Künstliche Intelligenz

Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?

herausgegeben von

dem Bundesministerium
für Umwelt, Naturschutz, nukleare Sicherheit
und Verbraucherschutz

und

Frauke Rostalski

Mohr Siebeck

Frauke Rostalski, geboren 1985; Studium der Rechtswissenschaften in Marburg; 2011 Promotion Rechtswissenschaften; 2017 Promotion Philosophie; seit August 2018 Inhaberin des Lehrstuhls für Strafrecht, Strafprozessrecht, Rechtsphilosophie und Rechtsvergleichung an der Universität zu Köln.
orcid.org/0000-0002-5606-3639

Veröffentlicht mit Unterstützung des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz.

ISBN 978-3-16-161298-5 / eISBN 978-3-16-161299-2
DOI 10.1628/978-3-16-161299-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Laupp & Göbel in Gomaringen gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Inhaltsverzeichnis

Trainingsdaten und die Rechte von betroffenen Personen

– in der DSGVO und darüber hinaus?

Gerrit Hornung[1]

I. Einleitung

Die Herausforderungen algorithmenbasierter Datenverarbeitung werden in den Rechtswissenschaften seit etlichen Jahren diskutiert. Dies begann bereits in einer Zeit, in der es noch um die rechtlichen Anforderungen an die Verwendung herkömmlicher Algorithmen ging, die also noch nicht als Künstliche Intelligenz (KI) bezeichnet werden konnten.[2] Mit der fortschreitenden Entwicklung der Modelle und Algorithmen, etwa im Bereich von Technologien maschinellen Lernens,[3] intensivierten sich die entsprechenden rechtswissenschaftlichen Analysen.[4]

Erst in jüngerer Zeit gewinnt demgegenüber die Erkenntnis Raum, dass es sich bei den identifizierten rechtlichen Problemen der KI teilweise nicht um solche der verwendeten Algorithmen selbst handelt. Während prinzipielle Probleme

---

[1] Der Text ist im Zusammenhang mit Arbeiten des BMBF-Projekts „Künstliche Intelligenz zur Analyse und Fusion von Erdbeobachtungs- und Internetdaten zur Unterstützung bei der Lageerfassung und -einschätzung" (AIFER, FKZ 13N15528) sowie der Projektgruppe „Nachhaltige Intelligenz – intelligente Nachhaltigkeit" des hessischen Zentrums verantwortungsbewusste Digitalisierung (ZEVEDI) entstanden, deren Sprecher der Verfasser ist.

[2] S. z. B. die Diskussion um die (In-)Transparenz der Scorewert-Berechnung durch die SCHUFA; dazu BGHZ 200, 38; *Hammersen/Schade*, DuD 2014, 399; *Paal*, JZ 2014, 1006.

[3] Insbesondere Verfahren des deep learning, dazu aus technischer Sicht *Goodfellow/Bengio/Courville*, Deep Learning, 2016; *Russell/Norvig*, Artificial Intelligence: A Modern Approach, 4. Auflage 2020, 750 ff.; zu den soziotechnischen Voraussetzungen des deep learning s. *Mühlhoff*, ZfM 2/2019, 56.

[4] Grundsätzlich zu den rechtlichen Herausforderungen der KI z. B. *Hoffmann-Riem*, AöR 142 (2017), 1; *Wischmeyer*, AöR 143 (2018), 1; *Herberger*, NJW 2018, 2825; *Martini*, Blackbox Algorithmus, 2019; s. ferner die Beiträge in *Kaulartz/Braegelmann* (Hrsg.) Rechtshandbuch AI and Machine Learning, 2020; *Beck/Kusche/Valerius* (Hrsg.), Digitalisierung, Automatisierung, KI und Recht, 2020; *Ebers/Heinze/Krügel/Steinrötter* (Hrsg.), Künstliche Intelligenz und Robotik, 2020; *Wischmeyer/Rademacher* (Hrsg.), Regulating Artificial Intelligence, 2020; *Chibanguza/Kuß/Steege* (Hrsg.), Künstliche Intelligenz. Recht und Praxis automatisierter und autonomer Systeme, 2021; *Dederer/Yu-Cheol Shin* (Hrsg.), Künstliche Intelligenz und juristische Herausforderungen, 2021; *Ebers/Steinrötter* (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021; *Busch/De Franceschi* (Hrsg.), Algorithmic Regulation and Personalized Law, 2021; zu den Herausforderungen für die demokratische Gesellschaft s. die Beiträge in *Unger/v. Ungern-Sternberg*, Demokratie und künstliche Intelligenz, 2019; s. a. das Gutachten der *Datenethikkommission*, 2019, 159 ff.

der Lesbarkeit der Entscheidungen und ihrer – hiervon zu unterscheidenden – Verständlichkeit bzw. Nachvollziehbarkeit für Menschen eher vom verwendeten KI-Modell abhängen (also z. B. ein bestimmter Subtyp neuronaler Netze), werden Verzerrungseffekte oftmals durch das Training dieses Modells hervorgerufen. Dabei werden Trainingsdaten verwendet und im Rahmen des Trainings die Parameter des Modells kontinuierlich angepasst, um die Ergebnisgenauigkeit zu verbessern. Dementsprechend können Fehler entweder dadurch hervorgerufen werden, dass die zum Training der Algorithmen verwendeten Daten fehlerhaft, nicht repräsentativ oder in anderer Weise ungeeignet sind, oder durch eine fehlerhafte Anpassung der Parameter. Datenqualität und Parametrierung hängen insoweit zusammen, als z. B. eine gewisse fehlende Repräsentativität der Trainingsdaten (wenn diese beispielsweise deutlich mehr Daten von Männern als von Frauen enthalten) durch entsprechende Parameter ausgeglichen werden kann, wenn sie erkannt wird.

Fehlt es an einer in dieser Weise notwendigen Reaktion auf verzerrende Trainingsdaten oder weisen diese prinzipielle Beschränkungen auf, die durch die Parametrierung nicht ausgeglichen werden können, so besteht ein erhebliches Risiko, dass das spezifische Zusammenwirken des verwendeten Algorithmus mit den ihm zur Verfügung gestellten Trainingsdaten zu Verzerrungs- und Diskriminierungseffekten führt.[5] Dies wirft etliche Rechtsprobleme auf, deren Diskussion noch in ihren Anfängen steht.[6] Zwei wichtige Fragen sind dabei die nach den bereits geltenden rechtlichen Anforderungen an den Umgang mit Trainingsdaten einerseits, der Sinnhaftigkeit und etwaigen Ausgestaltung einer entsprechenden Regulierung andererseits.

Da viele Trainingsdaten personenbezogen sind oder ein Personenbezug zumindest nicht ausgeschlossen werden kann, liegt es nahe, beide Fragen (auch) aus

---

[5] Zu den Diskriminierungsrisiken des Einsatzes von KI z. B. *Ernst*, JZ 2017, 1026, 1032 ff.; *Wischmeyer*, AöR 143 (2018), 1, 26 ff.; *Steege*, MMR 2019, 715; *Wildhaber/Lohmann/Kasper*, ZSchwR I 2019, 459; *Mann/Matzner*, Big Data & Society 2019, 1; *Martini*, Blackbox Algorithmus, 2019, 47 ff., 73 ff.; *Wildhaber/Lohmann/Kasper*, ZSchwR I 2019, 459; *Mann/Matzner*, Big Data & Society 2019, 1; *Beck/Grunwald/Jacob/Matzner*, Künstliche Intelligenz und Diskriminierung. Whitepaper der Plattform Lernende Systeme, 2019; *Kolleck/Orwat*, Mögliche Diskriminierung durch algorithmische Entscheidungssysteme und maschinelles Lernen – ein Überblick. TAB-Hintergrundpapier Nr. 24, 2020; *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2020; *Hacker*, ZGE 2020, 239, 251 ff.; s. a. die Unterrichtung der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale, BT-Drs. 19/23700, 60 ff. sowie Entschließung des Europaparlaments v. 6.10.2021, P9_TA(2021)0405, in der die Risiken von Verzerrungen in Trainingsdaten betont werden (Rn. 8) und ihre Dokumentation gefordert wird (Rn. 19).

[6] S. bisher v. a. *Hacker*, ZGE 2020, 239; *ders.*, GRUR 2020, 1025 sowie den Beitrag in diesem Band; s. ferner aus v. a. datenschutzrechtlicher Perspektive *Heinemeyer*, CR 2019, 147; *Niemann/Kevekordes*, CR 2020, 17; *dies.*, CR 2020, 179; *Raji*, DuD 2021, 303; *Boenisch*, DuD 2021, 448; *Valkanova*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.1; *Kaulartz*, ebd., Kap. 8.9; *Vogel*, Künstliche Intelligenz und Datenschutz, 2022, 49 ff., 69 f.; zur Haftung für Trainingsdaten *Hacker*, ZGE 2020, 239, 249 ff.; *Zech*, NJW 2022, 502.

datenschutzrechtlicher Sicht zu analysieren. Dies kann wiederum aus einer eher objektivrechtlichen Perspektive erfolgen, die Datenschutz maßgeblich als Instrument zur Begrenzung von Datenmacht begreift,[7] oder aus der Perspektive der betroffenen Person im Sinne von Art. 4 Nr. 1 DSGVO, bei der es sich typischerweise um eine Verbraucherin oder einen Verbraucher handeln wird. Der Beitrag wählt die zweite Perspektive und untersucht – im Sinne des Leitthemas der Verbraucherrechtstage 2021 –, welchen Beitrag das Datenschutzrecht leisten kann, um eine vertrauenswürdige Verwendung von KI in Deutschland und Europa zu befördern. Der Text erläutert zunächst Interessenlagen und Herausforderungen, bevor die datenschutzrechtlichen Betroffenenrechte auf ihre Leistungsfähigkeit zum Schutz der betroffenen Person vor unangemessener und zu weitreichender Datenverarbeitung befragt werden. Im letzten Schritt wird diskutiert, ob die Unzulänglichkeiten des gerade datenschutzrechtlichen Zugriffs auf das Problem der Trainingsdaten regulatorisch angegangen werden sollten, und ob der Vorschlag der europäischen Kommission für ein „Gesetz über Künstliche Intelligenz"[8] (oftmals auch „KI-Verordnung" genannt; im Folgenden KOM-E) insoweit Verbesserungen bringen würde.

Noch während des europäischen Gesetzgebungsverfahrens hat sich der schleswig-holsteinische Gesetzgeber entschlossen, mit dem seit dem 15.4.2022 geltenden § 8 des schleswig-holsteinischen IT-Einsatz-Gesetz (ITEG SH)[9] eine erste verbindliche nationale Regulierung zu Trainingsdaten zu verabschieden.[10] Auch wenn eine verabschiedete KI-Verordnung diese Regelungen verdrängen bzw. modifizieren wird, ist dieser erste Schritt bemerkenswert; die Norm wird deshalb im Folgenden an geeigneten Stellen berücksichtigt.

---

[7] S. zu diesem Ansatz z. B. *v. Lewinski*, Die Matrix des Datenschutzes, 2014, 55 ff.; in historischer Perspektive *v. Lewinski*, in: Arndt u. a. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht, 2009, 201 ff.

[8] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union v. 21.4.2021, COM(2021) 206 final; zu Hintergründen und ersten Analysen s. z. B. *Veale/Borgesius*, CRi 2021, 97; *Geminn*, ZD 2021, 354; *Spindler*, CR 2021, 361; *Grützmacher*, CR 2021, 433; *Kau*, CR 2021, 498; *Kalbhenn*, ZUM 2021, 663; *Valta/Vasel*, ZRP 2021, 142; *Ebers*, RDi 2021, 588; *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188; *Rostalski/Weiss*, ZfDR 2021, 329; *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528; *Wiebe*, BB 2022, 899; zur Entwicklung *Hacker*, NJW 2020, 2142; breitere Analyse des Entwurfs mit Blick auf eine Regulierung von KI bei *Kau*, ZG 2021, 217; zu verbleibenden Regulierungsspielräumen der Mitgliedstaaten *Hornung*, DuD 2022, 561.

[9] Gesetz über die Möglichkeit des Einsatzes von datengetriebenen Informationstechnologien bei öffentlich-rechtlicher Verwaltungstätigkeit (IT-Einsatz-Gesetz – ITEG), GVBl. SH Nr. 5, 296; s. die Begründung, LT-Drs. SH 19/3267, 15 f., 69 f., 136 ff.

[10] Ein solches „Vorpreschen" nationaler Gesetzgeber lässt sich auch in anderen Regelungsbereichen mitunter beobachten, beispielsweise bei der IT-Sicherheitsregulierung (IT-Sicherheitsgesetz und NIS-Richtlinie) oder der Plattformregulierung (Netzwerkdurchsetzungsgesetz und Digital Services Act).

II. „Gute" Trainingsdaten

Ob Verbraucherschutz durch „gute" Trainingsdaten befördert werden kann, hängt zunächst von der Frage ab, was gute und was schlechte Trainingsdaten sind. Dies wird vielfach von den spezifischen Anforderungen zunächst des Trainings- und später des Einsatzszenarios des KI-Algorithmus abhängen. Verallgemeinernd lassen sich generische Anforderungen wie Repräsentativität und Aktualität festmachen.[11] Jedenfalls in erster Näherung bieten auch Art. 10 Abs. 3 und Abs. 4 KOM-E – sowie nunmehr als erste nationale Regelung § 8 Abs. 3 ITEG SH – sinnvolle Anhaltspunkte für die Frage, was qualitativ hochwertige Trainingsdaten ausmacht.

1. Begriff

Die Europäische Kommission schlägt in Art. 10 Abs. 3 S. 1 KOM-E vor, Trainings-, Validierungs- und Testdatensätze einheitlichen Anforderungen zu unterwerfen, soweit es sich um Hochrisiko-KI-Systeme (Art. 6 KOM-E)[12] handelt. Nach den Begriffsbestimmungen des KOM-E sind

- „Trainingsdaten" Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter und die Gewichte eines neuronalen Netzes angepasst werden (Art. 3 Nr. 29 KOM-E),
- „Validierungsdaten" Daten, die zum Bewerten des trainierten KI-Systems und zum Abstimmen seiner nicht lernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Überanpassung zu vermeiden; der Validierungsdatensatz kann ein separater Datensatz oder Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung sein (Art. 3 Nr. 30 KOM-E), und
- „Testdaten" Daten, die für eine unabhängige Bewertung des trainierten und validierten KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen (Art. 3 Nr. 31 KOM-E).

Diese Definitionen entsprechen einem üblichen Vorgehensmodell beim Training von KI-Systemen.[13] Für dieses Training steht in der Praxis eine gewisse Menge

---

[11] S. den Beitrag von *Abedjan* in diesem Band; s. ferner das Gutachten der *Datenethikkommission*, 2019, 94, 168 sowie aus rechtlicher Sicht näher *Hacker*, ZGE 2020, 239, 262 ff.

[12] Der KOM-E unterscheidet in einem risikobasierten Ansatz zwischen verbotenen Praktiken im Bereich der KI (Art. 5 KOM-E), Anforderungen an Hochrisiko-KI-Systeme (v.a. Art. 6–15 KOM-E) und sonstigen KI-Systemen; s. näher *Geminn*, ZD 2021, 354, 355 ff.; *Spindler*, CR 2021, 361, 362; *Valta/Vasel*, ZRP 2021, 142 f.; *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188, 1189 ff.; *Bomhard/Merkle*, RDi 2021, 276, 279 ff.; *Rostalski/Weiss*, ZfDR 2021, 329, 337 ff.; allgemein zu datenschutzrechtlichen Risikokriterien für KI *Rost*, DuD 2018, 558, 561 ff.

[13] *Niederée/Nejdl*, in: Ebers/Heinze/Krügel/Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik, Rechtshandbuch, 2020, § 2 Rn. 28 ff.; § 8 Abs. 1 ITEG SH spricht von Daten „zum Zweck der Entwicklung und des Trainings", ohne beide Begriffe allerdings zu definieren.

von Daten zur Verfügung, auf die das System angewendet werden kann (z. B. um ein Objekt in einem Bild zu identifizieren). Diese Menge wird in zwei Teilmengen aufgespalten: zum einen der Datensatz, der (als Trainingsdaten i. S. v. Art. 3 Nr. 28 KOM-E) zum initialen Training des Modells verwendet wird, zum anderen der – meist kleinere – Datensatz, mit dem (als Testdaten i. S. v. Art. 3 Nr. 31 KOM-E) nach Abschluss des Trainings geprüft wird, wie gut das Training funktioniert hat. Um dies beurteilen zu können, darf das trainierte System zuvor nicht mit den Testdaten in Berührung kommen. Die in Art. 3 Nr. 30 KOM-E geregelten Validierungsdaten sind ein Spezialfall der Trainingsdaten, mit denen das KI-System bewertet wird und seine nicht lernbaren Parameter sowie der Lernprozess abgestimmt werden. Dies bezieht sich insbesondere auf das Risiko einer Überanpassung („Overfitting"), bei der das System so stark auf die Trainingsdaten angepasst wurde, dass es auf anderen Daten nicht oder nicht in hinreichender Qualität funktioniert.

Im Ergebnis ist der Unterschied zwischen den drei Datentypen also eine reine Willensentscheidung desjenigen, der das System trainiert, validiert und testet – die Daten gehören nicht als solche in eine der drei Gruppen. Da alle drei Phasen zu einem Begriff des Trainings im weiteren Sinne gerechnet werden können (wenn das abschließende Testen nicht zufriedenstellend ausfällt, wird erneut trainiert; d. h. das Testen ist Teil des rekursiven Trainingszyklus), wird im Folgenden der Begriff der Trainingsdaten als Oberbegriff für die drei genannten Gruppen verwendet.[14] Soweit konkrete Bestimmungen des KOM-E thematisiert werden, folgt die Terminologie allerdings den Begriffsbestimmungen in Art. 3 Nr. 29–31 KOM-E.

Nach Art. 10 Abs. 3 S. 1 KOM-E müssen Trainings-, Validierungs- und Testdatensätze relevant, repräsentativ, fehlerfrei und vollständig sein. § 8 Abs. 3 ITEG SH formuliert völlig anders und verlangt, dass die bei der Entwicklung und beim Training – außerdem, über Art. 30 Abs. 3 KOM-E hinausgehend, auch beim Einsatz – der Systeme verwendeten Daten „nicht-diskriminierend, integer, objektiv und valide" sind. Diese völlige Überlappungsfreiheit der verwendeten Begriffe ist angesichts der Tatsache bemerkenswert, dass der KOM-E ein halbes Jahr vor dem Gesetzesentwurf zum ITEG SH veröffentlicht wurde; auch die Begründung nimmt (weder zu dieser Norm[15] noch an einer anderen Stelle überhaupt) auf den KOM-E Bezug. Wie groß die inhaltlichen Unterschiede der Begriffe sind, muss angesichts der Tatsache offenbleiben, dass weder die schleswig-holsteinische Begründung noch der KOM-E[16] Erläuterungen bieten.

Gemäß Art. 10 Abs. 3 S. 2 KOM-E haben Trainings-, Validierungs- und Testdatensätze geeignete statistische Merkmale aufzuweisen, gegebenenfalls auch

---

[14] S. zum Begriff auch *Niederée/Nejdl*, in: Ebers/Heinze/Krügel/Steinrötter (Fn. 13), § 2 Rn. 31.
[15] LT-Drs. SH 19/3267, 155.
[16] EG 44 S. 3 KOM-E wiederholt insoweit lediglich Art. 10 Abs. 3 S. 1 KOM-E.

bezüglich der Personen oder Personengruppen, auf die das Hochrisiko-KI-System bestimmungsgemäß angewandt werden soll. Diese Merkmale der Datensätze können durch einzelne Datensätze oder eine Kombination solcher Datensätze erfüllt werden (Art. 10 Abs. 3 S. 3 KOM-E). Ergänzt wird dies in Art. 10 Abs. 4 KOM-E durch Anforderungen mit Bezug auf die spätere Einsatzumgebung. Die Trainings-, Validierungs- und Testdatensätze müssen danach, soweit dies für die Zweckbestimmung erforderlich ist, den Merkmalen oder Elementen entsprechen, die für die besonderen geografischen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind.

2. Interessenlagen

In etlichen Situationen werden sowohl der datenschutzrechtlich Verantwortliche (also typischerweise der Nutzer des KI-Systems)[17] als auch die betroffenen Personen ein Interesse an der Einhaltung dieser Vorgaben, also an der Verwendung qualitativ hochwertiger Trainingsdaten haben. Irrelevante, nicht repräsentative, fehlerhafte oder unvollständige Trainingsdaten zu verwenden, kann zu – im weitesten Sinne – falschen oder unangemessenen Ergebnissen führen.[18] Hieran haben typischerweise weder der Nutzer des KI-Systems noch derjenige ein Interesse, der Adressat einer KI-basierten Entscheidung wird.[19] Allerdings sind die Folgen derartiger falscher oder unangemessener Ergebnisse vielfach ungleich verteilt. Aus Sicht des Nutzers kann es sich um ein prinzipielles „GIGO"-Problem („Garbage In, Garbage Out") handeln, das zur Unbrauchbarkeit des gesamten Systems führt. Wenn demgegenüber falsche und unangemessene Ergebnisse lediglich in Einzelfällen auftreten, mag es aus Perspektive des Nutzers immer noch sinnvoll sein, das System zu verwenden, weil es beispielsweise kostengünstiger als die manuelle Bearbeitung ist oder im Durchschnitt bessere Ergebnisse liefert.[20] Den im konkreten Einzelfall negativ Betroffenen, beispielsweise diskriminierten Verbraucherinnen und Verbrauchern, wird eine solche Effizienzbetrachtung hingegen nicht gerecht.

Aus einer datenschutzrechtlichen Perspektive sollte außerdem nicht übersehen werden, dass auch der Einsatz besonders guter Trainingsdaten ein Problem für

---

[17] Hier verwendet i. S. v. Art. 3 Nr. 4 KOM-E: eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet.

[18] S. zu den Diskriminierungsrisiken die Nachweise in Fn. 5; zu Haftungsfragen *Hacker*, ZGE 2020, 239, 249 ff.; *Zech*, NJW 2022, 502.

[19] Zu den Interessen und den mit ihnen verbundenen „regulatorischen Risiken" s. *Hacker*, ZGE 2020, 239, 243 ff.

[20] Insoweit sind Anforderungen an die Qualität von Trainingsdaten wie in Art. 10 Abs. 5 KOM-E nur auf den ersten Blick „eigentlich selbstverständliche Anforderungen" (so *Spindler*, CR 2021, 361, 367).

Verbraucherinnen und Verbraucher sein kann. Qualitativ hochwertige KI-basierte Entscheidungen können zu ihren Gunsten, sehr leicht aber auch zu ihren Lasten eingesetzt werden. Dies betrifft zum einen den privaten Bereich, wenn beispielsweise mittels individualisierter Verhaltensprofile Vorhersagen über das Konsumverhalten getroffen werden, um dieses im Interesse der Anbieter zu beeinflussen.[21] Zum anderen ist auch der Bereich der politischen Willensbildung betroffen, etwa im Bereich von Mikrotargeting im Wahlkampf.[22] Diese und andere Beispiele machen deutlich, dass sich die Interessen von Verbraucherinnen und Verbrauchern auf keinen Fall darin erschöpfen, nur Adressaten von mit guten Daten trainierten KI-Systemen zu werden. Vielmehr kommt hier zum Tragen, dass eines der Ziele des Datenschutzrechts die Verhinderung zu starker Machtungleichgewichte ist; informationelle Selbstbestimmung ist gefährdet, wenn die betroffenen Personen nicht mehr wissen „wer was wann und bei welcher Gelegenheit über sie weiß",[23] und die Wissenden – also einflussreiche staatliche oder private Akteure – mittels KI-Algorithmen ihre Informationsmacht noch weiter ausbauen.

Unabhängig von der Frage, ob es sich um gute oder schlechte Trainingsdaten handelt, kann aus datenschutzrechtlicher Sicht auch das Training selbst ein Problem darstellen. Es geht dann nicht um Fragen des späteren Einsatzes eines mehr oder weniger gut trainierten KI-Systems in der Praxis, sondern um die vorgelagerte Verwendung personenbezogener Daten, einschließlich derjenigen solcher betroffenen Personen, die mit dem späteren KI-System gar nicht in Kontakt kommen. Die Risikolagen liegen dementsprechend auf einer anderen Ebene: Die ursprünglich zu anderen Zwecken erhobenen Daten werden nunmehr für das Training verarbeitet, länger aufbewahrt, an Forschungs- und Entwicklungspartner übermittelt oder sind schlimmstenfalls beim späteren Einsatz des KI-Systems erkennbar.[24] Diese Vorgänge können die Missbrauchsgefahren erheblich ansteigen lassen.

III. Betroffenenrechte in der Datenschutz-Grundverordnung

Datenschutzrecht gilt nur für personenbezogene Daten (Art. 2 Abs. 1 DSGVO, § 1 Abs. 1 S. 1 BDSG und entsprechende Normen der Landesdatenschutzgesetze). Daraus ergeben sich zwei Anwendungsfälle für die datenschutzrechtliche Perspektive auf KI-Trainingsdaten: zum einen das Training mit personenbezogenen Daten, zum anderen der Einsatz (wie auch immer) trainierter KI-Systeme in spä-

[21] S. etwa *Gausling*, ZD 2019, 335; zur Dynamisierung von Preisen etwa *Bernhardt*, NZKart 2019, 314; zu Transparenzanforderungen aus Verbrauchersicht *Gerpott/Mikolas*, InTeR 2021, 122.

[22] Dazu aus rechtlicher Sicht *Richter*, in: FS für Alexander Roßnagel, 2020, 303 ff.; *Radtke*, K&R 2020, 479.

[23] BVerfGE 65, 1 (43) – Volkszählung.

[24] Zu diesem Problem eines Personenbezugs von KI-Modellen s. *Kaulartz*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.9 Rn. 2 ff.

teren Anwendungen unter Einsatz personenbezogener Daten. In beiden Fällen können die Betroffenenrechte nach der Datenschutz-Grundverordnung eine Rolle spielen.

1. Die datenschutzrechtlichen Betroffenenrechte

Das Datenschutzrecht kennt schon seit vielen Jahren ein relativ festes Set von Betroffenenrechten. Bereits das erste Bundesdatenschutzgesetz aus dem Jahre 1977 umfasste Rechte auf Auskunft, Berichtigung, Sperrung und Löschung (verankert in § 4 i. V. m. §§ 13, 14, 26, 27, 32, 33 BDSG 1977). Auf europäischer Ebene enthielt die Datenschutz-Richtlinie 95/46/EG ebenfalls derartige Rechte (Art. 12) sowie Informationspflichten (Art. 10 und Art. 11), ein Widerspruchsrecht (Art. 14) und Rechte bei automatisierten Einzelentscheidungen (Art. 15).

Die Datenschutz-Grundverordnung hat diese Rechte im Grundsatz übernommen, die entsprechenden Bestimmungen jedoch stark ausgebaut, erweitert und präzisiert. Dies hat zu einer Fülle von neuen Streitfragen geführt, die an dieser Stelle nicht diskutiert werden können.[25] Im Überblick: Art. 12 DSGVO regelt nunmehr vor die Klammer gezogen Anforderungen an transparente Information, Kommunikation und Modalitäten für die Ausübung der Betroffenenrechte. Sodann folgen Informationspflichten für den Fall der Erhebung personenbezogener Daten bei der betroffenen Person (Art. 13 DSGVO) und bei anderen Stellen oder Gelegenheiten (Art. 14 DSGVO). Mit diesen proaktiven Informationspflichten korrespondiert das ebenfalls transparenzorientierte Auskunftsrecht in Art. 15 DSGVO.

Weiterhin enthalten sind in neu gefasster Form die Rechte auf Berichtigung (Art. 16 DSGVO), auf Löschung (Art. 17 DSGVO; nunmehr synonym – und gegenüber dem Norminhalt deutlich überschießend – „Recht auf Vergessenwerden" genannt), auf Einschränkung der Verarbeitung (Art. 18 DSGVO, vormals Sperrung), auf Widerspruch (Art. 21 DSGVO) sowie im Bereich der automatisierten Entscheidungen im Einzelfall einschließlich Profiling (Art. 22 DSGVO). Eine echte, das Datenschutzrecht in Richtung Wettbewerbs-, Kartell- und Verbraucherschutzrecht transzendierende Neuerung ist das Recht auf Datenübertragbarkeit (Art. 20 DSGVO).[26] Art. 23 DSGVO gestattet Beschränkungen der Betroffenen-

---

[25] S. nur zur Frage der Reichweite des Auskunftsrechts in Art. 15 DSGVO: *Kremer*, CR 2018, 560; *Zikesch/Sörup*, ZD 2019, 239; *Brink/Joos*, ZD 2019, 483; *Wybitul/Brams*, NZA 2019, 672; *Schulte/Welge*, NZA 2019, 1110; *Koreng*, NJW 2021, 2692; *Krämer/Burghoff*, ZD 2022, 428; *Gaul/Pitzer*, DB 2022, 1321; *Lembke/Fischels*, NZA 2022, 513. Die Norm beschäftigt inzwischen umfangreich die Justiz; s. nur aus der höchstrichterlichen Rechtsprechung BGH, NJW 2021, 2726; ZD 2022, 326; BVerwG, NVwZ 2021, 80; BAG, NJW 2021, 2379; BFHE 274, 496; DStRK 2020, 54; der BGH hat Fragen zum kostenfreien Auskunftsanspruch eines Patienten gegen seinen Arzt dem EuGH vorgelegt, s. BGH, GesR 2022, 360.

[26] Zu den Neuerungen der Betroffenenrechte schon *Hornung*, in: Hill/Schliesky (Hrsg.), Die Neubestimmung der Privatheit. E-Volution des Rechts- und Verwaltungssystems IV, 2014, 139 ff.; s. ferner *Reich*, VuR 2018, 293.

rechte durch Rechtsvorschriften der Union oder der Mitgliedstaaten, wenn die Beschränkungen den Wesensgehalt der Grundrechte und Grundfreiheiten achten sowie in einer demokratischen Gesellschaft notwendig und verhältnismäßig zur Sicherung enumerativ aufgelisteter gegenläufiger Interessen sind.

Im Grundsatz greifen alle diese Betroffenenrechte in beiden oben genannten KI-Szenarien, also sowohl beim Training von KI-Systemen mit personenbezogenen Daten als auch beim Einsatz von KI-Systemen in personenbezogenen Anwendungen.[27] Allerdings kommen nicht in jedem Fall die Besonderheiten von KI zu tragen. Die folgende Darstellung konzentriert sich deshalb auf einige zentrale Fragestellungen.

2. Ansprüche gegen die Verwendung zu Trainingszwecken

Im Trainingsszenario wäre aus verbraucherschutzrechtlicher Perspektive ein Anspruch gegen die Verwendung der „eigenen" personenbezogenen Daten zu Testzwecken das stärkste Betroffenenrecht. Da das Datenschutzrecht keinen expliziten Unterlassungsanspruch kennt, kommen derartige Ansprüche typischerweise im Gewande des Löschungsanspruchs daher.[28] Personenbezogene Daten sind insbesondere zu löschen, wenn sie unrechtmäßig verarbeitet werden (Art. 17 Abs. 1 lit. d DSGVO). Dies verweist auf das datenschutzrechtliche Verbotsprinzip,[29] rechtlich als Grundsatz der Rechtmäßigkeit in Art. 5 Abs. 1 lit. a und Art. 6 DSGVO verankert. Danach ist für jede Verarbeitung personenbezogener Daten eine sie legitimierende Rechtsgrundlage erforderlich.

a) Zulässigkeitstatbestände

Mangels eines expliziten Erlaubnistatbestands für die Verarbeitung zum Training von KI-Algorithmen richtet sich die datenschutzrechtliche Zulässigkeit nach den allgemeinen Regeln des Art. 6 DSGVO;[30] dies gilt jedenfalls vorbehaltlich einer

---

[27] S. näher *Niemann/Kevekordes*, CR 2020, 179, 181 ff.; *Krügel/Pfeiffenbring*, in: Ebers/Heinze/Krügel/Steinrötter (Fn. 13), § 11 Rn. 29 ff.

[28] Dies gilt auch für den EuGH, etwa in den Entscheidungen zum Recht auf Vergessenwerden (EuGH, Urt. v. 13.5.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google Spain; Urt. v. 24.9.2019, Rs. C-136/17, ECLI:EU:C:2019:773 – CG u. a.; Urt. v. 24.9.2019, Rs. C-507/17, ECLI:EU:C:2019:772 – Google; dazu Hornung, in: FS für Alexander Roßnagel, 2020, 379 ff.). Die Frage, ob es – beispielsweise als Minus zum Löschungsanspruch nach Art. 17 DSGVO und insoweit in diesem verankert – einen allgemeinen datenschutzrechtlichen Unterlassungsanspruch gibt, kann hier nicht vertieft werden, s. dazu LG Frankfurt, ZD 2019, 410; LG Wiesbaden, MMR 2022, 313; *Leibold/Laoutoumai*, ZD-Aktuell 2021, 05583; *Worms*, in: BeckOK Datenschutzrecht, Art. 17 Rn. 77a f.

[29] S. z. B. *Karg*, DuD 2013, 75 ff.; kritisch zur Terminologie *Roßnagel*, NJW 2019, 1.

[30] S. dazu *Niemann/Kevekordes*, CR 2020, 17, 22 ff.; allgemeiner zur Zulässigkeit der Datenverarbeitung zu Testzwecken *Heinemeyer*, CR 2019, 147; allgemeiner für KI-Systeme *Conrad*, InTeR 2021, 147 (v. a. zur Einwilligung). Für wissenschaftliche Forschung gelten Sonderregeln, die hier ausgeklammert werden, s. z. B. *Meszaros/Ho*, Computer Law & Security Review 41 (2021), 105532.

Sperrwirkung von Art. 54 KOM-E (s. u. III 2. d). Von den dort genannten Alternativen dürften etliche nur selten einschlägig werden. Denn die Verarbeitung personenbezogener Daten zum Training von KI-Systemen wird nur in Ausnahmefällen zur Erfüllung einer rechtlichen Verpflichtung (lit. c), zum Schutz lebenswichtiger Interessen (lit. d) oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (lit. e) erforderlich sein. Die Erforderlichkeit zur Erfüllung eines Vertrags (Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO) kommt in Betracht, wenn das Training selbst Vertragsgegenstand ist oder es um eine personalisierte Dienstleistung geht, die nur auf der Basis eines Trainings mit den personenbezogenen Daten der betroffenen Person angeboten werden kann. Allerdings ist die Rechtsgrundlage sodann auf das Training mit den personenbezogenen Daten des Vertragspartners beschränkt; die Verarbeitung von Daten Dritter kann nicht auf Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO gestützt werden.

In den meisten Fällen wird es um die Frage einer Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a i. V. m. Art. 7 und Art. 4 Nr. 11 DSGVO), das Problem gleichgewichtiger oder überwiegender berechtigter Interessen eines privaten Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO) bzw. Verhältnismäßigkeitsüberlegungen im Rahmen von Verarbeitungsgeneralklauseln für den öffentlichen Bereich gehen (Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2 und 3 DSGVO i. V. m. § 3 BDSG bzw. entsprechenden Normen der LDSGe). Der Weg über Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO versagt freilich, soweit es um besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO geht.[31] Denn dann greift das dort geregelte zusätzliche Verarbeitungsverbot, das nur in den Fällen des Art. 9 Abs. 2 DSGVO überwunden werden kann. Dessen Ausnahmetatbestände enthalten keine allgemeine Interessenabwägung wie in Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Die Einwilligung kann hingegen weiterhin verwendet werden, muss nach Art. 9 Abs. 2 lit. a DSGVO aber ausdrücklich erteilt werden. Die übrigen Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO können in einigen Fällen für die Verarbeitung als KI-Trainingsdaten einschlägig sein (zum Beispiel lit. e, wenn die betroffene Person die Daten offensichtlich selbst öffentlich gemacht hat), dies ist aber im Einzelfall zu beurteilen.

b) Zweckänderung nach der DSGVO

Im Rahmen der erforderlichen Einzelfallprüfung sind verschiedene Szenarien zu unterscheiden. Gerade mit einer Einwilligung nach Art. 7 i. V. m. Art. 4 Nr. 11 DSGVO kann der Verantwortliche Daten zum originären Zweck des Trainings

[31] Dies umfasst personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Zum Problem der Anwendung auf Machine Learning s. *Niemann/Kevekordes*, CR 2020, 179.

von KI-Algorithmen erheben und weiterverarbeiten. Unter bestimmten Voraussetzungen ist aber auch die Zweckänderung für Daten möglich, die zunächst zu einem anderen Zweck erhoben wurden. Schließlich kann es auch darum gehen, Daten an andere Verantwortliche weiterzugeben, um beispielsweise das Wissen über selten auftretende Anomalien (etwa Unfallursachen im Straßenverkehr) mit anderen zu teilen und diesen ebenfalls die Möglichkeit zu geben, ihre Algorithmen entsprechend zu trainieren.

In der Praxis wird es oftmals um den Fall der Zweckänderung gehen, wenn beispielsweise bestehende Kundendatenbanken, Sammlungen mit Behandlungsinformationen von Patienten oder Verwaltungsakten bereits über einen längeren Zeitraum angelegt wurden und ihr Einsatz zum Training neuer Algorithmen nunmehr als vielversprechend erscheint.[32] Der in Art. 5 Abs. 1 lit. b DSGVO geregelte Grundsatz der Zweckbindung enthält eine Privilegierung der Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke; diese Verarbeitung gilt als nicht unvereinbar mit dem ursprünglichen Zweck, wenn Sicherungsmittel nach Art. 89 Abs. 1 DSGVO ergriffen werden.[33] Jenseits dieser Fälle ist jedoch eine Prüfung erforderlich, ob der neue Verarbeitungszweck mit dem ursprünglichen „vereinbar" ist. Hierfür gibt Art. 6 Abs. 4 DSGVO Kriterien vor.

Auch diese Vorschrift wirft etliche Probleme auf.[34] Für die hier diskutierte Konstellation ist insbesondere wichtig, dass die risikobezogenen Abwägungskriterien nur teilweise so verallgemeinert werden können, dass sie pauschale Argumente für die Zweckänderung umfangreicher Datenbestände liefern. Dies trifft beispielsweise auf die geeigneten Garantien wie Verschlüsselung oder Pseudonymisierung zu (Art. 6 Abs. 4 lit. d DSGVO), weil diese durch den Verantwortlichen einheitlich angewendet und dementsprechend einheitlich in die Abwägung eingebracht werden können. Es gilt aber bereits nur noch mit Einschränkungen – d. h. bei ähnlich strukturierten Daten – für die Kriterien der Verbindung zwischen altem und neuem Zweck (lit. a), des Erhebungszusammenhangs (lit. b) und die Frage, ob besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO verarbeitet werden (lit. c). Hier können sich bereits deutliche Unterschiede zwischen ein-

---

[32] *Niemann/Kevekordes*, CR 2020, 17, 24; *Valkanova*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.1 Rn. 3 ff.

[33] Zu dieser Privilegierung s. *Werkmeister/Schwaab*, CR 2019, 85; *Weichert*, ZD 2020, 18; am Beispiel von Patientendaten *Spitz/Jungkunz/Schickhardt/Cornelius*, MedR 2021, 499; allgemeiner zum Datenschutz in der Forschung *Roßnagel*, ZD 2019, 157.

[34] Dies betrifft schon die grundsätzliche Frage, ob im Falle der Einschlägigkeit von Art. 6 Abs. 4 DSGVO die Weiterverarbeitung sich auf die ursprüngliche Rechtsgrundlage stützt (dafür z. B. *Roßnagel*, in Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 6 Abs. 4 Rn. 12 m. w. N.; *Kühling/Martini*, EuZW 2016, 448, 451; *Hornung/Hofmann*, ZD-Beilage 4/2017, 8) oder zusätzlich eine weitere Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO erforderlich ist (so *Schantz*, NJW 2016, 1841, 1844; *Albrecht*, CR 2016, 88, 92).

zelnen betroffenen Personen ergeben. Die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person (Art. 6 Abs. 4 lit. d DSGVO) werden sogar oftmals eine Betrachtung ihrer konkreten Umstände erfordern. Im Ergebnis wird es deshalb schwierig sein, die einheitliche Zweckänderung für große Datenbestände nach diesen Kriterien übergreifend zu legitimieren. Zu diesem Problem der Einzelfallabhängigkeit tritt hinzu, dass die Sensibilität der Daten gerade im Anwendungsbereich von Art. 9 DSGVO (beispielsweise bei Gesundheitsdaten) die Zweckänderung deutlich einschränkt.

c) Zweckänderung im KOM-E

Bedeutsam ist deshalb, dass Art. 6 Abs. 4 DSGVO neben der Zweckänderung aufgrund des erläuterten Vereinbarkeitstests auch die Möglichkeit vorsieht, dass die Zweckänderung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift der Union oder der Mitgliedstaaten legitimiert wird. Für entsprechende Normen gelten dieselben Anforderungen wie für eine Einschränkung der Betroffenenrechte nach Art. 23 DSGVO (s. o.). Solche Rechtsvorschriften schlägt die Kommission in Art. 10 Abs. 5 KOM-E sowie in Art. 54 Abs. 1 KOM-E vor.[35]

aa) Vermeidung von Verzerrungen

Nach Art. 10 Abs. 5 KOM-E dürfen Anbieter von Hochrisiko-KI-Systemen Daten nach Art. 9 Abs. 1 DSGVO[36] verarbeiten, soweit dies für die Beobachtung, Erkennung und Korrektur von „Verzerrungen" im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist. Dies ist ein hoher Maßstab, der über die übliche Erforderlichkeitsprüfung im Datenschutzrecht hinausreicht. Die Anbieter müssen außerdem angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen, wozu auch technische Beschränkungen einer Weiterverwendung und modernste Sicherheits- und Datenschutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung gehören,

[35] Im Folgenden wird die Frage ausgeklammert, ob die vorgeschlagenen Regelungen tatsächlich eines der Ziele in Art. 23 Abs. 1 DSGVO verfolgen. Für Art. 10 Abs. 5 KOM-E kommt Art. 23 Abs. 1 lit. i DSGVO in Betracht, da Verzerrungen die Rechte und Freiheiten natürlicher Personen beeinträchtigen können. Letztlich spielt die Frage aber keine Rolle, weil die Regelungen des KOM-E spezieller sind und (entgegen der Formulierung in Art. 6 Abs. 4 DSGVO) nicht den Vorgaben der DSGVO folgen müssen. Diese entsprechen zwar hinsichtlich der Verhältnismäßigkeitsanforderungen im Wesentlichen den Vorgaben in Art. 52 Abs. 1 GRCh. Dieser kennt aber keine enumerative Liste zulässiger Gemeinwohlziele.

[36] Zusätzlich werden Daten nach Art. 10 RL (EU) 2016/680 und Art. 10 Abs. 1 VO (EU) 2018/1725 genannt. Diese regeln allerdings dieselben Daten und unterscheiden sich nur hinsichtlich des persönlichen Anwendungsbereichs (Strafverfolgungsbehörden bzw. Organe, Einrichtungen und sonstige Stellen der Union; beides ist nach Art. 2 Abs. 2 lit. d und Abs. 3 DSGVO von dieser ausgenommen). Da der persönliche Anwendungsbereich allerdings in Art. 10 Abs. 5 KOM-E ohnehin anders bestimmt wird, erschließt sich der Mehrfachverweis nicht.

wenn der verfolgte Zweck durch eine Anonymisierung erheblich beeinträchtigt würde. Mit der Verpflichtung auf „modernste" Maßnahmen wird ein sehr hoher Standard vorgegeben, der über den Stand der Technik hinausreichen und dem aus dem deutschen Recht bekannten Stand von Wissenschaft und Technik entsprechen wird.[37]

Art. 10 Abs. 5 KOM-E zielt erkennbar auf die Vermeidung von Ungleichheitseffekten und Diskriminierungen sowie darüber hinaus auf die allgemeine Qualität von Entscheidungs(unterstützung)systemen mithilfe von KI. Denn um herauszufinden, ob ein KI-System Menschen beispielsweise nach ihrer rassischen und ethnischen Herkunft, ihren genetischen oder biometrischen Daten oder ihrer Gesundheit ungleich behandelt, wird man – vorbehaltlich der Verfügbarkeit synthetischer Trainingsdaten – typischerweise nicht umhinkommen, personenbezogene Daten zu genau diesen Merkmalen zu verarbeiten.[38] Der Vorschlag entbindet als gesetzliche Verarbeitungsbefugnis die Anbieter davon, von jeder betroffenen Person eine ausdrückliche Einwilligung einzuholen. Um diese Einschränkung der Rechtsposition von Verbraucherinnen und Verbrauchern auch grundrechtlich rechtfertigen zu können, hat die Kommission hohe technische und organisatorische Kompensationsmaßnahmen vorgesehen. Insofern ist die Vorschrift ein sinnvoller Regelungsansatz, wirft in der vorgeschlagenen Form allerdings dennoch mehrere Fragen auf.

Erstens ist nicht eindeutig, was mit „Verzerrungen" gemeint ist. Nach Art. 10 Abs. 2 lit. f KOM-E müssen Daten-Governance- und Datenverwaltungsverfahren eine Untersuchung „im Hinblick auf mögliche Verzerrungen (Bias)" umfassen. Es geht also um Schieflagen, Bevorzugungen und Benachteiligungen sowie diskriminierende Effekte – der Bezug zwischen Verzerrungen und Diskriminierungen kommt in EG 33 S. 1 und besonders deutlich in EG 44 S. 6 KOM-E zum Ausdruck.[39] Damit ist die Zielrichtung der Regelung umschrieben. Was genau (relevante) Verzerrungen ausmacht und umfasst, verbleibt dennoch deutlich im Unklaren.

Zweitens erstreckt sich Art. 10 Abs. 5 KOM-E nur auf Daten nach Art. 9 Abs. 1 DSGVO. Es bleibt also offen, inwieweit die Anbieter zur Vermeidung von Verzerrungen auch „einfache" personenbezogene Daten verarbeiten dürfen. Für einen Umkehrschluss, also ein Verarbeitungsverbot, gibt es keinen Anhaltspunkt im KOM-E; ein solches Verbot der Verarbeitung einfacher Daten wäre angesichts der Verarbeitungsbefugnis für sensible Daten auch nicht zu rechtfertigen. In diese Richtung deutet auch EG 44 S. 6 KOM-E, demzufolge die Anbieter angesichts des

---

[37] S. dazu allgemein BVerfGE 49, 89 (136); BVerfG, NJW 1980, 759, 761 f.; BVerwGE 92, 185 (196); BVerwGE 106, 115; *Seibel*, NJW 2013, 3000, 3003; aus datenschutzrechtlicher Perspektive *Bartels*/*Backer*, DuD 2018, 214, 215.

[38] Dazu *Žliobaitė*/*Custers*, Artificial Intelligence and Law 24 (2016), 183.

[39] S. a. das Gutachten der *Datenethikkommission*, 2019, 231.

erheblichen öffentlichen Interesses „auch" besondere Kategorien personenbezogener Daten verarbeiten dürfen, um Verzerrungen in Hochrisiko-KI-Systemen zu beobachten, zu erkennen und zu korrigieren. Die Kommission geht also offenbar davon aus, dass andere Daten auf Basis anderer Rechtsgrundlagen ebenfalls verarbeitet werden können. Gegen den Willen der betroffenen Personen kommt dies insbesondere auf Basis einer Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO bzw. im Rahmen von Generalklauseln wie Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2 und 3 DSGVO i. V. m. § 3 BDSG in Betracht (s. o.). Im Rahmen der entsprechenden Abwägungen sind zwar wie bei Art. 10 Abs. 5 KOM-E technische und organisatorische Maßnahmen des Verantwortlichen zu berücksichtigen.[40] Es wäre aber vorzugswürdig, wenn der Gesetzgeber die Verarbeitungsbefugnis und spezifische, KI-bezogene Abwägungskriterien auch für normale personenbezogene Daten in der Verordnung regeln würde.

Eine ähnliche Frage ergibt sich drittens aus der Beschränkung des Vorschlags auf Hochrisiko-KI-Systeme. Verzerrungseffekte können auch bei KI-Systemen eintreten, die nicht in diese Kategorie fallen. Da es sich bei der Risikokategorisierung um eine typisierende Einordnung handelt, kann die Verzerrung in atypischen Einzelfällen für Verbraucherinnen und Verbraucher durchaus gravierende Folgen haben, obwohl es sich nicht um ein Hochrisiko-KI-System handelt. Gegen eine Ausweitung der Verarbeitungsbefugnis in Art. 10 Abs. 5 KOM-E auf alle KI-Systeme lässt sich (sowohl rechtspolitisch als auch hinsichtlich einer Analogie) allerdings anführen, dass der Bedarf nach einer Verarbeitung von Daten nach Art. 9 Abs. 1 DSGVO bei Hochrisiko-KI-Systemen deutlich größer ist, da diese eben mit typisiert erhöhten Risiken für Verbraucherinnen und Verbraucher verbunden sind. Insofern handelt es sich weniger um eine Abwägung zwischen den Interessen der Anbieter bzw. Nutzer des KI-Systems im Verhältnis zu den betroffenen Personen, sondern um eine Abwägung zwischen den Interessen der späteren Adressaten des Hochrisiko-KI-Systems einerseits und der betroffenen Personen andererseits, deren Daten zur Vermeidung von Verzerrungen verarbeitet werden sollen. Angesichts dieser Gemengelage sollte der europäische Gesetzgeber die Frage aber explizit entscheiden. Dies gilt insbesondere, weil eine Analogie zu Art. 10 Abs. 5 KOM-E für nicht erfasste, „normale" KI-Systeme aufgrund des risikoklassenorientierten Regelungsansatzes und der detaillierten Vorschläge der Kommission zwar zweifelhaft, methodisch aber immerhin möglich wäre.

bb) KI-Reallabore

Art. 54 Abs. 1 KOM-E enthält eine detaillierte Befugnis zur Zweckänderung von Daten, die rechtmäßig für andere Zwecke erhoben wurden; sie ist dementspre-

[40] S. allgemein zur Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO z. B. *Robrahn/Bremert*, ZD 2018, 291; *Herfurth*, ZD 2018, 514.

chend ausweislich EG 72 S. 4 KOM-E ausdrücklich als Regelung im Sinne von Art. 6 Abs. 4 DSGVO zu sehen. Diese dürfen in einem „KI-Reallabor" verarbeitet werden, um innovative KI-Systeme zu entwickeln oder zu erproben, wenn diese ein erhebliches öffentliches Interesse im Bereich der Straftatbekämpfung, der öffentlichen Sicherheit und öffentlichen Gesundheit oder des Umweltschutzes verfolgen. Anders als Art. 10 Abs. 5 KOM-E ist die Regelung nicht auf Daten nach Art. 9 Abs. 1 DSGVO beschränkt, sondern gestattet umfassend die Verarbeitung der personenbezogenen Daten von Verbraucherinnen und Verbrauchern als datenschutzrechtlich betroffene Personen.[41] Art. 54 Abs. 1 KOM-E enthält sodann eine Vielzahl insbesondere organisatorischer Anforderungen an die Datenverarbeitung sowie eine Löschpflicht, um die Grundrechte der betroffenen Personen zu schützen.

Die Regelung stellt im Ergebnis erkennbar hohe Anforderungen an die Zweckänderung. Welche Relevanz sie erlangen wird, hängt maßgeblich davon ab, wie die konkrete Ausgestaltung der KI-Reallabore ausfallen wird. Nach Art. 53 Abs. 1 KOM-E werden sie von den zuständigen Behörden eines oder mehrerer Mitgliedstaaten oder vom europäischen Datenschutzbeauftragten eingerichtet. Sie bieten eine kontrollierte Umgebung, um die Entwicklung, Erprobung und Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem „spezifischen Plan" zu erleichtern.[42] Die Modalitäten und Bedingungen für den Betrieb der KI-Reallabore werden allerdings erst nach Art. 53 Abs. 6 KOM-E in Durchführungsrechtsakten der Kommission festgelegt. Ob Entwickler und Anbieter von KI-Systemen von der Option einer Entwicklung unter „direkter Aufsicht und Anleitung der zuständigen Behörden" (Art. 53 Abs. 1 S. 2 KOM-E) Gebrauch machen werden, dürfte maßgeblich von dieser konkreten Ausgestaltung abhängen.

d) Exkurs: Zweckänderung nach § 8 Abs. 1 und 2 ITEG SH

Eine deutlich weitergehende Befugnis zur Zweckänderung als in Art. 10 Abs. 5 und Art. 54 Abs. 1 KOM-E enthält § 8 ITEG SH. § 8 Abs. 1 S. 1 ITEG SH legitimiert die Verarbeitung von (personenbezogenen und nicht personenbezogenen) Daten durch Träger der öffentlichen Verwaltung zum Zweck der Entwicklung und des Trainings von „datengetriebenen Informationstechnologien" (dies sind der Sache nach KI-Systeme).[43] § 8 Abs. 1 S. 2 ITEG SH beschränkt die Verarbeitung perso-

[41] Kritisch *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188, 1192.

[42] S. zu diesen „regulatory sandboxes" *Spindler*, CR 2021, 361, 371.

[43] § 3 Abs. 1 Nr. 1 ITEG SH definiert datengetriebene Informationstechnologien als Basisdienste, Fachverfahren oder Fachanwendungen, die zur effizienten Lösung einer speziellen Aufgabe oder einer komplexen Fragestellung auf Grundlage eines Datensatzes mit Hilfe spezieller Systeme, wie künstlicher neuronaler Netze und maschineller Lernverfahren, eingesetzt werden und ohne aktiven Eingriff Parameter der Entscheidungsfindung weiterentwickeln. Das Gesetz verwendet also nicht den Begriff der KI, regelt diese aber der Sache nach. Dies ist auch Absicht des Gesetzgebers, s. ausdrücklich LT-Drs. SH 19/3267, 15 f.

nenbezogener Daten zu Zwecken des Trainings (nicht der Entwicklung) sodann auf solche Fälle, in denen ein effektives Training nur mit unverhältnismäßigem Aufwand auf andere Weise erfolgen kann. Dies dürfte der Sache nach dem verschärften Maßstab der unbedingten Erforderlichkeit in Art. 10 Abs. 5 KOM-E entsprechen.

§ 8 Abs. 2 S. 1 ITEG SH beschränkt sodann den Kreis derjenigen Daten, die einer Zweckänderung unterzogen werden dürften. Wenn personenbezogene Daten zu Trainingszwecken verarbeitet werden sollen oder nicht auszuschließen ist, dass personenbezogene Daten betroffen sein könnten, so dürfen nur solche Daten verarbeitet werden, die im Zusammenhang mit der zu trainierenden Aufgabenwahrnehmung erhoben und gespeichert wurden. Ein Datenaustausch über verschiedene Bereiche der öffentlichen Verwaltung hinweg ist damit ausgeschlossen oder zumindest auf solche Bereiche beschränkt, bei denen dieselbe Aufgabe erfüllt wird. § 8 Abs. 2 S. 2 ITEG SH enthält die Vorgabe, die Daten vor einer Verarbeitung zu Trainingszwecken zu pseudonymisieren, sofern der Zweck dadurch nicht verhindert wird. Dies ist in § 10 Abs. 5 KOM-E ebenfalls enthalten, dort werden aber weitergehende technische und organisatorische Maßnahmen angeordnet (s. o.).

Art. 10 Abs. 5 KOM-E und § 8 ITEG SH weisen zwei entscheidende Unterschiede auf. Zum einen ist Art. 10 Abs. 5 KOM-E – wie die meisten Vorgaben des Entwurfs – auf Hochrisiko-KI-Systeme beschränkt, während § 8 ITEG SH die Zweckänderung für alle KI-Systeme in der öffentlichen Verwaltung legitimiert. Zum anderen ist § 8 ITEG SH nicht auf den Zweck der Vermeidung von Verzerrungen beschränkt, sondern betrifft allgemein die Verarbeitung zu Zwecken der Entwicklung und des Trainings von KI-Systemen (die Verarbeitung beim späteren Einsatz richtet sich nach allgemeinen Regeln). Dies entspricht weitgehend der Zielrichtung von Art. 54 Abs. 1 KOM-E für die Entwicklung und Erprobung. Allerdings ist diese Norm viel enger als § 8 ITEG SH, weil erhebliche Anforderungen an die Verarbeitung durch KI-Reallabore festgeschrieben werden, die weit über die im Vergleich rudimentären Vorgaben in § 8 ITEG SH hinausgehen.

Sollte der Verordnungsentwurf in dieser Form beschlossen werden, wird deshalb die Frage zu beantworten sein, ob die unionsrechtliche Zweckänderungsbefugnis nationale Regelungen sperrt, die an sich auf Basis der Öffnungsklauseln der DSGVO zulässig wären. Hierfür könnte man anführen, dass andernfalls die hohen Vorgaben von Art. 54 Abs. 1 KOM-E sehr leicht unterlaufen werden könnten. Andererseits sind die dort geregelten KI-Reallabore ein sehr spezieller Anwendungsfall. Da sie bisher noch nicht einmal konzeptionell wirklich existieren (Modalitäten und Bedingungen für den Betrieb werden nach Art. 53 Abs. 6 KOM-E in Durchführungsrechtsakten festgelegt, s. o.), würde die Annahme einer Sperrwirkung die allermeisten Anwendungsfälle einer Zweckänderung personenbezogener Daten zur Entwicklung und Erprobung von KI-Systemen verbieten. Für eine solche Wirkung des Entwurfs bietet der KOM-E weder in EG 72 noch

an sonstiger Stelle einen Anhaltspunkt; ohne einen solchen sollte eine so weitgehende Rechtsfolge nicht angenommen werden.

3. Transparenzpflichten

Neben der Zulässigkeit der Datenverarbeitung und einem etwaigen Abwehranspruch gegen diese spielt die Transparenz eine zentrale Rolle sowohl im Verbraucherschutz- als auch im Datenschutzrecht. Das Bundesverfassungsgericht hat dies bereits im Volkszählungsurteil mit der eingängigen Formulierung hervorgehoben, mit dem Recht auf informationelle Selbstbestimmung, „wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".[44]

a) Transparenzpflichten bei der Zweckänderung zu Testzwecken

Sekundärrechtlich ist der Transparenzgrundsatz in Art. 5 Abs. 1 lit. a DSGVO verankert und wird maßgeblich durch das Auskunftsrecht (Art. 15 DSGVO) und die Informationspflichten der Art. 13, 14 DSGVO konkretisiert.[45] Beide Vorschriften verpflichten nicht nur bei der Datenerhebung dazu, die betroffene Personen zu informieren (Art. 13 Abs. 1, Art. 14 Abs. 1 DSGVO). Darüber hinaus muss nach Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO ein Verantwortlicher, der beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den sie erlangt wurden, der betroffenen Person vor der Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß dem jeweiligen Abs. 2 der Vorschrift zur Verfügung stellen.[46] Dies gilt im Ausgangspunkt für alle oben erwähnten Zweckänderungsbefugnisse im geltenden Recht (vor allem Art. 6 Abs. 4 DSGVO und § 8 ITEG SH) und würde auch für die Zweckänderungen nach dem KOM-E gelten.

Wurden die Daten nicht bei der betroffenen Person erhoben, so kann die Informationspflicht entfallen oder durch öffentliche Informationen zum Beispiel auf einer Webseite ersetzt werden, wenn die Erteilung der Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (Art. 14 Abs. 5 lit. b DSGVO).[47] Im Falle der Datenerhebung bei der betroffenen

---

[44] BVerfGE 65, 1 (43).

[45] S. zum Transparenzgrundsatz ausführlich *Manthey*, Das Datenschutzrechtliche Transparenzgebot, 2020; zur Umsetzung im Bereich von KI s. *Gausling*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.3; zum Problem der (fehlenden) Nachvollziehbarkeit von KI-Systemen noch näher unten IV 1.

[46] Zu dieser Transparenz bei Zweckänderung s. *Bäcker*, in: Kühling/Buchner (Hrsg.), DSGVO BDSG, 3. Auflage 2020, Art. 13 Rn. 69 ff.; Paal/Hennemann, in: Paal/Pauly (Hrsg.), DSGVO BDSG, 3. Auflage 2021, Art. 13 Rn. 33, jeweils m. w. N.

[47] Zur Auslegung und Reichweite dieser Ausnahme s. *Bäcker*, in: Kühling/Buchner (Fn. 46), Art. 14 Rn. 53 ff.; *Hennemann*, in: Paal/Pauly (Fn. 46), Art. 14 Rn. 40 ff., jeweils m. w. N.

Person existiert in Art. 13 DSGVO keine derartige Ausnahme. Einschränkungen sind allerdings auf der Basis von Art. 23 DSGVO zulässig (s. o.). Hiervon hat der deutsche Gesetzgeber v. a. in §§ 32, 33 BDSG Gebrauch gemacht.[48] Diese Normen dürften allerdings höchstens in sehr speziellen Einzelfällen der Zweckänderung von Daten zum Training von KI-Systemen greifen. Im Grundsatz werden deshalb die Rechte von Verbraucherinnen und Verbrauchern zumindest insoweit gewahrt, als ihnen eine solche Zweckänderung bereits vor der Weiterverarbeitung mitzuteilen ist.

b) Weitergabe der Trainingsdaten an andere betroffene Personen?

Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO enthalten die Pflicht, zumindest in Fällen einer automatisierten Entscheidungsfindung einschließlich Profiling nach Art. 22 DSGVO „aussagekräftige Informationen über die involvierte Logik" sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zur Verfügung zu stellen. Diese in ihrer Reichweite stark streitige Vorschrift[49] greift allerdings im Moment der Zweckänderung der Daten zum Zwecke des Trainings von KI-Systemen nicht, da dieses Training nicht in eine automatisierte Entscheidungsfindung für die betroffenen Personen mündet, deren Daten verarbeitet werden. Bei der späteren automatisierten Entscheidungsfindung unter Verwendung eines so trainierten KI-Systems ist die Regelung hingegen anwendbar.

Ob die Information über die involvierte Logik auch eine Information über die Trainingsdaten einschließt, ist offen. Die bisherige Rechtsprechung berücksichtigt zur Einschränkung des Auskunftsanspruchs insbesondere gegenläufige Betriebs- und Geschäftsgeheimnisse der Anbieter hinsichtlich der verwendeten Algorithmen.[50] Analog dazu wird es jedenfalls unzulässig sein, personenbezogene Trainingsdaten aus einer Phase der Entwicklung oder Implementierung des KI-Systems an eine andere natürliche Person herauszugeben, die nach den Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO zu informieren ist, weil das fertige KI-System eine auf sie bezogene automatisierte Entscheidungsfindung vornimmt. Hierfür spricht auch, dass die Regelungen systematisch keine Zweckänderungs-

[48] S. zur Problematik dieser Einschränkungen und ihrer DSGVO-Konformität *Dix*, in Simitis/Hornung/Spiecker gen. Döhmann (Fn. 34), Art. 13 Rn. 23.

[49] Der BGH hat zu § 34 S. 1 Nr. 4 BDSG a. F. entschieden, dass der Auskunftsanspruch nicht die sogenannte Scoreformel, also die abstrakte Methode der Scorewertberechnung, umfasst, s. BGHZ 200, 38 (Rn. 27); s. a. Fn. 2. Es spricht viel dafür, dass die DSGVO über das Auskunftsrecht nach dem BDSG a. F. hinausgeht (a. A. wohl VG Wiesbaden, VuR 2022, 70), da die Formulierung zur involvierten Logik neu ist. In welchem Umfang Informationen über diese Logik bereitzustellen sind, ist aber unklar, s. näher *Kumkar/Roth-Isigkeit*, JZ 2020, 277, 281 ff.; *Sesing*, MMR 2021, 288.

[50] S. Fn. 49.

bzw. Übermittlungsbefugnisse der Verantwortlichen sind.[51] Demgegenüber ist es vorstellbar, dass Informationen allgemeiner Art über die verwendeten Trainingsdaten bereitzustellen sind, wenn sich hieraus die entscheidenden Informationen ergeben, um beispielsweise die Auswirkungen der Verarbeitung für die betroffene Person transparent zu machen.

c) Trainingsdaten als Teil der Dokumentation

Nach Art. 18 und Art. 16 lit. c KOM-E muss der Anbieter eines Hochrisiko-KI-Systems eine technische Dokumentation nach Art. 11 Abs. 1 KOM-E erstellen, bevor es in Verkehr gebracht oder in Betrieb genommen wird. Die Dokumentation enthält nach Art. 11 Abs. 1 UAbs. 2 S. 2 i. V. m. Anhang IV Nr. 2 lit. d und g KOM-E auch Angaben über Trainings-, Validierungs- und Testdaten. Aufzunehmen sind:

- Datenanforderungen in Form von Datenblättern, in denen die Trainingsmethoden und -techniken und die verwendeten Trainingsdatensätze beschrieben werden, mit Angaben zu Herkunft, Umfang und Hauptmerkmalen dieser Datensätze; Angaben zur Beschaffung und Auswahl der Daten; Kennzeichnungsverfahren (z. B. für überwachtes Lernen), Datenbereinigungsmethoden (z. B. Erkennung von Ausreißern);
- verwendete Validierungs- und Testverfahren, mit Angaben zu den verwendeten Validierungs- und Testdaten und deren Hauptmerkmalen;
- Parameter, die zur Messung der Genauigkeit, Robustheit, Cybersicherheit und der Erfüllung anderer einschlägiger Anforderungen nach Titel III Kapitel 2 sowie potenziell diskriminierender Auswirkungen verwendet werden;
- Testprotokolle und alle von den verantwortlichen Personen datierten und unterzeichneten Testberichte, auch in Bezug auf die in Buchstabe f genannten vorab bestimmten Änderungen.

Diese Angaben enthalten nicht die Trainings-, Validierungs- und Testdaten selbst,[52] sodass sich insoweit keine datenschutzrechtlichen Probleme ergeben; ähnliches dürfte für die Dokumentationspflicht in § 8 Abs. 4 ITEG SH gelten.[53] Demgegen-

[51] Systematisch wäre zumindest zu verlangen, dass zu den Tatbestandsvoraussetzungen der Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO eine datenschutzrechtliche Befugnis zur (ggf. erneuten) Zweckänderung der personenbezogenen Trainingsdaten eingreift. Hierbei müssten die Grundrechte und Grundfreiheiten der betroffenen Personen berücksichtigt werden.

[52] Forderung nach einer Dokumentation dieser Daten in der Entschließung des Europaparlaments v. 6.10.2021, P9_TA(2021)0405, Rn. 19.

[53] Gemäß § 8 Abs. 4 S. 1 ITEG SH dokumentiert die öffentliche Stelle zwar „die für die Entwicklung und den Einsatz der datengetriebenen Informationstechnologien verwendeten Daten". Dies umfasst sprachlich auch die Daten selbst. S. 2 verlangt sodann aber, dass mindestens die Quelle der Daten, der Datenlieferant, der Erhebungskontext und der Erhebungszeitpunkt zu dokumentieren sind, nach S. 3 „sollen" (nur) „soweit möglich" auch die Mess- und Erhebungsmethode dokumentiert werden. Die Dokumentation der Daten selbst ist also jedenfalls nicht zwingend, entgegen dem Wortlaut von S. 1 mutmaßlich sogar nicht durch den Gesetzgeber beabsichtigt.

über sind Angaben über diese Daten sowie Informationen enthalten, die für die Kontrolle diskriminierender Auswirkungen auf Verbraucherinnen und Verbraucher relevant sein können. Die Dokumentation nach Art. 11 KOM-E ermöglicht somit auch eine auf die Trainings-, Validierungs- und Testdaten bezogene Kontrolle durch Dritte.

Allerdings erstreckt sich diese Kontrollmöglichkeit nicht auf die späteren Adressaten von KI-Systemen. Die Dokumentation dient zwar der Einhaltung der Anforderungen der Verordnung (Art. 11 Abs. 1 UAbs. 2, EG 46 KOM-E). Dies erstreckt sich jedoch nur auf Behörden und sonstige staatliche Stellen (v.a. Art. 64 Abs. 3 KOM-E, s.a. EG 79 KOM-E). Die Marktüberwachungsbehörden haben nach Art. 64 Abs. 1 KOM-E sogar uneingeschränkten Zugang zu den von Anbietern genutzten Trainings-, Validierungs- und Testdatensätzen, auch über Anwendungsprogrammierschnittstellen (API) oder sonstige für den Fernzugriff geeignete technische Mittel und Instrumente. Demgegenüber findet sich an keiner Stelle eine Regelung dazu, ob die Adressaten von Hochrisiko-KI-Systemen Zugang zur Dokumentation erhalten, um ihre Verbraucherschutzrechte zu wahren. Die Regelungen zur Dokumentation teilen insoweit die allgemeine Schieflage des KOM-E, der sehr stark auf eine behördlich überwachte Regulierung der KI-Systeme setzt, dabei jedoch Verbraucherinnen und Verbraucher als Akteure völlig außen vor lässt.

IV. Regulierungsbedarf jenseits des Datenschutzrechts?

Als Zwischenergebnis lässt sich festhalten, dass das geltende Datenschutzrecht durchaus Instrumente enthält, um die Rechte von betroffenen Personen hinsichtlich der Verwendung ihrer personenbezogenen Daten zum Training von KI-Systemen sowie hinsichtlich des späteren Einsatzes von mit personenbezogenen Daten trainierten KI-Systemen zu wahren. Allerdings bleiben diese Instrumente aufgrund des Erfordernisses des Personenbezugs fragmentarisch und enthalten teilweise deutliche tatbestandliche Einschränkungen bzw. Unklarheiten. Dies führt zur Frage, ob der Gesetzgeber tätig werden sollte.

1. Unterlassungsansprüche gegen unzulänglich trainierte KI?

Fraglich ist insbesondere, ob die Vorgaben aus Art. 10 Abs. 3 S. 1 KOM-E aus der Perspektive von Verbraucherinnen und Verbrauchern fruchtbar gemacht werden können. Mit anderen Worten: Wie können diese sich dagegen wehren, zu Adressaten von KI-Systemen zu werden, wenn die Trainings-, Validierungs- und Testdatensätze nicht relevant, repräsentativ, fehlerfrei und vollständig waren?

Das geltende Datenschutzrecht erweist sich dabei erneut als unzulänglich. Sofern das System mit eigenen, unrichtigen personenbezogenen Daten der Adressaten trainiert, validiert oder getestet wurde, besteht ein Berichtigungsanspruch

nach Art. 16 DSGVO. Dies dürften jedoch Sonderfälle sein. Unrichtige Daten über andere Personen, unrichtige anonyme Daten und unrichtige Sachdaten werden nicht erfasst. Dasselbe gilt für irrelevante und nicht repräsentative Daten: Der Berichtigungsanspruch ist ein Individualrecht, das vor unzutreffenden Fremdbildern schützen soll; selbst im Falle der Verwendung eigener personenbezogener Daten geht dies aber nicht so weit zu verhindern, dass richtige Daten für Zwecke verwendet werden, für die sie nicht relevant sind. Zwar könnte man insoweit den übergeordneten Grundsatz der Datenrichtigkeit (Art. 5 Abs. 1 lit. d DSGVO) oder den Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a DSGVO) in Erwägung ziehen. Allerdings dürfte es ausgeschlossen sein, aus diesen einen allgemeinen subjektiven Anspruch auf Unterlassung der Anwendung eines unzulänglich trainierten KI-Systems abzuleiten.[54]

Je nach der späteren Verwendungsumgebung kann sich ein solcher Anspruch allerdings auch aus dem Datenschutzrecht oder aus anderen Rechtsgrundlagen ergeben. Wenn ein unzulänglich trainiertes KI-System nunmehr unrichtige personenbezogene Daten produziert, so greift Art. 16 DSGVO. Außerhalb des Datenschutzrechts werden in vielen Fällen Mängelgewährleistungsansprüche, vertraglichen Nebenpflichten, das Produkt- oder Produzentenhaftungsrecht oder Ansprüche aus dem Staatshaftungsrecht[55] einschlägig sein. Ob sich insoweit aus der Perspektive von Verbraucherinnen und Verbrauchern relevante Lücken bei der Durchsetzung ihrer Rechte ergeben, bedürfte einer weitergehenden Analyse.

Prima facie dürften die eigentlichen Probleme weniger in der Verfügbarkeit der jeweiligen Abwehransprüche als vielmehr auf der Beweisebene liegen. Die vielfach diskutierten „Blackbox"-Probleme beim Einsatz von KI greifen auch hier: Je elaborierter die Systeme werden und je mehr sie in den verschiedenen Phasen der Entwicklung, der Konfiguration und des späteren Einsatzes trainiert werden, desto schwerer werden Verbraucherinnen und Verbraucher den Nachweis erbringen können, dass im Einzelfall unrichtige oder unangemessener Ergebnisse produziert werden oder gar dass diese Ergebnisse auf die Verwendung von Trainings-, Validierungs- und Testdatensätze zurückgehen, die nicht relevant, repräsentativ, fehlerfrei und vollständig waren. Dies ist ein systemisches Problem, da die (Un-)Fähigkeit von KI-Systemen, Entscheidungsgrundlagen und Entscheidungskriterien dem Benutzer zu erklären, also für ihn nachvollziehbar zu machen, sich oftmals auch auf den Nutzer erstreckt.[56] Der EuGH hat unlängst hervorgehoben,

---

[54] S. zur unklaren Reichweite des Grundsatzes der Richtigkeit bei Anwendung auf KI *Roßnagel*, in Simitis/Hornung/Spiecker gen. Döhmann (Fn. 34), Art. 5 Rn. 148 f., *Hacker*, ZGE 2020, 239, 245; s. ferner die Überlegungen bei *Hoeren*, MMR 2016, 8.

[55] Speziell zu dieser Frage und den Herausforderungen im Bereich von Kausalität und Verschulden s. *Roth-Isigkeit*, AöR 145 (2020), 321; *Martini/Ruschemeier/Hain*, VerwArch 112 (2021), 1.

[56] S. zu diesem zentralen Problem z. B. *Sudmann*, Digital Culture & Society 2018, 181; *Wischmeyer*, AöR 143 (2018), 1, 42 ff.; *Martini*, Blackbox Algorithmus, 2019, 28 ff.; *Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung, 2019, 520 ff.; *Malgieri*, Computer Law & Security Review 35 (2019) 105327; *Käde/von Maltzan*, CR 2020, 66.

dass KI-Systeme, die an einer mangelnden Nachvollziehbarkeit leiden und es dadurch unmöglich machen, den Grund für einen Grundrechtseingriff zu erkennen (konkret: einen Treffer in einer Passenger Name Records (PNR)-Datenbank), mit dem Recht auf einen wirksamen gerichtlichen Rechtsbehelf nach Art. 47 GRCh in Konflikt kommen können.[57] Ansätze zu einer technischen Lösung im Sinne einer „Explainable AI"[58] stellen derzeit eine der zentralen rechtlichen Forderungen und zugleich eine der größten technischen Herausforderung der KI-Forschung dar. Perspektivisch wird hier die Frage zu beantworten sein, ob diesen Problemen durch erweiterte Dokumentationspflichten (wie im KOM-E, aber erweitert um eine Zugänglichkeit für die Adressaten der KI-Systeme), Beweislasterleichterungen, Ansprüche auf Begründung und Erklärung[59] oder vorverlagerte Abwehransprüche begegnet werden muss.

2. Regulierungsbedarf für anonyme und synthetische Trainingsdaten?

Im Anschluss an diese Überlegungen stellt sich die Frage, ob der europäische oder der nationale Gesetzgeber den Umgang mit Trainingsdaten umfassend regulieren sollte. Dies würde nicht nur personenbezogene Daten, sondern auch anonyme Daten sowie synthetische Daten erfassen, also solche Trainingsdaten, die speziell für das Training generiert werden und beispielsweise personenbezogene Daten simulieren.[60]

a) Fehlende Eignung des Anwendungsbereichs und der Schutzinstrumente des Datenschutzrechts

Die deutlichste Einschränkung des Datenschutzrechts hinsichtlich seiner Eignung zum Schutz von Verbraucherinnen und Verbrauchern beim Einsatz von KI-Sys-

---

[57] EuGH, Urt. v. 21.6.2022 – C-817/19 – PNR-Daten, Rn. 194 f. = EuZW 2022, 706.

[58] S. aus verschiedenen Perspektiven *O'Hara*, Computer Law & Security Review 39 (2020), 105474; *Rohlfing u. a.*, Explanation as a social practice, IEEE Transactions on Cognitive and Developmental Systems, DOI: 10.1109/TCDS.2020.3044366; zu Umsetzungsmöglichkeiten z. B. *Waltl/Vogl*, DuD 2018, 613; *Käde/von Maltzan*, CR 2020, 66, 69 ff.; *Körner*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 2.4; *Hacker/Krestel/Grundmann/Naumann*, Artificial Intelligence and Law 28 (2020), 415; *Bibal/Lognoul/de Streel/Frénay*, Artificial Intelligence and Law 29 (2021), 149 ff.

[59] Für ein subjektives „Recht auf Erklärung" nach der DSGVO *Vogel*, Künstliche Intelligenz und Datenschutz, 2021, 172 ff.; Vorschlag für eine umfassende „reviewability" bei *Cobbe/Singh*, Computer Law & Security Review 39 (2020), 105475; s. auch die Überlegungen bei *Busch*, Algorithmic Accountability, ABIDA Gutachten, 2018, 56 ff.; *Martini*, Blackbox Algorithmus, 2019, 176 ff.; *Sesing*, MMR 2021, 288; zu Transparenzfragen auch *Wischmeyer*, in: Wischmeyer/Rademacher (Hrsg.), Regulating Artificial Intelligence, 2020, 75 ff.; Vorschläge de lege ferenda bei *Martini*, Blackbox Algorithmus, 2019, 340 ff.

[60] *Meents*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.8 Rn. 45 ff.; *Kaulartz*, ebd., Kap. 8.9 Rn. 22 ff.; ausführliche rechtliche Bewertung bei *Raji*, DuD 2021, 303; Lösungswege für datenschutzkonformes Training auch bei *Boenisch*, DuD 2021, 448; *Stock/Petersen/Behrendt/Federrath/Kreutzburg*, Informatik Spektrum 45 (2022), 137.

temen ist die Beschränkung auf personenbezogene Daten. Das Datenschutzrecht schützt zwar nicht nur das Grundrecht auf Schutz personenbezogener Daten, sondern – schon ausweislich Art. 1 Abs. 2 DSGVO – auch weitere Grundrechte und Grundfreiheiten natürlicher Personen. Dies bezieht sich insbesondere auf den Schutz vor Diskriminierungen (Art. 20 ff. GRCh).[61] Dies erweitert den sachlichen Anwendungsbereich nach Art. 2 Abs. 1 DSGVO jedoch nicht, sodass die Auswirkungen der Verwendung ungeeigneter oder verzerrender anonymer oder sachbezogener Trainingsdaten nicht erfasst werden.

Hinzu kommen die soeben beschriebenen Probleme einer Ergebniskontrolle: Diese birgt das Risiko, zu spät zu kommen und an Beweisproblemen zu scheitern. Etliche bekannt gewordene Fälle von verzerrenden Ergebnissen, Diskriminierungen und vergleichbaren Effekten deuten außerdem darauf hin, dass die intrinsische Motivation der Anbieter und Nutzer von KI-Systemen zur Verwendung hochwertiger Trainingsdaten[62] nicht hinreichend ist, um derartige negative Wirkungen zu vermeiden. Führt man sich schließlich die besondere Bedeutung der Trainingsdaten für die Auswirkungen von KI-Systemen vor Augen, so spricht viel dafür, der „Algorithmenkontrolle"[63] eine Datenkontrolle zumindest an die Seite zu stellen.[64]

Das Datenschutzrecht ist für eine solche Kontrolle noch aus weiteren Gründen nicht hinreichend geeignet. Selbst wenn sein sachlicher Anwendungsbereich eröffnet ist, ist es typischerweise blind für etwaige Folgewirkungen der Zulässigkeit oder Unzulässigkeit einer Datenverarbeitung für Dritte. Mit Blick auf das Ziel der Entwicklung hochwertiger KI-Systeme kann das Datenschutzrecht damit einerseits zu eng, andererseits aber auch zu weit sein:

Einerseits ist es für die Frage der Zulässigkeit einer Datenverarbeitung nach Art. 6 Abs. 1 DSGVO typischerweise irrelevant, ob die Verarbeitung negative Folgen für Dritte mit sich bringt. Dies ist besonders deutlich bei der Einwilligung, gilt aber auch für die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO, bei der zwar auf Seiten des Verantwortlichen auch die berechtigten Interessen eines Dritten in Anschlag gebracht werden können, nicht aber auf Seiten der betroffenen Person. Mit anderen Worten spielt es für die Zulässigkeit der Trainingsdatenverarbeitung auf Basis einer Einwilligung oder der Interessenabwägung keine Rolle, ob hierdurch negative Auswirkungen auf andere zu erwarten sind.

Andererseits kann es dazu kommen, dass Trainingsdaten aus individuellen, in der betroffenen Person liegenden Gründen nicht verarbeitet werden dürfen (bei-

---

[61] S. *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 34), Art. 1 Rn. 31 f., 36 ff.

[62] S. o. unter II. 2.

[63] S. *Martini*, DVBl 2014, 1481 (1488).

[64] Zur Notwendigkeit s. insoweit schon Europäische Kommission, Weißbuch zur Künstlichen Intelligenz, COM(2020) 65 final, 22 f.; *Hacker*, NJW 2020, 2142, 2144 f.; *ders.*, ZGE 2020, 239, 242 ff., 259 ff.

spielsweise wegen möglicher negativer Folgen für sie, Art. 6 Abs. 4 lit. d DSGVO). Auch dabei spielt es keine Rolle, ob durch diese Unzulässigkeit und das dadurch verursachte Fehlen eines einzelnen Trainingsdatensatzes in einer entsprechenden Datensammlung beispielsweise Verzerrungseffekte in den Trainingsdaten eintreten und damit wiederum Dritte Nachteile erleiden.

Schlussendlich können auch die typischen Schutzinstrumente des Datenschutzrechts Probleme für den Einsatz von Trainingsdaten mit sich bringen. Schon die Pseudonymisierung, insbesondere aber die Anonymisierung kann die Qualität der Trainingsdaten verschlechtern, wenn sie ernsthaft betrieben werden. Denn angesichts des sehr breiten Begriffs des personenbezogenen Datums[65] muss für eine echte Anonymisierung erheblich mehr unternommen werden, als lediglich den Namen zu entfernen. Zusätzlich ist die Entfernung solcher Teile der verbleibenden Daten erforderlich, die es mit entsprechendem Zusatzaufwand ermöglichen, die betroffene Person zu ermitteln.[66] Für diese Frage sind nach EG 26 S. 3 DSGVO alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Hierfür spielen nach EG 26 S. 4 DSGVO alle objektiven Faktoren eine Rolle, insbesondere die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, jeweils bezogen auf die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen. Dies kann eine Einzelfallbetrachtung erfordern und je nach technologischem Fortschritt auch ein „schleichendes" Eintreten des Personenbezugs implizieren.[67] Eine echte Anonymisierung kann damit zwar zum einen dem Verantwortlichen die datenschutzrechtskonforme Verwendung der Daten zum Training von KI-Systemen ermöglichen.[68] Will der Verantwortliche allerdings vollständig anonymisieren und damit auch das Risiko ausschließen, dass die trainierten Modelle nachträglich die personenbezogenen Daten preisgeben,[69] wird

---

[65] Im Streit zwischen den sogenannten relativen und absoluten Begriffen des Personenbezugs (dazu im Überblick *Hofmann/Johannes*, ZD 2017, 221; ausführlich *Schmidt-Holtmann*, Der Schutz der IP-Adresse im deutschen und europäischen Datenschutzrecht, 2014; *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015) hat sich der EuGH zwar formal für den relativen Begriff entschieden, der auf die Identifizierbarkeit für den konkreten Verantwortlichen abstellt (s. EuGH, Urt. v. 19.10.2016, Rs. C-582/14, NJW 2016, 3579 – Breyer). Zugleich sind die Kriterien, die das Gericht jedenfalls für den Personenbezug der IP-Adresse angibt, so weit gefasst, dass das Ergebnis zumindest in diesem Fall dem eines absoluten Begriffs des Personenbezugs ähnelt.

[66] S. zu den Anforderungen an die Anonymisierung insoweit *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 34), Art. 4 Nr. 5 Rn. 50 ff.; speziell für Trainingsdaten *Niemann/Kevekordes*, CR 2020, 17, 19; allgemeiner für KI-Systeme *Vogel*, Künstliche Intelligenz und Datenschutz, 2022, 216 ff.

[67] Dazu *Hornung/Wagner*, CR 2019, 565.

[68] S. *Roßnagel/Geminn*, ZD 2021, 487; dort auch zur Notwendigkeit einer Vorsorgeregelung zur Verhinderung der Herstellung des Personenbezugs. Zur Zulässigkeit der Anonymisierung als datenschutzrechtliche Verarbeitung s. *Hornung/Wagner*, ZD 2020, 223 m. w. N.

[69] S. dazu *Kaulartz*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.9 Rn. 9 ff.

er im Zweifel substantielle Teile der Daten entfernen und die damit verbundenen Einschränkungen der Qualität der Trainingsdaten hinnehmen müssen.

Ähnliche Probleme können sich durch die Beachtung der Grundsätze der Verarbeitung nach Art. 5 DSGVO einstellen.[70] So verlangt beispielsweise der Grundsatz der Datenminimierung, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen (Art. 5 Abs. 1 lit. c DSGVO).[71] Der Maßstab für die Notwendigkeit kann jedoch nicht der des späteren Einsatzzweckes eines KI-Systems sein. Denn um solche Systeme zu trainieren, bedarf es einer Negativkontrolle, die verhindert, dass ein System falschpositive Ergebnisse liefert. Mit anderen Worten: Man kann ein KI-System nicht darauf trainieren, PKWs zu erkennen, in dem man es ausschließlich mit Bildern von PKWs trainiert. Derartige Notwendigkeiten führen dazu, dass sowohl in der Trainingsphase als auch für eine spätere Qualitäts- und Ergebniskontrolle gerade solche Daten gebraucht werden, die auf den ersten Blick wegen Art. 5 Abs. 1 lit. c DSGVO nicht verarbeitet werden dürften.

Ein weiteres Beispiel für einen vergleichbaren Effekt ist der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO. Danach müssen personenbezogene Daten anonymisiert oder gelöscht werden, wenn sie für die Zwecke, für die sie verarbeitet werden, nicht mehr erforderlich sind. Dies könnte auf den ersten Blick dafür sprechen, nach Abschluss des Trainings eines KI-Systems die verwendeten Trainingsdaten zu löschen. Allerdings würde dies einen späteren Vergleich mit der Leistungsfähigkeit eines anderen KI-Systems erschweren, weil dies die Verwendung identischer Trainingsdaten erfordern kann. Auch für Dokumentationen oder spätere Haftungsfragen kann sich eine fortdauernde Relevanz der Daten ergeben, die einer Löschung entgegensteht.

b) Vorschläge im KOM-E

Mit Art. 10 KOM-E unternimmt die Kommission den Versuch eines umfassenden regulatorischen Zugriffs auf die Trainings-, Validierungs- und Testdatensätze von Hochrisiko-KI-Systemen. Dabei wird die größte Einschränkung des Datenschutzrechts beseitigt, da nicht nur personenbezogene Daten von den Qualitätskriterien erfasst sind. Dieses Modell – das auch der schleswig-holsteinische Gesetzgeber in § 8 Abs. 3 ITEG SH gewählt hat – ist auch aus Verbraucherschutzsicht zu begrüßen.

Ähnliches gilt für den Ansatz, losgelöst von den Grundsätzen der Verarbeitung in Art. 5 DSGVO selbstständige Qualitätskriterien zu regulieren, die den spezifischen Erfordernissen des Trainings von KI-Systemen entsprechen. Dabei gibt es

---

[70] S. allgemein zu KI und den Grundsätzen der Datenverarbeitung *Paal*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.7 Rn. 4 ff.; s. a. *Vogel*, Künstliche Intelligenz und Datenschutz, 2022, 86 ff.

[71] Forderung der Anwendung auf KI-Trainingsdaten z. B. im Gutachten der *Datenethikkommission*, 2019, 120; zur Umsetzung *Meents*, in: Kaulartz/Braegelmann (Fn. 4), Kap. 8.8 Rn. 9 ff.

im Detail zwar noch Verbesserungsbedarf.[72] Es ist aber erkennbar, dass beispielsweise das Kriterium der Relevanz eines Datensatzes für das Training, die Validierung oder das Testen eines KI-Systems (Art. 10 Abs. 3 S. 1 KOM-E) deutlich besser geeignet ist als das Kriterium, ob es im datenschutzrechtlichen Sinne auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist (Art. 5 Abs. 1 lit. c DSGVO).

Noch offen ist insoweit allerdings die Frage des erforderlichen Aufwands aufseiten der Anbieter. Die Anforderungen in Art. 10 Abs. 2 bis Abs. 4 KOM-E sind (ebenso wie die in § 8 Abs. 3 ITEG SH) bemerkenswert kategorisch formuliert. Nimmt man den Wortlaut ernst, so dürften etliche Anbieter in erhebliche Probleme kommen, denn gerade bei innovativen KI-Systemen kann es vorkommen, dass sich erst im Nachgang Unzulänglichkeiten der Trainings-, Validierungs- und Testdatensätze herausstellen. Auch bei gut verstandenen KI-Systemen dürfte es selbst mit erheblichem Aufwand unmöglich sein, in jedem Einzelfall zu 100 % relevante, repräsentative, fehlerfreie und vollständige (Art. 10 Abs. 3 S. 1 KOM-E) oder zu 100 % nicht-diskriminierende, integre, objektive und valide (§ 8 Abs. 3 ITEG SH) Daten zu verwenden.[73] Eine wichtige Frage wird deshalb sein, nach welchem zeitlichen Horizont sich die Beurteilung richtet. Außerdem wird man nicht umhinkommen, den zumutbaren Aufwand für Anbieter abzugrenzen, den sie im Rahmen von Art. 10 Abs. 2 bis Abs. 4 KOM-E betreiben müssen. Dazu bedarf es einer Diskussion darum, wie viele Fehler in den Datensätzen und welche Fehlerverteilung (z. B. auf unterschiedliche Adressaten oder Adressatengruppen) noch tolerabel sind. Die Formulierung von Art. 10 Abs. 3 und Abs. 4 KOM-E spricht dafür, dass insoweit im Bereich von Hochrisiko-KI-Systemen sehr hohe Maßstäbe anzulegen sind.

In bestimmten Fällen wird man die Anforderungen der Relevanz, Repräsentativität, Fehlerfreiheit und Vollständigkeit außerdem auf den konkreten Einsatzzweck und das konkrete Trainingsmodell beziehen und insoweit einschränkend interpretieren müssen. Wenn ein KI-System beispielsweise auf die Erkennung sehr seltener Ereignisse (schwere Verkehrsunfälle o. ä.) trainiert werden soll, so kann es dazu kommen, dass die verwendeten Trainingsdaten nur sehr eingeschränkt repräsentativ und in keiner Weise vollständig sind. Sofern man sich hierüber allerdings beim Training bewusst ist, können mit geeigneten KI-Algorithmen, die dies berücksichtigt, doch gute KI-Modelle trainiert werden. Sofern dies erfolgt und die verbleibenden Einschränkungen der Aussagekraft der Trainingsergebnisse transparent gemacht werden, sollte dies nicht als Verstoß gegen Art. 10 Abs. 3 KOM-E verstanden werden.

---

[72] S. dazu den Beitrag von *Hacker* in diesem Band.

[73] S. *Hacker*, ZGE 2020, 239, 265 f.; kritisch zum Entwurf aus diesem Grund *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528, 533.

Schließlich ist in diesem Zusammenhang der Vorschlag für die Zulässigkeit der datenschutzrechtlichen Zweckänderung im Rahmen der Verarbeitungsbefugnis nach Art. 10 Abs. 5 KOM-E erneut zu würdigen. Diese knüpft die Kommission einerseits gerade nicht an eine Einwilligung, sondern an die Erforderlichkeit für die Beobachtung, Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen. Dies ist funktional angemessen, weil sonst das Risiko bestünde, dass Verzerrungseffekte nicht erkannt oder sogar verstärkt würden, wenn einzelne betroffene Personen die Einwilligung erteilen, andere sie verweigern. Andererseits statuiert der KOM-E einen verschärften Erforderlichkeitsmaßstab und verbindet diesen mit der Vorgabe „modernster" technischer und organisatorischer Sicherheit- und Datenschutzmaßnahmen.[74] Dies erscheint als ein angemessener Kompromiss zwischen den Notwendigkeiten des Trainings von KI-Systemen zur Vermeidung von Diskriminierungen einerseits, den berechtigten Datenschutzinteressen von Verbraucherinnen und Verbrauchern andererseits.

Begleitet werden die Anforderungen in Art. 10 KOM-E durch Transparenzvorgaben, die über die des Datenschutzrechts hinausgehen.[75] Relevante Informationen über die verwendeten Trainings-, Validierungs- und Testdatensätze unter Berücksichtigung der Zweckbestimmung des KI-Systems müssen dem Nutzer nach Art. 13 Abs. 2 i V m Abs. 3 lit. b KOM-E bereitgestellt werden. Erforderlich sind präzise, vollständige, korrekte und eindeutige Informationen in einer für die Nutzer relevanten, barrierefrei zugänglichen und verständlichen Form. Freilich ist der Nutzer eben nicht die Verbraucherin oder der Verbraucher, sondern nach Art. 3 Nr. 4 KOM-E der Verwender des KI-Systems,[76] und über eine Weitergabe der Informationen an die betroffenen Verbraucherinnen und Verbraucher schweigt der Entwurf. Für den Umgang mit der nach § 8 Abs. 4 ITEG SH für öffentliche Stellen verpflichtenden Dokumentation gibt es sogar gar keine Regelungen hinsichtlich der weiteren Verwendung und etwaiger Auskunftsrechte Dritter; auch die Verordnungsermächtigung in § 11 Abs. 1 S. 2 Nr. 3 ITEG SH bezieht sich nur auf die Dokumentations- und Protokollierungspflichten selbst.

Dagegen enthält Art. 52 KOM-E Transparenzpflichten, die gegenüber den von KI-Systemen betroffenen natürlichen Personen zu erfüllen sind. Diese erfassen insbesondere den Umstand, dass mit einem KI-System interagiert wird (Art. 52 Abs. 1 KOM-E) sowie Fälle der Emotionserkennung und Biometrie (Abs. 2) wie auch von Deepfakes (Abs. 3). Die Pflichten beziehen sich aber nicht auf die Transparenz hinsichtlich der verwendeten Trainings-, Validierungs- und Testdatensätze.

---

[74] S. o. unter III. 2. c) aa).
[75] S. *Spindler*, CR 2021, 361, 368.
[76] S. o. unter II. 2.

V. Ausblick

Im Ergebnis ist der Vorschlag der Kommission zum Umgang mit Trainings-, Validierungs- und Testdatensätzen bei allen Diskussionspunkten im Detail ein Schritt in die richtige Richtung. Er löst die Regulierung von Trainingsdaten aus dem datenschutzrechtlichen Korsett, ohne Brüche mit diesem zu verursachen und ohne das Kind mit dem Bade auszuschütten, indem für das Ziel einer Führungsrolle der Europäischen Union bei der Entwicklung von KI-Systemen[77] personenbezogene Daten von Verbraucherinnen und Verbrauchern völlig freigegeben würden.

Angesichts der für Verstöße gegen Art. 10 KOM-E geltenden Sanktionen steht auch zu erwarten, dass die Norm in der Praxis beachtet werden wird. Die Nichtkonformität eines KI-Systems mit den Anforderungen aus Art. 10 KOM-E soll nach Art. 71 Abs. 3 lit. b KOM-E mit Geldbußen von bis zu 30 Mio. € oder – im Falle von Unternehmen – von bis zu 6 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres belegt werden können, je nachdem, welcher Betrag höher ist. Für Organe, Einrichtungen und sonstige Stellen der Union beträgt die mögliche Geldbuße nach Art. 72 Abs. 2 lit. b KOM-E immerhin noch 500.000 €.

Allerdings verbleiben zwei grundsätzliche Probleme des Kommissionsentwurfs, nämlich zum einen der fehlende Fokus auf Verbraucherinnen und Verbraucher und zum anderen die Beschränkung von Art. 10 KOM-E auf Hochrisiko-KI-Systeme.

Der erste Punkt ist allgemeiner Natur. Der Entwurf nimmt deutlich zu wenig die Perspektive der Adressaten von KI-Systemen ein. Der starke Fokus auf eine behördliche Durchsetzung der materiellrechtlichen Anforderungen im gesamten KOM-E muss zumindest ergänzt werden um eine auch prozedural gestärkte Rechtsposition von Verbraucherinnen und Verbrauchern. Es ist bezeichnend, dass Verbraucherschutz im Entwurf nur sehr allgemein genannt wird (S. 4, 13, 15, EG 28). Als Personen werden Verbraucherinnen und Verbraucher ausschließlich im Finanzbogen zum KOM-E erwähnt, und auch hier nur mit dem lapidaren Satz, sie „sollten davon profitieren, dass das Risiko von Verletzungen ihrer Sicherheit oder ihrer Grundrechte eingedämmt wird".[78] Grundrechtsverletzungen sind hingegen nicht nur etwas, das der europäische Gesetzgeber einzudämmen hat, sondern sollten auch sekundärrechtlich zu individuellen Rechtsschutzmöglichkeiten führen.[79]

---

[77] COM(2021) 206 final, S. 1.

[78] COM(2021) 206 final, S. 104.

[79] S. zu Ansprüchen der Betroffenen als Teil eines Regulierungsrahmens für Trainingsdaten *Hacker*, ZGE 2020, 239, 268 ff.; fehlende Individualrechte werden auch kritisiert von *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528, 537.

Es ist zwar durchaus plausibel, dass die materiellen Anforderungen an KI-Systeme auch mit den bestehenden Rechtsschutzinstrumenten des Verbraucherschutzrechts aktiviert werden können. Denn die Festlegung von Standards beispielsweise zum Einsatz qualitativ hochwertiger Trainings-, Validierungs- und Testdatensätze in Art. 10 KOM-E werden auch Auswirkungen auf Produkteigenschaften oder Verkehrserwartungen haben.[80] Das aktuelle Rechtsetzungsverfahren bietet aber die Chance, Verbraucherinnen und Verbrauchern den Zugriff auf zumindest einige der neuen Governance-Instrumente zu geben. Hiervon sollte der europäische Gesetzgeber Gebrauch machen.

Der zweite Punkt, die Beschränkung von Art. 10 KOM-E auf Hochrisiko-KI-Systeme, wurde bereits hinsichtlich der unklaren Auswirkungen auf die Verarbeitungsbefugnis in Art. 10 Abs. 5 KOM-E thematisiert.[81] Hinsichtlich der Anforderungen an Trainings-, Validierungs- und Testdatensätze in Art. 10 Abs. 2 bis Abs. 4 KOM-E ist der limitierte Regelungsansatz auf den ersten Blick noch schwerer verständlich – es wäre nicht zu rechtfertigen (und ist von der Kommission sicher nicht beabsichtigt), den Anbietern und Nutzern von „normalen" KI-Systemen im Umkehrschluss zu Art. 10 Abs. 3 KOM-E die Verwendung irrelevanter, nicht repräsentativer, falscher und unvollständiger Trainingsdaten zu gestatten.

Erklärbar ist die Beschränkung des Anwendungsbereichs durch den abgestuften Regulierungsansatz des KOM-E, der lediglich als besonders riskant bewertete KI-Systeme strengeren materiellrechtlichen und erheblichen verfahrensrechtlichen Anforderungen unterwerfen will. KI-Systeme, die unterhalb dieser Schwelle bleiben, sollen aus Verhältnismäßigkeitsgründen nicht mit bürokratischen Vorgaben überfrachtet werden. Zumindest bei Art. 10 KOM-E wäre insoweit allerdings eine Trennung zwischen materiellrechtlichen Vorgaben einerseits, verfahrensrechtlichen Anforderungen und Sanktionen andererseits angezeigt. Insbesondere die sehr hohen Bußgelder in Art. 71 Abs. 3 lit. b KOM-E müssten für normale KI-Systeme entfallen oder erheblich abgesenkt werden. Auch bei der Frage, wie streng die Anforderungen an die Qualität der Trainings-, Validierungs- und Testdatensätze zu fassen sind, wird man Abstriche machen müssen. Denn wenn sogar bei Hochrisiko-KI-Systemen die Vorgaben der Art. 10 Abs. 2 bis Abs. 4 KOM-E nicht zu 100 % erfüllbar sind, kann dies von den Anbietern anderer KI-Systeme nur in abgestufter Form erwartet werden.[82] Das ändert aber nichts daran, dass aus Verbraucherschutzsicht eine Regelung zu den materiellen Anforderungen an

---

[80] S. zum Charakter der Bestimmungen des KOM-E als Schutzgesetze i. S. v. § 823 Abs. 2 BGB *Grützmacher*, CR 2021, 433; dies wird dort bejaht (437 ff., speziell zu Art. 10 KOM-E 439 f.); in diese Richtung auch *Spindler*, CR 2021, 361, 362; zu haftungsrechtlichen Fragen der Qualität von Trainingsdaten auch *Hacker*, ZGE 2020, 239, 249 ff.; *Zech*, NJW 2022, 502; zum Staatshaftungsrecht s. Fn. 55.

[81] S. o. unter III. 2. c) aa).

[82] S. a. *Hacker*, ZGE 2020, 239, 267.

Trainings-, Validierungs- und Testdatensätze für alle KI-Systeme begrüßenswert wäre, weil so auch klargestellt würde, dass Verbraucherinnen und Verbraucher eine berechtigte Verkehrserwartung dahingehend haben, dass sämtliche KI-Systeme in der Praxis entsprechende Qualitätsanforderungen einhalten.