„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

9/2026
September 2026

Wer überwacht die KI?

Die KI-VO schreibt für Hochrisiko-KI-Systeme eine menschliche Aufsicht vor

Aller guten Dinge sind drei?

Neuer Gesetzesentwurf enthält Regelungen zur Verarbeitung von Verkehrsdaten und zur Speicherung von IP-Adressen

Was bedeutet digitale Souveränität für Universitäten und Hochschulen?

Digitale Abhängigkeiten können die akademische Selbstbestimmung gefährden. Wie können Hochschulen ihre digitale Souveränität stärken?

Kurzbeitrag: Aufsichtspflicht für KI-Content

Für KI-generierte Inhalte haftet, wem diese als eigene Äußerung zugerechnet werden können

Wer überwacht die KI?

Die KI-VO schreibt für Hochrisiko-KI-Systeme eine menschliche Aufsicht vor

Von Philipp Schöbel

Im Infobrief wurden schon mehrere Aspekte der Verordnung über Künstliche Intelligenz (KI-VO) besprochen.[1] Hochschulen und Forschungseinrichtungen können nicht nur Betreiber:innen, sondern auch Anbieter:innen von Hochrisiko-KI-Systemen sein.[2] In diesem Fall müssen sie unter anderem sicherstellen, dass das Hochrisiko-KI-System die Anforderungen an die menschliche Aufsicht erfüllt (Art. 14 i.V.m. Art. 16 lit. a KI-VO).

I. Einleitung

Die autonome Ausführung von Arbeitsabläufen durch KI führt dazu, dass Entscheidungen, die ursprünglich durch Menschen getroffen wurden, an technische Systeme ausgelagert werden. Dadurch kann es zu Risiken für die Grundrechte der betroffenen Personen kommen. Werden etwa Studienplätze mittels eines KI-Systems vergeben, besteht die Gefahr, dass einzelne Personengruppen durch das System diskriminiert werden. Die Ursache hierfür kann etwa darin liegen, dass diskriminierende Annahmen in den Datensätzen enthalten sind, mit denen das dem KI-System zugrunde liegende Modell trainiert wurde. Die Folge wäre etwa, dass Menschen, die eigentlich einen Studienplatz bekommen sollten, der Zugang zum Studium aufgrund einer falschen maschinellen Entscheidung verwehrt wird.

Verschiedene Anforderungen an die Entwicklung von KI-Systemen sollen die Grundrechte von betroffenen Personen schützen. Hierzu gehören die Einrichtung eines Risikomanagementsystems (Art. 9 Abs. 2 S. 2 lit. a KI-VO), Anforderungen an die Daten (Art. 10 Abs. 2 S. 2 lit. f KI-VO), die Bereitstellung einer Betriebsanleitung (Art. 13 Abs. 3 lit. b Ziff. iii KI-VO) sowie die Sicherstellung menschlicher Aufsicht (Art. 14 Abs. 2 KI-VO).

II. Der Begriff der menschlichen Aufsicht in der KI-VO

Neben dem Grundrechtsschutz soll das Konzept der menschlichen Aufsicht dafür sorgen, dass die menschliche Autonomie nicht untergraben wird.[3] Für das Konzept der menschlichen Aufsicht über KI-Systeme werden oftmals drei verschiedene Umsetzungsarten beschrieben: „Human in the Loop", „Human on the Loop" und „Human in Command".[4] „Human in the Loop" meint, dass ein Mensch die Fähigkeit hat, in jeden Entscheidungszyklus des überwachten KI-Systems einzugreifen. Dagegen bedeutet „Human on the Loop", dass ein Mensch den Betrieb des KI-Systems überwacht und in den Entwurfsszyklus des KI-Systems eingreifen kann. Bei diesem Ansatz ist kein menschliches Eingreifen in jede einzelne Entscheidung erforderlich.[5] Mit „Human in Command" ist gemeint, dass ein Mensch den Gesamtbetrieb des KI-Systems überwachen kann und darüber

1 Siehe etwa: Schöbel, AI Act – Licht der Europäischen Union, DFN-Infobrief Recht 12/2024, S. 7 - 12; Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025, S. 2 - 7; KI-Modelle made in Europe?, DFN-Infobrief Recht 4/2025, S. 14 - 20; Friedl, Mit digitalen Wasserzeichen zu klareren Informationsökosystemen?, DFN-Infobrief Recht 5/2026, S. 2 - 5.

2 Vgl. Schöbel, Was sind Quasi-Anbieter von KI-Systemen?, DFN-Infobrief Recht 1/2026, S. 11 - 14.

3 Hochrangige Expertengruppe für künstliche Intelligenz, Ethikleitlinien für vertrauenswürdige KI, 2019, S. 19, abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/ethics-guidelines-trustworthy-ai, alle Quellen zuletzt abgerufen am 20.07.2026.

4 Hochrangige Expertengruppe für künstliche Intelligenz, Ethikleitlinien für vertrauenswürdige KI, 2019, S. 19.

5 Schippel, KIR 2025, 368, 371.

hinaus die Entscheidungsmöglichkeit über das „Wann“ und „Wie“ des Einsatzes des KI-Systems hat. Dies bedeutet, dass die überwachende Person über Einsatz, Unterbrechung und Außerkraftsetzung des KI-Systems entscheiden kann und dessen gesellschaftliche, rechtliche und ethische Auswirkungen steuert.[6] Die KI-VO selbst bestimmt nicht ausdrücklich, welche dieser drei Umsetzungsarten mit Art. 14 Abs. 1 KI-VO verfolgt wird.[7] Jedoch werden die weiteren Anforderungen der KI-VO so ausgelegt, dass die menschliche Aufsicht regelmäßig im Sinne des „Human in Command“ umzusetzen ist.[8]

III. Akteur:innen der menschlichen Aufsicht

Für die menschliche Aufsicht sind zwei verschiedene Akteur:innen in der KI-VO verantwortlich. Die Anbieter:innen müssen das Hochrisiko-KI-System so entwickeln, dass es während seiner Verwendung von Menschen wirksam beaufsichtigt werden kann (Art. 14 Abs. 1 KI-VO). Daneben bestehen Pflichten zur Umsetzung der menschlichen Aufsicht für die Betreiber:innen des KI-Systems. Betreiber:innen von Hochrisiko-KI-Systemen sind dazu verpflichtet, natürlichen Personen die Aufsicht über das KI-System zu übertragen (Art. 26 Abs. 2 KI-VO). Diese Personen müssen zum einen über die für die menschliche Aufsicht erforderliche Kompetenz und Ausbildung verfügen. Zum anderen müssen sie auch die erforderlichen Befugnisse haben. Es reicht nicht, wenn eine Person zwar kompetent, aber nicht befugt oder zwar inkompetent, aber befugt ist, die menschliche Aufsicht auszuüben.[9] Eine Person, die etwa den Einsatz von KI-Systemen im Bereich der Hochschulzulassung überwacht, muss über die erforderlichen Fähigkeiten, Kenntnisse und das Verständnis verfügen, um die KI-spezifischen Risiken für die Grundrechte der betroffenen Bewerber:innen einzuschätzen (vgl. Art. 3 Nr. 56 KI-VO) und die Befugnis haben, Fehler zu verhindern und zu korrigieren.

IV. Anforderungen an die menschliche Aufsicht

Die menschliche Aufsicht dient der Verhinderung und Minimierung der Risiken für Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird (Art. 14 Abs. 2 KI-VO). Die menschliche Aufsicht muss grundsätzlich während des gesamten Lebenszyklus des Hochrisiko-KI-Systems möglich sein.[10] Die Anforderungen an die Aufsichtsmaßnahmen sind nicht starr und müssen den Risiken, dem Grad der Autonomie und dem Kontext der Nutzung des Hochrisiko-KI-Systems angemessen sein (Art. 14 Abs. 3 KI-VO). Dabei wird grundsätzlich zwischen zwei Arten von Vorkehrungen unterschieden, zwischen deren Umsetzung die Anbieter:innen entscheiden können: Maßnahmen, die in das System integriert sind, und Maßnahmen, die von den Betreiber:innen umgesetzt werden.[11]

Die Anforderungen an die menschliche Aufsicht werden in fünf Anforderungskategorien näher konkretisiert. Diese umfassen das Verständnis der Systemfähigkeiten und -grenzen (Art. 14 Abs. 4 lit. a KI-VO), das Bewusstsein für Automatisierungsverzerrungen (Art. 14 Abs. 4 lit. b KI-VO), die Fähigkeit zur Interpretation der Systemausgaben (Art. 14 Abs. 4 lit. c KI-VO), die Entscheidungskompetenz (Art. 14 Abs. 4 lit. d KI-VO) sowie die technische Eingriffs- und Unterbrechungsmöglichkeit (Art. 14 Abs. 4 lit. e KI-VO).[12]

1. Verständnis der Systemfähigkeiten und -grenzen

Das Hochrisiko-KI-System soll so zu Verfügung gestellt werden, dass es den Betreiber:innen ermöglicht, die einschlägigen Fähigkeiten und Grenzen des Hochrisiko-KI-Systems angemessen zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen

6 Schippel, KIR 2025, 368, 371.

7 Bogdan, ZfPC 2026, 90, 93.

8 Schippel, KIR 2025, 368, 371; Bogdan, ZfPC 2026, 90, 93; Buchner, in: BeckOK KI-Recht, 6. Ed. 1.5.2026, KI-VO Art. 14 Rn. 37.

9 Vgl. I. Eisenberger/Th. Binder, in: Martini/Wendehorst, 2. Aufl. 2026, KI-VO Art. 26 Rn. 25.

10 Schippel, KIR 2025, 368.

11 Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 86.

12 Vgl. Schippel, KIR 2025, 368, 369.

(Art. 14 Abs. 4 lit. a Hs. 1 KI-VO). Die umfasst auch das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung (Art. 14 Abs. 4 lit. a Hs. 2 KI-VO).
Für ein Systemverständnis sind zum einen allgemeine Grundkenntnisse der eingesetzten Technologie und zum anderen spezifische Kenntnisse über das eingesetzte KI-System relevant.[13] Das Verständnis des eingesetzten KI-Systems kann etwa durch technische Hinweise, eine Betriebsanleitung oder eine Testphase vermittelt werden.[14] Die Erwartungen der Anbieter:innen an die vorhandenen Kompetenzen der Aufsichtspersonen dürfen nicht unrealistisch sein; insoweit ist von einer durchschnittlichen Person ohne außergewöhnliches Talent auszugehen.[15] Eine ordnungsgemäße Überwachung erfordert tatsächliche Kontrolle und kein bloßes „Durchwinken" von KI-Entscheidungen.[16] Ein Beispiel für eine Umsetzungsmaßnahme sind etwa Visualisierungswerkzeuge, die Einflussfaktoren, Aktivierungsmustern und Modellverläufen darstellen, um so die Erkennung von Auffälligkeiten des KI-Systems zu ermöglichen.[17]

2. Bewusstsein für Automatisierungsverzerrungen

Nach der zweiten Anforderungskategorie sollen Betreiber:innen in die Lage versetzt werden, sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in die von einem Hochrisiko-KI-System hervorgebrachte Ausgabe („Automatisierungsbias") bewusst zu bleiben (Art. 14 Abs. 4 lit. b Hs. 1 KI-VO). Dies gilt insbesondere, wenn Hochrisiko-KI-Systeme Informationen oder Empfehlungen ausgeben, auf deren Grundlage natürliche Personen Entscheidungen treffen (Art. 14 Abs. 4 lit. b Hs. 2 KI-VO). Die Aufsichtspersonen sollen etwa durch Training zur kritischen Distanz gegenüber KI-Ausgaben befähigt werden.[18] Ein Beispiel für Sicherungsmaßnahmen sind etwa kontextbezogene Warnhinweise, die eine menschliche Nachprüfung empfehlen.[19] Für besonders grundrechtssensible Bereiche wird gefordert, dass neben Warnhinweisen von den Aufsichtspersonen eine Begründung verlangt wird, in der sie ihre Auseinandersetzung mit der Entscheidung des Systems darlegen.[20]

3. Fähigkeit zur Interpretation der Systemausgaben

Das KI-System soll den Betreiber:innen so zur Verfügung gestellt werden, dass sie seine Ausgaben richtig interpretieren können (Art. 14 Abs. 4 lit. c KI-VO). Die menschliche Aufsichtsperson muss in der Lage sein, die Informationen oder Empfehlungen des verwendeten KI-Systems richtig einzuordnen.[21] Dies setzt ein technisches Grundverständnis und ein Verständnis der Logik des eingesetzten KI-Systems voraus.[22] Auch hier können verschiedene Erklärbarkeitsmechanismen verwendet werden, wobei die tatsächliche Komplexität eines KI-Systems nicht immer darstellbar sein wird.[23] Inhaltlich ähnelt die Anforderung zur Interpretationsfähigkeit der Anforderung des Systemverständnisses (Art. 14 Abs. 4 lit a KI-VO).[24]

4. Entscheidungskompetenz

Das alleinige Erkennen einer fehlerhaften KI-Entscheidung durch eine Aufsichtsperson reicht regelmäßig nicht aus, um Schäden

13 Schippel, KIR 2025, 368, 369; Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 98.

14 Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 98; Schippel, KIR 2025, 368, 369.

15 Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 98.

16 Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 100; Schippel, KIR 2025, 368, 369.

17 Bomhard/Wietzke, in: Bomhard/Pieper/Wende, 1. Aufl. 2025, KI-VO Art. 14 Rn. 22.

18 Schippel, KIR 2025, 368, 370.

19 Bomhard/Wietzke, in: Bomhard/Pieper/Wende, 1. Aufl. 2025, KI-VO Art. 14 Rn. 25.

20 Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 113.

21 Buchner, BeckOK KI-Recht, 6. Ed. 1.5.2026, KI-VO Art. 14 Rn. 56.

22 Schippel, KIR 2025, 368, 370.

23 Bomhard/Wietzke, in: Bomhard/Pieper/Wende, 1. Aufl. 2025, KI-VO Art. 14 Rn. 26.

24 Hilgendorf/Härtlein, in: HK-KI-VO, 1. Aufl., KI-VO Art. 14 Rn. 8.

zu verhindern.[25] Die Aufsichtspersonen müssen daher die Möglichkeit haben, in den Prozess des KI-Systems einzugreifen.[26] Die Betreiber:innen sollen in der Lage sein, in einer bestimmten Situation zu beschließen, das Hochrisiko-KI-System nicht zu verwenden oder die Ausgabe des Hochrisiko-KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen (Art. 14 Abs. 4 lit. d KI-VO).

5. Technische Eingriffs- und Unterbrechungsmöglichkeit

Schließlich soll es den Betreiber:innen möglich sein, in den Betrieb des Hochrisiko-KI-Systems einzugreifen oder ihn zu unterbrechen (Art. 14 Abs. 4 lit. e KI-VO). Das KI-System muss etwa durch eine „Stopptaste" in einem sicheren Zustand zum Stillstand gebracht werden können (Art. 14 Abs. 4 lit. e KI-VO). Das Anhalten mittels Stopptaste darf seinerseits nicht zu erneuten Risiken führen.[27] Im Fall eines selbstfahrenden Fahrzeugs bedeutet dies etwa, dass das Fahrzeug auf dem Standstreifen und nicht auf der Fahrbahn zum Stehen kommt.[28]

V. Betriebsanleitung und menschliche Aufsicht

Das Hochrisiko-KI-System muss mit einer Betriebsanleitung versehen sein (Art. 14 Abs. 2 KI-VO). Dort muss auch die Umsetzung der menschlichen Aufsicht dargestellt werden (Art. 13 Abs. 3 lit. d KI-VO). Die Betriebsanleitung enthält Informationen, um den Betreiber insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung des KI-Systems zu informieren (Art. 3 Nr. 15 KI-VO). Die Informationen der Betriebsanleitung müssen vollständig, korrekt und eindeutig sein (Art. 13 Abs. 2 KI-VO). Zudem muss die Form der Informationen für die Betreiber:innen relevant, barrierefrei zugänglich und verständlich sein.

VI. Fazit

Auch KI-Anwendungen im Hochschulbereich können anwendungsbezogene Hochrisiko-KI-Systeme darstellen (Art. 6 Abs. 2 i. V. m. Anhang III KI-VO).[29] Die KI-VO schreibt für Hochrisiko-KI-Systeme eine menschliche Aufsicht vor. Als Anbieter:innen wären Hochschulen und Forschungseinrichtungen dazu verpflichtet, für ihre KI-Systeme entsprechende Vorkehrungen zu treffen. Als Betreiber:innen müssen sie die menschliche Aufsicht beim Betrieb umsetzen. Diese Pflichten sind im Hochschulbereich besonders relevant, weil Entscheidungen wie die Nichtzulassung zu einem Studiengang oder das Nichtbestehen einer Prüfungsleistung erhebliche nachteilige Auswirkungen auf die Grundrechte der betroffenen Personen haben können.

Das Europäische Parlament und der Rat haben sich im Rahmen des sogenannten „KI-Omnibus"[30] geeinigt, die Geltung der Pflichten für Hochrisiko-KI-Systeme zeitlich zu verzögern. Danach sollen Pflichten für Hochrisiko-KI-Systeme in den Bereichen Bildung und Personalmanagement ab Dezember 2027 gelten.

---

25 Martini, in: ders./Wendehorst, 2. Aufl. 2026, KI-VO Art. 14 Rn. 124.

26 Buchner, BeckOK KI-Recht, 6. Ed. 1.5.2026, KI-VO Art. 14 Rn. 58.

27 Bomhard/Wietzke, in: Bomhard/Pieper/Wende, 1. Aufl. 2025, KI-VO Art. 14 Rn. 29; Hilgendorf/Härtlein, in: HK-KI-VO, 1. Aufl., KI-VO Art. 14 Rn. 10.

28 Buchner, BeckOK KI-Recht, 6. Ed. 1.5.2026, KI-VO Art. 14 Rn. 61.

29 Schöbel, KI-Folgenabschätzung für Hochschulen?, DFN-Infobrief Recht 7/2026, S. 8 f.

30 Siehe dazu Schöbel, Die KI-VO im Omnibus, DFN-Infobrief Recht 2/2026, S. 2 - 5.

Aller guten Dinge sind drei?

Neuer Gesetzesentwurf enthält Regelungen zur Verarbeitung von Verkehrsdaten und zur Speicherung von IP-Adressen

Von Anna Maria Yang-Jacobi

Zweimal sind Regelungen zur Vorratsdatenspeicherung in Deutschland bereits aufgrund von Urteilen europäischer und nationaler Gerichte gescheitert. Nun wagt die Bundesregierung den dritten Versuch und stellte im April 2026 einen Gesetzesentwurf zur IP-Adressspeicherung und Datenerhebung im Strafverfahren[1] vor. Dafür plant die Bundesregierung, die Strafprozessordnung (StPO) und andere Gesetze wie das Telekommunikationsgesetz (TKG) anzupassen. Klarheit bringt der Gesetzesentwurf jedoch nicht. Vielmehr halten die Diskussionen rund um die Einführung dieser Form von Vorratsdatenspeicherung weiter an.

I. Das ewige Dilemma der Vorratsdatenspeicherung

Die Vorratsdatenspeicherung beschäftigt Gesetzgebung und Gerichte schon seit zwei Jahrzehnten. Bei den bisherigen Versuchen handelt es sich immer wieder um einen Fall von: Gut gemeint, aber schlecht gemacht. So leuchtet es zwar grundsätzlich ein, dass Befugnisse von Strafverfolgungs- und Sicherheitsbehörden in Zeiten von Messenger-Diensten und digitalen Plattformen angepasst werden müssen. Immerhin nutzen auch Täter:innen mobile Endgeräte mit Internetzugang, um Straftaten zu planen, zu verabreden oder Taten direkt online zu begehen. Die Mobilfunk- und Internetverbindungen sowie die daraus folgenden Informationen sind somit wichtige Daten für Behörden. Sie liegen jedoch zunächst nur bei den jeweiligen Anbietern der Dienste. Folglich müssen die staatlichen Behörden Auskunft über die Daten verlangen und sind abhängig davon, welche Daten und für wie lange Anbieter bestimmte Daten speichern. Solche Speicherpflichten und Auskunftsverlangen stellen jedoch erhebliche Eingriffe in Grundrechte dar und bergen die Gefahr einer weitgehenden Massenüberwachung der Bevölkerung. Die konkrete Ausgestaltung der gesetzlichen Voraussetzungen gestaltet sich deswegen als äußerst komplex.

1. Die wichtigsten Gerichtsentscheidungen

Die EU verabschiedete Regelungen zur Vorratsspeicherung von Daten erstmals 2006 in einer europäischen Richtlinie (Vorratsdatenspeicherungs-RL).[2] Danach sollten Daten, die zu einem Kommunikationsvorgang gehören, für mindestens sechs Monate und maximal zwei Jahre gespeichert werden. Außerdem sollte zuständigen nationalen Behörden unter bestimmten Voraussetzungen Zugang zu den Daten gewährt werden. Der deutsche Gesetzgeber setzte die Vorgaben der Richtlinie im TKG um und sah eine sechsmonatige Speicherpflicht vor. Das Bundesverfassungsgericht (BVerfG) erklärte die deutschen Regelungen jedoch für unvereinbar mit dem grundrechtlich geschützten Fernmeldegeheimnis (Art. 10 Abs. 1 GG).[3] In den folgenden Jahren beschäftigte sich auch der Europäische Gerichtshof (EuGH) mit der Vereinbarkeit der Vorratsdatenspeicherungs-RL und der Charta der Grundrechte der Europäischen Union

1 Bundesregierung, Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren (Gesetzesentwurf IP-Adressspeicherung), abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RegE/RegE_IP_Speicherung.pdf?__blob=publicationFile&v=3 (alle Links dieses Beitrags wurden zuletzt am 20.7.2026 abgerufen).

2 Richtlinie 2006/24/EG.

3 BVerfG, Urt. v. 2.3.2010, 1 BvR 256/08.

(GRCh). 2014 entschied der Gerichtshof, dass die Richtlinie einen unverhältnismäßigen Eingriff in das Recht auf Privatleben und das Recht auf Schutz personenbezogener Daten, Art. 7 und 8 GRCh, darstelle.[4] Der EuGH kritisierte in seinem Urteil die genaue Ausgestaltung der Vorratsdatenspeicherung, erklärte sie aber nicht für per se unzulässig.[5]

Der deutsche Gesetzgeber reagierte auf das Urteil des EuGH und verabschiedete 2015 ein Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten.[6] Verkehrsdaten sollten danach für zehn Wochen und Standortdaten für vier Wochen zu speichern sein. Auch die Regelungen dieses Gesetzes wurden jedoch gerichtlich beanstandet. Der EuGH entschied 2022 im sogenannten Spacenet-Urteil,[7] dass auch diese nationalen Regelungen nicht mit dem Unionsrecht vereinbar seien.[8] Das Bundesverwaltungsgericht (BVerwG)[9] urteilte daraufhin 2023, dass die Regelungen des TKG nicht mit Unionsrecht vereinbar seien und nicht mehr angewendet werden dürften.[10]

In der Zwischenzeit traf der EuGH jedoch weitere konkretisierende Entscheidungen zur Vorratsdatenspeicherung. In der Rechtssache La Quadrature du Net II[11] stellte der EuGH wiederholt fest, dass die verschiedenen gespeicherten Daten verknüpft werden könnten und so ein Profil des Nutzers gebildet werden kann. Dies stelle einen schweren Eingriff in die Grundrechte von Betroffenen aus Art. 7 und 8 GRCh dar und habe zudem Folgen für die Ausübung der Meinungsäußerungsfreiheit nach Art. 11 GRCh. Sofern die IP-Adressen jedoch getrennt von anderen Daten gespeichert werden, könnte die Speicherung der IP-Adresse auch bei anderen Straftaten wie Urheberrechtsverstößen erfolgen.[12]

2. Voraussetzungen der Vorratsdatenspeicherung

Mit den Jahren kristallisierte sich durch die Rechtsprechung somit heraus, welche Voraussetzungen für die Vorratsdatenspeicherung und die IP-Adressspeicherung bestehen. Zusammenfassend gilt bislang: Eine anlasslose, unterschiedslose, flächendeckende und zeitlich unbegrenzte Vorratsdatenspeicherung ist weiterhin unvereinbar mit der GRCh.[13] Allerdings differenzierte der EuGH auch dahingehend, dass eine anlasslose, unterschiedslose Vorratsdatenspeicherung zum Schutz der nationalen Sicherheit, beispielsweise vor Terrorismus, möglich sei, diese aber auf das zeitlich absolut Notwendige beschränkt sein und einer wirksamen gerichtlichen Kontrolle unterliegen müsse.[14] Für die Bekämpfung schwerer Kriminalität und die Verhütung ernster Bedrohungen der öffentlichen Sicherheit sei immerhin eine gezielte Vorratsdatenspeicherung zulässig, die sachlich und zeitlich auf das absolut Notwendigste begrenzt sein müsse.[15] Eine anlasslose Vorratsspeicherung von IP-Adressen ist grundsätzlich möglich, sofern materielle und prozedurale Voraussetzungen zur Nutzung der Daten vorgesehen sind und diese strikt eingehalten

4 EuGH, Urt. v. 8.4.2014, C-293/12 und C-594/12.

5 Genauer zur Geschichte der Vorratsdatenspeicherungs-RL und dem ersten EuGH-Urteil, siehe Klein, Knock-Out in (vorerst) letzter Runde, DFN-Infobrief Recht 05/2014.

6 BGBl, 10.10.2015, https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__//*[@attr_id='bgbl115s2218.pdf'].

7 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a.

8 Zum Sachverhalt und den Gründen ausführlich Palenberg, Hamstern verboten, DFN-Infobrief Recht 11/2022; Palenberg, Im Hamsterrad gefangen, DFN-Infobrief Recht 11/2023.

9 BVerwG, Urt. v. 14.8.2023, 6 C 6.22.

10 Dazu bereits Palenberg, Hamstern verboten, DFN-Infobrief Recht 11/2022; Palenberg, Im Hamsterrad gefangen, DFN-Infobrief Recht 11/2023.

11 EuGH, Urt. v. 30.4.2024, C-470/21, La Quadrature du Net II, Rn. 122.

12 Ausführlicher zur Entscheidung und den Leitlinien des EuGH siehe Tech, Die Quadratur des Netzes, DFN-Infobrief Recht 10/2024.

13 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 60 ff.

14 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 72, 93.

15 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 73, 75.

werden.[16] Für die Speicherung von IP-Adressen gilt zudem bei Straftaten im Allgemeinen, dass der behördliche Zugang nur dem Ziel der Identifizierung einer verdächtigen Person dienen darf und rechtliche sowie technische Mittel zur Überprüfung vorliegen müssen.[17]

Außerdem besteht seit der Klarstellung die Möglichkeit des Quick-Freeze-Verfahrens. Beim Quick-Freeze-Verfahren können bereits vorliegende Verkehrs- und Standortdaten, die nach gesetzlichen Vorgaben nach einiger Zeit gelöscht bzw. anonymisiert werden müssen, nachträglich auf behördliche Anordnung für einen längeren Zeitraum gesichert, also „eingefroren", werden. Diese Sicherungsanordnung gilt nur bei einer schweren Bedrohung der öffentlichen Sicherheit oder der Begehung einer schweren Straftat.[18] Sie bedarf einer wirksamen gerichtlichen Kontrolle und kann jedoch auf bestimmte Standorte ausgedehnt werden.[19] Bei diesem Sicherungsvorgang können auch Daten anderer Personen als der konkret verdächtigen Person gespeichert werden, wie beispielsweise Daten des Opfers und seines sozialen oder beruflichen Umfelds.[20] Der Datenabruf durch die Strafverfolgungsbehörden, also das „Auftauen" der Daten, erfolgt dann zu einem späteren Zeitpunkt. 2022 stellte das damals noch von der FDP geführte Bundesjustizministerium einen Referentenentwurf vor, der die Einführung des Quick-Freeze-Verfahrens vorsah.[21] Mit dem Bruch der Ampelkoalition scheiterte jedoch auch dieses Gesetzesvorhaben.

II. Einordnung der Vorratsdatenspeicherung

Die Diskussionen zur Vorratsdatenspeicherung betreffen bestimmte Kategorien von Daten und Konstellationen. Für einige Datenkategorien und Verarbeitungssituationen bestehen bereits gesetzliche Vorgaben im TKG und Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG).

1. Um welche Daten geht es?

Das TKG und das TDDDG enthalten bereits Bestimmungen zu unterschiedlichen Datenkategorien, die bei einem Telekommunikationsvorgang entstehen oder für diesen von Bedeutung sind. Allgemein kann zwischen sogenannten Verkehrs-, Standort-, Nutzungs- und Bestandsdaten differenziert werden. Diese werden teilweise in § 3 TKG legaldefiniert. Die Regelungen zum Umgang mit personenbezogenen Daten bei Telekommunikationsdiensten und bei der Nutzung digitaler Dienste sind seit 2021 im TDDDG zu finden. § 2 TDDDG enthält eine speziell für das TDDDG geltende Definition der Bestandsdaten und eine Definition der Nutzungsdaten.

Die Diskussionen zur Vorratsdatenspeicherung beziehen sich auf die sogenannten Verkehrsdaten. Nach § 3 Nr. 70 TKG sind Verkehrsdaten Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich ist. Dabei handelt es sich um alle Daten, die erkennen lassen, von welchem Anschluss wann mit wem wie lange kommuniziert wurde.[22] Es geht also gerade nicht um den Inhalt der Kommunikation, sondern um die äußeren Umstände der Kommunikation. Zu den Verkehrsdaten gehören Rufnummern, Anschlüsse, IP-Adressen und Nutzerkennungen, aber auch Datenmengen oder zeitliche Daten.

Zu den Verkehrsdaten gehören die sogenannten Nutzungsdaten.[23] Nach § 2 Abs. 2 Nr. 3 TDDDG sind Nutzungsdaten personenbezogene Daten eines Nutzers von digitalen Diensten, deren Verarbeitung erforderlich ist, um die Inanspruchnahme von digitalen Diensten zu ermöglichen und abzurechnen. Dazu gehören Identifikationsmerkmale, der Beginn, das Ende und der Umfang der Nutzung und Angaben über die genutzten Dienste. Im Kontext der Vorratsdatenspeicherung taucht auch der Begriff der Standortdaten auf. In § 3 Nr. 56 TKG sind Standortdaten definiert als Daten, die in einem Telekommunikationsnetz oder

16 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 101.

17 EuGH, Urt. v. 30.4.2024, C-470/21, La Quadrature du Net II, Rn. 164.

18 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 118.

19 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 114-120.

20 EuGH, Urt. v. 20.9.2022, C-793/19 und C-794/19, Spacenet u. a., Rn. 117 ff.

21 https://cdn.netzpolitik.org/wp-upload/2022/10/2022-10-25_BMJ_RefE_Sicherungsanordnung-StPO.pdf

22 Braun, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, TKG § 3 Rn. 170.

23 Ettig, in: Taeger/Gabel, DSGVO/BDSG/TDDDG, 5. Aufl. 2026, TDDDG § 2 Rn. 28.

von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben. Entsprechend können mithilfe dieser Daten Rückschlüsse auf den Standort der Nutzenden gezogen werden.

Eine weitere Datenkategorie sind die sogenannten Bestandsdaten. Gemäß § 3 Nr. 6 TKG sind Bestandsdaten die Daten eines Endnutzers, die erforderlich sind für die Begründung, die inhaltliche Ausgestaltung, die Änderung oder die Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste. Zu den Bestandsdaten gehören nur personenbezogene Daten wie beispielsweise der Name, die Anschrift, das Geburtsdatum der Nutzenden, die E-Mail- und IP-Adresse sowie der Username und die Zahlungsdaten.[24]

2. Welche Regelungen gelten momentan?

Das TKG und das TDDDG enthalten bereits Vorschriften, die konkrete Datenkategorien betreffen. So sind Anbieter von Telekommunikationsdiensten nach §§ 172-174 TKG verpflichtet, Bestandsdaten zu erheben, zu speichern und Sicherheitsbehörden unter bestimmten Voraussetzungen Auskunft darüber zu erteilen. Auch die Bestandsdatenauskunft war bereits Gegenstand von Gerichtsentscheidungen. Dabei bestätigte das Bundesverfassungsgericht (BVerfG) 2020 in einer Entscheidung zur Vorgängerregelung des § 174 TKG das sogenannte Doppeltürmodell.[25] Das BVerfG entwickelte dieses im Rahmen des Umgangs staatlicher Behörden mit personenbezogenen Daten.[26] Bei einem Datenaustausch muss nach dem Doppeltürmodell zwischen zwei „Türen" unterschieden werden, die jeweils unabhängig voneinander „geöffnet" werden müssen. Sowohl die auskunftserteilende Stelle, die die Daten übermittelt, als auch die auskunftsersuchende Stelle, die die Daten empfängt, greifen in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung ein. Beide Stellen brauchen somit eine Rechtsgrundlage und der Verwendungszweck der Daten muss in beiden Rechtsgrundlagen hinreichend normenklar begrenzt sein. Erst dann können sich beide „Türen öffnen" und die Daten übertragen und empfangen werden. Im Rahmen der Neufassung des TKG wurde die Regelung angepasst, sodass § 174 TKG nun den Voraussetzungen für die auskunftserteilende Stelle entspricht.

Für die Verkehrsdaten enthält das TKG mit §§ 175-181 TKG Vorschriften zur Speicherung von Verkehrsdaten, die jedoch nach den Urteilen des EuGH und des BVerwG unvereinbar mit dem Unionsrecht und somit nicht anwendbar sind. So fehlte es bislang an einer Übermittlungsnorm für Telekommunikationsdienste-Anbieter zur Übermittlung von Verkehrsdaten an Strafverfolgungsbehörden.[27]

Das TDDDG enthält mit §§ 9-12 TDDDG Regelungen zur Verarbeitung von Verkehrsdaten. Die Anbieter können Verkehrsdaten jedoch nur verarbeiten, wenn dies der Aufrechterhaltung der Telekommunikation, der Entgeltabrechnung, dem Aufbau weiterer Verbindungen oder der Beseitigung von Störungen oder Fehlern an Telekommunikationsanlagen dient. Andere Zwecke sind nicht umfasst. Die §§ 21-23 TDDDG regeln die Auskunft über Bestandsdaten speziell bei Anbietern digitaler Dienste. Spezielle Auskunftsbefugnisse gelten auch bei Nutzungsdaten im Rahmen des § 24 TDDDG, der jedoch deutlich weniger Möglichkeiten vorsieht als die Bestandsdatenauskunft nach § 22 TDDDG. Regelungen zum Umgang mit Verkehrs-, Nutzungs- und Bestandsdaten existieren somit bereits in ausgewählten Konstellationen.

III. Die Zukunft von Datenerhebung, Quick-Freeze und IP-Adressspeicherung?

Durch den neuen Gesetzesentwurf plant die Bundesregierung, zahlreiche Gesetze zu ändern. Gerade in der StPO[28] sollen Anpassungen erfolgen, um den Strafverfolgungsbehörden selbst

24 Bortnikov, in: Geppert/Schütz, Beck'scher TKG-Kommentar, 5. Aufl. 2023, TKG § 3 Rn. 18; vgl. Ettig, in: Taeger/Gabel, DSGVO/BDSG/TDDDG, 5. Aufl. 2026, TDDDG § 2 Rn. 26.

25 BVerfG, NJW 2020, 2699.

26 BVerfG, NJW 2012, 1419 Rn. 123.

27 Eine Herleitung aus anderen Normen des TDDDG, der Telekommunikations-Überwachungsverordnung (TKÜV), der Datenschutz-Grundverordnung (DSGVO) oder der StPO ist nicht möglich, siehe Bäcker, GSZ 2023, 257, 259 ff. sowie Wäger, MMR 2026, 15, 18 f.

28 Aufseiten der Ermittlungsbehörden sind Rechtsgrundlagen zur Erhebung von Verkehrsdaten (§ 100g StPO-E), Bestandsdaten (§ 100j StPO-E) und Nutzungsdaten (§ 100k StPO-E) sowie dazugehörige Verfahrensregelungen (§ 101a StPO-E) vorgesehen.

entsprechende Befugnisse zur Erhebung von Bestands- und Verkehrsdaten zuzuweisen. Aufseiten der Telekommunikationsdienste sind drei Neuerungen von grundlegender Bedeutung. Die bisherigen Regelungen zur Vorratsdatenspeicherung nach §§ 175-181 TKG sollen hierzu aufgehoben und durch die neuen §§ 175-177 TKG-E ersetzt werden.

1. Vorgesehene Änderungen im TKG

§§ 175-177 TKG-E setzen die Datenverarbeitung bei Auskunftserteilung, das Quick-Freeze-Verfahren bzw. die Sicherungsanordnung und die IP-Adressspeicherung um. Zunächst will die Bundesregierung über § 175 TKG-E das Doppeltür-Erfordernis erfüllen und eine Übermittlungsnorm aufseiten der Telekommunikationsdienste schaffen. So sollen Erbringer von oder Mitwirkende an öffentlich zugänglichen Telekommunikationsdiensten nach § 175 Abs. 1 TKG-E Verkehrsdaten zur Auskunftserteilung gegenüber den in § 175 Abs. 3 TKG-E aufgeführten Strafverfolgungs- und Sicherheitsbehörden verarbeiten dürfen. § 175 Abs. 2 TKG-E konkretisiert die Übermittlungsnorm der auskunftserteilenden Stellen. § 175 Abs. 3 TKG-E zählt sodann die staatlichen Stellen auf, denen Auskunft erteilt werden darf, und normiert die Befugnis zur zweckändernden Verwendung der Daten. § 175 Abs. 4 TKG-E verweist auf § 174 Abs. 6 S. 2 und Abs. 7 TKG und gibt Instruktionen zur Übermittlung vor.

§ 176 TKG-E ermöglicht das Quick-Freeze-Verfahren im Rahmen der Telekommunikationsdienste. So sind Erbringer von oder Mitwirkende an öffentlich zugänglichen Telekommunikationsdiensten künftig zur Verarbeitung von Verkehrsdaten zur Erfüllung von Sicherungsanordnungen befugt, wenn dies zur Erfüllung einer Sicherungsanordnung durch zuständige Stellen erforderlich ist, § 176 Abs. 1 TKG-E. Die Bundesnetzagentur (BNetzA) geht von etwa 3.000 Verpflichteten aus.[29] § 176 Abs. 2 TKG-E zählt technische Sicherungspflichten auf. Nach § 176 Abs. 3 TKG-E ist Stillschweigen über die Umstände gegenüber den Betroffenen und Dritten zu wahren, und § 176 Abs. 4 TKG-E sieht weitere Möglichkeiten zur technischen Ausgestaltung der Pflichten über eine Rechtsverordnung vor. Die Veränderungen der StPO hinsichtlich der Sicherungsanordnung zeigen jedoch, dass es sich nur um eine abgeschwächte Form des Quick-Freeze-Verfahrens handelt, da die Staatsanwaltschaft die erste Anordnung ohne Einbeziehung eines Gerichts veranlassen kann (§ 101a Abs. 1 Nr. 3 StPO-E).

Die IP-Adressspeicherung ist in § 177 TKG-E zu finden, als Pflicht zur Speicherung und Befugnis zur Verwendung von Verkehrsdaten zur Identifizierung von Anschlussinhabern. § 177 Abs. 1 TKG-E adressiert in Kontrast zu §§ 175, 176 TKG-E nur Erbringer von Internetzugangsdiensten. Von der Pflicht ausgenommen sind beispielsweise Messenger- und E-Mail-Dienste, Bereitsteller lokaler drahtloser Netzwerke, die den Zugang zum Internet lediglich vermitteln und keine öffentlichen IP-Adressen vergeben.[30] Der dahinterliegende Anbieter von Internetzugangsdiensten ist stattdessen nach § 177 Abs. 1 TKG-E verpflichtet.[31] Die Bundesregierung geht von etwa 700 verpflichteten Unternehmen aus.[32] Diese sollen bestimmte, in der Vorschrift aufgezählte Daten speichern, wie beispielsweise die öffentliche IP-Adresse, Portnummern, Anschlüsse sowie Benutzerkennungen und zeitliche Daten. Die Speicherdauer beträgt drei Monate, was die Bundesregierung als „notwendige Dauer“ betrachtet.[33] Die Kommunikationsinhalte oder Daten anderer Dienste sollen explizit nicht gespeichert werden. § 177 Abs. 2, Abs. 3 TKG-E enthalten daran anschließende Pflichten, wie in § 177 Abs. 3 Nr. 2 TKG-E z. B. die technisch wirksame Trennung der IP-Adressen von anderen vorhandenen Endnutzerdaten. Die Daten dürfen sodann nach § 177 Abs. 4 TKG-E für eine Auskunft i. S. d. § 174 Abs. 1 S. 3 TKG oder auch nach der E-Evidence-Verordnung[34] verwendet werden. Zuletzt ist auch in § 177 Abs. 5 TKG-E die Möglichkeit weiterer Ausgestaltungen der Pflichten in einer Rechtsverordnung festgelegt, sowie die Kontrolle der Vorgaben durch die BNetzA.

Die Bundesregierung betont im Gesetzesentwurf, dass die Speicherung der IP-Adressen und weiterer aufgezählter Verkehrsdaten zwar alle Nutzer:innen von Internetzugangsdiensten

29 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 34.

30 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 66.

31 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 66.

32 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 34 f.

33 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 67 ff.

34 Zur E-Evidence-Verordnung siehe auch Bielzer, Elektronische Beweismittel ohne Grenzen, DFN-Infobrief Recht 8/2026.

in Deutschland betreffen, aber die Daten nur zur Identifizierung des Anschlussinhabers anhand einer IP-Adresse führen können.[35] Es handele sich um keine Vorratsdatenspeicherung aller Verkehrs- und Standortdaten. Profile der Nutzer:innen ließen sich gerade nicht erstellen.[36]

2. Bisherige Reaktionen und Kritik

Der Gesetzesentwurf hat zahlreiche Reaktionen hervorgerufen.[37] Verbände und Organisationen der Zivilgesellschaft übten vor allem Kritik. So reiche eine freiwillige Datenspeicherung der Anbieter von Telekommunikationsdiensten in gut drei von vier Verfahren.[38] Als Alternativen werden etwa Login-Fallen vorgeschlagen.[39] Außerdem wird betont, dass das Quick-Freeze-Verfahren bereits ausreichen würde und die Sicherungsanordnung doch gerade aufzeige, dass es Alternativen gibt und Daten bei Bedarf erhoben und später gezielt abgefragt werden können.[40] Weitere Kritik wird an den zusätzlichen Kosten geübt, die durch eine Speicherpflicht entstünden.[41] Der Kosten-Nutzen ist fraglich, da die Identifikation durch Virtual Private Networks (VPN) oder Tor-Netzwerke, die die ursprüngliche IP-Adresse maskieren, leicht umgangen werden könne.[42] Aus rechtlicher Sicht wird bezweifelt, dass der Gesetzesentwurf den Vorgaben des EuGH gerecht wird. Die Trennung der IP-Adressen und weiterer Datenkategorien wird infrage gestellt, da es an technischen Kriterien fehle und gerade im Zusammenspiel mit Bestandsdaten und weiteren Daten „genaue Schlüsse auf das Privatleben“ gezogen werden könnten.[43] Zuletzt kritisierten mehrere Stellen, wie etwa die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), das Vorliegen von „absoluter Notwendigkeit“ bei einer Speicherdauer von drei Monaten.[44]

IV. Ausblick und Fazit

Der Bundesrat hat den Gesetzesentwurf grundsätzlich begrüßt und kleinere Anpassungen gefordert, wie die Benennung der Rechtsgüter im Rahmen der §§ 175, 176 TKG-E, um dem Doppeltür-Erfordernis hinreichend gerecht zu werden.[45] Zusätzlich schlug der Bundesrat jedoch auch weitreichendere Änderungen des Gesetzesentwurfs vor. So soll der Kreis der berechtigten Stellen auch auf Landesbehörden erweitert werden.[46] Der Bundesrat bat zudem um Prüfung, ob die Speicherfrist nach § 177 Abs. 1 S. 1 TKG-E auch auf bis zu sechs Monate ausgeweitet werden könnte.[47]

Eine erste Lesung im Bundestag erfolgte Ende Juni 2026 und endete mit der Überweisung in den zuständigen Ausschuss zur weiteren Beratung.[48] Es bleibt nun abzuwarten, wie das weitere

35 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 24.

36 Bundesregierung, Gesetzesentwurf IP-Adressspeicherung, S. 24.

37 Eine Aufzählung von Kritikpunkten einzelner Verbände und Parteien ist bei Netzpolitik.org zu finden, https://netzpolitik.org/2026/dritter-versuch-bundesregierung-beschliesst-anlasslose-vorratsdatenspeicherung/.

38 D 64, S. 1 f., https://d-64.org/wp-content/uploads/2026/01/2026-01-30-D64_VDS-Stellungnahme.pdf.

39 D 64, S. 2, https://d-64.org/wp-content/uploads/2026/01/2026-01-30-D64_VDS-Stellungnahme.pdf.

40 D 64, S. 3, https://d-64.org/wp-content/uploads/2026/01/2026-01-30-D64_VDS-Stellungnahme.pdf.

41 Bereits zum Referentenentwurf: Bundesrechtsanwaltskammer (BRAK), Januar 2026, S. 5, https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2026/stellungnahme-der-brak-2026-07.pdf.

42 Krempl, 26.4.2026, https://www.heise.de/news/Teure-digitale-Spurensuche-Milliardeninvestitionen-fuer-die-neue-IP-Speicherung-11272367.html.

43 Bereits zum Referentenentwurf: BRAK Januar 2026, S. 6 f., https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2026/stellungnahme-der-brak-2026-07.pdf.

44 Steiner, 6.5.2026, https://www.heise.de/news/BfDI-Neue-Sicherheitsbefugnisse-nicht-zulaessig-11284895.html.

45 Bundesrat, Drs. 263/1/26, 1.6.2026, S. 1, 3-4, 12, https://dserver.bundestag.de/brd/2026/0263-1-26.pdf.

46 Bundesrat, Drs. 263/1/26, 1.6.2026, S. 1, 3 f., https://dserver.bundestag.de/brd/2026/0263-1-26.pdf.

47 Bundesrat, Drs. 263/1/26, 1.6.2026, S. 13, https://dserver.bundestag.de/brd/2026/0263-1-26.pdf.

48 Bundestag, Plenarprotokoll, S. 10360-10367, https://dserver.bundestag.de/btp/21/21085.pdf#P.10361.

Gesetzgebungsverfahren verläuft. Erst nach erfolgreicher Verabschiedung und Inkrafttreten des Gesetzes stellen sich weitere Folgefragen zur genauen Anwendung und eventuellen Auswirkungen auf Hochschulen und Forschungseinrichtungen. Die Kritik und Debatten zeigen jedoch: Das Thema bleibt kontrovers. So stellt sich auch am Ende die Frage, ob denn nun tatsächlich aller guten Dinge drei sind.

Was bedeutet digitale Souveränität für Universitäten und Hochschulen?

Digitale Abhängigkeiten können die akademische Selbstbestimmung gefährden. Wie können Hochschulen ihre digitale Souveränität stärken?

Von Dr. Paul Friedl

Digitale Souveränität ist längst mehr als ein hohles Buzzword. Ob Rechenkapazitäten, Cloud-Infrastruktur, oder Lehrsoftware: Universitäten und Hochschulen müssen heute souveräne Lösungen finden, um auch in Zukunft qualitatives, selbstbestimmtes Forschen und Unterrichten garantieren zu können. Dabei sind viele schwierige Entscheidungen zu treffen. Welche Strategien können dem Hochschulsektor im Aufbau digitaler Souveränität helfen?

I. Der Fall Khan: wenn Software zum Machtfaktor wird

OpenDesk, ein Open-Source-Programmpaket, das vergleichbar mit Microsoft Office alle zentralen Bereiche digitaler Büroarbeit abdecken soll und von der Bund-Tochter „Zentrum für Digitale Souveränität der Öffentlichen Verwaltung" entwickelt wird, ist wahrscheinlich wenigen ein Begriff. Ein prominenter Kunde existiert allerdings bereits: der Internationale Strafgerichtshof (IStGH) in Den Haag, der mit OpenDesk bisher bezogene Microsoft-Dienstleistungen ersetzen will.[1] Aus freien Stücken geschah dieser Umzug allerdings nicht. Grund des Umzugs war vielmehr, dass Microsoft im Februar 2025 den E-Mail-Account des IStGh-Chefanklägers Karim Khan deaktiviert hatte und ihn dadurch von der Ausführung seiner Arbeit abhielt.[2] Dem waren Sanktionen durch die Executive Order 14203 vorausgegangen,[3] mit denen US-Präsident Donald Trump den IStGH und Karim Khan belegt hatte, um den Erlass von Haftbefehlen gegen den israelischen Ministerpräsidenten Benjamin Netanjahu und dessen ehemaligen Verteidigungsminister Joaw Galant zu vergelten. Microsoft kam zum Schluss, dass diese Sanktionen der Bereitstellung von Diensten an Khan entgegenstünden und setzte diese Sanktionen technisch um. Gleichzeitig machte dies sichtbar, wie verwundbar Institutionen durch ihre Abhängigkeit von einzelnen Technik-Anbietern sind.

II. Digitale Souveränität: Kern einer Idee

Digitale Souveränität. So heißt die vermeintliche Lösung gegen derartige Verwundbarkeiten, die seit einigen Jahren hitzig diskutiert wird. Doch so eindrücklich der Fall des IStGH ist, so komplex und vielschichtig ist die Frage, was mit digitaler Souveränität eigentlich gemeint ist. Im Kern meint digitale Souveränität die Fähigkeit von Staaten, Gesellschaften, Individuen etc. digitale Technologien, Daten und Infrastrukturen unabhängig, frei und

1 Christoph Kerkmann, Strafgerichtshof ersetzt Microsoft durch deutsche Lösung (Handelsblatt, 30.10.2025), abrufbar unter: https://www.handelsblatt.com/technik/it-internet/software-strafgerichtshof-ersetzt-microsoft-durch-deutsche-loesung/100166382.html (alle Webinhalte zuletzt abgerufen am: 08.07.2026).

2 Stefan Krempl, Criminal Court: Microsoft's email block a wake-up call for digital sovereignty (Heise, 12.05.2025), abrufbar unter: https://www.heise.de/en/news/Criminal-Court-Microsoft-s-email-block-a-wake-up-call-for-digital-sovereignty-10387383.html.

3 Donald Trump, Executive Order 14203 „Imposing Sanctions on the International Criminal Court" (06.02.2025).

selbstbestimmt nutzen zu können.[4] Anders ausgedrückt: Abhängigkeiten, die auf allen Ebenen des sogenannten Tech-Stacks, d. h. der Gesamtheit der Ressourcen, Technologien etc., die für die Entwicklung und den Betrieb digitaler Werkzeuge notwendig sind, bestehen können, sollen abgebaut oder überwunden werden. Digitale Souveränität kann sich also auf Hardware – etwa Chips, Netzwerk- oder Cloud-Infrastruktur-, Software- (beispielsweise KI-Modelle) oder KI-basierte Programme – und auch auf Daten beziehen. Darüber hinaus kann sie die für Entwicklung, Betrieb und Nutzung solcher Infrastruktur notwendigen Ressourcen und Rohstoffe (z. B. Energie oder seltene Erden) und das dafür erforderliche Know-how einbeziehen. Wenn auf politischer Ebene derzeit über digitale Souveränität geredet wird, geht es dementsprechend etwa um Projekte wie EuroStack – einen Vorschlag für den Aufbau unabhängiger europäischer digitaler Infrastruktur, vom Halbleiter bis zur digitalen Plattform –[5] oder um den Bau von AI-Gigafactories,[6] mit denen die EU Rechenkapazitäten für das Training und den Betrieb großer KI-Modelle aufbauen und so die Abhängigkeit von amerikanischen oder chinesischen Hyperscalern[7] verringern will.

III. Digitale Souveränität: Fluchtpunkte einer Debatte

Diese relative Klarheit des Begriffskerns darf nicht darüber hinwegtäuschen, dass die Beweggründe hinter Forderungen nach digitaler Souveränität durchaus unterschiedlich sein können.

Der Fall des IStGH zeigt, dass es bei digitaler Souveränität einerseits darum gehen kann, die Erbringung eigener (kritischer) Leistungen und Dienste sicherzustellen. Unabhängigkeit soll also gegenüber anderen Akteuren bestehen, die über einen metaphorischen „Kill Switch" verfügen könnten, einen „Ausschalter", über den der Betrieb des abhängigen Akteurs jederzeit zum Erliegen gebracht werden kann. Ähnliche Effekte können freilich auch über prohibitiv hohe Preise oder andere unerfüllbare Vertragsbedingungen erreicht werden.

Ähnlich verhält es sich mit Abhängigkeiten, die die eigene Handlungsmacht beschränken, etwa bezogen auf Möglichkeiten der Datenanalyse. Cloud-Infrastrukturbetreiber verlangen für das Abziehen von Daten beispielsweise regelmäßig hohe Egress-Gebühren, sodass ein Wechsel oder eine externe Auswertung bei großen Datenmengen schnell kostspielig wird. Gleichzeitig können proprietäre Dateiformate dazu führen, dass sich Daten nur auf der bisher verwendeten Plattform (sinnvoll) verarbeiten lassen. Beides erzeugt Lock-in-Effekte und kann Nutzer in der Verwendungsfreiheit ihrer Daten beschränken.

Eine weitere Dimension digitaler Souveränität liegt im wirtschaftlichen Bereich: Wer für digitale Infrastruktur und Dienste nicht auf „externe", sondern auf „interne" Akteure zurückgreift, kurbelt dadurch die eigene Wirtschaft an und schafft Bedingungen, unter denen eigene Innovation und technologische Entwicklung wahrscheinlicher werden. Das umfasst zum einen das Halten oder die Verlagerung der Wertschöpfung in den eigenen Bereich, aber auch den Aufbau eigener Expertise.

Schließlich kann digitale Souveränität dazu dienen, eigene Daten und eigenes Wissen zu schützen. Dabei kann es sich um „klassischen" Datenschutz handeln, also den Schutz personenbezogener Daten, aber auch um jegliches anderes wertvolles Wissen, beispielsweise sicherheitsrelevantes Wissen, Geschäftsgeheimnisse oder Forschungsdaten.

IV. Digitale Souveränität: universitäre Herausforderungen im KI-Bereich

Auch für Universitäten und Hochschulen wirft der Komplex „Digitale Souveränität" also ein breites Spektrum unterschiedlicher

4 Zum Begriff auch Julie Pohle und Thorsten Thiel, „Digitale Souveränität - Von der Karriere eines einenden und doch problematischen Konzepts", in: Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt (2021).

5 Eurostack, Building Europe's Digital Future, abrufbar unter: https://eurostack.eu/.

6 European Commission, AI Gigafactories, abrufbar unter: https://commission.europa.eu/topics/competitiveness/competitiveness-coordination-tool-projects/ai-gigafactories_en.

7 Als Hyperscaler bezeichnet man die weltweit größten Anbieter von Cloud-Diensten (oftmals nur: Amazon Web Services, Microsoft Azure und Google Cloud). Die Bezeichnung stammt von der Fähigkeit dieser Dienste, Speicher- und Rechen-Ressourcen nahezu beliebig und in kürzester Zeit an den jeweiligen Kundenbedarf anpassen zu können, also eine sehr hohe Skalierbarkeit dieser Ressourcen sicherstellen zu können.

Fragen auf und verlangt, ganz verschiedene Herausforderungen zu bewältigen.[8] Im Kern geht es dabei immer darum, möglichst große Gestaltungsautonomie über die eng verzahnten Felder der Wissensproduktion und -vermittlung zu gewinnen. Ein Blick auf einzelne Herausforderungen im Feld der Künstlichen Intelligenz macht dies anschaulich:[9]

Um eigene große KI-Sprachmodelle trainieren zu können, die etwa auch die eigenen Anforderungen an sprachliche Repräsentanz, Transparenz oder Nachvollziehbarkeit besser bedienen, oder global kompetitive Forschung in diesem Bereich betreiben zu können, bedarf es hinreichender Rechenkapazitäten, die in Europa derzeit nur sehr begrenzt verfügbar sind. Sind keine hinreichenden Rechenkapazitäten verfügbar, um leistungsstärkste Frontier-Modelle selbst zu entwickeln und zu betreiben, muss in diesem Bereich auf kommerzielle Angebote zurückgegriffen werden. Dies kreiert nicht nur schwer beherrschbare Kostenrisiken, sondern macht regelmäßig auch eine Datenübermittlung an die Anbieter notwendig, die auch sensible Daten, etwa personenbezogene Informationen oder Forschungsdaten und -ergebnisse, erfassen kann. Ähnliche Probleme stellen sich auch in anderen Forschungsbereichen, die auf Hochleistungs-Compute-Infrastrukturen angewiesen sind, wobei natürlich immer auch die Frage besteht, ob externe Cloud-Infrastrukturen die Rechen- und Analysekapazitäten bereitstellen, die für die eigene Forschung notwendig sind und eine angemessene Datenportabilität gewährleisten. Gleichzeitig riskiert die fehlende Verfügbarkeit digitaler Forschungsinfrastruktur die Abwanderung wissenschaftlichen Talents und damit auch eine Vertiefung bestehender Expertise-Defizite.

Auch in der Lehre kann ein Mangel an eigenen KI-Kapazitäten aber die eigene Handlungsfähigkeit beschränken. Beispielsweise kann die Abhängigkeit von amerikanischen Anbietern dazu führen, dass Lernanwendungen für Studierende nicht datenschutzkonform (und damit überhaupt nicht) betrieben werden können oder Lösungen zum Einsatz kommen, die nicht die eigenen sprachlichen oder (wissenschafts-)kulturellen Präferenzen bedienen. Sollen KI-Tools in der Prüfungsbewertung eingesetzt werden, steht zu befürchten, dass kommerzielle Tools nicht die hinreichenden Standards an Transparenz und „Explainability" erreichen. Bei diesen Beispielen handelt es sich aber natürlich nur um eine sehr begrenzte Auswahl der vielen Herausforderungen, denen sich Universitäten jetzt ausgesetzt sehen. Diese Einschätzung wird durch die begründete Annahme untermauert, dass es sich bei Künstlicher Intelligenz um technologische Infrastruktur handelt, die künftig „in allen wissenschaftlichen Arbeitsprozessen präsent" sein wird.

V. Souveräne Kooperation statt Autarkie

Deutsche und europäische Hochschulen haben diese Herausforderungen längst erkannt und arbeiten aktiv an Strategien, die eigene digitale Souveränität zu stärken. Das vielleicht zentralste Gebot der Stunde lautet dabei: Kooperation. Nur wo es Universitäten und Hochschulen gelingt, sich miteinander und mit Partnern aus Wirtschaft und Verwaltung regional, national und im besten Falle europäisch zu vernetzen, können Ressourcen so aufgebaut und gebündelt werden, dass kommerziellen Angeboten effektive Alternativen entgegengesetzt werden können. Das reicht von der Entwicklung abgestimmter Souveränitätsstrategien über die Bündelung finanzieller Ressourcen für den Kauf und Betrieb von Rechenkapazitäten bis zur gemeinsamen Entwicklung hochschuladäquater KI-Tools und dem Expertise-Pooling durch kontinuierlichen Austausch.

Gleichzeitig muss im Blick behalten werden, dass es sich bei digitaler Souveränität in erster Linie um ein strategisches Problem handelt. Der Aufbau von Infrastrukturen bedarf Zeit und Ressourcen; Entscheidungen können selten schnell, leicht oder ohne Kosten rückabgewickelt werden. Und so wie es bei der Nutzung externer Dienste zu Lock-in-Effekten kommen kann, kann auch die Entwicklung und Nutzung eigener Lösungen Lock-in-Effekte auslösen. Entscheidungen über digitale Souveränität müssen daher wohlüberlegt und mit Blick auf ihre langfristigen Folgen getroffen werden. Auch bewusst gewählte Abhängigkeiten können die richtige und oftmals einzig realistische Lösung sein. Außerdem setzt Souveränität nicht zwingend vollständige Autarkie voraus, und auch kommerzielle Angebote können Autonomie

8 Für einen Überblick zu digitaler Souveränität an Hochschulen, siehe auch Hochschulforum Digitalisierung, „Hochschulen zwischen digitaler Souveränität und digitaler Abhängigkeit: Verunsicherung vs. Selbstbestimmung" (Juni 2024); Arbeitsgruppe der CIOs der Universitäten in Baden-Württemberg und der Universitäten und Hochschulen für angewandte Wissenschaft (HAWs) in Bayern, „CIO-Positionspapier Digitale Souveränität an Universitäten und Hochschulen" (28.03.2025).

9 Für einen Überblick zur KI-Souveränität an Hochschulen, siehe auch Hochschulforum Digitalisierung, „Souveräne KI-Infrastrukturen an Hochschulen - Reflexionen und Handlungsperspektiven" (Dezember 2025).

vermitteln. Ein funktionierender, kompetitiver Markt mit verschiedenen – im besten Falle auch europäischen – Anbietern verschafft Hochschulen selbst dort Verhandlungsmacht, wo sie entsprechende Produkte nicht in Eigenregie betreiben. Wo echte Auswahl besteht (oder hinreichende Kaufkraft), lassen sich eigene Wünsche und Bedingungen auch gegenüber externen Anbietern durchsetzen. Gestaltungsautonomie erwächst dann nicht allein aus Besitz, sondern aus der Fähigkeit, wählen und wechseln (oder bezahlen) zu können.[10]

VI. Recht als Hebel digitaler Souveränität

Nicht zuletzt hat auch das Recht erheblichen Einfluss auf die digitale Souveränität, etwa indem es einzuhaltende Standards vorschreibt, die für digitale Souveränität notwendigen Kooperationen ermöglicht, erleichtert oder Rechte an Daten und deren Weiternutzung regelt. Der europäische Gesetzgeber ist dabei zunehmend darauf aus, das europäische Recht gezielt zur Stärkung digitaler Souveränität nutzbar zu machen. Ein Instrument, das der europäische Gesetzgeber nun vorgeschlagen hat, ist der kürzlich vorgestellte „Cloud and AI Development Act" (CADA), mit dem das Cloud- und KI-Ökosystem in der EU gestärkt werden soll.[11] Der nächste Beitrag in dieser zweiteiligen Reihe wird sich deshalb diesem neuen CADA widmen und dessen Bedeutung für Universitäten und Hochschulen eruieren.

10 Ein Beispiel eines solchen Wechsels bietet der Umzug der obersten deutschen Gerichte von der Plattform X (damals noch Twitter) auf das quelloffene, dezentrale Netzwerk Mastodon, siehe auch Rennert, Musk? Oh no! Mastodon!, DFN-Infobrief Recht 2/2023.

11 Europäische Kommission, Vorschlag für das Cloud and AI Development Act (03.06.2026), abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/proposal-cloud-and-ai-development-act-cada.

DFN Infobrief-Recht-Aktuell

- ## Datenschutzrecht/Arbeitsrecht: Urteil des EuGH vom 18. Juni 2026 (C-484/24) zu Beweisverwertungsverboten bei rechtswidrig erlangten personenbezogenen Daten

  Das Landesarbeitsgericht (LAG) Niedersachsen legte dem EuGH eine Frage zur Auslegung des Unionsrechts vor. Eine Arbeitgeberin vermutete, dass eine Mitarbeiterin Unternehmensgegenstände bei ebay verkaufte. Zur Überprüfung dieses Verdachts loggte sie sich ohne Zustimmung in deren geschützten ebay-Account ein. Nachdem sich der Verdacht bestätigte, erhob sie Schadensersatzklage. Für das LAG Niedersachsen stellte sich daher die Frage, ob eine rechtswidrige Datenerhebung vorlag. Im Vorabentscheidungsverfahren entschied der EuGH, dass rechtswidrig erlangte personenbezogene Daten nicht allein deshalb einem prozessualen Beweisverwertungsverbot unterliegen. Vielmehr ist im Einzelfall zu prüfen, ob ihre Verarbeitung oder Verwendung unter Beachtung der datenschutzrechtlichen Grundsätze zulässig ist. Maßgeblich ist insbesondere der Grundsatz der Datenminimierung. Soweit erforderlich, ist der Umfang der Datenanwendung auf das notwendige Maß zu beschränken, etwa durch Schwärzung, Anonymisierung oder andere geeignete Maßnahmen zur Datenminimierung.

  Hier erhalten Sie den Link zum Urteil (alle Links dieser Seite wurden zuletzt am 24.08.2026 abgerufen):
  https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62024CJ0484

- ## Urheberrecht: Urteil des Landgerichts München I vom 31. Juli 2026 (42 O 763/25) zum Auskunfts-, Unterlassungs- und Schadensersatzanspruch der GEMA gegen SUNO

  Die GEMA klagte als Verwertungsgesellschaft bekannter Musikstücke gegen Rechtsverletzungen, die möglicherweise durch die Memorisierung und die Ausgabe des Outputs im Rahmen des Trainings des KI-Modells der Beklagten begangen worden sein könnten. SUNO ist eine US-amerikanische Anbieterin eines auf künstlicher Intelligenz beruhenden Musikgenerators. Es wurden Rechtsverletzungen in den U.S.A. und Deutschland geltend gemacht. Nach der Entscheidung des Gerichts ist durch die Memorisierung eine Verletzung des Vervielfältigungsrechts nach § 16 Urheberrechtsgesetz (UrhG) gegeben. Zudem sei im Angebot des Modells selbst und der Anwendung zur Generierung von Musik ein Verstoß gegen das unbenannte Recht der öffentlichen Wiedergabe nach § 15 Abs. 2 UrhG zu sehen.

  Hier erhalten Sie den Link zur Pressemitteilung:
  https://www.justiz.bayern.de/gerichte-und-behoerden/landgericht/muenchen-1/presse/2026/16.php

- ## Informationsfreiheitsrecht: Entschließung der Informationsfreiheitsbeauftragten zum Einsatz von KI zur Anonymisierung von Gerichtsentscheidungen

  Die Konferenz der Informationsfreiheitsbeauftragten hat am 24. Juli 2026 eine Entschließung veröffentlicht. Darin begrüßt sie den Einsatz von KI zur Anonymisierung von Gerichtsentscheidungen und begründet dies damit, dass dadurch der Öffentlichkeit ein breiter Zugang zu gerichtlichen Entscheidungen ermöglicht werden kann. Der dafür erforderliche Aufwand für die Gerichte und die Justizverwaltung könne dadurch verringert werden.

  Hier erhalten Sie den Link zur Pressemitteilung der IFK:
  https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/IFK/2026/20260727-IFK-PM-Anonymisierung-Gerichtsentscheidungen.pdf

Kurzbeitrag: Aufsichtspflicht für KI-Content

Für KI-generierte Inhalte haftet, wem diese als eigene Äußerung zugerechnet werden können

Von Sofie Leonhard

Die Flut von KI-generierten Inhalten wirft auch äußerungsrechtliche Fragen auf: Wer haftet, wenn „KI-Content" Persönlichkeitsrechte verletzt? Drei Entscheidungen der Landgerichte aus den letzten Jahren machen deutlich: Auch für solche Inhalte gelten die allgemeinen äußerungsrechtlichen Regeln. Haftbar für KI-Output ist also, wem dieser als eigene Äußerung zugerechnet werden kann.

I. Hintergrund

1. Was darf man eigentlich alles (nicht) sagen?

Um zu ergründen, wann Äußerungen rechtswidrig sind, ist ein Blick in das Grundgesetz (GG) erforderlich: Art. 5 Abs. 1 GG gewährleistet die Meinungsäußerungsfreiheit. Diese gilt allerdings nicht ohne Grenzen. Die bewusste Verbreitung unwahrer Tatsachen fällt von vornherein nicht unter seinen Schutz. Aber auch die Kundgabe von wahren Tatsachenbehauptungen oder Werturteilen kann gem. Art. 5 II GG dann unzulässig sein, wenn durch sie Persönlichkeitsrechte verletzt werden. Persönlichkeitsrechte wie das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG oder das Unternehmenspersönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. 19 Abs. 3 GG schützen insbesondere den sozialen Geltungsanspruch ihres Inhabers. Wird dieser „gute Ruf" durch eine Äußerung beschädigt, so kann der Betroffene u.U. zivilrechtliche Ansprüche geltend machen.[1]

2. Wer haftet für eine Äußerung?

Ansprüche können sich nicht nur gegen denjenigen richten, der sich selbst geäußert hat. Haftbar ist vielmehr jeder, dem die persönlichkeitsrechtsverletzende Äußerung als eigene zugerechnet werden kann. Zugerechnet werden kann eine fremde Äußerung zunächst demjenigen, der sie sich „zu eigen gemacht" hat. Ein „Zu-eigen-machen" liegt vor, wenn die fremde Äußerung so wiedergegeben wird, dass sie als eigene erscheint.[2] Wegen „Zu-eigen-machens" von fremden Äußerungen haften insbesondere auch Websitenhaber:innen, wenn sie nach außen erkennbar die Verantwortung für die Inhalte ihrer Website übernommen haben.[3] In eigener Person zugerechnet werden kann eine Äußerung allerdings auch dem bloßen „Verbreiter". Voraussetzung für die Verbreiterhaftung ist, dass die Äußerung weitergegeben wurde, ohne dass sich der Verbreiter von ihrem Inhalt distanziert oder diesen zuvor auf Wahrheit und Verletzungspotenzial überprüft hat.[4]

---

1 Unter Umständen sind rechtswidrige Äußerungen sogar strafbar, so etwa Beleidigungen oder Verleumdungen gem. § 185 bzw. § 186 Strafgesetzbuch (StGB). Bei der zivilrechtlichen Haftung sind ggf. die Haftungsprivilegien des DSA zu berücksichtigen.

2 Vgl. Bundesgerichtshof (BGH), Urt. v. 27. 3. 2012 – VI ZR 144/11 Rn. 11 – RSS-Feeds m.w.N.

3 Vgl. BGH, Urteil vom 4.4.2017 – VI ZR 123/16 Rn. 26 – klinikbewertungen.de.

4 Beater, MedienR, Rn. 442 ff.; 1488 ff.

II. Haftung für KI-Output

Drei Entscheidungen der Landgerichte machen deutlich, dass die soeben dargestellten Zurechnungsregeln auch für KI-generierte Inhalte gelten.

1. Die maßgeblichen Entscheidungen

Die erste Entscheidung erging bereits im Jahr 2024: Ein Familienunternehmen wehrte sich gegen Inhalte eines Online-Portals, auf dem Nutzer:innen Wirtschaftsinformationen über deutsche Firmen abrufen konnten.[5] Das Portal hatte fälschlicherweise eine Meldung veröffentlicht, demzufolge das klagende Unternehmen wegen Vermögenslosigkeit aus dem Handelsregister gelöscht werden sollte. Diese Fehlinformation war auf Veranlassung des Websiteninhabers von einem KI-System generiert worden. Dieser hatte das System dazu programmiert, voll automatisiert Daten aus öffentlichen Registern (z. B. dem Handelsregister) auszuwerten, aufzubereiten und zu veröffentlichen. Das Landgericht (LG) Kiel entschied, dass sich der Inhaber des Portals die KI-generierte Meldung zurechnen lassen musste und daher für diese haftete. Er habe die KI bewusst eingesetzt, selbst (aus Sicht des Gerichtes unzulänglich) programmiert und sich ihren Output „zu eigen gemacht", indem er nach außen erkennbar die inhaltliche Verantwortung für seine Website übernommen habe.[6]

In diesem Sinne entschied auch das LG Hamburg im Jahr 2025. Im Fall ging es um einen Post des KI-gestützten X-Accounts @grok, welcher von X (vormals Twitter) selbst betrieben wird und den Namen eines ebenfalls von der Plattform betriebenen Chatbots trägt.[7] Den Post hatte „Grok" automatisch als Antwort auf eine Nutzer:innenanfrage veröffentlicht. Darin wurde fälschlicherweise die Behauptung aufgestellt, der politisch aktive Verein „Campact e.V." beziehe einen hohen Anteil seiner finanziellen Mittel aus staatlicher Förderung. Gegen diese Darstellung wehrte sich der Verein „Campact": Er sah sich durch die Aussage in seinem Vereinspersönlichkeitsrecht verletzt. Das Gericht kam zu dem Ergebnis, dass X für die Falschaussage haftete: Durch die Präsentation auf dem von ihr betriebenem Account habe sich die Plattform den KI-generierten Post „zu eigen gemacht".[8]

Zuletzt hatte das LG München I darüber zu entscheiden, ob der Suchmaschinenbetreiber Google für unwahre Tatsachenbehauptungen in seinen „Übersichten mit KI" haftet.[9] Die „Übersichten mit KI" werden generiert, indem auf Suchanfragen von Nutzer:innen Informationen von relevanten Websites durch ein KI-System ausgewertet und zusammengefasst angezeigt werden. Im betroffenen Fall wurden bei Suchanfragen, die den Namen eines Verlages in Kombination mit bestimmten Stichwörtern enthielten, Übersichten angezeigt, die den Verlag u. a. fälschlicherweise mit Betrugsmaschen und unseriösen Geschäftspraktiken in Verbindung brachten. Der Verlag machte nun einen Anspruch auf Unterlassung gegen Google geltend. Das LG München bejahte die Haftung des Suchmaschinenbetreibers für die angezeigten Fehlinformationen: Google habe das eingesetzte KI-System selbst eingeführt, kontrolliere seine Funktionsweise und biete es den Nutzer:innen an.[10] Bezüglich des durch die „KI-Übersichten" verbreiteten Inhalts habe Google dabei zumutbare Überprüfungspflichten verletzt.[11] Die rechtswidrigen Äußerungen musste sich der Suchmaschinenbetreiber deshalb als eigene zurechnen lassen.

2. Bedeutung der Ergebnisse

Für KI-Output haftet also, wer sich diesen „zu eigen macht" oder ihn auf unzulässige Weise verbreitet. Dies gilt auch für

5 LG Kiel, Urteil vom 29.2.2024 – 6 O 151/23.

6 LG Kiel, Urteil vom 29.2.2024 – 6 O 151/23 Rn. 45. Zu diesem Ergebnis war das LG Düsseldorf bereits 2020 in einem ähnlichen Fall gelangt, vgl. LG Düsseldorf, Urteil vom 29.01.2020 - 12 O 163/19 Rn. 27 f. Das LG Düsseldorf hatte eine Haftung des Websiteinhabers allerdings noch i. E. abgelehnt. Im weiteren Verfahrensgang wurde diese wiederum vom OLG Düsseldorf bejaht, vgl. Oberlandesgericht (OLG) Düsseldorf, Urteil vom 18.03.2021 - I-16 U 136/20.

7 LG Hamburg, Beschluss vom 23.9.2025 – 324 O 461/25.

8 LG Hamburg, Beschluss vom 23.9.2025 – 324 O 461/25 Rn. 7.

9 LG München I, Urteil vom 28.5.2026 – 26 O 869/26.

10 LG München I, Urteil vom 28.5.2026 – 26 O 869/26 Rn. 34.

11 LG München I, Urteil vom 28.5.2026 – 26 O 869/26 Rn. 17.

Sachverhaltskonstellationen, in denen KI-generierte Inhalte nicht automatisch, sondern manuell, (etwa durch „Screenshots“ oder „copy and paste“) veröffentlicht werden. Auch in Fällen, in denen ein Chatbot einen rechtswidrigen Inhalt nur gegenüber einer einzelnen Person wiedergibt, können äußerungsrechtliche Ansprüche gegen denjenigen in Betracht kommen, dem die Aussagen des Chatbots zugerechnet werden können. Hier müssten, sofern eine natürliche Person betroffen ist, wohl zudem die Regelungen der DSGVO Beachtung finden.[12]

3. Welche Fragen sind noch offen?

Einige praxisrelevante Fragen bezüglich der automatisierten Generierung und Veröffentlichung von Inhalten sind allerdings noch offen. Nicht abschließend geklärt ist zunächst, ob die Zurechnung des Outputs als eigene Aussage des Veranlassers durch einen eindeutigen Hinweis auf den Einsatz von KI vermieden werden kann.[13] Das LG Kiel hatte einen solchen Hinweis in den Allgemeinen Geschäftsbedingungen (AGBs) der Website unberücksichtigt gelassen.[14] Das LG München I hatte selbst die Bezeichnung der Anzeige als „Übersicht mit KI“ nicht als hinreichend angesehen, um eine Zurechnung abzulehnen.[15] Ob jedenfalls eine ausdrückliche Distanzierung diese ausschließen kann, ist indes noch offen.

Unklar ist auch, welche Überprüfungspflichten bei der automatisierten Veröffentlichung von KI-Output eingehalten werden müssen. Offen ist zunächst, ob diese bereits vor Veröffentlichung des Inhalts oder erst nach dem Hinweis auf eine mögliche Rechtsverletzung einsetzen.[16] Auch der Umfang der Überprüfungspflichten wurde von den Gerichten bisher nicht abschließend festgelegt. Dabei ist insbesondere fraglich, welche Kontrollmechanismen sowohl den Persönlichkeitsrechten der Betroffenen ausreichend Rechnung tragen als auch technisch möglich und praktikabel sind.[17]

III. Fazit

Im Ergebnis lässt sich festhalten, dass für von KI generierte, persönlichkeitsrechtsverletzende Inhalte die allgemeinen äußerungsrechtlichen Haftungsregeln Anwendung finden. Wem ein rechtswidriger Inhalt zugerechnet werden kann, der kann vom Betroffenen zivilrechtlich in Anspruch genommen werden. Ob der verletzende Inhalt durch einen Menschen oder von KI erstellt, automatisiert oder manuell veröffentlicht oder nur gegenüber einer einzelnen Person wiedergegeben wurde, ist dabei unerheblich. Ob diese Haftung durch Distanzierung von veröffentlichten Inhalten oder die Einhaltung von Überprüfungspflichten ausgeschlossen werden kann, ist indes noch offen. Bis eine genauere Konturierung der Haftungsmodalitäten erfolgt, ist von einer automatisierten Veröffentlichung KI-generierter Inhalte abzuraten. Diese sollten vielmehr vor Veröffentlichung möglichst auf Wahrheitsgehalt und Verletzungspotenzial überprüft werden.

---

12 Vgl. Ory, KIR 2026, 81 (83).

13 Eine bloße Kennzeichnung des Inhalts nach Maßgabe des Art. 50 Abs. 4 UAbs. 2 der europäischen Verordnung über Künstliche Intelligenz (KI-VO) genügt jedenfalls nicht, um eine Zurechnung auszuschließen. Hierzu ausführlich Ory, KIR 2026, 81 (82).

14 Hierzu ausführlich Hirzle, RDi 2025, 39 (41).

15 LG München I, Urteil vom 28.5.2026 – 26 O 869/26 Rn. 43.

16 Diese Frage wurde vom LG München I thematisiert, i. E. jedoch offengelassen, vgl. LG München I, Urteil vom 28.5.2026 – 26 O 869/26 Rn. 45.

17 Siehe hierzu ausführlicher Bierekoven, RDi 2026, 43 (45); Burgemeister, GRUR-RR 2026, 78 (80); Hirzle, RDi 2025, 39 (40 f.); Voßberg, GRUR-Prax 2025, 771.

Impressum

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Humboldt-Universität Berlin.

Humboldt-Universität zu Berlin
Lehrstuhl für Bürgerliches Recht und Recht der Digitalisierung

Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Unter den Linden 11, 10117 Berlin

Tel. (030) 838-66754

E-Mail: recht@dfn.de

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn