Margrit Seckelmann[1] und Jan Horstmann

Künstliche Intelligenz im Hochschulbereich und Datenschutz

Übersicht

I. Einführung
1. Die richtigen Noten für die falschen Studierenden?
2. Grundlegende Einsichten für KI im Hochschulbereich
II. Potenziale von KI an der Hochschule: Lehre im Fokus
III. Spannungslagen zwischen KI und Datenschutz
1. Relevante Merkmale von KI
a) Grundlagen
b) Trennung und Verschränkung der Datenverarbeitung in Training und Einsatz
2. Ausgewählte datenschutzrechtliche Anforderungen und resultierende Spannungen
a) Sachlicher und persönlicher Anwendungsbereich
b) Datenschutzgrundsätze des Art. 5 DS-GVO
c) Rechtsgrundlagen
d) Übermittlung in Drittstaaten
e) Profiling und automatisierte Entscheidung im Einzelfall
f) Technisch-organisatorischer Datenschutz und Datenschutz-Folgenabschätzung
V. Fazit und Ausblick

I. Einführung

1. Die richtigen Noten für die falschen Studierenden?[2]

Gut gemeint ist nicht immer gut. Das demonstriert ein Beispiel aus Großbritannien, das unter dem etwas plakativen Titel „F*ck the Algorithm!" in die jüngere Bildungsgeschichte eingegangen ist. Der entsprechende Zornesruf erklang im Sommer 2020 vor dem Parlament in Westminster aus den Mündern hunderter Schülerinnen und Schüler. Er wurde zu einem Zeichen des Widerstands gegen ein Vorhaben des englischen Amts für die Regulierung von Prüfungen und Abschlüssen (Office of Qualifications and Examinations Regulation, Ofqual). Da in der Covid-19-Pandemie keine Abschlussarbeiten in Präsenz hatten durchgeführt werden können, wollte Ofqual die Abschlussnoten der Schülerinnen und Schüler für das zum Hochschulstudium berechtigende Advanced bzw. A-Level des General Certificate of Education durch einen Algorithmus festlegen lassen.[3] Dieser sollte eigentlich für Objektivität sorgen. Da sich aus der Forschung ergeben hatte, dass Lehrende bei einer Ersetzung schriftlicher Examina durch Noten für den Gesamteindruck von der Leistungsfähigkeit der Schülerinnen und Schüler (was zunächst überlegt worden war) dazu neigen, deren Leistungen positiver einzuschätzen, entschied sich das Ofqual für die Festlegung der Abschlussnote aufgrund einer parametrisierten Formel (eines Algorithmus), aus welcher dann die Abschlussnote abgeleitet wurde. Mit anderen Worten wurden in dem betreffenden „Pandemie"-Jahrgang keine Prüfungen mehr durchgeführt, sondern die Hochschulzugangsberechtigung wurde aufgrund eines Algorithmus ermittelt, der im Wesentlichen auf drei Variablen beruhte: der historischen Notenverteilung der drei vergangenen Jahre der Schule, dem Rang der Schülerin oder des Schülers innerhalb eines Fachs an der jeweiligen Schule (anhand der Einschätzung der Lehrenden[4]) sowie vorherigen Klausurnoten sowohl der historischen als auch der zu beurteilenden Schülerinnen und Schüler.

Das Problem dieser „Objektivität" war jedoch, dass sie einen verborgenen Bias enthielt. In Großbritannien ist das Bildungswesen nach wie vor von großen Unterschieden geprägt. Allerdings sorgen eine weitgehende Vereinheitlichung und die zeitgleiche Durchführung der A-Level-Prüfungen in England dafür, dass die Noten landesweit weitgehend vergleichbar sind. Um den Zugang zu den bekannten Einrichtungen in Oxford, Cambridge oder auch London wird intensiv konkurriert, gute Noten sind hierfür essenziell. Da es *Ofqual* zuließ, dass es in denjenigen Fällen, in denen in einem Fach an einer Schule weniger als 15 Schülerinnen und Schüler die Abschlussprüfung abzulegen hatten, aus praktischen Gründen doch wieder auf die Einschätzungen der Lehrenden

[1] Der Beitrag beruht auf dem Vortrag von Prof. Dr. Margrit Seckelmann beim 16. Hochschulrechtstag in Erlangen am 28.09.2023.

[2] Die Überschrift ist eine abgewandelte Version einer Überschrift der FAZ zur geschilderten Begebenheit, https://www.faz.net/aktuell/politik/ausland/britische-pruefungsergebnisse-die-not-mit-den-noten-16915526.html (Abruf 30.01.2024).

[3] In den übrigen Teilen des Vereinigten Königreichs gab es ähnliche Vorgänge. Ein ausführlicher technischer Bericht zu Ofquals Erwägungen und Methodik ist im Internet verfügbar: Ofqual, Awarding GCSE, AS, A level, advanced extension awards and extended project qualifications in summer 2020: interim report, https://assets.publishing.service.gov.uk/media/5f3571778fa8f5173f593d61/6656-1_Awarding_GCSE__AS__A_level__advanced_extension_awards_and_extended_project_qualifications_in_summer_2020_-_interim_report.pdf (Abruf 31.01.2024).

[4] Laut Ofqual (Fn. 2, S. 13ff.) sind die Einschätzungen der Lehrenden in relativer Hinsicht verlässlicher als in absoluter Hinsicht.

gesetzt werden sollte, wäre dieses – so vermutete man jedenfalls – Schülerinnen und Schülern an Privatschulen und in kleinen Kursen, vor allem in bildungsbürgerlich konnotierten Fächern wie Latein, Altgriechisch oder Kunstgeschichte, zugutegekommen. Zudem floss die allgemeine Notenverteilung an der betreffenden Schule aus den letzten Jahrgängen in die Formel ein und hätte zusätzlich diejenigen fleißigen und intelligenten Personen benachteiligt, die in der Abschlussprüfung trotz schlechter Startbedingungen beachtliche Punktzahlen erzielt hätten. Dieser implizite Bias wäre – hätte es keine Proteste dagegen gegeben – dadurch verstärkt worden, dass das zur Anfechtung der Noten vorgesehene Verfahren als kompliziert und kostenpflichtig erschien, so dass viele hiervor zurückgescheut hätten. Als dann noch bekannt wurde, dass aufgrund der Pandemie insgesamt weniger Studienplätze angeboten werden sollten, lief das Fass über – und es kam zu den eingangs erwähnten Protesten, bei denen interessanterweise die Schuld beim Algorithmus gesucht wurde. Letzten Endes wurde die angekündigte Formel nicht angewendet, es wurden die algorithmisch vergebenen Noten zurückgezogen und durch die Einschätzung der Lehrenden ersetzt.[5] Ob die gefundene Lösung allerdings mehr oder vielmehr weniger Bildungsgerechtigkeit enthielt, wurde danach von den Schülerinnen und Schülern nicht mehr problematisiert, denn in ihren Augen stand eines fest: Der Algorithmus war schuld.

2. Grundlegende Einsichten für KI im Hochschulbereich

Was lässt sich aus diesem Beispiel für den Einsatz von KI im deutschen Hochschulbereich lernen? Einerseits fallen zunächst die Unterschiede zu diesem (für die Bildungssoziologie hochinteressanten Beispiel[6]) auf. Es macht auf der anderen Seite aber zwei grundlegende Einsichten für den Datenschutz im Hochschulbereich beim KI-Einsatz sehr deutlich:

Erstens lassen sich dieser und ähnliche Fälle des Einsatzes von KI mit den klassischen Begriffen des Datenschutzrechts nur begrenzt fassen. Denn zum einen gibt es auf die im Falle Ofqual berechtigterweise aufgeworfene Frage, für welche Zwecke man überhaupt KI nutzen sollte, keine Antwort. Zum anderen lag ein Großteil des Problems gerade in der Heranziehung der statistischen Verteilung von Noten in vorherigen Jahren für die Entscheidung über die aktuellen Schülerinnen und Schüler.[7] Zwar wird durch die Entscheidung über die individuelle Note letztlich ein Personenbezug hergestellt.[8] Skandalisiert wurde jedoch die Anknüpfung an gruppenbezogene Merkmale, also ein Bias, der – wie bei KI-Applikationen häufig - daraus resultiert, dass aus dem (historischen) Verhalten vieler auf das mögliche Verhalten eines Einzelnen geschlossen wird.[9] Und das wirft wiederum eine zentrale Thematik der Debatten um Datenschutz und KI auf: Inwieweit ist das Datenschutzrecht das richtige Instrument, um einen Schutz vor „unangemessenen Schlussfolgerungen“[10] zu gewährleisten? Beide Problemstellungen lassen sich nicht mit dem personenbezogenen Ansatz des Datenschutzrechts allein behandeln. Es kommt auch auf noch offene Fragen seines Zusammenspiels mit anderen Normen an, insbesondere dem technikbezogenen Ansatz der KI-Verordnung (KI-VO) der EU,[11] die einen ersten Baustein des KI-Rechts darstellt. Für KI-Systeme zur Anwendung in Einrichtungen der allgemeinen und beruflichen Bildung aller Stufen sind nach der KI-VO bei einer Reihe von Einsatzzwecken,

5 Zum Ganzen: *Craven*, Ofqual grades algorithm: A recipe for unfairness, https://upreach.org.uk/news/ofqual-grades-algorithm-a-recipe-for-unfairness, abgerufen am 31.012024; *Willis/Chiusi*, United Kingdom – Research, in Chiusi et al., Automating Society Report 2020, S. 280; Kolkman, LSE Blog vom 26.08.2020, https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/, abgerufen am 31.01.2024.

6 S. die beginnende wissenschaftliche Durchdringung bei *Gardner*, IEEE Tech. & Soc. Mag. Jg. 41 Ausgabe 2 (2022), 84-89; *Mallett*, Reviewing the impact of OFQUAL's assessment 'algorithm' on racial inequalities in Lander/Kay/Holloman, COVID-19 and Racism – Counter-Stories of Colliding Pandemics (2023), S. 187-198.

7 Zum Schluss von Verhaltensdaten Vieler auf das zukünftige Handeln des Einzelnen *Seckelmann*, Verwaltung 2023, 1 (26f.).

8 Nach der Rechtsprechung sowie langjähriger Ansicht der Aufsichtsbehörden ist der Personenbezug anhand des Inhalts, des Zwecks und der Auswirkungen einer Information zu beurteilen, s. insb. EuGH, 20.12.2017, C-434/16 - Nowak = ZD 2018, 113; s.a. Art.-29-Datenschutzgruppe, WP136 – Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20.6.2007.

9 Seckelmann (Fn. 7), 26f.

10 *Wachter/Mittelstadt*, Columbia Business L. Rev. 2019, 494. In seiner grundrechtlichen Konzeption ist jedenfalls das Recht auf informationelle Selbstbestimmung als akzessorischer Vorfeldschutz vor freiheitsbegrenzenden Entscheidungen anderer angelegt, s. *Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts in Hoffmann-Riem, Offene Rechtswissenschaft, S. 570f.; krit. zu einem datenschutzrechtlichen Schutz vor unangemessenen Schlussfolgerungen *Steinbach*, Regulierung algorithmenbasierter Entscheidungen - grundrechtliche Argumentation im Kontext von Artikel 22 DSGVO (2021), S. 220.

11 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 (Gesetzgebungsverfahren COD 2021/0106). Da sich der Gesetzgebungsprozess zum Zeitpunkt des Verfassens in der finalen Phase befand, wird hier die vom EP am 13.3.2024 angenommene Fassung (Dokument-Nr. P9_TA(2024)0138 zugrunde gelegt, deren Annahme durch den Rat erwartet wird. Zur Übersetzung wurde teilweise die allgemeine Ausrichtung des Rates vom 6.12.2024 (ST 15698 2022 INIT) herangezogen.

insbesondere Zulassung und Bewertung (einschließlich Zwischenbewertungen), die Vorgaben für Hochrisiko-KI-Systeme anwendbar (Art. 6 Abs. 2 iVm Annex III Nr. 3 KI-VO).

Zweitens sind im Bildungsbereich existenzielle Güter der (beruflichen) Chancengleichheit und persönlichen Entfaltung betroffen. Es ist ein Versprechen von KI, dass diese Güter mittels Effizienz und Standardisierung nachgerade „automatisch" maximiert würden. Zweifelsohne bietet zudem insbesondere generative KI ein enormes Potenzial zur Ausbildung und Entfaltung von Kreativität. Doch müssen Chancengleichheit und persönliche Entfaltung als umkämpfte, diskursiv bestimmte und verteilte Güter angesichts der oft verborgenen „Prägekraft der Technik"[12] auch gegen diese behauptet werden.[13] Das ruft grundrechtliche Verbürgungen (insbesondere Art. 2 Abs. 1, Art. 2 Abs. 1 iVm Art. 1 Abs. 1, Art. 3, Art. 5 Abs. 3, Art. 12 GG sowie Art. 7, 8, 13 S. 2, 14, 15 GRCh) auf, die hinter den hier behandelten Normen des Datenschutzrechts stehen. Sie müssen im weitgehend staatlich geprägten Hochschulbereich durch die Hochschulen selbst zur Geltung gebracht werden.[14] Diese Belange sind also bei den folgenden Ausführungen zu den Spannungslagen zwischen KI und Datenschutzrecht im Bewusstsein zu behalten.

II. Potenziale von KI an der Hochschule: Lehre im Fokus

Künstliche Intelligenz verfügt als Querschnitts-[15] oder „Meta-Technologie"[16] über kaum überschaubare Einsatzmöglichkeiten, die sich durch die Dynamik der technischen wie sozialen Entwicklung laufend erweitern. Entsprechend vielfältig sind auch die Einsatzmöglichkeiten im Hochschulbereich. Mit der Verbreitung großer Sprachmodelle (Large Language Models) wie ChatGPT für den Einsatz durch private Nutzerinnen und Nutzer ohne besondere Vorkenntnisse bestehen breite Einsatzmöglichkeiten in allen Bereichen des Hochschulrechts von der Bewerbung bis zur Prüfung, insbesondere in der Produktion, im Erwerb und in der Repräsentation von Wissen. Ein Beispiel ist die Illustration von Wissen durch KI-Systeme, die aus Texteingaben Bilder generieren.[17] Mittels Schnittstellen können auf Sprachmodellen beruhende KI-Systeme bei Verfügbarkeit entsprechender Daten grundsätzlich auch für den konkreten Einsatzzweck angepasst werden.[18]

KI kann nunmehr also an allen Stationen einer Hochschullaufbahn eingesetzt werden: Bei der Zulassung Studierender, in der Lehre, im Selbststudium, in der Durchführung und Bewertung von Prüfungsleistungen, in beruflichen Auswahlentscheidungen,[19] in der Forschung sowie in der Verwaltung. Die Einsatzszenarien lassen sich grob in bewertende Anwendungen wie Prüfungsbewertung und Auswahlentscheidungen sowie vorrangig kreative und didaktische Anwendungen einteilen. Während KI in die Forschung idR weniger institutionell durch die Hochschule eingeführt werden dürfte, sondern von den Forschenden selbst als Arbeitsmittel herangezogen wird, bieten sich besonders im Bereich der Lehre, grundrechtlich verstanden als systematisch angelegte Verbreitung des in der Forschung Erkannten,[20] spannende Einsatzmöglichkeiten und zugleich Herausforderungen durch die grundrechtliche Betroffenheit der Studierenden.[21] Besonders im Selbststudium und in Ergänzung von Lehrangeboten können KI-Systeme eine strukturierende und unterstützende Funktion einnehmen. Dies kann verschiedene KI-Elemente wie beispielsweise Empfehlungsalgorithmen sowie Chatbots umfassen und diese kombinieren. Die Übergänge sind dabei fließend. Chatbots etwa könnten Lerninhalte – mit dem jeweiligen relevanten Lernstoff – nicht nur empfehlen,

12 *Wischmeyer*, AöR 2018, 1 (20ff.).

13 In diese Richtung deutet die Lehre, die *Kolkman* (Fn. 5) aus dem Eingangsbeispiel zieht: „Algorithmic accountability" erfordert die Ausbildung kritischer Öffentlichkeiten für Algorithmen.

14 Neben Studierenden und Lehrenden kommt auch privaten und öffentlichen Hochschulen der Schutz der Wissenschaftsfreiheit zu (*Kempen* in BeckOK Grundgesetz, *Epping/Hillgruber*, 56. Ed. Stand 15.8.2023, Art. 5 Rn. 185). Dies wird relevant, wenn staatliche Regelungen Vorgaben zum KI-Einsatz in Forschung oder Lehre enthalten, wird hier aber nicht behandelt.

15 *Djeffal*, DuD 2021, 529 (531).

16 *Oster*, JZ 2021, 167.

17 Von einem beeindruckenden Beispiel, in dem auch zusammenhängende Geschichten mit KI in die Form eines Comics gebracht wurden berichtet Heaven, MIT Technology Review, 5.3.2024, https://www.technologyreview.com/2024/03/05/1089458/generative-ai-turn-my-story-into-comic-images-lore-machine/ (Abruf 6.3.2024).

18 Für ChatGPT s. FAQ: Enterprise privacy at OpenAI, Stand 10.01.2024, https://openai.com/enterprise-privacy.

19 S. dazu *Herrmann*, ODW 2024, 25-44.

20 *Kempen* in BeckOK GG, *Epping/Hillgruber*, 56. Ed. Stand 15.8.2023, Art. 5 Rn. 183.

21 Hier wird davon ausgegangen, dass Lehrende den KI-Einsatz selbst in die Lehre aufnehmen. Die Einführung von KI kann als äußere Beeinflussung des grundrechtlich geschützten methodischen Ansatzes der Lehre (*Kempen* in BeckOK GG, *Epping/Hillgruber*, 56. Ed. Stand 15.8.2023, Art. 5 Rn. 183) im Einzelfall auch einen Eingriff in die Lehrfreiheit (Art. 5 Abs. 3 GG) darstellen (s. *Heckmann/Rachut*, ODW 2024, 85 (88)). In diesem Zusammenhang wären auch mögliche Bedrohungen der Freiheit der Lehre zu reflektieren, die durch die Fortentwicklung eines zunächst durch die Lehrperson autonom eingeführten KI-Systems im Zeitverlauf entstehen können.

sondern in unterschiedlicher Darreichungsform generieren, um die präferierte (oder gar algorithmisch als am effektivsten ermittelte) Lernform individueller Studierender zu bedienen oder einfach das Lernen abwechslungsreicher zu gestalten. In der Lehre ergeben sich die Einsatzfelder des (ggf. begleiteten) Selbststudiums, der Präsenzlehre sowie der Prüfung. Die folgenden, nur beispielhaft aufgezählten Einsatzmöglichkeiten veranschaulichen die Breite und Vielfalt der Konstellationen:

Im Selbststudium:
- Auswahl und Empfehlung von Lerninhalten anhand allgemeiner Vorgaben des Lehrpersonals, potenziell auch anhand des Lernstands oder Vorlieben individueller Studierender (Empfehlungssysteme)
- Aufbereitung und Präsentation des Lernstoffs in immer wieder abgewandelter und ggf. personalisierter Form durch Sprachmodelle, wobei ein KI-Chatbot neben vielen anderen beispielsweise die Rolle eines sokratischen Dialogpartners einnehmen kann[22]
- Erstellung und Auswertung von Tests zur Selbstüberprüfung, auch mittels Abwandlung oder Personalisierung, Bewertung von Übungsaufgaben
- Erkennen von Lerndefiziten durch Auswertung des Lernfortschritts, um Beratungs- oder Fördermaßnahmen zu ergreifen

In der Präsenzlehre:
- Erstellung von Lehrmaterialien
- Einbindung von generativer KI zur Vermittlung von Fähigkeiten für den wissenschaftlichen oder künstlerischen Umgang mit KI

In der Prüfung:[23]
- Erkennung von Täuschungsversuchen (sog. E-Proctoring[24] oder Erkennung von KI-generiertem Text[25])
- Auswertung der Prüfungsleistung vollständig oder teilweise durch ein KI-System[26]
- Auswertung der Prüfungsleistung durch Lehrende, KI-Assistenz beim Verfassen von Korrekturanmerkungen und Voten [27]

Die Einsatzfelder gehen durchaus fließend ineinander über, wie schon die unverbindliche Lernstandsüberprüfung, abschlussrelevante Studienleistungen ohne Notenbewertung oder das Selbststudium mit anlassbezogener Einbindung des Lehrpersonals verdeutlichen. Abstrakt gesprochen besteht eine steigende Grundrechtsrelevanz, je mehr der KI-Einsatz von einer ermöglichenden Erweiterung der Lernmittel im Selbststudium in die heteronome Prüfungssituation übergeht, wobei er zusehends die eigene Sphäre der Studierenden verlässt und künftige berufliche sowie persönliche Entfaltungschancen betroffen sind. Datenschutzrechtliche Bestimmungen sind aber in allen Fällen relevant.

III. Spannungslagen zwischen KI und Datenschutz

Da KI-Training und der hier im Fokus stehende KI-Einsatz in aller Regel personenbezogene Daten benötigen, ist zumeist auch das Datenschutzrecht einschlägig. Auch das Aufkommen der großen Sprachmodelle blieb nicht ohne datenschutzrechtliche Implikationen: Nachdem die italienische Datenschutzaufsichtsbehörde den Betrieb von ChatGPT für Italien im März 2023 vorübergehend untersagt und kurz darauf unter Auflagen wieder zugelassen hat,[28] scheint sich nun – auch in Anbetracht von Alternativen, die mehr Datenschutz bieten – bei den Aufsichtsbehörden die Ansicht durchzusetzen, dass sie unter Beachtung bestimmter Maßnahmen datenschutzkonform eingesetzt werden können.[29]

Mit einigen Vorschriften jedoch gerät KI aufgrund ihrer technischen Funktionsweise und den wirtschaftlichen Bedingungen ihrer Herstellung und ihres Einsatzes in besondere Spannung.

22 Überblick bei *Sabzalieva/Valentini*, ChatGPT and Artificial Intelligence in higher education – Quick start guide, S. 9, https://www.iesalc.unesco.org/wp-content/uploads/2023/04/ChatGPT-and-Artificial-Intelligence-in-higher-education-Quick-Start-guide_EN_FINAL.pdf (Abruf 28.2.2024).

23 Eine umfassende Syematisierung und rechtliche Einordnung bieten *Heckmann/Rachut* (Fn. 21), 85.

24 Zur datenschutzrechtlichen Bewertung ausführlich *Giannopoulou/Ducato/Angiolini/Schneider*, JIPITEC 2023, 278.

25 Dazu *Hoeren* in Salden/Leschke, Didaktische und rechtliche Perspektiven auf KI-gestütztes Schreiben in der Hochschuldbildung (2023), S. 32f.

26 Dazu insb. aus prüfungsrechtlicher Perspektive *Hoeren* (Fn. 25), 35ff.

27 S. ebd.

28 Pressemitteilungen und Verfügungen des Garante per la protezione dei dati personali sind, teilweise mit englischer Übersetzung, abrufbar unter https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847 (Abruf 7.3.2024).

29 So hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) eine erste Checkliste erstellt: Checkliste zum Einsatz LLM-basierter Chatbots, Stand 13.11.2023, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checkliste_LLM_Chatbots_DE.pdf (Abruf 7.3.2024).

1. Relevante Merkmale von KI

a) Grundlagen

KI bezeichnete ursprünglich ein Forschungsfeld mit dem Ziel der Simulation möglichst aller Aspekte der (menschlichen) Intelligenz durch Computer.[30] Die hier interessierenden KI-Systeme sind solche, die überwiegend auf maschinellem Lernen beruhen, also mittels der Auswertung von Daten (Trainingsdaten) unter Verwendung statistischer und mathematischer Methoden eine Funktion ermitteln, um Eingabewerten eine Ausgabe zuzuordnen. Dass sich die verwendeten Trainingsdaten stark auf das finale KI-System niederschlagen, offenbart sich im Bonmot „garbage in, garbage out": auf einer unzureichenden Datengrundlage lässt sich kein brauchbares KI-System trainieren.[31]

Auf diese überragenden Bedeutung von Daten, die auch auf den hier im Fokus stehenden KI-Einsatz durchschlägt, gehen viele der Spannungen mit dem Datenschutzrecht zurück. Viele KI-Systeme, die gute Ergebnisse erzielen, beruhen im Übrigen auf neuronalen Netzen oder ähnlichen Techniken (insbesondere dem sog. Deep Learning). Dabei lassen sich aufgrund der großen Datenmengen, komplexer mathematischer Gewichtungen in den verdeckten Schichten des Netzwerks und einiger Methoden zur Reduzierung der benötigten Rechenleistung, die Faktoren, die eine bestimmte Ausgabe ausschlaggebend sind, nicht eindeutig und erst recht nicht für Nutzerinnen und Nutzer intuitiv verständlich nachvollziehen (Black-Box-Problematik).[32] Wichtig ist darüber hinaus, KI-Systeme als sozio-technische Systeme[33] zu begreifen, d.h. ihre Wechselwirkung mit institutionellen, ökonomischen und psychologischen Faktoren und Prozessen zu berücksichtigen, die die konkreten Formen und Wirkungen des KI-Einsatzes beeinflussen. Schließlich geschieht die Herstellung von KI-Systemen in verzweigten Wertschöpfungsketten bzw. Ökosystemen, die im Falle vieler beliebter KI-Systeme durch US-amerikanische und chinesische Unternehmen dominiert werden. Dass die substanzielle Durchsetzung europäischen Datenschutzrechts gegen diese trotz beachtlicher Bußgelder an Grenzen stößt, ist bekannt. Für einzelne betroffene Personen resultiert die Kombination dieser Umstände darin, dass ihnen Art und Umfang der Verarbeitung personenbezogener Daten im Wesentlichen oft verborgen bleiben und schon mangels Wissens ihrer Kontrolle entzogen sein können.

b) Trennung und Verschränkung der Datenverarbeitung in Training und Einsatz

Bei KI lassen sich die Phasen des Trainings und des Einsatzes unterscheiden. In beiden können personenbezogene Daten verarbeitet werden. Auf die Datenverarbeitung zu Trainingszwecken soll hier zwar nicht näher eingegangen werden,[34] stets zu berücksichtigen ist aber, dass sie sich stark auf die Qualität des KI-Systems im Einsatz auswirkt. Das Datenschutzrecht stellt dies vor das grundlegende Problem, dass die Verarbeitung personenbezogener Daten einer Gruppe natürlicher Personen im Training Erkenntnisse über andere Personen ermöglicht und sich auf ihre Rechte, Freiheiten und Interessen, zuweilen auch als Gruppe, auswirken kann, während der Datenschutz überwiegend individuell und an der einzelnen Verarbeitung orientiert konzipiert ist.[35]

Spezielle Probleme können durch die Trennung der beiden Phasen auftauchen, wenn die Datenverarbeitung für das Training eines Systems in Drittstaaten[36] stattfindet. In der Regel dürften einzelne Datenverarbeitungen (z.B. das sog. Labelling der Daten) in Form einer Auftragsverarbeitung oder durch gesonderte Einheiten des Verantwortlichen durchgeführt werden. Für Datenübermittlungen an diese sind dann zusätzlich zu den allgemeinen Anforderungen der DS-GVO die speziellen Bedingungen der Art. 44 ff. DS-GVO einzuhalten.[37] Bei einer vollständigen Entwicklung eines Systems außerhalb des räumlichen Anwendungsbereichs der DS-GVO hingegen können EU-Datenschutzstandards im Training

30 S. *McCarthy/Minsky/Rochester/Shannon*, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, gekürzte Fassung in AI Magazine 2006, 12-14.

31 Instruktiv zur Bedeutung der Datengrundlage und damit verbundener Gestaltungsentscheidungen *Barocas/Selbst*, 104 Cal. L. Rev. (2016), 671-732; *Lehr/Ohm*, 51 UC Davis L. Rev. (2017), 653-717.

32 Einführend *Burrell*, Big Data & Society 2016 (1), 1-12; *De Laat*, Philos. Technol. 2018, 525 (529ff.).

33 Prägnant *Wischmeyer* (Fn. 12), 21: "sozio-technische Assemblage". S.a. Datenethikkommission der Bundesregierung, Gutachten, 2019, S. 25 (Empfehlung 36).

34 Dazu *Hornung*, Trainingsdaten und die Rechte von betroffenen Personen – in der DSGVO und darüber hinaus? in BMUV/*Rostalski*, Künstliche Intelligenz – Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, S. 91-120.

35 Zur möglichen Absicherung gruppenbezogener Ziele durch die DS-GVO *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Bertelsmann Stiftung 2018, S. 39f.

36 Außerhalb des Europäischen Wirtschaftsraums (EU-Staaten sowie Norwegen, Liechtenstein, Island).

37 *Zerdick* in Ehman/Selmayr, 2. Aufl. 2018, Art. 44 DS-GVO Rn. 13.

unterschritten werden, später aber ein Einsatz im Anwendungsbereich der DS-GVO stattfinden.[38]

Überdies können Systeme eingesetzt werden, bei denen in der Einsatzphase laufend neues Feedback für den lernenden Algorithmus generiert wird und damit ein weiteres Training erfolgt. Gerade bei KI, die als Dienstleistung angeboten (AI as a Service, AIaaS) oder auf Plattformen eingebunden wird, ist es möglich, dass die während des Einsatzes eingegebenen Daten vom Dienstleister wiederum als Trainingsdaten verwendet werden. Teilweise bieten AIaaS-Anbieter gegen Aufpreis Leistungen an, in denen Eingaben nicht für das Training verwendet werden.[39]

2. Ausgewählte datenschutzrechtliche Anforderungen und resultierende Spannungen

Die allgemeinen Vorschriften der DS-GVO gelten für die Herstellung (insbesondere das Training) und den Einsatz von KI im Hochschulbereich, sofern dabei personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DS-GVO). Die DS-GVO wird durch Landes- und Bundesrecht ausgefüllt und ergänzt insbesondere die Landesdatenschutz- und Landeshochschulgesetze.[40]

a) Sachlicher und persönlicher Anwendungsbereich

Die für die Anwendung der DS-GVO ausschlaggebenden Merkmale der Verarbeitung und der personenbezogenen Daten sind in Art. 4 Nr. 1, 2 DS-GVO definiert. Eine Verarbeitung ist entsprechend der offenen Aufzählung in Art. 4 Nr. 4 DS-GVO jeder Vorgang im Zusammenhang mit personenbezogenen Daten, woraus sich für den hiesigen Zusammenhang keine wesentliche Einschränkung des Anwendungsbereichs ergibt.

Das wichtigste Kriterium für die Abgrenzung personenbezogener Daten von nicht erfassten Sachdaten, statistischen oder anonymen Daten (ErwG 26 DS-GVO) ist der Bezug zu einer identifizierten oder identifizierbaren natürlichen Person (betroffene Person). Dass durch die Verknüpfung von Datenbeständen und leistungsstarke mathematisch-statistische Modelle die Möglichkeiten der Identifizierung und Ableitung von Wissen um natürliche Personen – oder jedenfalls von stochastisch hinreichend treffsicheren Schlussfolgerungen – im hiesigen Kontext enorm weit geworden sind, ist beinahe ein datenschutzrechtlicher Allgemeinplatz.[41] Dies liegt nicht zuletzt in der weiten Auslegung des Personenbezugs durch den EuGH und die Art.-29-Datenschutzgruppe begründet.[42] Es lässt sich sogar die noch nicht zufriedenstellend gelöste Frage aufwerfen, ob KI-Modelle selbst personenbezogene Daten enthalten, da sie die in den Trainingsdaten vorhandenen Informationen abbilden und diese sich in informationstechnischen Angriffsszenarien ggf. sehr granular rekonstruieren lassen.[43] Die Anonymisierung als Strategie der Vermeidung datenschutzrechtlicher Herausforderungen wirft selbst datenschutzrechtliche Fragen auf und ist bei KI oft technisch anspruchsvoll.[44] Grundsätzlich ist demnach davon auszugehen, dass in allen Phasen des KI-Einsatzes in personenbezogenen Kontexten wie dem Hochschulbereich personenbezogene Daten verarbeitet werden. Bei den oben exemplarisch aufgeführten Einsatzzwecken sind die betroffenen Personen vorrangig Studierende, während bei anderen Einsatzzwecken auch Beschäftigte betroffen sein können.

Perspektivisch (und im Einzelfall auch heute) scheint es möglich, dem Personenbezug speziell für das KI-Training mittels der Verwendung synthetischer Daten auszuweichen. Diese enthalten keine Informationen über natürliche Personen, weisen aber die für das KI-Training notwendigen statistischen Eigenschaften auf. Für die Erstellung solcher Daten wird echten Datensätzen beispielsweise mittels Techniken der differential privacy randomisierte Information (noise) hinzugefügt und ein Datensatz mit annähernd gleichen statistischen Eigenschaften generiert.[45] Man kann jedoch nicht pauschal davon ausgehen, dass die Schwelle der DS-GVO zum Personenbezug durch ein verbleibendes Risiko der Re-Iden-

38 U.U. mag sich dies über die Datenqualität mittelbar auch auf betroffene Personen in der Union auswirken, durch die DS-GVO jedoch wird es nicht adressiert. Die KI-VO hingegen adressiert den internationalen Datenverkehr indirekt: Sie gilt für in der EU auf den Markt gebrachte und eingesetzte Systeme und sogar, wenn nur das Ergebnis eines Systems in der EU verwendet wird (Art. 2 Abs. 1 lit. a), c)). Art. 10 des KI-VO fordert mit Blick auf die Datenqualität u.a., dass Trainingsdatensätze geeignete statistische Eigenschaften hinsichtlich der vom Einsatz eines Hochrisiko-KI-Systems betroffenen Personen oder Gruppen aufweisen (Abs. 3 S. 2) sowie den geographischen Kontext berücksichtigen (Abs. 4). Dies muss nach Art. 11 auch dokumentiert werden.

39 So im Team-Abonnement von OpenAI für GPT-4 oder bei Verwendung einer Schnittstelle (API), s. FAQ: Enterprise privacy at OpenAI (Fn. 18).

40 Hier wird exemplarisch das nds. Landesrecht herangezogen.

41 Grundlegend *Barocas/Nissenbaum* in Lane et al., Privacy, Big data, and the Public Good: Frameworks for Engagement (Cambridge UP 2014), S. 44-75; Mit reformorientierten Überlegungen *Karg*, ZD 2012, 255.

42 *Purtova*, Law, Innovation & Technol. 2018, 40; *Ziebarth* in Sydow/Marsch, 3. Aufl. 2022, Art. 4 DS-GVO Rn. 37.

43 *Veale/Binns/Edwards*, Phil. Trans. R. Soc. A 2018, 376:20180083; von Maltzan/Käde, DSRITB 2020, 505; *Boenisch*, DuD 2021, 448.

44 Dazu mwN *Winter/Battis/Halvani*, ZD 2019, 489; anschaulich zur Problematik *Martini*, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz 2019, S. 160ff.

45 *Winter/Battis/Halvani* (Fn. 44), 492f.; *Beduschi*, Big Data & Society 2024 (1), 1-5.

tifizierung bei synthetischen Daten nicht überschritten wird.[46] Zudem scheinen Aufwand und technische Reife den flächendeckenden Einsatz noch nicht zu ermöglichen.[47] Es kommt hier darauf an, mit verfeinerter Technik eine präzise Balance zwischen der Begrenzung von Informationsverlust und Identifizierungsrisiken herzustellen und diese rechtlich abzusichern. Unabhängig vom Personenbezug stellen sich bei diesen Techniken Fragen von Transparenz und Fairness, umso mehr mit Blick auf einen späteren, personenbezogenen Einsatz.[48]

Auch wenn sie nicht zwingend den Personenbezug ausschließen, sind die Erkenntnisse in diesem Bereich bei der Festlegung geeigneter technisch-organisatorischer Datenschutzmaßnahmen (Art. 24 Abs. 1, 32, 35 Abs. 7 lit. d) DS-GVO) zu berücksichtigen.

Persönlich treffen datenschutzrechtliche Pflichten v.a. den Verantwortlichen. Dies ist laut Art. 4 Nr. 7 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Da es auf die Entscheidung über Zwecke und Mittel der Verarbeitung ankommt, schließt die Auslagerung der Verarbeitung selbst an eine andere Stelle wie bei der Auftragsverarbeitung (Art. 4 Nr. 8 DS-GVO) die Verantwortlichkeit nicht aus. Entschließt sich die Hochschule, eine bestimmte KI-Anwendung, bei deren Einsatz personenbezogene Daten verarbeitet werden, für ihre Zwecke – insbesondere die Ergänzung bestimmter Lehrtätigkeiten – einzusetzen, so entscheidet sie damit idR über die Zwecke und Mittel der Datenverarbeitung im Einsatz. Für die zuvor zwecks KI-Training geschehene Datenverarbeitung ist die Hochschule hingegen nur verantwortlich, wenn sie dieses Training selbst durchgeführt oder beauftragt hat. Manche Drittanbieter verarbeiten die im KI-Einsatz von der Hochschule erhobenen personenbezogenen Daten allerdings auch zu Zwecken des fortwährenden KI-Trainings. Wenn dies nicht ausgeschlossen ist, erscheint eine Verantwortlichkeit der Hochschule grundsätzlich auch für ihren tatsächlichen Veranlassungsbeitrag hierzu möglich, nämlich die Erhebung und Übermittlung der Daten.[49]

b) Datenschutzgrundsätze des Art. 5 DS-GVO

Das Herzstück der materiellen Vorgaben der DS-GVO sind die Datenschutzgrundsätze des Art. 5 Abs. 1 DS-GVO. Sie sind bei jeder Datenverarbeitung zu beachten[50] und auch bei der Umsetzung der speziellen Pflichten zu berücksichtigen, wenn diese einen Interpretationsspielraum lassen, z.B. bei der Bestimmung der Speicherdauer von personenbezogenen Daten.[51]

Besondere Probleme im Zusammenhang mit KI werfen insbesondere die Grundsätze der Verarbeitung nach Treu und Glauben (engl. fairness), Transparenz und Zweckbindung auf.

Der Grundsatz von Treu und Glauben erfordert eine Rücksichtnahme auf die Interessen der betroffenen Person[52] und ihre legitimen Erwartungen.[53] Im Zusammenhang mit KI wird betont, dass dies neben einer gewissen Transparenz auch impliziere, bei der Gestaltung der Verarbeitung besonders ihre Auswirkungen auf betroffene Personen (wie z.B. Diskriminierung) unter Berücksichtigung der speziellen Umstände sowie Machtasymmetrien abzuschätzen und die Datenverarbeitung dem angemessen zu gestalten.[54] Machtasymmetrien können sich v.a. aus der geringen Nachvollziehbarkeit von KI-Outputs sowie aus einem Mangel an Einblick in, aber auch bereits Überschaubarkeit der einer KI zugrunde gelegten Annahmen, Daten, Korrelationen und Schlüsse für die betroffenen Personen ergeben.[55] Auch die scheinbare Objektivität und eingeschränkte Angreifbarkeit der Ergebnisse von KI-Systemen sind hier zu nennen.[56]

Für den eng mit dem Grundsatz von Treu und Glauben verbundenen Transparenzgrundsatz bestehen vordringlich ähnliche Herausforderungen aufgrund der Black-Box-Problematik. Transparenzpflichten durchziehen die DS-GVO, insbesondere in Form der Informations- und Auskunftspflichten (Art. 13-15 DS-GVO). Für KI sind besonders die Pflichten zur Bereitstellung von aussagekräftigen Informationen zur involvierten Logik

46 Überblick mwN bei *Beduschi* (Fn. 45).

47 Vgl. *Winter/Battis/Halvani* (Fn. 44), 493.

48 Für die Festlegung von prinzipienartigen Richtlinien für synthetische Daten *Beduschi* (Fn. 45).

49 Vgl. EuGH, 29.7.2019, C-40/17 - Fashion ID Rn. 75ff.

50 EuGH, 7.12.2023, C-634/21 - Schufa Holding (Scoring) = NJW 2024, 413 Rn. 67 mwN.

51 *Schantz* in BeckOK DatenschutzR, 46. Ed. Stand 1.11.2022, Art. 5 DS-GVO Rn. 2.

52 *Schantz* in BeckOK DatenschutzR, 46. Ed. Stand 1.11.2021, Art. 5 DS-GVO Rn. 8.

53 *Krügel/Pfeiffenbring* in Datenschutzrechtliche Herausforderungen von KI in Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik (2020), § 11 Rn. 22.

54 *Malgieri*, FAT* '20, 154 (169).

55 *Bayamlioglu*, EDPL 2018, 433 (435-438).

56 Prägnant *Pasquale*, The Black Box Society - The Secret Algorithms That Control Money and Information (2016), S. 15 am Beispiel des Finanzsektors: „patina of inevitability". Vgl. Auch *Wischmeyer* (Fn. 12), 21.

bei automatisierter Entscheidungsfindung (Art. 13 Abs. 2 lit. f), 14 Abs. 2 lit. g), 15 Abs. 1 lit. h) DS-GVO) relevant. Sie bieten im Lichte des Transparenzgrundsatzes (sowie des Grundsatzes von Treu und Glauben) angewendet Potenzial, die inhärenten Transparenz- und Bestreitbarkeitsdefizite von KI zu adressieren. Dabei wird eine Vielzahl von Formen der Transparenz und benachbarten Konzepten diskutiert.[57] Das Potenzial ist aber angesichts von Beschränkungen und Streitigkeiten bezüglich des Anwendungsbereichs und Inhalts der genannten Pflichten stark begrenzt.[58] Zugleich ist Transparenz kein Allheilmittel für die Wahrung der dahinterstehenden Schutzgüter wie Autonomie oder Nichtdiskriminierung, da die Wirkungsmechanismen komplex sind und Transparenz häufig nicht zu selbstbestimmtem Handeln führt oder das Erkennen gruppenbezogener Benachteiligungen erlaubt.[59]

Der Grundsatz der Zweckbindung wird bei KI insbesondere dadurch infrage gestellt, dass potenziell alle Daten wertvolle Trainingsdaten für die Weiterentwicklung eines Systems oder das Training neuer Systeme darstellen.[60] Doch der Zweckbindungsgrundsatz fordert, dass personenbezogene Daten nur verarbeitet werden, wenn und soweit dies für den ursprünglichen Zweck ihrer Erhebung erforderlich ist. Zwar gelten Ausnahmen (s. Art. 6 Abs. 4 DS-GVO), die sog. Zweckvereinbarkeit ist aber insbesondere aufgrund einer fehlenden Verbindung des KI-Trainings zum ursprünglichen Zweck (idR Durchführung der Lehre) fraglich.[61] Insbesondere hat die Hochschule daher darauf zu achten, ob Anbieter von KI-Systemen, die zum Zweck der Hochschullehre eingesetzt werden, Daten auch für eigene Zwecke, z.B. für das Training verwenden und dies möglichst auszuschließen. Eine (Teil-)Verantwortlichkeit der Hochschule für diese zweckändernde Datenverarbeitung ist dabei nämlich idR schwierig auszuschließen (s. oben).

Den Verantwortlichen trifft darüber hinaus nach Art. 5 Abs. 2 DS-GVO eine Rechenschaftspflicht für die Einhaltung der Datenschutzgrundsätze. Herausfordernd ist dies insbesondere beim Rückgriff auf Drittanbieter, in deren Datenverarbeitung die Hochschule selbst nur einen begrenzten Einblick hat.

Erneut sei hier auf die Verschränkung von Trainingsphase und KI-Einsatz hingewiesen, die auch Bedeutung iRd Datenschutzgrundsätze erlangt. Besonders betrifft dies die Grundsätze der Transparenz und der Rechenschaftspflicht, die häufig die Berücksichtigung der Gestaltung des KI-Systems erfordern.[62] Perspektivisch könnten die Pflichten zur Dokumentation und Transparenz für die Anbieter von Hochrisiko-KI-Systemen (Art. 11, 13 KI-VO) für die datenschutzrechtlich Verantwortlichen die Berücksichtigung von gestalterischen Vorentscheidungen bei der Erfüllung ihrer eigenen Pflichten ermöglichen. Im Übrigen ist besonders die Rechenschaftspflicht bei der Auswahl von Dienstleistern und dem Abschluss entsprechender Verträge zu berücksichtigen.

c) Rechtsgrundlagen

Nach Art. 6 Abs. 1 UAbs. 1 DS-GVO erfordert jede Verarbeitung personenbezogener Daten eine der dort aufgeführten Rechtsgrundlagen. Da die Öffnungsklausel in Art. 6 Abs. 2, 3, Art. 89 DS-GVO nur die Verarbeitung zu „wissenschaftlichen und historischen Forschungszwecken" erfasst, sind die davon Gebrauch machenden mitgliedstaatlichen Regelungen zugunsten der Lehre nicht anwendbar.[63]

Für den KI-Einsatz in der Lehre kommt daher zunächst die Einwilligung der betroffenen Person, idR Studierende, nach Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO in Betracht. Dafür muss die betroffene Person nach Art. 4 Nr. 11 DS-GVO freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich eine Willensbekundung abgeben, dass sie mit der Datenverarbeitung einverstanden ist. Problematisch ist bei KI die Bestimmtheit für den konkreten Fall. Diese muss hinreichend konkret mindestens die involvierten Stellen, verarbeiteten Daten und die verfolgten Verarbeitungszwecke in Bezug nehmen (ErwG 32 DS-GVO).[64] Werden bei der Nutzung von KI im Hochschulkontext neben den für diese Nutzung selbst erforderlichen Datenverarbeitungen zusätzliche Verarbeitungen durch Dritte vorgenommen, z.B. aufgrund der Nutzung von Drittanbieter-KI, bei der Nutzungsdaten für das weitere Training verwen-

57 Als erste Auswahl und mwN s. *Edwards/Veale*, 16 Duke L. & Tech. Rev. (2017), 18 (54ff.); *Malgieri/Comandé*, IPDL 2017, 243; *Kumkar/Roth-Isigkeit*, JZ 2020, 277 (283ff.).

58 Grundlegend *Wachter/Mittelstadt/Floridi*, IDPL 2017, 76; *Edwards/Veale* (Fn. 57), 44ff.; optimistischer *Goodman/Flaxman*, AI Mag 2017, 50 (55); *Selbst/Powles*, IDPL 2017, 233. Einen weiteren Anwendungsbereich bietet jedoch das „Recht auf Erklärung" bei Hochrisiko-KI-Systemen im neuen Art. 86 KI-VO.

59 *Edwards/Veale* (Fn. 57), 65ff.; *Dreyer/Schulz* (Fn. 35), S. 26f.

60 Vgl. *Hornung* (Fn. 34), S. 100; mit mwN auch *Krügel/Pfeiffenbring* (Fn. 53), § 11 Rn. 24.

61 Laut HmbBfDI (Fn. 29), S. 2 fehlt zudem idR eine Rechtsgrundlage.

62 Treffend *De Laat*, (Fn. 32), 530: „[...]any account of how an algorithm has been constructed, cannot do without an account of how datasets have been used in the process (say, as concerns possibly biased data). So accounting for machine learning models can only make sense if all phases are taken into account."

63 *Krügel* in Krügel/Schmieder NDSG, 1. Aufl. 2023, § 12 Rn. 10.

64 *Ernst* in Paal/Pauly, 3. Aufl. 2021, Art. 4 DS-GVO Rn. 78.

det werden, erscheint es kaum darstellbar, die betreffenden Verarbeitungsvorgänge hinreichend bestimmt in die Einwilligung aufzunehmen. Als weitere Hürde dürfte das Erfordernis der Freiwilligkeit die Einwilligung als Rechtsgrundlage in vielen Situationen ausschließen. Art. 7 Abs. 4 DS-GVO und ErwG 43 konkretisieren die Voraussetzungen der Freiwilligkeit, wobei insbesondere ErwG 43 auf ungleiche Ungleichgewichte zwischen betroffener Person und Verantwortlichem als Ausschlussgrund abstellt, für das die Behördenstellung des Verantwortlichen als Indiz in der gelten kann. Wenngleich ErwG 43 trotzdem eine Einzelfallprüfung nahelegt, ist die Freiwilligkeit gegenüber einer Behörde ein Ausnahmefall.[65] Die Freiwilligkeit ist damit v.a. dann zu verneinen, wenn die Hochschule in hoheitlicher Tätigkeit oder deren Vorbereitung handelt wie etwa bei Prüfungen, aber angesichts der Bedeutung des Studienabschlusses für die Lebensgestaltung und Wahrnehmung grundrechtlicher Freiheiten auch, wenn die Teilnahme an dem mit der Datenverarbeitung verbundenen Angebot essenziell ist, um ohne wesentliche Verlängerung der Studiendauer oder Einbußen bei der Benotung einen Studienabschluss zu erreichen. Schließlich ist die Einwilligung jederzeit widerruflich (Art. 7 Abs. 3 DS-GVO), was sie für eine ihrem praktischen Zweck nach dauerhafte oder mit Interessen der betroffenen Person potenziell konfligierende Datenverarbeitung (beispielsweise zu Prüfungszwecken) nicht sinnvoll erscheinen lässt.

Denkbar ist eine Einwilligung in der Hochschullehre insbesondere für Zusatzangebote in der Lehre wie z.B. optionale Kursangebote, die für die Erreichung von berufsqualifizierenden Abschlüssen keine notwendige Voraussetzung sind. Je stärker der Studienerfolg aber durch derartige Angebote beeinflusst wird, desto eher kann es jedoch zu psychologischen und ökonomischen Drucksituationen kommen, die die Freiwilligkeit der Einwilligung infrage stellen.

Hochschulen nehmen grundsätzlich Aufgaben im öffentlichen Interesse wahr, sodass idR und vorzugswürdig eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO in Betracht kommt, die sich nach Ab. 3 aus dem Unions- oder mitgliedstaatlichen Recht ergeben muss. Einschlägige Regelungen bieten die Landeshochschul- und Landesdatenschutzgesetze. § 17 Abs. 1, 4 NHG erlaubt den niedersächsischen Hochschulen neben weiteren Zwecken etwa u.a. die Verarbeitung von personenbezogenen Daten, die für die Einschreibung, die Teilnahme an Lehrveranstaltungen und Prüfungen, die Nutzung von Hochschuleinrichtungen Hochschulmitgliedern erforderlich und durch Ordnungen festgelegt sind, wobei § 17 Abs. 3 NHG die Verarbeitung dieser Daten generalklauselartig auch für die Erfüllung anderer Aufgaben nach § 3 NHG erlaubt. Eine mittelbare Beschränkung dürfte sich aus den lehrbezogenen Aufgaben der Hochschule ergeben, die nach § 3 NHG insbesondere "die Vorbereitung auf berufliche Tätigkeiten, die die Anwendung wissenschaftlicher Erkenntnisse und Methoden oder die Fähigkeit zu künstlerischer Gestaltung voraussetzen" (Nr. 2), umfassen. Zu beachten ist, dass die vermittelten Erkenntnisse und Methoden wissenschaftlich sein oder die Fähigkeit zur künstlerischen Gestaltung betreffen müssen. Von einer wissenschaftlich-methodischen Vorgehensweise ist freilich auch die Erprobung neuer Formate und Medien umfasst,[66] ein KI-Einsatz allein zwecks Neuigkeitswerts oder „Show-Effekts" könnte im Einzelfall problematisch sein. Eingedenk der Lehrfreiheit (Art. 5 Abs. 3 GG) ist aber eine weite, die autonomen Gesetzmäßigkeiten der Wissenschaft berücksichtigende Auslegung geboten. Darüber hinaus ist zu beachten, dass auch die Arbeitswelt von der Verbreitung von KI geprägt wird. Der geschulte Umgang mit (generativer) KI wird voraussichtlich zu einer Schlüsselanforderung in nahezu allen Tätigkeitsbereichen von Beschäftigten mit wissenschaftlicher oder künstlerischer Ausbildung werden.[67] Die Vorbereitung auf entsprechende berufliche Tätigkeiten und die Vermittlung eines kritisch-methodischen Umgangs mit der Technologie wird die Hochschullehre daher nur angemessen leisten können, wenn sie in gewissem Umfang generative KI einsetzen und den Umgang mit ihr einüben lassen kann. Die mit dem Einsatz verbundene Datenverarbeitung muss freilich weiterhin den Datenschutzgrundsätzen und weiteren Regeln der DS-GVO und dem grundrechtlichen Verhältnismäßigkeitsgrundsatz entsprechen.[68]

Damit ist entscheidend, dass die zu verarbeitenden Daten gemäß § 17 Abs. 3 NHG in einer universitären Ordnung in hinreichender Bestimmtheit bezüglich der Datenarten, der Verarbeitungsverfahren und mit Benennung des jeweiligen Verarbeitungszwecks festgelegt werden. Hinzu treten Bestimmungen zu technisch-organisatorischem Datenschutz und zu Löschpflichten. Je nach Einsatzzweck und Gegebenheiten an der Hochschule kommen Studienordnungen, Prüfungsordnungen[69] oder gesonderte Ordnungen zum Einsatz von E-Learning in Betracht. Aufgrund der oben angesprochenen, grundrechtsrelevanten Merkmale von KI scheint es sinnvoll,

[65] *Frenzel* in Paal/Pauly, 3. Aufl. 2021, Art. 7 DS-GVO Rn. 19.

[66] Vgl. *Patzke* in Epping NHG, 2. Aufl. 2024, § 3 Rn. 10 zu neuen Lehrmethoden und E-Learning.

[67] Vgl. *Günther/Gerigk/Berger*, NZA 2024, 234 mwN.

[68] Vgl. *Forgó/Graupe* in Epping NHG, 2. Aufl. 2024, § 17 Rn. 23.

[69] Zu den Regelungsspielräumen *Heckmann/Rachut* (Fn. 21), 89.

auch Fragen der Anbieterwahl und der Gewährleistung von Transparenz der Systeme zu regeln. Besonders zu beachten ist bei allen gemäß Art. 6 Abs. 1 UAbs. 1 lit. e) DS-GVO auf die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe gestützten Rechtsgrundlagen wie § 17 Abs. 1, 3 NHG, dass betroffene Personen gemäß Art. 21 Abs. 1 DS-GVO unter Vortrag von aus ihrer besonderen Situation entspringenden Gründen ein unionsrechtlich verankertes Widerspruchsrecht haben. Schließlich erfordert § 17 Abs. 3 S. 2 NHG die frühestmögliche[70] Anonymisierung, was bei leistungsstarker KI mit einer Vielzahl von Eingangsdaten auf die dargestellten Schwierigkeiten stößt. Soweit zudem der Zweck des KI-Einsatzes die Personalisierung der Lernumgebung oder der Lerninhalte beinhaltet, wird er idR einen Personenbezug erfordern. Dies verschiebt den Schutz der betroffenen Personen zum Verhältnismäßigkeitsgrundsatz und zur technischen und organisatorischen Gestaltung der KI-Systeme und ihres Einsatzes.

d) Übermittlung in Drittstaaten

Gegenüber der Entwicklung eigener Systeme ist die Verwendung von durch Dritte entwickelten KI-Systemen in aller Regel technisch und wirtschaftlich einfacher. Die Dominanz von Anbietern aus Drittstaaten führt dazu, dass es dabei für Hochschulen nahe liegt, für die Einbindung von KI auf diese Anbieter zurückzugreifen, die bisweilen personenbezogene Daten in die USA oder andere Drittstaaten übermitteln.[71] Die DS-GVO geht aber davon aus, dass bei der Übermittlung von Daten an Stellen außerhalb ihres Anwendungsbereichs ein hinreichendes Datenschutzniveau nur unter zusätzlichen Bedingungen angenommen werden kann, die in den Art 44ff. DS-GVO niedergelegt sind. Für Verantwortliche führt dies zu zusätzlichen Unwägbarkeiten und Anforderungen. Eine Grundlage für Datentransfers stellen die Beschlüsse der EU-Kommission über ein angemessenes Datenschutzniveau in Drittstaaten dar (Art. 45 DS-GVO). Im Falle der USA sind die dortigen Regelungen jedoch trotz einem Angemessenheitsbeschluss auf Grundlage von Übereinkommen zu besonderen Datenschutzrahmen vom EuGH wiederholt als unzureichende Grundlage für eine Übermittlung personenbezogener Daten qualifiziert wurden.[72] Die derzeitige Lösung für Datenübermittlungen in die USA ist das Trans-Atlantic Data Privacy Framework, bei dem jedoch auch aufgrund bereits angekündigter Klagen ebenfalls Unsicherheit verbleibt.[73]

Bei der Auswahl von KI-Systemen ist deshalb sorgfältig zu prüfen, ob Datenübermittlungen in Drittstaaten ausgeschlossen werden können. Auch im Hinblick auf die technisch-organisatorischen Maßnahmen (dazu unten) scheint es vorzugswürdig, Systeme nach Möglichkeit per Schnittstelle auf eigenen Servern zu betreiben oder personenbezogene Daten nur auf dem Gerät der oder des Nutzenden zu verarbeiten.

e) Profiling und automatisierte Entscheidung im Einzelfall

Einige Anwendungen von KI können im Einzelfall ein Profiling beinhalten. Dies gilt etwa, wenn personenbezogene Daten analysiert werden, um damit E-Learning-Angebote zu personalisieren und mithilfe von Schlüssen auf Merkmale wie Arbeitsleistung, persönliche Vorlieben oder Interessen z.B. Lernmaterial zu empfehlen oder das Umfeld auf einer E-Learning-Plattform zu gestalten. Eine Analyse solcher Aspekte stellt Profiling iSd Art. 4 Nr. 4 DS-GVO dar. Dieses ist in der DS-GVO über diese Definition hinaus nicht speziell geregelt, jedoch deutet die DS-GVO eine graduelle Steigerung einiger Pflichten an, wenn Profiling vorliegt.[74] Dies gilt insbesondere für Transparenzpflichten. Im Rahmen der Anwendung unbestimmter Rechtsbegriffe, die insbesondere in Rechtsgrundlagen und Datenschutzgrundsätzen vorhanden sind, ist ein Profiling als besonders eingriffsintensive Datenverarbeitung zu berücksichtigen.

Profiling kann auch in eine automatisierte Entscheidungsfindung im Einzelfall gemäß Art. 22 DS-GVO

70 Dies ist an der Erforderlichkeit für den Verarbeitungszweck zu bemessen, *Forgó/Graupe* in Epping NHG, 2. Aufl. 2024, § 17 Rn. 38.

71 Beispielsweise hat der LfDI Baden-Württemberg bei einer Prüfung von Microsoft Office 365 in einer für den Schuleinsatz konfigurierten Version weiterhin Datentransfers, insbesondere von Telemetrie- und Diagnosedaten, in die USA festgestellt, die nicht unterbunden werden können, https://www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen/ (Abruf 6.3.2024). In den Datenschutzhinweisen von OpenAI heißt es knapp: „Where required, we will use appropriate safeguards for transferring Personal Information outside of certain countries. We will only transfer Personal Information pursuant to a legally valid transfer mechanism.", https://openai.com/policies/privacy-policy (Abruf 6.3.2024).

72 EuGH, 6.10.2015, C-362/14 - Schrems = NJW 2015, 3151 und EuGH, 16.7.2020, C-311/18 - Facebook Ireland und Schrems = NJW 2020, 2613.

73 *Glocker*, ZD 2023, 189 (192ff.).

74 Für Beispiele aus der Praxis s. *Barros* Vale/Zanfir-Fortuna, Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities (2023), S. 20. Zu Informations- und Auskunftspflichten s.a. *Sesing*, MMR 2021, 288 (289f.).

übergehen. Eine solche Entscheidungsfindung, wie sie im Ausgangsbeispiel Ofqual anzunehmen sein dürfte,[75] unterliegt den zusätzlichen Rechtmäßigkeitsanforderungen einer speziellen Rechtsgrundlage für die Entscheidungsfindung sowie speziellen Schutzmaßnahmen (beispielsweise der Gewährleistung eines Rechts auf Anfechtung und menschliche Überprüfung). Derzeit ist keine der Rechtsgrundlagen aus Art. 22 Abs. 2 DS-GVO für die Hochschule einschlägig,[76] sodass KI-Einsatz im Anwendungsbereich der Regelung ausscheidet. Anwendbar sind diese Regelungen aber nur dann, wenn eine Entscheidung ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruht und rechtliche Wirkung entfaltet oder die betroffene Person in sonstiger Weise erheblich beeinträchtigt.

Ausgehend vom grundsätzlichen Befund der automatisierten Datenverarbeitung bei KI-Einsatz (III.2.a) sind das ausschließliche Beruhen einer Entscheidung darauf und die Wirkungen der Entscheidung für den Anwendungsbereich ausschlaggebend. Nachdem bislang – durchaus verbunden mit Kritik – die Anwendbarkeit dieser Regelungen auf die automatisierte Entscheidungsvorbereitung ganz überwiegend verneint wurde,[77] hat der EuGH in seiner jüngsten Entscheidung zum Kreditscoring die konzeptionelle Verbindung zwischen Profiling und automatisierter Einzelfallentscheidung unterstrichen und den Art. 22 DS-GVO für eine graduelle Anwendung geöffnet.[78] Das im Fall betroffene Kreditscoring, eine Form des bewertenden Profilings, kann danach nicht per se als reine Vorstufe zu einer automatisierten Entscheidung eingeordnet werden, sondern ist bereits selbst als Entscheidung iSd Art. 22 DS-GVO anzusehen, wenn ein vertragsbezogenes Verhalten Dritter, dem das Ergebnis des Profilings übermittelt wird, maßgeblich davon abhängt. Löst das Verhalten des Dritten eine den Anforderungen von Art. 22 DS-GVO entsprechende rechtliche Folge oder Beeinträchtigung unmittelbar aus, wird diese dem Profiling gewissermaßen zugerechnet.[79] Das Urteil lässt weitere Schlüsse zu: Insbesondere eröffnet es die Möglichkeit, dass eine mit KI-Unterstützung durch einen Menschen getätigte Entscheidung entsprechend dem zweiten Tatbestandsmerkmal des Art. 22 Abs. 1 DS-GVO ausschließlich auf einer automatisierten Verarbeitung beruhend einzustufen ist, wenn die finale Entscheidung dieses Menschen von der KI von einer durch KI mittels Profiling oder ähnliche automatisierte Datenverarbeitung ermittelten Bewertung maßgeblich abhängt.[80] Damit muss für die Beurteilung eines die Ausschließlichkeit unterbrechenden menschlichen Dazwischentretens statt einer formellen Betrachtung substanziell die Mensch-Maschine-Interaktion unter Beachtung von Faktoren wie insbesondere der Präsentationsform des KI-Outputs und ihrer arbeitsvertraglichen, betriebsorganisatorischen und arbeitspsychologischen Einbindung betrachtet werden.[81] In Zukunft können bei Hochrisiko-KI-Systemen dazu die Maßnahmen herangezogen werden, die das eingesetzte System aufgrund der Anbieterverpflichtung zur Gestaltung zugunsten wirksamer menschlicher Aufsicht in Art. 14 KI-VO ermöglicht[82] und die nach Art. 26 Abs. 2 KI-VO auch vom Nutzer umgesetzt worden sind. Die Beurteilung der Maßgeblichkeit ist von einer sorgfältigen Einzelfallprüfung abhängig.[83]

Nach alledem ist neben offensichtlichen Anwendungsfällen wie der vollautomatisierten Erkennung von Täuschungsversuchen oder Auswertung von Prüfungsleistungen auch beim Einsatz generativer KI für das Verfassen einer Prüfungsbewertung die Anwendbarkeit des Art. 22 DS-GVO denkbar. Zwar könnte man annehmen, es fehle an personenbezogenen Daten, wenn lediglich die Antworten eines Prüflings ohne identifizierende Merkmale in ein KI-System eingegeben werden,[84] doch dürfte nach EuGH-Rechtsprechung ein Personenbezug für die Hochschule bestehen, da die Antworten ihrem Verarbeitungszweck nach für die Bewertung des für sie identifizierbaren Prüflings verwendet werden.[85]

Auf dieser Datenverarbeitung kann eine Entscheidung nicht erst dann ausschließlich beruhen, wenn die

75 Zum Zeitpunkt des Einsatzes des Ofqual-Algorithmus im Sommer 2020 war das Vereinigte Königreich seit dem 31.01.2020 aus der Europäischen Union ausgetreten, jedoch galt ihr Inhalt als UK GDPR soweit ersichtlich bis 31.12.2020 unverändert fort. Im Zwischenbericht von Ofqual (Fn. 3) finden sich keine rechtlichen Ausführungen.

76 Eine vertragliche Notwendigkeit, lit. a), scheidet hier ebenso aus wie eine Einwilligung, lit. c) (s.o.). Allenfalls käme eine gesetzliche Regelung, lit. b), in Betracht, die soweit ersichtlich fehlt.

77 *Horstmann/Dalmer*, ZD 2022, 260 (263) mwN; zur Kritik *Krügel/Pfeiffenbring* (Fn. 53), § 11 Rn. 46ff.

78 EuGH, C-634/21 - Schufa Holding (Scoring) = NJW 2024, 413, Rn. 40ff.

79 Krit. *Thüsing/Peisker/Musiol*, RDV 2023, 82; *Taeger*, BKR 2024, 41; *Marsch/Kratz*, NJW 2024, 392 (393 Rn. 4f.).

80 So die Interpretation bei *Heine*, NZA 2024, 33 (36).

81 Vgl. dies nur andeutend *Heine* (Fn. 80), 36: Beurteilung im Einzelfall „anhand der internen Regeln und Praktiken des Verantwortlichen".

82 Diese sind auch in die zum KI-System gehörige Dokumentation (Art. 11 iVm Annex IV Nr. 2 (e), 3 KI-VO) sowie die Gebrauchsanweisungen (Art. 13 Abs. 3 (d) KI-VO) aufzunehmen.

83 Für eine Einzelfallprüfung des Dazwischentretens bei Entscheidungsempfehlungen schon *Horstmann/Dalmer* (Fn. 77), 262; *Heine* (Fn. 80), 36.

84 So geht *Hoeren* (Fn. 25), S. 37, jedenfalls davon aus, dass bei einem Einsatz von KI-Schreibtools in diesem Fall "datenschutzrechtlich nichts zu befürchten" sei, geht später aber trotzdem auf Art. 22 DS-GVO ein.

85 S. EuGH, 20.12.2017, C-434/16 - Nowak = ZD 2018, 113 Rn. 30.

korrigierende Person die zu einer Prüfungsleistung gehörenden Antworten vollständig als sog. Prompt eingibt und die Bewertung der KI unbesehen übernimmt, da dann ein menschliches Dazwischentreten ausbleibt. Auch vor der dargelegten EuGH-Entscheidung war es ganz hM, dass ein dazwischentretender Mensch jedenfalls eine inhaltliche Prüfung (mit umstrittener Tiefe) vornehmen und somit von den KI-generierten Ergebnissen abweichen können und dürfen muss.[86] Diese Prüfungskompetenz muss, wie das EuGH-Urteil bekräftigt, auch tatsächlich wahrgenommen werden.[87] Zentrales Merkmal des Art. 22 Abs. 1 DS-GVO ist die Entfaltung rechtlicher Wirkungen oder eine sonstige Beeinträchtigung in erheblicher Weise. Eine rechtliche Wirkung haben Verwaltungsakte wie Immatrikulation oder Exmatrikulation. Hängt von einer Prüfungsbewertung der Tatbestand eines gebundenen Verwaltungsaktes ab, wie im Falle des endgültigen Nichtbestehens (§ 19 Abs. 2 S. 2 Nr. 2 b) NHG), liegt es nahe, schon der Prüfungsbewertung diese rechtliche Wirkung zuzuordnen, da im Anschluss schon rechtlich kein Raum für eine menschliche Überprüfung in der Sache bleibt. Der unbestimmte Rechtsbegriff der sonstigen Beeinträchtigung in erheblicher Weise bedarf hingegen erheblicher Konkretisierung. Hierbei ist vor allem darauf abzustellen, wie nachhaltig auf die Position der betroffenen Person eingewirkt wird.[88] Bei der Bewertung der Erheblichkeit sind Auswirkungen auf Umstände, Verhalten und Entscheidungen der betroffenen Person ebenso zu berücksichtigen wie mögliche Diskriminierungen (s. ErwG 71 S. 6 DS-GVO)[89] und die Dauer der Auswirkungen.[90] Die Auswirkungen von Prüfungsentscheidungen sind in allen Aspekten für die persönliche und berufliche Lebensführung beträchtlich. Das Eingangsbeispiel verdeutlicht dabei, dass Notengebung indirekt auch über den Zugang zu Bildungseinrichtungen entscheidet. In grundrechtlichen Wertungen ausgedrückt kann eine Ungleichbehandlung beim Zugang zu Bildungseinrichtungen neben einer Diskriminierung auch eine Beeinträchtigung des Rechts auf Bildung aus Art. 14 GRCh darstellen.[91] Daher besteht beim Einsatz von KI in der Prüfung das Risiko eines zumindest mittelbaren Grundrechtseingriffs durch algorithmischen Bias. Schließlich ist zu beachten, dass nicht nur negative Entscheidungen vom Art. 22 DS-GVO erfasst werden. Vielmehr ist gerade die Benotung paradigmatisch dafür, dass die binäre Unterscheidung zwischen negativen und positiven bzw. belastenden und begünstigenden Entscheidungen für die Beurteilung der erheblichen Beeinträchtigung zu schematisch ist.[92] Aufgrund dieser Grundrechtsrelevanz überschreiten Prüfungsentscheidungen auch ohne die Folge des endgültigen Nichtbestehens in aller Regel die Schwelle der Erheblichkeit.

Weniger eindeutig zu beurteilen sind Leistungs- oder Lernstandsüberprüfungen ohne Außenwirkungen, beispielsweise Übungsklausuren und Tests, die auch im Selbststudium auf E-Learning-Plattformen erfolgen können. Denkbar ist sowohl die Auswahl und Zusammenstellung der Testaufgaben als auch ihre Auswertung mittels KI. Eine rechtliche Wirkung bleibt hierbei aus. Auch sind diese Bewertungen nicht unmittelbar mit Folgen für Rechte oder Freiheiten der betroffenen Personen verbunden. Naheliegend scheint hingegen angesichts des mit solchen Tests verfolgten didaktischen Zwecks, dass sie sich über Lernmotivation und Selbstbild der Studierenden mittelbar auf den Studienerfolg auswirken. Auch ist besonders zu berücksichtigen, dass an Hochschulen regelmäßig minderjährige Studierende betroffen sind. Diese sind als Kinder iSd DS-GVO zu verstehen[93] und die Regeln des Art. 22 DS-GVO in der Folge strenger zu handhaben (s. ErwG 71 S. 5).[94] Die Anwendbarkeit des Art. 22 DS-GVO erscheint daher zwar idR fernliegend, doch nicht vollkommen ausgeschlossen. Dies sollte reflektiert werden, wenn über die Einführung entsprechender Systeme nachgedacht wird.[95] Dies gilt besonders mit Blick darauf, die bei der Beurteilung der erheblichen Beeinträchtigung zu berücksichtigenden Biases und Diskriminierungsrisiken abzuschätzen.

Eine neue Qualität würde freilich erreicht, wenn die Ergebnisse die individuelle Sphäre der Studierenden ver-

86 *Krügel/Pfeiffenbring* (Fn. 53), § 11 Rn. 45 mwN.

87 *Krügel/Pfeiffenbring* (Fn. 53), § 11 Rn. 45; *Günther/Gerigk/Berger* (Fn. 67), 236.

88 *Martini* in Paal/Pauly, 3. Aufl. 2021, Art. 22 DS-GVO Rn. 27.

89 *Heine* (Fn. 80), 36.

90 Art.-29-Arbeitsgruppe, WP251rev.01 – Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, 6.2.2018, S. 23.

91 *Jarass* in Jarass, Charta der Grundrechte der EU, 4. Auflage 2021, Art. 14 Rn. 10.

92 *Martini* in Paal/Pauly, 3. Aufl. 2021, Art. 22 DS-GVO Rn. 28.

93 Eine Legaldefinition mit der Altersgrenze von 18 Jahren in Art. 4 Nr. 18 des DS-GVO-Kommissionsentwurfs wurde zwar abgelehnt, Art. 8 Abs. 1 S. 1 DS-GVO zeigt aber, dass die Altersgrenze jedenfalls über 16 Jahren liegt (für Volljährigkeit als Grenze *Martini/Nink*, NVwZ-Extra 2017, 1 (6 Fn. 53). Auch die Auslegung im Lichte der GRCh und internationalen Rechts spricht für diese Grenze (*Frei*, Bucerius L. J. 2022, 74 (75)).

94 Dies ist auch die Schlussfolgerung der Art.-29-Arbeitsgruppe (Fn. 90), S. 31 aus ErwG 71 S. 5, dessen Wortlaut im Kontrast zum Fehlen eines absoluten Verbots in den verfügenden Teil steht.

95 Zudem ist zu beachten, dass der Anwendungsbereich des Hochrisiko-Regimes im KI-VO in Annex III Nr. 3 (b) gegenüber dem ursprünglichen Kommissionsentwurf auch auf KI-Systeme zur Bewertung von Lernergebnissen ausgeweitet wurde, auch wenn diese Ergebnisse zur Steuerung des Lernprozesses dienen.

ließen und beispielsweise genutzt würden, um Lehrende auf Defizite individueller Studierender hinzuweisen oder Studierende direkt bestimmten Kursangeboten zuzuweisen. Ein solcher didaktischer Einsatz nähert sich dem Einsatz zu Prüfungszwecken an und die vorhandene Außenwirkung könnte in vielen Fällen den Anwendungsbereich des Art. 22 DS-GVO eröffnen.[96]

Soll andersherum die Möglichkeit der Teilnahme an einem Kursangebot – sei es zur Auswahl förderungsbedürftiger oder besonders leistungsfähiger Kursteilnehmender – ohne wesentliche menschliche Mitwirkung vom Ergebnis eines KI-Systems abhängen, ist Art. 22 DS-GVO vollumfänglich einschlägig. Vorzugswürdig erschiene es in dieser Hinsicht, Selbstüberprüfungen mithilfe von KI zu ermöglichen, das Aufsuchen von Unterstützungsangeboten aber den Studierenden selbst anheimzustellen. Auf diese Weise können mögliche Vorteile von KI bei der Allokation von Lehrangeboten mit datenschutzrechtlichen Anforderungen vereinbart werden.

Zusammenfassend ist eine vollständige Delegation der Bewertung von Prüfungsleistungen an ein KI-System damit mangels entsprechender Rechtsgrundlagen aus Art. 22 Abs. 2 DS-GVO und auch prüfungsrechtlich idR ausgeschlossen.[97] Die Verwendung als rein sprachliche Formulierungshilfe oder zur ergänzenden Überprüfung der eigenen Einschätzung schließt dieser Befund hingegen auch für Einsatzzwecke über der Erheblichkeitsschwelle des Art. 22 Abs. 1 DS-GVO nicht aus, solange die menschliche Beurteilung maßgeblich bleibt. Je stärker sich aus einem KI-generierten Ergebnis eine in sich bereits abgeschlossene und vollständige Bewertung ergibt und je intransparenter diese zustande kommt,[98] desto eher sind systemgestalterische und arbeitsorganisatorische Maßnahmen zu treffen, die eine Wahrnehmung der inhaltlichen Prüfungskompetenz durch die Lehrenden auch de facto sicherstellen. Bei Tests mit rein didaktischer Zielsetzung, die nicht die Sphäre des Selbststudiums verlassen, ist eine Einzelfallprüfung notwendig. Didaktische Anwendungen, die Lernmaterial aufbereiten und präsentieren, überschreiten die Erheblichkeitsschwelle des Art. 22 DS-GVO idR nicht – dennoch sollten mögliche Risiken, beispielsweise durch Biases, ungleiche Ausgangsbedingungen für Studierende bezüglich der effektiven Anwendung oder die Wahrnehmung von KI-Vorschlägen als besonders objektiv oder autoritativ (sog. automation bias) vorab reflektiert werden.

Ergänzt werden diese Regelungen der DS-GVO in Zukunft um die Vorgaben aus den Art. 14, 26 Abs. 2 KI-VO. Danach müssen Anbieter von Hochrisiko-KI-Systemen diese so gestalten, dass sie während ihres Einsatzes eine wirksame menschliche Aufsicht erlauben (Abs. 1). Diesem Ziel dienen je nach Risiko, Autonomielevel und Kontext die technische Konstruktionsweise (Abs. 3 a)) und die Identifizierung von im Einsatz umzusetzenden Maßnahmen (Abs. 3 b)). Die in Art. 14 Abs. 4 KI-VO aufgezählten Anforderungen dahingehend, zu welchen konkreten Formen von Aufsicht die KI-Systeme die beaufsichtigenden Menschen befähigen müssen, dürften auch die Gewährleistung menschlichen Eingreifens beim Einsatz von Drittanbieter-KI in der Entscheidungsfindung erleichtern. Die Nutzer, hier die Hochschulen, trifft auch nach der KI-VO die Pflicht, diese Maßnahmen entsprechend den Gebrauchsanweisungen umzusetzen und für eine entsprechende Kompetenz, Schulung und Berechtigung sowie notwendige Unterstützung der beaufsichtigenden Menschen zu sorgen (Art. 26 Abs. 1, 2 KI-VO). Die Wirkung dieser technikbezogenen Vorschriften für die praktische Umsetzung der DS-GVO sollte nicht unterschätzt werden. Dies gilt nicht nur für ein menschliches Dazwischentreten während der Entscheidungsfindung, sondern auch für die menschliche Überprüfung bei erlaubten automatisierten Entscheidungen im Rahmen des gemäß Art. 22 Abs. 2 lit. b) iVm ErwG 71 S. 4, Abs. 3 DS-GVO zu gewährleistenden Anfechtungsrechts.

f) Technisch-organisatorischer Datenschutz und Datenschutz-Folgenabschätzung

Ein großer Teil der konkreten Auswirkungen und Risiken des KI-Einsatzes lässt sich auf Fragen zurückführen, die durch die Inbezugnahme der personenbezogenen Daten des Einzelnen nur unzureichend adressiert werden – etwa solche der verwendeten statistisch-mathematischen Methoden, impliziter Annahmen und der Validität und Legitimität gruppenbezogener Schlussfolgerungen. Daher ist der klassische Ansatz des individuellen Schutzes in Bezug auf konkrete Verarbeitungstätigkeiten in seiner Steuerungskraft bei KI begrenzt.[99] Das lässt technische, organisatorische und system- statt verarbeitungsbezogene Vorgaben des Datenschutzrechts an

[96] EuGH, 7.12.2023, C-634/21 - Schufa Holding (Scoring) = NJW 2024, 413, Rn. 48-50 verdeutlicht, dass die beeinträchtigende Wirkung einer automatisierten Bewertung auch durch menschliches Verhalten vermittelt werden kann.

[97] Letztere ist vom Landesrecht und den Prüfungsordnungen abhängig, s. *Hoeren* (Fn. 25), S. 36f. Auch das Erfordernis bestimmter, personengebundener Qualifikationen des Prüfenden (dazu *Epping* in Epping NHG, 2. Aufl. 2024, § 24 Rn. 50) kann den KI-Einsatz mittelbar einschränken.

[98] Zu diesem Risiko auch HmbBfDI (Fn. 29), S. 4f.

[99] *Dreyer/Schulz* (Fn. 35), S. 39.

Bedeutung gewinnen. Diese dürften mit den technikrechtlichen Anforderungen der KI-VO in der Umsetzung die größten Synergien aufweisen und in der Schutzwirkung ergänzen.

Eine Pflicht zur Datenschutz-Folgenabschätzung (DSFA, Art. 35 DS-GVO) liegt bei vielen Einsatzmöglichkeiten von KI nahe, insbesondere bei profilingähnlichen Analysen oder Bewertungen oder dem Einsatz von nach dem Stand der Technik neuen Technologien. Da an der Hochschule mit Studierenden, insbesondere bei Minderjährigkeit und in Prüfungssituationen, besonders schutzbedürftige Personen betroffen sind, ist in einem solchen Fall aufgrund der Kombination zweier Risiko-Indikatoren auch nach Meinung der Aufsichtsbehörden in den meisten Fällen die DSFA gemäß Art. 35 Abs. 1 DS-GVO obligatorisch.[100] Die DSFA ist vor dem Beginn des KI-Einsatz nach den Maßgaben des Art. 35 Abs. 7-11 DS-GVO durchzuführen. Zukünftig bietet es sich an, sie gemeinsam mit der ggf. nach Art. 27 KI-VO verpflichtenden Abschätzung der Grundrechtsauswirkungen vorzunehmen.

Zentral für den technischen und organisatorischen Datenschutz sind die Art. 24, 25, 32 DS-GVO. Der Verantwortliche hat danach unter Berücksichtigung des Stands der Technik, der Kosten und der spezifischen Merkmale und Umstände der Verarbeitung sowie der (ggf. im Rahmen der DSFA ermittelten) damit verbundenen Risiken technische und organisatorische Maßnahmen zur wirksamen Umsetzung der Datenschutzgrundsätze und des Schutzes der betroffenen Personen zu ergreifen. Die Orientierung an den Datenschutzgrundsätzen, insbesondere der Datenminimierung und der Zweckbindung, zeigt dabei die Stoßrichtung der Maßnahmen nach Art. 25 DS-GVO auf, während Art. 32 DS-GVO v.a. Datensicherheitsmaßnahmen erfordert.[101] Insbesondere bei der Einbindung von KI-Systemen auf E-Learning-Plattformen oder sonstiger Nutzung mit einem personengebundenen Konto sind datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) vorzunehmen, wozu eine pseudonyme Nutzungsmöglichkeit gehören kann. Aber schon in der Systemgestaltung ist der Datenschutz zu berücksichtigen. Letztlich spricht dies für die Auswahl und Gestaltung von datensparsamen KI-Systemen und die Nutzung einer möglichst geringen Zahl an personenbezogenen Parametern gemessen am Einsatzzweck.

Ein Datenschutzniveau im Sinne dieser Vorgaben kann erreicht werden, wenn die Hochschule die Nutzung von KI-Angeboten über eine Schnittstelle (API) mittels hochschulgebundener Konten bzw. Anwendungen ermöglicht. Das Beispiel von ChatGPT verdeutlicht dies: Durch den Anbieter OpenAI werden in diesem Fall laut eigener Beschreibung keine eingegebenen Daten für das Training verwendet und die Identität der Nutzenden ist OpenAI nicht bekannt.[102] Erste deutsche Hochschulen bieten deshalb bereits eine solche Nutzung von ChatGPT für ihre Studierenden an.[103] Dabei werden neben den für die Website-Bereitstellung technisch erforderlichen Log-Files lediglich personenbezogene Login-Daten eingegeben, um die Zugangsberechtigung zu überprüfen.[104] Unklar bleibt dabei, was mit bei der Nutzung anfallenden Nutzungs- und Metadaten geschieht. Nutzen die Studierenden hingegen - freilich idR außerhalb der rechtlichen Verantwortlichkeit der Hochschule - private Konten zu studienbezogenen Zwecken, besteht aber auch dieser Schutz nicht, zudem kann es durch Verbindung studienbezogener und privater Informationen zu einem tieferen Eingriff in das Privatleben kommen.[105] Daher erscheint es auch unter diesem Gesichtspunkt sinnvoll, klare Regelungen für den Einsatz von (generativer) KI in der Lehre in universitäre Ordnungen aufzunehmen, die den Einsatz unter der Voraussetzung einer solchen datenschutzfreundlichen Gestaltung ermöglichen. Eingedenk der obigen Feststellung, dass auch Forschende proaktiv den Einsatz von KI als Arbeitsmittel erproben, können entsprechende APIs zur Verbesserung des Datenschutzes (sowie des Schutzes forschungsbezogener Geheimhaltungsinteressen) auch für Forschende bereitgestellt werden.

V. Fazit und Ausblick

Mit der Verbreitung von KI kommt es auch den Hochschulen zu, die Potenziale des KI-Einsatzes in ihren Aufgabenbereichen aufzunehmen und insbesondere die Einbindung von KI in die Lehre kurz- bis mittelfristig aktiv zu gestalten. So können sie ihre ausbildungsbezogenen Aufgaben in einem absehbar von KI geprägten

[100] Art.-29-Arbeitsgruppe, WP248 Rev. 01 - Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", S. 10ff.

[101] Hierbei sind KI-spezifische Angriffsrisiken zu berücksichtigen, s. u.a. *Veale/Binns/Edwards* (Fn. 43); *Boenisch* (Fn. 43).

[102] FAQ: Enterprise privacy at OpenAI (Fn. 18).

[103] Forschung & Lehre: Erste Hochschulen bieten ChatGPT an, https://www.forschung-und-lehre.de/management/erste-deutsche-hochschulen-bieten-chatgpt-an-6040 (Abruf 29.02.2024).

[104] Datenschutzerklärung zu HAWKI: GPT für die Hochschule, https://ai.hawk.de/views/datenschutz.html (Abruf 29.02.2024).

[105] Analog empfiehlt der HmbBfDI (Fn. 29), S. 2, aus diesen Gründen die Bereitstellung dienstlicher Konten für Mitarbeitende.

Umfeld adäquat erfüllen. Denn der wissenschaftlich geschulte, d.h. methodische und kritische, Umgang mit KI-Anwendungen ist nicht nur Teil beruflicher Anforderungen an Hochschulabsolventen,[106] sondern auch der persönlichen Entfaltung und demokratischen Teilhabe in einer immer stärker von Algorithmen geprägten Gesellschaft förderlich. Diesen Blick auf die Entwicklung nimmt der europäische Gesetzgeber wenigstens in Ansätzen normativ auf, indem er den im Bildungsbereich oft einschlägigen Anforderungen an Hochrisiko-KI in der KI-VO Forderungen nach Digitalkompetenzen und AI literacy zur Seite stellt (u.a. ErwG 20, 91, 165, Art. 4, 95 KI-VO). Wer wäre in einer besseren Position zur Verwirklichung dieser Forderung als die Hochschulen?

Das heißt nicht, allen durch KI geweckten Erwartungen eilig zu entsprechen. Klare Grenzen für unerwünschte Formen der Automatisierung liefert das Datenschutzrecht, insbesondere mit dem Verbot der automatisierten Entscheidung im Einzelfall und zumal bei Betroffenheit schutzbedürftiger Gruppen. Darüber hinaus aber gibt das Datenschutzrecht, ebenso wie die künftige KI-Regulierung, Verantwortlichen einen Gestaltungsauftrag für einen grundrechtskonformen und abgewogenen KI-Einsatz, den erste Hochschulen bereits angenommen haben. Technik- und systembezogene Vorgaben spielen dabei eine herausgehobene Rolle. Mit Verweis auf das Eingangsbeispiel sei aber daran erinnert, dass KI-Lösungen an der Hochschule auch jenseits rein technischer Gestaltungsoptionen offen für Kritik und Partizipation sowie die Wahrnehmung autonomer Handlungsspielräume gestaltet werden müssen. Im Datenschutzrecht bieten dabei vor allem die Datenschutzgrundsätze die materielle Orientierung. Doch auch wenn man die Relevanz des Datenschutzrechts nicht abstreiten kann, ist es kein „Law of Everything"[107] für Fragen des KI-Einsatzes. Den im Hochschulbereich betroffenen Grundrechten und anderen einfachrechtlichen Vorgaben muss daher in ihrem Zusammenspiel mit dem Datenschutzrecht entsprechende Aufmerksamkeit gelten. In Zukunft wird zudem die KI-VO häufig neben der DS-GVO Anwendung finden und wichtige Qualitäten der KI-Systeme und ihres Einsatzes prägen, etwa bei Transparenz und Erklärbarkeit sowie Schutz vor Biases und Diskriminierung.

Konkret können Hochschulen in ihren Satzungen Regelungen zur Ermöglichung des KI-Einsatzes festlegen. Dabei bieten sich neben den gesetzlich notwendigen datenschutzrechtlichen Regelungen auch Gestaltungs- und Verfahrensvorschriften an. Zu berücksichtigen ist, dass personenbezogene Daten in der digitalen Gesellschaft nicht mehr lediglich für die organisatorische Durchführung der Hochschullehre notwendig sind (so wie es den gesetzlichen Rechtsgrundlagen wie § 17 NHG noch erkennbar zugrunde liegt), sondern faktisch auch beim eigentlichen Lehren und Lernen mit digitalen Mitteln eine Rolle spielen.

Prof. Dr. Margrit Seckelmann ist Professorin für Öffentliches Recht und das Recht der digitalen Gesellschaft an der Leibniz Universität Hannover (Institut für Rechtsinformatik).

Dipl.-Jur. Jan Horstmann ist wissenschaftlicher Mitarbeiter am Institut für Rechtsinformatik, Leibniz Universität Hannover.

[106] Zumal solcher, die die in Zukunft zu gewährleistende, effektive menschliche Aufsicht über Hochrisiko-KI-Systeme übernehmen werden (Art. 14, 26 Abs. 2 KI-VO).

[107] *Purtova* (Fn. 42).