not zählt,⁴⁷⁹ käme dann große Relevanz zu. Würde man in Übertragung von *Pawliks* Auslegung von § 323c StGB auch noch die „lapidarste“ Straftat ausreichen lassen, weil auch hinsichtlich dieser den Staat eine Schutzpflicht trifft oder er sie zumindest übernommen hat, dann würde damit eine *Omnibus*-Klausel maschineller Straftatvorsorge durch *Impossibility Structures* kreiert. Wenn man darüber hinaus bedenkt, dass die Rechtsordnung insgesamt zentral auf der Idee des Rechtsgüterschutzes aufbaut, dann wird klar, wie weitreichend nicht nur das Optimierungspotential, sondern *prima facie* auch der Optimierungsdruck in Sachen Rechtsdurchsetzung sein wird. Denn Unglücksfälle sind nicht nur auf Straftaten beschränkt. Die Nothilfe-Konstellation passt damit auf viele, wenn nicht sogar die meisten Formen von Rechtspflichten.

479 s. bei/in → § 2 Fn. 442/443.

Ist das alles – rechtspolitisch reflektiert – unreal? Unreal in dem Sinn, dass doch kein 235
Gesetzgeber eine so breit angelegte Pflicht zur technischen Intervention beschließen
würde? Naja – es sei nur nochmals an Art. 25 Abs. 1 DSGVO erinnert:⁴⁸⁰ Angesichts
des extrem weiten Begriffs des personenbezogenen Datums und der Tatsache, dass
heutige Datenverarbeitungen fast stets automatisiert im Sinn der DSGVO erfolgen
und somit den Anwendungsbereich der Verordnung eröffnen, liefert die Norm ein
eindrückliches Beispiel aus dem *geltenden* Technikrecht (im weiteren Sinn) für eine
schon jetzt besonders weitgehend formulierte gesetzliche Forderung nach *Impossibi-*
lity Structures.

Pragmatisch gedacht kann freilich solange Entwarnung gegeben werden, solange die 236
,intelligenten‘ Systeme nicht zu einer anspruchsvollen Kontexterkenkung im Sinn
der oben – als eher ferne Zukunftsperspektive – beschriebenen *General Artificial*
*Intelligence*⁴⁸¹ in der Lage sind. Denn sowohl Art. 25 Abs. 1 DSGVO als auch § 323c
StGB enthalten letztlich derart breit angelegte Pflichten, dass sie mit der aktuell
verfügbaren Generation künstlicher Intelligenz noch nicht umsetzbar sind. Die Zahl
der *False Positives* und *False Negatives* wäre derart hoch, dass schon vor jeder
rechtlichen Abwägung aus rein pragmatischen Gründen ein Einsatz in der Breite
nicht sinnvoll wäre.

An dieser Stelle möchte ich die Analyse von möglichen *Impossibility Structures* als 237
Ausstattung mit einer sogleich folgenden Zusammenfassung und Einordnung beenden
(sogleich, → 6.), um sodann weitere Differenzierungen der Rechtsrealisierungstechnologien in die
Diskussion einzuführen (anschließend → III. bis V.). Auf die besondere Relevanz einer möglichen
Hilfeleistungspflicht und den mit ihrer Übertragung bzw. Übertragbarkeit auf Maschinen verbundenen
Konsequenzen komme ich im Rahmen des Fazits dieses § 2 allerdings nochmals ausführlich zurück (→ VI. =
S. 165 ff.).

6. Zum Stand der Diskussion: dogmatische Gelassenheit, rechtstheoretische Besorgnis – beides unbegründet?

Die soeben genannten Anwendungsszenarien und -bereiche für den Einsatz von 238
Impossibility Structures haben illustriert, dass ihr Einsatz gegenwärtig noch recht
punktuell erfolgt, dass aber normativ gleich mehrfach Anknüpfungspunkte bestehen,
von einer erheblichen Ausweitung dieses Einsatzes in der Zukunft auszugehen.
Hier soll es nun darum gehen, zunächst die aktuell bereits diskutierten Vorschläge
zum rechtsdogmatischen Umgang mit solchen Strukturen zusammenzufassen, die
von einer gewissen Gelassenheit geprägt sind (dazu sogleich, → a.); ich meine,

480 Hierzu oben, ab → S. 143.

481 s. hierzu oben, bei → § 1 Rn. 43.

dass durchaus Grund besteht, hier etwas genauer und kritischer zu hinterfragen, ob wir dogmatisch wirklich schon hinreichend gut gerüstet sind, um *Impossibility Structures* adäquat bewältigen zu können (dazu → b.). Umgekehrt glaube ich, dass die rechtstheoretische Diskussion – diese ist von erheblicher Besorgnis geprägt – etwas gelassener und nüchterner geführt werden könnte (dazu dann → c.).

- 239 a. *Rechtsdogmatische Bewältigung durch Überwachungsakzessorietät.* Die ernsthafte verfassungsrechtsdogmatische Diskussion von *Impossibility Structures* als potentiell flächendeckendes Phänomen ist vergleichsweise jung.⁴⁸² Sie nahm im Wesentlichen erst mit den jüngsten Fortschritten in Sachen KI und Digitalisierung an Fahrt auf. Die Auseinandersetzung ist zugleich, wie gesagt, von einer gewissen Gelassenheit geprägt. Die „Probleme“ einer potentiell vollständigen oder zumindest massiv gesteigerten „Rechtsdurchsetzung“ könnten „schon mit bestehenden [dogmatischen] Figuren differenziert adressiert werden“.⁴⁸³
- 240 aa. *Eingriff vor allem in das Recht auf informationelle Selbstbestimmung.* In der Tat liegt es nahe, *Impossibility Structures* sozusagen ‚überwachungsakzessorisch‘ zu verarbeiten:⁴⁸⁴ „Denn eine vorbereitende Beobachtung, ein Vollzug oder eine Sanktionierung setzen immer den Zugriff auf entsprechende personenbezogene Daten voraus und aktivieren damit [das Recht auf informationelle Selbstbestimmung]“. Folglich könne die dazu ergangene, die flächendeckend-anlasslose *Überwachung* effektiv einhegende Rechtsprechung auch zur Verarbeitung von *Impossibility Structures* eingesetzt werden.⁴⁸⁵
- 241 Das gilt – mit etwas größerem argumentativen Aufwand – auch im Fall von *privat* eingesetzten Unmöglichkeitstechnologien, jedenfalls dann und insoweit, als deren Einsatz hoheitlich vorgeschrieben oder – etwa durch Haftungsregeln – hinreichend stark veranlasst ist.⁴⁸⁶ Denn mit der hoheitlichen (quasi-)Verpflichtung zur Nutzung

482 Breitere Aufmerksamkeit erlangten solche (auch analoge) Strukturen bislang eher in der Kriminologie, vgl. hierzu *Hastedt*, MMR 2021, 696 ff.

483 *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 143.

484 Vgl. dazu auch schon *Rademacher*, JZ 2019, 702 (705 ff.).

485 *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 146; ähnl. *Wischmeyer*, in: Baumgärtel/Hoppen (Hg.), Informationstechnik und Recht, 2021, S. 9 Rn. 15 ff.; *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 45 ff.

486 Darauf ist das Erkenntnisinteresse vorliegend gerichtet. Ob diese Rechtsprechungslinie auch weiterhilft, wenn Private *Impossibility Structures* gänzlich freiwillig zu eigenen oder zu Gunsten Dritter einsetzen, ist weniger eindeutig zu beantworten; s. hierzu u. a. *Becker*, ZUM 2019, 636 (638 ff.); *N. Kuhlmann*, in: Fries/Paal (Hg.), Smart Contracts, 2019, S. 117 ff.; *F. Hofmann*, in: Fries/Paal (Hg.), Smart Contracts, 2019, S. 125 ff.; *Oster*, in: Ahlberg/Götting/Lauber-Rönsberg (Hg.), BeckOK Urheberrecht, 32. Ed. 15.9.2021, § 1 UrhDaG Rn. 12; ausf. *G. Wagner*, AcP 222 (2022), 56. Auf das auch ohne staatliche Vorgabe zur Verwendung von *Impossibility Structures* geltende private Datenschutzrecht verweisen *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 147. In denjenigen Fällen, in denen die Rechtsdurchsetzung mit dem Zugriff auf den Besitz eines anderen verbunden ist – z. B. denkbar i. R. sog. *Smart Contracts*, wo etwa eine Batterie eines geleasteten Kfz das Wiederaufladen verweigert – steht nach Auffassung von *Kuschel*, AcP 220 (2020), 98 ff., das possessorische Besitzschutzrecht entgegen (§§ 858 ff.

solcher Strukturen liegt in der Regel ein gezielt-mittelbarer Eingriff in das Recht auf informationelle Selbstbestimmung der zur *Compliance* gezwungenen Personen vor, sodass eine Übertragung der Grundsätze insofern tatsächlich recht zwanglos erfolgen kann.⁴⁸⁷

Der damit ermöglichte Rückgriff auf die Anlassdogmatik des Bundesverfassungsgerichts⁴⁸⁸ scheint folglich eine nach Maßgabe des Verhältnismäßigkeitsprinzips situativ anpassungsfähige und vor allem wirkungsvolle Einhegung auch von physisch wirksamen *Compliance*-Strukturen zu versprechen. Ein flächendeckender Einsatz der Technologie wäre damit grundsätzlich unzulässig. Angelehnt an die ebenfalls quantitativ orientierte Überwachungsgesamtrechnung schlägt *Anne Paschke* zusätzlich vor, eine „Determinierungsgesamtrechnung“ aufzumachen, die der Besonderheit der physischen Komponente Rechnung trägt.⁴⁸⁹

bb. Prima-facie-Konvergenz mit der Rechtsprechung des EuGH. Auf den ersten Blick lässt sich diese Position gut mit der beschriebenen vorsichtigen Entwicklung der EuGH-Rechtsprechung zum Recht der Onlinekommunikation und zum dort ausdrücklich normierten Verbot vereinbaren, den Diensteanbietern zu einer „allgemeinen Überwachung“ der Nutzer zu verpflichten. Der EuGH grenzt die unzulässigen *allgemeinen* von potentiell zulässigen *spezifischen Überwachungspflichten* und den damit verbundenen – eben quasi akzessorischen – Filter-Vorgaben ab.⁴⁹⁰ Dabei scheint sich die Spezifität mittlerweile allerdings nicht mehr, wie ursprünglich, nach der Menge des zu filternden Online-Inhalts zu bestimmen, sondern wird durch

BGB). Diese Auffassung wird geteilt vom OLG Düsseldorf, Urt. v. 7.10.2021, Az. I-20 U 116/20 = JZ 2022, 359 – Verbotene Eigenmacht durch Fernsperrung einer vermieteten E-Auto Batterie; der BGH, Urt. v. 26.10.2022, Az. XII ZR 89/21 = NJW 2022, 3575 – Fernabschaltung einer Autobatterie durch Vermieter, lässt die Frage bzgl. des Besitzschutzes offen (a. a. O., Rn. 17, 23), kommt allerdings in Anwendung von § 307 BGB zum selben Ergebnis, nämlich Unzulässigkeit jedenfalls einer Fernabschalteinrichtung für eine gemietete Autobatterie: Die entgegen der gesetzlichen Vermutung den Mieter treffende Last, sich gegen eine aus seiner Sicht unrechtmäßige Abschaltung der Batterie gerichtlich zur Wehr setzen zu müssen (statt umgekehrt), stelle eine unangemessene Benachteiligung des Mieters dar (a. a. O., Rn. 25 ff.). Monographisch zum Thema nun *Sander*, Besitz(schutz) smarter Sachen, 2024, *Duden*, Digitale Sachherrschaft, 2023.

487 *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 147; ausf. dazu auch *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 42 f.

488 Vgl. oben, → § 2 Rn. 82 ff.

489 *Paschke*, MMR 2019, 563 (567); zustimmend *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 49. Ausf. dazu unten, ab → S. 448.

490 Bei dieser Rspr. fällt allerdings auf, dass der EuGH in den neueren Urteilen nicht (mehr) den Datenschutz (d. h. das unionale Pendant zur informationellen Selbstbestimmung) als Abwägungsgut gegen die Filterung heranzieht, sondern fast nur noch die Meinungs- und Informationsfreiheit der Nutzer, vgl. die Nachw. oben, → § 2 Rn. 156. Allerdings lässt sich bei Filtersystemen, die einem *Notice-and-stay-down*-oder gar einem *Notice-and-prevent*-Modell folgen, die Verarbeitung von personenbezogenen Daten gar nicht vermeiden, wenn und weil dafür die gesamten Plattformen regelmäßige ‚abgescannt‘ werden müssen und ggf. auch IP-Adressen gespeichert und genutzt werden (müssen), um Nutzer über eine Filterung zu informieren; s. dazu ausf. *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 167 ff.

Rekurs auf eine je nach Kontext hinreichend konkrete Initial-Tat bewirkt,⁴⁹¹ die so konkret beschrieben werden muss, dass die digitalen Diensteanbieter in die Lage versetzt sind, zur weiteren proaktiven Verhinderung einer Wiederholung der Tat automatisierte und damit vergleichsweise kostengünstige Erkennungstechnologien zu nutzen.⁴⁹² Diese unionale Rechtsprechungslinie harmonisiert relativ gut mit der Anlassdogmatik des Bundesverfassungsgerichts, zumal deshalb, weil zu der mehr oder weniger intensiven Anlassbindung *auf Seiten der Plattformbetreiber* und sonstigen Diensteanbieter auch die besondere Verantwortung qua Beherrschung einer kommunikativen Gefahrenquelle eine Rolle spielt. Lediglich die mittlerweile fehlende mengenmäßige Begrenzung der Filterpflichten dürfte wohl in Richtung einer vom Bundesverfassungsgericht kritisch gesehenen flächendeckenden Überwachung gehen.⁴⁹³ (Wie die unten folgenden Ausführungen zu Art. 17 DSM-RL zeigen werden, zeichnen sich allerdings speziell im Urheberrecht einige Unterschiede zwischen der grundsätzlichen Anlassbindung nach bundesverfassungsrechtlicher Lesart und der Spezifität der Überwachung im Sinn der neuen EuGH-Rechtsprechung ab; dazu weiter unten ab → S. 210).

244 *cc. Verfassungsrechtliche Hürden spezifisch für den Einsatz von Impossibility Structures.* Zur Frage der Anlassbindung des Einsatzes treten einige weitere, für *Impossibility Structures* spezifische konstitutionelle Hürden hinzu, die allerdings dogmatisch ebenfalls noch relativ problemlos zu bewältigen sind (zu auf einen genauen zweiten Blick sichtbaren Inkongruenzen, die sich nicht so leicht auflösen lassen, siehe ab → S. 173):

245 *Erstens* muss von Grundrechts wegen auch Rücksicht auf die wirtschaftlichen Interessen der in der Regel privaten Anbieter, Hersteller und Betreiber von Systemen genommen werden, die zum Einbau von *Impossibility Structures* verpflichtet und damit zu Erfüllung einer öffentlichen und/oder drittnützigen Aufgabe in Dienst genommen werden;⁴⁹⁴ besonders gut sichtbar ist diese wirtschaftlich begründete

491 s. oben, → Rn. 153, 155 (Rs. *Glawischnig*), → Rn. 164 (Rs. *Cyando*), → Rn. 168 (zur TCO-VO), und → Rn. 173 (zum DSA), jeweils in diesem § 2. Nicht mehr hierzu passt freilich die Entscheidung des EuGH zu Art. 17 Abs. 4 DSM-RL, auf die weiter unten ausf. einzugehen sein wird, s. ab → S. 210.

492 Vgl. oben, → § 2 Rn. 155.

493 s. → § 2 Rn. 103. Insofern dürfte auch ein Rückgriff auf BVerfG, Urt. v. 2.3.2010, Az. 1 BvR 256/08 = BVerfGE 125, 260 – Vorratsdatenspeicherung, nicht zu einer positiveren Einschätzung führen: In seiner ersten Entscheidung zur Vorratsdatenspeicherung hat das BVerfG es zwar zugelassen, dass Private flächendeckend Telekommunikationsdaten speichern müssen, hat den *Abruf* dieser Daten zu straf- und gefahrenabwehrrechtlichen Zwecken aber ausdr. vom Vorliegen eines entsprechenden Verdachts abhängig gemacht, vgl. a. a. O., Rn. 228, 231.

494 *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), *GVwR I*, 32022, § 26 Rn. 147; *Krönke*, Öffentliches Digitalwirtschaftsrecht, 2020, S. 95 f.; vgl. zur Frage einer möglichen Ausgleichspflichtigkeit der Indienstnahme am Bsp. von Kraftwerksstilllegungen *Burgi/Krönke*, *VerwArch* 109 (2018), 423 ff. Die wirtschaftlichen Interessen von Herstellern, Diensteanbietern usw. dürften umso geringer wiegen, je mehr diese Anbieter aufgrund von Marktmacht, *Gate-Keeper*-Eigenschaften usw. selbst (quasi) unmittelbar Grundrechtsverpflichtete werden. Zum Thema nun ausf. *Ollig*, Europäische Plattformverfassungen, 2025, S. 182 ff.

Rücksichtnahme immer noch in der Rechtsprechung des EuGH zu (eventuellen) Filterpflichten im Online-Kommunikationsverkehr.⁴⁹⁵

Zweitens geht mit *Impossibility Structures* definitionsgemäß eine physische Wirkung einher. *Impossibility Structures* greifen im Vergleich zur *Intelligent Surveillance* also immer auch in die allgemeine Handlungsfreiheit oder gegebenenfalls speziellere Freiheitsrechte ein, unter Umständen auch in die Gesundheit von Personen.⁴⁹⁶ Der Einsatz von *Impossibility Structures* stellt damit einen Unterfall von Vollstreckungsrecht dar. Folglich versteht sich zunächst von selbst, dass das konkrete *Mittel*, durch das dieser physische Eingriff bewirkt wird, selbst verhältnismäßig sein muss. Um ein bekanntes extremes Beispiel zur Illustration zu wählen: Erkennt unser Haushaltsroboter iC aus dem obigen Beispiel, dass der Besucher B aus dem Haushalt der A einen Apfel stehlen möchte, dürfte die verhältnismäßige/erforderliche Verunmöglichungshandlung nicht in einem tödlichen Angriff bestehen.⁴⁹⁷ 246

Drittens geht mit der physischen Wirkung das Risiko eines *physisch* wirksamen *Overblocking* einher, während im Fall von Überwachung falsch-positive Treffer in der Regel ‚nur‘ zu – *ex post* betrachtet – ungerechtfertigten weiteren (menschlichen) Ermittlungsmaßnahmen führen dürften (das berühmte „behördliche Interesse“, das sich auf den Einzelnen fokussiert⁴⁹⁸). Zu berücksichtigen ist dabei, dass sich solche physischen Folgen auch im Rahmen von (Vollzugs-)Folgenbeseitigungsansprüchen zwar manchmal, aber nicht stets durch *ex post* ansetzende Rechtsschutzverfahren beseitigen lassen. So mag es im vieldiskutierten Bereich des urheberrechtlich bedingten *Overblocking* tatsächlich so sein, dass eine spätere – nach erfolgreichem internen oder gegebenenfalls auch gerichtlichen Rechtsschutz erfolgende – Publikation eines zunächst geblockten Meinungsbeitrags zu spät kommt, um tatsächlich noch zu der Debatte beitragen zu können, zu der er beitragen sollte. Auch das ist im Rahmen der Verhältnismäßigkeitsprüfung bei der Entscheidung über den Einsatz der Struktur zu berücksichtigen. 247

Viertens ist – quasi als Spiegelbild zur grundrechtlich relevanten Belastung der privaten Anbieter/Nutzer von rechtsrealisierenden Technologien (soeben, erstens) – zu bedenken, dass die Übertragung von Rechtsrealisierungsaufgaben auf Private auch demokratierechtliche Fragen aufwirft. Zu berücksichtigen ist insofern der Funktionsvorbehalt des Art. 33 Abs. 4 GG, der die Ausübung hoheitlicher Befugnisse grundsätzlich Beamten in einem besonderen Dienst- und Treueverhältnis 248

495 s. die Nachw. oben, → § 2 Rn. 155.

496 Bernzen/Kehrberger, RW 10 (2019), 374 (391 ff.) m. w. N. Ausf. Beaucamp, Rechtsdurchsetzung durch Technologie, 2022, S. 41 ff.

497 Vgl. zur Diskussion sogar i. R. des bekanntlich bes. scharfen Notwehrrechts nur Erb, in: Erb/Schäfer (Hg.), MüKo StGB, 42020, § 32 Rn. 201 ff.

498 Vgl. BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 43.

vorbehält;⁴⁹⁹ was aber voraussetzt, dass *staatlich* Gewalt ausgeübt wird,⁵⁰⁰ was in unseren Konstellationen wiederum regelmäßig gerade nicht der Fall sein wird.⁵⁰¹ Ausgangspunkt zur Beantwortung der damit aufgeworfenen Frage nach verbleibender staatlicher Verantwortung ist, dass eine Einschaltung von Privaten als „Verwaltungshelfer“ zur Durchsetzung von Recht (so *Michael Pawlik* zu § 323c StGB⁵⁰²) auch vor dem Hintergrund von Demokratieprinzip, Gewaltmonopol und des damit verbundenen Funktionsvorbehalts des Grundgesetzes nichts grundlegend Neues ist, sondern uns in vielen Bereichen des Rechts begegnet,⁵⁰³ und dort das öffentliche Recht lediglich herausfordert, von direkten Operationsmodi auf Gewährleistungsarrangements umzustellen (Gewährleistungsverwaltungsrecht).⁵⁰⁴ Sowohl das Demokratieprinzip als auch der beamtenrechtliche Funktionsvorbehalt zeigen sich für Modernisierungen und Re-Fokussierungen der *prima facie* hoheitlichen Tätigkeit der Rechtsdurchsetzung offen (vgl. auch Art. 33 Abs. 5 GG).⁵⁰⁵ Sie erzeugen allerdings Argumentationslasten und wären sicherlich dann verletzt, wenn staatlicherseits eine vollständige Auslagerung rechtsdurchsetzender Tätigkeiten angestrebt würde, *ohne* entsprechende Gewährleistungsreserven bereit zu halten. (Zu bedenken ist zudem, dass spezifisch Art. 33 Abs. 4 GG unter dem Vorbehalt steht, dass sich das eventuelle Einsatzgebot für *Impossibility Structures* nicht aus dem Unionsrecht ergibt, da der Funktionsvorbehalt nicht zu den änderungsfesten Bestimmungen des Grundgesetzes zählt.⁵⁰⁶)

499 Zum Streitstand, was genau unter „Ausübung hoheitsrechtlicher Befugnisse“ gemeint ist und folglich den Funktionsvorbehalt auslöst, s. *Brosius-Gersdorf*, in: *Dreier* (Hg.), GG Bd. II, ²2015, Art. 33 Rn. 152 ff. m. w. N.; speziell zum umstr. Privatisierungsverbot a. a. O., Rn. 157.

500 Grundlegend immer noch *Vofßkuhle*, VVDStRL 62 (2002), 266 (292 ff.).

501 Insb. wird es an einer Beleihung i. d. R. fehlen; für Bsp. s. *Vofßkuhle*, VVDStRL 62 (2002), 266 (301 ff.).

502 s. soeben, → § 2 Rn. 220.

503 Vgl. *Vofßkuhle*, VVDStRL 62 (2002), 266 (268): „Beteiligung Privater an der Erfüllung öffentlicher Aufgaben [als] Alltäglichkeit“. Speziell zur Gewährleistung der Staatsaufgabe „Sicherheit“ unter Einbeziehung Privater a. a. O., S. 275 m. w. N.

504 So auch schon *Wischmeyer*, in: *Baumgärtel/Hoppen* (Hg.), *Informationstechnik und Recht*, 2021, S. 9 Rn. 24. Es ist daher eine zu enge Perspektive, wenn bei Verwendung von *Smart-Contract*- oder von anderen Rechtsdurchsetzungstechnologien pauschal von einer „vollständigen Privatisierung der Rechtsdurchsetzung“ gesprochen wird, so *G. Wagner*, AcP 222 (2022), 56 (62); s. dazu nochmals unten, → § 2 Rn. 418 ff. und ab → S. 381.

505 Zu den Maßstäben und den damit verbundenen großen Gestaltungsspielräumen des Gesetzgebers *Vofßkuhle*, VVDStRL 62 (2002), 266 (297 f.) m. w. N. Speziell zu Filtertechnologien *Eifert*, NJW 2017, 1450 (1451): „Auch im Hinblick auf Hass-Kommentare ist nicht einsichtig, wieso diese nicht erst recht auf private Initiative hin zu löschen sein sollen, verletzen sie doch in erheblicher Zahl private Rechte. Schließlich ist zu betonen, dass es hier nicht um eine Letztentscheidung der Privaten, sondern nur um eine Erstentscheidung geht. Die letzte Entscheidung liegt formal immer bei den staatlichen Gerichten [...]. Weil Aufwand und Kostenrisiko des Klagewegs im Verhältnis zu den verfolgten Interessen aber üblicherweise unverhältnismäßig groß sind, kann die faktische Wirkung der Erstentscheidung durch die Intermediäre freilich kaum überschätzt werden. Die Erstentscheidung über die Löschung treffen entsprechend unvermeidlich die Intermediäre, wenn und weil sie nicht vollständig aus jeder Verantwortlichkeit entlassen werden sollen.“

506 Zu den Fragen demokratischer Legitimation beim Einsatz von künstlich-intelligenter Rechtsdurchsetzung durch den Staat selbst s. *Unger*, in: *ders./Ungern-Sternberg* (Hg.), *Demokratie und künstliche Intelligenz*, 2019, S. 113 (122). An dieser Stelle nur folgende Anm. zu dieser Diskussion: M. E. ergibt sich der

Aus den vier genannten Gesichtspunkten folgt – da sie grundsätzlich der Abwägung mit entgegenstehenden Gütern zugänglich sind⁵⁰⁷ – kein absolutes Einsatzverbot.⁵⁰⁸ Aber daraus scheint (!) ein gegenüber einer vergleichbaren *Intelligent Surveillance* jedenfalls *nochmals* erhöhtes Eingriffsgewicht zu resultieren, das es nahe zu legen scheint,⁵⁰⁹ den Einsatz von *Impossibility Structures* auf spezifische Konstellationen zu beschränken, und erst recht von einer flächendeckenden physischen Verhaltenssteuerung Abstand zu nehmen.

Eine verfassungsrechtliche Einhegung rechtsdurchsetzungsfähiger Technologien jenseits spezifisch-situativer Abwägungsoffenheit versucht hingegen zu liefern, wer den Einsatz von Technologien der künstlichen Intelligenz *technologiespezifisch* zu einer Frage der Menschenwürde erklärt (Art.1 Abs.1 GG, gleichsinnig Art.1 GRC).⁵¹⁰ Wegen Art.79 Abs.3 GG wäre diese Strategie besonders dauerhaft und könnte auch gegen unionsrechtlich angeordnete Unmöglichkeitstrukturen ins Feld

geforderte Legitimationszusammenhang (oder, mit Hoffmann-Riem, a. a. O., S. 129 [144 f.], das geforderte Legitimationsnetz, mittlerweile weniger gebräuchlich: die notwendige Legitimationskette) nicht aus der einzelnen Person des Amtsträgers. Denn der für sich genommen ist dem anderen Menschen (eben auch) eine *Black Box* (vgl. unten, ab → S. 308). Legitimation ergibt sich erst aus dem *Interaktionszusammenhang* zwischen Menschen, in dem Bedeutung durch menschlich nachvollziehbare Interaktion geschaffen wird. Dieser Vorgang der Konstruktion von intersubjektiv nachvollziehbarer Bedeutung erfolgt immer *ex post*; a. A. aber wohl Unger, a. a. O., S. 113 [128], wonach *ex post* Beurteilung der blinde Fleck sei, weil demokratische Legitimation einen prospektiven Charakter haben müsse. Die Beurteilung, dass bzw. ob die Steuerungsleistung von Gesetz und Aufsicht im konkreten Handeln eines Amtsträgers (richtig) gewirkt hat, lässt sich aber immer nur *ex post* beurteilen, und *ex ante* nur auf Basis bisheriger Erfahrungen prognostizieren. Nicht entscheidend ist daher auch die eventuelle ‚Unvorhersehbarkeit‘ der Maschine. Denn die ist dem Amtsträger *in concreto* eben auch zu eigen. Wichtig ist bei diesem vielmehr *ex ante* auch ‚nur‘ Verlässlichkeit (unten, → S. 363 ff.) und die Einbindung in eine Architektur, die diese Verlässlichkeit gewährleistet und forciert (dazu → S. 365 ff. und → S. 381 ff.). Oder, nochmals anders gewendet: Erst in der konkreten *Begegnung* eines Rechtsunterworfenen mit dem Beamten aktualisiert sich dessen demokratische Legitimation (demokratische Steuerung, Aufsicht und Kontrolle), und nicht schon in der isolierten *Person* des Amtswalters. Legitimation wird damit durch eine gesamthafte Verfahrensarchitektur konstituiert, die die Kontestation ermöglicht, dass diese *konkrete* Entscheidung *nicht* mit dem Willen des Legitimationssubjekts übereinstimme.

507 s. nur Britz/Eifert, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 147; Bernzen/Kehrberger, RW 10 (2019), 374 (403 ff.). Für eine Argumentation mit dem Rechtsstaatsprinzip s. Beaucamp, Rechtsdurchsetzung durch Technologie, 2022, S. 55 f., 67 f.

508 Zur Frage der Schrankenschränke des Zensurverbots, die spezifisch im Bereich der Kommunikationsgrundrechte wirken kann, → § 2 Rn. 338 und ab → S. 422.

509 Zu den Inkongruenzen von *Intelligent Surveillance* und *Impossibility Structures*, die der Konstruktion eines simplen Stufenverhältnisses hinsichtlich des Eingriffsgewichts entgegenstehen, ab → S. 173.

510 Vgl. etwa L. Hagen et al., in: Oberreuter (Hg.), Staatslexikon, ⁸2017, Abschnitt II.3.3: „Zudem ist das Recht zukunftsgerichtet, deshalb notwendig abstrakt und offen gehalten, konkretisierungs-, wertungs- und abwägungsbedürftig. Die im Kern auf einem Binärcode beruhenden Informationsstrukturen der digitalen Systeme werden dies in der Gesamtheit – jedenfalls auf absehbare Zeit – nicht angemessen rezipieren und verarbeiten können. Über die Verhältnisse des Menschen werden und sollten auch in Zukunft Menschen Recht sprechen. Dies ist in letzter Konsequenz *eine Frage der menschlichen Würde*“. Hervorhebung hier. Noch allgemeiner Becker, ZUM 2019, 636 (644): „Menschliches Verhalten muss aus menschlicher Sicht beurteilt werden.“ Vor dem Hintergrund von Art. 22 DSGVO wäre die Entgegnung hierauf: *Ja, aber nicht immer und nicht nur; der Zeitpunkt spielt eine Rolle, und das Betroffenenverhalten*. Zur Diskussion m. w. N. auch Schulz/Schmees, in: Augsberg/Schuppert (Hg.), Wissen und Recht, 2022, S. 561 (582 f.).

geführt werden. Aus der Verankerung in der Menschenwürde würde folgen, dass der Einsatz von KI-basierten Systemen nicht dazu führen darf, dass Menschen zum *Objekt* maschineller Entscheidung werden dürfen. Gleiches gilt freilich auch für menschliche Entscheidungen über andere Menschen, sodass die eigentlich relevante Frage ist, ob Menschen zum Objekt werden, *weil* sie Gegenstand maschinellen Entscheidens sind. Die Frage wird heute zu Recht weitgehend verneint,⁵¹¹ unter anderem auch vom europäischen Gesetzgeber, der mit Art. 22 DSGVO sowie Art. 11 JI-Richtlinie gerade kein unbedingtes Verbot automatisierten Entscheidens über Menschen statuiert hat (einschließlich *realen* Handelns im polizei- und sicherheitsrechtlichen Bereich), sondern ein komplexes Regel-Ausnahme-Gegenausnahme-Verhältnis, das im Ergebnis relativ viel Automatisierung zulässt, sofern „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der [von der automatisierten Entscheidung] betroffenen Person“ getroffen werden (Art. 22 Abs. 2 lit. b bzw. Abs. 3 DSGVO und Art. 11 Abs. 1 JI-Richtlinie).

- 251 Es ist vor diesem Hintergrund keineswegs mehr selbstverständlich, dass jene bisher auf Alternativlosigkeit basierende „implizite [...] Erwartung“ fortbesteht, „dass im demokratischen Rechtsstaat Subjekte über Subjekte entscheiden sollten, also Entscheidungen zur Verteilung von Freiheit ihrerseits ein Produkt zur Freiheit befähigter Wesen“⁵¹² sein *müssten*. Diskutiert wird folglich nicht mehr so sehr über das *Ob* der Übertragung von Entscheidungskompetenzen auf KI-Systeme, sondern vielmehr über das *Wie*.⁵¹³
- 252 Freilich steht in Sonderfällen noch das *Ob* in Zweifel: Das betrifft zum einen die vor allem im Völkerrecht zu verortende Frage, ob, wo und wann automatisierte *Waffensysteme* eingesetzt werden dürfen.⁵¹⁴ Für das nationale Recht und gerade auch mit Blick auf die oben genannten Anwendungsbeispiele von KI-basierten Systemen bei der Optimierung der Rechtsdurchsetzung relevanter dürfte die jüngst etwa von *Hans Peter Bull* zur Diskussion gestellte These sein, dass spezifisch Gesichtserkennungssoftware – ein zentrales Anwendungsfeld aktueller künstlicher Intelligenz – gegen Art. 1 Abs. 1 GG verstoße. *Bull* zufolge ist das so :

„Das menschliche Gesicht ist besonders schutzbedürftig, weil es [...] untrennbarer, unverlierbarer und öffentlich sichtbarer Ausdruck der Persönlichkeit ist. Seine Digitalisierung und Benutzung als Identitätskennzeichen bedeutet eine Missachtung der Person und berührt die menschliche Würde, die der Staat zu achten und zu schützen hat. Würde das digitalisierte Abbild des menschlichen Gesichts als Anknüpfungspunkt für technikgestützte Kontrollen genutzt, wäre die Verfügbarkeit des Einzelnen für diejenigen, die diese Technik beherrschen,

511 Statt vieler *Wismeyer*, in: Ebers et al. (Hg.), *RechtsHdb. KI und Robotik*, 2020, § 20 Rn. 45 ff., dort bes. Fn. 76 für weitere Nachw.

512 *Möllers*, in: Voßkuhle/Eifert/Möllers (Hg.), *GVwR I*, ³2022, § 2 Rn. 36.

513 *Wismeyer*, in: Ebers et al. (Hg.), *RechtsHdb. KI und Robotik*, 2020, § 20 Rn. 46.

514 Dazu *Stellpflug*, in: Ebers et al. (Hg.), *RechtsHdb. KI und Robotik*, 2020, § 32 m. w. N.

wesentlich gesteigert [...]. Die ‚Digitalisierung‘ der körperlichen Erscheinung würde m. E. gegen die Menschenwürde verstoßen und sollte ausdrücklich verboten werden.“⁵¹⁵

Man wird über die hinter dieser Auslegung stehenden Argumente diskutieren können. Allein, die Verortung in der Menschenwürdegarantie kann nicht überzeugen, was eine praktische Kontrollüberlegung zeigt: Würde die These stimmen, dass Gesichtserkennung einen Würdeverstoß darstellt, dann würden *Apple & Cie.* jeden Tag milliardenfach gegen die Würde der Nutzer ihrer *Smartphones* und *Tablets* verstoßen, wenn diese ihre Geräte mithilfe von *Face ID* und ähnlichen Gesichtserkennungsanwendungen entsperren. Denn bekanntlich ist die Würdegarantie zumindest des Art. 1 Abs. 1 GG unmittelbar drittschützend und auch für ihren Inhaber nicht disponibel. Diese Kontrollüberlegung zeigt, dass es eben stets auf den Zweck und den Verwendungskontext künstlich-intelligenter Systeme ankommt und ein isoliertes Abstellen auf ihre Leistungsfunktionen und Inputdaten rasch in die Irre führt.

b. Unterschiede und Inkongruenzen zur Überwachungskonstellation, ‚blinde Flecken‘ in Randbereichen. Bei aller Anknüpfbarkeit an vertraute dogmatische Figuren und der daraus folgenden Gelassenheit sollten bestimmte strukturelle Unterschiede zwischen Überwachung und Verunmöglichung nicht übersehen werden. Diese Unterschiede lassen es bei genauem Hinsehen dann doch zweifelhaft erscheinen, dass *Impossibility Structures* wirklich schon durch die „bestehenden Figuren“ hinreichend „differenziert adressiert werden“ können.⁵¹⁶ Ich will diese Einwände jeweils exemplarisch anhand der soeben unter → 3. (Datenschutzrecht⁵¹⁷), → 4. (Straßenverkehrsrecht⁵¹⁸), und → 5. (Verbot der Unterlassung von Hilfe⁵¹⁹) genannten Anwendungsbeispiele näher erläutern:

aa. ... am Beispiel des Datenschutzrechts. Mit seinem ausgedehnten Anwendungsbereich,⁵²⁰ seinen gerade im privaten Datenschutzrecht hochgradig unbestimmten Abwägungsklauseln,⁵²¹ seinen vielfältigen prozeduralen Verpflichtungen sowie den damit jeweils verknüpften massiven Haftungs- und Sanktionsdrohungen⁵²² erzeugt das Datenschutzrecht für private wie auch für öffentliche Datenverarbeiter⁵²³ einen erheblichen, zugleich diffusen Befolgungsdruck: Da das Recht *prima facie* so diffus bzw. im prozeduralen Bereich so kompliziert ist, müssen Datenverarbeiter unter der beständigen Sorge agieren, dass ihr Verhalten *ex post* von den zuständigen Stellen als

515 Bull, AöR 145 (2020), 291 (319).

516 Vgl. für die These, dass das recht zwanglos möglich sei, nochmals Britz/Eifert, in: Voßkuhle/Eifert/Möller (Hg.), GVwR I, 3/2022, § 26 Rn. 143.

517 Oben, → S. 143 ff.

518 Oben, → S. 146 ff.

519 Oben, → S. 150 ff.

520 s. Art. 2 DSGVO und die Einschätzung von GA Bobek dazu, → § 2 Rn. 182.

521 Vgl. insb. Art. 6 Abs. 1 S. 1 lit. f DSGVO.

522 Art. 82 ff., bes. Art. 83 Abs. 5 DSGVO.

523 s. Art. 7 Abs. 1, Artt. 8, 9 Abs. 2, 10, und bes. Artt. 12 ff. DSGVO.

rechtswidrig beurteilt und eventuell mit erheblichen Sanktionen belegt werden wird. Das dabei behördlicherseits bestehende Sanktionsermessen kann und soll zwar selbstverständlich dem Gebot der Verhältnismäßigkeit entsprechend so angewandt werden, dass ein einfacher/erstmaliger Verstoß nicht bereits existenzvernichtende Sanktionen nach sich zieht – aber: *man weiß ja nie*.⁵²⁴ Durch den Verzicht auf ‚harte‘ sanktionsrechtliche Leitlinien⁵²⁵ steht eben doch potentiell eine Strafdrohung von bis zu 20.000.000 EUR zunächst einmal im Raum. *Paart* man nun dieses (oder eben vergleichbare) Rechtsregime mit ‚intelligenter‘ *Überwachung*, dann dürfte greifbar werden, welche massiven Einschüchterungseffekte davon auf den ungehinderten Verkehr personenbezogener Daten ausgehen können.

- 256 Blicken wir nun auf die *Impossibility Structures*: Behandelt man sie überwachungs-akzessorisch – eben wenn und weil sie *auch*, um funktionieren zu können, personenbezogene Daten verarbeiten müssen –, dann unterstellt man beiläufig (oder setzt voraus), dass vergleichbare *Chilling Effects* greifen. Das ist aber keineswegs selbstverständlich: Denn im Fall einer Unmöglichkeitstruktur wird das Verhalten, das potentiell rechtswidrig ist, ja gerade *verhindert*, sodass es *zumindest als vollendete Tat* (im weiten, nicht zwangsläufig nur strafrechtlichen Sinn) auch nicht mehr sanktioniert werden kann. Plakativ ausgedrückt: Das einschüchternde Gefühl des *man weiß ja nie*, welches mit einer Überwachung, die zunächst und definitionsgemäß geschehen lässt, um *ex post* zu sanktionieren oder sonst wie zu reagieren,⁵²⁶ wäre durch die Gewissheit eines *das darf ich nicht* ersetzt – zumindest *dann*, wenn keine Sanktion für den bloßen Versuch droht und/oder der Versuch nicht sogar noch bei berufener Stelle gemeldet wird (dann wären wir wieder bei *Intelligent Surveillance*).
- 257 Das bedeutet: Gerade im Bereich schwer zu befolgenden Rechts können *Impossibility Structures* eine die *Rechtsbefolgung erleichternde und assistierende Funktion* haben, die anstelle von Einschüchterung eine *Entlastung* bewirkt.⁵²⁷ Nicht nur die Angst vor sanktions- oder haftungsrechtlichen Folgen könnte damit erheblich gemindert werden, sondern auch schlicht der kognitive und praktische Aufwand der Rechtsbefolgung an sich. Natürlich kommt es dafür auf die konkrete Ausgestaltung nicht nur der eigentlichen *Impossibility Structure*, sondern des sie sozusagen umgebenden Regelungsarrangements an (wann greift die Verunmöglichung, gibt es Sanktionen für den bloßen Versuch etc.). Aber im Grundsatz ist das – also die potentielle

524 Vgl. für diese Argumentationsfigur des *Man-weiß-ja-nie* als Hintergrundfolie der Dogmatik der Einschüchterungseffekte schon Rademacher, JZ 2019, 702 (705 f.).

525 Vgl. Art. 85 Abs. 2 DSGVO, der eine lange Liste teils sehr vage formulierter Faktoren enthält, die bei der Verhängung von Sanktionen „im Einzelfall [...] gebührend berücksichtigt“ werden müssen.

526 Auch Moll/F. Schneider, Monatsschrift für Kriminologie und Strafrechtsreform 104 (2021), 92 (8) weisen darauf hin, dass bei den von ihnen untersuchten Studien zum Nachweis bzw. zur Widerlegung von *Chilling Effects* staatlicher Überwachung „das zugrundeliegende Motiv [jeweils] identisch ist[:] abstrakt befürchtete Sanktionen sollen vermieden werden“.

527 Dazu nochmals vertiefend → S. 358 f.

Entlastungsfunktion – eine bislang dogmatisch und theoretisch wenig ausgelotete Funktion von *Compliance*-Strukturen.

Diese Entlastung ergibt gerade im diffusen Datenschutzrecht offensichtlich guten 258 Sinn, weshalb wiederum Art. 25 Abs. 1 DSGVO mit seiner potentiell flächendeckenden Anordnung von Unmöglichkeitsstrukturen auch *prima facie* viel weniger unfreiheitlich wirkt, als es in anderen, von den Rechtsadressaten einfacher zu bewältigen Rechtsbereichen der Fall sein würde. Übrigens: Mit der Anlassdogmatik des Bundesverfassungsgerichts (einschließlich der Ausnahme der besonderen Verantwortlichkeit qua Gefahrschaffung/-beherrschung⁵²⁸) lässt sich Art. 25 Abs. 1 DSGVO nicht mehr erklären:⁵²⁹ Weder sind die Vorgaben anlassgebunden, noch kann die Verarbeitung von personenbezogenen Daten pauschal als besonders gefahrgeneigte Tätigkeit gewertet werden, ohne das Konzept gänzlich zu verwässern⁵³⁰ – dafür ist sie zu allgegenwärtig.

bb. ... am Beispiel des Straßenverkehrsrechts. Ein weiterer Unterschied zur Überwa- 259 chungskonstellation lässt sich am Straßenverkehrsrecht illustrieren, dort speziell an § 1e Abs. 2 Nr. 5 StVG. Zur Erinnerung: Ein autonomes Kfz muss *grundsätzlich* von der sogenannten Technischen Aufsicht, also einem Menschen, übersteuert werden können; es muss aber seinerseits die Technische Aufsicht ausnahmsweise übersteuern können, wenn es erkennt, dass das menschlich angewiesene „Fahrmanöver am Verkehr teilnehmende oder unbeteiligte Personen gefährden würde“ – das ist der oben sogenannte ‚doppelte Boden‘ der Regelungen zum autonomen Fahren, der das Fahrzeug partiell zur *Impossibility Structure* macht.⁵³¹ Die m. E. offensichtliche Legitimität einer Unmöglichkeitsstruktur an dieser spezifischen Stelle rührt daher, dass hier eine – jedenfalls in aller Regel – rechtswidrige Handlung *durch* ein KI-System ausgeführt werden würde, das von vornherein und zwangsläufig – eben um seine regulären Funktionen erfüllen zu können – mit entsprechenden Erkenntnistechnologien ausgestattet ist/sein muss.

Noch deutlicher wird die Legitimität von *Impossibility Structures*, wenn wir vom § 1e 260 Abs. 2 Nr. 5 StVG vermutlich zugrundeliegenden Szenario einer ‚nur‘ fahrlässigen Gefährdung von Personen durch die Technische Aufsicht in ein Vorsatzszenario wechseln: Dass ein intelligentes robotisches System den Befehl „Töte so viele Menschen wie möglich“ wird verweigern müssen, liegt auf der Hand. Formaler ausgedrückt: Ein KI-System darf und muss eine Handlung, die es gleichsam zu einem (Mit-)Täter bzw. (Mit-)Störer im Rahmen der jeweiligen Verantwortungssysteme

528 s. dazu oben, bei → § 2 Rn. 106.

529 Unmittelbar einschlägig sind im Fall des Art. 25 DSGVO natürlich nur die Unionsgrundrechte. Es geht mir um die Stimmigkeit und ‚Durchhaltbarkeit‘ der Argumentation des BVerfG.

530 Zu ähnl. Bedenken hinsichtlich der Steuer- und Geldwäscheüberwachung schon → § 2 Rn. 105.

531 Vgl. oben, → § 2 Rn. 192 f.

machen würde, verweigern, wenn, weil und sobald es technisch dazu in der Lage ist, eine solche Einordnung vorzunehmen (d. h. eine *Law-abiding Technology*⁵³² ist/sein können muss).⁵³³

261 cc. ... am Beispiel von § 323c StGB. können wir noch einen Schritt weiter gehen: In dem den Überlegungen zugrundeliegenden und – wie schon gesagt – futuristischen Szenario geht es um die Frage, ob rechtswidrige menschliche Handlungen, die *im Beisein* einer entsprechend rechtserkenntnisfähigen künstlichen Intelligenz geschehen, von dieser KI verhindert werden muss bzw. verhindert werden darf. Ich habe oben argumentiert, dass die Frage grundsätzlich und in der Logik des § 323c StGB denkend, mit einem Ja beantwortet werden kann.⁵³⁴ Mit Überwachungsakzessorität lässt sich diese Konstellation nicht mehr recht fassen, wenn und weil sich die besondere Legitimation von § 323c StGB gerade aus dem zufälligen Anwesend-Sein des zur Hilfe Verpflichteten ergibt.⁵³⁵ Ich komme speziell auf diesen Gedanken der Hilfeleistung im Fazit zu → § 2 ausführlich zurück.⁵³⁶

262 dd. ... bei der Erfassung bestimmter Sonderformen von *Impossibility Structures*. Denken wir abschließend nun noch einen Schritt weiter und kombinieren dafür eine *anwesende* rechtserkenntnis- und aktionsfähige Technologie mit den neuen Erkenntnismethoden, die oben⁵³⁷ beschrieben wurden: Man stelle sich eine hochgradig avancierte *Impossibility Structure* vor, die ausschließlich mit LiDAR- oder vergleichbaren Technologien arbeitet, und die in der Lage ist, entsprechend der Idee von § 323c StGB Rechtsverletzungen zu verhindern bzw. ihre weitere Ausführung zu unterbinden. In dem Fall würde das Recht auf informationelle Selbstbestimmung keinen Schutz mehr liefern, *weil* keine personenbezogenen Daten verarbeitet werden und *wenn* das System auch nicht darauf angelegt wäre, eine *ex-post*-Identifikation zu leisten.⁵³⁸ Natürlich würde in dem Fall noch für den physischen Zugriff als solchen (jedenfalls wenn das System hoheitlich vorgeschrieben ist) Art. 2 Abs. 1 GG oder ein spezielles deutsches oder unionales Grundrecht greifen – aber doch nur *insoweit*, als die Verunmöglichung Rechtsgüter/-handlungen betrifft, die nicht rechtswidrig sind (also z. B.: kein letaler Schuss, um einen geringfügigen Angriff auf das Eigentum abzuwehren⁵³⁹). Der vom Recht auf informationelle Selbstbestimmung *im Vorfeld* von Rechtsverletzungen geleistete Schutz hingegen, der den Einzelnen davor bewahrt, „beliebig [über die eigene] Rechtschaffenheit Rechenschaft ablegen zu müssen“,⁵⁴⁰

532 Zum Begriff oben, → § 1 Rn. 59.

533 s. zur Frage der Verallgemeinerung dieser Norm schon soeben, → § 2 Rn. 204 f.

534 s. soeben, → § 2 Rn. 220.

535 Vgl. oben, → § 2 Rn. 232.

536 Unten, → § 2 Rn. 428 ff.

537 Oben, → § 2 Rn. 28 ff.

538 Zu deren Relevanz → § 2 Rn. 129.

539 s. dazu knapp → § 2 Rn. 246.

540 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51.

dieser Schutz greift nicht mehr. Das Gedankenexperiment, so futuristisch und so beschränkt hinsichtlich des Anwendungsbereichs⁵⁴¹ es uns zunächst erscheinen mag, ist doch geeignet, die Nachhaltigkeit der Bewältigung von *Impossibility Structures* allein durch das Recht auf informationelle Selbstbestimmung in Zweifel zu ziehen.

ee. Gebot einer eigenständigen Dogmatik für Impossibility Structures. Die soeben 263
schlaglichtartig illustrierten Unterschiede und Inkongruenzen zwischen Überwachungs- und Verunmöglichungsszenarien tauchen in der bisherigen Diskussion über *Impossibility Structures* so noch nicht auf, wenn und weil sie rein *überwachungsakzessorisch* geführt wird. Das ist praktisch gesehen weitgehend unschädlich, vielleicht einmal abgesehen davon, dass die möglicherweise entlastende und deshalb willkommene Funktion von *Impossibility Structures* allzu *restriktiv* – da eben *überwachungsakzessorisch* – behandelt zu werden droht. Gerade die Überlegungen, die hier zuletzt angestellt wurden, und die zugegebenermaßen weit in die Zukunft ausgreifen, was die technische Leistungsfähigkeit der Systeme anbelangt, zeigen aber auch, dass die *überwachungsakzessorische* Bewältigung, weil sie auf dem Recht auf informationelle Selbstbestimmung aufbaut, zu *permissiv* sein könnte. Deshalb: Es bedarf einer von vornherein eigenständigen Dogmatik von und für *Impossibility Structures*, die den Unterschieden zwischen Überwachung und Verunmöglichung gerecht wird und das eine nicht als schlicht Mehr des anderen behandelt.

c. Rechtstheoretische Implikationen von Impossibility Structures. Die *rechts-theoretische* 264
Diskussion zu *Impossibility Structures* unterscheidet nun dezidiert zwischen Überwachung und Verunmöglichung und ist ohne Scheu zukunftsorientiert; d. h., sie geht mittlerweile durchaus der Frage nach, welche Rückwirkungen die zumindest denkbare flächendeckende Einführung von Rechtsverletzungen verhindernden Arrangements auf das Recht und seine Funktionen haben könnte.⁵⁴² Und *diese* Diskussion ist *nicht* von Gelassenheit geprägt, sondern von einer sehr deutlich artikulierten Besorgnis. Zwei Stränge lassen sich dabei unterscheiden, die freilich miteinander verflochten sind:

aa. Entdialogisierung der Rechtsanwendung. Die erste Besorgnis soll hier als Gefahr 265
der Entdialogisierung von Rechtsbefolgung und -anwendung bzw. Rechtsdurchsetzung bezeichnet werden. Beispielhaft hierfür stehen die Überlegungen von Klaus Günther, der anhand von ‚intelligenten‘ – d. h. Normbefolgung erzwingenden – Fahrzeugen, Upload-Filtern, und *Smart Contracts* argumentiert, dass sich

541 LiDAR- und vergleichbare Technologien werden sich *eventuell* einmal zur Erfassung physischer Handlungen von Menschen eignen, vgl. → § 2 Rn. 28 ff.; zur Überwachung bzw. Verunmöglichung von Kommunikation etwa taugen sie schon methodisch (wohl) nicht.

542 Zu nennen sind bspw. *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 63 ff. (wobei sich dort auch rechtssoziologische Erwägungen finden); *Günther*, in: Forst/Günther (Hg.), *Normative Ordnungen*, 2021, S. 523 ff.; *Burchard*, ebd., S. 553 ff.; *Burchard*, JRE 27 (2019), 527, S. 527 ff.; *Möllers*, *Die Möglichkeit der Normen*, 2018, S. 452 ff., 471 ff.

„[p]erfekte Normbefolgung [...] nicht mehr *mit* dem, sondern *ohne* den Adressaten [vollziehe]. Die Norm selbst wird in einen technischen Vorgang transformiert, an den sich die Betroffenen nur noch anpassen, den sie durch ihr Verhalten aber nicht mehr beeinflussen können. [...] Die Person der Normadressat*innen wird dabei so konfiguriert, als sei sie ein potentiell störungsanfälliger Teil des technischen Normrealisierungsprozesses.“⁵⁴³

- 266 Dadurch, dass folglich Normen nicht mehr als „Gründe“ für ihre Adressaten fungieren würden, sich *eventuell* dem Normbefehl entsprechend zu verhalten,⁵⁴⁴ verliere der Prozess der Normrealisierung seinen „kommunikativen“ Charakter,⁵⁴⁵ wodurch wiederum die für normative Ordnungen prägende „Praxis der Verantwortung, Rechtfertigung und Kritik ihrer Anwendungsoperationen“⁵⁴⁶ verloren zu gehen drohe. Die – in der *rechtsdogmatischen* Diskussion soweit ersichtlich ausnahmslos geforderte – Möglichkeit von *ex-post*-Rechtsschutz und damit eines zumindest nachgelagerten Diskussionsforums taucht bei *Günther* soweit ersichtlich zwar nicht explizit auf; allerdings reiche sie gerade nicht aus, so lässt sich *Günther* m. E. deuten, weil Normen in den von ihm sogenannten smarten Ordnungen „[m]it ihrer Verdinglichung [in ihrem] Verbindlichkeitsanspruch zunehmend fraglos und ihre Rechtfertigung und Kritik ähnlich sinnvoll wie beim Wetter“ würden.⁵⁴⁷
- 267 *bb. Entflexibilisierung der Rechtsanwendung.* Eng verknüpft mit der Frage nach der Entdialogisierung von Recht bzw. den entsprechenden Befolgings- und Anwendungsoperationen ist die Beobachtung einer durch die „Verdinglichung“ (*Günther*) drohenden Entflexibilisierung. Herausgestellt ist damit das normative Leistungspotential des Vollzugs- und Sanktionenrechts, insbesondere der *darin* verbauten Ermessensspielräume zur Realisierung eines Interessensausgleichs (Verhältnismäßigkeit im Einzelfall), den das materielle Recht nicht vorwegnehmen kann oder nicht vorwegnehmen will.⁵⁴⁸ Fallen Norm und Normrealisierung durch den Einsatz von *Impossibility Structures* in eins, dann gehen *diese* Ermessensspielräume *an dieser spezifischen Stelle* notwendigerweise verloren.

543 *Günther*, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (535). Hervorhebungen im Original.

544 *Ibid.*, S. 538, unter Verweis auf *Joseph Raz*.

545 Vgl. *ibid.*, S. 545. Vgl. auch schon *Hildebrandt*, Smart Technologies and the End(s) of Law, 2016, S. 181: Recht als „platform for argument and contestation“.

546 *Günther*, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (542). Ähnl. *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 69: „Der Verstoß gegen eine Rechtsnorm und der sich daraus ergebende rechtliche Konflikt bieten stets auch die Möglichkeit der Rechtsfortbildung. Diese ist im Rechtsstaat Aufgabe der Gerichte. Wenn durch die Architektur der digitalen Sphäre geformte Strukturen zur Durchsetzung von Regeln abweichendes Verhalten unmöglich machen, schließen sie ein Herantragen des juristischen Konflikts an die Gerichtsbarkeit und damit eine richterliche Entscheidung aus.“

547 *Günther*, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (545).

548 Vgl. dazu *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn.145; *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 67 ff.; früh und grundlegend schon *F. Hofmann*, in: Fries/Paal (Hg.), Smart Contracts, 2019, S. 125 (130 ff.).

Das macht in einem ersten Schritt Rückfragen an das materielle Recht unausweichlich: Ist es tatsächlich auf seinen vollen Vollzug angelegt, oder sind unter dem Prinzip der Verhältnismäßigkeit gebotene situative Anpassungen des tatsächlichen Realisierungsanspruchs der Norm bisher im Vollzugs- und Sanktionenrecht (vielleicht bislang unbemerkt) verarbeitet? Wenn es beispielsweise stimmt, dass ein Rotlichtverstoß eines Fußgängers „am helllichten Tage an einer übersichtlichen Stelle auf einer weder von einem Auto befahrenen noch von einem weiteren Fußgänger gesäumten Straße“ wegen Unverhältnismäßigkeit nicht sanktioniert [und auch nicht verhindert?⁵⁴⁹] werden darf,⁵⁵⁰ ist der materielle Normbefehl, die Straße trotz frappanter Ungefährlichkeit nicht zu queren, wohl doch allein der Verlegenheit geschuldet, unter den Funktionsbedingungen *nicht* smarter Zeitschalt-Ampeln ein Ordnungssystem zu schaffen, das den Verkehr in der Regel hinreichend verlässlich regelt, im Einzelfall aber einen Normbefehl aussprechen muss, der selbst eine Form von normativem *Overblocking* darstellt⁵⁵¹ und damit unbeachtlich ist.⁵⁵² Seine technische Erzwingung wäre damit ebenfalls *Overblocking* der Fortbewegungsfreiheit unseres Fußgängers und müsste sich in einer Abwägung von Nutzen und Schaden rechtfertigen.

Was also – sollen *Impossibility Structures* eingesetzt werden – ausgehend von diesem zugegeben trivialen Beispiel erforderlich ist, ist eine bewusstere Zusammenschau von materiellem und Vollzugsrecht und eine Herausarbeitung der *für den konkreten Rechtssatz* spezifischen Eigenleistungen des Vollzugsrechts. Das ist keineswegs trivial, eben weil derzeit das Vollzugs- und Sanktionenrecht eine oftmals übersehene, aber gewichtige Funktion beim Interessenausgleich haben. Anschlussfähig sind insoweit die Überlegungen von Franz Hofmann, der – zunächst am Beispiel des Immaterialgüterrechts – argumentiert hat, dass das, was in einem praktisch-realen Verständnis Recht ist, sich als Produkt aus dem materiellen Recht und der Wahrscheinlichkeit seiner Durchsetzung ergebe.⁵⁵³

Besonders deutlich – aber damit in gewisser Weise auch schon wieder uninteressant – wird die Spannweite der insoweit bestehenden Eigenleistungen des Vollstreckungs- und Sanktionenrechts beim ausschließlich symbolischen Recht (unterstellt, dass es

549 In diese Richtung, mit dem Bsp. der Geschwindigkeitsbegrenzung, deren „einhundertprozentig[e]“ Durchsetzung nach Auffassung des Autors „evident unverhältnismäßig“ wäre (warum eigentlich?), F. Hofmann, in: Fries/Paal (Hg.), Smart Contracts, 2019, S. 125 (137).

550 Rostalski, GA 166 (2019), 481 (484).

551 So schon Rademacher, JZ 2019, 702 (710).

552 Ähnl., am Bsp. von Parkverboten, G. Wagner, AcP 222 (2022), 56 (96).

553 F. Hofmann, in: Fries/Paal (Hg.), Smart Contracts, 2019, S. 125 (130 ff.); noch spezieller zum Immaterialgüterrecht ders., Der Unterlassungsanspruch als Rechtsbehelf, 2017, passim; anknüpfend und verallgemeinernd G. Wagner, AcP 222 (2022), 56 (90 ff.); auch Wischmeyer, in: Baumgärtel/Hoppen (Hg.), Informationstechnik und Recht, 2021, S. 9 Rn. 36.

das noch⁵⁵⁴ gibt): Vor dessen Hintergrund entspräche die vollständige Realisierung des materiellen, aber eben nur symbolischen Rechts

„schon deshalb nur scheinbar dem [demokratischen] Ideal, weil die Gesetze immer eine doppelte Bedeutung als Symbol und als Verwirklichungsanspruch haben und sich die Anteile unterschiedlich gestalten können – bis hin [eben] zur sog. symbolischen Gesetzgebung, die von vornherein nicht auf Verwirklichung angelegt ist.“⁵⁵⁵

- 271 Spannender ist, dass sich sämtliche Rechtsmaterien, die ihrer Normstruktur nach eine Abwehr von bloßen Gefahren statt realen Rechtsgutverletzungen bezwecken, besonders (neu) rechtfertigen müssen, wenn unter den Funktionsbedingungen einer verlässlich eingriffsbereiten KI eine Steuerung näher am unmittelbar gewünschten Schutzgut möglich wird. Neben dem soeben schon erwähnten Straßenverkehr steht hier vor allem das Datenschutzrecht unter einem möglicherweise zunehmenden Rechtfertigungsdruck.⁵⁵⁶ handelt es sich doch dabei insgesamt um Vorfeldschutz, der lediglich potentielle Gefahren verhindern soll statt gezielt reale Rechtsgutbeeinträchtigungen zu erfassen.
- 272 Verallgemeinernd lässt sich somit festhalten, dass der *tatsächliche* Realisierungsanspruch einer Norm ermittelt und gegebenenfalls durch eine Anpassung des materiellen (von der *Impossibility Structure* unmittelbar zu realisierenden) Rechts in eben diesem – also dem materiellen Recht – mit abgebildet werden muss;⁵⁵⁷ oder es müsste in einem zweiten Schritt im Wege einer Abwägung gerechtfertigt werden, warum die Übertragung des ‚nur‘ *normativen* = *kommunikativen Overblocking*, das in einem überschießenden Normbefehl liegt, in eine nun sogar *physisch* wirksame Struktur ausnahmsweise doch gerechtfertigt ist. Die Problematik wird dadurch potenziert, dass schon die Übertragung bestehender Differenzierungen bzw. bestehender Flexibilitäten im existierenden *materiellen* Recht (Abwägungsklauseln, Er-

554 In der frühen Neuzeit war der lediglich symbolische Erlass von Gesetzen durchaus üblich, die „[ihren] Sinn in sich selbst“ trugen, so *Schlumbohm*, *Geschichte und Gesellschaft* 23 (1997), 647 (659): Gesetze sollten demnach v. a. der Selbstproklamation einer „Obrigkeit als gute Obrigkeit“ dienen (S. 660, Hervorhebung im Original). Zur früheren Erwartung an die Rechtsdurchsetzung s. die These von *Schlumbohm* a. a. O., bes. S. 659 f.: „In der Frühen Neuzeit scheint [...] der rechten Form der Publizierung nicht selten mehr Aufmerksamkeit gegolten zu haben als der Überwachung der Befolgung. [...] Durch [die Publikation] erwies sich die Obrigkeit als gute Obrigkeit, zunächst im christlichen Sinn, in späterer Zeit nach aufgeklärter Art; sie gab kund, daß sie durch Ge- und Verbote die rechte Ordnung proklamierte. Das war schon ein wesentlicher Teil dessen, was von der Herrschaft erwartet wurde. Gewiß sollte sie sich auch um eine Realisierung dieser guten Ordnung bemühen, aber den Erwartungen der Zeitgenossen scheint in dieser Hinsicht ein exemplarisches auswählendes partielles Vorgehen genügt zu haben. [...] Daß es von jeher im Lande Sitte war, die Hochfürstlichen Verordnungen vor den Gemeinden herabzulesen und sodann nicht zu halten, ist wohl erst seit dem späten 18. Jahrhundert unerträglich geworden. Zuvor war beim Erlassen von Gesetzen der symbolische Aspekt ebenso wichtig, manchmal wichtiger, als die Absicht, tatsächliches Verhalten zu ändern.“ Hervorhebung im Original.

555 *Britz/Eifert*, in: *Vofkuhle/Eifert/Möllers* (Hg.), *GVwR I*, ³2022, § 26 Rn. 143, dort Fn. 447.

556 Vgl. hierzu schon *Rademacher*, *JZ* 2019, 702 (710).

557 Vgl. auch *F. Hofmann*, in: *Fries/Paal* (Hg.), *Smart Contracts*, 2019, S. 125 (137 ff.); *G. Wagner*, *AcP* 222 (2022), 56 (97).

messenstatbestände etc.) in technische Regeln erhebliche Schwierigkeiten bereitet (siehe ausführlich → § 3), womit die Sorge verbunden ist, dass die Überführung von Normen in Technik selbst zu Vereinfachungen und Pauschalisierungen zwingt, die das Recht ärmer, jedenfalls weniger Einzelfall-adäquat machen könnten, als es jetzt ist.⁵⁵⁸

cc. Re-Dialogisierung und -Flexibilisierung durch ex-post-Lösungen. Das freilich 273 führt nun wieder zurück zu der Frage, ob und wo eine Re-Dialogisierung und -Flexibilisierung der Anwendungsoperation durch *ex-post*-Lösungen (Beschwerdeverfahren, Rechtsschutz oder ähnliche) gerechtfertigt sein kann, die es dem originären (also menschlichen) Erstadressaten einer technisch vollzogenen Norm möglich machen, aber eben auch zumuten, gegen eine technische (vermeintlich oder tatsächlich: falsche) Realisierung vorzugehen.

Dass diese Abwägung durchaus zugunsten von *ex-post*-Lösungen ausgehen kann, 274 die dem Erstadressaten Angriffslasten aufbürden, die es in der analogen Welt nicht gab,⁵⁵⁹ zeigen die referierten Beispiele aus der Rechtsprechung des EuGH und der unionalen Gesetzgebung.⁵⁶⁰ Dieser Punkt ist von zentraler Bedeutung: Eine Bestandsgarantie für das überkommene Vollzugsrecht in dem Sinn, dass jeder physische Vollzug eine menschliche Vollzugsentscheidung im Einzelfall voraussetzen und damit jedenfalls weiterhin als Ort des (weiteren⁵⁶¹) Interessensausgleichs bzw. einer entsprechenden Diskussion bereitstehen würde, also eine Bestandsgarantie des analogen Status quo, die gibt es nicht.⁵⁶²

Aus der Rechtsprechung lässt sich aber immerhin als eine *dogmatische* Konsequenz 275 aus der *theoretischen* Diskussion um den Verlust von Flexibilitätsreserven des Vollzugs- und Sanktionenrechts ableiten, dass *Impossibility Structures* prinzipiell *nicht* im Wege von Generalklauseln eingeführt werden dürfen. Erforderlich ist stattdessen eine auf den *spezifischen* Rechtssatz ausgerichtete Diskussion um die Leistungsfähigkeit der Technik, die Möglichkeit und Zumutbarkeit aktiven Handelns der in welcher Form auch immer ‚geblockten‘ Erstadressaten des Rechtssatzes gegen die Blockierung, sowie eine Diskussion um den spezifischen Realisierungsanspruch des materiellen Rechts. Übergreifend geleitet werden muss diese Analyse von den Kriterien der *Rechtzeitigkeit* von *ex-post*-Lösungen, der *Reversibilität* etwaiger Beein-

558 Günther, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (542 f.); vgl. auch G. Wagner, AcP 222 (2022), 56 (98); dazu auch unten, → S. 291 ff.

559 Vgl. Hoffmann-Riem, AöR 145 (2020), 1 (34): „Hier führt der Einsatz von Techniken zur Veränderung der Wirkungsweise von Recht und zugleich zu Veränderungen in den Machtverhältnissen der an dem Rechtsverhältnis Beteiligten.“ – die, so ist zu ergänzen, in manchen Fällen unerwünscht, in anderen durchaus erwünscht sein können.

560 → § 2 Rn. 153 ff. und → § 2 Rn. 157 ff. bzw. → § 2 Rn. 166 ff.

561 D. h. neben dem materiellen Recht und den Möglichkeiten einer *ex-post*-Korrektur.

562 Ausf. Beaucamp, Rechtsdurchsetzung durch Technologie, 2022, S. 67 f. und passim.

trächtigungen individueller oder kollektiver Güter und/oder gegebenenfalls hinreichender *Kompensationsmöglichkeiten* im Fall eines *Over-* bzw. *Underblocking*.⁵⁶³ Es geht um Risikoverteilung, die vom materiellen Recht auszugehen hat, dabei den Faktor *Zeit* hinreichend berücksichtigt, und somit an das Recht des einstweiligen, insbesondere des vorbeugenden Rechtsschutzes erinnert.⁵⁶⁴ Auch wenn an dieser Stelle keine Analyse zur Übertragbarkeit der Kriterien aus diesem Bereich geleistet werden kann, zeigt der gedankliche Exkurs auf, dass die Aufgabe einer gestaltenden Neuverteilung von Durchsetzungsrisiken von Recht und Rechten keine unbekannte ist.

- 276 Hat sich damit also gezeigt, dass es gute Gründe gibt, zwischen Überwachung und Verunmöglichung durch neue Technologien rechtsdogmatisch und rechtstheoretisch zu unterscheiden, so drängt sich geradezu die Frage auf, ob es zwischen *Impossibility Structures* auf der einen und *Intelligent Surveillance* auf der anderen Seite nicht noch weitere ‚intelligente‘ Strukturen bzw. Arrangements geben könnte, die die Gefahren der Entdialogisierung und Entflexibilisierung vermeiden, aber gleichwohl einen Impuls in Richtung einer gegenüber dem Status quo verbesserten Rechtsrealisierung liefern können. Solche Zwischenmodelle gibt es und um sie wird es nun unter → III. und → IV. gehen.

III. Compliance Assistance Technologies (i. e. S.)

- 277 Zunächst soll auf der Suche nach Zwischenmodellen der Gedanke der *Assistenz* bei der Realisierung von Recht⁵⁶⁵ wieder aufgegriffen werden. Wie gesagt hat der Einsatz von digitalen *Impossibility Structures* gerade im physischen wie auch virtuellen Massenverkehr mit seinen vielen niedrigschwelligen Regelbrüchen eine besondere Plausibilität: Es ging in allen soeben genannten Einsatzfeldern stets um die Verarbeitung von alltäglich massenhaft anfallenden Daten bzw. um Alltagssachverhalte mit – im Fall von Rechtsverstößen – oft geringen Einzelschadenssummen,⁵⁶⁶ sodass menschliche Überwachung oder anschließende menschliche Durchsetzung der Regeln unmöglich oder unökonomisch wären. KI hingegen ist geradezu für die

563 Vgl. hierzu BVerfG NVwZ 2009, 240 (240 f.), zu Art. 19 Abs. 4 GG, dort auch – S. 242 – zu dreipoligen Rechtskonstellationen, in denen sich pauschale Aussagen zur Verteilung von Beweis- und Angriffslasten und der Ausgestaltung des einstweiligen Rechtsschutzes richtigerweise von vornherein verbieten.

564 Vgl. insoweit immer noch instruktiv *Schoch*, Vorläufiger Rechtsschutz und Risikoverteilung im Verwaltungsrecht, 1990, S. 966 ff.; hierzu auch *Schmidt-Aßmann*, in: Dürig/Herzog/Scholz (Hg.), GG, Lfg. 92 August 2020, Art. 19 Abs. 4 Rn. 278, demzufolge die Frage nach dem „rechtzeitigen“ Rechtsschutz als Teil des Gebots *wirksamen* Rechtsschutzes – und d. h.: *real* wirksamen Rechtsschutzes – letztlich die gesamte Dogmatik der grundrechtlichen Rechtsschutzgarantie durchziehe.

565 s. soeben, → § 2 Rn. 257.

566 Wenn man von terroristischen Anschlägen einmal absieht.

schnelle, kostengünstige und potentiell ubiquitäre Verarbeitung großer Datenmengen prädestiniert, einschließlich der zielgerichtet-physischen Verhinderung rechtlicher Devianz.⁵⁶⁷

Perfekt ist die Passung gleichwohl (noch) nicht: Denn – um in den Beispielen von 278
→ II., zu bleiben – sowohl das Straßenverkehrsrecht als auch das Datenschutzrecht, wie auch das Urheber- und erst recht das Ehrschutzrecht zeichnen sich trotz oder vielleicht gerade wegen ihrer Alltäglichkeit durch große Kontextsensibilität aus. Die *prima facie* häufig eindeutigen Regeln kennen zahlreiche Ausnahmen, deren Aktivierung stark von den Umständen des Einzelfalls abhängt; und das gilt sowohl tatsächlich wie auch rechtlich, wenn und weil nach der rechtlich geleiteten Suche nach einschlägigen Tatsachen anschließend Abwägungsentscheidungen zu treffen sind. Es sei nur kurz auf die Schranken des Urheberrechts in §§ 44a ff. UrhG hingewiesen oder auf die Anwendung von Normen des rechtfertigenden Notstands im Straßenverkehrsrecht. Zwar können bestimmte Abwägungsparameter und -ergebnisse in verallgemeinerter Form auch einer KI ‚beigebracht‘ werden:⁵⁶⁸ Etwa, dass in einer Dilemma-Situation im Straßenverkehr einem Unfallgeschehen mit ‚nur‘ Tierschaden der Vorzug vor Menschenleid zu geben ist. Und auch der ethisch immer wieder neu diskutierte Lorenfall ist rechtlich recht eindeutig zu beantworten und damit potentiell programmierbar.⁵⁶⁹

In vielen anderen Fällen gilt das aber nur eingeschränkt: Ob etwa das Überfahren 279
der roten Ampel tatsächlich im Sinn des rechtfertigenden Notstandes erforderlich ist, um den Schwerverletzten auf der Rückbank ins nächstgelegene Krankenhaus zu bringen, dürfte in der notwendigen Allgemeinheit derzeit noch schwer programmier- oder trainierbar sein, selbst unter Rückgriff auf hybride Modelle von KI.⁵⁷⁰ Dasselbe gilt erst recht für die Frage, ob ein negatives Werturteil über eine andere Person z. B. in den sozialen Medien im konkreten Fall noch erlaubte Meinungsäußerung oder schon unzulässige Beleidigung ist. Denn selbst in den vom Bundesverfassungsgericht für *ohne* Einzelfallabwägung für unzulässig erklärten Fallgruppen der Schmähkritik, Formalbeleidigung und des Menschenwürdeverstosses durch den Inhalt der Äußerung dürfte nur die Formalbeleidigung ohne Weiteres automatisiert

567 s. systematisch zum Mensch-Maschine-Leistungsvergleich unten, → S. 278 ff.

568 Dazu nochmals unten mehr, → § 3 Rn. 54 ff.

569 Vgl. zur ethischen Diskussion und zu einer Studie über „mehrheitsfähige“ Kriterien zur Entscheidung in moralischen Dilemma-Situationen *Awad et al.*, *Nature* 563 (2018), 59.

570 s. dazu → S. 59 ff.

erkennbar sein; nur sie fordert ausdrücklich⁵⁷¹ keine Kontextualisierung des Gesagten.⁵⁷²

- 280 Technisch ausgedrückt ist daher die Gefahr von *False Positives* und *False Negatives*,⁵⁷³ die bei der Anwendung von *Impossibility Structures* definitionsgemäß sogleich in ein *physisch* (un)wirksames *Over-* bzw. *Underblocking* umschlagen, in vielen Anwendungsbereichen erheblich. Die Zurückhaltung des Europäischen Parlaments jenseits von Art. 25 Abs. 1 DSGVO, den Einsatz von „technischen Mitteln“ zur Verhinderung von rechtswidrigem Verhalten vorzuschreiben, ist folglich gut nachvollziehbar.⁵⁷⁴ Aber: Die hier folgenden Ausführungen (und später noch die Überlegungen unter → IV.) sollen zeigen, dass Rechtsrealisierung durch und mit KI keine Entweder-oder-Frage ist.

1. Begriff

- 281 Soll trotz der soeben benannten Schwierigkeiten nicht auf den Nutzen automatisierter Systeme der Rechtsrealisierung verzichtet werden, wäre zunächst, als erste Alternative zu *Impossibility Structures*, an den Einsatz reiner Unterstützungssysteme zu denken, die hier als *Compliance Assistance Technology* im engen Sinn bezeichnet werden. Die Idee dahinter ist, dass ein automatisiertes Erkennungssystem, wenn und wo die Gefahr des *Overblocking* für zu groß erachtet wird, die Nutzer eben nicht blockiert bzw. allgemeiner: eine Rechtsfolge nicht automatisiert bewirkt, sondern nur, aber immerhin, informiert, dass ein begonnenes Verhalten rechtswidrig sein könnte oder auch: informiert, welches Verhalten rechtmäßig wäre.⁵⁷⁵
- 282 Es geht also um den *konkreten*, d. h. auf einen Sachverhalt konkretisierten „Zugang zu Normwissen“⁵⁷⁶ gerade auch für juristische Laien, die nach der Konzeption zahlreicher Normen zugleich Erstanwender des Rechts sind bzw. zumindest sein (können) müssen. Gefragt ist nach Technologien, die Subsumtionsschlüsse für die weitere Verwendung durch Menschen, einschließlich juristischer Laien, liefern können.⁵⁷⁷ Dass sich Teile der *rechtstheoretischen* Lehre mit dieser Perspektive –

571 Irritierenderweise aber auch nur „in der Regel“, s. BVerfG, Beschl. v. 19.5.2020, Az. 1 BvR 2397/19 = NJW 2020, 2622, Rn. 21.

572 Zu diesen drei Kategorien die Übersicht *ibid.*, Rn. 18 ff. Krit. zum Stand der Ehrschutz-vs.-Meinungsfreiheit-Judikatur des BVerfG *Teichmann*, JZ 2020, 549 ff. Die Rspr. verteidigend hingegen *Hong*, *Apropos Künast-Fall*, Verfassungsblog v. 20.06.2020 (online).

573 Zu den Begriffen oben, → § 1 Rn. 12.

574 Vgl. am Bsp. der VO (EU) 2021/784 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (TCO-VO) oben, → § 2 Rn. 168.

575 Konstruktiv deckt sich das mit der von *Hähnchen/Bommel*, JZ 2018, 334 (337) sog. „präventiven Rechtsberatung“.

576 *Hoffmann-Riem*, AöR 145 (2020), 1 (17, 8).

577 Da Subsumtionsschlüsse definitionsgemäß ein Produkt von Sachverhaltswissen und Normwissen darstellen, wird im Folgenden auch nicht strikt zwischen Technologien zur Beantwortung von Rechts- bzw.

Laien als Rechtsanwender – schon traditionell und auch gerade wieder neu im Zusammenhang mit Technologien der Rechtsdurchsetzung/-erkenntnis⁵⁷⁸ schwertun (weil sie Rechtsanwendungsoperationen im eigentlichen Sinn Juristen vorbehalten wollen⁵⁷⁹), ändert nichts daran, dass Normen nur selten zuerst an Juristen, sondern oft zuerst eben an Laien adressiert sind und daher von diesen verstanden und realisiert werden müssen. Auf diesen Grundlagenstreit wird später nochmals ausführlich zurückzukommen sein, wenn es in → Kapitel 2 um die Maßstäbe geht, die an rechtserkenntnis- und rechtsrealisierungsfähige Technologien anzulegen sind.⁵⁸⁰ Hier soll nur die Einsicht genügen, dass Laien bei der Realisierung des zwar an sie gerichteten, aber paradoxerweise nicht wirklich für sie geschriebenen Rechts in aller Regel Hilfe benötigen, womit eben das Konzept von *Compliance Assistance* relevant wird.

Um den Verzicht auf die physische Komponente auch terminologisch anzuzeigen, 283 spreche ich von *Compliance Assistance Technologies*, nicht von *Structures*. Den Begriff der *Compliance* (statt einfach Befolgungsassistentz oder auch Rechts-IT) verwende ich in Anlehnung an den Sprachgebrauch der wirtschaftsrechtlichen Literatur.⁵⁸¹ Betont wird damit, dass es um mehr geht als um die Selbstverständlichkeit der Befolgung von Recht, nämlich um organisatorische und in diesem Sinn potentiell systematisch-allgegenwärtige Formen der Befolgungs- und damit Realisierungs-Assistentz.⁵⁸² Das ‚i. e. S.‘ stelle ich den *Compliance Assistance Technologies* hier deshalb nach, weil natürlich in einem weiten Sinn auch die anderen *Structures*, um die es soeben ging (*Impossibility Structures*) sowie sogleich noch gehen wird (*Justification Structures*), eine Art von Assistentz bei der Realisierung von Recht leisten können und sollen – nur eben eine physische (deshalb alle zusammenfassend: *Compliance Assistance Technologies* i. w. S.; dieser weite Ober- oder Sammelbegriff wird insbesondere in → § 4 nochmals eine wichtige Rolle spielen⁵⁸³).

Tatsachenfragen unterschieden. Ein Subsumtionsschluss enthält notwendigerweise Antworten auf beide Fragen.

578 s. hierfür insb. *Kotsoglou*, JZ 2014, 451 ff. und deutlich *ders.*, JZ 2014, 1100 (1101): „Es muss also gezeigt werden, dass wir [...] unausweichlich zum Ergebnis kommen, dass juristische Problemstellungen (Sachverhalte) Laien nicht verständlich gemacht werden können.“

579 s. dazu informativ *Funke*, in: Hilbert/Rauber (Hg.), Warum befolgen wir Recht? 2019, S. 201 (204 ff.) m. w. N., der allerdings selbst die (wie ich) „These“ vertritt, dass „Normkonkretisierung [...] eine Angelegenheit derjenigen Adressaten [ist], an die das Recht als Verhaltensordnung sich richtet“ (a. a. O., S. 203).

580 s. dazu → S. 327 ff.

581 s. zu diesem Modebegriff statt vieler *Bachmann*, in: Grundmann/Merkt/Mübert (Hg.), FS Hopt, 2020, S. 17 ff., wonach *Compliance* – über die „Selbstverständlichkeit“ der Forderung nach Regelbeachtung (ebd.) hinausgehend – Folgendes bedeutet: „Die sog. Compliance-Pflicht stellt daher im Kern eine Pflicht zur Einrichtung einer die Einhaltung von Rechtsnormen gewährender *Organisation* dar“ (ebd., S. 18). Hervorhebung im Original.

582 Vgl. auch *Burchard*, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 553 (578): „Die Prädiktions- ist in *extremo* eine Compliancegesellschaft, die internalisierte Selbstkontrolle normalisiert.“

583 Dort ab → S. 342.

2. ... im Straßenverkehrsrecht

- 284 Ein basales Beispiel einer *Compliance Assistance Technology* findet sich heute bereits in den meisten Kraftfahrzeugen. Deren Navigationssysteme zeigen der Fahrerin Geschwindigkeitsübertretungen an, häufig begleitet von einem akustischen Warnsignal. Die Fahrerin kann dann natürlich weiterhin selbst entscheiden, ob ein aus ihrer Sicht hinreichender Rechtfertigungsgrund besteht, das Verhalten fortzusetzen. Seit dem 6. Juli 2022 ist der Einbau von solchen sogenannten „intelligenten Geschwindigkeitsassistenten“ in der EU für alle neuen Fahrzeugtypen verpflichtend vorgeschrieben, seit dem 7. Juli 2024 dürfen keine neuen Fahrzeuge mehr zugelassen werden, welche die Technik nicht verbaut haben.⁵⁸⁴ Die Technik muss so eingerichtet sein, „dass der Fahrer über den Beschleunigungsregler oder über gezielte, angemessene und wirksame Rückmeldungen darauf aufmerksam gemacht wird, dass die geltende Geschwindigkeitsbeschränkung überschritten wird“. Er muss diese Funktion abschalten können, wobei sie nach einem Neustart des Wagens wieder aktiv sein muss.⁵⁸⁵
- 285 Ebenfalls seit 2022 sind zudem noch weitere „hochentwickelte Fahrassistenzsysteme“ in neue Kraftfahrzeuge einzubauen, wozu auch ein „Warnsystem bei Müdigkeit und nachlassender Aufmerksamkeit des Fahrers“ sowie ein „hochentwickeltes Warnsystem bei nachlassender Konzentration des Fahrers“ gehören.⁵⁸⁶ Insoweit fehlt interessanterweise eine Regelung zur Abschaltbarkeit. Auf eine künftige Folge­regelung zielt offenbar die Verpflichtung ab, Kraftfahrzeuge mit einer „Vorrichtung zum Einbau einer alkoholempfindlichen Wegfahrsperr­e“ auszustatten⁵⁸⁷ – nur eine *Vorrichtung zum Einbau*, die Wegfahrsperr­e muss also *noch* nicht selbst verbaut sein.
- 286 Der „Zustand und Grad der Aktivierung aller [dieser] Sicherheitssysteme an Bord“ müssen Gegenstand einer „ereignisbezogenen Datenaufzeichnung“ sein.⁵⁸⁸ Es ist daher ein Datenschreiber ähnlich der von Flugzeugen bekannten *Black Box* zu verbauen, der

„im Zeitraum kurz vor, während und unmittelbar nach einem Zusammenstoß [Daten] [auf]zeichnet und [s]peichert [über] Fahrzeuggeschwindigkeit, Abbremsen, Position und Nei­gung des Fahrzeugs auf der Straße, [über] Zustand und Grad der Aktivierung aller Sicherheits­systeme an Bord, das auf dem 112-Notruf basierende bordeigene eCall-System, Aktivierung der Bremsen sowie sonstige relevante Eingabeparameter für die bordseitigen aktiven Sicherheits-

584 s. Art. 6 Abs. 1 lit. a, Abs. 2 VO (EU) 2019/2144 v. 27.11.2019 über die Typgenehmigung von Kraftfahr­zeugen und Kraftfahrzeuganhängern; zu den Anwendungszeitpunkten s. Art. 16 sowie die insgesamt hilfreiche Übersicht unter <https://www.bmv.de/SharedDocs/DE/Artikel/StV/Strassenverkehr/neue-fahrzeug-sicherheitssysteme.html>, besucht am 11.6.2025.

585 Art. 6 Abs. 2 lit. b VO (EU) 2019/2144.

586 Art. 6 Abs. 1 lit. c bzw. d VO (EU) 2019/2144.

587 Art. 6 Abs. 1 lit. b VO (EU) 2019/2144.

588 Art. 6 Abs. 1 lit. g, Abs. 4 lit. a VO (EU) 2019/2144.

und Unfallvermeidungssysteme, wobei dafür gesorgt sein muss, dass die Daten höchst präzise sind und kein Datenverlust entsteht.“⁵⁸⁹

Diese Datenaufzeichnung darf ausdrücklich nicht deaktiviert werden können,⁵⁹⁰ 287 was aus strafrechtlicher Perspektive schon zu der naheliegenden Frage geführt hat, ob alsbald diese „intelligenten Agenten als Zeugen im Strafverfahren“ zur nachträglichen Sachverhaltsaufklärung etwa nach einem Unfall herangezogen werden dürfen.⁵⁹¹ *Nemo-tenetur*-Grundsatz, Kernbereichsschutz und konventionsrechtliches Konfrontationsrecht sind hier aufgerufen. Die strafrechtswissenschaftliche Diskussion darüber, ob im Fall der Verwendung von Daten aus zwingend zu verbauenden Datenschreibern jeweils ein Verstoß vorliegen würde oder nicht, steht noch am Anfang.⁵⁹² Konkret mit Blick auf die Fahrsicherheitsassistent-Rechtssetzung der EU scheint mir die Frage freilich geklärt zu sein. Nach Art. 6 Abs. 4 lit. d VO (EU) 2019/2144 dürfen

„die Daten, die [die Datenschreiber] aufzeichnen können, den nationalen Behörden auf der Grundlage des Unionsrechts oder des nationalen Rechts im Einklang mit der [DSGVO] *ausschließlich* für den Zweck der Unfallforschung und -analyse, einschließlich für die Zwecke der Typgenehmigung von Systemen und Bauteilen, [...] zur Verfügung gestellt werden können.“ Hervorhebung hier.

Eine Verwendung der Daten, die übrigens von vornherein anonymisiert gespeichert werden müssen,⁵⁹³ 288 für Zwecke der Strafverfolgung dürfte damit ausgeschlossen sein. Die Verwendung des Begriffs „ausschließlich“ legt zudem nahe, dass auch die diversen Zweckänderungsklauseln aus dem Datenschutz- und Strafprozessrecht vorliegend nicht greifen, eine Verwendung also *nicht* zulassen dürften. Deziert anders verhält es sich übrigens mit den Fahrzeugdaten, die nach nationalem Recht beim automatisierten und autonomen Fahren anfallen bzw. gespeichert werden müssen.⁵⁹⁴

Zur Abrundung sei kurz auf Ideen der Industrie in Sachen *Compliance*-(Fahr-)Assistenz hingewiesen, die noch einen Schritt weiter gehen. So hat sich 2021 ein Industrie-Konsortium um den Software-Anbieter *Tome* (Detroit, USA) unter Beteiligung von Ford, Bosch und einigen Fahrradherstellern gebildet mit dem Ziel, eine Marken-übergreifend einsetzbare Software unter Nutzung der *Bluetooth*-Technologie zu entwickeln, die es Fahrrädern und E-Scootern erlauben soll, mit den Automobilen

589 Art. 6 Abs. 4 lit. a VO (EU) 2019/2144.

590 Art. 6 Abs. 4 lit. b VO (EU) 2019/2144.

591 *Gless/Weigend*, JZ 2021, 612.

592 Vgl. die Problemübersicht *ibid.*, S. 615 ff.

593 s. Art. 6 Abs. 4 lit. c, ii), Abs. 5 VO (EU) 2019/2144. Insofern ist es etwas befremdlich, dass Abs. 4 lit. d auf die Einhaltung der DSGVO verweist, da diese auf anonymisierte Daten nicht anwendbar ist.

594 Hier sind die oben, → S. 146 ff., bereits erwähnten §§ 1g, 63a StVG einschlägig.

zu „reden“, mit denen sie den Straßenraum teilen,⁵⁹⁵ vor allem also zu warnen, wenn Kollisionen drohen. Die Fahrzeuge sollen offenbar noch nicht selbsttätig darauf reagieren, sollen aber wiederum ihre Fahrer auf die Gefahr hinweisen können.

3. ... im Online-Kommunikationsrecht

- 290 Noch sehr rudimentär, aber von der Tendenz her schon als *Compliance Assistance Technologies* beschreibbar, sind Teilfunktionen von Online-Lehr- und Lernsystemen wie Stud.IP. Diese Software bietet Lehrenden unter anderem die Möglichkeit, Dateien mit Studierenden zu teilen. Dabei kann es rasch zu Urheberrechtsverstößen kommen. Die Plattform will nun den Nutzern die Einhaltung des Urheberrechts dadurch erleichtern, dass diese vor jedem Upload das jeweilige Material selbst urheberrechtlich einordnen müssen, damit der Vorgang abgeschlossen werden kann. Können oder wollen sich die Nutzer urheberrechtlich nicht festlegen und wählen daher „ungeklärte urheberrechtliche Situation“, erfolgt zwar technisch ein Upload, aber die Studierenden können auf eine solche Datei nicht zugreifen. Gegenwärtig erfolgt die rechtliche Einordnung – zumindest bei Stud.IP – ohne KI-Einsatz, nämlich durch die Auswahl einer der folgenden Optionen: „ungeklärte urheberrechtliche Situation“, „gemeinfreie Werke“, „frei nutzbare Werke“, „selbstverfasste Werke“, „Werke mit Campus- oder Nationallizenzen (Lizenz liegt vor)“, „Sprachwerke gem. § 60a UrhG“ und schließlich „Sonstige Werke gem. § 60a UrhG“ (sogenannte Wissenschaftsschranke⁵⁹⁶). Diese Einordnung wird aber immerhin durch kleine Erläuterungstexte zu den Nutzungs- bzw. Schutzkategorien unterstützt, die einigermaßen laienfreundlich erläutern, unter welchen Voraussetzungen z. B. eine Berufung auf § 60a UrhG möglich ist.⁵⁹⁷ Kleine graphische Symbole sollen die Zuordnung weiter erleichtern (z. B. ein §-Zeichen für „Werke mit Campus- oder Nationallizenzen“).⁵⁹⁸

595 So die Zeitungsüberschrift zu dem Projekt, s. D. Brown, The Washington Post v. 13.1.2021 (Onlinequelle).

596 § 60a UrhG lautet: „(1) Zur Veranschaulichung des Unterrichts und der Lehre an Bildungseinrichtungen dürfen zu nicht kommerziellen Zwecken bis zu 15 Prozent eines veröffentlichten Werkes vervielfältigt, verbreitet, öffentlich zugänglich gemacht und in sonstiger Weise öffentlich wiedergegeben werden 1. für Lehrende und Teilnehmer der jeweiligen Veranstaltung, 2. für Lehrende und Prüfer an derselben Bildungseinrichtung sowie 3. für Dritte, soweit dies der Präsentation des Unterrichts, von Unterrichts- oder Lernergebnissen an der Bildungseinrichtung dient. (2) [...]“

597 Die Erläuterung zu § 60a UrhG lautet bspw.: „Urheberrechtlich geschützte Sprachwerke dürfen Sie auch ohne gesonderte Vereinbarung oder Erlaubnis für die Lehre nutzen. Typische Beispiele für Sprachwerke sind: deutsche und ausländische Verlagsprodukte (Buchauszüge, Zeitungs- oder Zeitschriftenartikel); Auszüge aus vergriffenen Büchern; auf Internetseiten frei zugängliche Texte [...]. Dabei müssen folgende Kriterien erfüllt werden: – Es handelt sich um [...] nicht mehr als 15% oder ein Werk geringen Umfangs von nicht mehr als 25 Seiten. – Einzelne Aufsätze und Artikel aus wissenschaftlichen und Fachzeitschriften [...]. – Der Teilnehmerkreis ist abgeschlossen. Die Datei kann erst heruntergeladen werden, wenn der Zugang zur Veranstaltung geschlossen ist. [...] – Die Bereitstellung ist im Rahmen des Zwecks geboten, dient ausschließlich der Veranschaulichung im Rahmen der Lehrveranstaltung und dient dem eigenen wissenschaftlichen Gebrauch der Teilnehmer.“

598 Zu Erkenntnissen der Kommunikationsforschung bei der Nutzung von Graphiken speziell für den Bereich von Urheberrechten auch Specht, Diktat der Technik, 2019, S. 416 ff.

Es wäre denkbar, die Nutzer bei dieser Selbsteinschätzung künftig durch eine Text-, 291
Bild- und gegebenenfalls auch Audioerkennung zu unterstützen. Die könnte sie
z. B. auf größere, wörtlich aus anderen Werken stammende Passagen und damit auf
die Notwendigkeit einer Urheberrechtsschranke hinweisen bzw. darauf aufmerksam
machen, dass die unter § 60a UrhG zulässige Maximalveröffentlichung von 15%
eines Buches überschritten ist. Das würde mühsames Zusammenrechnen ersparen.

Unter Umständen wird Stud.IP auch schon zur *Impossibility Structure*: Wählt ein 292
Nutzer die Wissenschaftsausnahme des § 60a UrhG, dann folgt aus dieser rechtli-
chen Einordnung, dass das Material nur einem geschlossenen Personenkreis zum
Abruf bereitgestellt werden *darf* (z. B. einer bestimmten Schulklasse, einem Seminar
an der Universität). Stud.IP sorgt nun technisch dafür, dass das Material solange
nicht abgerufen werden *kann*, bis die Lehrperson den entsprechenden Kurs auf
„geschlossen“ gestellt hat.

Das Automatisierungsniveau ist hier insgesamt noch sehr begrenzt; und aktuell 293
hindert das System die Lehrperson auch nicht daran, einfach „gemeinfreies Werk“
oder „selbstverfasstes Werk“ anzukreuzen, sodass ein Upload ohne Einschränkungen
möglich wird. Es handelt sich eben nur um eine Assistenzstruktur. Das Potential
für weitere Automatisierungen bis hin zu *Impossibility Structures* liegt aber auf der
Hand.

4. ... im Infektionsschutzrecht

Ein weiteres Beispiel für *Compliance Assistance Technologies* kann dem Infektions- 294
schutzrecht entnommen werden. Nicht nur das föderale System, sondern mehr
noch der Grundsatz der Verhältnismäßigkeit haben zu einer erheblichen orts- und
zeitbezogenen Diversität und Kleinteiligkeit der in den Jahren 2020 bis 2023 gel-
tenden Corona-Schutzbestimmungen geführt. Die grundrechtlich *prima facie* gut
begründbare Differenziertheit der ständig wechselnden Bestimmungen hat aber
nicht nur ihre Anwendung durch die Adressaten massiv erschwert, sondern auch
die Akzeptanzbereitschaft gesenkt. Das zugrundeliegende Rechtswissensproblem hat
den Einsatz avancierter Technologien zur *Compliance*-Assistenz offensichtlich gera-
dezu herausgefordert. Umso erstaunlicher war, dass die Corona-Warn-App bis zum
Schluss meines Wissens über keine Funktionalität verfügte, die den Bürgern die am
konkreten Ort ihres Aufenthalts für ihre geplante Tätigkeit geltenden Regeln in einer
nachvollziehbaren Weise hätte vermitteln können. Dabei wird davon ausgegangen,
dass

„in England der nutzerorientierte große Funktionsumfang der britischen App zur breiten Akzeptanz in der Gesellschaft führte. Sie informiert Nutzer, ob ihre Postleitzahl gerade zum Risikogebiet gehört.“⁵⁹⁹

- 295 An eher unerwarteter Stelle, nämlich in die Warn-App NINA wurde eine vergleichbare Funktion allerdings sehr wohl eingespielt.⁶⁰⁰ NINA steht für *Notfall-Informationen- und Nachrichten-App des Bundes*. Es ist eine Applikation des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK), die nach der Beschreibung des Bundesamtes unter anderem enthält:

„wichtige Warnmeldungen des Bevölkerungsschutzes für unterschiedliche Gefahrenlagen wie zum Beispiel Gefahrstoffausbreitung oder einen Großbrand. Wetterwarnungen des Deutschen Wetterdienstes und Hochwasserinformationen der zuständigen Stellen der Bundesländer sind ebenfalls in die Warn-App integriert.“⁶⁰¹

- 296 Eine spezifische Rechtsinformationsfunktion im Sinn einer *Compliance Assistance* lässt diese Zweckbestimmung nicht erwarten. Gleichwohl war NINA der Ort, an dem die Bundesregierung im Dezember 2020 eine Funktion integrierte, um die Corona-Bestimmungen vergleichsweise übersichtlich abrufbar zu machen, die am Standort des Nutzers galten. Standortspezifisch aufgelistet wurden z. B. die Kontaktbestimmungen „Im öffentlichen Raum“ oder „Bei der Arbeit“, die Verpflichtungen zum Tragen medizinischer Masken (bei Gaststätten z. B.: „drinnen [OP-Maske, FFP2, KN95/N95], entfällt am Platz“) oder zu Testungen (etwa „private Feiern mit Tanz: Testpflicht“⁶⁰²). Es handelte sich um Kurzdarstellungen, die teils offensichtlich den Zugriff auf weitere Informationsquellen notwendig machten. Etwa: „Impfpflicht in bestimmten Gesundheitsbereichen“ (Hervorhebung hier). In solchen Fällen fanden sich dann häufig als „weiterführende Informationen“ Links etwa auf das Infektionsschutzgesetz oder auf amtliche Informationsseiten zur SARS-CoV-2-Arbeitsschutzverordnung. Über Änderungen der Rechtslage informierte NINA durch Push-Nachrichten, wenn der Nutzer dies wünschte. Schwach war, dass die App den Aktualisierungsstand der Rechtslage nicht auswies.

- 297 Was das „Warngebiet“ – oder, in diesem Fall passender: das Informationsgebiet – anbelangte, ließ sich dieses um den durch GPS ermittelten Standort des Nutzers oder auch eine frei gewählte Adresse herum stufenweise eingrenzen: ca. 1 km² Umfang, ca. 9 km² Umfang, auf die Gemeinde, oder auf den Landkreis. Die Aufbereitung der rechtlichen Vorgaben wurde ausweislich eines „Disclaimers“ von der Deutschen Presse-Agentur im Auftrag des BBK geleistet; und, nicht überraschend, sollte für „die

599 Dössel et al., Apps und wearables für die Gesundheit, 2021, S. 43 f.

600 Version 3.3 von Dezember 2020, vgl. die Pressemitteilung unter www.bundesregierung.de/breg-de/theme/n/coronavirus/warn-app-nina-1749214, besucht am 18.1.2021.

601 So die Beschreibung des Bundesamtes, abrufbar unter www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/warn-app-nina_node.html, besucht am 19.10.2021.

602 Für den Standort Stadt Bielefeld am 19.10.2021 ermittelt.

Richtigkeit, Vollständigkeit und Aktualität der Kurzdarstellung [...] trotz sorgfältiger Recherche keine Gewähr und Haftung übernommen werden.“ „Bei Fragen“ solle sich die Nutzerin an ihre „örtlich zuständige Gesundheitsverwaltung“ wenden, wobei insoweit ein Online-Tool des Robert-Koch-Instituts verlinkt war, das bei der Suche nach diesem zuständigen Amt behilflich war. Die Nutzung von NINA war (und ist) freiwillig,⁶⁰³ Rechtsgrundlagen für die Verwendung z. B. der Standortdaten oder IP-Adressen (= personenbezogene Daten) sind laut Datenschutzerklärung die Einwilligung der Nutzenden⁶⁰⁴ sowie „über den Zeitpunkt [des] Besuchs hinaus[gehend]“⁶⁰⁵ die katastrophenschutzrechtliche Aufgaben-Generalklausel (Art. 6 Abs. 1 lit. e DSGVO i. V. mit § 6 Zivilschutz- und Katastrophenhilfegesetz – ZSKG: Warnung der Bevölkerung).

Die *Compliance Assistance*, die NINA damit lieferte, war also eindeutig keine Nutzung von KI. Es handelte sich letztlich um eine Standorterkennung unter Nutzung der entsprechenden Möglichkeiten des verwendeten Endgeräts. NINA erleichterte insofern lediglich die Suche nach den an einem konkreten Ort geltenden Regeln und beschrieb diese in einer vergleichsweise einfachen Sprache. Unschärfen blieben dabei vielfach erhalten, so galt am Tag meines Tests für Versammlungen etwa „Unter Auflagen; teilweise Maskenpflicht (OP-Maske, FFP2, KN95/N95); teilweise Testpflicht“, was die Rechtsfindung sicherlich nicht abschließend ermöglichte, aber immerhin strukturierte Anhaltspunkte dafür lieferte, dass für den konkreten Nutzer gegebenenfalls weitere Nachforschungs- und Informationsobliegenheiten bestehen konnten. 298

5. ... im Verbraucherschutzrecht

Mit den beiden folgenden Beispielen soll nun die Perspektive geweitet werden. 299 Bislang ging es um Konstellationen, in denen Mensch und Maschine sozusagen ‚zu zweit allein‘ agieren, vom technisch assistierten Menschen nämlich ein Tun oder Unterlassen gefordert wird (langsamer fahren, kein Upload, Verzicht auf Besuche oder Veranstaltungen), *ohne* dass dieses Verhalten eine *konkrete* dritte Person betraf. Nun folgen zwei Beispiele für Mehrpersonen-Arrangements, in denen eine dritte Person das eigentliche *Ziel* der gesetzlichen Regelung ist. Diese ist aber nicht zugleich der *unmittelbare* Rechts- und damit Steuerungsadressat der Verhaltenspflicht.

603 Wahrscheinlich auch deswegen ist rechtswissenschaftliche Lit. zu NINA und vergleichbaren Angeboten wie Katwarn selten; s. immerhin Schaller, ZD-Aktuell 2016, 5425.

604 Vgl. Nr. 2.2.1 der Datenschutzerklärung der NINA-App, Stand 16.6.2021, abrufbar unter www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/NINA-Datenschutzerklaerung/nina-datenschutzerklaerung_node.html?sessionId=l65BF4993BEA05B927AFE54431F296E5.live341, besucht am 19.10.2021.

605 Vgl. Nr. 2.1 der Datenschutzerklärung der NINA-App, Stand 16.6.2021, abrufbar unter www.bbk.bund.de/DE/Warnung-Vorsorge/Warn-App-NINA/NINA-Datenschutzerklaerung/nina-datenschutzerklaerung_node.html?sessionId=l65BF4993BEA05B927AFE54431F296E5.live341, besucht am 19.10.2021.

Das klingt speziell, dürfte regulatorisch aber einen häufigen Fall abbilden, weil damit *Compliance-Assistance*-Konstellationen aus dem Feld der Anreiz- und Informationssteuerung (sogleich hier) wie auch der Leistungsverwaltung (dazu → 6.) abgedeckt sind. Beide der folgenden Beispielfelder sind noch weitgehend fiktiv, werden aber in den jeweiligen Spezialdiskursen bereits als mögliche Einsatzfelder von künstlicher Intelligenz erörtert. Zu beachten ist zudem, dass sich die folgenden Regelungskomplexe (also Verbraucherschutzrecht hier und sodann das Recht der Studienzulassung) nicht mehr vorrangig an jedermann (im Sinn von echten juristischen Laien) richten, aber auch nicht dezidiert an Volljuristinnen.

- 300 Aus der Anreiz- und Informationssteuerung sei hier zunächst das Verbraucherschutzrecht herausgestellt. Es verpflichtet Unternehmen vielfach dazu, Verbraucher in bestimmter Weise zu informieren. KI-basierte Optimierung würde hier bedeuten, derartige Informationen bzw. Anreize, wo sie zu Steuerungszwecken eingesetzt werden,⁶⁰⁶ auch im Massenverkehr personalisieren zu können, d. h. sie in Länge, Tiefe und Detailgrad auf den konkreten Empfänger zuzuschneiden. Bislang wird beim ‚Design‘ des Steuerungsinstruments stattdessen meist vom Durchschnittsverbraucher, -nutzer, -bürger etc. ausgegangen.⁶⁰⁷ Natürlich würde die Informations*handlung* in der Praxis automatisiert erfolgen, so dass wir es auf den ersten Blick phänomenologisch sogar mit einer *Impossibility Structure* zu tun haben könnten. Das ist aber deshalb nicht der Fall, wenn und weil das Unternehmen, das die Daten KI-basiert erhebt und auswertet, die für eine differenzierte Information/Ansprache notwendig sind, den eigentlichen Mechanismus der Verknüpfung und Informationsübertragung weiterhin selbst kontrolliert, also jederzeit intervenieren und eben doch auch weiterhin die *nicht* rechtmäßige Handlung vornehmen könnte.
- 301 *Christoph Busch* definiert solche Versuche granular differenzierender Informationspflichterfüllung als eine Form von *Personalized Law*.⁶⁰⁸ Man wird sich fragen müssen, ob wirklich schon das *Recht* personalisiert ist, oder ob solches Recht nicht einfach nur personalisierte und differenzierte (*Busch* treffend: „granulare“) Informationen und Anreize – d. h. Real- und nicht Rechtsakte – auf der Anwendungsebene *verlangt*. Würde man hier bereits von *Personalized Law* sprechen, wäre jede Ermessensvorschrift des Verwaltungsrechts bereits *Personalized Law*, was einen Verwaltungsrechtler wohl überraschen würde. Es erscheint insoweit treffender, mit *Philipp*

606 Dazu statt vieler *Hermes*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hg.), GVwR II, ²2012, § 39 Rn. 52 m. w. N.

607 Instruktiv *Hacker*, in: Busch/Franceschi (Hg.), Algorithmic Regulation and Personalized Law, 2021, S. 241, Abschnitt L.

608 *Chr. Busch*, University of Chicago Law Rev. 86 (2019), 309 ff. Ausf. zu dieser Thematik aus privatrechtlicher Perspektive die Beiträge in Busch/Franceschi, Algorithmic Regulation and Personalized Law, 2021; für einen „general framework for thinking about the new personalization of law“ vgl. *Casey/Niblett*, University of Chicago Law Rev. 86 (2019), 333 ff. Monographisch und unter Berücksichtigung auch verfassungsrechtlicher Erwägungen *P. M. Bender*, Grenzen der Personalisierung des Rechts, 2023, passim.

Hacker in unserem Beispiel von einem *Personalization Law* zu sprechen⁶⁰⁹ und damit einen Rechtsakt zu bezeichnen, der Personalisierung im Einzelfall verlangt. Aber letztlich ist das eine Frage der Perspektive bzw. genauer: die Frage danach, ob man unter *Law* nur die abstrakte Regel oder auch den konkreten einzelnen Anwendungsfall erfassen will, selbst dann, wenn sich dieser als Realakt darstellt.

Auf diese Kategorisierung kommt es hier aber letztlich ohnehin nicht an. Maßgeblich ist die Einschätzung von *Busch*, dass es spezifisch die KI-basierten Technologien sind, die es in bestimmten Rechtsbereichen, in denen bislang noch Typisierungen überwiegen, erlauben, die Rechtsanwendung weiter in Richtung Einzelfall(-Adäquanz) zu verschieben. Denn:

“[T]he optimal complexity of legal rules – and the granularity of the entire legal system – is limited by the bounded capacity of human information processing [and] typification is essentially the answer to an information problem – a concession to the imperfections of a legal system administered by humans. In the near future, however, big data, superhuman information processing capacities and artificial intelligence could redefine the optimal complexity of legal rules and refine their content to a hitherto unachievable level of granularity. [...] As a result, regulatory errors stemming from over- and underinclusive norms based on coarse-grained typifications can be reduced”.⁶¹⁰

Autoren, die KI- bzw. Big-Data-gestützte Personalisierung in diesem Bereich an-
denken, verweisen beispielhaft auf verbraucher- und datenschutzrechtliche Informa-
tionspflichten, etwa Artt. 12 ff. DSGVO,⁶¹¹ Art. 6 Abs. 1 der Verbraucherrechte-Richt-
linie 2011/83/EU⁶¹² oder Artt. 23 Abs. 2, 24 der MiFID II Richtlinie 2014/65/EU.⁶¹³
Während in diesen Bereichen die Information der Betroffenen (im Datenschutz-
recht), des Verbrauchers oder der Kundin immer noch zentraler Baustein der gesetz-
lichen Regulierungsstrategie ist, wird immer klarer, dass undifferenzierte und vor al-
lem (zu) viele Informationen die Adressaten häufig überfordern oder schlicht nicht
interessieren. Das Stichwort lautet *Information Overload*, das regulatorische Ziel
wird häufig verfehlt.⁶¹⁴ Die Idee, Informationen auf Basis der einem sozialen Netz-
werk, einer Bank usw. verfügbaren personenbezogenen Daten so zuzuschneiden,
dass sie die Interessen, die Vorbildung und sogar die besonderen psychologischen

609 s. *Hacker*, ERPL 25 (2017), 651 (656), der an anderer Stelle aber ebenfalls von “personalized law” spricht, z. B. S. 655 f.

610 *Chr. Busch*, University of Chicago Law Rev. 86 (2019), 309 (314). Ähnl. schon *Hacker*, ERPL 25 (2017), 651 (658 f.): “A central problem for the contemporary theory of private law [...] is the staggering degree of heterogeneity within the groups the law traditionally distinguishes between – be it differences in experience, rationality, willpower, economic resources, or else. Personalization can bring behavioural science and technology to bear on these problems. Legal categories can thus be rendered more precise, granular and refined.”

611 s. dafür *Chr. Busch*, University of Chicago Law Rev. 86 (2019), 309 (319 ff.).

612 s. *ibid.*, S. 315 ff.; *Hacker*, in: *Busch/Franceschi* (Hg.), *Algorithmic Regulation and Personalized Law*, 2021, S. 241 Rn. 24 ff.

613 *Ibid.*, Rn. 27 ff.

614 Dazu schon *Hermstrüwer*, *Informationelle Selbstgefährdung*, 2016, S. 82 f. m. w. N.

Anfälligkeiten (*Biases*)⁶¹⁵ einer Nutzerin bzw. Kundin besser treffen, erscheint daher als sinnvoller und *prima facie* sogar angezeigter Optimierungsschritt.

304 Ähnlich plausibel erscheinen die Überlegungen im Bereich der Anreize-Steuerung bzw. des sogenannten *Nudging*. Als konkretes Themenfeld werden hier in der Debatte um ein *Personalized Law* in der Regel *Default Rules* genannt,⁶¹⁶ also Voreinstellungen oder Standardvorgaben.⁶¹⁷ Beispielsweise sind in den USA Kreditnehmer seit 2010 gesetzlich gegen Überziehungskredite geschützt, wovon sie aber aus-*opten* können. Studien legen nahe, dass ausgerechnet besonders vulnerable Gruppen, die ihre Abhängigkeit von Überziehungskrediten systematisch unterschätzen, von diesem *Opt-out* Gebrauch machen. Als Vorschlag einer Personalisierung des entsprechenden Regimes wird daher von *Philipp Hacker* vorgeschlagen, in solchen und vergleichbaren Fällen die „stickiness“⁶¹⁸ der Voreinstellung (im Beispiel: Beschränktheit von Überziehungskrediten als Standard) spezifisch für solche Kunden zu erhöhen, die auf Basis der vorhandenen Daten und entsprechender verhaltenswissenschaftlich informierter Musteranalysen als besonders vulnerabel errechnet werden. Das soll etwa durch zusätzliche *Risk Awareness Tests* oder durch Verweis auf passende Beratungsangebote (Schuldnerberatung) als Bedingung des *Opt-out* umgesetzt werden.⁶¹⁹

305 Konkrete Anwendungsbeispiele *de lege lata* scheint es für derartige Optimierungen bislang kaum zu geben. Genannt wird in der Debatte häufig § 504a BGB,⁶²⁰ der eine besondere „Beratungspflicht bei Inanspruchnahme der Überziehungsmöglichkeit“ bei Verbraucherdarlehensverträgen vorsieht. Absatz 1 S. 1 der Norm lautet:

„Der Darlehensgeber hat dem Darlehensnehmer eine Beratung gemäß Absatz 2 anzubieten, wenn der Darlehensnehmer eine ihm eingeräumte Überziehungsmöglichkeit ununterbrochen über einen Zeitraum von sechs Monaten und durchschnittlich in Höhe eines Betrags in Anspruch genommen hat, der 75 Prozent des vereinbarten Höchstbetrags übersteigt.“

306 Es handelt sich dabei um ein einfaches Muster, das eine Automatisierung, allerdings keinen Einsatz von KI-Technologie verlangt. Der in der Literatur genannte Wunsch, auf solche und ähnliche Konstellationen KI- und Big-Data-basierte sowie verhal-

615 s. bes. *Hacker*, ERPL 25 (2017), 651 (672 f.), der das *De-biasing* durch gezielt aufbereitete Informationen und Warnungen allerdings bereits zum engeren Feld des *Nudging* rechnet.

616 Mit vielen Anwendungsideen *Porat/Strahilevitz*, in: *Busch/Franceschi* (Hg.), *Algorithmic Regulation and Personalized Law*, 2021, S. 5 Rn. 56 ff.

617 Die Wortwahl rund um Anreize und *Nudging* ist uneinheitlich. Vgl. für eine vielschichtige Differenzierung *J. Wolff*, *Anreize im Recht*, 2021, einerseits allg. S. 21 f., und speziell zu Voreinstellungen, die *Wolff* als „Nudging“ in Gesetzesform bezeichnet, S. 142 ff.: „Um keinen Anreiztypus, und bei näherem Hinsehen überhaupt nicht um ein Instrument, mit dem unmittelbar Verhalten beeinflusst werden soll, handelt es sich bei den sog. Standardvorgaben“ (142). „Vielmehr verbindet der Gesetzgeber als Steuerungsakteur Tatbestand und Rechtsfolgen im Falle der Standardvorgaben, weil ihm selbst am Eintritt der Rechtsfolgen gelegen ist.“ (143).

618 *Hacker*, ERPL 25 (2017), 651 (671).

619 *Hacker*, in: *Busch/Franceschi* (Hg.), *Algorithmic Regulation and Personalized Law*, 2021, S. 241 Rn. 34.

620 *Chr. Busch*, *University of Chicago Law Rev.* 86 (2019), 309 (317).

tenswissenschaftlich informierte Muster anzuwenden, speist sich einerseits aus dem Wunsch, die Muster granularer und damit passender zu machen,⁶²¹ aber vor allem auch aus dem Bestreben, Schutz *ex ante* anbieten zu können, also bevor die in § 504a BGB vorausgesetzte Ver- oder sogar Überschuldung eingetreten ist.⁶²²

Dass zumindest der deutsche Gesetzgeber davor zurückschreckt, Private oder auch Behörden zu solchen anspruchsvolleren KI- und verhaltenswissenschaftlich gestützten Informationen und Anreizen zu verpflichten, hat natürlich einerseits etwas damit zu tun, dass digitale Personalisierung datenintensiv ist: Sie setzt voraus, die Nutzenden bzw. ihr Online-Verhalten möglichst detailliert zu erfassen. Die Zurückhaltung könnte aber *auch* damit zu tun haben, dass bislang eben solche Musteranalysen vor allem von Unternehmen privatnützig, d. h. im Zweifel *gegen* ihre Kunden eingesetzt werden, und sich damit ein negativ konnotiertes Narrativ über die differenzierten Einsatzmöglichkeiten der Technologie legt.⁶²³ Das Stichwort hierzu lautet *Dark Patterns* und es bezeichnet Benutzeroberflächen, die Benutzer unbewusst zu einem Tun oder Unterlassen veranlassen, dass sie „sonst nicht tun würden“⁶²⁴ Gemeint sind damit etwa die „austricksende“ Gestaltung von *Cookie*-Bannern, personalisierte Preise von Online-Händlern oder auch schlicht personalisierte Werbung.⁶²⁵ 307

Diese geläufige Darstellung ist negativ *geframed* und verbindet sich mit der tendenziell vorsichtigen deutschen Haltung gegenüber dem *Nudging* in seinen (auch) analogen verhaltenswissenschaftlich fundierten Formen, *soweit* dabei psychologische Dispositionen von Individuen *unbewusst* zu Steuerungszwecken ausgenutzt werden.⁶²⁶ Der Umstand, dass es den Vertretern von *Personalized Law* tendenziell darum geht, durch den Einsatz von KI und Big Data solche nachteiligen Dispositionen zu kompensieren, geht vor dem Hintergrund dieser sozusagen doppelten Vorbelastung des Gegenstands offenbar etwas unter; anders ausgedrückt: Während die Debatte um die *Risiken* der Personalisierung von Informations- und Anreizhandeln die Regulierer in den vergangenen Jahren erreicht hat (siehe insbesondere Art. 5 308

621 Ibid., S. 318.

622 Hacker, in: Busch/Franceschi (Hg.), *Algorithmic Regulation and Personalized Law*, 2021, S. 241 Rn. 35.

623 Vgl. in diese Richtung auch Chr. Busch, in: ders./Franceschi (Hg.), *Algorithmic Regulation and Personalized Law*, 2021, S. 279 Rn. 18 ff.

624 Vgl., m. w. N., Weinzierl, NVwZ-Extra 2020, I.

625 Diese und weitere Bsp. *ibid.*, S. 3.

626 s. zu dieser Diskussion O'Hara, AöR 145 (2020), 133, bes. S. 139 (und ff.): „Ihr Spezifikum [das von *Nudges*] liegt nicht etwa im Steuerungsergebnis, also darin, dass die Betroffenen bestimmte Arten von Dingen tun, die der Entscheidungsarchitekt will. [...] | Die Besonderheit liegt in der Art und Weise, in der die Betroffenen in die Steuerung eingebunden werden [...] Soweit *Nudges* aus juristischer Sicht zu einer eigenständigen Kategorie von Maßnahmen zählen, fußen sie auf Phänomenen des automatischen, unreflektierten Denkens.“

Abs.1 lit.a AI Act), scheint das hinsichtlich der *Chancen* noch nicht der Fall zu sein.⁶²⁷

6. ... im Recht der Studienplatzvergabe

- 309 In hoch entwickelten und stark verdichteten Gesellschaften ist die Teilhabe an knappen Gütern ein zentrales Element der Sozial- und Wirtschaftspolitik, und hat damit starke freiheitsrechtliche Implikationen.⁶²⁸ Für uns ist das relevant, weil bei der Erfüllung der damit aktivierten, in der Regel derivativen Teilhabeansprüche zunehmend granulare Auswahl- bzw. Verteilungsmaßstäbe gelten, bei deren Befriedigung künstliche Intelligenz eine wichtige Rolle spielen kann. Ein mittlerweile geläufiger Begriff für die damit angesprochenen Verteilungsverfahren ist der des *Matching*.⁶²⁹
- 310 Sinnvoll kann KI-gestütztes *Matching* beispielsweise im Kommunal- und Wirtschaftsverwaltungsrecht sein, wenn es um den Zugang zu öffentlichen Einrichtungen geht, über den kriteriengeleitet zu entscheiden ist, z. B. nach Eignung und Leistung.⁶³⁰ *Matching* kann nach dem letzten *Numerus-clausus*-Urteil des Bundesverfassungsgerichts aber insbesondere auch für die Verteilung von Studienplätzen interessant werden. Simple, dafür aber mehr oder weniger zufallsbasierte Auswahlkriterien wie Ortspräferenz oder Wartezeit/Priorität⁶³¹ der Bewerber (oder gar Losentscheide⁶³²) hat das Gericht in dieser Entscheidung weitgehend zurückgedrängt; stattdessen habe sich die Vergabe knapper Studienplätze nach Art. 12 Abs. 1 i. V. mit Art. 3 Abs. 1 GG „grundsätzlich⁶³³ an dem Kriterium der Eignung [zu] orientieren“,⁶³⁴ wobei die Eignung „für das Studium und – soweit prognostizierbar – den

627 Ähnl. auch Chr. Busch, in: ders./Franceschi (Hg.), *Algorithmic Regulation and Personalized Law*, 2021, S. 279 Rn. 6: “One [sic] the one hand, it is necessary to define the limits for the novel personalization techniques [...]. On the other hand, the new technologies can be utilized for tailoring legal rules to small segments of the population or even individuals. So far, the scholarly discourses about the two aspects of law and personalization have been somewhat detached from each other, but it seems that they are the two sides of the same coin.”

628 Die nachfolgenden Ausführungen stellen in Teilen eine aktualisierte und angepasste Fassung meiner bereits in *Rademacher*, RdJB 69 (2021), 254 ff. veröffentlichten Überlegungen dar.

629 s. bspw. – für den Bereich *Human Resources* – Delecraz et al., *Journal of Responsible Technology* 11 (2022), 100041; ausf. *Hermstrüwer*, *Mechanische Gerechtigkeit*, 2025, passim.

630 Vgl. etwa *Spitzlei*, *VerwArch* 111 (2020), 439 (471).

631 Ob es sich bei der Entscheidung nach Priorität um ein Zufallskriterium handelt, ist umstr. Dafür bspw. *Voßkuhle*, *Die Verwaltung* 31 (1999), S. 21 (39).

632 Von der Bundestagsfraktion DIE LINKE im Anschluss an die *Numerus-clausus*-III-Entscheidung des BVerfG gefordert, s. BT-Drs. 19/10623 v. 5.6.2019, S. 2.

633 D. h. unbeschadet einiger bestimmter, sozialstaatlich und mit dem Gemeinwohl begründeter Ausnahmen, s. BVerfG, Urt. v. 19.12.2017, Az. 1 BvL 3/14 = BVerfGE 147, 253 – *Numerus Clausus* III, Rn. 124. Das Gericht nennt als Bsp. Härtefälle oder Studienplatzvergaben zur Deckung besonderer Bedarfe wie die Sanitätsdienste der Bundeswehr.

634 BVerfG, Urt. v. 19.12.2017, Az. 1 BvL 3/14 = BVerfGE 147, 253 – *Numerus Clausus* III, Rn. 108.

Beruf [gemeint ist], zu deren möglichst vollständiger Erfassung die für die Auswahlentscheidung herangezogenen Kriterien geeignet sein müssen.“⁶³⁵

Die von diesem Gerechtigkeitsmaßstab abweichenden Kriterien Ortspräferenz und Wartezeit hat das Gericht nur in engem Umfang für zulässig erklärt, wenn und soweit die Ermittlung der Eignung der Bewerber in sehr aufwendigen Verfahren erfolge (und die Ortspräferenz statistisch die Wahrscheinlichkeit erhöht, dass ein derart aufwendig erzeugtes Studienangebot dann auch tatsächlich angenommen wird) bzw. weil die leistungsbezogene Ermittlung „in Grenzbereichen“ nicht zuverlässig funktioniere und die Wartezeit demgegenüber als Ausdruck der Motivation der Bewerber immerhin mittelbar eignungsrelevant sei.⁶³⁶ Letztlich geht es also beiden Hilfskriterien um die Bewältigung von Ressourcen- und damit verbundenen Wissensgenerierungsproblemen der zuständigen Verwaltung.⁶³⁷ Dass KI bei solchen Eignungsprognosen eine wichtige assistierende Funktion haben und damit die nicht-egnungsbezogenen Kriterien noch weiter zurückdrängen *könnte*, liegt auf der Hand⁶³⁸ – zumindest in der Theorie einer gut funktionierenden Technologie.

In der Praxis ist das Bild derzeit gemischt: Während in anderen Staaten Auswahlentscheidungen bzw. Entscheidungen im Vorfeld von universitären Entscheidungen (wie etwa die Bewertung von Zugangstests) bereits durch KI-basierte Verfahren der Mustererkennung getroffen werden,⁶³⁹ ist die deutsche Rechtspolitik zurückhaltend. Bislang beschränkt sich die Nutzung von sogenannter *Education Technology* (oder kurz *Edtech*⁶⁴⁰) auf Assistenzsysteme, die Studierenden und vereinzelt auch Lehrenden während des Studiums Unterstützung bieten sollen;⁶⁴¹ etwa, indem sie individualisierte Curricula vorschlagen oder individuelle Studienprobleme erkennen und

635 Ibid., Rn. 118. s. auch Rn. 111: „Die zur Vergabe knapper Studienplätze herangezogenen Kriterien müssen die Vielfalt der möglichen Anknüpfungspunkte zur Erfassung der Eignung abbilden.“

636 s. BVerfG, Urt. v. 19.12.2017, Az. 1 BvL 3/14 = BVerfGE 147, 253 – Numerus Clausus III, Rn. 168 zur grds. Nicht-Berücksichtigungsfähigkeit der Ortspräferenz der Bewerber; Rn. 170 zur Ausnahme, und Rn. 218 zur grds. Nicht-Berücksichtigung der Wartezeit, Rn. 219 zur Ausnahme. Interessanterweise schafft es das Gericht damit, zwei an sich – aus Sicht der gewählten Regelungsstrategie der Zulassung nach *Eignung* – irrationale/zufällige Kriterien doch wieder leistungsbezogen zu wenden und damit in die regulatorische Strategie systemgerecht zu integrieren. Für eine vollständige Streichung der Wartezeitquote *Coelln*, NJW 2018, 361.

637 Ausf. Rademacher, RdJB 69 (2021), 254 (260 ff.).

638 Vgl. allgemein zur Relevanz von *Big Data* bzw. KI bei staatlichen Auswahlentscheidungen und der Möglichkeit, diese nach dem Zufallsprinzip (Losentscheid) zu treffen, *Spitzlei*, VerwArch III (2020), 439 (471): „Sobald mit dem Abstellen auf [den Zufall] eine Abweichung von einem bestimmten Gerechtigkeitsmaßstab verbunden ist, kann dies nur unter Verweis auf die damit verbundene Entlastung der Verwaltung gerechtfertigt werden. Der technologische Fortschritt scheint geeignet, diese Entlastungsfunktion und damit die Berechtigung von [Zufallsentscheidungen] in absehbarer Zeit stark einzuschränken“.

639 s. für Bsp. Rademacher, RdJB 69 (2021), 254 (257 ff.); Pasquale, *New laws of robotics*, 2020, S. 60 ff.

640 Ibid., S. 61. Yoan Hermstrüwer spricht in Anlehnung an das sog. *Predictive Policing* von *Predictive Schooling*, s. AöR 145 (2020), 479 (480). Für die Unterscheidung von *Adaptive Learning* und *Personalized Learning* s. Hao, MIT Technology Rev. v. 2.8.2019 (Onlinequelle).

641 Ausf. zu einem solchen Programm, dass die Hochschule der Medien in Stuttgart unter dem Namen „Learning Analytics für Studienerfolg und Prüfungsleistungen“ (LAPS) testet, *Uphues*, DÖV 2020, 234 ff.

aus diesem Anlass persönliche (menschliche) Beratung ermöglichen bzw. empfehlen. Technisch geht es aber in jedem Fall darum, durch möglichst umfangreiche Datenanalysen Schülern oder Studierenden zum ‚richtigen‘ Zeitpunkt mit den ‚richtigen‘ Lern- und Lehrinhalten in der ‚richtigen‘ Form zu konfrontieren, so dass der Lernerfolg am größten ist. Es fehlt(e) aber auch für den deutschen Bildungsraum nicht an optimistischen Prognosen, dass „[b]ereits in drei bis fünf Jahren [...] Methoden der Künstlichen Intelligenz die Hochschulbildung verändert haben“ werden.⁶⁴²

313 Die Gründe für die Zurückhaltung speziell bei der *Zulassungsentscheidung* sind angesichts der methodischen Grundlagen der Technologie jedoch einleuchtend:

- *Edtech* speziell in dieser Phase wäre noch datenintensiver als in anderen Bereichen, weil sich die Daten idealerweise über lange Zeiträume *schulischer* Aktivitäten von Bewerbern erstrecken müssten (und damit Kinder betreffen⁶⁴³), und weil jedenfalls für das Training der Muster Studienverläufe und -abschlüsse *gegenwärtiger* und bestenfalls noch die Karrieren *ehemaliger* Absolventen erfasst und analysiert werden müssten. In der Literatur wurde sogar erwogen, außerschulische bzw. -universitäre Quellen zu erschließen, etwa *Social Media Accounts*.⁶⁴⁴ Eine Vielzahl von datenschutzrechtlichen Datenerhebungs- und Zweckänderungsklauseln wäre erforderlich, sollte eine so breit vernetzte Datenauswertung rechtlich ermöglicht werden.⁶⁴⁵ Einfache Varianten einer Zulassungs-KI könnten sich natürlich auf leicht(er) zu erhebende Daten bzw. entsprechende Muster beschränken, wie etwa die Abitur-Noten;⁶⁴⁶ sie würden damit aber das Big-Data-Versprechen einer möglichst umfassenden Kriterienbildung und -auswertung (die das Bundesverfassungsgericht ja auch gefordert hat) nicht einlösen.⁶⁴⁷
- Anknüpfend an die intensiven datenschutzrechtlichen Diskussionen um ein „Recht auf Erklärung“ automatisierter Einzelfallentscheidungen⁶⁴⁸ steht zudem die Frage im Raum, ob und wie eine Studienzulassungs-KI ihre Entscheidungen

Zu vergleichbaren Systemen in den USA und Neuseeland *Martini et al.*, *Automatisch erlaubt?* 2020, S. 22 ff., m. w. N. auch zu Projekten in Deutschland.

642 *Claudia de Witt*, Fernuni Hagen, Interview, zitiert nach *Schumann*, *Deutscher Bildungsserver*, 1.7.2019. Früh und optimistisch auch *Mayer-Schönberger/Cukier*, *Lernen mit Big Data*, 2014.

643 Vgl. dagegen tendenziell *ErwGr. 71* zur DSGVO: „Diese Maßnahme [automatisierte Einzelfallentscheidung i. S. v. Art. 22 DSGVO] sollte kein Kind betreffen.“ Dazu *Bygrave*, in: *Yeung/Lodge (Hg.)*, *Algorithmic Regulation*, 2019, S. 248 (252).

644 *Martini et al.*, *Automatisch erlaubt?* 2020, S. 17.

645 Vgl. dazu schon *Rademacher*, *RdJB* 69 (2021), 254 (263 ff.) m. w. N.

646 Mit diesem, dem französischen Recht entnommenen Bsp. (dem Uni-Zulassungsprogramm *Parcoursup*), arbeitet etwa *Hermstrüwer*, *AöR* 145 (2020), 479 (480 und *passim*).

647 Für ein Negativ-Bsp. s. *Hao*, *MIT Technology Rev.* v. 20.8.2020 (Onlinequelle).

648 Vgl. Art. 22 Abs. 3 DSGVO i. V. m. *ErwGr. 71*, S. 4 ff. Die Frage, ob sich daraus ein Recht auf Erklärung vollständig automatisierter Einzelfallentscheidungen ableiten lässt, ist umstr., wurde aber überwiegend verneint, s. statt vieler *Wachter/Mittelstadt/Floridi*, *International Data Privacy Law* 7 (2017), 76 ff. Vgl. nun aber, zu Art. 15 Abs. 1 lit. h DSGVO, *EuGH*, *Urt. v. 27.2.2025*, *Rs. C-203/22* (*Dun & Bradstreet Austria*), *Rn. 43 ff.*, dazu unten ausf., → § 4 *Rn. 148 ff.*

so menschlich nachvollziehbar vermitteln könnte, dass ein menschlicher Sachbearbeiter die Entscheidung noch sinnvoll verantworten bzw. ein sinnvoller Widerspruch bzw. Rechtsschutz der nicht zugelassenen Bewerber möglich wäre. Das *Black-Box-Problem* stellt sich hier mit Dringlichkeit.⁶⁴⁹

- Eng verknüpft sind damit schließlich gleichheitsrechtlich motivierte Anfragen an die Systeme, die sich bei so weit in die Zukunft auswirkenden Prognoseentscheidungen wie solchen über die Studien- und Berufseignung besonders aufdrängen.⁶⁵⁰ Allzu leicht, so die verbreitete Befürchtung, schlagen die oben skizzierten statistischen Unzulänglichkeiten KI-gestützter Verfahren (*Sampling Bias*, *Proxy Discrimination*, *Modelling Bias*⁶⁵¹) sich in solchen Konstellation in einer Perpetuierung bestehender Ungleichheiten nieder, die dem Ideal einer tatsächlich möglichst *nur* eignungsbezogenen Entscheidung offensichtlich widersprechen.⁶⁵²

Bei allen berechtigten Bedenken ist zu berücksichtigen, dass eben in anderen Staaten 314 bereits intensiv auch über den zulassungsrechtlichen Einsatz von *Edtech* nachgedacht wird. Und es ist zu beachten, dass die EU mit diesem Einsatz rechnet: Sie hat im AI Act „KI-Systeme, die bestimmungsgemäß zur Feststellung des Zugangs oder [zur] Zulassung oder zur Zuweisung natürlicher Personen zu Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen“ (Anhang III Nr. 3 lit. a AI Act), zwar als Hochrisiko-KI kategorisiert. Sie will die Technologie damit aber eben nicht als *zu* riskant verbieten, sondern sieht neben Risiken auch erhebliche Chancen,⁶⁵³ was ‚lediglich‘ zu einer besonderen Regulierungsbedürftigkeit führen soll.⁶⁵⁴

Wichtig ist hier abschließend noch der Hinweis, dass mit einer Auswahl- und Verteilungsentscheidung jedenfalls im öffentlich-rechtlichen Bereich häufig natürlich noch 315 keine *Realisierung* von Recht im eigentlichen Sinn bewirkt wird. Wäre das so, wären wir tatsächlich phänomenologisch nicht mehr im Bereich der *Compliance Assistance*, sondern hätten potentiell in den Bereich der *Impossibility Structures* gewechselt, wenn und weil die (Universitäts-)Verwaltungen automatisiert zur Gewährung der (rechtmäßigen) Leistung gezwungen wären, ohne selbst noch auf den Prozess einwirken zu können. Eine solche *vollständige* Verselbstständigung des Verfahrens wird aber von niemanden diskutiert. Es geht also bei den diskutierten Systemen nicht um Verunmöglichung, sondern Assistenz bei der bzw. zur rechtmäßigen, eben leistungs-

649 Dazu auch Rademacher, RdJB 69 (2021), 254 (266 ff.) m. w. N.

650 Vgl. nur ErwGr. 56 zum AI Act, der allerdings durchaus ausgewogen Chancen und Risiken von KI im Bildungsbereich adressiert.

651 Dazu schon oben, → § 1 Rn. 31, → § 1 Rn. 32 und → § 1 Rn. 35.

652 s. die Nachw. zur Diskussion bei Rademacher, RdJB 69 (2021), 254 (268 ff.).

653 s. ErwGr. 56 zum AI Act.

654 Vgl. für eine erste Einschätzung der mit dem Entwurf für einen AI Act vorgeschlagenen Regelungen speziell zu *Edtech* Rademacher, RdJB 69 (2021), 254 (271 ff.).

und eignungsgerechten Auswahl, die letztlich weiterhin von den Universitäten bzw. dem dort eingesetzten Personal geleistet werden soll.

7. Zur (fehlenden) übergreifenden Diskussion

- 316 Nach meinem Eindruck fehlt es bislang an einer übergreifenden Diskussion um *Compliance Assistance Technologies* spezifisch unter dem Gesichtspunkt einer optimierten Realisierung von Recht, die versuchen würde, die Chancen und Risiken dieses Technologieeinsatzes mit *Intelligent Surveillance* und *Impossibility Structures* in Bezug zu setzen.⁶⁵⁵ Das ist eine gewichtige Leerstelle der Debatte: Wie ich später noch zeigen möchte, sind *Compliance Assistance Technologies* ein Weg, die immer weiter zunehmende Komplexität des modernen Rechts⁶⁵⁶ zu bewältigen, und damit das rechtstheoretische Paradoxon eines Rechts aufzulösen, das sich zwar an Laien als (Steuerungs-)Adressaten *richtet*, aber für Juristinnen *geschrieben* ist. Das hat mittlerweile auch die EU-Kommission erkannt, deren *Office of Publications* an einer – vermutlich NLP-basierten – KI arbeitet, die ihren eigenen Beamten (sic!), aber auch Unternehmen, Bürgern und Einwohnern der EU künftig als eine Art Rechts-Suche-Chatbot zur Verfügung stehen und dabei unterstützen soll, dass in ihrem Fall/auf sie anwendbare EU-Recht finden und anwenden zu können⁶⁵⁷ – also mindestens eine Vorstufe der *Compliance Assistance* i. e. S. *par excellence*.
- 317 Nimmt man diese Perspektive der Assistenz ein, lassen sich *Compliance Assistance Technologies* nicht mehr allein in Akzessorietät zu Überwachung und Zwang konzeptionalisieren. Denn sie verlangen – indem sie dem Adressaten der Information letztlich die Entscheidung über die Befolgung freistellen – gerade nicht Rechenschaft über seine Rechtschaffenheit ab, sondern nehmen ihn einerseits als zuständigen Rechtsadressaten ernst, erkennen aber andererseits an, dass die meisten Adressaten – da sie juristische Laien sind – mit dieser Zuständigkeit gewisse Schwierigkeiten haben dürften. *Compliance Assistance Technologies* könnten den Bürger damit aus seiner unmündig-paradoxen (oder sogar kafkaesken?) Rolle als *rechtstheoretisch unzuständiger Rechtsadressat* befreien; was aber dennoch wiederum *nicht* bedeutet, dass Überwachung und Zwang beziehungslos neben *Compliance Assistance* stehen würden. Diese unvollständigen Gedanken und komplexen Vorankündigungen sollen in → § 4 aufgelöst werden.

655 Knappe, gute Überlegungen finden sich bei *Beaucamp*, Rechtsdurchsetzung durch Technologie, 2022, S. 180 f.; zur Möglichkeit des automatisierten/unterstützten Rechtswissenserwerbs spezifisch durch juristische Laien s. grundlegend schon *Raabe et al.*, *Recht Ex Machina*, 2012, deutlich S. 5 und passim.

656 Zu den Möglichkeiten, rechtliche Komplexität empirisch zu messen, nun *Beckedorf*, Komplexität des Rechts, 2025, passim.

657 Bericht von *Herwig Hofmann* beim INDIGO-Workshop am 12.5.2023 in Barcelona.

Hier seien zunächst noch einige konventionellere und das heißt: zunächst einige 318 kategorisierende Beobachtungen zu *Compliance Assistance Technologies* angestellt. Tatsächlich dürften diese Technologien zunächst nämlich dazu führen, die Komplexität des Rechts weiter zu *steigern*. Aber der Reihe nach:

a. Dimensionen von Rechtswissensproblemen. Die in diesem Abschnitt III. genannten Beispiele waren sehr breit gefächert, teils auch noch fiktiv. Die breite Darstellung wurde gewählt um zu illustrieren, wie divers die Dimensionen an Rechtswissensproblemen sind, die *Compliance Assistance Technologies* erfassen könn(t)en: 319

- *Hinsichtlich des notwendigen Normwissens* hatten wir es beispielsweise zu tun mit einem sehr speziellen und Laien eher unbekanntem Rechtsgebiet (Urheberrecht) und mit einem zwar einfachen und in der Regel bekannten, aber erfahrungsgemäß häufig gebrochenen und dann unter Umständen sehr schadensträchtigen Recht (Straßenverkehrsrecht); schließlich mit regional und temporal stark ausdifferenziertem bzw. volatilem Recht (Infektionsschutzrecht).
- *Hinsichtlich des normativ geforderten Sachverhaltenswissens* sollten insbesondere die beiden letzten Beispielsfelder (Verbraucherschutzrecht und Recht der Studienzulassung) aufzeigen, dass wir es einerseits mit einer erheblichen Breitenproblematik zu tun haben können (also *individualisierte* Verbraucherinformationen im digitalen, d. h. schnellen Massendatenverkehr zu liefern), andererseits mit einer ungewöhnlichen Tiefenproblematik (i. e. bei der Anfertigung individueller, sehr langfristiger Prognoseentscheidungen im Studienzulassungsrecht).
- *Hinsichtlich des erwartbaren Adressatenwissens* – und entsprechender Kontextualisierungsfähigkeiten – spannen die Anwendungsbeispiele den Bogen über unterschiedlich vorinformierte Akteure, die vom rechtsfernen Jedermann (Infektionsschutzrecht, Urheberrecht, Verbraucherschutzrecht) über zumindest spezifisch geschulte Autofahrer (Straßenverkehrsrecht) bis hin zu rechtlichen Semi-Profis reichen (im Bereich der Studienzulassung).

b. Steuerungswirkungen bei den Adressaten. Hinsichtlich ihrer Steuerungswirkung 320 auf diese Adressaten sind *Compliance Assistance Technologies* in allen Fällen und definitionsgemäß zunächst bloße Information. Sie sollen der redlichen, normbefolgungswilligen Bürgerin, der Unternehmerin oder dem Verwaltungsbeamten der Universität Unterstützung bieten gegen die Überforderung, die mit einer immer komplexeren und dichten Rechtslage bzw. dem deshalb erforderlichen, immer schwieriger zu erlangenden Sachverhaltenswissen einhergeht. Der Einsatz ist dabei sozusagen echt freiwillig denkbar (wie im Fall von NINA), kann alternativ privat bzw. vom Arbeitgeber gleichsam ‚aufgenötigt‘ sein (wie im Beispiel der Urheberrechtskontrolle auf Stud.IP), oder kann schließlich gesetzlich vorgeschrieben und ausgestaltet werden (so die ‚intelligenten‘ Kfz-Assistenzsysteme nach der VO [EU] 2019/2144 und die noch fiktiven Überlegungen zum Einsatz im Verbraucherschutz-

und Studienzulassungsrecht). Freilich könnte auch im Bereich des ‚echt‘ freiwilligen Einsatzes von Assistenztechnologien perspektivisch ein mittelbar-faktischer Einsatzdruck entstehen, wenn und soweit der Einsatz der Vermeidung eigener straf- oder zivilrechtlicher Haftung der Nutzer dienen kann.⁶⁵⁸

- 321 *Assistance Technologies* nutzen durch den Verzicht auf eine *ex post* nur vielleicht korrigierbare Zwangsstruktur die besseren Kontextualisierungsfähigkeiten des Menschen. Es sind also schon definitionsgemäß hybride Mensch-Maschine-Arrangements, wobei die (Nicht-)Realisierung stets dem Menschen als sozusagen physischer Komponente des Systems obliegt. Voraussetzung für ein *gelingendes* Arrangement ist aber, dass die Software den menschlichen Nutzern *akteursgerecht* hinreichend präzise und zugleich nachvollziehbare Informationen liefert, damit diese die ausgeworfenen Subsumtionsschlüsse gegebenenfalls kritisch hinterfragen können.⁶⁵⁹ Denn auch im Fall *formal* reiner Assistenzstrukturen besteht selbstverständlich die Gefahr, dass das System *materiell* zur Herausbildung eines gelebten Rechts führt, das dem geschriebenen – gemessen an den Maßstäben der juristischen Methode – nicht ‚richtig‘ entspricht. Auch im Bereich von Subsumtionsschlüssen kann der vielfach beschriebene *Automation Bias* – sinngemäß: *ich glaube technologisch erstellten Informationen, weil sie technologisch erstellt sind* – Bedeutung und (negative) Konsequenzen erlangen.⁶⁶⁰

- 322 Auf eine weitere, versteckte Wirkungsdimension von Information über das rechtlich Gesollte weist *Christoph Möllers* hin, die gerade auch für unser Thema einer Realisierungsoptimierung wichtig ist:

„Eine erste Wirkung von Normen kann dadurch entstehen, dass der Hinweis auf eine bestimmte Möglichkeit das Ergreifen anderer Möglichkeiten faktisch erschwert. [...] Indem ich durch eine Norm eine bestimmte Möglichkeit auszeichne, herausgebe und explizit mache, nehme ich autorisiert Aufmerksamkeit in Anspruch, die für die anderen Möglichkeiten nicht mehr zur Verfügung steht. [...] Mit der Wahrnehmung der Norm nehme ich den sozialen Zusammenhang wahr, der die Norm autorisiert hat und der mich auch dann beeindrucken kann, wenn ich die Norm verletze. Anders formuliert: Auch wenn ich die Norm nicht befolge, möchte ich mich mit der Autorität, die hinter ihr steht, nicht anlegen, sei es, weil sie mich bedroht, sei es, weil ich sie trotz meines abweichenden Verhaltens anerkenne. Darum breche ich die Norm heimlich und bringe dadurch ein Stück ihrer Wirksamkeit zum Ausdruck.“⁶⁶¹

658 Vertiefend hierzu unten, → S. 348 ff.

659 Für einen Vorschlag zur Konturierung solcher Arrangements auf mittlerer Abstraktionshöhe, die auch *Impossibility Structures* und *Justification Structures* mit einbezieht, s. unten, ab → S. 351.

660 Dazu unten mehr, → § 4 Rn. 77.

661 *Möllers*, Die Möglichkeit der Normen, 2018, S. 425.

Nehmen wir an, dass diese soziologisch imprägnierten Überlegungen richtig sind.⁶⁶² 323
 Dann liegt in der automatisierten Hinweisfunktion auf die normativ gewünschte Verhaltensmöglichkeit, die *Compliance Assistance Technologies* liefern, bei aller theoretischen Freiwilligkeit eventuell doch eine Art von Realisierungsnudging (= autorisierte Fokussierung von Aufmerksamkeit, in den Worten von Möllers), das zur Realisierung beiträgt *entweder*, weil es die Realisierung tatsächlich wahrscheinlicher macht, *oder*, weil es rechtlich deviantes Verhalten zumindest bewusst macht, und dadurch in die Heimlichkeit drängt; mit der Folge, dass die intersubjektive Infragestellung der Norm durch sichtbare Devianz unwahrscheinlicher wird. Auch hierauf komme ich in → § 4 nochmals ausführlich zurück (→ S. 393 ff.).

c. Rückwirkungen auch auf das Recht? Selbst dann, wenn es nun im Zuge der 324
 KI-Regulierungsbemühungen gelingt, Arrangements zu schaffen, die hochwertige (zumindest *meist* richtige, nachvollziehbare etc.) Rechtsinformationen bereitstellen, die das ‚richtige‘ Recht nicht verzerren (siehe soeben), dann ist gleichwohl anzunehmen, dass die Verfügbarkeit immer genauer arbeitender *Assistance Technologies* Rückwirkungen auf das Recht haben wird, die über dessen bessere Erkennbarkeit für Laien hinausgehen. Einmal könnten die Technologien zu einem *strengerem* Fahrlässigkeitsmaßstab hinsichtlich der tolerablen Rechts(un)kenntnis führen, insbesondere im Rahmen der Regeln über Verbotsirrtümer. Viel wichtiger aber ist, dass *Assistance Technologies* es dem Gesetzgeber und den Gerichten weiter erleichtern, die Komplexität des Rechts hin zu einer immer weiter verfeinerten Einzelfalladäquanz zu erhöhen. Im Steuerrecht mit seinen diversen Assistenzsystemen ist das bereits Thema gewesen:

“Zelenak argues that tax-return-preparation software eliminated that ‘complexity restraint’, freeing legislators to impose ever more baroque provisions. [T]he rise of computational complexity in the tax code embod[ies] an enduring problem in automation. Technologists cannot assume that computational solutions to one problem | will not affect the scope and nature of that problem.”⁶⁶³

In Europa, unter Geltung des Verhältnismäßigkeitsprinzips und immer weiter ausdifferenzierter *materieller* Gleichbehandlungsgebote,⁶⁶⁴ 325
 könnte die Verfügbarkeit von avancierten Assistenztechnologien von den Gesetzgebern sogar *verlangen*, die Komplexität immer weiter zu steigern. Beispielhaft dafür eine Überlegung von Philipp Hacker:

“Equal treatment may even require the application of different norms if Big Data analysis reveals relevant differences between persons [...]. Relevant differences among actors may now,

662 Ibid., S. 424, bezeichnet die Frage, ob sich eine „immanente“ Wirkung von (zur Kenntnis gebrachten) Normen empirisch nachweisen lässt, als „offene Frage“.

663 Pasquale, *George Washington Law Rev.* 87 (2019), 1 (9 f.).

664 Dazu auch unten, → § 6 Rn. 21.

on many occasions, become observable thanks to the use of Big Data. If certain disclosures only work for certain actors, it would seem to violate equality to knowingly apply them to those actors who do not benefit from them”.⁶⁶⁵

- 326 *Hacker* hat diese Überlegungen über die von ihm näher untersuchten Informationssysteme im Verbraucherschutzrecht angestellt. Aber sie fügen sich ein in den großen Trend hin zu den von *Gertrude Lübbe-Wolff* sogenannten „milden [= differenzier- ten, sachangemessenen, verhältnismäßigen⁶⁶⁶] Rechtszuständen“, die das moderne deutsche und europäische Recht immer stärker prägen, deren „Setzung, Administration und Durchsetzung [aber] ungeheure Ressourcen erfordert, deren Verfügbarkeit alles andere als eine Selbstverständlichkeit ist.“⁶⁶⁷ Typisierungen hingegen waren und sind ein Mittel der Ressourcenschonung,⁶⁶⁸ sind vom modernen Recht aber immer weniger gut gelitten. Damit sind wir wieder beim Ressourcenproblem des Rechtswissens und der Rechtsrealisierung angelangt, das *gelingende* KI zwar nicht ganz beseitigen, aber doch immer weiter abschwächen kann. Funktionierende (!) *Compliance Assistance Technologies* können zwar definitionsgemäß nicht durchsetzen, aber sie können die ‚richtige‘ Auslegung des Rechts zumindest *sichtbar* machen. Insgesamt können sie damit die Basisbedingung für seine *Realisierung* schaffen.

IV. Justification Structures

„Bei allen Versuchen, Klarheit herzustellen
– gesetzliche Normen sind keine klaren ‚Linien‘,
die man nicht überschreiten darf,
sondern ‚Zonen‘, in denen erst ausgehandelt wird,
was geduldet wird und was nicht (Williams 1970, S. 413).“

Stefan Kühl⁶⁶⁹

- 327 Die soeben unter → III. beschriebenen Assistenzstrukturen ergeben vor allem dann Sinn, wenn ein grundsätzlicher Normbefolgungswille besteht bzw. unterstellt werden kann, dessen Umsetzung angesichts der Komplexität des modernen Rechts *ohne* technische Unterstützung an Grenzen stoßen könnte. In vielen Bereichen freilich ist der Normbefolgungswille zweifelhaft, weil sich der Normbefolgungsnutzen nicht

⁶⁶⁵ *Hacker*, ERPL 25 (2017), 651 (659 f.).

⁶⁶⁶ Vgl. *Lübbe-Wolff*, Das Dilemma des Rechts, 2017, S. 22.

⁶⁶⁷ *Ibid.*, S. 62.

⁶⁶⁸ *Ibid.*, S. 63: „Die sturen Formalismen des älteren Rechts, die kruden Methoden der Sachverhaltsfeststellung, die Härte der Sanktionen, die aus heutiger Sicht eklatanten Mängel an vernünftiger rechtlicher Differenzierung waren nicht einfach bloß Resultat menschlichen Unverständes. In ihnen spiegelt sich die Begrenztheit der Ressourcen für die Entwicklung und Administration des Rechts.“

⁶⁶⁹ *Kühl*, Brauchbare Illegalität, 2020, S. 39.

hinreichend unmittelbar oder nicht hinreichend individuell erschließen mag. Die schwache Disziplin beim Einhalten der Corona-Schutzvorschriften hat das anschaulich illustriert. Ähnlich dürfte es mit der Geltung des Urheberrechts im digitalen Raum bestellt sein, die wahrscheinlich nicht nur wegen des mangelnden rechtlichen Verständnisses der Nutzer prekär ist. Eine Lösung sind dann eben die schon beschriebenen *Impossibility Structures* (oben, → II.). Diese Strukturen haben aber zumindest auf absehbare Zeit mit den Unzulänglichkeiten der Filtertechnologien zu kämpfen, die z. B. die kontextabhängigen Schranken des Urheberrechts schwer erkennen können.

1. Begriff und erste Anwendung im Online-Kommunikationsrecht

Einen dritten Weg zwischen reiner Hilfe zur – freiwilligen und daher prekären – 328 Rechtsbefolgung durch Assistenztechnologien und deren – eventuell überschießen- der und daher potentiell dysfunktionaler – Erzwingung durch Unmöglichkeitsstrukturen geht das noch recht junge Urheberrechts-Diensteanbieter-Gesetz (UrhDaG), das der Umsetzung von Art. 17 DSM-RL dient. Diese Norm⁶⁷⁰ stellt die nationalen Gesetzgeber vor einen auf den ersten Blick erheblichen „Ziel- und Pflichtenkonflikt“⁶⁷¹: Einerseits sollen Plattformen („Diensteanbieter zum Teilen von Online-Inhalten“⁶⁷²) nach Art. 17 Abs. 1 DSM-RL künftig für rechtswidrigen Upload ihrer Nutzer genauso haften, als handele es sich um eine eigene Verwertungshandlung.⁶⁷³ Das gilt nur dann nicht, falls sie „nach Maßgabe branchenüblicher Sorgfalt“ dafür sorgen, dass urheberrechtlich geschützte Inhalte „nicht [ohne entsprechende Berechtigung] verfügbar sind“ (Art. 17 Abs. 4 DSM-RL).⁶⁷⁴ Nach einhelliger Auffassung heißt das: Sie haften (nur) dann nicht, wenn sie Upload-Filter für die Erkennung und Verhinderung eben solcher widerrechtlicher Uploads ihrer Nutzer einsetzen.⁶⁷⁵ Andererseits verlangt dieselbe Norm in ihrem Absatz 7, dass der Einsatz derartiger Filter „nicht bewirken darf“, dass urheberrechtlich *zulässige* Nutzungen blockiert werden, zu denen eben auch Karikaturen, Zitate usw. gehören können, die mittels automatisierter Filter so schwierig zu erkennen sind (Verbot des *Overblocking*).

670 s. oben, → § 2 Rn. 150.

671 Lennartz/Möllers, GRUR 2021, 1109.

672 s. Art. 2 Nr. 6 DSM-RL (EUR) 2019/790.

673 Vgl. auch § 1 Abs. 1 UrhDaG. Zum Unterschied zwischen täterschaftlicher Haftung und der zuvor geltenden Störerhaftung (§ 10 TMG a. F.) s. F. Hofmann, NJW 2021, 1905 (1906).

674 s. zu den unterschiedlichen Regelungsoptionen für eine Haftung der Plattformen für nutzerseitigen Upload F. Hofmann, ZUM 2019, 617 (619 ff.).

675 s. die Nachw. in → § 2 Fn. 326. Vgl. aber auch GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 78, der davon ausgeht, dass aus der Haftung auch eine vor- ausgehende Verhaltenspflicht zur Verhinderung von urheberrechtswidrigem Upload folge; relativierend dann aber a. a. O., Rn. 86: „in der Praxis [sic!] die Bedeutung echter *Verpflichtungen*“ (Hervorhebung im Original).

- 329 *a. Begriff.* Der Bundesgesetzgeber hat sich der Herausforderung mit dem UrhDaG rechtstechnisch in einer Weise gestellt, die ich hier als *Justification Structure* einführen möchte. Kurz gesagt besteht die gewählte Umsetzungslösung aus der Kombination – *erstens* – einer KI-basierten Unmöglichkeitstruktur (= Upload-Filter, nach der Gesetzesbegründung sogenannter „Pre-Check“⁶⁷⁶), dessen Einsatz die Inhaber von Urheberrechten von den Diensteanbietern *de facto*⁶⁷⁷ verlangen dürfen, den aber – *zweitens* – ein Nutzer des Dienstes unter bestimmten Umständen⁶⁷⁸ dadurch *selbst* deaktivieren kann, dass er sich ausdrücklich auf eine gesetzliche Erlaubnis beruft (sogenannte „Kennzeichnung als erlaubte Nutzung“).⁶⁷⁹ Der Diensteanbieter muss den Nutzer im Moment des geplanten Uploads auf das Erfordernis einer gesetzlichen Erlaubnis für den Upload hinweisen,⁶⁸⁰ falls der Pre-Check positiv ‚angeschlagen‘ hat.⁶⁸¹
- 330 Das Modell des UrhDaG wandelt sich nun dadurch von der – gegenüber dem Beispiel von Stud.IP wegen des Pre-Checks natürlich ohnehin schon sehr viel anspruchsvolleren – *Compliance Assistance Technology* zur *Justification Structure*, dass die Deaktivierung des Filtermechanismus – *drittens* – mit einer Information des *Rechteinhabers* verbunden sein muss,⁶⁸² sodass dieser also weiß, dass eine Nutzerin sein Werk verwendet und vor allem in die Lage versetzt ist, deren dafür gegebene Begründung (= Berufung auf ein Nutzungsrecht) kritisch zu hinterfragen, um gegebenenfalls dagegen vorzugehen. Ein entsprechendes, internes Beschwerdeverfahren

676 BT-Drs. 19/27426 v. 9.3.2021, S. 141.

677 s. § 7 Abs. 1 UrhDaG [Qualifizierte Blockierung]. Nach dieser Norm sind Diensteanbieter nicht *ausdrücklich* verpflichtet, Filtertechnologien einzusetzen; die Erfüllung des Anspruchs der Rechteinhaber ist sozusagen technologieneutral formuliert (vgl. auch § 7 Abs. 2 S. 2 UrhDaG: „Beim Einsatz automatisierter Verfahren sind die §§ 9 bis 11 anzuwenden.“). Doch ist eine rein menschliche Umsetzung des Blockiervorgangs jedenfalls bei größeren Plattformen nicht realistisch: allg. Auffassung, vgl. nur *F. Hofmann*, NJW 2021, 1905 ff.

678 s. § 9 Abs. 2 UrhDaG: „Für nutzergenerierte Inhalte, die 1. weniger als die Hälfte eines Werkes eines Dritten oder mehrerer Werke Dritter enthalten, 2. die Werkteile nach Nummer 1 mit anderem Inhalt kombinieren und 3. Werke Dritter nur geringfügig nutzen (§ 10) oder *als gesetzlich erlaubt gekennzeichnet sind* (§ 11), wird widerleglich vermutet, dass ihre Nutzung nach § 5 gesetzlich erlaubt ist (mutmaßlich erlaubte Nutzungen).“ Hervorhebung hier.

679 Die Gesetzesbegründung spricht hier sprachlich wenig naheliegend von einem „Pre-Flagging“, s. BT-Drs. 19/27426, S. 141.

680 Der einschlägige § 11 UrhDaG [Kennzeichnung als erlaubte Nutzung] lautet: „(1) Soll ein nutzergenerierter Inhalt beim Hochladen automatisiert blockiert werden und handelt es sich nicht um eine geringfügige Nutzung nach § 10, so ist der Diensteanbieter verpflichtet, 1. den Nutzer über das Blockiervorgang des Rechteinhabers zu informieren, 2. den Nutzer zugleich mit der Information nach Nummer 1 auf die Anforderlichkeit einer gesetzlichen Erlaubnis nach § 5 für eine öffentliche Wiedergabe hinzuweisen und 3. es dem Nutzer zu ermöglichen, die Nutzung als nach § 5 gesetzlich erlaubt zu kennzeichnen.“

681 Unklar bleibt, ob das UrhDaG es ausreichen lassen will, wenn/dass der Nutzer abstrakt auf das Erfordernis irgendeiner gesetzlichen Erlaubnis hingewiesen wird, oder ob ihm nicht – etwa nach dem Vorbild von Stud.IP (s. oben, → § 2 Rn. 290) – laiengerecht aufbereitete Informationen dazu geliefert werden müssen oder wenigstens sollten, welche Erlaubnisse denn in Frage kommen.

682 § 9 Abs. 3 UrhDaG [Öffentliche Wiedergabe mutmaßlich erlaubter Nutzungen] lautet: „Der Diensteanbieter informiert den Rechteinhaber sofort über die öffentliche Wiedergabe und weist ihn auf das Recht hin, nach § 14 Beschwerde einzulegen, um die Vermutung nach Absatz 2 überprüfen zu lassen.“

beim Diensteanbieter verlangen die §§ 13 ff. UrhDaG. Im Unterschied zu den aktuell freiwillig angebotenen Streitmechanismen zum Schutz von Urheberrechten z. B. auf YouTube,⁶⁸³ verlangt § 14 Abs. 3 Nr. 3 UrhDaG, dass der Diensteanbieter selbst (oder unter Rückgriff auf eine anerkannte externe Beschwerdestelle, § 15 UrhDaG) über die Beschwerde eines blockierten Nutzers entscheiden muss,⁶⁸⁴ und zwar innerhalb einer Woche und durch eine „natürliche“ und „unparteiische“ Person. Der Nutzer muss sich also vermittelt über das interne Beschwerdeverfahren vor dem Rechteinhaber *und* einem Dritten rechtfertigen, er wird gegebenenfalls⁶⁸⁵ sogar aus der – ihn vor einer Konfrontation zunächst schützenden – Anonymität oder Pseudonymität des Online-Verkehrs herausgestellt.

b. Details der Regelung im Urheberrechts-Diensteanbieter-Gesetz. Das soeben im 331 Überblick geschilderte Rechtfertigungs-Arrangement ist in seinen Details komplex und das Ergebnis eines von vielen Akteuren kontrovers begleiteten Gesetzgebungsverfahrens. Interessant ist, dass das finale UrhDaG gegenüber dem ersten Diskussions- und dem Referentenentwurf (RefE) aus dem Bundesjustizministerium einige nennenswerte Verschärfungen zugunsten der Rechteinhaber und damit *pro* Filterung aufweist.

Erstens fällt auf, dass die Kennzeichnungsmöglichkeit als erlaubte Nutzung in der finalen Fassung nur noch für *gesetzliche* Erlaubnisgründe vorgesehen ist; der Referentenentwurf wollte eine Berufung auch auf „vertragliche“ Erlaubnisse ermöglichen.⁶⁸⁶ Offenbar geht der Gesetzgeber davon aus, dass auch Individual-Lizenzen sofort an den Diensteanbieter gemeldet werden, sodass es schon von vornherein nicht zu einem Blockierverlangen des Rechteinhabers kommen dürfte.

Zweitens hat der Gesetzgeber den sozusagen technologischen, doppelten Boden, den 333 der Referentenentwurf vorsah, modifiziert: So sollte nach § 12 S. 1 UrhDaG-RefE die

683 Vgl. die Schilderung des Streitmechanismus, den *Youtube* anbietet, bei Schillmöller/Doseva, MMR 2022, 181 (182 ff.): Den Mechanismus zeichne negativ aus, dass das Unternehmen lediglich eine Infrastruktur zur Verfügung stelle, ohne selbst entscheidend oder schlichtend in die Auseinandersetzung von Uploader und Rechteinhaber einzugreifen; das löse *Chilling Effects* zu dessen – also des Rechteinhabers – Gunsten aus: „Die Rechtsinhaber entscheiden selbst, ob ihre Ansprüche zutreffen, sowie über weitere Sanktionen, die den Uploader treffen können. Dabei tritt zu keiner Zeit ein Devolutiveffekt ein, der das Verfahren YouTube selbst oder einer anderen unabhängigen Instanz zur Entscheidung vorlegt. Es fehlt also im internen Beschwerdeprozess von YouTube eine unabhängige Entscheidungsinstanz.“

684 Für eine erste Analyse des vom UrhDaG vorgesehenen Beschwerdeverfahrens s. Schillmöller/Doseva, MMR 2022, 181 (185 ff.).

685 Falls entsprechende Möglichkeiten zur Auskunft nach dem TTDSG bestehen (§§ 21 ff.). Zur unbefriedigenden Fassung (damals noch von § 14 Abs. 3-5 TMG) Buchheim, JZ 2021, 539 ff.; auch Alacayir, GRUR-Prax 2022, 271 ff.; zu möglichen Lösungen de lege ferenda Janal, ZEuP 2021, 227 (260 ff.) m. w. N., bes. S. 272: „Ist die Rechtmäßigkeit der Inhalte umstritten, kann einem Privatnutzer im Regelfall zugemutet werden, zwischen der Sperre des Inhalts und der Aufdeckung seiner Identität zu wählen. Ist dies im Einzelfall nicht zumutbar, bedarf es einer verfahrensrechtlichen Absicherung der Pseudonymität des Nutzers während des Gerichtsverfahrens zur Klärung der Rechtmäßigkeit des Inhalts.“

686 s. § 8 Abs. 1 Nr. 3 UrhDaG-RefE v. 24.6.2020.

„Rechtfertigung“ des Upload-willigen Nutzers nur dann irrelevant sein, die *Impossibility Structure* des Filters sich also vom Nutzer selbst *nicht* deaktivieren lassen, falls diese Rechtfertigung „offensichtlich unzutreffend ist“, was „insbesondere dann der Fall sein [sollte], wenn der vom Nutzer hochgeladene Inhalt zu mindestens 90 Prozent mit den vom Rechtsinhaber zur Verfügung gestellten Informationen [über sein Werk] übereinstimmt“.⁶⁸⁷ Das Gesetz versperrt die Rechtfertigungsoption nun schon dann, wenn der Upload mindestens die Hälfte des geschützten Werks enthält und (!) er nicht mit anderen Inhalten kombiniert ist.⁶⁸⁸ Die Kombination mit anderen Inhalten sei einerseits typisch für Zitat, Parodie oder Pastiche, und sei andererseits technologisch gut erkennbar.⁶⁸⁹

- 334 Schließlich – *drittens* – hat der Gesetzgeber die Durchsetzungsmöglichkeiten der Rechteinhaber auf andere Weise gestärkt, indem er ein sogenanntes „roter-Knopf“-Verfahren⁶⁹⁰ als Teil des Beschwerdemechanismus geschaffen hat (§ 14 Abs. 4 UrhDaG): Demnach bleibt es zwar dabei, dass der hochladende Nutzer den Filter selbst durch Berufung auf eine gesetzliche Nutzungserlaubnis deaktivieren kann. Der Rechteinhaber, der ja über den Upload informiert wird (§ 9 Abs. 3 UrhDaG), kann aber dann, wenn er als ein „vertrauenswürdiger Rechtsinhaber“⁶⁹¹ registriert ist, eine sofortige Blockierung des hochgeladenen Inhalts noch *vor* Abschluss des Beschwerdeverfahrens nach § 14 UrhDaG verlangen. Diesen roten Knopf muss *beim Rechteinhaber* allerdings zwingend eine „natürliche Person“ betätigen,⁶⁹² der doppelte Boden zugunsten des Rechteinhabers muss also ein menschlicher sein. Der Diensteanbieter hat hingegen kein Ermessen mehr, sondern muss sofort und automatisiert

687 § 12 S. 1 UrhDaG-RefE v. 24.6.2020 [Sperrung und Entfernung bei Kennzeichnung als erlaubte Nutzung]: „¹Die Sperrung und Entfernung ist trotz Kennzeichnung nach § 8 Absatz 2 durchzuführen, wenn diese offensichtlich unzutreffend ist. ²Dies kann bei der Berufung auf gesetzliche Erlaubnisse insbesondere dann der Fall sein, wenn der vom Nutzer hochgeladene Inhalt zu mindestens 90 Prozent mit den vom Rechtsinhaber zur Verfügung gestellten Informationen übereinstimmt. ³Satz 2 gilt nicht für einzelne Abbildungen.“

688 s. für den Text von § 9 UrhDaG schon in → § 2 Fn. 678.

689 Oster, in: Ahlberg/Götting/Lauber-Rönsberg (Hg.), BeckOK Urheberrecht, 32. Ed. 15.9.2021, § 9 UrhDaG Rn. 8.

690 BT-Drs. 19/27426 v. 9.3.2021, S. 143.

691 s. zu diesem Status *ibid.*, S. 144: „Die Vertrauenswürdigkeit des Rechtsinhabers ist vom Diensteanbieter zu beurteilen und kann sich beispielsweise aus dem Umfang des beim Diensteanbieter hinterlegten werthaltigen Repertoires, dem damit verbundenen Einsatz besonders qualifizierten Personals oder auch aus der erfolgreichen Durchführung etlicher Beschwerdeverfahren in der Vergangenheit ergeben. Bei Streitigkeiten über die Vertrauenswürdigkeit eines Rechtsinhabers (und damit zugleich über den Zugang zum ‚roten Knopf‘) kann diese Frage auch gerichtlich geklärt werden. Erforderlich ist immer eine Prüfung durch eine vom Rechtsinhaber beauftragte natürliche Person. Unzulässig ist es daher, den ‚roten Knopf‘ über automatisierte Verfahren auszulösen. Löst der Rechtsinhaber den Mechanismus nach § 14 Absatz 4 UrhDaG-E dennoch automatisiert aus, kann er nicht mehr als vertrauenswürdiger gelten.“

692 § 13 Abs. 4 UrhDaG. Zur Erläuterung BT-Drs. 19/27426 v. 9.3.2021, S. 143: „§ 14 Absatz 4 UrhDaG-E trägt dem Umstand Rechnung, dass die generell-abstrakt definierten Voraussetzungen für mutmaßlich erlaubte Nutzungen in einem gewissen Umfang auch Nutzungen online verfügbar machen können, bei denen sich die Vermutung bei einer menschlichen Überprüfung ohne weiteres widerlegen ließe.“

blockieren.⁶⁹³ Vorkehrungen gegen den Missbrauch sowohl der Möglichkeit zur Kennzeichnung als erlaubte Nutzung wie auch des roten Knopfes finden sich in den Schlussbestimmungen des UrhDaG in § 18.⁶⁹⁴ Wichtig ist abschließend der Hinweis, dass der Rechtfertigungsversuch durch „Kennzeichnung als erlaubte Nutzung“ dem Nutzer *keinen* Schutz gegen zivil- oder strafrechtliche Inanspruchnahme vermittelt (keine *Safe-Harbour*-Wirkung).⁶⁹⁵

Anders verhält es sich hingegen bei der bislang hier noch nicht näher beschriebenen „geringfügigen Nutzung“. Das ist *neben* der „Kennzeichnung als erlaubte Nutzung“ das zweite Arrangement, mit dem der Gesetzgeber einem *Overblocking* vorbeugen will: Enthält ein Upload weniger als die Hälfte des geschützten Werkes und wird er mit anderen Inhalten kombiniert (bis hierher Voraussetzungen wie eben), *und* hat er *zusätzlich* einen in § 10 UrhDaG genau spezifizierten, maschinell gut erfassbaren geringen Umfang (z. B. „Nutzungen bis zu 15 Sekunden je einer Tonspur“, § 10 Nr. 2 UrhDaG), dann liegt ebenfalls eine „mutmaßlich erlaubte Nutzung“ i. S. von § 9 UrhDaG vor. Der vom Diensteanbieter genutzte Filter darf also nicht blockieren, diesmal *ohne* dass es einer vom Nutzer ausdrücklich geäußerten Rechtfertigung bedarf. Der Nutzer wird in dieser Variante auch nicht darüber informiert, dass er eine möglicherweise rechtswidrige Nutzung vornimmt. Freilich ist das verzichtbar, denn der Nutzer ist für den Zeitraum „bis zum Abschluss eines Beschwerdeverfahrens nach § 14 UrhDaG urheberrechtlich nicht verantwortlich“ (§ 12 Abs. 3 UrhDaG). Der *Rechteinhaber* muss auch in dieser Variante über den Upload informiert werden (§ 9 Abs. 3 UrhDaG). 335

Greift keine der beiden genannten Optionen (also weder Verfügbarkeit einer *Justification Structure* noch „geringfügige Nutzung“), dann erlaubt bzw. drängt⁶⁹⁶ das Re- 336

693 BT-Drs. 19/27426 v. 9.3.2021, S. 143: „Wird eine mutmaßlich erlaubte Nutzung vom Diensteanbieter öffentlich wiedergegeben, erhält der betroffene Rechtsinhaber einen Hinweis nach § 9 Absatz 3 UrhDaG-E. Hierauf kann er mit der Beschwerde und der Erklärung nach § 14 Absatz 4 UrhDaG-E reagieren. Der Diensteanbieter ist dann zur sofortigen Blockierung bis zum Abschluss des Beschwerdeverfahrens verpflichtet. Ein Ermessen steht dem Diensteanbieter nicht zu; eine weitere Prüfung des Sachverhalts oder die Beteiligung des Nutzers unterbleiben. Die sofortige Blockierung ist automatisiert durchzuführen und hat also vorbehaltlich technischer Verzögerungen sofort stattzufinden.“

694 § 18 UrhDaG [Maßnahmen gegen Missbrauch] lautet auszugsweise: „(3) Verlangt ein Rechtsinhaber wiederholt fälschlicherweise die sofortige Blockierung mutmaßlich erlaubter Nutzungen während des Beschwerdeverfahrens nach § 14 Absatz 4, so ist er für einen angemessenen Zeitraum von diesem Verfahren auszuschließen. (4) [...] (5) Kennzeichnet ein Nutzer eine Nutzung wiederholt fälschlicherweise als erlaubt, so hat der Diensteanbieter den Nutzer für einen angemessenen Zeitraum von der Möglichkeit zur Kennzeichnung erlaubter Nutzungen auszuschließen.“

695 Vgl. *e contrario* § 12 Abs. 3 UrhDaG [Vergütung durch Diensteanbieter; Verantwortlichkeit].

696 Vgl. zu der etwas komplexeren Frage, ob das UrhDaG tatsächlich *Filterpflichten* auferlegt, nochmals oben, → § 2 Rn. 328, mit Fn. 675. Zudem ist zu beachten, dass das UrhDaG der zumindest auf *Youtube* beliebten Praxis der sog. „Monetarisierung“ nicht entgegensteht. Hierbei werden Inhalte, die von den automatisierten Urheberrechts-Erkennungstechnologien der Plattform („Content ID“) als geschütztes Material identifiziert werden, auf Wunsch der Rechteinhaber *nicht* blockiert, sondern es werden die im Zusammenhang mit dem Upload erzielten Werbeeinnahmen statt an die Uploader an die Rechteinhaber

gime des UrhDaG auf die Nutzung von Upload-Filtern als *Impossibility Structures*: Algorithmisch als unzulässig qualifizierter Upload muss dann zunächst blockiert werden. Der Nutzer, der sich gleichwohl berechtigt fühlt, die Inhalte öffentlich zugänglich zu machen, ist auf *ex post* wirksame Beschwerdeverfahren verwiesen.⁶⁹⁷ Dass es solche geben *muss*, sehen Art. 17 Abs. 9 UAbs. 1 („wirksame und zügige“ interne „Beschwerde- und Rechtsbehelfsverfahren“) und Art. 17 Abs. 9 UAbs. 2 S. 5 DSM-RL vor (die „Mitgliedstaaten gewährleisten, dass die Nutzer Zugang zu einem Gericht“ haben). Das UrhDaG setzt diese Vorgaben im schon erwähnten § 14 um bzw. stellt in § 13 Abs. 4 klar, dass die Möglichkeit gerichtlichen Rechtsschutzes „unberührt“ bleibt.

337 *c. Einschätzung des Generalanwalts zur Unionsrechtskonformität.* Die Einschätzung von Generalanwalt Saugmandsgaard Øe zur Klage Polens gegen Art. 17 Abs. 4 DSM-RL soll hier ausführlich dargestellt werden, obwohl der EuGH selbst schon sein Urteil gesprochen hat (dazu → d.). Grund dafür ist, dass der EuGH dem Generalanwalt *erstens* im Ergebnis folgt (= Art. 17 Abs. 4 DSM-RL sei *per se* unionsrechtskonform, es komme aber auf die konkrete mitgliedstaatliche Umsetzung an), dass der Generalanwalt *zweitens* die hier (!) interessierenden Elemente des deutschen *Umsetzungsgesetzes* implizit positiv gewertet hat, und dass der Generalanwalt *drittens* deutlich realitätsnäher argumentiert und er im Gegensatz zum Gerichtshof auf die rechtlich und tatsächlich kritischen Punkte tatsächlich eingeht.

338 Aber der Reihe nach: Zunächst ist festzuhalten, dass der Generalanwalt das politisch aufgeladene und missverständliche Wort der „Zensur“ bewusst meidet. Er spricht stattdessen nüchtern von „vorbeugenden Maßnahmen“ und „präventiven Einschränkungen“.⁶⁹⁸ Solche präventiven Einschränkungen würden den Wesensgehalt von Art. 11 GRC dann antasten, wenn dadurch

„die Vermittler, die diese Meinungsäußerungs-Infrastrukturen [= soziale Plattformen und Netzwerke] kontrollieren, von staatlicher Seite unmittelbar oder mittelbar dazu verpflichtet [würden], die Inhalte der Nutzer ihrer Dienste generell präventiv zu überwachen und nach rechtswidrigen oder sogar bloß unerwünschten Informationen jeglicher Art zu durchforsten[. Dann] wäre diese Kommunikationsfreiheit als solche in Frage gestellt.“⁶⁹⁹

339 Art. 15 E-Commerce-RL (jetzt Art. 8 DSA) mit seinem Verbot, den Diensteanbietern eine „allgemeine Überwachungspflicht“ aufzuerlegen, sei daher als „allgemei-

ausgeschüttet (= Monetarisierung des – tatsächlichen oder vermeintlichen – Urheberrechtsverstoßes). Da das Beschwerdeverfahren gegen eine solche Umlenkung der Geldströme zumindest von/auf *Youtube* sehr Rechteinhaber-freundlich ausgestaltet ist (s. soeben, in → § 2 Fn. 683), könnte das dazu verleiten, auf ein Blockiervorgang zu verzichten und damit das UrhDaG und dessen Beschwerdeverfahren (§§ 13 ff. UrhDaG) zu umgehen; vgl. zu den Details Schillmöller/Doseva, MMR 2022, 181 (186).

697 Vgl. hierzu auch F. Hofmann, NJW 2021, 1905 (1909 f.).

698 GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 77.

699 Ibid., Rn. 104.

ner Grundsatz des Internetrechts“ zu betrachten. Dieser sei vorliegend allerdings nicht verletzt: Die Pflicht zur automatisierten Filterung nach Urheberrechtsverstößen durch Sharing-Dienste-Anbieter sei nach den Maßstäben der jüngeren EuGH-Rechtsprechung keine *allgemeine*, sondern eine *spezifische* und damit eine grundsätzlich zulässige Überwachungspflicht,⁷⁰⁰ die deshalb auch den Wesensgehalt des Rechts auf freie Meinungsäußerung wahre.⁷⁰¹ Das gelte deshalb bzw. insoweit, als die Filterpflicht auf die von dem Rechteinhaber ausdrücklich benannten Inhalte beschränkt werde, und zwar in „wortgleicher“ (wohl auch: bildgleicher, tongleicher) oder „sinngleicher“ Form.⁷⁰² Das meine identische Reproduktionen bzw. solche, die

„mit [nur] unbedeutenden Änderungen versehen [seien], so dass die Öffentlichkeit sie von den Originalgegenständen nicht unterscheiden würde (z. B. bei rein technischen Veränderungen zur Umgehung des Filtersystems, wie etwa einer Änderung des Formats, der Umkehrung oder Änderung der Bildgeschwindigkeit usw.)“.⁷⁰³

Nach diesen Maßstäben soll also *Spezifität* der Überwachung schon dadurch 340 hergestellt sein, dass der Rechteinhaber sein *Recht*, wohlgemerkt: nicht etwa eine initiale *Rechtsverletzung*, präzise benannt habe.⁷⁰⁴ Es ergibt vor diesem Hintergrund Sinn, nicht mehr (nur) von einer *Notice-and-stay-down*-Verpflichtung zu sprechen, sondern von einer *Notice-and-prevent*-Pflicht,⁷⁰⁵ die nun im digitalen Urheberrecht bzw. genauer: im Anwendungsbereich des Art. 17 Abs. 4 DSM-RL/des § 7 UrhDaG gilt. Die Allgemeinheit der Überwachung ergibt sich damit konzeptionell nicht mehr – wie noch in der älteren Rechtsprechung des EuGH zu Art. 15 E-Commerce-RL⁷⁰⁶ – aus der „Menge der zu überprüfenden Informationen“, sondern ergibt sich bzw. besser: wird aufgehoben durch die „Präzision der Nachforschungen“, die dem Diensteanbieter auferlegt werden. Konsequenz: Wenngleich also der Wesensgehalt der Meinungs- und Informationsfreiheit einer undifferenzierten präventiven Überwachungspflicht entgegenstehe, sei der Unionsgesetzgeber nicht gehindert, „*bestimmten* Online-Vermittlern *bestimmte* aktive Maßnahmen zur Überwachung ganz *bestimmter* rechtswidriger Informationen vor[zuschreiben]“. ⁷⁰⁷

Die Vorschriften müssten aber auch noch dem Grundsatz der Verhältnismäßigkeit 341 genügen. In diesem Zusammenhang stellt der Generalanwalt dann ganz auf die Gefahr des *Overblocking*⁷⁰⁸ ab. Deutlicher als der EuGH macht der Generalanwalt klar,

700 Ibid., Rn. 107 f., 200 ff.

701 Ibid., Rn. 104, 115, 200 ff.

702 Ibid., Rn. 201.

703 Ibid., Rn. 202.

704 Ibid., Rn. 114.

705 *Pravemann*, GRUR 2019, 783 (786); *F. Hofmann*, NJW 2021, 1905 (1907).

706 s. hierzu und dem Wandel der Rspr. schon oben, → § 2 Rn. 155.

707 GA *Saugmandsgaard Øe*, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat). Hervorhebung hier.

708 Zum Begriff *ibid.*, Rn. 141 ff.

dass diese Gefahr beim Einsatz automatisierter Werkzeuge nicht *per se* gegen die Zulässigkeit automatisierter Filterwerkzeuge spreche,⁷⁰⁹ sondern selbst einer Abwägung der widerstreitenden Interessen (Urheberrecht vs. Meinungsfreiheit der Nutzer⁷¹⁰) zugänglich sei.⁷¹¹ Allerdings müsse das Risiko des *Overblocking* (einschließlich eines möglichen *Overclaiming*⁷¹²) verfahrensmäßig doppelt in die Zange genommen werden: Einmal *ex post*, wie es auch Art. 17 Abs. 9 DSM-RL ausdrücklich vorsieht, indem also gegen Filterungen Rechtsschutz in Form eines internen Beschwerdeverfahrens ermöglicht wird, das rechtsstaatlichen Anforderungen genügt;⁷¹³ zum anderen, so *Saugmandsgaard Øe* weiter, müsse das *Overblocking* schon *ex ante* durch geeignete Maßnahmen angegangen und soweit wie möglich verhindert werden. Denn

„die Existenz solcher [*ex post* wirksamer] Verfahrensgarantien [entbindet] nach der Rechtsprechung des Gerichtshofs und des EGMR die Behörden nicht davon, die *Nebeneffekte* einer Filter- und Sperrmaßnahme [*ex ante*] zu minimieren. Hierbei handelt es sich um verschiedene und *kumulative* Verpflichtungen. [...] Wären [die] Nutzer gezwungen, ihre Rechte systematisch im Beschwerdeverfahren geltend zu machen, würde sehr wahrscheinlich ein Großteil von ihnen davon absehen, weil sie insbesondere nicht über genügend Know-how verfügen, um beurteilen zu können, ob ihre Nutzung dieser Objekte zulässig ist und ob eine solche Beschwerde daher begründet wäre. Ein präventives ‚Overblocking‘ all dieser berechtigten Nutzungen und die systematische Abwälzung der Beweislast auf die Nutzer könnte somit kurz- oder langfristig zu einem ‚Chilling Effect‘ auf die Meinungs- und schöpferische Freiheit führen, was sich in einem Rückgang der Aktivitäten dieser Nutzer niederschlagen würde.“⁷¹⁴

709 Ibid., Rn. 183.

710 Der GA bejaht eine hohe Eingriffsintensität in das Recht auf freie Meinungsäußerung, s. *ibid.*, Rn. 102 ff.: „Vorbeugende Maßnahmen zur Informationskontrolle gelten im Allgemeinen [...] als besonders gravierende Eingriffe in das Recht auf freie Meinungsäußerung, da sie ausüfern können. In einer demokratischen Gesellschaft werden solche vorbeugenden Maßnahmen grundsätzlich abgelehnt, weil sie durch die Einschränkung bestimmter Informationen schon vor deren Verbreitung jede öffentliche Debatte über den Inhalt verhindern und damit die Meinungsfreiheit ihrer eigentlichen Funktion als Motor des Pluralismus berauben. [...] [103] Diese Überlegungen treffen auf das Internet in vollem Umfang zu. [...] Plattformen tragen [...] zu einer Art ‚Demokratisierung‘ der Informationserzeugung bei und sind, obwohl sie von privaten Betreibern verwaltet werden, *de facto* zu wesentlichen Infrastrukturen für die Meinungsäußerung im Internet geworden. Das Recht auf freie Meinungsäußerung umfasst daher beim derzeitigen Stand der Kommunikationsmittel insbesondere die Freiheit, auf diese Plattformen zuzugreifen und sich auf ihnen grundsätzlich ohne Einmischung seitens des Staates zu äußern. [104] Würden die [Betreiber] von staatlicher Seite unmittelbar oder mittelbar dazu verpflichtet, die Inhalte der Nutzer ihrer Dienste generell präventiv zu überwachen und nach rechtswidrigen oder sogar bloß unerwünschten Informationen jeglicher Art zu durchforsten, wäre diese Kommunikationsfreiheit als solche in Frage gestellt. Dann wäre meines Erachtens der ‚Wesensgehalt‘ des in Art. 11 der Charta vorgesehenen Rechts auf freie Meinungsäußerung angetastet.“

711 GA *Saugmandsgaard Øe*, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 183 f.

712 Vgl. *ibid.*, Rn. 148.

713 *Ibid.*, Rn. 178.

714 *Ibid.*, Rn. 181 bzw. 187.

Daraus folge, dass von vornherein

342

„die Fehlerquote so gering wie möglich gehalten werden [müsse]. Deshalb sollte in Fällen, in denen es nach dem derzeitigen Stand der Technik nicht möglich ist, etwa bei bestimmten Arten von Werken und Schutzgegenständen, ein automatisches Filter-Tool zu verwenden, ohne dass dies zu einer nicht vernachlässigbaren Zahl ‚falsch positiver‘ Ergebnisse führt, die Verwendung eines solchen Tools aus meiner Sicht gemäß Art. 17 Abs. 7 ausgeschlossen werden. [...] Um die Gefahr des ‚Overblocking‘ zu minimieren und damit die Achtung des Rechts auf freie Meinungsäußerung zu gewährleisten, kann ein Vermittler meines Erachtens daher nur verpflichtet werden, Informationen zu filtern und zu sperren, deren Rechtswidrigkeit zuvor von einem Richter festgestellt wurde, oder, wenn dies nicht der Fall ist, solche, deren Rechtswidrigkeit sich *ohne Weiteres aufdrängt*, d. h., *offenkundig* ist, ohne dass sie eigens in ihrem Kontext beurteilt werden müssten.“⁷¹⁵

Diese Offenkundigkeit soll dann durch die schon erwähnte, durchaus restriktive 343
Beschränkung der Filterung auf identische oder sinngleiche Uploads erzielt werden.⁷¹⁶ Die genauen technischen Details müssten und dürften zwar Kommission und Mitgliedstaaten näher regeln.⁷¹⁷ Dankenswerterweise schließt der Generalanwalt an seine grundsätzlichen Überlegungen aber konkrete Beispiele an, wie die technische Umsetzung in einer aus seiner Sicht verhältnismäßigen Weise aussehen könnte:

„In der Praxis werden diese Lösungen darin bestehen, dass in die Tools zur Inhaltserkennung Parameter integriert werden, mit deren Hilfe sich das Offenkundige vom Mehrdeutigen unterscheiden lässt. Dies kann je nach Art der Schutzgegenstände und der in Betracht kommenden Ausnahmen variieren. So wird es sich z. B. als notwendig erweisen, die von diesen Tools ermittelten Übereinstimmungsquoten zu berücksichtigen und Schwellenwerte festzulegen, oberhalb deren die automatische Sperrung von Inhalten gerechtfertigt ist und unterhalb deren die Anwendung einer Ausnahme, wie etwa der Zitatschranke, vernünftigerweise in Betracht kommt. Eine solche Lösung könnte mit einem Mechanismus gekoppelt werden, der es den Nutzern erlaubt, zum Zeitpunkt des Hochladens oder unmittelbar danach zu signalisieren (*flagging*), ob für sie nach ihrer Meinung eine Ausnahme oder Beschränkung gilt, woraufhin der betreffende Anbieter den fraglichen Inhalt manuell zu überprüfen hätte, um festzustellen, ob die Anwendung dieser Ausnahme oder Beschränkung offensichtlich ausgeschlossen ist oder im Gegenteil vernünftigerweise in Betracht kommt.“⁷¹⁸

Saugmandsgaard Øe zitiert das deutsche UrhDaG zwar nicht.⁷¹⁹ Dennoch spiegelt 344
sich das Gesetz in durchaus differenzierter Weise in den beispielhaften Ausführungen des Generalanwalts zum *Flagging* gut wider. Dabei ist das Regelungsarrangement des UrhDaG noch komplexer und erinnert ein wenig an ein Ping-Pong-Spiel zwischen den Beteiligten. Und trotz der eben genannten, im Gesetzgebungsverfahren

715 Ibid., Rn. 214 bzw. 198.

716 s. schon *soeben*, → § 2 Rn. 339, a. E.

717 GA *Saugmandsgaard Øe*, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 210.

718 Ibid., Rn. 211.

719 Vgl. aber Fn. 251 der Schlussanträge (*ibid.*) für Hinweise auf Vorarbeiten der Kommission und der Rechtswissenschaft.

ren noch vorgenommenen Schärfungen des Arrangements *zugunsten* der Rechteinhaber finden sich im Schrifttum nach wie vor Stimmen, die von einer Überprivilegierung der Nutzer unter anderem durch die Möglichkeit der „Kennzeichnung als erlaubte Nutzung“ ausgehen.⁷²⁰ Vor diesem Hintergrund muss die Unionsrechtskonformität der UrhDaG hier auch nicht final bewertet werden, gewisse Zweifel bleiben bestehen; insbesondere erscheint die *Flagging*-Möglichkeit, indem sie auf Uploads beschränkt ist, die weniger als 50 % des geschützten Werkes umfassen, angesichts der sehr engen Begriffe von Identität bzw. Sinngleichheit, die der Generalanwalt anlegt, zu restriktiv. Aber zumindest die für uns interessanten Elemente des UrhDaG sind durch die Schlussanträge mit einem gewissen unionalen Konformitätsanschein versehen worden.

- 345 d. *Erhebliche Unstimmigkeiten in der einschlägigen EuGH-Entscheidung*. Der EuGH geht in seinem Urteil auf all die genannten, durchaus komplexen Punkte nicht oder nur oberflächlich ein. In weiten Teilen erschöpft sich das Urteil in einer Nacherzählung des Vortrags der Parteien und einer Paraphrase von Art. 17 DSM-RL. Bei genauem Hinsehen lassen sich allerdings doch für uns relevante Punkte herausfiltern. Die zentrale rechtsdogmatische Frage – ob nämlich vorliegend eine allgemeine oder eine spezifische Überwachungspflicht vorliegt – wird recht knapp damit abgehandelt, Ersteres zu verneinen,⁷²¹ wenn und weil die Verpflichtung zur Filterung sich nur auf von den Rechteinhabern gemeldete Werke beziehe *und* die Diensteanbieter insoweit nicht verpflichtet sein könnten/dürften,

„das Hochladen und die öffentliche Zugänglichmachung von Inhalten zu verhindern, die sie im Hinblick auf die von den Rechteinhabern bereitgestellten Informationen sowie etwaige Ausnahmen und Beschränkungen in Bezug auf das Urheberrecht eigenständig inhaltlich beurteilen müssten, um ihre Rechtswidrigkeit festzustellen.“⁷²²

- 346 Es kann davon ausgegangen werden, dass der EuGH damit das Offenkundigkeitserfordernis, das der Generalanwalt formuliert hat, übernehmen wollte, freilich ohne es vergleichbar deutlich zu formulieren. Es bleibt jedenfalls dabei, dass hier die Spezifität der Überwachung schon dadurch hergestellt ist, dass der Rechteinhaber sein Recht exakt genug benennt, um es ohne eigene Beurteilung der Rechtmäßigkeit, d. h. im Kern: automatisiert durchsetzbar zu machen.

720 Bes. krit. Lennartz/Möllers, GRUR 2021, 1109 (1115 f.). Eine positivere Würdigung findet sich bei F. Hofmann, NJW 2021, 1905 (1908) m. w. N. zum Streitstand.

721 EuGH, Urt. v. 26.4.2022, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 89: „Da die Übermittlung der Informationen [der Rechteinhaber über ihre geschützten Werke] ohne jeden Zweifel die Voraussetzung für die eventuelle Feststellung der Haftung in Bezug auf die Diensteanbieter darstellt, werden diese nämlich ohne diese Informationen nicht dazu veranlasst, dafür zu sorgen, dass die betreffenden Inhalte nicht verfügbar sind.“

722 EuGH, Urt. v. 26.4.2022, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 90.

Im Grunde unergiebig, weil konfus, ist das Urteil sodann im Umgang mit der Gefahr des *Overblocking*. Der durchaus zentrale Begriff fällt im Urteil nicht. Immerhin erkennt der EuGH aber an bzw. übernimmt die allseits geteilte Einschätzung, dass die neue Haftungsregelung des Art. 17 Abs. 4 lit. b und c DSM-RL den Diensteanbietern 347

„*de facto* eine vorherige Kontrolle der Inhalte auferlegt, die Nutzer auf ihre Plattformen hochladen möchten, sofern sie von den Rechteinhabern die in Art. 17 Abs. 4 Buchst. b und c vorgesehenen Informationen oder Hinweise erhalten haben[, wozu sie] in Abhängigkeit von der Zahl der hochgeladenen Dateien und der Art des fraglichen Schutzgegenstands [...] auf Instrumente zur automatischen Erkennung und Filterung zurückzugreifen [hätten].“⁷²³

Die Gefahr eines *Overblocking* lässt sich beim Einsatz solcher Filter nie ganz vermeiden. Doch genau davon *scheint* dann der EuGH im Rahmen der Verhältnismäßigkeitsprüfung auszugehen: 348

„Insoweit ist darauf hinzuweisen, dass Art. 17 Abs. 7 Unterabs. 1 der Richtlinie 2019/790 ausdrücklich klarstellt, dass „[d]ie Zusammenarbeit zwischen den Diensteanbietern für das Teilen von Online-Inhalten und den Rechteinhabern [...] nicht bewirken [darf], dass von Nutzern hochgeladene Werke oder sonstige Schutzgegenstände, bei denen kein Verstoß gegen das Urheberrecht oder verwandte Schutzrechte vorliegt, nicht verfügbar sind, und zwar auch dann, wenn die Nutzung eines Werkes oder sonstigen Schutzgegenstandes im Rahmen einer Ausnahme oder Beschränkung [in Bezug auf diese Rechte] erlaubt ist“. Nach seinem eindeutigen Wortlaut beschränkt sich Art. 17 Abs. 7 Unterabs. 1 der Richtlinie 2019/790, anders als Art. 17 Abs. 4 Buchst. b und Buchst. c letzter Satzteil dieser Richtlinie, nicht darauf, von den Diensteanbietern für das Teilen von Online-Inhalten zu verlangen, dass sie zu diesem Zweck „alle Anstrengungen“ unternehmen, sondern schreibt ein bestimmtes zu erreichendes Ergebnis vor.“⁷²⁴

Und davon abgesetzt subsumiert der EuGH, dass er ja 349

„bereits festgestellt [habe], dass ein Filtersystem, bei dem die Gefahr bestünde, dass es nicht hinreichend zwischen einem unzulässigen Inhalt und einem zulässigen Inhalt unterscheidet, so dass sein Einsatz zur Sperrung von Kommunikationen mit zulässigem Inhalt führen könnte, mit dem in Art. 11 der Charta verbürgten Recht auf freie Meinungsäußerung und Informationsfreiheit unvereinbar wäre und das angemessene Gleichgewicht zwischen ihm und dem Recht des gesetzlichen Eigentums nicht beachten würde.“⁷²⁵

Die hier zitierten Absätze lesen sich *prima facie* so, als wolle der EuGH Filtersysteme bzw. eine Verpflichtung zu deren Nutzung nur zulassen, sofern sie *perfekt* funktionieren, also *keinerlei False Positives* produzieren. 350

Will man dem EuGH eine solch naiv-unrealistische Annahme nicht unterstellen, bleibt entweder die Deutung, er habe durch Postulierung eines unerfüllbaren Maßstabs Polen in der Sache, aber nicht im Tenor Recht geben wollen; oder man wird in 351

723 Ibid., Rn. 53 f.

724 Ibid., Rn. 77 f.

725 Ibid., Rn. 86.

der soeben zitierten Aussage des EuGH den Begriff „hinreichend“ sehr stark gewichten müssen, mit dem Ziel, das zu erwartende *Overblocking* eben doch auch selbst zum Gegenstand einer Abwägung machen zu können – so, wie vom Generalanwalt auch explizit vorgesehen.⁷²⁶ Für letztere Lesart spricht m. E., abgesehen von der Grammatik, alles:

- *erstens* die Vermutung, dass der EuGH nicht faktisch so naiv bzw. rechtspolitisch nicht so unlauter gewesen sein kann, bewusst unerfüllbar hohe Maßstäbe in tatsächlicher Hinsicht zu formulieren;
- *zweitens* der Umstand, dass der EuGH an anderer Stelle im Rahmen der Verhältnismäßigkeitsprüfung es für wichtig und richtig erkannt hat, dass der Unionsgesetzgeber in Art. 17 Abs. 9 DSM-RL die Diensteanbieter dazu verpflichtet, „wirksame und zügige Beschwerde- und Rechtsbehelfsmechanismen zur Verfügung zu stellen“,⁷²⁷ um „das Recht der Nutzer von Diensten für das Teilen von Online-Inhalten auf freie Meinungsäußerung und Informationsfreiheit in den Fällen [zu] schützen, in denen die Anbieter dieser Dienste trotz der Garantien, die in diesen Bestimmungen vorgesehen sind, dennoch irrtümlich oder ohne Grundlage zulässige Inhalte sperren sollten.“⁷²⁸ Nähme man den EuGH bezüglich des Leistungsmaßstabs der Filtersysteme beim Wort (= scheinbar keine *False Positives* zulässig), dürfte es solche Fälle aber gar nicht geben, bzw. sobald eine Beschwerde *ein einziges Mal* wegen Fehlleistung eines Filters begründet wäre, müsste das ganze System sofort offline gestellt werden;
- und schließlich – *drittens* – würde die strenge Auslegung des EuGH von Art. 17 Abs. 7 UAbs. 1 DSM-RL, nähme man den Gerichtshof wirklich beim Wort, sogar dazu führen, dass *menschliche* Kontrollen von Inhalten seitens der Plattform unzulässig würden. Dabei können ja schließlich auch Fehler gemacht werden. Damit entstünde ein erheblicher innerer Widerspruch zu Art. 17 Abs. 4 lit. c 1. Fall DSM-RL (Sperrung/Entfernung eines Inhalts aufgrund eines konkreten „begründeten Hinweises“ eines Rechteinhabers – selbstverständlich kann es auch hier zu *Overblocking* kommen), was ebenfalls darauf schließen lässt, dass der EuGH die Maßstäbe in der Sache nicht ganz so hoch ‚hängen‘ wollte, wie er sie formuliert hat.

352 Die Unzulänglichkeit des Urteils des EuGH ist so massiv, dass viel dafür spricht, sich, was die weitere Ausgestaltung bzw. eine eventuelle Überprüfung der Ausgestaltung in den Mitgliedstaaten anbelangt, an die Schlussanträge des Generalanwalts zu halten. Für uns wichtig sind aber im Folgenden ohnehin nicht die Details der Umsetzung von Art. 17 Abs. 4 DSM-RL, sondern ist vielmehr die grundsätzliche

726 s. soeben, → § 2 Rn. 341.

727 EuGH, Urt. v. 26.4.2022, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 94.

728 Ibid., Rn. 93.

strukturelle Form dessen, was hier als *Justification Structure* eingeführt und für den Bereich der Urheberrechtsdurchsetzung im digitalen Raum erstmals mit dem (mutmaßlichen) Placet der europäischen Gerichtsbarkeit normiert wurde. Auf den grundsätzlich-strukturellen Fragen wird im Weiteren auch wieder der Fokus liegen.

2. Rechtsdogmatisch-konzeptionelle Übertragbarkeit auf andere Rechtsgebiete?

Die Details des UrhDaG und vor allem die Frage nach der Legitimität der Ausgestaltung des Urheberrechts als Ausschließlichkeitsrecht, welche die Debatte um Upload-Filter im Hintergrund stets begleitet hat und weiter begleitet,⁷²⁹ soll also nicht vom Grundsätzlichen ablenken:

a. Konzeptionelle Übertragbarkeit, gestufte Übergänge und Fehlerfolgen. Zunächst ist festzuhalten, dass das Konzept der *Justification Structure* sich auf andere Anwendungsszenarien übertragen lässt, in denen auf eine physisch wirksame Komponente der Rechtsrealisierung nicht verzichtet werden soll, man aber zugleich ein übermäßiges *Overblocking* (im verallgemeinernden Sinne von: zu viele *False Positives*) durch den Einsatz von *Impossibility Structures* sensu stricto vermeiden will.

Man denke an das geläufige, oben schon genannte Beispiel des selbstfahrenden Autos, wo viele Rechtfertigungstatbestände für *prima facie* rechtswidrige Nutzungen auf absehbare Zeit von KI wahrscheinlich nicht erkannt werden können – etwa die Erlaubnis, zur Rettung von Menschenleben eine rote Ampel zu überfahren oder die Geschwindigkeitsregeln zu missachten. Soweit deshalb nicht auf *Impossibility Structures* zurückgegriffen werden soll (was wie gesagt als klassische Abwägungsfrage verarbeitet werden kann⁷³⁰), kommt also immer noch eine *Justification Structure* in Betracht: Die auf Rechtsbefolgung gestellte Software des Fahrzeugs lasse sich also etwa durch Betätigung eines roten Knopfes – ‚Notfall!‘, ‚Rechtfertigung!‘ – übersteuern, aber nur um den Preis, dass sich der die Ausnahme beanspruchende Normadressat zumindest im Nachhinein gegenüber einer Aufsichtsbehörde oder gegenüber einer eventuell geschädigten Person rechtfertigen müsste. Damit würde übrigens auch die Darlegungslast der analogen Welt abgebildet.⁷³¹

Realisiert ist das bislang nicht, die aktuellen Vorschriften zu Fahrzeugen, die noch einen Fahrer im eigentlich Sinn haben (hoch- und vollautomatisierte Fahrfunktionen in der Terminologie von § 1a StVG), verlangen noch zwingend eine Über-

⁷²⁹ Dazu nur Becker, ZUM 2019, 636 ff.

⁷³⁰ Britz/Eifert, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 147.

⁷³¹ Vgl. auch Oster, in: Ahlberg/Götting/Lauber-Rönsberg (Hg.), BeckOK Urheberrecht, 32. Ed. 15.9.2021, § 9 UrhDaG Rn. 9: „Im Urheberrecht muss sich der Nutzer, der sich auf eine Schranke beruft, deren Voraussetzungen nachweisen“, mit dem anschließenden Hinweis, dass eine „mutmaßlich erlaubte Nutzung“ keine Darlegungs- oder gar Beweislastumkehr in einem gerichtlichen Verfahren bewirken solle.

steuerungsmöglichkeit der Technik, ohne dass dies mit einer technischen Rechtfertigungsnotwendigkeit oder -möglichkeit verknüpft wäre.⁷³² Auch hier wäre dann – wie im Fall von § 9 Abs. 2 UrhDaG – eine äußere Grenze, ein ‚doppelter Boden‘ definierbar: Etwa Übersteuerung + Rechtfertigung *ja* im Fall von Geschwindigkeitsübertretungen und sonstigen ‚kleineren‘ Regelverstößen,⁷³³ hingegen *nein*, wenn das Auto ‚erkennt‘, dass es in eine Menschenmenge gelenkt werden soll. Insofern ist auch nochmals der Blick auf § 1e Abs. 2 Nr. 5 StVG zu lenken, der schon heute für Anwendungen des autonomen Fahrens verlangt, dass ein Fahrzeug „ein von der Technischen Aufsicht vorgegebenes Fahrmanöver zu überprüfen und dieses nicht auszuführen [hat], [...] wenn das Fahrmanöver am Verkehr teilnehmende oder unbeteiligte Personen gefährden würde“ – in allen anderen Fällen regelwidrigen Verhaltens hingegen besteht die Übersteuerungsmöglichkeit der Technischen Aufsicht.⁷³⁴

- 357 Neben solchen differenzierenden Übergängen von der *Justification* hin zur *Impossibility Structure* ist noch eine weitere ‚Stellschraube‘ zur Ausgestaltung der Rechtfertigungsstrukturen in den Blick zu nehmen: Die Reaktionsfolgen auf einen *zurückgewiesenen* Rechtfertigungsversuch sind selbst wiederum differenziert gestaltbar. Auch hier liefert das Beispiel des UrhDaG gedankliche Anstöße. Wenn es stimmt, dass – wie Generalanwalt Saugmandsgaard Øe meint – die „Nutzer [von Online-Kommunikationsmitteln wie insbesondere Sharing-Plattformen] nicht über genügend Know-how verfügen, um beurteilen zu können, ob ihre Nutzung [von Werken] zulässig ist“,⁷³⁵ dann erscheint es angemessen, das Rechtfertigungsarrangement hinsichtlich der Rechtsfolgen eher an eine *Compliance Assistance* anzunähern, also z. B. im Fall eines im Ergebnis zurückgewiesenen Rechtfertigungsversuchs einen ‚unvermeidbaren Verbotsirrtum‘ (in der Terminologie des StGB) gesetzlich zu fingieren. Dabei könnte die Zahl solcher ‚Unwissen-schützt-vor-Strafe‘-Fiktionen auch begrenzt werden,⁷³⁶ etwa auf die ersten fünf Uploads oder auf die ersten fünf zurückgewiesenen Kennzeichnungen als erlaubte Nutzung im Sinne des UrhDaG. Die von Saugmandsgaard Øe aus dem von ihm unterstellten rechtlichen Unwissen der Nutzer abgeleiteten *Chilling Effects*⁷³⁷ könnten auf diese Weise skaliert genutzt werden,

732 Art. 6 Abs. 4 lit. d VO (EU) 2019/2144, demzufolge die Daten, die der Datenschreiber von Fahrzeugen über die unionsrechtlich vorgeschriebenen Fahrassistentenfunktionen erstellt, nur für ganz bestimmte Zwecke genutzt werden dürfen (s. oben, → § 2 Rn. 287 f.), spricht zudem dagegen, dass die Mitgliedstaaten eine entsprechende Rechtfertigungsstruktur aktuell verlangen dürfen.

733 Dazu, dass unter den Bedingungen einer optimierten Rechtsdurchsetzung auch viele Normen auf den Prüfstand gehören, die aktuell menschliche Unzulänglichkeit einpreisen und deshalb ‚überschießende‘ Vorgaben machen (so eventuell das Verbot einer roten Fußgängerampel an einer gut einsehbaren Straßenstelle zu einer Zeit ohne jeden Auto-Verkehr), schon → § 2 Rn. 268 ff.).

734 Vgl. auch schon oben, → § 2 Rn. 192 f.

735 GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 187.

736 Der Gedanke findet sich schon bei N. Kuhlmann, in: Fries/Paal (Hg.), Smart Contracts, 2019, S. 117 (123).

737 GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 187.

d. h. könnten zunächst durch Gewährung der Fiktion für einen gewissen Zeitraum abgestellt werden, könnten aber eben auch nach einer gewissen, nachhaltigen Serie von Verstößen durch denselben Nutzer wieder gezielt aktiviert werden, wenn und weil nach einem gewissen Maß an *unterstellt* unbewusster Devianz einem Nutzer zumutbar wäre, sich eben besser zu informieren. Das UrhDaG sieht eine solche *Safe-Harbour*-Wirkung einer „Kennzeichnung als erlaubte Nutzer“ nicht vor,⁷³⁸ sodass auf die allgemeinen Regeln des Zivil- und Strafrechts zurückgegriffen werden muss.

Nur nebenbei sei in diesem Zusammenhang noch bemerkt, dass die Einschätzung 358 des Generalanwalts ein desaströses Urteil über den Zustand des Urheberrechts fällt: Im Grunde sagt *Saugmandsgaard Øe* an der zitierten Stelle, dass das immerhin strafbewehrte Urheberrecht durch seine Erstadressaten nicht mehr verstanden werden kann. Darauf wird noch zurückzukommen sein.⁷³⁹

Die Skalierung der Rechtsfolgen eines zurückgewiesenen Rechtfertigungsversuchs 359 lassen sich weiter treiben: Neben einer *erstens* vollständigen oder zeitlich/dem Umfang nach begrenzten *Safe-Harbour*-Wirkung kann die Folgenseite auf *zweitens* nur zivilrechtliche Konsequenzen, auf *drittens* eine Ahndung ‚nur‘ nach Ordnungswidrigkeitenrecht oder eben *viertens* auch auf strafrechtliche Konsequenzen (eventuell sogar unter Einschluss der Versuchsstrafbarkeit) gerichtet sein. Der rechtspolitisch besonders charmante Nutzen der verstärkten Nutzung von Rechtfertigungsstrukturen würde freilich darin liegen, dank des physisch verstärkten *Compliance*-Drucks – flankiert durch zivil- oder vielleicht auch ordnungsrechtliche Sanktionen – den psychischen Abschreckungseffekt eines immer weiter ausgedehnten (Neben-)Strafrechts nicht mehr zu brauchen.⁷⁴⁰ Es könnte damit endlich zu dem vielfach geforderten, bislang aber nicht realisierten (im Gegenteil!) Rückbau des Strafrechts und der damit verbundenen *Chilling Effects* kommen. Neben dem Urheberrecht wäre hier beispielsweise an das Verkehrsstrafrecht und das Steuerstrafrecht zu denken. Schließlich könnte an allen Stellen des soeben beschriebenen Folgenregimes (weiterhin) menschliches Ermessen ‚verbaut‘ werden, wo das beispielsweise zur Umsetzung von Billigkeits- und Menschlichkeitsaspekten gewünscht wird.

738 Vgl. § 12 Abs. 3 UrhDaG, wonach ein Nutzer nur „[i]m Falle einer geringfügigen Nutzung (§ 10) [...] für die öffentliche Wiedergabe mutmaßlich erlaubter Nutzungen bis zum Abschluss eines Beschwerdeverfahrens nach § 14 urheberrechtlich nicht verantwortlich“ ist; eine Kennzeichnung als erlaubte Nutzung ist keine „geringfügige Nutzung“, s. § 9 Abs. 2 Nr. 3, § 11 UrhDaG.

739 s. unten, → § 4 Rn. 12 f.

740 Zur Diskussion um die „Alternativen im Recht zum Strafrecht“ immer noch aktuell *Haffke*, in: Schünemann (Hg.), FS Roxin, 2001, S. 955 ff. Die dort und generell in der Strafrechtswissenschaft immer wieder aufgeworfene Frage, ob das (sekundäre) Sanktionenrecht überhaupt in der Lage ist, steuernd auf die Adressaten der (primären) Verhaltenspflichten zu wirken, wird hier nicht vertieft, sondern mit *Haffke* dahingehend ‚beantwortet‘, dass „es ersichtlich um empirische Fragen [geht], die verlässlich wohl nur durch ein Sozialexperiment in vivo beantwortet werden können und aus diesem Grund wohl letztlich unbeantwortet bleiben werden.“ Es bleibt m. a. W. bei der Einschätzungsprärogative des Gesetzgebers, vgl. a. a. O., S. 958, 960.

- 360 *b. Anschlussfähigkeit an die Anlassdogmatik des Bundesverfassungsgerichts?* Folgt man der vom Bundesverfassungsgericht postulierten Rechtschaffenheitsvermutung,⁷⁴¹ scheint sich auch vor *Justification Structures* diese normativ-philosophisch grundierte Schranke zu senken, geht es doch gerade um eine mehr oder weniger flächendeckende und anlasslose Abfrage der Rechtschaffenheit der – zum Beispiel – Uploader. Damit scheinen sich gerade *Justification Structures* auch gut überwachungsakzessorisch (und d. h.: *abwehrend*) bewältigen zu lassen.
- 361 Freilich haben sich der EuGH und sein Generalanwalt von der grundsätzlichen Anlassbezogenheit, die das Bundesverfassungsgericht für Rechtschaffenheitsabfragen fordert, mit der Entscheidung zu Art. 17 DSM-RL verabschiedet, mit – wegen der Verankerung der Rechtsprechung im allgemein gültigen Verbot der „allgemeinen Überwachung“ – potentiell erheblicher Breitenwirkung über den sehr spezifischen Sektor der Urheberrechtsdurchsetzung hinaus: Indem die Unionsgerichtsbarkeit nunmehr zentral auf die „Präzision der Nachforschungen“ abstellt, und nicht mehr auf die Menge der Daten oder die Breite der Erhebungsquelle,⁷⁴² ist jedenfalls für den Bereich der Onlinekommunikation die Notwendigkeit eines konkreten Anlasses aufgegeben. Das bloße Benennen eines Rechts, kombiniert mit der faktischen Möglichkeit seiner automatisierten Durchsetzung, stellt jedenfalls keinen konkreten Anlass einer Überwachung dar, der ja über die bloße Inhaberschaft an einem Recht hinausgehen muss, um von einer allgemein-anlasslosen Rechtmäßigkeitskontrolle unterscheidbar zu sein. Begrifflich wird diese wichtige Kategorienverschiebung im Wechsel vom *Notice-and-stay-down*- zum *Notice-and-prevent*-Modell etwas unvollkommen angedeutet: Einmal bezieht sich *Notice* eben auf eine geschehene Rechtsverletzung, das andere Mal auf ein bestehendes Recht *vor* einer eventuellen Verletzung. Auch die Rechtfertigung von anlasslosen Kontrollen, die das Bundesverfassungsgericht vor dem Hintergrund einer besonderen Verantwortlichkeit für gefährträchtiges Verhalten für möglich hält,⁷⁴³ greift im Urheberrecht nicht; es sei denn, man wollte der Nutzung von Sharing-Plattformen durch Uploader generell eine besondere Gefährlichkeit ähnlich der Nutzung eines Kfz im Straßenverkehr zuweisen.
- 362 Statt sich mit der Suche nach Anlässen oder der Konstruktion einer besonderen generellen Gefährlichkeit von Video- und Audiouploads aufzuhalten, findet der Generalanwalt etwas abgesetzt von der Frage nach der (Un-)Zulässigkeit einer allgemeinen Überwachung, nämlich im Rahmen der Angemessenheitsprüfung, schlicht

741 s. oben, → S. 103 ff. Zur Erinnerung: Nach dieser Rspr. haben Bürger einen Anspruch darauf, sich „grundsätzlich fortbewegen zu können, *ohne* dabei beliebig staatlich registriert zu werden, *hinsichtlich* ihrer *Rechtschaffenheit* Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein [...]“ So BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51. Hervorhebung hier.

742 Oder die „Breite des Diagnosefensters“, so Rademacher, AöR 142 (2017), 366 (378).

743 Dazu oben, → § 2 Rn. 106.

gute Gründe für die stärkere Indienststellung der Diensteanbieter zur Durchsetzung des Urheberrechts:

- *erstens* den „großen wirtschaftlichen Schaden, der den Rechteinhabern durch die unerlaubte Veröffentlichung ihrer Werke auf Online-Sharing-Diensten [...] entsteht“;
- *zweitens* die „Tatsache, dass die Rechteinhaber aus denselben Gründen mit Hilfe des Systems der ‚Meldung und Entfernung‘ [*Notice and take down*] nur schwer kontrollieren können, wie ihre Werke auf diesen Diensten genutzt werden“;
- *drittens* die „Schwierigkeiten, auf die sie bei der gerichtlichen Verfolgung der verantwortlichen Nutzer stoßen,“ und
- *viertens* den „Umstand, dass die Überwachungspflichten nur für bestimmte Vermittler gelten[, nämlich solche, die durch] die Förderung der von ihnen bereitgestellten Inhalte einen gewissen Einfluss auf die öffentlich zugänglichen Informationen ausüben[, was] die betreffenden Anbieter in gewissem Maße in die Nähe traditioneller Vermittler wie z. B. Herausgeber“ rücke.⁷⁴⁴

Man darf freilich annehmen, dass diese Gründe schon eine Rolle spielten bei der Auslegung des Begriffs der „allgemeinen Überwachung“, vermerkte der Generalanwalt doch schon in diesem Zusammenhang, dass, 363

„[w]ürde man eine Überwachungspflicht als ‚allgemein‘ qualifizieren, sobald ein Vermittler mit Hilfe von EDV-Tools *de facto* alle von den Nutzern seines Dienstes hochgeladenen Inhalte filtern muss, auch wenn sich die Suche auf konkrete Rechtsverstöße bezieht, [...] dies die bedauerliche Konsequenz [hätte], dass der technologische Fortschritt, der eine solche Filterung möglich macht, ignoriert und dem Unionsgesetzgeber ein wertvolles Instrument zur Eindämmung gewisser Arten von unzulässigen Inhalten aus der Hand genommen würde.“⁷⁴⁵

Auch vor dem Hintergrund der Entscheidung zu Art. 17 Abs. 4 DSM-RL scheint es mir daher plausibel, die weiter oben⁷⁴⁶ bereits angeregte Umstellung der recht engen Anlassdogmatik auf eine allgemeinere *Dogmatik der guten Gründe* in Erwägung zu ziehen. 364

c. Unzulänglichkeit einer bloß überwachungsakzessorischen Bewältigung. Wie dem auch sei, vor allem ist es – wie schon im Fall der *Impossibility Structures* – letztlich ohnehin zu einfach gedacht, bei der rechtlichen Bewältigung von *Justification Structures* allein auf Überwachungsakzessorietät zu setzen; auch hier gilt es, die Unterschiede zur Überwachung zu berücksichtigen: 365

⁷⁴⁴ Alle Zitate in der Aufzählung von GA Saugmandsgaard Øe, Schlussanträge v. 15.7.2021, Rs. C-401/19 (Polen/Parlament und Rat), Rn. 137.

⁷⁴⁵ Ibid., Rn. 113.

⁷⁴⁶ s. oben, → § 2 Rn. 122 ff.

- 366 Der *Chilling Effect*, der dadurch ausgelöst wird, dass sich der Nutzer gegenüber dem Rechteinhaber eventuell direkt rechtfertigen muss (mit allen ungewissen Konsequenzen des oben beschriebenen ‚man weiß ja nie‘ zivil- oder strafrechtlicher Sanktionierung⁷⁴⁷), steht unter der vom Nutzer selbst beherrschten Bedingung, dass er *wetermacht* – trotz des Hinweises auf ein möglicherweise rechtswidriges Upload-Verhalten und der anschließend einsetzenden Dialogisierung des Vorgangs. Der Nutzer hat damit die Möglichkeit, mit seinem *Versuch* rechtswidrigen Handelns davonzukommen; oder, falls er weitermachen möchte, informiert und gewissermaßen mit offenem Visier in die Auseinandersetzung zu treten, dass/ob sich die KI irrt, ein Rechtfertigungsgrund vorliegt, den die KI nicht erkannt hat, oder gar ein neuer Rechtfertigungsgrund – etwa von Verfassungen wegen – geschaffen werden muss.
- 367 Rechtfertigungsstrukturen sind folglich gegenüber dem Bürger anspruchsvoll. Aber die bürgerliche Adressatenstellung im Recht *ist* häufig außerordentlich anspruchsvoll, und eine gelungene (!) *Justification Structure* müsste (!) – ähnlich der *Compliance Assistance Technology* – als wichtigen Baustein eine starke Informationskomponente enthalten,⁷⁴⁸ die dem mit dem automatisierten *prima-facie*-Rechtswidrigkeitsvorwurf konfrontierten Bürger die Möglichkeit gibt abzuschätzen, ob der Vorwurf *in concreto* stimmt oder doch eine Form versuchten automatischen *Overblocking* darstellt. Vor allem aber: *Justification Structures* machen den Bürger im Gegensatz zur Überwachung *nicht* zu einem Objekt staatlicher bzw. staatlich mandatierter beliebiger Beobachtung und anschließender *eventueller* Sanktionierung (woraus eben der berühmte *Chilling Effect* entsteht), sondern geben ihm die Steuerungsmacht über den Vorgang selbst in die Hand. Ganz streng genommen ist für den Bürger mit diesem Arrangement die *Möglichkeit* einer Sanktionierung seines Verhaltens sogar sehr *exakt* vorhersehbar, nämlich von seinem informierten Verhalten abhängig, womit eine der zentralen Rationalitäten der Anlassdogmatik des Bundesverfassungsgerichts sogar erfüllt ist. Ergänzt man das Arrangement um Modellierungen auf der Folgenseite – schwächt also etwa die *Sanktionsdrohung* bewusst durch eine mehr oder weniger begrenzte oder befristete, vorhersehbare *Safe-Harbour*-Wirkung eines Rechtfertigungseinwands ab – stärkt das den dialogischen Charakter der Rechtsbefolgung/-durchsetzung weiter, bzw. schwächt die potentiell unerwünschten *Chilling Effects* weiter ab.
- 368 Freilich, der Bürger ist in eine Struktur eingebunden, die ihm Aufwand bereitet und ihn bzw. seine Handlungen potentiell aus der Anonymität beispielsweise des Online-Kommunikationsverkehrs herausstellen kann. Die soeben angestellten Überlegungen werden daher aus Sicht vieler – so meine Vermutung – nicht geeignet sein, Rechtfertigungsstrukturen *ganz und gar* aus der Überwachungsakzessorietät und

747 s. oben, → § 2 Rn. 255.

748 Vgl. beispielhaft oben, → § 2 Rn. 290.

den damit begründeten verfassungsrechtlichen Beschränkungen herauszuheben. Aber zumindest im Rahmen der allfälligen Abwägung sei bedacht, dass hinreichend gut funktionierende *Justification Structures* sowohl hinsichtlich der *Chilling Effects* als auch hinsichtlich des Ausgeliefertseins des Bürgers an ein staatliche/staatlich mandatierte Beobachtung (= Rechtschaffenheitsabfragen) erhebliche Unterschiede gegenüber Überwachung aufweisen, die nicht übersehen werden sollten.

3. Theoretische Folgerung: Rechtsanwendungsoperation bleibt ein kommunikativer Prozess, allerdings in formalisierter(er) Struktur.

Damit noch einmal weg von den dogmatischen Überlegungen und hin zum theoretisch relevanten Kern der *Justification Structure*: Ihr Proprium gegenüber der *Impossibility Structure* ist es insoweit, dass sie den menschlichen Adressaten einer Norm als bisherigen Erstanwender im Erstzugriff nicht vollständig verdrängt bzw. auf lediglich *ex post* wirksame Beschwerdemechanismen verweist; sondern dass sie den Anwendungsprozess selbst in ein komplexeres, nämlich schon in der ersten Anwendungsoperation *formalisiert dialogisches* Arrangement verwandeln, in dem Erstadressat, Norm-Begünstigter und gegebenenfalls weitere Dritte (z. B. die Plattformen) „in eine Praxis der Verantwortung, Rechtfertigung und Kritik ihrer Anwendungsoperationen eingebettet sind.“⁷⁴⁹

Wohlgemerkt: Klaus Günther hat diesen soeben zitierten, affirmativen Satz zur Beschreibung von *bisheriger* Rechtsanwendung durch *Menschen*, insbesondere Gerichte, bezogen und in Opposition gesetzt zu dem, was Günther als „smarte Ordnung“ (die zumindest *auch Impossibility Structures* nach hiesiger Diktion einschließt⁷⁵⁰) bezeichnet.⁷⁵¹ Ich habe mit der Konzeptionalisierung des im UrhDaG aufgebauten Arrangements als *Justification Structure* beispielhaft versucht zu zeigen, dass „Verantwortung, Rechtfertigung und Kritik“ und die aus diesen Konflikten resultierenden Lernprozesse⁷⁵² dann, wenn Algorithmen nicht als Substitut menschlicher

749 Günther, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (542).

750 Günthers Begriff der smarten Ordnung ist allerdings weiter, s. Günther, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (525): „[...] Ordnungen, die darauf ausgerichtet sind, durch intelligentes Design und mit Hilfe algorithmischer Operationen Abweichungen von ihren Normen zu minimieren oder ganz unmöglich zu machen“. Damit setzt er Dinge gleich (z. B. die hier sog. *Impossibility Structures* mit Anwendungen, die eher dem *Nudging* zuzurechnen sind), die m. E. einer differenzierten Betrachtung wert sind.

751 Ähnl. Hoffmann-Riem, Recht im Sog der digitalen Transformation, 2022, S. 267: „Die [von einer algorithmischen Durchsetzungsmaßnahme Betroffenen] haben keine Chance, vor der Sanktion [gemeint sein dürfte Durchsetzung] Einwände vorzubringen oder Einreden zu erheben – weder gegen die angeblich verletzte Regel noch gegen deren Anwendung im Einzelfall“. Deshalb sei der Einsatz solcher Technologie „Ausdruck einer Machtasymmetrie“.

752 Vgl. Günther, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 523 (547), der freilich davon ausgeht, dass „smarte Ordnungen“ solche „Konflikte mit anderen und daraus resultierende Lernprozesse“ gerade vermeiden würden. Für zwingend halte ich diese Schlussfolgerung, wie dargelegt, nicht.

Rechtsanwendung, sondern als Baustein für Rechtsanwendung in hybriden Interaktionszusammenhängen eingesetzt werden, dass also Verantwortung, Rechtfertigung und Kritik dann sogar gezielter und formalisierter und damit in gewisser Weise ‚besser‘ arrangiert werden können als in rein menschlichen Anwendungsszenarien. Der Unterschied einer *Justification Structure* zum Technologie-freien Status quo ist daher in gewisser Weise (nur), dass sie (die *Justification Structure*) einen *nicht* in Ruhe einen potentiellen Normverstoß begehen lässt, den Adressaten also nicht die Auseinandersetzung mit dem ihm geltenden Recht erspart, aber gleichzeitig auch nicht von vornherein eine bestimmte Auslegung/Anwendung aufzwingt, wie es die *Impossibility Structure* tun würde, sondern ihn zum strukturierten Diskurs *fordert*.

- 371 Schließlich bleibt der Konflikt beim Einsatz von *Justification Structures* je nach konkreter Ausgestaltung gerade auch *in Ansehung* des schon erfolgten Normverstoßes und seiner Folgen möglich. Das Arrangement kann mit anderen Worten so ausgestaltet werden, dass Abweichung möglich bleibt, nur eben keine unerkannte. Damit sei auch ein Urteil von *Christoph Möllers* über den Einsatz von Algorithmen zur Normverwirklichung mindestens ergänzt:

„Eine wichtige Besonderheit von Algorithmen liegt darin, dass ihre Anwendung keinen Raum für Entscheidung kennt. Das bedeutet, dass über Algorithmen keine Kontingenzen oder Streitstände kultiviert werden können.“⁷⁵³

- 372 Das können sie *dann* nicht, wenn man den Algorithmus isoliert und ohne den potentiell hybriden Interaktionszusammenhang in den Blick nimmt, in den Algorithmen zusammen mit Menschen und in Organisationen eingebunden sein können. Ginge es der „Theorie normativer Ordnungen“ also tatsächlich ‚nur‘ um „dieses diskursive Ernstnehmen des Einzelnen – seiner (objektiven oder subjektiven) Infragestellung des [im konkreten Fall:] Strafrechts“, mit dem Ziel „[d]abei kritisch zu prüfen, ob die vormals guten[n] Gründe [für eine Strafnorm immer] noch tragen“,“⁷⁵⁴ dann wären also *Justification Structures* anscheinend der Königsweg, um die Flexibilitätsreserven einer normativen Ordnung zu erhalten, gleichzeitig die Realisierungswahrscheinlichkeit des Rechts insgesamt zu erhöhen. Dass bzw. ob es um mehr als Dialog geht, wird die zentrale Frage von → Kapitel 3 sein.

V. Sonderfall: Preference Assistance Technologies

- 373 Bevor wir ein Zwischenfazit von Kapitel 1 ziehen können, soll am Beispiel sozialer Medien abschließend noch eine weitere Technologie-Kategorie aufgemacht werden,

⁷⁵³ Möllers, Die Möglichkeit der Normen, 2018, S. 471.

⁷⁵⁴ So Burchard, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 553 (577), mit dem Bsp. des strafrechtlichen Verbots homosexuellen Geschlechtsverkehrs, das „nicht zuletzt“ durch Akte der Devianz zu Fall gebracht worden sei.

die m. E. einen Unterfall der *Compliance Assistance Technologies* darstellt: die hier sogenannten *Preference Assistance Technologies*.

Es geht hier nicht um die Durchsetzung staatlich gesetzten Rechts, sondern um 374 die möglichst exakte Realisierung der Präferenzen von Bürgern, im Folgenden im Beispiel konkret: der Nutzer von sozialen Medien. Wir sind damit im Grenzbereich zum Zivilrecht, das ausweislich der einleitenden Bemerkungen zu diesem § 2 nicht unmittelbar Gegenstand unserer Betrachtungen sein soll.⁷⁵⁵ Allerdings scheint mir die These berechtigt, dass individuelle Präferenzen – unter anderem gestützt auf Art. 2 Abs.1 GG – in den vergangenen Jahrzehnten eine Aufwertung zu einem immer dominanteren Maßstab unseres Gesellschaftssystems insgesamt erfahren haben;⁷⁵⁶ die fortschreitende Überformung des Zivilrechts durch die Grundrechte gehört mit dazu, ist Motor und Resultat der Entwicklung.

Die folgenden Ausführungen zu einem konkreten Anwendungsbeispiel sollen diese 375 sehr breite These etwas verständlicher machen und kleinarbeiten. Letztlich scheinen mir die Überlegungen theoretisch auf alle Bereiche übertragbar, in denen individuelle Präferenzen durch rechtliche Aufwertung zu Recht werden können: also theoretisch in allen Fällen subjektiver Rechte. Und auch das ist ein Feld, wo, so unterstelle ich, viele zunächst ein Zu-wenig an Befolgung und Durchsetzung des Rechts diagnostizieren dürften, also ein Zu-viel an Verhaltenskontingenz der – zivilrechtlich gesprochen – Anspruchsgegner. Der geläufige Spruch „Recht haben und Recht bekommen sind zwei Paar Schuhe“ kommt in den Sinn. Dass im Folgenden das Beispiel des individualisierten Medienkonsums herausgegriffen wird, liegt daran, dass hier bereits umfangreiche staatliche Regulierung und Selbstregulierung der Akteure und damit rechtswissenschaftlich verwendbares Anschauungsmaterial existiert, das die Gesamtthese dieses Kapitels stützt, dass neue Technologien Kontingenzerfahrungen immer weiter aus der Rechtsanwendung verdrängen sollen und verdrängen werden.

1. Worum es hier nicht geht: die (eindeutig) dunklen Seiten der Personalisierbarkeit durch künstliche Intelligenz

Vorab einige Worte zum generellen Diskurs um die Regulierung(sbedürftigkeit) 376 sozialer Medien im weiteren Sinn und damit zugleich dazu, worum es hier nicht gehen soll. Es finden sich im rechtswissenschaftlichen Schrifttum mindestens drei eng verflochtene Diskursstränge im Zusammenhang mit sozialen Medien bzw. In-

⁷⁵⁵ s. oben, → § 2 Rn. 4.

⁷⁵⁶ Zur Frage, ob individuelle Wünsche schon als solche – also ohne rechtsförmliche Umsetzung bspw. durch die grundrechtsgestützte Privatautonomie – *Normen* sind, bejahend Möllers, Die Möglichkeit der Normen, 2018, S. 160; anders reine, d. h. nicht *entäußerte* Präferenzen: keine Normen (a. a. O., S. 76 ff.).

ternet-Intermediären⁷⁵⁷ und deren KI-Nutzung,⁷⁵⁸ die sich vor allem in Form von Such-, Priorisierungs- und *Matching*-Algorithmen zeigen. Da die Begrifflichkeiten (Intermediäre, Plattformen, Netzwerke usw.) nicht einheitlich gebraucht werden, seien als soziale Medien und Intermediäre im hier zugrunde gelegten weiten Sinn beispielhaft genannt: Suchmaschinen wie *Google* und soziale Netzwerke wie *Facebook*, Nachrichten-Aggregatoren wie *Google News* und *Facebook News Feed*, Mikro-Blogging-Dienste wie *Twitter* (jetzt *X*), *Instagram* und *TikTok*, sowie Sharing-Plattformen, zuvorderst natürlich *YouTube*.⁷⁵⁹ Beobachtet wird hier übergreifend

- *erstens* die Bildung von – tatsächlich oder vermeintlich – demokratiegefährdenden Echokammern und Filterblasen;⁷⁶⁰
- *zweitens* eine Dynamisierung der individuellen Kommunikation, was nicht nur positiv zu verstehen ist, sondern vielmehr Anlass zu einer dynamisierten (Selbst-)Regulierung geben soll;
- und *drittens*, vor allem aus kartell- und verbraucherschutzrechtlicher Perspektive, eine erhebliche Meinungs- und Steuerungsmacht der Intermediäre,⁷⁶¹ mit Rückwirkungen auf die Dogmatik der (un)mittelbaren Grundrechtsbindung privater Akteure.⁷⁶²

377 Ein gemeinsamer Nenner dieser kritischen Beobachtungen ist die durch den KI-Einsatz der sozialen Medien ermöglichte Personalisierung von Kommunikation bzw. genauer: des Medien- und Kommunikationskonsums. Diese Personalisierung kann exogen motiviert erfolgen, d. h. etwa durch Wahlkämpferinnen, die im Wege des sogenannten *Microtargeting* potentiellen Wählern individualisierte Nachrichten dergestalt zukommen lassen können, dass die Überzeugungswahrscheinlichkeit beson-

⁷⁵⁷ Zum Begriff statt vieler *Paal/Hennemann*, JZ 2017, 641 und ff. m. w. N.

⁷⁵⁸ Zu den sozialen Medien aus einer spezifischen KI-Perspektive *Krönke*, in: Wischmeyer/Rademacher (Hg.), *Regulating Artificial Intelligence*, 2020, S. 145 ff.

⁷⁵⁹ Vgl. *Paal/Hennemann*, JZ 2017, 641. In der Terminologie des Medienstaatsvertrags vom 14-28.4.2020 handelt es sich bei den genannten Anbietern um sog. Medienintermediäre i. S. v. § 2 Abs. 2 Nr. 16: Demnach „ist Medienintermediär jedes Telemedium, das auch journalistisch-redaktionelle Angebote Dritter aggregiert, selektiert und allgemein zugänglich präsentiert, ohne diese zu einem Gesamtangebot zusammenzufassen“. Es gelten dann die §§ 91-96 MStV, für Video-Sharing-Dienste (§ 2 Nr. 22, 23) greifen noch *zusätzlich* §§ 97-99. Abzugrenzen sind Medienintermediäre insb. von den Medienplattformen nach § 2 Abs. 2 Nr. 14, 78-90 MStV. Zu den Definitionen ausf. *Siara*, MMR 2020, 523 ff. Eine eher ökonomisch informierte Terminologie findet sich bei *Krönke*, *Öffentliches Digitalwirtschaftsrecht*, 2020, S. 14 f. Soziologisch zunächst eine zu undifferenzierte Begriffspraxis diagnostizierend und dann entsprechende Vorschläge unterbreitend *Reckwitz*, *Die Gesellschaft der Singularitäten*, 2018, S. 262 ff.

⁷⁶⁰ Dazu insb., auch empirisch, *Schemmel*, *Der Staat* 57 (2018), 501, bes. S. 509 ff. Für Nachw. auch *Martini*, *Blackbox Algorithmus*, 2019, S. 100. *Reckwitz*, *Die Gesellschaft der Singularitäten*, 2018, S. 261, 264 f., spricht in diesem Zusammenhang auch von „digitalen Neogemeinschaften“, die „sich als Kollektive singularisieren“. Hervorhebung im Original.

⁷⁶¹ s. statt vieler *Paal/Heidtke*, ZUM 2020, 230 (231) m. w. N.

⁷⁶² Vgl. in diesem Zusammenhang grundlegend OLG München, Beschl. v. 24.8.2018, Az. 18 W 1294/18 = NJW 2018, 3115 – Hassrede; zum Thema insgesamt statt vieler *Lüdemann*, MMR 2019, 279 ff.

ders hoch sein soll – Stichwort *Cambridge-Analytica*-Skandal.⁷⁶³ Besonders problematisch ist *Microtargeting* wohl (nur) dann, wenn die Personalisierungsmöglichkeiten genutzt werden, um unterschiedlichen Personen je individuell passende, sich aber *widersprechende* Wahlversprechen zukommen zu lassen, was in Richtung eines unlauteren Wettbewerbs und bewusster Täuschung mindestens eines der beiden Adressaten geht.⁷⁶⁴

Um diese je nach Einsatzfeld mehr oder weniger dunkle Seite der exogen motivierten Personalisierung soll es hier *nicht* gehen, sondern am Beispiel des *bewussten*, also endogen motivierten Medienkonsums um die *prima facie* helle Seite: Jeder und jede, so das Versprechen von personalisierenden Medien- und Informationsintermediären an ihre Nutzer, erhält z. B. in den personalisierbaren Newsfeeds von *Facebook* oder *Google News* oder über die Vorschlagsalgorithmen von *Twitter* (jetzt *X*), möglichst genau den Inhalt angezeigt, der seinen bzw. ihren algorithmisch ermittelten Präferenzen am ehesten entspricht – *Cass Sunsteins Daily Me*.⁷⁶⁵ 378

2. Der gesellschaftlich-verfassungsrechtliche Hintergrund von Diensten wie Google News: Präferenzoptimierung als Gebot?

Mit *Google News* soll hier ein solcher Anbieter kurz näher vorgestellt werden. Versucht man, Informationen über die Funktionsweise des Newsfeeds zu erhalten, dann leitet einen der Anbieter von der eigentlichen Nachrichten(aggregations)seite⁷⁶⁶ aus recht intuitiv zu einer mit „*So werden Meldungen für Google News ausgewählt*“⁷⁶⁷ überschriebenen Informationsseite. Dort lässt sich zunächst erfahren, dass *Google News* in bestimmten Bereichen der Seite „[v]on Computern ausgewählt[e]“ Nachrichten für alle Nutzer anhand der Kriterien Sprache und Region anzeigt. In anderen, entsprechend gekennzeichneten Bereichen von *Google News* werden „[p]ersonalisierte Nachrichten“ angezeigt, die „[u]nsere Algorithmen [...] basierend auf den folgenden Faktoren“ auswählen: „Google News-Einstellungen: Ihre Interessen und Quellen“ und „Bisherige Aktivitäten auf Google: Ihre Aktivitäten in Google-Diensten und auf YouTube“. Über einen direkt folgenden Link können Nutzer „Einstellun- 379

763 Die VO (EU) 2024/900 v. 13.3.2024 über die Transparenz und das Targeting politischer Werbung stellt u. a. eine Reaktion auf diese Vorgänge dar; sehr krit. dazu *D. Holznagel*, Verfassungsblog v. 13.3.2023 (Onlinequelle).

764 Dazu auch *Schemmel*, *Der Staat* 57 (2018), 501 (508 f.); zur Manipulation von Kunden, d. h. in einem kommerziellen Bereich, *Ebers*, *MMR* 2018, 423 ff. Einschlägig nun auch Art. 5 Abs. 1 lit. a AI Act.

765 *Sunstein*, #Republic, 2017, S. 1 ff.

766 Google News stellt kein eigenes redaktionelles Angebot dar, sondern sammelt (aggregiert) die Angebote klassischer Online-Medien auf seiner Seite.

767 s. https://support.google.com/googlenews/answer/9005749?hl=de&ref_topic=7688382, besucht am 12.6.2025.

gen ändern und frühere Aktivitäten ansehen“ und auch löschen.⁷⁶⁸ Unter „Inhalte personalisieren“ sind hier gezielte Änderungen möglich, wobei *Google* Folgendes ermöglicht: „Interessen folgen“ und „Interessen nicht mehr folgen“, Meldungen mit „Mag ich“ oder „Mag ich nicht“ bewerten, sowie „Meldungen von einer Quelle ausblenden“. Unter „Meine Google-Aktivitäten“ können selbige nicht nur angezeigt, sondern auch gelöscht und es kann festgelegt werden, welche Aktivitäten getrackt werden. Eine Erläuterung, ob, wie oder gar warum bzw. warum nicht eine *ganz bestimmte* Aktivität die Darstellung von Meldungen in *Google News* beeinflusst hat oder beeinflussen wird, kann – soweit ersichtlich – bislang nicht abgerufen werden.

- 380 Wie wichtig freilich gerade die Auswertung des Nutzerverhaltens für gelungene Personalisierungen ist, hat *Jens Prüfer* am Beispiel der Personalisierung speziell der Suchmaschine von *Google* aufgezeigt: Für häufige Suchanfragen gebe es keine großen Qualitätsunterschiede. Aber:

„je seltener die Anfragen würden, desto schlechter würden Suchmaschinen, die Ergebnisse würden also schlechter, je weniger nutzergenerierte Daten die Suchmaschine zur Verfügung hätte. Das Problem: ‚Diese seltenen und sehr seltenen Suchen machen aber über 70 Prozent der Gesamtanfragen aus.‘ [...] Die Unterschiede in den Ergebnissen hänge ausschließlich an der unterschiedlichen Menge der nutzergenerierten Daten. Wenn ein Anbieter schon viele ähnliche ebenfalls obskure Suchanfragen habe, tue er sich leichter, passende Ergebnisse prominent anzuzeigen.“⁷⁶⁹

- 381 Nun geht es hier nicht darum, das Phänomen personalisierten Medienkonsums und vor allem seiner Konsequenzen *empirisch* zu hinterfragen. Es bleibt umstritten, ob durch Personalisierung z. B. wirklich Echokammern mit demokratieschädlicher Wirkung entstehen,⁷⁷⁰ oder ob die dynamisierte Kommunikation tatsächlich dazu führt, dass diffamierende Inhalte oder Desinformationen schneller, mit größerer Reichweite und stärkerer Wirkung geteilt werden.⁷⁷¹
- 382 Es geht hier vielmehr darum, dass die beschriebene Personalisierung, *wenn* sie endogen motiviert ist, *der Grundidee nach* die perfekte Optimierung eines zentralen Gerechtigkeitsmaßes der gegenwärtigen deutschen und wohl auch europäischen Gesellschaftsordnung ist: der freien individuellen Selbstentfaltung.

768 s. <https://support.google.com/googlenews/answer/7688469?sjid=11490836516901393309-EU>, besucht am 12.6.2025.

769 Zitiert nach *Vöß*, Tagesspiegel Background Digitalisierung & KI v. 13.1.2021; s. auch *Prüfer/Schottmüller*, *Journal of Industrial Econ.* 69 (2021), 967 ff.

770 Dazu *Paal/Heidtke*, *ZUM* 2020, 230 (231); *Schemmel*, *Der Staat* 57 (2018), 501 (507 ff., 509 ff.); jeweils m. w. N.

771 Für eine aktuelle Übersicht über die Empirie s. *Perkowski*, *Desinformationsregulierung* (Manuskript 2025), Kap. 1.B; *Eifert*, in: *Hermstrüwer/Lüdemann* (Hg.), *Der Schutz der Meinungsbildung im digitalen Zeitalter*, 2020, S. 189 (193), spricht von einer bislang nur „anekdotalen Evidenz“ individual- oder gemeinschaftlicher „Kampagnen“ unter Ausnutzung der spezifischen Dynamiken sozialer Medien (s. auch schon in → § 2 Fn. 760). Das soll aber kein unbedingtes Regulierungshindernis sein.

Der selbstbestimmt gestaltete Medienkonsum (und die darüber ermöglichte freie Meinungsbildung) ist ein zentraler Aspekt des von *Andreas Reckwitz* ausgemachten Trends der „Singularisierung“ des spätmodernen Menschen.⁷⁷² Entgegen der in der Rechtswissenschaft nach wie vor vorherrschenden These, dass der Gebrauch von KI-Technologien wegen des heute noch fragmentarischen Charakters künstlich-intelligenter Auswertungen⁷⁷³ zuvorderst, quasi *strukturell*, zu überschießenden *Generalisierungen* führe, beschreibt *Reckwitz* „[d]ie digitalen Technologien [als zentrales Element] einer *allgemeinen Infrastruktur zur Fabrikation von Singularitäten*“.⁷⁷⁴ Denn:

„Dadurch, dass Suchmaschinen und Plattformen wie Google und Facebook Beobachtungsprofile der Nutzer erstellen[, sehen sich d]ie Subjekte [...] einer sozusagen maßgeschneiderten kulturellen Umwelt gegenüber, die versucht, sich so weit wie möglich ihrer aktuellen *Wunsch-Interessen-Struktur anzupassen*“.⁷⁷⁵

Das ist die auch für unsere Zwecke weiterführende Perspektive: eine Perspektive also, die nicht in den vielfältigen Pathologien – jetzt wieder speziell – der Möglichkeiten personalisierten Medienkonsums denkt,⁷⁷⁶ sondern *gute* Funktionalität entlang der eigentlichen *Idee* von Personalisierungstechnologien annimmt.⁷⁷⁷ Voraussetzung dafür ist, dass die Personalisierung nicht nur auf Beobachtung basiert, sondern – insofern über *Reckwitz* hinausgehend – die Personalisierung dem Nutzer mindestens bekannt gemacht, besser noch: zur *eigenen Gestaltung* jenseits des Beobachteten und der daraus gezogenen Schlüsse freigegeben ist. Etwa, indem wie im Beispiel von *Google News* eine Konfiguration der Personalisierung durch gezieltes Löschen und die bewusste Auswahl präferierter oder abgelehnter Themen ermöglicht wird. Die bestehenden Informationsasymmetrien zwischen Nutzern und Personalisierungsanbietern müssen folglich (selbst-)regulatorisch abgebaut werden. Denn zur modernen, grundrechtlich geschützten und damit zu optimierenden Selbstbestimmung gehört – nach Überwindung aller deterministischen Gesellschafts- und Menschenbilder und zumindest nach weit verbreiteter Auffassung – vor allem auch die grundsätzliche Definitionshoheit darüber, was dem Einzelnen das für ihn selbst Optimale ist. Es geht um Selbstoptimierung unter Selbstdefinition des Optimalen. *Wenn* also die genannten Voraussetzungen vorliegen, dann gilt mit *Mario Martini* schlicht:

⁷⁷² *Reckwitz*, Die Gesellschaft der Singularitäten, 2018, S. 9 ff.

⁷⁷³ s. ausf. → § 3 Rn. 46 ff.

⁷⁷⁴ *Reckwitz*, Die Gesellschaft der Singularitäten, 2018, S. 229, Hervorhebung im Original.

⁷⁷⁵ So *ibid.*, S. 258, mit Blick auf *Facebooks News Feed*. Hervorhebung hier. s. auch a. a. O., S. 260: „Diese Singularisierung ist von vornherein *subjektbezogen*: Es wird entlang der besonderen Interessen und Wünsche des Subjekts singularisiert.“ Hervorhebung im Original.

⁷⁷⁶ s. *soeben*, → § 2 Rn. 377.

⁷⁷⁷ Auf dieser Perspektive bauen auch die – freilich vielfach kritisierten – Überlegungen von *Sunstein*, #Republic, 2017 auf: „Machine-learning can be used (and probably is being used) to produce *fine-grained distinctions*“ (S. 4).

„[D]ass sich zahlreiche Nutzer bewusst für personalisierte Angebote entscheiden, ist gerade Ausdruck autonomer Ausübung der Freiheitsgarantien, die die Verfassung unter besonderen Schutz stellt“.⁷⁷⁸

385 Hinzu tritt das pragmatisch-nüchterne Argument, dass eine vernünftige (ergo selbstbestimmte) Nutzung der digitalen Welt ohne Personalisierungsmechanismen und den damit verbundenen „Integrations-, Informations-, Transaktions- und Ordnungsfunktionen“⁷⁷⁹ heute nur noch schwer vorstellbar ist (Personalisierung als „Antwort auf das digitale Aufmerksamkeitsproblem [...], das durch die schiere Masse der Texte und Bilder entsteht“⁷⁸⁰).⁷⁸¹ In sozialwissenschaftlicher Terminologie ist das das „essentielle“ oder „instrumentelle“ Verhältnis von digitaler Technologie zu Freiheit, oder, einfacher ausgedrückt: individuelle *Freiheit* wird *durch die digitalen Technologien* gemehrt oder gar erst erlangt,⁷⁸² wenn es gelingt, die menschliche Freiheit (Autonomie) bei Nutzung der Technologie zu erhalten/zu erreichen.⁷⁸³

386 Das heißt auch: Dem Zufall muss hier nichts mehr überlassen bleiben.

3. Die regulatorisch-einfachrechtliche Ebene: Präferenzoptimierung als Rechtsanspruch

387 Greift das einfache Recht das alles regulatorisch bereits auf? Das Problem ist, dass die geltende Medienregulierung insoweit nicht einfach zu beschreiben ist, da noch nicht ganz klar ist, in welchem Verhältnis die inhaltlich einschlägige nationale Regulierung in Deutschland (also der Medienstaatsvertrag [MStV]) zum neuen unionsrechtlichen Plattformregulierungsrecht im DSA steht.⁷⁸⁴ Die Länder, die den MStV mit dem 5. Medienänderungsstaatsvertrag vom 27. Februar/7. März 2024 bereits an den DSA angepasst haben, gehen bezüglich der uns sogleich interessierenden Normen nicht davon aus, dass Änderungen notwendig sind. Ich beschränke mich im Folgenden auf diese für uns relevanten Aspekte der Regulierung: Transparenz und Nicht-Diskriminierung des Zugangs.

388 *a. Algorithmen-Transparenz für die Nutzer.* Konzeptionell zielt die Plattformregulierung im MStV vor allem darauf ab, die soeben benannten *exogenen* Gefahren

778 Martini, Blackbox Algorithmus, 2019, S. 103.

779 So die überzeugende Strukturierung der Leistungen von Internet-Plattformen und Netzwerken bei Krönke, Öffentliches Digitalwirtschaftsrecht, 2020, S. 16 ff.

780 Reckwitz, Die Gesellschaft der Singularitäten, 2018, S. 289.

781 Paal/Heidtke, ZUM 2020, 230 (231).

782 s. zu den differenzierenden Begriffen von „Freiheit“ in Relation zu Technik ausf. B. Wagner, in: Oswald/Borucki (Hg.), Demokratietheorie im Zeitalter der Frühdigitalisierung, 2020, S. 201 ff. Zum essentialistischen und instrumentellen Freiheitsbegriff a. a. O., S. 203 ff. bzw. 205.

783 Ibid., S. 208 ff.

784 s. ausf. und übersichtlich zum Anpassungsbedarf S. Kuhlmann, ZUM 2023, 170 (171 ff.), zum MStV differenziert ebd., ab S. 175.

sozialer Medien (Manipulation der Nutzer und Marktmacht der Intermediäre) einzuhegen; andersherum formuliert: Es ist das Ziel der Regulierung, den Nutzern die autonome, also möglichst rein *endogen* motivierte Nutzung auch von stark personalisierter Kommunikation in ihrerseits optimierter Weise zu ermöglichen. Zunächst ist in diesem Sinn § 93 MStV über die „Transparenz“ von Medienintermediären⁷⁸⁵ zu nennen. Demnach müssen die Anbieter von Diensten wie *Google News* usw.

„(1) [...] zur Sicherung der Meinungsvielfalt nachfolgende Informationen leicht wahrnehmbar, unmittelbar erreichbar und ständig verfügbar zu halten: 1. die Kriterien, die über den Zugang eines Inhalts zu einem Medienintermediär und über den Verbleib entscheiden, 2. die zentralen Kriterien einer Aggregation, Selektion und Präsentation von Inhalten und ihre Gewichtung einschließlich Informationen über die Funktionsweise der eingesetzten Algorithmen in verständlicher Sprache.

(2) ¹Anbieter von Medienintermediären, die eine thematische Spezialisierung aufweisen, sind dazu verpflichtet, diese Spezialisierung durch die Gestaltung ihres Angebots wahrnehmbar zu machen. ²[...]

(4) Anbieter von Medienintermediären, die soziale Netzwerke anbieten, haben dafür Sorge zu tragen, dass Telemedien im Sinne von § 18 Abs. 3^[786] gekennzeichnet werden.“

Die Norm erhebt unbefangen betrachtet anspruchsvolle Forderungen in Sachen 389 „Transparenz“. Sie scheinen über das, was z. B. *Google News* anbietet, hinauszugehen, jedenfalls dann, wenn Nr. 2 so ausgelegt würde, dass Nutzer eine Information über die *Gewichtung* der Kriterien für *konkrete* Selektionen des Algorithmus im Einzelfall verlangen könnten.⁷⁸⁷ Wie konkret und detailscharf die Transparenzpflichten des Medienstaatsvertrags tatsächlich wirken werden, kann hier offen bleiben.⁷⁸⁸ Wo-

785 s. zum Begriff bei und in → § 2 Fn. 759.

786 § 18 Abs. 3 [Informationspflichten und Auskunftsrechte] lautet „¹Anbieter von Telemedien in sozialen Netzwerken sind verpflichtet, bei mittels eines Computerprogramms automatisiert erstellten Inhalten oder Mitteilungen den Umstand der Automatisierung kenntlich zu machen, sofern das hierfür verwandte Nutzerkonto seinem äußeren Erscheinungsbild nach für die Nutzung durch natürliche Personen bereitgestellt wurde. ²[...]“.

787 Also nicht nur: ‚Dir werden Meldungen über Tiere angezeigt, weil unser Algorithmus errechnet hat, dass Du Dich für Tiere interessierst‘, sondern bspw.: ‚Dir wird diese Reportage über Katzen vorgeschlagen, zu 75 %, weil Du ‚Tiere‘ als Dich interessierende Themen ausgewählt hast, zu 25 %, weil Du vorgestern und gestern Katzenbilder auf der Homepage X geöffnet hast‘.

788 Nach im medienrechtlichen Schrifttum h. M. geht es § 93 MStV *nicht* um konkrete Gewichtungen, die einzelnen Meldungen/Anzeigen zugrunde liegen, vgl. etwa *Cornils*, ZUM 2019, 89 (101 f.): „Der E-MedienStV erlegt den Plattformbetreibern bzw. Medienintermediäranbietern gleichsam ‚abgespeckte‘ Informationspflichten auf: Nicht die einem nicht fachspezialisierten Publikum sowieso nicht zugänglichen informationstechnischen Details (d. h. der Code und die Prozessierungen), wohl aber die maßgebenden ‚Grundsätze‘ (für die Plattform-Angebotsgestaltung) bzw. ‚Kriterien‘ (für den Zugang und die Präsentation zu bzw. durch Intermediäre) der Auswahlentscheidung sollen in ‚leicht erkennbarer Weise‘ bzw. ‚verständlicher Sprache‘ dargelegt werden müssen. Allerdings ist auch die Problemlösungseignung dieser auf das Verstehen-Können der Nutzer ausgerichteten Version von Transparenz, die nun recht eigentlich das Kernstück der neuen Intermediärsregulierung ist, keineswegs zweifelsfrei: Transparenz dieser Art steht unter Vergeblichkeitsverdacht. Sie läuft in das Dilemma, entweder, will sie tatsächlich bindungsstarke Maßstäbe errichten, doch wieder ein hohes Maß kleinteiliger Information über die Prozessierungen einfordern zu müssen, damit aber kaum anders als eine Offenlegung des Algorithmus sowohl die Ver-

möglich ist § 93 MStV angesichts der vielfältigen Transparenzanforderungen, die für Online-Plattformen nach dem DSA gelten, sogar teilweise unanwendbar.⁷⁸⁹ Dessen Artt. 9 bis 12, 14 Abs. 1, 15, 24, 27, 32, 39, und 42 sehen – in unterschiedlicher Intensität – für alle vom DSA erfassten, dort sogenannten Anbieter von Vermittlungsdiensten Transparenzpflichten vor, die auch und gerade den Einsatz algorithmischer Auswahl- und Empfehlungssysteme betreffen (siehe insbesondere Art. 14 Abs. 1, 5, 6 DSA).

- 390 Aber gleichviel, ob nun § 93 MStV oder die genannten DSA-Vorschriften zur Anwendung kommen, für uns ist wichtiger: Die Normen sind letztlich alle ganz der Selbstoptimierbarkeit des eigenen Medienkonsums verpflichtet, indem sie dem und der Einzelnen ermöglichen sollen,

„vielfaltsverengende Tendenzen [zu] erkennen und – z. B. durch die aktive Auswahl anderer Inhalte(-anbieter) – etwaigen Verengungsprozessen [zu] begegnen sowie dem Einschluss in ‚Filterblasen‘ entkommen zu können.“⁷⁹⁰

- 391 Wenn daher gesagt wird bzw. – mit Blick auf die teilweise verdrängende Wirkung des DSA – gesagt wurde, dass die §§ 91 ff. MStV die freie Meinungsbildung *und* -vielfalt im Zeitalter sozialer Medien bewahren sollen, dann muss das jedenfalls für § 93 MStV dahin eingeschränkt werden, dass er dem Individuum nur (aber immerhin) die Möglichkeit gibt, zu erkennen, dass er eventuell „vielfaltsverengenden Tendenzen“ ausgesetzt ist, ihm aber gerade nicht das Recht nimmt, sich diesen bewusst auszusetzen. § 93 MStV ist daher ein verfahrensmäßiger Baustein dessen, was Sunstein als „*architecture of control*“ über den eigenoptimierten Medienkonsum beschrieben hat.⁷⁹¹

- 392 *b. Nicht-diskriminierender Zugang.* Deutlicher und materiell auf Meinungsvielfalt ausgerichtet, nämlich *prima facie* von der „Wunsch-Interessen-Struktur“⁷⁹² des nutzenden Individuums *unabhängig*, ist § 94 MStV konzipiert. Es handele sich dabei, so die Einschätzung im Schrifttum, um den in der Gesetzgebungsphase „am stärksten umstrittene[n] Gegenstand der zukünftigen Medienintermediärsregulierung“.⁷⁹³ Die

pflichteten als auch die Schutzadressaten (und wohl auch die Aufsichtsinstanzen) zu überfordern. Oder sie beschränkt sich auf das Gebot zwar nachvollziehbarer, aber weder besonders informativer (über den jedem halbwegs Interessierten ohnehin zugänglichen Informationsgehalt hinausgehender) Beschreibung allgemeiner Maximen zum Geschäftsmodell und zur Sortierationalität, von denen keine wirklich disziplinierende oder kontrollmaßstabsetzende Wirkung ausgeht. Solche Erklärungspflichten dürften über eine Alibi-Bedeutung kaum hinauskommen.“ Deutlich positiver die Einschätzung und direkte Antwort auf Cornils von Paal/Heidtke, ZUM 2020, 230 (236 f.).

789 So auch m. E. überzeugend S. Kuhlmann, ZUM 2023, 170 (175 f.).

790 Paal/Heidtke, ZUM 2020, 230 (236).

791 Sunstein, #Republic, 2017, S. 1.

792 Reckwitz, Die Gesellschaft der Singularitäten, 2018, S. 258.

793 Paal/Heidtke, ZUM 2020, 230 (237). Dort auch eine Übersicht über die Kritik an § 94 MStV, die sich allerdings v. a. auf Details bezieht, wie zu große Unbestimmtheit oder unzureichenden Schutz wegen der Beschränkung auf journalistisch-redaktionelle Inhalte.

Norm verlangt von Medienintermediären „Diskriminierungsfreiheit“ ihres Angebots und lautet:

„(1) Zur Sicherung der Medienvielfalt dürfen Medienintermediäre journalistisch-redaktionell gestaltete Angebote, auf deren Wahrnehmbarkeit sie besonders hohen Einfluss haben, nicht diskriminieren.

(2) Eine Diskriminierung [i. S. d.] Absatzes 1 liegt vor, wenn ohne sachlich gerechtfertigten Grund von den nach § 93 Abs. 1 bis 3 zu veröffentlichenden Kriterien zugunsten oder zulasten eines bestimmten Angebots systematisch abgewichen wird oder diese Kriterien Angebote unmittelbar oder mittelbar unbillig systematisch behindern. (3) [...]“

Die Vorschrift muss hinsichtlich ihrer regulatorischen Stoßrichtung differenziert betrachtet werden: Halbsatz 1 von § 94 Abs. 2 MStV unterstützt genau besehen lediglich das Transparenzgebot des § 93 MStV, indem er eine Abweichung von den zu offenbarenden Selektionskriterien grundsätzlich für unzulässig erklärt. Man wird sich fragen dürfen, ob diese Anordnung nicht implizit bereits in § 93 Abs. 1 MStV enthalten ist, da es dem Ziel der Transparenz offensichtlich zuwiderliefe, wenn ein Anbieter Selektionskriterien benennen würde, von denen er (bzw. der von ihm verwendete Algorithmus) systematisch abweicht.⁷⁹⁴ Jedenfalls ist es das Ziel der Norm, durch einen „Abbau von Informationsasymmetrien im Verhältnis von Nutzern und Medienintermediären“⁷⁹⁵ die „Nutzerautonomie“⁷⁹⁶ zu optimieren. 393

Spannender ist Halbsatz 2 von § 94 Abs. 2 MStV, wonach Selektionskriterien „journalistisch-redaktionell gestaltete Angebote“ i. S. von Absatz 1 nicht „unmittelbar oder mittelbar unbillig systematisch behindern“ dürfen. Das könnte so verstanden werden, dass diese besonders qualifizierten journalistischen Anbieter einen Anspruch darauf haben,⁷⁹⁷ dass sich auch die *Nutzer* des intermediären Dienstes ihren Inhalten aussetzen lassen müssen, auch wenn sie das nicht wollen. Eine solche Konfrontationspflicht mit unerwünschten Inhalten und Meinungen⁷⁹⁸ ist dem grundrechtlichen Status quo jenseits der pflichtigen Schulzeit⁷⁹⁹ fremd.⁸⁰⁰ Vor allem: „Ein [so konzipiertes] Vielfaltsgebot liefe [...] sowohl dem Geschäftsmodell als auch den 394

⁷⁹⁴ Vgl. – zu Art. 14 DSA – ebenso *Raue*, in: Hofmann/Raue (Hg.), NK-DSA, 2023, Art. 14 Rn. 76.

⁷⁹⁵ *Paal/Heidtke*, ZUM 2020, 230 (234).

⁷⁹⁶ *Ibid.*, S. 236.

⁷⁹⁷ Zur eingeschränkten Durchsetzbarkeit der in § 94 Abs. 1, 2 MStV angeordneten Diskriminierungsfreiheit s. dessen Abs. 3: „Ein Verstoß kann nur von dem betroffenen Anbieter journalistisch-redaktioneller Inhalte bei der zuständigen Landesmedienanstalt geltend gemacht werden. ²In offensichtlichen Fällen kann der Verstoß von der zuständigen Landesmedienanstalt auch von Amts wegen verfolgt werden.“

⁷⁹⁸ Bzw. etwas genauer: Eine Pflicht, die Konfrontation mit unerwünschten Inhalten und abweichenden Meinungen dulden zu müssen.

⁷⁹⁹ Grundlegend *Volkman*, Darf der Staat seine Bürger erziehen? 2012.

⁸⁰⁰ Auch die aus dem überkommenen Rundfunkrecht bekannten *Must-carry*-Pflichten sind bzw. wären anders gelagert als eventuelle Konfrontationspflichten i. R. von Intermediär-Diensten, weil es hier – also im klassischen Rundfunk – eine Personalisierung von vornherein nicht gab, mit *Must-carry*-Pflichten also lediglich ein Angebot ausgestaltet wurde bzw. wird, das der Selbstbestimmung durch die Nutzenden weitestgehend entzogen war (Zuschauer-/Hörer-Kritik lasse ich hier einmal außen vor).

Erwartungen der Nutzer zuwider“.⁸⁰¹ „[M]any people do like echo chambers, and they very much want to live in them“.⁸⁰²

- 395 Tatsächlich dürfte es gerade *nicht* Anliegen von § 94 MStV sein, eine Konfrontationspflicht auf Seiten der Nutzer der Dienste zu begründen; es scheint vielmehr allgemein geteilte Auffassung zu sein, dass die Schutzrichtung der Norm allein gegen die Anbieter der Dienste gerichtet ist,

„indem mithilfe der Vorschrift allfällige Manipulationen an den Such- und Auswahlalgorithmen zum Zwecke der Benachteiligung von Inhalteanbietern vor allem aus ökonomischen und politischen Gründen verhindert sowie auf diese Weise eine unverfälschte Auffindbarkeit und Wahrnehmbarkeit meinungsbildungsrelevanter Inhalte abgesichert werden sollen“.⁸⁰³

- 396 „Verfälscht“ meint also offenkundig *nicht*: ‚verfälscht von den – algorithmisch beobachteten oder menschlich bestimmten – Präferenzen der Nutzer‘, sondern soll nur die Verfälschung durch die wirtschaftlichen oder politischen Interessen der Anbieter ausschließen, die geneigt sein könnten, z. B. unliebsame Berichterstattung über sie selbst oder ihre Werbekunden etc. herauszufiltern bzw. umgekehrt insofern positive Inhalte in den Vordergrund zu spielen.⁸⁰⁴ Wollte § 94 MStV demgegenüber tatsächlich nutzerbezogene Konfrontationspflichten mit *ihr oder ihm* unliebsamen Inhalten statuieren, dann hätte die Regelung angesichts der ihr eigenen, ganz auf die autonome Meinungsbildung der Nutzer bezogenen Grundtendenz der Regulierung (vgl. eben besonders § 93 MStV) das sehr viel deutlicher machen müssen. Kurz: § 94 Abs. 2 MStV dürfte einer Optimierung der Personalisierung von Angeboten *seitens der Nutzer selbst* also nicht im Wege stehen.

- 397 Hinzuweisen ist noch darauf, dass § 94 Abs. 2 MStV auch nicht vom DSA verdrängt wird, da der DSA die „Regulierung der Prinzipien, nach denen bestimmte Angebote – konkret journalistisch-redaktionell gestaltete – ausgesteuert und angezeigt werden dürfen“, nicht adressiert.⁸⁰⁵

- 398 *c. Jeder (s)ein eigener Redakteur?* Um nun wieder das größere Bild in den Blick zu nehmen: Unterstellt man ein gutes Funktionieren der Personalisierungsalgorithmen in Umsetzung der soeben beschriebenen Regulierungskonzepte der Transparenz

801 Martini, Blackbox Algorithmus, 2019, S. 225.

802 Sunstein, #Republic, 2017, S. 5.

803 Paal/Heidtke, ZUM 2020, 230 (234).

804 Vgl. auch Martini, Blackbox Algorithmus, 2019, S. 215.

805 Der Anwendungsbereich des DSA ist demnach schon gar nicht eröffnet, vgl. S. Kuhlmann, ZUM 2023, 170 (176). Allerdings bleibt abzuwarten, wie weit der Anwendungsbereich der nach Art. 14 Abs. 4 DSA eröffneten AGB-Inhaltekontrolle gezogen werden wird; falls sich in deren Anwendung auch sog. *Must-carry*-Pflichten durchsetzen sollten, lägen durchaus auch journalistisch-redaktionelle Inhalte im Anwendungsbereich des DSA (mit entsprechenden Rückwirkungen auf die [Un-]Anwendbarkeit von § 94 MStV), vgl. hierzu knapp Rademacher, in: Hofmann/Raue (Hg.), NK-DSA, 2023, Vor Art. 49 ff. Rn. 15; Raue, ebd., Art. 14 Rn. 72 ff., bes. Rn. 89 zur Beachtung der Medienfreiheit und von Pluralismus.

und Diskriminierungsfreiheit,⁸⁰⁶ dann wird der Mensch, der den Dienst nutzt, sein *eigener* – autonomer – *Redakteur*, wenn und weil eine Optimierung seines Medienkonsums exakt gemäß seinen Präferenzen erfolgt. Wenn das so stimmt, dann sind die Personalisierungsalgorithmen ein Instrument einer medienbezogenen individuellen *“architecture of control”*⁸⁰⁷ und fügen sich damit in den Gerechtigkeitsmaßstab einer möglichst umfassenden Selbstbestimmung bruchlos ein. Auf einer vom konkreten Beispiel abgehobenen Ebene: Der Einzelne wird „Autor des eigenen Lebens“.⁸⁰⁸ Dass wir bzw. vor allem die Anbieter der genannten Dienste so weit (noch) nicht sind, sei hier sofort eingeräumt. Derzeit mag noch viel eher gelten:

„Bei Suchmaschinen und Personalisierungsdiensten ist nicht mehr der Mensch der Redakteur, sondern eine Software, die vom menschlichen Such- und Auswahlverhalten lernt und algorithmisch steuert, wie sie Informationen auswählt, indexiert und dem Nutzer darbietet.“⁸⁰⁹

Aber wie zu Beginn gesagt, will ich im Rahmen dieses Buches eben das Experiment 399 wagen, ein gutes Funktionieren der künstlichen Intelligenz zu unterstellen. Im Fall des Medienkonsums vermittelt Personalisierungsalgorithmen würde das bedeuten, dass „Herrin“ über die Selektionsleistungen der eingesetzten Algorithmen – im Fall erfüllter Transparenz und nutzerseitiger Manipulierbarkeit der maßgeblichen Kriterien, wie es bei *Google News* zumindest in Ansätzen schon der Fall ist – die Nutzerin selbst sein wird. „Der Nutzer lässt [!] Dienste [...] die digitale Welt bewusst nach seinen Kriterien strukturieren.“⁸¹⁰ Dazu würde natürlich gehören, dass diejenigen von uns, die nicht in Echokammern und Filterblasen leben wollen, sondern regelmäßig mit gegenläufigen Thesen und unliebsamen Inhalten konfrontiert werden wollen, ein solches Profil eben auch erzeugen können müssten – das wäre dann ein Algorithmus, der *Sunsteins Opposing View Points Button* oder *Serendipity Button* funktional abbilden und integrieren könnte.⁸¹¹ Art. 38 DSA fordert dies nun, zumindest für die Anbieter von sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen.⁸¹²

Wenn das gelingt, dann wendet sich – gemessen am aktuellen meinungsfreiheits- 400 rechtlichen Gerechtigkeitsmaßstab – die negative oder zumindest warnende Konnotation des folgenden Ausspruchs von *Boris Paal* und *Moritz Hennemann* in eine positive:

806 Unterstellt man also einmal den von *Matthias Cornils* insoweit geäußerten „Vergeblichkeitsverdacht“ als unbegründet, vgl. ZUM 2019, 89 (102).

807 *Sunstein*, #Republic, 2017, S. 1: „What matters is that with the Daily Me [= stark personalisierter Medien- und Informationskonsum], everyone could enjoy an *architecture of control*. Each of us would be fully in charge of what we see and hear.“ Hervorhebung im Original.

808 *Habermas*, Die Zukunft der menschlichen Natur, 2013, S. 54 f., 77.

809 *Martini*, Blackbox Algorithmus, 2019, S. 100.

810 *Ibid.*, S. 225.

811 s. *Sunstein*, #Republic, 2017, S. 232; näher zu diesen Konzepten unten, → § 6 Rn. 65 f.

812 Zur Norm unten, → § 6 Rn. 66.

„Der ‚Herr‘ über den Algorithmus ist somit zu einem guten Teil ‚Herrscher‘ über die Meinungsbildung: Wer den jeweiligen Algorithmus konfiguriert, trifft wesentliche Auswahl- und Wertungsentscheidungen betreffend die angezeigten Informationen und damit (auch) für die in Ansehung der demokratischen Willensbildung zentrale Meinungsbildung.“⁸¹³

- 401 Bei *Paal* und *Hennemann* ist der Herr natürlich noch das den Algorithmus einsetzende private Unternehmen, und das ist intuitiv erkennbar ein Problem.⁸¹⁴ Aber wenn nun die „Herrin“ die Nutzerin selbst wäre, wäre aus (gegenwärtig vorherrschender) grundrechtlicher bzw. regulatorischer Sicht ein durchaus wünschenswerter Zustand eingetreten.⁸¹⁵ Optimierte ist damit zwar nicht die Realisierung *staatlichen* Rechts, aber doch immerhin die *durch staatliches Recht*, nämlich die Grundrechte, gestützte Selbstbestimmung des und der Einzelnen.
- 402 Theoretisch wäre es denkbar, entsprechende *Architectures of Control* oder eben *Preference Assistance Technologies* in vielen, wenn nicht allen Bereichen einzusetzen, in denen Bürgern subjektive Rechte zur eigenen Verfügung zugewiesen sind. Ein weiteres aktuelles Beispiel stellen etwa die sogenannten PIMS dar. Die Abkürzung steht für *Personal Information Management Services* und meint Anwendungen, die es Nutzern erlauben, das datenschutzrechtliche Einwilligungsmanagement auf automatisierte Assistenten mit wählbaren, natürlich jederzeit modifizierbaren Voreinstellungen delegieren zu können.⁸¹⁶
- 403 Das alles zeigt, dass die Versuche, *Compliance Assistance* über die Optimierung des öffentlichen Rechts hinaus auch auf das Zivilrecht zu übertragen, bereits in Gang gekommen sind. Kontingente ist dann immer weniger das Verhalten der Anspruchsgegner, kontingente ist irgendwann nur noch der Wille des Rechtsinhabers – und das scheint, aus einer stark positivistisch betrachteten Perspektive, genau das zu sein, was grundrechtliche Selbstbestimmung und Privatautonomie auch gebieten.

813 *Paal/Hennemann*, JZ 2017, 641.

814 Nicht minder problematisch wäre es, wenn es stimmt, dass der Algorithmus bereits sein eigener Herr wäre, worauf *Martini* in dem Zitat bei → Fn. 809 abstellt. In dieselbe Richtung weist *Martinis* folgende Beobachtung: „Wie wirksam politische Parteien, andere Staaten und Dienstleister Facebook als Plattform zu manipulativen Zwecken nutzen konnten, war dem Konzern nach eigenem Bekunden selbst lange Zeit nicht bewusst. Erst spät reagierte die Unternehmensführung mit inhaltlich-bewertenden Gegenmaßnahmen in ihren Auswahl- und Sortieralgorithmen“, s. *Martini*, Blackbox Algorithmus, 2019, S. 101.

815 Damit ist nicht bestritten, dass man die damit ‚befeuerte‘ Individualisierung oder – in der Terminologie von *Reckwitz* – die Singularisierung auch durchaus kritisch sehen kann; allerdings ist das „auf erfolgreiche Selbstverwirklichung ausgerichtete Lebensführungsmodell“ (*Reckwitz*, Die Gesellschaft der Singularitäten, 2018, S. 431) nach Art. 2 Abs. 1 GG nicht nur zulässig, sondern, i. S. der bekannten „objektiven Werteordnung“, positiv konnotiert und als gesellschaftliches Maß valorisiert. Die krit. Reflexion der gesellschaftlichen ‚Strategie‘ der selbstbestimmten Selbstentfaltung liegt jenseits des Fokus dieser Untersuchung; s. dazu nur ebd., S. 433 f., 440, sowie *Schilling*, Authentizität, 2020, passim, bes. S. 135 ff.

816 Dazu, auch zur gegenwärtig geringen Verbreitung, *Dornis*, ZfPW 8 (2022), 310 (341).

VI. Zwischenfazit I: verminderte Kontingenz durch immer mehr ‚hilfsbereite‘
Maschinen?

„It may be true that the law cannot make a man love me,
but it can keep him from lynching me and [...] that’s pretty important.”

Martin Luther King⁸¹⁷

Die geschilderten Anwendungsbeispiele sind trotz ihrer großen Zahl noch punktu- 404
ell. Die Tendenz aber ist ablesbar: hin zu einem immer häufigeren Einsatz ‚intelli-
genter‘ kommunikations- und aktionsfähiger Systeme, mit dem Ziel, die Rechtsreali-
sierung physisch oder kommunikativ oder durch Mischformen zu optimieren. Des-
halb hat Elisabeth Joh recht, wenn sie darauf hinweist, dass es den Kern der Digitali-
sierung unserer Umwelt verfehlt, die Diskussion um die Zulässigkeit KI-getriebener
Law-Enforcement-Technologien als „Echo“ auf die Überwachungsstaatsdiskussionen
der vergangenen Jahrzehnte⁸¹⁸ zu führen. Wenn man so will, bleibt dieses Echo
in ein neoklassisches *Narrativ der Überwachung* eingespannt (zum Narrativ-Begriff
sogleich, → 1.).

Wie wir gesehen haben, lässt sich die gegenwärtige Erfassung von *Impossibility* 405
Structures – auf die der rechtswissenschaftliche Diskurs bislang fast exklusiv bezogen
ist – als eine ‚überwachungsakzessorische‘ Bewältigungsstrategie beschreiben. Diese
Strategie ist aber darauf angewiesen, dass die Qualifizierung ‚Überwachung‘ weiter-
hin zutrifft. Im Folgenden sollen einige der soeben schon gemachten Andeutungen
dazu, warum diese Beschreibung in Zukunft nicht mehr oder zumindest immer we-
niger passen könnte, zu einer These verdichtet werden: *Es wird immer weniger um
technologische ‚Überwachung‘ gestritten werden, und immer mehr um (unterlassene)
technische Hilfeleistung – mit, so meine Einschätzung, erheblichen Konsequenzen für
die rechtliche Zulässigkeit entsprechender Technologien (mehr/öfter!) und damit wie-
derum für die Kontingenz der Rechtsverwirklichung (weniger/reduzierter)*. Folgender-
maßen möchte ich die These/Einschätzung herleiten:

- Ausgangspunkt ist die Beobachtung, dass wir es phänotypisch bald nicht mehr
mit klassischer Überwachung zu tun haben werden, sondern mit einer jedenfalls
potentiellen *Infrastrukturalisierung der (Möglichkeit zur) Realisierung von Recht*
(dazu → 2.). Mit Joh gesprochen: “as cities become ‘smarter’, they increasingly
embed policing itself into the urban infrastructure.”⁸¹⁹

817 Zitiert nach *Capers*, NYU Law Rev. 94 (2019), 1 (22).

818 Joh, Int. J. Law in Context 26 (2019), 177.

819 Ibid., Hervorhebung hier. Vgl. mit dem Infrastrukturgedanken auch schon Hildebrandt, Smart Technolo-
gies and the End(s) of Law, 2016, S. 11 f., deren Bezugspunkt aber nicht die Infrastrukturalisierung der
(demokratischen) Rechtsdurchsetzung ist, sondern eine privatwirtschaftlich kontrollierte “technological
regulation” mit normativem Anspruch.

- Auf dieser Beobachtung aufbauend soll kurz erläutert werden, warum bzw. inwiefern aus der damit gegebenen *Möglichkeit*, die Rechtsdurchsetzung zu infrastrukturealisieren, in der Tendenz ein *faktischer* Druck folgen wird, die Rechtsdurchsetzung zu infrastrukturealisieren – und damit erheblich zu intensivieren (→ 3.).
- Es wird aber nicht beim faktischen (gesellschaftlich-politischen) Druck bleiben; es wird auch gute *normative* Argumente geben, in der digitalisierten Zukunft Rechtsdurchsetzung(sassistenz) in viel größerem Umfang zuzulassen, vielleicht sogar einzufordern. Der Grund dafür ist, dass wir es in Zukunft mit einem *Wechsel des Narrativs*, bzw. vorsichtiger ausgedrückt: mit einer Narrativ-Ergänzung zu tun bekommen werden: Neben und teilweise anstelle des Überwachungsnarrativs wird das hier sogenannte *Narrativ der Hilfeleistung* treten. Ich greife für diese These – das sei ebenfalls noch vorangestellt – erneut in die Zukunft aus, was die Leistungsfähigkeit ‚intelligenter‘ Systeme anbelangt (zu alledem → 4.).
- Ein Widerspruch gegen einige der insbesondere aus rechtstheoretischer Perspektive vorgetragenen Befürchtungen, die mit der Möglichkeit zunehmend KI-gestützter oder -assistierter Rechtsverwirklichung verbunden sind, schließt diesen § 2 ab (→ 5.).

1. Methodische Vorbemerkung: der Narrativ-Begriff im rechtswissenschaftlichen Gebrauch

- 406 Der ursprünglich literatur-, dann auch kulturwissenschaftliche Begriff des *Narrativs* ist in Mode gekommen und zumindest medial bereits etwas überstrapaziert. Für deutsche *rechtswissenschaftliche* Zwecke wurde er bislang aber noch kaum fruchtbar gemacht.⁸²⁰ Der Begriff scheint mir für unsere Zwecke gut zu passen, weil er rechtspolitische, gerichtliche und literarische Zugänge zur technologischen Überwachung als zusammenhängende und wechselwirksame ‚Erzählung‘ ausweist, welcher – das haben die Analysen oben, ab → S. 103, 166 und 217 gezeigt – hintergründig eine ‚Speicherwirkung‘ für die Lösung verwandter, aber neuer Phänomene (also *Impossibility Structures*) zugeschrieben werden kann.
- 407 Narrative im Recht haben damit mehr als nur einen heuristischen Wert. Konkret: Lässt sich eine Konstellation begrifflich als ‚Überwachung‘ qualifizieren, dann ist damit *mehr* aufgerufen als nur eine einfache, grundrechtlich regelhaft durch Abwägung zu bewältigende Gegenüberstellung von Rechts- und Schutzgütern. Vielmehr wird

820 s. Lomfeld, JZ 2019, 369: „Wie verschiedene Erzählungen über Recht und Gerechtigkeit wiederum die Auslegung und Wahrnehmung rechtlicher Normen und des Rechts insgesamt verändern, ist kaum untersucht.“ Vgl. auch Gephart, in: Pedersen/Ingebrigtsen/Gephart (Hg.), *Narratives in the criminal process*, 2021, S. 7 (8). Für eine ausf. Aufarbeitung des in der US-Rechtswissenschaft durchaus genutzten Terminus und zur Übertragbarkeit auf den dt. Rechtsdiskurs s. Blufarb, in: Fludernik/Schäfer (Hg.), *Erzählen und Recht/Narrative and Law*, 2022, S. 29 ff.; Blufarb, *Geschichten im Recht*, 2017, passim.

eine Erzählung aufgerufen, die bewusst oder unbewusst mit tatsächlichen Erfahrungen (Gestapo, Staatssicherheit, Facebook), literarischen Auseinandersetzungen (George Orwells 1984) und – als Reaktionen darauf – auch mit höchsttrichterlichen Entscheidungen rund um die Massenüberwachung des 20. Jahrhunderts (*Volkszählungsurteil*) verknüpft.⁸²¹ Diese Verknüpfung löst einen erheblichen, durchaus auch rechtlich-dogmatisch *wechselwirksamen* ‚Bias‘ aus; und zwar durch die mehr oder weniger subtile Verstärkung von Abwägungsgewichten, im Fall des Narrativs ‚Überwachung‘ natürlich klar *gegen* die Maßnahme gerichtet. Die Abwägung wird nicht nüchtern erfolgen, wie man annehmen könnte bzw. insinuierten würde, würde man ‚Überwachung‘ nüchtern lediglich als ‚Zweck‘ oder ‚Funktion‘ eines gesetzlichen Arrangements oder einer Ermächtigung ausweisen. Beide Begriffe (Zweck und Funktion) passen natürlich *auch* – aber m. E. reichen sie nicht aus, um die starke Wirkung des Begriffs ‚Überwachung‘ angemessen zu beschreiben.

Erhellend, was die rechtliche Wirkung von Narrativen anbelangt, ist übrigens ein 408
Seitenblick nach Japan: KI und vor allem Robotik sind dort durch populäre, langlaufende Zeichentrickserien (*Astro Boy*, *Doraemon*) anders als in Europa und im anglo-amerikanischen Kulturraum ganz überwiegend positiv konnotiert. Auch in Japan stehen die – mir zugänglichen – entsprechenden Forschungen noch am Anfang, aber es gibt schon erste Überlegungen dazu, ob bzw. dass diese positive Grundeinstellung zu einer insgesamt deutlich technologieaffineren Regulierung und Rechtsprechung beigetragen hat.⁸²²

Da Narrative also auch rechtswissenschaftlich relevant sind, soll *Johs* „Echo der 409
Überwachungsstaatsdiskussion“ nachfolgend als ein *Narrativ der Überwachung* auf den Begriff gebracht werden; und zwar mit dem Ziel, dessen m. E. *geringer* werden-
de Kraft beschreiben zu können. Die Abschwächung, so meine These, wird ausgelöst durch die breite Verfügbarkeit der in diesem § 2 beschriebenen neuen Technologien, die bis zu ihrer *Infrastrukturalisierung* reicht; sukzessive wird dadurch das Narrativ der Überwachung durch ein *Narrativ der Hilfeleistung* verdrängt oder zumindest überlagert, das wiederum – siehe soeben – normative Wirkung entfalten wird. Um

821 s. aus der *Law- & Literature*-Perspektive (und zivilrechtlich geprägt) ebenso *Lomfeld*, JZ 2019, 369 (370): „Literatur und Kunst sind Quellen inhaltlicher wie performativer Inspiration für das Recht. Zur ‚Erfindung‘ rechtlicher Begriffe bedient sich die Rechtswissenschaft bei literarischen Vorlagen. Der Gedanke der ‚Genossenschaft‘ etwa blühte zum stehenden Begriff mit den literarischen Utopien des 19. Jahrhunderts auf. [...] Recht übernimmt Metaphern und füllt sie mit neuem Inhalt. Begriffliche Prägungen wie etwa juristische Person‘ entfalten eine eigene sozial wirkmächtige rechtliche Ästhetik. [N]arrative Jurisprudenz [...] beleuchtet sprachliche und narrative Herkunft wie Bedeutungsumfeld juristischer Begriffe. Die Kontextualisierung legt normative wie kulturelle Hinter-Gründe der Begriffe offen.“ Für Nachw. zur Bedeutung von *George Orwells* 1984 auch für die Rspr. des US Supreme Court s. *Capers*, NYU Law Rev. 94 (2019), 1 (44), dort Fn. 229. Allg. zur Einordnung des Rückgriffs auf Dystopien *Posner*, Law and literature, 2009, S. 393 ff.

822 s. *Lintvedt*, The Digital Constitutionalist v. 5.5.2023 (Onlinequelle); kulturwissenschaftlich zum Phänomen *Wagner*, Robotopia Nipponica, 2013, passim. Herzlichen Dank an *Osamu Nishigami* für viele fruchtbare Diskussionen und Recherchehilfe zu diesen Fragen!

diesen Wechsel und seine Wirkungen wird es in diesem Zwischenfazit vor allem gehen.

2. Ausgangspunkt: Infrastrukturalisierung der (Möglichkeit zur) Rechtsanwendung

- 410 Ausgangspunkt für die hier zu entwickelnde These ist die Beobachtung und Prognose, dass unsere Umwelt eine zunehmend ‚smarte‘, d. h. unter Einsatz von Technologien der künstlichen Intelligenz digitalisierte und digital vernetzte Infrastruktur erhalten bzw. in Teilen sogar *sein* wird. *Artificial Intelligence of Things* (AIoT), *Ambient Intelligence* (AmI)⁸²³ oder digitaler Zwilling/*Smart Dust*⁸²⁴ sind Stichworte hierzu. Oder, mit *Andreas Reckwitz* gesprochen: „Technik ist immer weniger ein Werkzeug, sondern wird immer mehr zu einer technologischen Umwelt, in der sich die Subjekte bewegen“.⁸²⁵
- 411 Man muss dafür gar nicht an die kompletten *Smart Cities*⁸²⁶ in Toronto (gescheitert⁸²⁷), bei Tokyo, in Dubai⁸²⁸ und Saudi Arabien⁸²⁹ (jeweils im Bau) denken, wo Staaten und/oder private Anbieter ganze Stadteile und Städte als vollvernetzte Strukturen neu errichten woll(t)en. Von der ökonomisch und zunehmend auch ökologisch getriebenen Steigerung der Effizienz unserer Lebensräume sind vielmehr auch die alten Räume und Infrastrukturen erfasst:
- *Öffentliche Räume (Stadt, Land, Verkehr)*: neben optischer auch akustische,⁸³⁰ sogar geruchsbasierte⁸³¹ Erfassung des öffentlichen Raums; Automatisierung des

823 *Hildebrandt*, *Smart Technologies and the End(s) of Law*, 2016, S. 8.

824 *Smart Dust* beschreibt Sensoren, die so klein sind, dass sie praktisch überall, auch in der Luft, ausgebracht werden können. Die Technik wurde bereits in den 1990er Jahren erwähnt, befindet sich aber nach wie vor im experimentellen Stadium, s. etwa *Geißler*, *BigData Insider* v. 2.1.2023 (Onlinequelle).

825 *Reckwitz*, *Die Gesellschaft der Singularitäten*, 2018, S. 237.

826 Allg. zum Konzept der *Smart City* *While/Marvin/Kovacik*, *UrbanStudies* 58 (2021), 769 ff.; *Albino/Berardi/Dangelico*, *Journal of Urban Technology* 22 (2015), 3 ff. Für Deutschland grundlegend *Bundesinstitut für Bau-, Stadt- und Raumforschung*, *Smart City Charta*, Mai 2017 (Onlinequelle). Eine aktuelle Projekt-Übersicht findet sich hier: <https://www.smart-city-dialog.de/ueber-uns/modellprojekte-smart-cities>, besucht am 13.6.2025. Krit., wegen der mit der Technologisierung der Stadt möglichen Abkehr vom baurechtlichen Leitbild der funktionengetrennten Stadt, *Sinder*, *Die Verwaltung* 54 (2021), 157 ff.

827 Zu den Kontroversen *Artyushina*, *Telematics and Informatics* 55 (2020), 101456 ff.

828 Der District 2020 als Nachnutzung der Expo 2020 in Dubai ist als *Smart City* konzipiert, hierzu *G. V. Müller*, *NZZ* v. 29.11.2021 (Onlinequelle).

829 Dazu *Alshuwaihat/Aina/Binsaedan*, *Heliyon* 8 (2022), e11138; *Al-sayed et al.*, *PO* 13 (2022), 15.

830 Zu Überlegungen einer Erfassung von bestimmten Geräuschen (z. B. Hilferufen, Stürzen, Schüssen) s. www.axis.com/de-de/solutions/sound-detection, besucht am 13.6.2025; für die USA und die dortige Nutzung entsprechender Sensorik im öff. Raum sehr krit. *Goodman*, *UIC John Marshall Law Rev.* 54 (2021), 797 ff.; s. auch schon *Rademacher*, in: *Wischmeyer/Rademacher* (Hg.), *Regulating Artificial Intelligence*, 2020, S. 225 Rn. 10. Aus dem dt. Recht kann wieder auf § 44 PolG BaWü verwiesen werden, der bereits Tonaufnahmen im öffentlichen Raum zulässt (→ § 2 Rn. 22 f.). Allerdings ist die in Abs. 4 der Norm enthaltene Ermächtigung zur „automatischen Auswertung“ auf die „angefertigten Bildaufzeichnungen“ beschränkt.

831 Zu ersten Erfolgen *Michalowski*, *MIT News* v. 18.10.2021 (Onlinequelle).

Verkehrsmanagements⁸³² und – durch selbstfahrende Kraftfahrzeuge, autonome Drohnen etc. – Automatisierung des Personen- und Warenlieferverkehrs selbst;⁸³³ Digitalisierung und Vernetzung der Elektrizitätsinfrastruktur (*Smart Metering*),⁸³⁴ einschließlich der Digitalisierung und Automatisierung der städtischen Beleuchtung;⁸³⁵ Digitalisierung und Vernetzung der Wasserversorgung;⁸³⁶ Automatisierung an den Grenzen;⁸³⁷ Automatisierung und Optimierung der Landwirtschaft durch vielschichtige Vernetzung verschiedener IoT-Systeme (Landwirtschaft 4.0);⁸³⁸

- *Semi-öffentliche und private Räume*: Einzug von Industrie-, Haushalts- und Serviceassistenten bis hin zu humanoiden Fabrik- und Haushaltsrobotern;⁸³⁹ Digitalisierung und Automatisierung des privaten und kommerziellen Gebäudemanagements (*Smart Homes* und *Smart Facility Management*),⁸⁴⁰ Digitalisierung und Automatisierung von Arbeitsplätzen und -prozessen (*Smart Industry*),⁸⁴¹ einschließlich von Inspektions- und Wartungsarbeiten (*Smart Maintenance*);⁸⁴² smarte Selbstbedienungsgeschäfte in den USA, die das Verhalten des Kunden (Einkauf) automatisiert erkennen, bepreisen und abrechnen können⁸⁴³ (mittlerweile gibt es auch Test-Filialen in Deutschland⁸⁴⁴); vorsichtige, aber fortschreitende Automatisierung sogar im Gesundheitswesen.⁸⁴⁵

832 Vgl. *Tischbirek*, ZfDR 2021, 307 (311 ff.) m. w. N. zu weiteren Forschungsvorhaben.

833 Zu den schon frühen Plänen der Intel-Töchter *Mobiley* zur Einführung von „Robotaxis“ in Deutschland s. *dpa*, Automobil Industrie v. 5. 1.2023 (Onlinequelle); zu Drohnen *A. Williams*, NY Times v. 23.5.2020 (Onlinequelle).

834 Die Idee, die Energieversorgung ‚smart‘ zu gestalten, hat in Deutschland bereits eine lange Geschichte, scheiterte bislang aber relativ verlässlich u. a. an Datenschutzbedenken; vgl. hierzu schon *Guckelberger*, DÖV 2012, 613 ff.; zur Frage, inwieweit auch Fernzugriffsrechte Teil einer smarten Energieinfrastruktur sein können/sein dürfen, *Paulus/Matzke*, NJW 2018, 1905 ff.; aktuell und weiterführend *Diestelmeier/Cappelli*, EuCML 2023, 15. Eine Übersicht über mögliche KI-Einsatzfelder in der Energiewirtschaft liefert *Fritz*, in: Bruhn/Hadwich (Hg.), Künstliche Intelligenz im Dienstleistungsmanagement, 2021, S. 449.

835 *Figuerola*, San Diego Union-Tribune v. 23.12.2019 (Onlinequelle).

836 s. für eine Übersicht *Fu et al.*, Water Research 223 (2022), 118973 ff.

837 Einige Bekanntheit hat die Anwendung *iBorderCtrl* erhalten, die unter Nutzung von Gesichtserkennungssoftware als eine Art von Lügendetektor bei der Einreise fungieren soll; vgl. hierzu *Stoklas*, ZD-Aktuell 2018, 6363.

838 Vgl. *Bayer*, COMPUTERWOCHE v. 21.7.2020 (Onlinequelle).

839 Auch hier forciert von *Elon Musk*, s. für diese – freilich wieder zu vollmundige – Ankündigung aus dem Jahr 2021 *dpa*, F.A.Z. v. 23.8.2021, S. 20. Hierzu ausf. schon ab → S. 150.

840 Für eine bes. eindrückliche, wenn auch noch fiktionale Illustration *Hildebrandt*, Smart Technologies and the End(s) of Law, 2016, S. 1.

841 *Hunziker*, F.A.Z. v. 3.9.2021, S. 1 I.

842 Zum Konzept z. B. <https://alegerglobal.com/augmented-reality/anwendungsbereiche/smart-maintenance/>, besucht am 13.6.2025.

843 Z. B. *Amazon-Go*-Märkte und *Whole-Foods*-Märkte; zum Konzept *Petersdorff*, F.A.Z. v. 9.2.2022 (Onlinequelle). *Beer*, heise online v. 6.12.2016 (Onlinequelle); zur Entwicklung auch *Fuchs*, t3n Magazin v. 26.1.2018 (Onlinequelle). Zur Markteinführung in Europa *Smolka*, F.A.Z. v. 19.7.2022, S. 21.

844 *Spehr*, F.A.Z. v. 14.3.2023, S. T 1.

845 Z. B. Erstdiagnose durch Telemedizinangebote oder Unterstützung ärztlicher, vor allem radiologischer Diagnosen durch Bilderkennung; zum Einsatz robotischer Systeme schon *Orzechowski*, Healthcare Digital v. 29.7.2021 (Onlinequelle).

- *Vor allem anderen Kommunikation: Personal-Assistants* und KI-Agenten (AI Agents) auch jenseits des persönlichen Umfelds, Digitalisierung eines Großteils der menschlichen Kommunikation durch *Messenger*-Dienste, Online-Foren und -Plattformen, digitale Telefonie und Videokonferenzen,⁸⁴⁶ vielleicht sogar irgendwann Holographie, mit den oben⁸⁴⁷ bereits besprochenen vielfältigen Möglichkeiten der Kommunikationsüberwachung und gegebenenfalls unmittelbaren -steuerung.⁸⁴⁸ Außerdem hier zugehörig: die Digitalisierung städtischer und privater Dienstleistungen durch Online-Serviceportale,⁸⁴⁹ schließlich auch alle Aktionen im sogenannten *Metaverse*,⁸⁵⁰ die *per se* innerhalb einer virtuellen und damit digitalisierten Infrastruktur erfolgen werden (die Relevanz des Metaverse scheint derzeit, d. h. Stand 2025, aber wieder fraglich zu sein).

412 Diese lange, aber ganz bestimmt nicht vollständige Liste soll zeigen, dass hinter den oben ausführlicher geschilderten Anwendungsbeispielen automatisierter Rechtsrealisierung (und/oder automatisierter Assistenz zur Rechtsrealisierung) ein noch weit aus größeres ‚Reservoir‘ an ganz oder teilweise automatisierten Tätigkeiten und autonomen Strukturen liegt, die in den kommenden Jahren und Jahrzehnten in immer ‚smartere‘ Städte, Haushalte und Arbeitsplätze integriert werden. Diese Technik wird ebenfalls als ‚Trägerin‘ intelligenter Rechtserkenntnis- und Rechtsdurchsetzungsmechanismen in den genannten Abstufungen bereitstehen. *Smart-city*-Fähigkeiten in diesem anspruchsvoll-umfassenden Sinn können daher treffend als *Dual-use*-Technologien beschrieben werden.⁸⁵¹ Sie steigern nicht nur ökonomische und ökologische Effizienz (oder schlicht Bequemlichkeit) der Nutzer und Bewohner, sondern bieten zugleich eine Struktur zur Steigerung der Rechtstreue von kommunikativer *Compliance*-Assistenz bis hin zu physischer Bewirkung des Gesollten/Verunmöglichung des Verbotenen.

413 All diese die Umwelt neu mitkonstituierenden Technologien dienen freilich zunächst ökonomischen und meist privaten Zielen und jedenfalls nicht *per se* der Ermöglichung der Realisierung staatlichen Rechts. Der Unterschied ist wichtig, weil er die

846 Beispielhaft dazu M. Koch, heise online v. 20.8.2021 (Onlinequelle).

847 s. die ab → S. 99 genannten Anwendungen.

848 Zusätzlich kann auch noch auf die von der EU-Kommission zwischenzeitlich geplante Kommunikationsüberwachung zur Erkennung von Kinderpornographie hingewiesen werden, hierzu *EU-Kommission*, COM(2022) 209 final v. 11.5.2022, bes. Art. 4 des Entwurfs für eine VO zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern; zur Diskussion in den USA Cullen et al., *Laws* 2020, 9, 28. Drängend dürfte alsbald die Bekämpfung von betrügerischer Kommunikation unter Nutzung von *Deepfakes* werden. Die Kennzeichnungspflicht für *Deepfakes* nach Art. 50 AI Act könnte bald Gegenstand einer Diskussion um ihre möglichst weitgehende Absicherung durch *Impossibility Structures* werden. Zu *Deepfakes* schon in → Fn. 68 (Einleitung).

849 Für ein positives Bsp. Heath, How Estonia became an e-government powerhouse, *TechRepublic* v. 19.2.2019 (Onlinequelle).

850 Grundlegend Ball, Framework for the Metaverse, www.matthewball.vc/all/forwardtothemetaverseprimer, besucht am 9.9.2021. Für den dt. Rechtskreis einführend Kaulartz/Schmid, *RiD* 2022, 521 ff.

851 So Joh, *Int. J. Law in Context* 26 (2019), 177 (180).

Einführungsschwelle, die für *staatliche* Überwachungs- und Rechtsdurchsetzungstechnik im engen Sinn greift, *zunächst* einmal beseitigt.⁸⁵² Vielfach wird die Nutzung der Systeme *selbst* auf der – mehr oder weniger autonomen – Einwilligung der Nutzenden beruhen. Die entscheidende Frage hier ist nun: *Wird, darf* oder *soll* die Technologie zugleich als Trägerin von Rechtsdurchsetzungstechnologien genutzt *werden*, sobald und weil sie als Trägerin solcher Technologien genutzt werden *kann*?

3. Macht: zur (neuen) Möglichkeit ihrer Realisierung

Gestellt ist damit zunächst die *machtsoziologische* Frage, ob es nämlich Anhaltspunkte dafür gibt, dass die neuen Mittel der physischen Durchsetzung von Recht genutzt *werden* (werden). Es spricht einiges dafür, die Frage mit ja zu beantworten. Anknüpfend an *Luhmann*⁸⁵³ hat unter anderem *Ralf Poscher* herausgearbeitet, dass der moderne Staat Macht – im ursprünglichen Sinn von physisch wirksamer Gewalt – zur Durchsetzung von Recht nicht nur deshalb zurückhaltend einsetzt, weil er dadurch die Rechtsgüter der Adressaten der Machtausübung schont.⁸⁵⁴ Vielmehr war physischer Machteinsatz immer eine Frage knapper Ressourcen.⁸⁵⁵

852 Vgl. auch *Britz/Eifert*, in: Voßkuhle/Eifert/Möllers (Hg.), *GVwR I*, 3/2022, § 26 Rn. 147.

853 *Luhmann*, *Macht*, 2012, bei *Poscher* zitiert in der Originalausgabe von 1975.

854 Zu weit geht mir insofern *Möllers*, *Die Möglichkeit der Normen*, 2018, S. 451, wenn er unter Rekurs auf eine (freilich noch mehr zugespitzte) Aussage von *Hannah Arendt* formuliert, dass „[e]tablierte Herrschaftsordnungen [deshalb] gut beraten [seien], [eine] gewaltsame Durchsetzung [ihrer Normen] zu vermeiden, [weil] Gewaltanwendung [...] jenseits aller moralischen Einwände [indiziere], dass die Kosten der Norm, um deren Durchsetzung es geht, zu hoch sind.“ Das würde das Opfer einer Straftat sicherlich anders sehen, zumal es in solchen Situationen geradezu moralisch (und auch staatstheoretisch) geboten sein kann, Gewalt zur Verteidigung zu üben.

855 Eine weitere Ergänzung liefert die rechtshistorische Forschung zum Einsatz von Gewalt. Hierzu *Schlumbohm*, *Geschichte und Gesellschaft* 23 (1997), 647 (656 f.): „Bei der Kriminaljustiz z. B. bestand das Problem nicht allein darin, daß die Kräfte fehlten, alle Delinquenten [...] zu fassen. Auch die [...] Verhafteten wurden längst nicht immer nach der Schärfe des Gesetzes abgeurteilt. In Paris griff die Polizei Jahr für Jahr Hunderte von Männern wegen homosexueller Handlungen | auf; doch im ganzen 18. Jahrhundert wurde kaum ein Dutzend Fälle [...] vor einem ordentlichen Gericht verhandelt, wo die Todesstrafe drohte [...]. Die allermeisten ‚Delinquenten‘ ließ die Polizei ohne weitere Sanktionen nach einigen Tagen wieder frei. In den Kriminalakten eines deutschen Kleinstaats heißt es um 1770 über die Sanktionen, welche die Edikte gegen sog. ‚Zigeuner‘ vorsahen: ‚Es ist ... bekannt, daß sie mehr zum Schrecken als im Ernst und in der Absicht, sie also buchstäblich zu vollziehen, gegeben worden und daß sie daher nirgends in Teutschland zur wirklichen Ausübung gekommen‘. Auch die [...] Vermutung, daß die Zentrale gar nicht von allen Unzulänglichkeiten wissen konnte, die sich bei der Umsetzung ihres Gesetzesgebots auf lokaler Ebene zeigten, kann nicht voll befriedigen. Denn nicht wenige von diesen Abweichungen kamen zur Kenntnis der Regierung, und die Folge war keineswegs immer der verstärkte Impuls, dem obrigkeitlichen Wort Gehorsam zu verschaffen. Oft akzeptierte die Zentrale die entgegenstehende Praxis, indem sie deren Konsequenzen mildernd regelte. So läßt sich verschiedentlich beobachten, daß der Verstoß gegen gesetzlich zwingend vorgeschriebene Verfahrensregelungen nicht mit Ungültigkeit des Rechtsaktes bestraft, sondern umgekehrt die Beachtung durch Anreize prämiert wurde, z. B. durch einen privilegierten Status für formgerechte Ansprüche. Gelegentlich wiesen landesherrliche Reskripte die zuständigen Richter explizit an, bei der Durchführung bestimmter strafbewehrter Ordnungen ‚die Billigkeit‘ der ‚Schärfe‘ des Gesetzes vorzuziehen.“ *Schlumbohm* weist allerdings auch darauf hin, dass Gesetze in der (frühen) Neuzeit einen symbolischen Wert als Selbstproklamationen moralisch guter Herrschaft hatten (vgl. schon oben, in → Fn. 554).

„Macht lässt sich als Medium beschreiben, mit dem Gesellschaften ihre Komplexität bewältigen. [...] Moderne Gesellschaften benötigen in diesem Sinne mehr Macht als einfachere, weniger komplexe Gesellschaftsformen. Dem steigenden Machtbedarf kann aber nur durch die Potentialisierung von Machtausübung genügt werden. [...] Alle Macht auszuüben, würde den Machthaber überanstrengen. Moderne Gesellschaften müssen sich so organisieren, daß die Machtmittel und Sanktionen, die ihren Machthabern zur Verfügung stehen, nur in verschwindend wenigen Fällen eingesetzt werden. Dies gilt besonders für den Einsatz physischer Gewalt als zwar universell einsetzbarer und zentralisierbarer, aber politisch prekärer und ökonomisch kostbarer Machtgrundlage. Vor diesem machtsociologischen Hintergrund versteht sich, daß das Rechtssystem einen Mechanismus entwickeln mußte, der den Einsatz der staatlich monopolisierten physischen Gewalt weitgehend vermeidet.“⁸⁵⁶

- 415 Diesen Mechanismus sieht *Poscher* im jeweils rechtsgebietsspezifischen Vollstreckungsverfahren, das auf den zu vollstreckenden Titel folgt bzw. diesen jedenfalls in der Regel überhaupt erst einmal voraussetzt:

„Im Regelfall^[857] kann [gemeint ist wohl: darf] die Vollstreckung nicht gleich an den Erkenntnisakt anknüpfen. Mit Androhung, Fristsetzung und Festsetzung ist das Gesetz bemüht, alle kommunikativen Möglichkeiten zu nutzen, die Anwendung physischer Gewalt zu umgehen, und auf Einsicht und ‚freiwillige‘ Umsetzung des Verwaltungsakts durch den Bürger zu setzen, die eine Aktualisierung staatlicher Macht vermeiden. Die Retardierungen dienen sicher auch dem möglichst schonenden Umgang mit den Rechtsgütern des der Vollstreckung unterworfenen Bürgers und im Vergleich zu dem von Retardierungen weitgehend freien zivilprozessualen Vollstreckungsrecht der Kompensation des fehlenden gerichtlichen Erkenntnisverfahrens. Sie lassen sich aber auch als Illustration dafür lesen, wie sehr Staatsmacht auf Potentialität setzt und angewiesen ist.“⁸⁵⁸

- 416 Die wachsende Verfügbarkeit von *Impossibility* und *Justification Structures* verändert die Vorzeichen für *diesen* soziologisch-faktischen Grund für den Verzicht auf physische Wirkung.
- 417 Aus einer demokratischen Steuerungsperspektive scheint die Konsequenz dann einfach: Wenn die technologisch getriebene Infrastrukturalisierung dem Recht eine neue physisch wirksame Widerständigkeit und Durchsetzungskraft gibt, dann ist das der Idee demokratischer Steuerung nicht *per se* fremd, sich das auch zu Nutze zu machen – bislang hat noch niemand gefordert, dass es *leicht* sein müsse, gegen Recht verstoßen zu können.

856 *Poscher*, VerwArch 89 (1998), III, bes. S.117. Ähnl. auch *Waldhoff*, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR II, 2022, § 44 Rn. 75 m. w. N.

857 s. zum sofortigen Vollzug *Poscher*, VerwArch 89 (1998), III (130).

858 *Ibid.*, S. 117 f. Ähnl., sogar noch weitergehend formuliert *Luhmann*, Kontingenz und Recht, 2013, S. 93 f.: Notwendigkeit der „Virtualisierung von Gewalt“. Zur Frage, ob eine effektive Rechtsordnung ganz ohne den Einsatz von physisch und ggf. psychisch wirkendem Zwang denkbar ist, *Raz*, in: ders. (Hg.), The Authority of Law, 2009, S. 233 (245 f.); *Klement*, in: Hilbert/Rauber (Hg.), Warum befolgen wir Recht? 2019, S. 227 (230 ff.); *Potacs*, in: Bezemek/Ladavac (Hg.), The Force of Law Reaffirmed, 2016, S. 121 ff. Zur Verschmelzung des Rechtsbegriffs mit dem Zwangsmoment unter einer freiheitlich-rechtsstaatlichen Verfassung *Ha. Hofmann*, in: Brandt (Hg.), Rechtsphilosophie der Aufklärung, 1982, S. 12 (27 ff.).

Dabei gilt es zu beachten, dass die oben genannten Mittel physischer Machtausübung in Form von *Impossibility* und *Justification Structures* durch zunächst private Technologien mediatisiert sind und sein werden. Alles andere – also ein unmittelbar staatliches Konstrukt – ist auf absehbare Zeit und in größerem Umfang nicht realistisch. Auch die informatorisch arbeitenden *Compliance Assistance Technologies* i. e. S. sind mit Ausnahme von NINA private Anwendungen, die freilich teilweise staatlich mandatiert sind.⁸⁵⁹ Aus der Perspektive demokratischer Herrschaft ist es legitimatorisch relevant, wenn der eigentliche, soll heißen physische Machteffekt von privater Hand erfolgt bzw. wenn rechtsrelevante Informationen durch privates Design übermittelt werden.

Eine grundlegend neue bzw. problematische Privatisierung der Rechtsdurchsetzung ist das freilich dennoch nicht.⁸⁶⁰ Dieser – gerade im Zusammenhang mit den beschriebenen Upload-Filtern – vielfach erhobene Vorwurf übersieht, dass sich der demokratische Rechtsstaat schon immer Privater als – in der Terminologie von Michael Pawlik zu § 323c StGB – „Verwaltungshelfer“ bedient, um Recht zu realisieren; im Fall von § 323c StGB sogar sachbereichsunspezifisch. Das darf, so wird zutreffend für den Bereich der Rechtsdurchsetzung speziell durch Online-Plattformen argumentiert, aber erst recht sachbereichsspezifisch gelten, wenn Private durch die Bereitstellung und Kontrolle der Infrastruktur, vermittels derer die Rechtsverletzung begangen wird, einen kausalen Beitrag dazu leisten.⁸⁶¹ Auch Rechtsanwälte als klassische ‚Assistenten‘ der Rechtsermittlung und -vermittlung sind zuallererst Private ohne originäre demokratische Legitimation – freilich sind sie immerhin standesrechtlich reguliert.

Äquivalente Arrangements ließen sich auch für solche privaten Instanzen andenken, die *Compliance Assistance Technologies/Structures* ins Werk setzen sollen/dürfen, gegebenenfalls ergänzt um interne, den staatlichen Gerichten vorgeschaltete Streit-schlichtungsmechanismen. Zu fordern sind also situativ angepasste Arrangements, welche die fehlende personelle Legitimation dieser mediatisierten Ausübung von Staatsgewalt kompensieren können und die die jeweiligen Angriffslasten („Aktionslasten“⁸⁶²) und Angriffsanreize gegen die mediatisierte Herrschaftsausübung so ‚einstellen‘,⁸⁶³ dass *per saldo* ein ausgewogenes Verhältnis zwischen primärem Realisierungswunsch, damit verbundener Fehlertoleranz und der theoretischen Verfügbarkeit und tatsächlichen Wahrscheinlichkeit korrigierenden staatlichen Rechtsschutzes

859 s. dafür bspw. oben, → § 2 Rn. 284.

860 Dazu schon oben, bei den Details zu den *Impossibility Structures*, → § 2 Rn. 248.

861 Zutreffend gegen den Einwand der unzulässigen Privatisierung der Rechtsanwendung z. B. Eifert, NJW 2017, 1450 (1451); F. Hofmann, GRUR 2019, 1219 (1223); Raue, JZ 2018, 961 ff.; jeweils m. w. N.

862 Specht, GRUR 2019, 253 (259).

863 Vgl. dazu auch Becker, ZUM 2019, 636 (640 f.) m. w. N.

geschaffen ist, der eine öffentlich-rechtlich legitimierte Letztentscheidung und damit Verantwortungsübernahme ermöglicht.⁸⁶⁴

421 Dabei muss es natürlich auch um die technische Frage gehen, ob und wie sich rechtliche Regeln in maschinell nachvollziehbare Befehle übersetzen lassen. *Denga, Pohle* und *Hölzel* schlagen deshalb vor, anknüpfend an systemtheoretische Konzeptionen, dieses Doppel-Phänomen als „doppelte Delegation“ zu fassen: vom Staat auf Private und vom Recht in die Logik des technisch Machbaren.⁸⁶⁵ Staatliche Verantwortungsübernahme ohne Vorgaben an die Verlässlichkeit und Bestreitbarkeit maschineller Rechtsdurchsetzung(sassistentz) ist in der Tat nicht denkbar. Die ausführliche Diskussion um den Einsatz von Upload-Filtern zur Realisierung des Urheberrechts und das im Anschluss geschaffene, differenzierte Regime des UrhDaG stehen als Vorbild für den Versuch, ein in diesem Sinn doppelt (d. h. Delegation auf Technik und Delegation auf Private berücksichtigendes) ausgewogenes Realisierungsregime zu schaffen.⁸⁶⁶ Um die generalisierungsfähigen Anforderungen an solche Arrangements wird es zentral in → Kapitel 2 gehen. Unterstellen wir für den Moment weiterhin, dass die Arrangements gut genug funktionieren.

422 Das erlaubt es, wieder zurückzukommen auf die machtssoziologisch-faktische Frage: Bezieht man Private im großen Stil als Verwaltungshelfer ein, dann lassen digitalisiert-physisch wirksame Mechanismen der Rechtsrealisierung erstmals (und noch in Ansätzen) ein ‚ideales Recht‘ im kantischen Sinn möglich erscheinen. ‚Ideal‘ in dem Sinne, dass dieses Recht auch in der Lage wäre – wie es in dem berühmten Diktum heißt –, „ein Volk von Teufeln“ zur geordneten Staatlichkeit zu verhelfen. *Kant*, in der Interpretation von *Marcus Willaschek* gelesen:

„Der Grund dafür ist[, dass] es im Recht, anders als in der Ethik, nicht auf die Motive des Verhaltens ankommen darf, sondern allein auf die faktische, erzwingbare Rechtskonformität. Kants Ergebnis im § E lautet daher, dass das Recht nicht nur (gleichsam unter anderen) mit einer Befugnis zu zwingen verbunden ist, sondern: ‚Recht und Befugnis zu zwingen bedeuten [...] einerlei‘ (6:232) | Dieses Ergebnis hat eine überraschende Konsequenz: Wenn das einzig legitime Mittel zur Rechtsdurchsetzung der von Kant so genannte ‚äußere Zwang‘ ist, dann müsste eine vollständige Verwirklichung der Idee des Rechts darin bestehen, den angedrohten bzw. angewendeten Zwang genau so zu bemessen, dass Rechtsübertretungen *ausgeschlossen* sind. Und tatsächlich vergleicht Kant die Handlungen der Menschen in einem idealen Rechtssystem wiederholt mit der ‚freien Bewegung der Körper unter dem Gesetz der Gleichheit der Wirkung und Gegenwirkung‘ (z.B. 6:232). Das bedeutet, dass die Möglichkeit freier Handlungen durch

864 Vgl. statt vieler *Raue*, JZ 2018, 961 (962); s. dazu auch unten, bei → § 4 Rn. 87.

865 *Denga/Pohle/Hölzel*, RW 11 (2020), 420 ff. Die Autoren beziehen allerdings die erste Delegation (von Staat auf Private) in ihrer Definition nur auf die *Regelsetzung* durch Private (a. a. O., S. 423); hier könnte man sogar weiter fassen, weil auch dann, wenn der Staat selbst noch die Regeln setzt, diese im Zweifel durch die Technik privater Akteure umgesetzt werden müssen.

866 Dazu oben, → S. 205 ff.

„wechselseitigen Zwang“ auf die rechtlich erlaubten Handlungen beschränkt ist; ein Rechtsbruch wäre ebenso ausgeschlossen wie eine Wirkung ohne gleichgroße Gegenwirkung.“⁸⁶⁷

Aber, so Willaschek weiter: „dass es ein solches Rechtssystem empirisch nicht gibt und nie geben wird, würde wohl auch Kant nicht bestreiten.“⁸⁶⁸ Soll heißen: ganz abgesehen von der Frage, ob es normativ *wünschenswert* wäre, ein solch ‚ideales‘ Rechtssystem zu schaffen, es *geht* nicht.

Aber: Wird dieses auch und gerade in der rechtlichen Diskussion immer wieder referenzierte⁸⁶⁹ faktische ‚Nie‘ eines solchen ‚Rechtssystems für Teufel‘ prekär – was eben durch die Verfügbarkeit rechtsrealisierender Technologien wenigstens diskutabel wird –, dann wird die Diskussion viel stärker als zuvor auf die *normativen* Gründe dafür verlagert werden (müssen), Rechtsübertretungen doch nicht auszuschließen, *obwohl* man es *könnte*.⁸⁷⁰

4. Schutz: vom Überwachungs- zum Hilfeleistungsnarrativ

Wir sind kein Volk von Teufeln. Das ist *prima facie* die einfache *normative* Begründung dafür, warum Recht im Sinn von Kommunikation als Steuerungsinstrument *grundsätzlich* reichen kann und reichen muss. Dass die Rechtsumsetzung damit kontingent ist, etwas subjektiv Zufälliges besitzt, ist in Kauf zu nehmen.

Ins Verfassungsdogmatische überführt: Weil wir kein Volk von Teufeln sind (sondern auf der ethisch-moralischen Appellebene erreichbar, die Kant aus seiner Bestimmung eines ‚idealen‘ Rechts ja herausgefiltert hat⁸⁷¹), reiche grundsätzlich die Kommunikation des Gesollten aus. Die für ein umfassendes Zwangsregime im Sinn des Kant’schen idealen Rechts erforderliche, voraufgehende Überwachung⁸⁷² sei folglich nicht erforderlich, jedenfalls nicht verhältnismäßig.⁸⁷³ Dass damit zwangsläufig Lücken und Retardierungen im – gegebenenfalls dann ja doch einmal erforderlichen – Vollzug von Recht eintreten, ist notwendige und bewusst in Kauf genommene Konsequenz aus dem ‚vorgeschossenen‘ Vertrauen in die Rechtschaffenheit der

867 Willaschek, in: Gerhardt (Hg.), Kant im Streit der Fakultäten, 2008, S. 188 (194); zur Staatsphilosophie von Fichte s. Waechter, Sicherheit und Freiheit in der Rechtsphilosophie, 2016, S. 70: „Aus diesem Widerspruch heraus lässt Fichte den Staat entstehen. Beide Beteiligten [Bürger] müssten sich den gegenseitigen Angriff unmöglich machen.“

868 Willaschek, in: Gerhardt (Hg.), Kant im Streit der Fakultäten, 2008, S. 188 (202).

869 Vgl. neben Poscher u. a. auch Pawlik, Normbestätigung und Identitätsbalance, 2017, S. 36: „Dies würde allerdings nicht nur die bürgerliche Freiheit zerstören, sondern auch die organisatorischen Kapazitäten des Staates bei Weitem überfordern; dieser würde an seinem Überwachungshunger buchstäblich ersticken.“

870 So auch Britz/Eifert, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 144.

871 Vgl. ausf. Willaschek, in: Gerhardt (Hg.), Kant im Streit der Fakultäten, 2008, S. 188 ff.

872 Statt vieler Pawlik, Normbestätigung und Identitätsbalance, 2017, S. 36.

873 Präzise Britz/Eifert, in: Voßkuhle/Eifert/Möllers (Hg.), GVwR I, ³2022, § 26 Rn. 146 f. m. w. N.; ebenso, vor dem Hintergrund strafrechtlicher Theoriebildung, Burchard, JRE 27 (2019), 527 (550).

Bürger, d. h. ist aus einer Steuerungsperspektive Konsequenz des Vertrauens auf den Erfolg der Kommunikation des Gesollten.

- 427 Wenn man dieser Argumentation folgt, fällt man auf die Anlassdogmatik des Bundesverfassungsgerichts⁸⁷⁴ zurück, deren rechtsphilosophisches Kernpostulat es ja gerade ist, dass der Einzelne einen Anspruch darauf hat, nicht ständig ohne Anlass Rechtfertigung über die eigene Rechtschaffenheit ablegen zu müssen.⁸⁷⁵ Er hat mit anderen Worten ein Recht darauf, dass ihm vorbehaltlich anderer Erkenntnisse Vertrauen und nicht Misstrauen (= Überwachung) entgegengebracht werde.⁸⁷⁶ Damit könnte die Geschichte rechtlich-dogmatisch zu Ende erzählt sein. Ich meine, sie ist es nicht.
- 428 a. *Von der Überwachung zur Hilfeleistung: ein Wechsel des Narrativs.* Wir haben zu Beginn dieses Abschnitts von *Elisabeth Joh* gelesen, dass es dem Phänomen der Infrastrukturalisierung rechtserkenntnis- und rechtsdurchsetzungsfähiger Technologien nicht gerecht werden würde, sie mit dem „Echo“ des Überwachungsnarrativs zu erfassen. Ich schließe mich dem an. Denn ‚Überwachung‘ und damit auch das damit verbundene hier sogenannte *Überwachungsnarrativ* passen auf eine Welt infrastrukturalisierter Rechtsdurchsetzungsmöglichkeiten nicht mehr (→ aa.). Stattdessen werden wir es sehr viel häufiger mit Situationen zu tun haben, die sich im hier sogenannten *Hilfeleistungsnarrativ* abspielen werden (→ bb.). Dieser Narrativwechsel ist rechtsdogmatisch bedeutsam (→ cc.).
- 429 aa. *Warum ‚Überwachung‘ begrifflich immer seltener passen wird.* Der Begriff Überwachung passt nicht mehr bzw. passt immer weniger, weil ‚Überwachung‘ etwas *Hinzutretendes* impliziert, ein bewusstes *Hinschauen* zunächst ohne konkreten Anlass,⁸⁷⁷ in dem sich das Misstrauen oder doch wenigstens die Erwartung ausdrückt, der Überwachte werde oder könnte etwas tun oder unterlassen, das die Überwachung erst *ex post* betrachtet rechtfertigen *könnte* – es ist diese Reihenfolge des Geschehens, die den Vorwurf vom „Generalverdacht“⁸⁷⁸ oder auch vom Fortschreiten des „Prädiktionsstaats“⁸⁷⁹ evoziert.

874 s. ausf. oben, → § 2 Rn. 82 ff. Auch zur Alternative einer Umstellung auf *Gründe*.

875 BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15 = BVerfGE 150, 244 – Kennzeichenkontrollen II, Rn. 51.

876 Zur Bedeutung von ‚Vertrauen‘ als Grundlage der Rspr. auch schon oben, → § 2 Rn. 97, sowie nochmals ausf. unten, → S. 422 ff. Die von z. B. *Burchard*, JRE 27 (2019), 527 (551 f.), aus Art. 1 Abs. 1 GG abgeleitete Fundierung des Rechtssystems im Grundsatz eines (vorgeschossenen, kontrafaktisch zu gewährenden) Vertrauens in die rechtliche Rechtschaffenheit der Bürger erscheint damit also bereits verfassungsdogmatisch realisiert. Ähnl. auch *Rostalski*, GA 166 (2019), 481 (486), die allerdings weniger normativ als hegelianisch mit der natürlichen Vernunftbegabung des Menschen argumentiert.

877 Zu Anlässen für eine im Rechtssinn verhältnismäßige Überwachung → § 2 Rn. 105 ff.

878 Vgl. *Burchard*, in: Forst/Günther (Hg.), *Normative Ordnungen*, 2021, S. 553 (565), wo *Burchard* gerade die Möglichkeiten neuer Technologien zur flächendeckenden Überwachung i. S. hat, und wo der Begriff des Generalverdachts zumindest eher passt als bei punktuellen Maßnahmen anlassloser Überwachung.

879 Vgl. v. a. *Volkman*, NVwZ 2021, 1408 (114) m. w. N.

Das Bundesverfassungsgericht hatte in seinem Beschluss zu den automatisierten Kennzeichenkontrollen als idealisierten Startpunkt eine sozusagen leere und freie Welt vor sich, in der jeder und jede tun und lassen kann, was er bzw. sie möchte. In diese Freiheit tritt die staatliche Beobachtung von außen hinein, mit einer hemmenden Wirkung auch auf rechtmäßiges Verhalten der Überwachten (so die verfassungsgerichtliche These). Und deshalb ist die Überwachung nach überkommener Auffassung auch besonders rechtfertigungsbedürftig und zumindest in Deutschland und Europa engen Grenzen unterworfen. Diese Abfolge zeichnet staatliche *Überwachungsmaßnahmen* generell aus. Nur nebenbei sei hier angemerkt, dass die Abfolge natürlich unreal ist: Genauso wenig, wie es in unserer hochverdichteten Gesellschaft sinnvollerweise eine vorrechtliche Freiheit geben kann, so wenig gibt es eine leere Welt ohne – wenigstens *sozial-gesellschaftliche* – Kontrolle.

bb. Warum wir stattdessen häufiger im hier sog. Hilfeleistungsnarrativ agieren werden. Diese Abfolge wird sich in Zukunft aber ändern: Denn durch die Infrastruktur-Werbung von rechtserkenntnis- und rechtsdurchsetzungsfähigen Technologien wird das zur Hilfeleistung Fähige in Zukunft immer häufiger *schon da sein*. Damit kehren sich die Vorzeichen um:

Wie schon die polizeirechtlichen Generalklauseln für Fälle der *erkannten Gefahr*⁸⁸⁰ – in Abgrenzung zu den besonderen Ermächtigungen für informationelle Maßnahmen *im Vorfeld* der *erkannten Gefahr* – und wie vor allem § 323c StGB aus dem Jedermann geltenden Recht exemplarisch verdeutlichen,⁸⁸¹ ist dieses Schon-Da-Sein, wenn ein Rechtsverstoß zu geschehen droht, ein (narrativ) hoch bedeutsamer Vorgang: Es ist der Unterschied zwischen *grundsätzlich* unzulässiger, *spezifisch* begründungsbedürftiger Überwachung einerseits und *grundsätzlich* zu leistender (Not-)Hilfe andererseits, deren *Unterlassung* stattdessen guter Gründe bedarf. Oder, knapper gesagt: Es ist der Unterschied zwischen Hinschauen und Wegschauen.

Eine Folgefrage ist dann, im Fall *welcher* Rechtsbrüche dieses Wegschauen gesellschaftlich so unerträglich ist, dass eine *Rechtspflicht* zur Hilfe angeordnet werden soll. In der Manuskriptversion dieses Buches hatte ich es mir an dieser Stelle leicht gemacht und geschrieben, dass *grundsätzlich* jeder Verstoß gegen individual- und drittschützende Normen ausreichen könnte/müsste, um das Hilfeleistungsnarrativ zu aktivieren; und dass lediglich offen sei, wie mit Verstößen gegen solche, wegen

880 Zur möglichen Reduzierung des polizeilichen Ermessens hin zur Pflicht zum Einschreiten zum Schutz individueller Rechtsgüter (Ermessensreduzierung auf null) s. statt aller *Graulich*, in: Bäcker/Denninger/Graulich (Hg.), PolR-HdB, 72021, Abschnitt E Rn. 114 ff.; dort auch zum Verhältnis zu privatrechtlichem Rechtsschutz.

881 Zu dieser Norm und der Frage nach der Übertragbarkeit der darin enthaltenen allg. Pflicht zur Hilfe im Unglücksfall auf robotische Haushalts- und Servicehilfen oben, → § 2 Rn. 216 ff.

der Subjektivierungstendenzen des Unionsrechts⁸⁸² freilich immer seltener werden, Normen umzugehen sein werde, die wirklich *nur* Gemeinwohlüter schützen. Ralf Poscher danke ich für den Hinweis, dass ich es mir damit allzu leicht gemacht hatte. Wäre, so gab er sinngemäß zu bedenken, § 323c StGB denn genauso weit ausgreifend formuliert worden, wenn der Gesetzgeber/die Gesellschaft eine Welt vor Augen gehabt hätte, in der „umfassende effektive Hilfe gegenüber jedem Rechtsbruch erfolgen könnte“? Die kritische Nachfrage hilft mir, etwas genauer zu sein und ein Missverständnis zu vermeiden: Keineswegs *müsste* eine *technikrechtliche* Entsprechung zu § 323c StGB genau dessen Konturen haben.⁸⁸³ Es gibt gute Gründe, hier einerseits *mehr* Einsatz zu verlangen (die Unzumutbarkeitsschwelle dürfte für technische Systeme beispielsweise viel höher liegen als im Fall eines hilfeleistungsfähigen Menschen⁸⁸⁴), andererseits *weniger*, weil vielleicht – rechtspolitisch – nicht jeder Rechtsbruch gleichermaßen unerwünscht ist wie die in § 323c StGB genannten Fälle (zu der Frage, ob nicht erst die fehlende Relevanz bzw. sogar Beachtung der Norm diese erträglich macht, später⁸⁸⁵ mehr – vorweg: Ich meine nein, weiß aber aus den Diskussionen zu dieser Frage, dass mancher das anders sieht). *Hier* geht es mir zunächst nur um die *grundlegende Wertung*, dass es einen Unterschied macht, namentlich verfassungsrechtlich, ob wir es mit Hin- oder Wegschauen zu tun haben. ‚Nur‘ *dafür* steht § 323c StGB oder stehen die polizeilichen Generalklauseln hier exemplarisch, nicht mehr.

- 434 cc. *Verfassungs- und rechtsdogmatische Relevanz des Narrativwechsels: der Unterschied zwischen Hin- und Wegschauen.* Der Unterschied zwischen Hin- und Wegschauen hat harte verfassungsdogmatische Konsequenzen:⁸⁸⁶ Während in der Überwachungskonstellation die Grundrechte als *Abwehrrechte* unmittelbar aktiviert sind, weil ja eine Schutzpflicht *in concreto* nur bestehen *könnte*, ist es in der Hilfeleistungssituation die *Schutzpflicht*, die unmittelbar und zuerst aufgerufen ist. Das Abwehrrecht des ‚Angreifers‘, nicht zum ‚Objekt‘ physischer Rechtsdurchsetzung und dafür gegebenenfalls erforderlicher Datenverarbeitung zu werden, wird hier

882 Ob die im Unionsrecht betriebene *funktionale* Versubjektivierung der Rechtsordnung (dazu statt aller Ludwigs, in: Kahl/Ludwigs [Hg.], HVwR I, 2021, § 8 Rn. 37 f.) auch unmittelbar das Hilfeleistungsnarrativ eröffnen könnte, muss hier offenbleiben.

883 Hierzu schon oben, → § 2 Rn. 227 ff.

884 Oder sogar ganz fehlen, s. oben, → § 2 Rn. 222 ff.

885 Dazu → § 2 Rn. 464 ff.

886 Vgl. BVerfG, Urt. v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 – BKA-Gesetz, Sondervotum Schluckebier, Rn. 23, wonach es eine „nicht hinnehmbare Konsequenz [des BKAG-Urteils sei], dass der Rechtsstaat [bei Anfall von Zufallsfunden i. R. bestimmter eingriffsintensiver Überwachungsmaßnahmen wie Telefonüberwachungen u. U.] gezielt ‚wegsehen muss‘ und damit den potentiell betroffenen Einzelnen oder Rechtsgütern der Allgemeinheit der gebotene Schutz vorenthalten wird, um auf der anderen Seite dem Schutz der Daten derjenigen, mit denen sich die Maßnahmen befassen, den Vorrang einzuräumen“. Auf Schluckebiers Sondervotum und seine Bedeutung für unsere Konstellation komme ich unten, → § 2 Rn. 468 ff., ausf. zu sprechen.

in aller Regel⁸⁸⁷ zurückstehen müssen – wie im Fall des allgemeinen Polizeirechts oder eben im Fall des § 323c StGB, der die wohl allgemeinste, weil auch Private als Verwaltungshelfer (*Pawlik*) umfassend in den Dienst stellende Rechtspflicht zur Hilfeleistung darstellt. Das Argument ‚Generalverdacht‘, das in der Anlassdogmatik des Bundesverfassungsgerichts als Eingriffsschwelle dogmatisch ausbuchstabiert ist, verfängt dann nicht mehr, bzw. genauer gesagt: diese Hürde ist genommen, denn der Anlass, zu handeln (oder zu warnen, zu melden etc.) ist eben da.

Folgt man der erläuterten Idee der Übertragbarkeit von § 323c StGB auf intelligente Maschinen (wohlgemerkt: *de lege ferenda* und mit gegebenenfalls angepassten materiellrechtlichen Konturen),⁸⁸⁸ dann stellt auch das einfache Datenschutzrecht dem Narrativwechsel keine grundlegenden Hindernisse in den Weg, wäre doch die für das Funktionieren der oben genannten *Structures* allfällige Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung „erforderlich“ und damit zulässig (Art. 6 Abs. 1 lit. c, Art. 22 Abs. 2 lit. b DSGVO). 435

Im Folgenden will ich nun auf zwei Einwände gegen meine Argumentation eingehen, die durchaus gewichtig sind, die zumindest mich am Ende aber doch nicht überzeugen. Es geht einmal um einen technikbedingten Einwand (sogleich, → b., zu meinen Gegeneinwänden → c.) und einen normativen Einwand (→ d., dort auch direkt zu meinen Gegenargumenten). 436

b. Ein gewichtiger technikbedingter Einwand gegen den Narrativwechsel: Hilfsbereite Technologie schaut – anders als ein Mensch – nie einfach zufällig (!) ‚hin‘. Es gibt einen gewichtigen Einwand gegen die These vom anstehenden Narrativwechsel: Auch avancierte intelligente Systeme sind keine Menschen, die ein Geschehen i. S. von § 323c StGB oder vergleichbaren Verhaltenspflichten zufällig wahrnehmen und vor dem Hintergrund der Hilfeleistungspflicht ‚einfach so‘ richtig verarbeiten könnten. Aktuelle künstliche Intelligenz arbeitet noch hochgradig aufgabenspezifisch,⁸⁸⁹ d. h. sie erfüllt genau den Zweck, auf den sie trainiert wurde bzw. für den ihr – im Fall der symbolischen KI – entsprechende Regeln einprogrammiert worden sind. Eine *General Artificial Intelligence* mit der Fähigkeit zu generalisiertem Lernen und entsprechendem Anwenden gibt es *noch* nicht. 437

Unser Haushaltsroboter iC ist also – anders als ein menschlicher Haushaltsangestellter – nicht nur zur selektiven Wahrnehmung und Auswertung der aufgenommenen optischen oder sonstigen Input-Signale *fähig*, sondern die Festlegung des zu Selektierenden steht am Anfang seiner Programmierung/seines Trainings. Er *kann* nur *selektiert* und aufgabenspezifisch auswerten. Datenschutzrechtlich gesprochen kann 438

887 Vorbehaltlich allfälliger Überprüfung der Verhältnismäßigkeit der Mittel zur Durchsetzung des Rechts (also z. B.: kein Schuss zum Schutz des Eigentums am Apfel; s. schon oben, → § 2 Rn. 246).

888 s. ausf. oben, → S. 150 ff.

889 s. dazu einführend oben, → S. 44 ff., aber auch sogleich, bei → § 2 Rn. 442.

damit die enge Zweckbindung auf – im Beispiel – *nur* Haushaltshilfe ohne Weiteres realisiert werden; anders als bei einem Menschen, dem diese Zweckbindung gerade nicht einprogrammiert werden kann.

- 439 In den beiden Narrativen gesprochen: Die Überwachungsleistung als Voraussetzung der Hilfeleistungsfähigkeit ist dem (aus anderen Gründen ‚zufällig‘ anwesenden) Menschen von Natur aus mitgegeben, dem (aus anderen Gründen ‚zufällig‘ anwesenden) KI-System/Roboter eben nicht, sondern muss als positive Kompetenz implementiert werden, muss also eben doch *hinzugefügt* werden. Der Haushaltsroboter iC würde, wenn nicht darauf trainiert bzw. programmiert, folglich nicht ‚erkennen‘, wenn seine Besitzerin gerade unberechtigt urheberrechtlich geschütztes Material auf *YouTube* hochlädt oder wenn sie ihren Freund im Bett ersticht, selbst wenn iC direkt neben dem PC steht oder direkt mit ihm vernetzt ist bzw. gerade im Schlafzimmer den Boden reinigt.
- 440 Es herrscht also technisch bedingt doch das Überwachungsnarrativ? Die Überlegung, es handele sich um Hilfeleistung, wäre dann neutralisiert durch die Einsicht, dass Hilfe im technischen Fall vorausgehende Überwachung voraussetzt, und weil diese nicht bzw. nur unter engen Voraussetzungen sein darf,⁸⁹⁰ wird es jene nicht so häufig geben (dürfen), als dass sich der hier vertretene Narrativwechsel wirklich in großem Umfang einstellen könnte.
- 441 *c. Drei Gegeneinwände.* So kann man argumentieren. Ich halte diese Argumentation indes weder für nachhaltig noch – unter dem Gesichtspunkt staatlicher Schutzpflichten – für rechtlich dauerhaft durchhaltbar; auch empirisch-soziologisch betrachtet halte ich sie nicht für vermittelbar.
- 442 *aa. Der Einwand ist technologisch nicht nachhaltig.* Dieser Gegeneinwand kann knapp formuliert werden: An genereller künstlicher Intelligenz (*Artificial General Intelligence*/AGI) wird gearbeitet, sie wird weiterhin als (Fern-)Ziel der KI-Forschung ausgegeben.⁸⁹¹ Sobald ihre Entwicklung gelingt, wird es also doch auch technisch-formal um Weg- statt Hinschauen-Dürfen gehen, mit allen dieser Unterscheidung impliziten normativen Konsequenzen. Mit der sogenannten *General-purpose AI* (Anwendungsbeispiel ist das bekannte ChatGPT⁸⁹²) sind erste Schritte in diese Richtung bereits getan.⁸⁹³

890 Oben, → S. 102 ff., S. 165 ff.

891 s. oben, → § 1 Rn. 43 ff.

892 s. für weitere Bsp. s. den Nachw. in → § 1 Fn. 134.

893 Es ist die besondere Stärke der aktuell vieldiskutierten großen NLP-Anwendungen wie GPT, dass sie zunehmend „task-agnostic“ statt „task-specific“ lernen (T. B. Brown et al., in: Larochelle et al. [Hg.], *Advances in Neural Information Processing Systems* 33, 2020, S. 1877) und zunehmend auch multimodal arbeiten; s. hierzu ausf. oben, → § 1 Rn. 44 ff. und nochmals unten, → § 3 Rn. 36.

bb. Der Einwand ist gesellschaftlich dauerhaft nicht vermittelbar. Auch wenn aktuell verbreitete künstlich-intelligente Systeme noch nicht über generelle Intelligenz verfügen, sondern funktional trainiert oder programmiert werden, so *simulieren* sie jetzt schon multifunktionale – generelle, mit anderen Worten menschliche – Kompetenzen in zunehmendem Maße: Zentral steht dafür die Idee des *Personal Assistants*/KI-Agenten, wie er in jedem modernen *Smart Phone* und zunehmend in *Smart Home Devices* implementiert wird (Stand 2025 freilich noch mehr schlecht als recht funktioniert – aber das dürfte sich nun rasch ändern). Auch die oben⁸⁹⁴ beispielhaft vertieften Haushalts- und Servicehilfen werden sicherlich keine monofunktionalen Aktanten bleiben, sondern – mit Fortschreiten des technologisch Möglichen – neben dem Staubsaugen bald auch die Fensterreinigung übernehmen sollen usw. Insgesamt geht die technische Entwicklung in Richtung multifunktionaler Systeme, wie der Ausbau von Plattformsystemen, LLMs und zwischenzeitlich auch die Idee des Metaverse zeig(t)en.⁸⁹⁵

Gleichzeitig, auf einer phänomenologischen Ebene, vermenschlicht die Technologie dabei zunehmend. Denn von *Chatbots*, autonomen Fahrzeugen und den bislang vor allem industriell genutzten *Cobots*⁸⁹⁶ über privat und geschäftlich genutzte *Personal Assistants* und KI-Agenten bis hin eben zu flexibel einsetzbaren humanoiden Haushalts-, Service- und Industrierobotern – alle Systeme *sollen* gerade mit Menschen kommunikationsfähig und auf dieser für ihre soziale Einordnung zentralen Ebene uns ähnlich(er) werden.

Dieser Trend ist nicht nur pragmatisch-wirtschaftlich, vielleicht auch emotional getrieben, sondern durchaus rechtlich forciert; er entspricht nämlich der verbreiteten Forderung, die Ergebnisse von KI müssten *explainable* sein, d. h. ‚die KI‘ solle am besten *self-explaining* sein.⁸⁹⁷ Selbst wenn wir auf einer intellektuellen Ebene noch wissen (werden) bzw. uns nach Art. 50 AI Act gegebenenfalls sogar gesagt werden muss, dass beispielsweise ein hoch vernetzter *Personal Assistant* Soft- und Hardware ist: “for all practical purposes [it] often does resemble a person.”⁸⁹⁸

Die Technologie entwickelt sich damit, vermutlich inkrementell und nach Sachbereichen differenziert, hin zum eigenständig handlungs- und kommunikationsfähigen und so *wahrnehmbaren* Akteur; bzw. – in Anlehnung an *Bruno Latours* Neologismus, der das Unmenschliche eines Akteurs sichtbar machen soll: entwickelt

894 Oben, ab → S. 150.

895 s. dazu bei/in → § 2 Fn. 850.

896 Die Abkürzung steht für Mensch-Maschine-Kollaborationen ohne trennenden Schutzraum, die in industriellen Anwendungen schon seit einigen Jahren zum Einsatz kommen, vgl. aus der insoweit bislang spärlichen jur. Lit. *Umbreit*, ARP 2021, 60 ff.

897 Dazu schon oben, → § 1 Rn. 51 ff.

898 Vgl. auch *Hildebrandt*, *Smart Technologies and the End(s) of Law*, 2016, S. 2.

sich zum eigenständig wahrnehmbaren *Aktanten*.⁸⁹⁹ Mireille Hildebrandt spricht von einem neuen Animismus,⁹⁰⁰ der mit solchen Technologien Einzugs in die Welt halte.

- 447 Darauf aufbauend nun die hier zentrale Frage: Werden ‚intelligente‘ Produkte marktfähig sein, wenn sie sich zwar in ihrem funktionellen Alltag “for all practical purposes” einer Person annähern, sie aber dann, wenn es darauf ankommt, also wenn Menschen in ihrem sensorisch zugänglichen Umfeld Hilfe benötigen, stumm und tatenlos bleiben? Am konkreten Beispiel: Wären sie marktfähig, wenn für sie § 323c StGB und die darin enthaltene Rechtspflicht zur Hilfeleistung – anders als für alle ‚anderen‘ Menschen – *nicht* gälte?
- 448 Blickt man in eines der wirkmächtigsten literarischen Narrative zu Mensch-Roboter-Interaktionen, scheint die Antwort leicht zu fallen: Nach Isaac Asimovs erstem seiner berühmten drei Gesetze der Robotik müsste unsere KI, wenn sie denn könnte, helfen. Es lautet: “A robot may not injure a human being, or, through inaction, allow a human being to come to harm.”⁹⁰¹ Sie (die KI) müsste also ‘harm’ von anderen Menschen abwenden, es sei denn, dies würde zu einer ‘injury’ eines anderen Menschen führen (ein Element der Verhältnismäßigkeit der Mittel ist also auch schon verbaut). Asimovs Gesetze werden in der Fachdiskussion um ethische Robotik und Mensch-Maschine-Beziehungen breit rezipiert und zugleich kritisiert;⁹⁰² kritisiert allerdings, soweit ersichtlich, vor allem dafür, dass Gesetze 2 und 3 es dem Roboter nicht gestatten, sich einem menschlichen Befehl zu widersetzen, sich *selbst* zu schädigen, bzw. nicht gestatten, sich gegen Angriffe zur Wehr zu setzen.⁹⁰³ Diese spezielle Frage führt in die Diskussion um den ethischen, moralischen und gegebenenfalls auch rechtlichen Status intelligenter Systeme, die wir hier ausklammern können.
- 449 Hier geht es um *wahrscheinliche Erwartungen* einer breiteren Öffentlichkeit an die Hilfsbereitschaft von Maschinen, also darum, ob sie ab einem gewissen Grad der an ihren Interaktionsfähigkeiten bemessenen Vermenschlichung helfen *sollen*. Ich denke, dass die Frage – im Einklang mit Asimovs erstem Gesetz⁹⁰⁴ – *im Grundsatz*

899 s. für den jur. Diskurs die Begriffsaufarbeitung bei Teubner, AcP 218 (2018), 155 (164 ff.) m. w. N.; s. auch Wischmeyer, in: Kulick/Goldhammer (Hg.), Der Terrorist als Feind? 2020, S. 193 (201), bezogen auf intelligente Videoüberwachung: Durch die Fähigkeit, „abweichende“ Verhaltensweisen selbsttätig zu identifizieren, „wird die Videokamera endgültig vom bloßen Mittel der Gefahrenabwehrbehörden zu einem – in der Sprache der Akteur-Netzwerk-Theorie – eigenständigen Aktanten im Sicherheitsdispositiv“.

900 Hildebrandt, Smart Technologies and the End(s) of Law, 2016, S. viii ff.

901 Zitiert nach Anderson, AI & Society 22 (2008), 477 f.

902 Für eine aktuelle ethische Verarbeitung von Asimovs fiktionalen Gesetzen s. die Beiträge in Wallach/Asaro, Machine ethics and robot ethics, 2017; außerdem Murphy/Woods, IEEE Intelligent Systems 24 (2009), 14 ff.; Anderson, AI & Society 22 (2008), 477 ff.; McCauley, Ethics and Information Technology 9 (2007), 153 ff.

903 Zitiert nach Anderson, AI & Society 22 (2008), 477 (490 ff.).

904 Vgl. Murphy/Woods, IEEE Intelligent Systems 24 (2009), 14: “The three laws have been so successfully inculcated into the public consciousness through entertainment that they now appear to shape society’s

ohne jeden Zweifel zu bejahen ist; dass es aber natürlich im Detail dann darauf ankommt, welche „Unglücksfälle“ (in der Terminologie von § 323c StGB) am Ende tatsächlich zum Einschreiten verpflichten und welche nicht, welche Rechtsverstöße mit anderen Worten als lässlich gewertet würden und welche Regeln tatsächlich ernst gemeint (und also wirklich präventiv durchzusetzen) sind. Es wird einen Unterschied machen, ob der präsente humanoide Roboter stumm bleibt, wenn wir die rote Ampel überqueren oder einen Urheberrechtsverstoß begehen, oder ob er beim Mord ‚zusieht‘.

Das war nun bei genauem Hinsehen natürlich eine hochgradig voraussetzungsvolle These im Tatsächlichen, die einer differenzierenden empirischen Überprüfung bedarf. Eine solche kann hier nicht geleistet werden. Deshalb sei sie (die These) auch ausdrücklich nur zur Diskussion gestellt: 450

Ein Produkt, das nach der Wahrnehmung der Menschen einem Menschen vergleichbare Fähigkeiten hat (simulieren kann), diese im (näher zu bestimmenden) Not- und Unrechtsfall aber nicht zugunsten von Menschen bzw. ihrer Rechtsgüter einsetzt, ist nicht marktfähig, da sozial nicht akzeptanzfähig.

Anders gewendet: Dass eine technisch zur (Not-)Hilfe fähige Struktur diese Hilfe 451 nicht leisten muss (oder zumindest darf), nur weil das nicht ihrer unmittelbaren Zweckbestimmung entspricht, erschien mir (unternehmens)politisch auf Dauer kaum durchhaltbar.

Ähnlich skeptisch scheint mir übrigens auch *Christoph Burchard* zu sein, wenn er 452 schreibt, dass ein Verzicht auf die immer weitere Optimierung der Rechtsdurchsetzung durch KI

„gehörigen kriminalpolitischen und straftheoretischen Mut voraus[setze]. Immerhin müsste beispielhaft die öffentliche wie private Fremd- und Eigenüberwachung, die notwendig ist, um Predictive bzw. Big Data Policing zu ermöglichen, als übermäßig freiheitsinvasiv klassifiziert werden. Und der virtuelle Freiheitsgewinn der Vielen, die keiner Überwachung ausgesetzt werden, müsste dem realen Freiheitsverlust der Wenigen vorgezogen werden, die Opfer von Straftaten werden, die sich durch den Einsatz von KI (wohl) hätten verhindern lassen.“⁹⁰⁵

Da nun aber diese These von der fehlenden Akzeptabilität nur virtueller Freiheit 453 im Tausch gegen realen Rechtsgüterschutz hier nicht weiter fundiert werden kann, soll weiter nach rechtlich haltbare(re)n Argumenten für die These vom rechtlich relevanten Narrativwechsel gesucht werden.

expectations about how robots should act around humans.“ Die beiden Autoren schlagen selbst alternative Regeln vor (a. a. O., S. 19 f.), die sich aber an *Asimovs* Gesetzen orientieren.

905 *Burchard*, JRE 27 (2019), 527 (550). *Burchard* argumentiert ganz im Überwachungsnarrativ; der m. E. normativ bedeutsame Wechsel ins Hilfeleistungsnarrativ findet bei ihm, soweit ersichtlich, keine Erwähnung.

454 cc. Der Einwand ist auch rechtlich nicht durchhaltbar. Von genereller künstlicher Intelligenz sind wir noch ein Stück weit entfernt, und die These, dass menschlich scheinende KI aus gesellschaftlichen Akzeptanzgründen heraus Menschen zumindest zur Einhaltung bestimmter Regeln zwingen müsste, kann hier methodisch nicht weiter fundiert werden. Es gibt aber noch eine dritte, weniger empirische, sondern im Kern rechtliche Argumentation zur Untermauerung der These vom Narrativwechsel. Sie baut auf der Formulierung eines allgemeinen Rechtsgedankens der KI-Regulierung auf. Er lautet:

Autonome Maschinen, die sich durch einen dem Menschen angleichenden Aktionsradius mit entsprechenden Freiheitsgraden auszeichnen, müssen sich an die für Menschen im konkreten Handlungsumfeld geltenden Regeln halten (können).⁹⁰⁶ Sie müssen insoweit zur Law-abiding Technology werden.⁹⁰⁷

455 Exemplarisch, aber – wie oben bereits ausgeführt – verallgemeinerungsfähig⁹⁰⁸ stehen hierfür §§ 1a, 1e StVG. Zur Erinnerung: Die Normen besagen, dass sich hoch- und vollautomatisierte und autonome Fahrzeuge an die „an die Fahrzeugführung gerichteten Verkehrsvorschriften“ halten müssen, um genutzt werden zu dürfen. Die hier für den sehr spezifischen, im Alltag aber bedeutsamen Lebensraum ‚Straßenverkehr‘ enthaltene Compliance-Anordnung enthält den soeben genannten, zu

906 Vgl. für den Kontext des autonomen Fahrens auch schon früh *Prakken*, Artificial Intelligence and Law 25 (2017), 341, bes. S. 344 f.; verallgemeinernd und im Erg. wohl zu weitgehend die These von *Abbott*, The Reasonable Robot, 2020, S. 3 f., der für ein „default“ einer von ihm sog. „AI legal neutrality“ wirbt, die besagt, dass – vorbehaltlich guter Gründe für eine Abweichung – „the law should not discriminate between AI and human behaviour.“ [A]s AI increasingly occupies roles once reserved for people, AI will need to be treated more like people, and sometimes people will need to be treated more like AI.“ Zur Relevanz für die Einhaltung spezifisch strafrechtlicher Verhaltensvorgaben s. a. a. O., S. 15. Krit. zu einem solch weitreichenden *Default* hingegen *Craig*, Jerusalem Rev. of Legal Studies 25 (2022), 24 (25): „Rights and responsibilities should be allocated with a clear view to the relationships and subjectivities that they shape and the social values they advance.“ Differenzierend auch *Rachum-Twaig/Somech*, in: Barfield/Weng/Pagallo (Hg.), Cambridge Handbook on Human-Robot Interaction, Kap. 30, die danach fragen, welche sozialen Normen auf robotische Systeme übertragen werden sollen und müssen. In Ansätzen findet sich die „akteursbezogene Indifferenz des Rechts“ (s. *Esposito*, in: Beyes et al. [Hg.], Niklas Luhmann am OVG Lüneburg, 2021, S. 127 [130]) freilich schon bei *Luhmann*, Recht und Automation in der öffentlichen Verwaltung, 1997, S. 46 f.: „Die Art der ‚Anlage‘ auf der Programme ausgeführt werden, die Maschine bzw. das menschliche Gehirn, ist für die ‚Logik‘ und die Richtigkeit des Schlusses unerheblich [...]. Sind [bestimmte] Bedingungen erfüllt, dann gilt | im Prinzip, daß die Übertragung der Entscheidung auf Maschinen die Rechtslage selbst nicht verändert.“ Und noch viel grundlegender a. a. O., S. 60, dort Fn. 24: „Aufs letzte gesehen gibt es keine rationalen Gründe, die Menschenleistung der Maschinenleistung vorzuziehen. Und jedesmal, wenn die Befürworter des Menscheneinsatzes ihre Gründe präzise formulieren, schaffen sie damit zugleich die Grundlage für die Formulierung neuer äquivalenter Maschinenprogramme.“

907 s. zum Begriff schon → § 1 Rn. 59. Damit ist der Steuerungscharakter von Recht betont. Diese Betonung bedeutet allerdings mitnichten automatisch, dass sich Recht, soweit es sich an Menschen richtet, in diesem Steuerungscharakter erschöpfen muss (mir scheint, dass *Rösinger*, ZfDR 2021, 147 [149 f.], aber genau davon ausgeht), beantwortet m. a. W. nicht die Frage, ob es für Menschen eine Freiheit zum Rechtsverstoß/zur Selbstbestimmung über den eigenen Rechtsgehorsam gibt oder geben muss. Dazu dann → § 5.

908 s. oben, → § 2 Rn. 202 ff.

verallgemeinernden Rechtsgedanken: Denn wenn autonome Maschinen mit einem dem Menschen vergleichbaren Aktionsradius und entsprechenden Freiheitsgraden sich *nicht* an die für Menschen im konkreten Handlungsumfeld geltenden Regeln halten könnten, dann wären sie unbrauchbar. Es würde den Menschen in seiner Aktions- und Interaktionsfähigkeit in einer robotisierten Umwelt seinerseits massiv einschränken, wenn die von der Geltung der Gesetze und Rechtsvorschriften vermittelte Erwartungsstabilisierung hinsichtlich des Verhaltens Dritter für die Aktantengruppe ‚Roboter/KI‘ nicht greifen würde.⁹⁰⁹

Das ist zuerst auch ein soziologisches und rechtspolitisches Argument; es folgt aber dahinter – als harter verfassungsrechtlicher Kern – aus den Schutzpflichten des Grundgesetzes, die bekanntlich den Staat in ihrer Gesamtschau auf die Herstellung einer objektiven *Werteordnung* verpflichten. Bewusst ist hier einmal die Ordnung betont. Denn der Diskussion um die *Werte*-gerechten Inhalte dieser Ordnung vorgelegt erfordert Ordnung primär eben das: die Herstellung einer wechselseitig kommunizierbaren, kommunizierten und zumindest grundsätzlich auch gelebten (d. h. gegebenenfalls: durchgesetzten) Ordnung.⁹¹⁰ Auf unser Thema angewandt, verlangt das Schutz vor der Emergenz neuer, wirkmächtiger künstlicher Aktanten, die sich in ihrem autonomen Verhalten dem tradierten und legitimen Erwartungshorizont der Regelbefolgung entziehen (könnten) und damit die Grundlage einer geordneten Koexistenz von Mensch und Maschine, einschließlich der Menschen untereinander, (zer)stören würden.

Simple, plakative Beispiele: Der Einkaufsroboter darf natürlich nicht stehlen, auch wenn sein Auftrag lautet, die Lebensmittel ‚möglichst günstig zu beschaffen‘. Das autonome Fahrzeug darf natürlich nicht die direkte Route wählen, auch wenn diese schneller zum Ziel führt, wenn es dafür eine Fußgängerzone befahren müsste. Eine digitale Steuererklärungs-Assistenz darf natürlich nicht Nebeneinkünfte verschweigen, nur weil ihre Aufgabe die Optimierung der Steuerschuld ‚nach unten‘ ist. Der Haushaltsroboter darf nicht die Stromleitung der Wohnung nebenan anzapfen, wenn und weil seine Aufgabe ‚Reduzierung des eigenen Stromverbrauchs‘ ist. Der *Smart-Home*-KI-Agent darf nicht illegale *Videosharing*-Plattformen aufrufen, wenn wir es darum bitten, Vorschläge für einen Filmabend zu machen. Und so weiter.

909 Vgl. hierzu auch Kube, AöR 146 (2021), 494 (516), wenn auch ohne ausdr. Bezug zu intelligenten Systemen: „Ohne Vertrauen in das – seinerseits als Vertrauensspeicher dienende – Recht, in seinen Vollzug und seine Befolgung wäre ein geordnetes Zusammenleben nicht möglich.“ Zur damit angesprochenen „Erwartbarkeit wechselseitigen Erwartens“ Luhmann, in: ders. (Hg.), Ausdifferenzierung des Rechts, 1999, S. 191 (207) m. w. N.

910 Vgl. i. d. S. auch Kube, AöR 146 (2021), 494 (504 f.). Man kann diese Überlegung als „oberflächlich-rechtstheoretisches (Vor-)Verständnis“ werten/abtun und eine Theorie normativer Ordnungen anspruchsvoller als Arrangement für einen fortdauernden Widerstreit um die Rechtfertigung von Normen in Kenntnis ihrer Fehlbarkeit deuten wollen; so Burchard, in: Forst/Günther (Hg.), Normative Ordnungen, 2021, S. 553. Aber selbst dieser Widerstreit setzt, soll er zivilisiert erfolgen, eine physisch relevante (also wohl „oberflächliche“) Ordnung voraus.

- 458 Warum ist das für uns relevant? Bislang folgt aus diesen Überlegungen lediglich, dass der Roboter/der KI-Agent *selbst* in der Lage sein muss, sich an Recht zu halten, nicht aber, dass er es auch *gegenüber anderen* durchsetzen muss. Tatsächlich ist es für uns auf zwei Ebenen wichtig:
- 459 *Erstens* wird sich irgendwann die Frage stellen, ab wann ein System über hinreichend Autonomie bei der Erfüllung von Aufgaben verfügt, um wertungsmäßig vom Werkzeug zu einem der Mitstörer- oder Mittäterschaft fähigen Akteur zu werden.⁹¹¹ Wenn es soweit ist, dann werden wir ‚ihm‘ – dem Roboter – Mitstörer- und Mittäterschaft auf Ebene der Programmierung sicherlich verbieten müssen. Sein *Default Setting* wird auch insoweit fortdauernd *Compliance* sein müssen. Exemplarisch kann hier erneut auf das StVG verwiesen werden, diesmal auf dessen § 1e Abs. 2 Nr. 5. Die weiter oben⁹¹² schon besprochene Vorschrift besagt in ihren Nummern 3 und 4 sinngemäß, dass ein autonomes Fahrzeug erkennen können muss, ob „die Fortsetzung der Fahrt nur durch eine Verletzung des Straßenverkehrsrechts möglich wäre“. Dann muss es die Kontrolle an die menschliche Technische Aufsicht abgeben, die dann über die (rechtsverletzende) Weiterfahrt entscheiden muss und darf. Das aber gilt mit der Einschränkung, dass das Fahrzeug auch die menschliche Entscheidung bzw. das damit verbundene Fahrmanöver weiter selbsttätig überprüft und sie – die menschliche Entscheidung – blockieren muss, „wenn das Fahrmanöver [der Technischen Aufsicht] am Verkehr teilnehmende oder unbeteiligte Personen gefährden würde“ (§ 1e Abs. 2 Nr. 5 StVG). Das Fahrzeug muss insoweit zur *Impossibility Structure* werden, es darf, plakativ ausgedrückt: nicht zum Mit- bzw. Nebentäter⁹¹³ einer Körperverletzung durch die Technische Aufsicht werden. Wenn wir jetzt bedenken, dass *wir selbst* immer mehr von dem, was wir tun, *durch* ‚intelligente‘ oder *mithilfe* ‚intelligenter‘ Technologie tun, also z. B. kommunizieren, reisen, unsere Finanzen regeln, Wasser verbrauchen usw., dann bedeutet das, dass auch *unser Default Setting* bald sein könnte, dass wir insoweit nur noch Rechtmäßiges tun *können*.
- 460 *Zweitens* ist für uns aber noch wichtiger: Der hier formulierte allgemeine Rechtsgrundsatz hat zur Folge, dass, je höher der Autonomiegrad eines Aktanten ist, umso mehr Rechterkennungstechnologie schon zur Erfüllung der *eigentlichen* Funktionalitäten verbaut werden muss. Womit der eingangs⁹¹⁴ im Sinn des überkommenen Überwachungsnarrativs formulierte Einwand (= die Rechtserkenntnistheorie trete *hinzu* und sei damit phänomenologisch und folglich auch rechtlich Überwachung) dann doch sukzessive mit den wachsenden Aktionsmöglichkeiten der

911 Oben, → § 2 Rn. 204, 260.

912 Oben, → § 2 Rn. 193, 204.

913 In die im Strafrecht zu führende Diskussion, ob es fahrlässige Mittäterschaft gibt oder ob in diesem Fall metaphorisch sogar eher Alleintäterschaft ‚des autonomen Fahrzeugs‘ durch Unterlassen vorliegt, will ich hier nicht einsteigen.

914 s. soeben, → § 2 Rn. 437.

Systeme neutralisiert wäre. Dabei kann hier nicht ausbuchstabiert werden, welche Rechtspflichten für welche Aktionen bzw. ab welchem Aktionsradius von welchem Typus Maschine beherrscht werden können müssen. Wenn wir noch einmal an die robotischen Haushalts- und Servicehilfen denken: Sicherlich werden sie Normen zum Schutz von Leib, Leben, Freiheit und Eigentum, zur Koordination im Straßenverkehr, zur Regelbefolgung beim Einkauf oder zur rechtskonformen Kommunikation mit Besuchern oder online schneller beherrschen können müssen als steuerrechtliche Regeln. Wir können uns hier aber letztlich auf den Grundsatz zurückziehen: Je mehr und je allgemeiner eine Maschine das ihr geltende Recht in einer konkreten Situation erkennen und umsetzen können muss, umso mehr befinden wir uns in einer Situation, in der rechtserkenntnis- und aktionsfähige Technologie bereits *da* (aktiviert) ist, *bevor* eine mögliche Rechtsgutverletzung in der Maschine sensorisch zugänglichen Umfeld geschieht – und umso mehr sind wir eben statt im Überwachungs- im Hilfeleistungsnarrativ.

Wir befinden uns dann zunehmend in einer Konstellation, die – in der menschlichen Parallele – der von § 323c StGB entspricht. Gilt nun auch hier der oben formulierte allgemeine Rechtsgrundsatz, dass Maschinen grundsätzlich dieselben Regeln einhalten können müssen, die für Menschen in äquivalenten Situationen gelten? Wie schon dargelegt,⁹¹⁵ ist speziell § 323c StGB keine Norm, die schon *de lege lata* auf ‚intelligente‘ Maschinen anwendbar wäre. Die allgemeine Hilfeleistungspflicht dient nach aktuellen Auffassungen in der Strafrechtswissenschaft dem aktiven Individualgüterschutz und damit der staatlichen Schutzpflichtenerfüllung. Bekanntlich hat der Staat insoweit einen weiten Einschätzungsspielraum, ob und wie er diesen Pflichten nachkommt. Er wäre also von Rechts wegen nicht dazu *gezwungen*, eine ihrem Umfang nach § 323c StGB entsprechende Hilfeleistungspflicht auf Maschinen zu erstrecken.⁹¹⁶

Aber nach der hier vertretenen Auffassung *könnte* er sich dazu entscheiden, auch Maschinen bzw. deren Programmierer/Hersteller dazu zu verpflichten, dort, wo eine entsprechend erkenntnis- und aktionsfähige Maschine nach Maßgabe ihrer Sensorik ‚anwesend‘ ist, Hilfe zu leisten.⁹¹⁷ Die mit der begrifflichen Einordnung als ‚Überwachung‘ verbundenen, rechtlichen und darüber hinaus auch rechtspolitischen, historischen und wohl sogar emotionalen Gewichte, die *dagegen* streiten,⁹¹⁸ sind im Hilfeleistungsnarrativ nicht mehr aktiviert, sondern es greift, wie gesagt, in der Abwägung ein gegenteiliger ‚Bias‘: Besonders begründungsbedürftig wird sein,

915 s. oben, → § 2 Rn. 227 ff.

916 Dazu, dass § 323c StGB nach heute h. M. ein Instrument staatlicher Schutzpflichtenerfüllung ist (und nicht mehr der Durchsetzung einer gesellschaftlichen Solidaritätserwartung dient), → § 2 Rn. 220.

917 Dazu, dass bei der Ausgestaltung entsprechender Rechtspflichten auf die Rechte der Hersteller Rücksicht zu nehmen ist, oben, → § 2 Rn. 245.

918 s. hierfür oben, → § 2 Rn. 407.

warum die Maschine soll ‚wegschauen‘ dürfen (d. h. soll nicht helfen müssen), *obwohl* sie den Hilfeleistungsbedarf erkannt hat und entsprechend reaktionsfähig ist.

- 463 Wichtig ist zuletzt noch der Hinweis, dass es dem Gesetzgeber jedenfalls möglich und im Interesse der Verhältnismäßigkeit der Mittel der Hilfeleistung⁹¹⁹ auch aufgetragen ist, die Wirkungen und Wirksamkeit von maschinellen Hilfeleistungen über das gesamte Spektrum der genannten Technologien von *Compliance Assistance* (i. e. S.) über *Justification* bis hin zur *Impossibility Structure* rechtsguts- oder rechtsspezifisch zu skalieren.⁹²⁰ Auch hier liefert nochmals § 1a StVG ein Beispiel: Während das autonome Fahrzeug menschlich angeordnete Fahrmanöver verweigern muss, wenn sie *Personen* gefährden,⁹²¹ muss es Sachschäden, die durch Fahrmanöver entstehen, ‚lediglich‘ protokollieren und dem gegebenenfalls Geschädigten zur Rechtsverfolgung zugänglich machen.⁹²²
- 464 d. Ein normativer Einwand: Wohnt nicht doch einer jeden Hilfeleistungspflicht ein Moment der Überwachung inne (d. h. Gleichzeitigkeit der Narrative statt Alternativität)? Schließlich soll eine naheliegende Replik auf die soeben genannten Gegeneinwände durchdacht werden, über die ich namentlich mit Jens-Peter Schneider und Nikolaus Marsch viel diskutiert habe: Wohnt nicht einer allgemeinen Pflicht zur Hilfeleistung, die jeden Anwesenden – lediglich vorbehaltlich eigener Gefährdung – zur Hilfe in jedem Unglücksfall verpflichtet (um bei § 323c StGB zu bleiben⁹²³), doch immer *auch* ein Element der Überwachung inne? Implizit leitet Pawlik selbst mit seiner Analogie von der Inpflichtnahme des zur Hilfeleistung Verpflichteten als staatlichem „Verwaltungshelfer“ auf diese Überlegung hin: § 323c StGB als breitflächiges – von der öffentlich-rechtlichen Wissenschaft meines Wissens bislang freilich völlig übersehenes – staatliches Überwachungsarrangement? Und könnte es nicht sein, dass diese sehr allgemeine Überwachungsmaßnahme gegenwärtig nur deshalb erträglich ist, weil die Norm überhaupt nur auf zufällig Anwesende beschränkt ist *und* sie vermutlich bewusst oder unbewusst⁹²⁴ kaum beachtet wird, ihre Verletzung

919 s. oben, → § 2 Rn. 246 f.

920 s. dazu auch → § 2 Rn. 359.

921 s. dazu oben, → § 2 Rn. 193, 204.

922 s. dazu oben, → § 2 Rn. 194 f., 206 f.

923 Zur Erinnerung: Nach Auffassung von Michael Pawlik reicht sogar der einfache Diebstahl aus, um die Pflicht zur Hilfeleistung zu aktivieren, s. Pawlik, GA 142 (1995), 360 (366). Freilich ist Pawliks Position zum Umfang der von § 323c StGB auferlegten Pflichten bes. weitgehend, vgl. → § 2 Rn. 214. Namentlich der BGH verlangt eine Straftat von gewisser Schwere, vgl. BGH, Beschl. v. 10.3.1954, Az. GSSt 4/53 = BGHSt 6, 147 – Hilfeleistung nach Selbstmordversuch. Auf die Unbestimmtheit dieser Position sei hier nur am Rande hingewiesen.

924 Bspw. wegen fehlender Rechtskenntnis oder Aufmerksamkeit anwesender Menschen.

jedenfalls kaum Gegenstand von Strafverfahren ist?⁹²⁵ Die Fragen leiten hin zu schwierigen Überlegungen.

Klar ist dabei zunächst nur Folgendes: Es kann nicht in Abrede gestellt werden, dass die *praktischen* Abschwächungen, welche die Wirkmacht von § 323c StGB oder auch die Eingriffsbefugnisse einer *anwesenden* Polizistin erfahren,⁹²⁶ im Fall von rechts-erkenntnis- und entsprechend handlungsfähigen Technologien *nicht* mehr greifen. Das ist ja gerade der Clou der sich abzeichnenden Infrastrukturalisierung: Das Maß an Hilfe ist rein *praktisch* betrachtet potentiell unbegrenzt. Es wäre jedenfalls viel größer als die ‚Überwachung‘, welche die allgemeine *menschliche* Hilfeleistungspflicht oder die wenigen Streife gehenden Polizisten bewirken. Zumal, daran sei auch erinnert, auch der zweite Abschwächungsgrund bei Maschinen nicht greifen darf: Da diese sich qua Programmierung zwingend *law abiding* verhalten müssen,⁹²⁷ kommt die bewusste oder unbewusste Nichtbeachtung, die man für § 323c StGB einmal vermuten darf, hier nicht als Korrektiv in Frage.

Wenn wir daher einmal annehmen, dass das Hilfeleistungs- das Überwachungs-narrativ nicht komplett verdrängen würde, sondern sie beide *gleichzeitig* greifen würden, dann hätte das zur Folge, dass eben *auch* die Hürden der Anlassrechtsprechung des Bundesverfassungsgerichts⁹²⁸ zu überwinden wären, sollte der Gesetzgeber beschließen, die Hilfeleistungspflicht für KI-Aktanten zu normieren. Die Hürden wären dann zwar niedriger, eben weil es *auch* um akute Hilfeleistung ginge. Nichtsdestotrotz dürfte der Gesetzgeber den Rechtsgedanken von § 323c StGB nicht 1:1 auf Maschinen übertragen, sondern nur in abgeschwächter, z. B. auf hochrangige Rechtsgüter beschränkter Form. Tatsächlich ist das ein Kompromiss, der im geltenden Strafrecht an anderer Stelle schon umgesetzt wurde: § 138 StGB verpflichtet nicht zur Anzeige *aller* Straftaten (oder gar Rechtsverletzungen) mit dem Ziel, diese zu verhindern, sondern nur zur Anzeige bestimmter, schwerer Delikte.

Meines Erachtens ist es eine gefährliche Strategie, Überwachung und Hilfeleistung für parallel wirksam zu erklären: Gerade weil der Begriff der Überwachung – mit seinen dogmatischen Konsequenzen – die Qualität eines Narrativs hat, kann er auch Rückwirkungen auf gesellschaftliche Einstellungen haben: *Besagt* das Recht, dass in jeder Hilfeleistung eine Überwachung liegt, und weil ‚Überwachung‘ mindestens ambivalent, angesichts der Assoziationen, die damit verbunden sind, wohl sogar

925 Das Statistische Bundesamt weist für 2021 133 Verurteilungen wegen Verstoßes gegen § 323c StGB aus, im Vergleich zu 815.199 nach allgemeinem Strafrecht Verurteilten in diesem Jahr insgesamt, s. *Statistisches Bundesamt*, Rechtspflege 2021, S. 16, 42.

926 Auch diese müsste und dürfte ja nicht wegschauen, wenn sie eine Gefahr/Rechtsgutverletzung wahrnimmt, sondern dürfte und müsste verhältnismäßige Hilfe leisten; zur hiermit auch angerissenen Frage der Ermessensreduzierung auf Null schon in → § 2 Fn. 880.

927 s. soeben, → § 2 Rn. 454.

928 s. oben, → § 2 Rn. 82 ff.

negativ konnotiert ist, droht die Gleichsetzung einer Erosion der Hilfsbereitschaft in der Bevölkerung *zwischen Menschen* Vorschub zu leisten und ihr vor allem *Rechtfertigung* zu liefern. Das rät zu großer Vorsicht, was die Annahme von Gleichzeitigkeit der Narrative angeht.

468 Als hilfreich könnte es sich an dieser Stelle allerdings erweisen, die verfassungsgerichtliche Rechtsprechung zur sogenannten „hypothetischen Datenneuerhebung“⁹²⁹ vergleichsweise heranzuziehen. Die Rechtsprechung ist deshalb hier *prima facie* relevant, weil es darin auch um „Zufallsfunde“⁹³⁰ geht. *Wilhelm Schluckebier* verdeutlicht in seinem Sondervotum zum BKAG-Urteil des Verfassungsgerichts die Wirkungen der komplizierten Rechtsprechung⁹³¹ an anschaulichen Beispielen:⁹³² Darf das Bundeskriminalamt Hinweise auf einen Diebstahl oder eine Umweltstraftat, die „zufällig“ bei einer präventiven Telefonüberwachung erlangt wurden, an die zuständige Ortspolizeibehörde weiterleiten? Umgekehrt: Darf eine Landespolizeibehörde Hinweise auf einen drohenden Farbbeutelanschlag auf einen Politiker an das zuständige BKA weitergeben? Nach der geltenden Rechtsprechung dürfen die jeweiligen Behörden das *nicht* tun, weil das jeweils bedrohte Rechtsgut nicht so hochrangig ist, als dass es die eingriffsintensive Telefonüberwachung *hierfür* hypothetisch hätte rechtfertigen können. Ginge es hingegen – so führt *Thomas Schwabenbauer* die Beispiele von *Schluckebier* weiter – um Hinweise auf eine Tötung, dann wäre der Datenaustausch jeweils zulässig.⁹³³ Steckt hierin nicht – *mutatis mutandis* auf unsere Situation übertragen – die Aussage des Bundesverfassungsgerichts, dass Hilfeleistung nicht nur versagt werden darf, sondern versagt werden muss, weil sie ansonsten die grundrechtlichen Grenzen der – nach der Senatsmehrheit *noch zulässigen* – *Überwachung* von Individuen schwächen könnte?

469 Zunächst: Ich teile die Auffassung von *Schluckebier*, dass die Rechtsprechung der Senatsmehrheit zu Überwachungsmaßnahmen

„bei denen [...] Zufallserkenntnisse anfallen, [zu] kaum erträglichen Ergebnissen führ[t], weil [sie] von der rechtsstaatlichen Ordnung nicht mehr und nicht weniger verlangt, als vor drohenden Gefahren für ebenfalls wenigstens gewichtige Rechtsgüter *die Augen zu verschließen* und die Realisierung von Straftaten und die Beschädigung von Rechtsgütern hinzunehmen.“⁹³⁴

929 Hierzu ausf., allerdings krit., *Bäcker*, Kriminalpräventionsrecht, 2015, 486 ff.

930 *Schwabenbauer*, in: *Bäcker/Denninger/Graulich* (Hg.), *PolR-HdB*, 72021, Abschnitt G Rn. 29 f.

931 s. *Ibid.*, Rn. 249 ff. m. w. N. zur Rspr.

932 BVerfG, Urt. v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 – BKA-Gesetz, Sondervotum *Schluckebier*, Rn. 21 f.

933 *Schwabenbauer*, in: *Bäcker/Denninger/Graulich* (Hg.), *PolR-HdB*, 72021, Abschnitt G Rn. 254.

934 BVerfG, Urt. v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 – BKAG-Urteil, Sondervotum *Schluckebier*, Rn. 20. Hervorhebung hier.

Es ist genau dieser Umstand, dass in großem Umfang „gezielt ‚weg[ge]sehen [werden] muss“;⁹³⁵ der nach meiner Auffassung⁹³⁶ und offensichtlich auch für *Schluckebier* zu einer „nicht hinnehmbaren Konsequenz“⁹³⁷ führt.⁹³⁸ 470

Nun ist darauf hinzuweisen, dass auch *Schluckebier* dort vorsichtiger formuliert, wo es um „anlasslos in großer Breite erhobene Massendaten geht“,⁹³⁹ oder wo es um 471

„Erkenntnisse [geht], die mittels hochinvasiver, besonders schwerwiegender Eingriffe gewonnen worden sind, wie das etwa bei der Wohnraumüberwachung und der Online-Durchsuchung informationstechnischer Systeme der Fall ist.“⁹⁴⁰

„[A]llenfalls“ (!) hier könne das Wegsehen „seine Berechtigung“ haben.⁹⁴¹ Da es nun bei uns – angesichts der dargestellten Infrastrukturalisierung von rechtserkenntnisfähigen Technologien – ja gerade um massenhaft erhobene und potentiell auch aus hoch geschützten Räumen stammende Daten geht, stellt sich die Frage, ob man auch in unserer Konstellation mit *Schluckebier* ins Zweifeln kommen muss. 472

Ich meine nein: Denn *letztlich* wird auf einen genauen zweiten Blick der hier um des Argumentes willen angestellte Abgleich unserer Konstellation mit dem Konzept der hypothetischen Datenneuerhebung insgesamt schief und verliert seine Aussagekraft. Der ganz entscheidende Punkt in der Entscheidung der Senatsmehrheit im BKAG-Urteil war es ja, dass der „Zufallsfund“ aus einer eingriffsintensiven, vorausgehenden staatlichen *Überwachungsmaßnahme* wie eben z. B. einer Telefonüberwachung resultiert. Es handelt sich also streng genommen gar nicht um einen wirklichen „Zufallsfund“, wie er für die Konstellation der allgemeinen Hilfeleistungspflicht kennzeichnend wäre; sondern richtigerweise um ‚Beifang‘ einer staatlichen Überwachungsmaßnahme und -technologie, die *nicht* ohnehin schon ‚da‘ war.⁹⁴² 473

Damit führen letztlich alle Überlegungen zu dem Punkt, hinterfragen zu können und zu müssen, ob das ‚Schutzgut‘, das man mit dem *Verzicht* darauf schützen würde, eine Hilfeleistungspflicht trotz Möglichkeit der Hilfeleistung zu normieren, nicht letztlich doch der Selbstbestimmungswille eines Rechtsunterworfenen über seinen 474

935 Ibid., Rn. 23.

936 s. soeben, → § 2 Rn. 431 ff.

937 BVerfG, Urt. v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 – BKAG-Urteil, Sondervotum Schluckebier, Rn. 23.

938 Dazu, dass sich die Sicherheitsbehörden mittlerweile auch nach der Auffassung des Senats aber nicht ‚unwissender‘ stellen müssen, als sie es auch unter Zuhilfenahme von automatisierten Datenauswertungsmöglichkeiten sind, BVerfG, Urt. v. 16.2.2023, Az. 1 BvR 1547/19, 1 BvR 2634/20 = BVerfGE 165, 363 – Automatisierte Datenanalyse, Rn. 108; zur Einordnung ausf. oben, → § 2 Rn. 108 ff.

939 BVerfG, Urt. v. 20.4.2016, Az. 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 – BKAG-Urteil, Sondervotum Schluckebier, Rn. 23.

940 Ibid., Rn. 20.

941 Ibid.

942 Und die sich auch – im Gegensatz zum Streifengang einer Polizistin oder der Entgegennahme von Notrufen – ganz unstr. selbst als Grundrechtseingriff darstellt.

eigenen Rechtsgehorsam sein könnte – oder wenigstens ein *objektives* rechtliches Interesse am Erhalt individueller Verhaltenskontingenz. Ob es einen solchen Schutz bzw. ein solches Interesse gibt, ist allerdings die zentrale Frage von → § 5, der dort vertieft nachgegangen werden soll.⁹⁴³

- 475 Hier soll es nun ausreichen, nochmals festzuhalten, dass unabhängig davon, wie man sich zur Frage *Wechsel* oder *Ergänzung* der Narrative positioniert, die vorstehenden Überlegungen gezeigt haben, dass es dem Gesetzgeber *jedenfalls leichter* fallen dürfte, den Einsatz rechtserkenntnisfähiger Technologien vorzuschreiben, *so weit diese schon zur Funktionalität der entsprechenden Systeme verbaut sind*; mit der Folge, dass die im Radius dieser Systeme mögliche Verhaltenskontingenz deutlich abnehmen dürfte.
- 476 *e. Perspektive: Zukunft.* Abschließend ist hier nochmals der Hinweis angezeigt, dass, wie *Eric Hilgendorf* mit Blick auf § 1e Abs. 2 Nr. 2 bis 5 StVG richtig formuliert hat,⁹⁴⁴ die hier letztlich nur beispielhaft auch für künftige Regulierung hoch-autonomer robotischer und sonstiger ‚intelligenter‘ Systeme eingeforderten Rechtserkenntnis- und Rechtserkenntnisreaktions-Kompetenzen technisch anspruchsvoll sind. Offen gesagt dürfte es sich bei der StVG-Norm derzeit noch um einen Fall legislativer *Science Fiction* oder – weniger scharf formuliert – um zukunftsbezogene Rechtssetzung handeln. *Christoph Burchard* weist zutreffend auf die Gefahr hin, dass rechtswissenschaftliche Überlegungen, die diese *Science Fiction* aufgreifen und verallgemeinern, „naiv“ wirken können.⁹⁴⁵ Folgt man allerdings dem Ansatz der *Futurist Legal Studies*, dann ist es zumindest *auch* die Aufgabe von Rechtswissenschaft, Überlegungen in diesen Unsicherheitsbereichen anzustellen; solange es sich um futuristische Projektionen handelt, die auf Bestehendem aufbauen können, und nicht um rein utopistische (oder spiegelbildlich: rein dystopische) Spekulationen.⁹⁴⁶
- 477 Die vorstehenden Überlegungen, hoffe ich, sind dieser wichtigen Unterscheidung gefolgt: Natürlich ist es gegenwärtig noch einfach, den Diskurs um rechtsrealisierende Technologien weitgehend exklusiv im Narrativ der Überwachung zu halten. Die Technologien sind als *Zusatz* gut wahrnehmbar, wirken sozusagen als *Add on* zu den *eigentlichen* Funktionen von Technologien. Dieser Eindruck passt, weil KI-Technologien bislang noch *erkennbar* spezifisch konkrete Aufgaben wahrnehmen, d. h. monofunktional und eben noch keine Allrounder sind bzw. sein müssen, wie es ein menschlicher Beobachter wäre. Das Überwachungsnarrativ wird allerdings immer weniger passen bzw. immer weniger Gewicht besitzen, wenn die Technologien

943 s. unten, ab → S. 403.

944 s. für das Zitat → § 2 Rn. 193.

945 *Burchard*, in: Forst/Günther (Hg.), *Normative Ordnungen*, 2021, S. 553 (561).

946 Zur Methode oben, → Rn. 33 (Einleitung).

multifunktional agieren und multimodal verknüpft sind.⁹⁴⁷ Es wird vor allem dann nicht mehr passen, wenn die eigentliche Funktion so autonom agieren kann, dass sie ohne Kombination mit rechtsrealisierender Technologie nicht mehr denkbar sein wird: autonome Fahrzeuge, humanoide Roboter, oder *Personal Assistants*, welche die Steuererklärung selbstständig vorbereiten oder gar einreichen sollen. Spätestens dann scheint mir der Narrativwechsel vollzogen bzw. unvermeidbar, mit den soeben erläuterten normativen Folgerungen.

5. Zuletzt ein Widerspruch gegen die Thesen von der Naturalisierung und Entdialogisierung der Rechtsanwendung

So sehr die These von der zunehmend ‚smarten‘ Umwelt folglich an Plausibilität gewinnt, so wenig richtig erscheint es mir, die Infrastrukturalisierung der Technologie – und damit potentiell der Rechtsanwendung – pauschal mit einer „Naturalisierung“ des Rechts bzw. einer „Natürlichkeit“ seiner Anwendung gleichzusetzen. Deshalb möchte ich etwa *Klaus Günther* widersprechen. Er schreibt, dass „[d]ie technisch perfektionierte Normbefolgung [...] die Norm zu einem Teil der ersten Natur werden [lasse], wie das Gravitationsgesetz schon immer eines ist. Als Natur erscheint sie unveränderlich.“⁹⁴⁸ Mir erscheint die Aussage etwas zu undifferenziert. Die These der Unveränderlichkeit mag mit Blick auf eine Steuerung durch das sogenannte *Nudging* plausibel sein,⁹⁴⁹ bei dem dem Rechtsunterworfenen gar nicht klar ist, dass er gesteuert wird. Sie passt hingegen nicht bei algorithmischer Steuerung durch *Impossibility Structures*, *Justification Structures* und *Compliance Assistance Technologies* (die – wenn ich *Günther* richtig verstehe – alle Teil der von ihm sogenannten „smarten Ordnungen“ sind⁹⁵⁰). Anders als im Fall des *Nudging* ist es nämlich gerade *nicht* definitorisch konstitutiv für Rechtsrealisierung durch technologische *Compliance Structures*,⁹⁵¹ dass die Verhaltensbeeinflussung unbewusst⁹⁵² oder manipulativ⁹⁵³ erfolgt, also „less visible, less contestable“ ist als die Verhaltenssteuerung

947 s. dazu ausf. oben, → § 1 Rn. 46 f., sowie nochmals unten, → § 3 Rn. 72 f.

948 *Günther*, in: Forst/Günther (Hg.), *Normative Ordnungen*, 2021, S. 523 (547). Ähnl. (wohl) *Burchard*, a. a. O., S. 553 (579); *Rauber*, JZ 79 (2024), 174 (176 f.).

949 Dazu schon → § 2 Rn. 140.

950 s. oben, → § 2 Rn. 370.

951 Vgl. nochmals, → § 2 Rn. 140.

952 Dazu, dass dieses Element konstitutiv für eine abgrenzbare Definition des Konzepts des *Nudging* ist, *O'Hara*, AöR 145 (2020), 133 (166); s. zur Abgrenzung des *Nudging* von *rechtlicher* Anreizsteuerung *J. Wolff*, *Anreize im Recht*, 2021, S. 21 f. Eine aktuelle monographische Bearbeitung des *Nudging*-Themas aus grundrechtlicher Sicht liefert *F. Baer*, *Staatliche Steuerung durch Nudging im Lichte der Grundrechte*, 2023, passim.

953 Vgl. *Kreßner*, *Gesteuerte Gesundheit*, 2018, S. 200 ff., dort auch zu Unterscheidungen von manipulativ, suggestiv und persuasiv.

nur durch Normen.⁹⁵⁴ Sicherlich sind *Compliance Structures* denkbar, die unbewusst wirken und damit einen Unterfall von *Nudging* darstellen, was dann wiederum die Überlegungen in die *Nudging*-Debatte um- und ablenken würde. Das soll hier vermieden werden, wie die in diesem § 2 beschriebenen Beispiele illustrieren sollten. Davon qualifiziert keine einzige als *Nudging* im engeren Sinn.⁹⁵⁵ In allen hier genannten Beispielen ist es für die Nutzer der Technologie bzw. diejenigen, die mit den physischen oder kommunikativen Wirkungen der Technologie konfrontiert sind, vielmehr hinreichend transparent, dass sie eben technologischen Wirkungen (Widerständen oder Informationen) ausgesetzt sind. Sie alle erlauben also auch Kontestation in mehr oder weniger formalisierten Foren.

479 Richtig ist hingegen, dass diese Wirkungen jedenfalls im Fall von *Impossibility Structures* physisch und in den anderen Fällen eventuell psychisch nicht leicht veränderlich sind. Das ist gerade ihr Sinn und Zweck. Aber es kann ohne Schaden für die Funktionalität der Systeme transparent bleiben, dass es sich um künstliche (und eben nicht natürliche) Mechanismen handelt, die in Betrieb gesetzt sind und die auch wieder außer Betrieb genommen werden können und die in ihrer Funktion verändert werden können – weswegen zwar nicht das Bild der Natur, aber eben das Bild der Infrastruktur oder auch Umwelt (*Joh, Reckwitz*) gut passt: physisch oder psychisch wirksam und nicht leicht veränderlich, sondern möglicherweise Verhalten lenkend oder zumindest beeinflussend, aber mit gewissem Aufwand eben doch veränderlich. Infrastruktur kann als solche erkannt, verändert, zurück-, um- oder weitergebaut werden, die Schranke kann gehoben, der Tresor geöffnet werden, was für digitale *Compliance*-Systeme auch möglich bleibt – sie sind mit anderen Worten selbst auch kontingent.⁹⁵⁶

480 Mit der These der natürlichen Unveränderlichkeit eng verknüpft ist ein weiterer genereller Kritikpunkt am Einsatz künstlich-intelligenter Rechtsdurchsetzung: der Einwand der fehlenden Dialogfähigkeit der Systeme. Mit Natur kann man nicht kommunizieren. Dass auch dieser Einwand allerdings zu pauschal ist, habe ich oben bereits im Rahmen der beiden Abschnitte zu den *Impossibility Structures* und den

954 *Hildebrandt*, *Smart Technologies and the End(s) of Law*, 2016, S. 165, die den Einsatz von KI zur Verhaltenssteuerung auf von ihr sog. "pre-emptive technologies" zuspitzt, was begrifflich-konzeptionell einem *Nudging* unter Einsatz von digitalen Technologien entsprechen dürfte; vgl. auch a. a. O., S. 69: "[T]he paradigm of pre-emptive computing is subliminal intervention". Es geht *Hildebrandt* in ihrem Buch m. a. W. zentral um das Risiko der *unbewussten* Manipulation von Nutzern durch Informationstechnologien, s. ebd., S. 185.

955 Das gilt natürlich nur, falls man das Konzept nicht schlicht mit „Steuerung“ gleichsetzt und damit deskriptiv und dogmatisch wertlos macht. Für eine dogmatisch brauchbare Konturierung, die sich am Kriterium des *Sich-(nicht-)Bewusstseins* des Beeinflussten von der Verhaltensbeeinflussung orientiert, s. *O'Hara*, AöR 145 (2020), 133 (165 ff.).

956 Nur nebenbei sei abschließend erwähnt, dass selbst dann, wenn man die Technologien nicht (nur) als Teil der Umwelt, sondern tiefer wurzelnd als Teil der Natur metaphorisieren will, die Folgerung der Unveränderlichkeit nicht trägt: Mittlerweile kann der Mensch u. U. auch die Natur ändern.

Justification Structures zeigen wollen; es sei hier nur noch einmal daran erinnert, weil es in → Kapitel 2 gleich besonders wichtig wird:⁹⁵⁷ Je nach der Verortung des künstlich-intelligenten Systems in dem größeren Interaktionszusammenhang von Mensch und Maschine kann es sogar dazu beitragen, „Verantwortung, Rechtfertigung und Kritik“⁹⁵⁸ an Normen bzw. Normanwendungsoperationen organisationell stärker zu strukturieren und zu formalisieren, wodurch das geforderte „diskursive Ernstnehmen“⁹⁵⁹ des Normadressaten sogar gesteigert werden kann.

Richtig ist aber, dass dieser Diskurs in den genannten hybriden Interaktionszusammenhängen nunmehr, also wenn intelligente Technik eingebunden werden soll, zwischen Akteuren und Aktanten erfolgt, die *per se* keine gemeinsame Sprache sprechen.⁹⁶⁰ Das bleibt nicht ohne Folgen für die Ausgestaltung der Mensch-Maschine-Zusammenarbeit, die neue Übersetzungsleistungen zulassen und organisationell vorsehen muss. Sie sind letztlich die Bedingung dafür, dass die neue Arbeitsteilung von Mensch und Maschine bei der Realisierung von Recht rechtlich und sozial akzeptiert werden kann. Um die Konturen dieser Arbeitsteilung geht es im folgenden → Kapitel 2.

481

957 s. oben, → § 2 Rn. 264 ff. bzw. → § 2 Rn. 369 ff.

958 Günther, in: Forst/Günther (Hg.), *Normative Ordnungen*, 2021, S. 523 (542).

959 Vgl. Burchard, in: Forst/Günther (Hg.), *Normative Ordnungen*, 2021, S. 553 (579).

960 s. dazu unten, → § 3 Rn. 98 ff.

