Rechtliche Rahmenbedingungen für KI#Systeme: Immanente Herausforderungen und mögliche Lösungen durch Control-by-Design

Wilmer, Thomas

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Wilmer, T. (2021). Rechtliche Rahmenbedingungen für KI#Systeme: Immanente Herausforderungen und mögliche Lösungen durch Control-by-Design. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *30*(3), 56-62. https://doi.org/10.14512/tatup.30.3.56

OPEN ACCESS oekom

RESEARCH ARTICLE

Rechtliche Rahmenbedingungen für KI-Systeme

Immanente Herausforderungen und mögliche Lösungen durch Control by Design

Thomas Wilmer, *Institut für Informationsrecht, Hochschule Darmstadt, Haardtring 100, 64295 Darmstadt, DE (thomas.wilmer@h-da.de)*

Zusammenfassung • Der Autor stellt die komplexen rechtlichen Rahmenbedingungen für künstliche Intelligenz aus den Bereichen des Dateneigentums, des Datenschutzes und des Urheberrechts dar und erläutert, weswegen die unübersichtliche Rechtslage nicht dazu geeignet ist, auf Rechtssicherheit durch neue Regulierungen auf EU- oder nationaler Ebene zu hoffen. Stattdessen werden ein Regulierungsrahmen für zulässige Vertragsvereinbarungen sowie dazu passende Control by Design-Technikeinstellungen vorgeschlagen.

Legal framework conditions for AI systems. *Immanent challenges and possible solutions (control by design)*

Abstract • *The author presents the complex legal framework for artificial intelligence in data ownership, data protection, and copyright and explains why the confusing legal situation is not suitable for hoping for legal certainty through new regulations at the EU or national level. Instead, he proposes a regulatory framework for permissible contractual agreements and matching control-by-design settings.*

Keywords • *data ownership, data governance act, copyright, artificial intelligence*

Künstliche Intelligenz (KI) stellt aus rechtlicher Sicht verschiedene Herausforderungen an die Einordnung in das vorhandene Regulierungssystem: KI kann als Software mit vorgefertigten Programm-Elementen und von der Software selbst geschaffenen neuen Programmanteilen verstanden werden, was die Frage nach dem Geistigen Eigentum an den immateriellen Werten stellt, welche von der KI geschaffen werden. Daneben basiert KI immer auch auf einem (dann fortlaufend aktualisierten) Datensatz, welcher in aller Regel der Manifestation menschlicher oder maschineller Erfahrungswerte entspricht. Zu klären ist, wem dieser Datensatz zusteht. Soweit es sich hierbei um personenbezogene Daten handelt, gelten innerhalb der Europäischen Union strikte Regelungen zur Verwendbarkeit dieser Daten. Insgesamt stellt sich Frage nach Folgen des KI-Einsatzes für die Gesellschaft und nach der Transparenz der zugrunde gelegten oder neu geschaffenen Algorithmen sowie der Kontrolle der Einsatzbedingungen.

Bei kritischer Betrachtung der gängigen Geschäftsmodelle kann KI daneben auch als Mittel dienen, um Daten und Know-how der KI-Nutzer zu zentralisieren und dann wiederum allen zur Verfügung zu stellen, wobei die Wertschöpfung bei den KI-Betreibern verbleibt.

KI steht aktuell im Spannungsfeld zahlreicher neuer Regulierungsversuche auf nationaler und europäischer Ebene.

KI steht aktuell im Spannungsfeld zahlreicher neuer Regulierungsversuche auf nationaler und europäischer Ebene. Neben gesetzlichen Begrenzungen der Einsatzbereiche der KI und der Regelung der Verfügungsgewalt über Datensätze sollte verstärkt auch an die zentrale Frage gedacht werden, welche Möglichkeiten es gibt, vertragliche Vereinbarungen mit Endnutzern zur Nutzung der KI und Übertragung von Daten zu regulieren. Solche vertraglichen Vorgaben könnten dann in das Design der KI-Systeme einfließen und den Rahmen für eine Control by Design-Regelung bilden. Diese könnte eine übergeordnete datenschutzfreundliche Gesamteinstellung sein, welche sich an den Regelungen des Art. 25 EU-Datenschutzgrundverordnung (DSGVO) für Privacy-by-Design (datenschutzfreundliche Systemkonzep-

https://doi.org/10.14512/tatup.30.3.56
Received: Jun. 22, 2021; revised version accepted: Oct. 21, 2021; published online: Dec. 20, 2021 (peer review)

tion) und den Neuregelungen des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) orientiert.

Die Bedeutung der KI für Gesellschaft und Wirtschaft findet ihren Niederschlag in internationalen Bemühungen, die Entwicklung zu analysieren und zu regulieren. Nach Auffassung der deutschen Datenethikkommission (Datenethikkommission 2019) ist eine möglichst europäische Regulierungsreichweite analog zu den datenschutzrechtlichen Regelungen anzustreben. Das europäische Weißbuch zur künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen fordert „angesichts der erheblichen Auswirkungen, die KI auf unsere Gesellschaft und die notwendige Vertrauensbildung haben kann […], dass die europäische KI auf unseren Werten und Grundrechten wie Menschenwürde und Schutz der Privatsphäre fußt" (Europäische Kommission 2020a, S. 2).

Umsetzungsbedarf

Fraglich ist, inwiefern diese Ziele in einer funktionsfähigen, den Interessen der Betroffenen und der Wirtschaft angemessenen Form berücksichtigt werden können. Aus juristischer Sicht stellen sich eine ganze Reihe von Fragen aus verschiedenen Rechtsgebieten an den Einsatz der KI, einschließlich sämtlicher unscharf definierter Formen smarter und selbstlernender Produkte oder des Einsatzes sogenannter ‚Legal Tech' (Herberger 2018). Es bleibt zu klären, ob die neuen Regulierungsansätze und Absichtserklärungen mit bestehenden rechtlichen Rahmenbedingungen umzusetzen sind oder ob es einer grundsätzlich neuen Gesetzgebung bedarf, welche die Zulässigkeit des KI-Einsatzes in bestimmten Einsatzfeldern (etwa der Personal- oder Einstellungsbeurteilung oder des Kampfdrohneneinsatzes) oder in bestimmten Auswertungsbereichen (Big Data/gläserner Bürger) beschränkt. Anzustreben wäre eine homogene Regulierung sowohl der Fragen der Inhaberschaft der von der KI geschaffenen Softwareroutinen, der Zuordnung der ausgewerteten und erzeugten Datensätze, der Begrenzung der Einsatzgebiete und der Haftung für die Einsatzfolgen.

Diese Regelung müsste sich zugleich in KI-Systemen transparent abbilden lassen, so wie dies etwa beim Risikomanagement im Datenschutzbereich nach der DSGVO vorgesehen ist. Andernfalls droht eine Zersplitterung der gesetzlichen Lage, welche es den Betroffenen der KI-Nutzung erschwert, überhaupt einen Überblick über die KI-Nutzung zu erhalten. Je mehr Einzelregulierungen vorhanden sind, welche umfangreiche Informationspflichten enthalten, umso größer ist die Gefahr der sogenannten ‚Consent Fatigue' (Rauer und Ettig 2021): Nutzer verlieren das Interesse an der Wahrnehmung der zahllosen Informationen und sind bereit, Nutzungen zu akzeptieren, ohne überhaupt noch zu lesen, welchen Inhalt die Informationen haben, selbst wenn es eine transparente Zusammenfassung geben sollte. Als Musterbeispiel dafür können die ‚Cookie-Pop-Ups' gelten, die von vielen Nutzern nicht mehr gelesen, sondern nur noch akzeptiert werden. Nach einer Statista-Umfrage vom 04. 06. 2020 gaben 41 Prozent der Befragten in Deutschland an, sich grundsätzlich die Inhalte der Cookie-Hinweise nicht durchzulesen und einfach auf ‚Okay' oder ‚Cookies akzeptieren' zu klicken (Statista Research Department 2020).

Im Folgenden soll vor der Darstellung der auf deutscher und EU-Ebene geplanten Regelungen aufgezeigt werden, welche rechtlichen Rahmenbedingungen grundsätzlich zu beachten sind, die sich mit den Rechten an den durch KI betroffenen Daten und der zugrundeliegenden Software befassen.

Fragen des Geistigen Eigentums

Geistiges Eigentum an den in Programm- und Datenform vorliegenden Ergebnissen der KI wird vor allem an urheberrechtlichen Fragen auszurichten sein. Urheberrechtlich ist zu klären, wer der Schöpfer der Ergebnisse der KI ist, sowohl was neu generierten Programmcode als auch Datensätze betrifft. Handelt es sich um den Urheber des Programms, da dieser typischerweise bereits vorgefertigte Routinen in die KI implementiert hat, welche dann – ebenfalls nach vom Urheber vorgegebenen Algorithmen – zusammengesetzt werden (siehe Abb. 1)? Ist das Ergebnis der KI daher nichts weiter als eine verlängerte Schöpfung durch einen Programmierer? Falls dies so wäre, würde sich jedoch die Frage stellen, ob KI dann selbst eine ausreichende Kreativität beinhaltet und so wiederum die Schöpfungshöhe des Programms in Frage stellen. Der KI selbst Rechte an den Ergebnissen einzuräumen, würde offenlassen, wer über die Rechteeinräumung an Dritte entscheiden soll (Legner 2019): Die KI oder die Schöpfer der KI? Oder auch die Nutzer?

Unvorhersehbarkeit und Intransparenz dürfen nicht dazu führen, dass das Recht den Innovationszyklen der KI hinterherhinkt.

Grundsätzlich erfordert der Investitionsschutz nach dem geltenden Urheberrechtsgesetz eine menschliche Schöpfung. Je weiter sich das Schöpfungsergebnis durch den Einsatz von KI von den Vorgaben der Programmierung entwickelt, umso weniger kann der Schutz dem Urheber als menschlichem Schöpfenden zugerechnet werden (Specht-Riemenschneider 2021). Um die Rechtsunsicherheiten beim Investitionsschutz zu beseitigen, wird für die Softwareerzeugnisse der KI u. a. ein Schutzrecht für Algorithmenerzeugnisse gefordert (Specht-Riemenschneider 2021).

Eigentumsrechtliche Zuordnung der Datensätze

Neben den neu geschaffenen Softwareroutinen ist zu fragen, wer Inhaber der durch die KI geschaffenen Daten sein kann. Grundsätzlich geht die Rechtsprechung davon aus, dass Software eine Sache darstellt, da sie einen binären physikalischen Ladungszustand auf einem Datenträger repräsentiert. Folgt man dieser Auffassung und wendet sie auch auf sonstige Daten an, könnten die Inhaber der Hardware Ausschlussrechte gegenüber Dritten an den Ergebnissen der KI geltend machen. Gegen die dingliche beziehungsweise eigentumsrechtliche Zuordnung von Datensätzen wendet sich der Bundesbeauftragte für Datenschutz und Informationssicherheit mit der Forderung, dass statt „des verdinglichenden Datenbegriffes im Sinne eines ‚Dateneigentums' […] eine Datenwirtschaft den Leitbegriff der Information und damit auch die Wissensperspektive" (BfDI 2021, S. 2) betont werden sollten, damit „die gesellschaftlichen Herausforderungen […] mit Blick auf Daten als öffentliches Gut und die Potenziale von Open Source, Open Data und Stärkung von Demokratiestrukturen besser sichtbar" (ebd.) würden. Teils werden auch Rechte der Skribenten der Daten (also derjenigen, welche faktisch, etwa durch das Festlegen und Befahren einer Navigationsroute im Pkw, die Datenspur ‚schreiben') und der Datenbesitzer als Anhaltspunkt formuliert (Hoeren 2019).

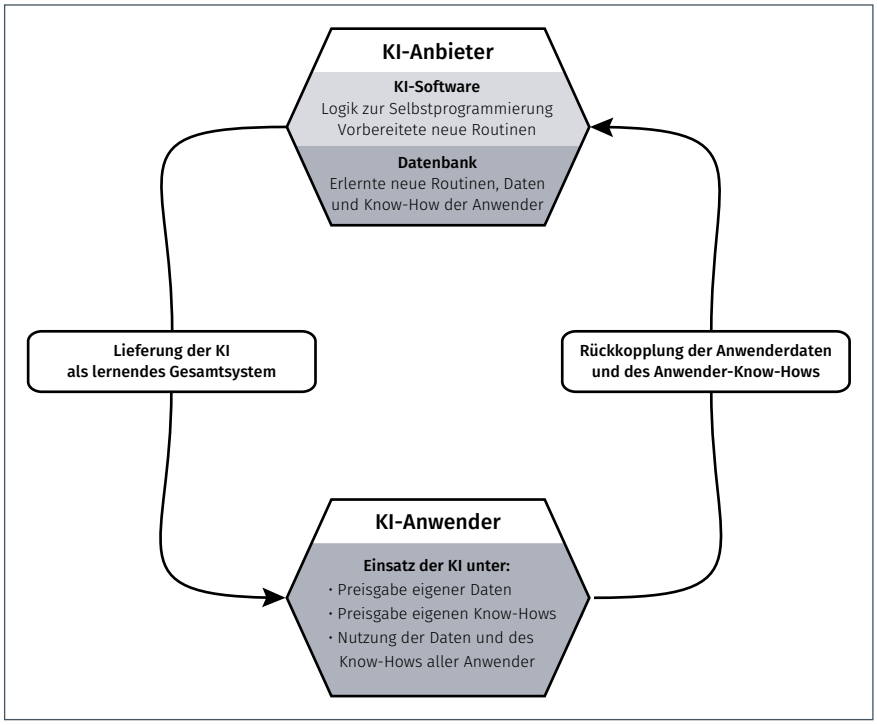

Abb. 1: Schematische KI-Darstellung für KI mit fortlaufender Rückkoppelung der Ergebnisse.
Falls man den Urheber des Programms nicht als Schöpfer des Ergebnisses der KI betrachtet, würde es sich bei den Ergebnissen (einschließlich neuer Algorithmen) nicht mehr um eine ‚menschliche' Schöpfung im Sinne des Urhebergesetzes handeln (Ory und Sorge 2019). Gleiches würde für den nach dem Urheberrecht möglichen Datenbankschutz gelten. In der Konsequenz wären die Ergebnisse dann gemeinfrei und würden der Allgemeinheit zur Verfügung stehen. Die Nichtzuordnung einer kreativen Leistung zu einem Menschen bedeutete damit, dass die Schöpfung von Ergebnissen durch KI nach urheberrechtlichen Maßstäben nicht zu kommerzialisieren wäre. *Quelle: eigene Darstellung*

Allein aus dem Versuch einer eigentumsrechtlichen Zuordnung lassen sich keine adäquaten Lösungen finden, da beispielsweise beim Wechsel des Geschäftsmodells vom Verkaufs eines smarten Produkts (samt KI) zu einer Vermietung der Systembetreiber die Zuordnung des Eigentums bzw. des Besitzes allein bestimmen könnte. Auch der Besitz als Anhaltspunkt ist manipulierbar (etwa durch die Verlegung der Daten in die Cloud), sodass die Skribenteneigenschaft noch am ehesten eine Rechtezuordnung an den Nutzer der KI erlaubt.

Schutz personenbezogener Daten

Datenschutzrechtlich können die Ergebnisse der KI nur relevant sein, wenn sie auf eine natürliche Person bezogen oder beziehbar sind. Ob dies zutrifft, kann nur anhand des Einsatzes der KI beurteilt werden. Liegt ein Personenbezug der auszuwertenden Daten vor, können KI-Einsätze nur auf Basis einer Rechtsgrundlage (u. a. Einwilligung, Vertragserfüllung, berechtigtes Interesse etc.) erfolgen. Bereits 15,9 % der 2019 vom Bundesverband der Personalmanager im März 2019 befragten Unternehmen setzen KI-Anwendungen in der Personalarbeit ein (BPM 2019). Nach den europäischen Maßstäben der DSGVO erfordert ein solcher Einsatz neben einer Rechtsgrundlage die Offenlegung der Scoring-Berechnungen und die Anwendung der Antidiskriminierungsgrundsätze des Allgemeinen Gleichbehandlungsgesetzes. Zu den Risiken im Datenschutzbereich wird auf die ‚Opazität' der KI verwiesen, welche keine transparenten Vorhersagen über das Verhalten der KI zulasse (Europäische Kommission 2020 a, S. 14). Als KI-immanente Risiken gelten Unvorhersehbarkeit und Intransparenz (Meyer 2018), diese dürfen jedoch nicht dazu führen, dass das Recht den Innovationszyklen der KI hinterherhinkt.

Problematisch kann der KI-Einsatz in Arbeitsverhältnissen sein, in welchem KI-Einsatz aufgrund einer Einwilligung – trotz des möglichen Machtungleichgewichts – denkbar ist. Nach einem datenschutz- und grundrechtlich kritisierten Urteil des Landesarbeitsgerichts München[1] kann sogar die Verarbeitung personenbezogener Beschäftigtendaten durch eine KI-Software

1 Beschluss vom 23. 07. 2020–2 Tabakverordnung 126/19.

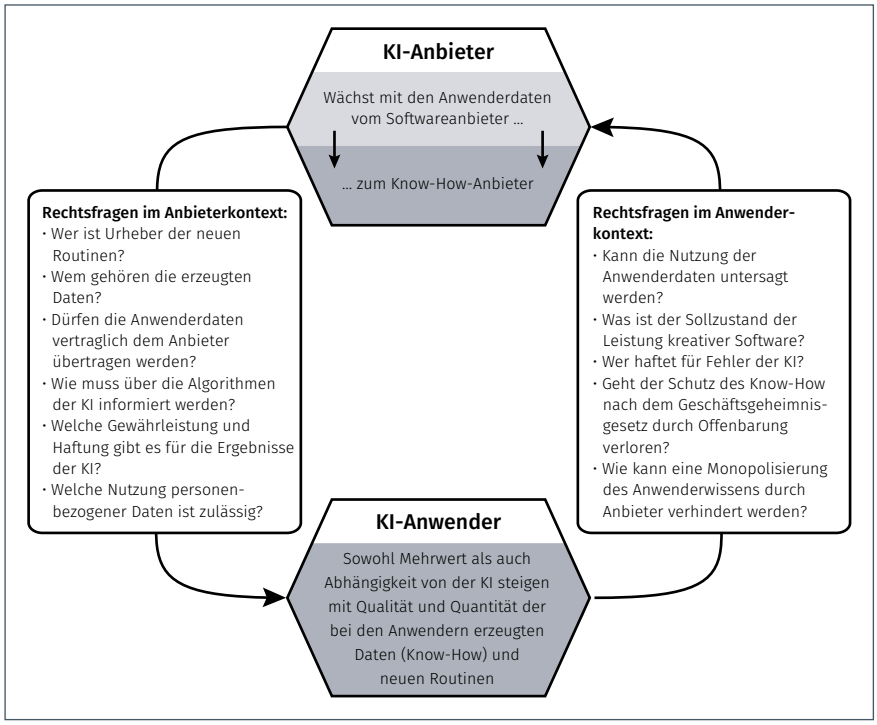

Abb. 2: Formaler Knowhow-Verlust durch Offenbarung des Knowhows an KI. *Quelle: eigene Darstellung*

für präventive Zwecke zulässig sein, wenn es darum geht, Auffälligkeiten des individuellen Arbeitsverhaltens zu erkennen (Wedde 2021).

Eine Einwilligung in die KI-Nutzung und entsprechende Big-Data-Anwendungen wird allerdings in aller Regel an den erforderlichen datenschutzrechtlichen Transparenzvorgaben scheitern. Die Zwecke der durch eine Einwilligung erlaubten Datenverarbeitung nach Art. 6 I a/Art. 7 DSGVO müssen konkret benannt werden. Dies gebietet auch das Prinzip der Zweckbindung nach Art. 5 I b DSGVO, was bei einer echten Big Data-Datenaggregation naturgemäß nicht der Fall sein wird, da es gerade die Idee einer Datenaggregation ist, noch unbekannte spätere Analyse und Netzwerkeffekte zu generieren (Holthausen 2021).

Diese Widersprüche zum Wunsch nach einer Big-Data-Nutzung in Europa lassen sich schwer auflösen. Nachdem sich die deutsche Bundesregierung mit den Eckpunkten einer Datenstrategie bemüht hat, eine Kommerzialisierung der Datenauswertung nicht grundsätzlich abzulehnen, wird diese Strategie vom Bundesbeauftragten für Datenschutz kritisch hinterfragt (BfDI 2021, S. 2). Auch die Idee, dem Konflikt mit dem Datenschutz durch eine Anonymisierung personenbezogener Daten zu entgehen, welche die Daten dem Anwendungsbereich der DSGVO entziehen würde, ist umstritten. Teilweise wird nämlich vertreten, dass die Anonymisierung selbst ebenfalls einer datenschutzrechtlichen Rechtsgrundlage bedarf (Hornung und Wagner 2020). Datenschutz kann jedenfalls dann Big-Data-Anwendungen entgegenstehen, soweit keine vollständige Anonymisierung der Daten vorgenommen werden kann (Roßnagel 2013). Selbst wenn eine Anonymisierung gelingt, sind Beeinträchtigungen der Grundrechtsausübung nicht ausgeschlossen. Roßnagel (2013, S. 566) weist für bestimmte Einsatzszenarien darauf hin, dass KI-Analysen etwa dazu führen können, dass „durch eine Big-Data-Analyse bekannt wird, dass Angehörige einer politischen Gruppe sich überdurchschnittlich oft an einem bestimmten Ort aufhalten, in einem bestimmten Geschäft einkaufen und ÖPNV fahren“. Dies könne wiederum dazu führen, dass „bei vielen, die vermeiden wollen, dieser Gruppe zugerechnet zu werden, […] dass sie den Ort, das Geschäft und vielleicht sogar das Verkehrsmittel meiden, um nicht in einen ihnen unangenehmen Verdacht zu geraten“ (ebd.). Damit verstärkten solche Analysen „die Normativität der Normalität“ (ebd.) und reduzierten die für die Demokratie notwendige ‚Soziodiversität‘.

Das Datenschutzrecht bietet somit keine befriedigende Auskunft über die Grenzen der Nutzungsmöglichkeit der KI, da der von dieser generierte Datensatz – durch Anonymisierung den Regelungen der Datenschutzgrundverordnung und weiterer in Verabschiedung befindlicher E-Privacy-Regelungen (Council of the European Union 2021) – der Kontrolle der Betroffenen entzogen werden kann.

Versuche der Monopolisierung der KI-Ergebnisse

Vertragsrechtlich sind in der Praxis Versuche zu verzeichnen, die Nutzern der KI zu verpflichten, die KI-Ergebnisse den Herstellenden zu übertragen, damit diese dann Zugriff auf die Ergebnisse erhalten und entsprechende Big Data-Anwendungen erstellen, um die Daten anderweitig nutzen zu können. Grenzen dieser Rückübertragungsversuche finden sich im Recht der Allgemeinen Geschäftsbedingungen und des Kartellrechts.

De lege lata ist mithin festzuhalten, dass die KI-Ergebnisse nicht ohne Weiteres den Herstellenden zustehen. Da jedoch die KI vertragliche Rahmenbedingungen voraussetzt, wird in aller Regel auch die Rückkopplung der KI-Ergebnisse den Herstellenden zu Gute kommen, siehe Abb. 2. Gesetzliche Haftungsregelungen wiederum werden den multikausalen Zusammenhängen bei KI-Ergebnissen und der Zersplitterung der Haftungszuordnung angesichts der Beweisnöte der Anwendern nicht gerecht.

Daher bedarf es einer Regelung der Datensouveränität der Betroffenen, die die Wissensagglomeration der Betreiber der KI-Systeme angemessen einbezieht.

Gesellschaftliche Folgen des KI-Einsatzes und Lösungsansätze

Angesichts der unübersichtlichen und zu komplexen rechtlichen Situation (Kühling und Sackmann 2020) besteht weiterer Handlungsbedarf zum Umgang mit der KI, eine lediglich beobachtende Haltung wird nicht genügen.

De lege ferenda werden Versuche unternommen, in einzelnen marktrelevanten Bereichen die Offenlegung von Algorithmen vorzugeben, welche beispielsweise die Funktionsweise digitaler Marktplätze und die Information über KI-Funktionsweisen betreffen:

Deutsche Gesetzgebung

Im Gesetzentwurf der Bundesregierung „zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union“ (Deutscher Bundestag 2021) werden in Artikel 246 d § 1 BGB-neu allgemeine Informationspflichten für Betreiber von Online-Marktplätzen festgelegt, etwa über die „Hauptparameter zur Festlegung des Rankings und die relative Gewichtung der Hauptparameter zur Festlegung des Rankings im Vergleich zu anderen Parametern“ zu informieren. Die Reform des Netzwerkdurchsetzungsgesetzes (NetzDG), welches sich mit der Bekämpfung von ‚Hate Speech‘ auf sozialen Plattformen befasst, greift die KI-Problematik auf, indem eine in § 2 Absatz 2 NetzDG festgelegte neue Informationspflicht vorsieht, dass über „Art, Grundzüge der Funktionsweise und Reichweite von gegebenenfalls eingesetzten Verfahren zur automatisierten Erkennung von Inhalten“ Auskunft gegeben werden muss.

Weiterhin wird in einer Neuregelung des Kartellrechts (§ 19 Abs. 2 Nr. 1 GWB) vorgesehen, dass unter bestimmten Umständen den Zugang zu Daten und gegebenenfalls auch KI-Datenbanken eröffnet werden muss (Huerkamp und Nuys 2021). Weiterhin wird im Betriebsrätemodernisierungsgesetz zur Stärkung der Stellung des Betriebsrats bei der Beurteilung von KI-Einsätzen die Hinzuziehung einer sachverständigen Person ermöglicht.

Europäische Ansätze

Umfassender als diese zersplitterten nationalen Ansätze fallen, wie im Folgenden dargestellt, europäische Regelungen zur KI-Kontrolle aus:

Artificial Intelligence Act

In diesem Verordnungsvorschlag (COM/2021/206 final) sollen unter anderem KI-Systeme verboten werden (Art. 5 des Verordnungsentwurfs), die Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person einsetzen oder eine Schwäche beziehungsweise Schutzbedürftigkeit einer bestimmten Gruppe von Personen ausnutzen sowie Systeme zur Klassifizierung der Vertrauenswürdigkeit natürlicher Personen und biometrische Echtzeit-Fernidentifizierungssysteme. Daneben sind Regelungen zur transparenten Information, zum Risikomanagement, zu Daten und Daten-Governance, zur menschlichen Aufsicht und zu weiteren Sicherheitsmaßnahmen bei ‚Hochrisiko‘-KI-Systemen vorgesehen.

Data Governance Act, Data Act

Mit dem Data Governance Act (Europäische Kommission 2020 b) soll generell die Bereitstellung von Daten geregelt werden. Dies gilt für Daten des öffentlichen Sektors zur Weiterverwendung in Fällen, in denen diese Daten den Rechten anderer unterliegen, die gemeinsame Datennutzung durch Unternehmen gegen Entgelt in jedweder Form, die Ermöglichung der Nutzung personenbezogener Daten mithilfe eines „Mittlers für die gemeinsame Nutzung personenbezogener Daten“ (Europäische Kommission 2020 b), der Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung (DSGVO) unterstützen soll, sowie die Ermöglichung der Nutzung von Daten aus altruistischen Gründen. Er soll nicht darauf abzielen, „wesentliche Rechte auf den Zugang zu Daten und deren Nutzung zu gewähren, zu ändern oder zu beseitigen“ (Europäische Kommission 2020 b). Es ist geplant, diese Art von Maßnahmen in einen möglichen Rechtsakt über Daten (2021) aufzunehmen (European Parliament 2021).

In Erwägungsgrund 6 des Data Governance Act wird darauf verwiesen, dass es für Datenbanken, die personenbezogene Daten enthalten, Techniken gibt, „die datenschutzfreundliche Analysen ermöglichen, zum Beispiel Anonymisierung, Pseudonymisierung, differentielle Privatsphäre, Generalisierung oder Datenunterdrückung und Randomisierung“ (Europäische Kommission 2020 b). Mithilfe dieser soll eine sichere Weiterverwendung personenbezogener Daten und vertraulicher Geschäftsdaten für Forschung, Innovation und statistische Zwecke gewährleistet werden können. Schließlich heißt es, dass die Verarbeitung personenbezogener Daten stets auf einem der Rechtsgründe beruhen solle, die in Artikel 6 DSGVO aufgeführt sind.

Die Abgrenzung der DSGVO zum Data Governance Act bleibt leider unklar (Graef et al. 2020), da nicht eindeutig geklärt ist, ob der Data Governance Act auch pseudonyme Daten erfasst. Die neue Gesetzgebung „wird die im Rahmen der Richtlinie über offene Daten noch zu erlassenden Vorschriften über hochwertige Datensätze ergänzen, die EU-weit den kostenlosen Zugang zu bestimmten Datensätzen in maschinenlesbarem Format und über genormte Anwendungsprogrammierschnittstellen […] regeln sollen. […] Für 2021 sind weitere konkrete Vorschläge für besondere Datenräume geplant, beispielsweise für einen europäischen Gesundheitsdatenraum und einen Datenraum für den Grünen Deal. All dies wird ergänzt durch einen neuen Rechtsakt über Daten, der den Bürgerinnen und Bürgern sowie den Behörden einen besseren Zugang zu Daten aus dem sogenannten Internet of Things der Industrie und zu Massendaten im Besitz von Unternehmen sichern und eine bessere Kontrolle über solche Daten verschaffen soll, um eine gerechtere Wirtschaft aufzubauen und Vorteile für die Gesellschaft insgesamt zu erzielen.” (Europäische Kommission 2020 c, 4) Soweit diese Regelungen parallel nebeneinander bestehen bleiben, wird der Wunsch nach einer transparenten Regelung jedoch unerhört bleiben.

Vorschläge zur vertraglichen Regulierung, zu Control by Design und Technikgestaltung

Politisch wünschbare Regulierungsansätze – und insbesondere der geplante europäische ‚Data Act' sollten daher Grenzen der Auswertbarkeit der KI-Ergebnisse durch die Systembetreiber festlegen, einen transparenten Einsatz der KI insbesondere in sensiblen persönlichkeitsrechtlichen Bereichen der Analyse (Medizin und Arbeitswelt) festlegen und arbeitsweltliche Grenzen des Ersatzes menschlicher Arbeitsleistung durch KI zumindest anstreben.

Denkbar wäre eine übergreifende Regulierung auf europäischer Ebene, welche technikorientiert, ähnlich wie die aktuell (erneut) in Verabschiedung befindliche E-Privacy-Verordnung, und szenariobasiert die Risiken der KI in den Blick nimmt und die erwähnten rechtliche Lücken schließt. Zugleich muss sie jedoch das Verhältnis zur Datenschutzgrundverordnung klarer als im Data Governance Act regeln und auch eine Einwilligung in noch nicht bekannte Auswertungsarten und Daten mit verschiedenen Stufen des Personenbezugs in bestimmten Fällen zulassen, wenn KI und Big Data ernsthaft betrieben werden sollen.

Hierzu kämen zwei Ansätze in Betracht:

Klauselregelungen für Datenübertragungen

Da die dargestellten gesetzlichen Regulierungsansätze völlig heterogene Fälle der Information der Nutzer über den KI-Einsatz (abhängig von der Art der Daten) vorsehen, sollte eine Rahmenregelung für zulässige Datenauswertungen sowohl für personenbezogene als auch für anonymisierte Daten vorgesehen werden (Schur 2020). Diese Klauselregelungen könnten sich an den AGB-Klauselregelungen der §§ 308, 309 BGB oder den sog. ‚grauen' und ‚schwarzen' Klauseln der EU-Gruppenfreistellungsverordnungen orientieren. So könnten – orientiert an den bekannten Technikfolgen der KI – die Grenzen einwilligungsfähiger personenbezogener Datenauswertungen und nicht personenbezogener Datenauswertungen unterschieden werden. Dies würde zugleich einen klaren Rahmen für die Ersteller und Betreiber von KI-Systemen darstellen, die Rechtssicherheit über die wirksamen Vereinbarungen mit den Nutzern erhalten. Denkbar wäre hier auch eine Beteiligung der Nutzer an der Wertschöpfung abhängig vom Umfang der Einwilligung in die Datenauswertung.

Control by Design

Analog zu den Regelungen der DSGVO für Privacy by Design könnte auch für nicht personenbezogene Daten – begrenzt durch die und angebunden an die oben erwähnten Klauselregelungen – eine Control by Design-Regelung eingeführt werden (der Begriff ‚Privacy' träfe hier nicht zu, da auch anonyme Auswertungen von der Datensouveränität umfasst wären).

So wie das im Entwurf vorliegende Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in seinen §§ 25, 26 den Einsatz von ‚Personal Information Management Services' regelt und eine transparente Einwilligung der Freigabe von Endnutzerdaten (etwa bei Cookies) ermöglicht, könnte auch im Data Act die im TTDSG vorgesehene Einschaltung von „Anerkannten Diensten zur Einwilligungsverwaltung" (§ 26 TTDSG) erfolgen.

In der konkreten Ausprägung der Einwilligung könnten auch banale Fragen wie die Haftung für Ergebnisse der KI-Aktivitäten gegenüber den beteiligten Akteuren (Hacker 2020; Zech 2019) oder die Übertragung der Scoring-Transparenz der DSGVO für nicht-personenbezogene KI-Daten berücksichtigt werden.

Die EU versucht in ihren Regulierungsansätzen, der Marktmonopolisierung im KI-Umfeld und der Monetarisierung der Nutzerdaten entgegenzuwirken, um auch altruistische Datenverwendungen zu ermöglichen und bei der Anwendung der KI die Grundrechte der Nutzer zu beachten. Eine entsprechende Umsetzung in der Praxis müsste sich jedoch am Kriterium der Umsetzbarkeit messen lassen, wenn sie erfolgreich sein soll.

Mit einer solchen – über den Data Governance Act hinausgehenden – Regelung des Control by Design wäre es denkbar, der Datensouveränität der Nutzer gerecht zu werden und zugleich eine sichere Rechtsgrundlage für die Betreiber der Systeme zu schaffen.

Angabe von Finanzierungsquellen

Der vorliegende Forschungsartikel hat keine Förderung erhalten.

Literatur

BfDI – Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2021): Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Ausschusses Digitale Agenda am 24. Februar 2021. Online verfügbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/StgN_StgN_Anh%C3%B6rung-Datenstrategie-Bundesregierung.pdf;jsessionid=7D1B64827D3B8DA4D33C87024D824D47.intranet242?__blob=publicationFile&v=4, zuletzt geprüft am 21. 10. 2021, S. 1.

BPM – Bundesverband der Personalmanager (2019): Künstliche Intelligenz in der Personalarbeit. Online verfügbar unter https://www.bpm.de/sites/default/files/20190429_auswertung_bpm-pressemitteilung_final_0.pdf, zuletzt aufgerufen am 18. 10. 2021.

Council of the European Union (2021): Proposal for a regulation of the European Parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/EC (regulation on privacy and electronic communications). Online verfügbar unter https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf, zuletzt geprüft am 21. 10. 2021.

Datenethikkommission (2019): Gutachten der Datenethikkommission der Bundesregierung, Potsdam, S. 224. Online verfügbar unter https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf, zuletzt geprüft am 26. 09. 2021.

Deutscher Bundestag (2021): Drucksache 19/27 655. Berlin: H. Heenemann. Online verfügbar unter https://dserver.bundestag.de/btd/19/276/1927655.pdf, zuletzt geprüft am 21. 10. 2021.

Europäische Kommission (2020 a): Weißbuch zur Künstlichen Intelligenz. Ein europäisches Konzept für Exzellenz und Vertrauen. Online verfügbar unter

https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf, zuletzt geprüft am 10. 11. 2021.

Europäische Kommission (2020 b): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz). Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0767&from=EN, zuletzt geprüft am 08. 11. 2021.

Europäische Kommission (2020 c): Verordnung über Daten-Governance – Fragen und Antworten. Online verfügbar unter https://ec.europa.eu/commission/presscorner/api/files/document/print/de/qanda_20_2103/QANDA_20_2103_DE.pdf, zuletzt geprüft am 25. 11. 2021.

European Parliament (2021): Legislative Train 09.2021. 2 a Europe fit for the digital age. Online verfügbar unter https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-europe-fit-for-the-digital-age/file/data-act, zuletzt geprüft am 21. 10. 2021.

Graef, Inge; Husovec, Martin; van den Boom, Jasper (2020): Spill-overs in data governance. Uncovering the uneasy relationship between the GDPR's right to data portability and EU sector-specific data access regimes. In: Journal of European Consumer and Market Law 9 (1), S. 3–16. https://doi.org/10.2139/ssrn.3369509

Hacker, Philipp (2020): Europäische und nationale Regulierung von Künstlicher Intelligenz. In: Neue Juristische Wochenschrift 73 (30), S. 2142–2147. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fnjw%2F2020%2Fcont%2Fnjw.2020.2142.1.htm&pos=1&hlwords=on, zuletzt geprüft am 21. 10. 2021.

Herberger, Maximilian (2018): „Künstliche Intelligenz" und Recht. In: Neue Juristische Wochenschrift 71 (39), S. 2825–2829. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fnjw%2F2018%2Fcont%2Fnjw.2018.2825.1.htm&pos=2&hlwords=on, zuletzt geprüft am 21. 10. 2021.

Hoeren, Thomas (2019): Datenbesitz statt Dateneigentum. In: Multimedia und Recht 22 (1), S. 5–8. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2019%2Fcont%2Fmmr.2019.5.1.htm&pos=1&hlwords=on, zuletzt geprüft am 21. 10. 2021.

Holthausen, Joachim (2021): Big data, people analytics, KI und Gestaltung von Betriebsvereinbarungen. Grund-, arbeits- und datenschutzrechtliche An- und Herausforderungen. In: Recht der Arbeit 74 (1), S. 19–32. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Frda%2F2021%2Fcont%2Frda.2021.19.1.htm&pos=3, zuletzt geprüft am 21. 10. 2021.

Hornung, Gerrit; Wagner, Bernd (2020): Anonymisierung als datenschutzrelevante Verarbeitung? In: Zeitschrift für Datenschutz 10 (5), S. 223–228. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2020%2Fcont%2Fzd.2020.223.1.htm&anchor=Y-300-Z-ZD-B-2020-S-223-N-1, zuletzt geprüft am 21. 10. 2021.

Huerkamp, Florian; Nuys, Marcel (2021): Datenzugang nach § 19 Abs. 2 Nr. 4 GWB n. F. – Geglückte „Klarstellung"? In: Neue Zeitschrift für Kartellrecht 9 (7), S. 327–329. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fnzkart%2F2021%2Fcont%2Fnzkart.2021.327.1.htm&pos=7, zuletzt geprüft am 21. 10. 2021.

Kühling, Jürgen; Sackmann, Florian (2020): Irrweg Dateneigentum. In Zeitschrift für Datenschutz 10 (1), S. 24–30. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2020%2Fcont%2Fzd.2020.24.1.htm&pos=16, zuletzt geprüft am 21. 10. 2021.

Legner, Sarah (2019): Erzeugnisse Künstlicher Intelligenz im Urheberrecht. In: Zeitschrift für Urheber und Medienrecht 63 (11), S. 807–812. Online verfügbar unter https://www.researchgate.net/profile/Sarah-Legner-2/publication/343510297_Erzeugnisse_Kunstlicher_Intelligenz_im_Urheberrecht/links/5fb4d44fa6fdcc9ae05ef8c8/Erzeugnisse-Kuenstlicher-Intelligenz-im-Urheberrecht.pdf, zuletzt geprüft am 21. 10. 2021.

Meyer, Stephan (2018): Künstliche Intelligenz und die Rolle des Rechts für Innovation. In: Zeitschrift für Rechtspolitik 51 (8), S. 233–237. Online verfügbar unter https://beck-online.beck.de/?vpath=bibdata%2fzeits%2fZRP%2fcont%2fZRP%2ehtm, zuletzt geprüft am 21. 10. 2021.

Ory, Stephan; Sorge, Christoph (2019): Schöpfung durch Künstliche Intelligenz? In: Neue Juristische Wochenschrift 72 (11), S. 710–712. Online verfügbar unter https://beck-online.beck.de/?vpath=bibdata%2Fzeits%2FNJW%2F2019%2Fcont%2FNJW%2E2019%2E710%2E1%2Ehtm, zuletzt geprüft am 21. 10. 2021.

Rauer, Nils; Ettig, Diana (2021): Update Cookies 2020. Aktuelle Rechtslage und Entwicklungen. In: Zeitschrift für Datenschutz 11 (1), S. 18–24. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2021%2Fcont%2Fzd.2021.18.1.htm&pos=2&hlwords=on, zuletzt geprüft am 21. 10. 2021.

Roßnagel, Alexander (2013): Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. In: Zeitschrift für Datenschutz 3 (11), S. 562–567. Online verfügbar unter https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzd%2F2013%2Fcont%2Fzd.2013.562.1.htm&anchor=Y-300-Z-ZD-B-2013-S-562-N-1, zuletzt geprüft am 21. 10. 2021.

Schur, Nico (2020): Die Lizenzierung von Daten. Einordnung, Grenzen und Möglichkeiten von vertraglichen Zugangs- und Datennutzungsrechten in der digitalen Ökonomie. In: Jeanette Hofmann; Ingolf Pernice; Thomas Schildhauer; Wolfgang Schulz (Hg.): Internet und Gesellschaft. Schriften des Alexander von Humboldt Institut für Internet und Gesellschaft: Tübingen Mohr Siebeck.

Specht-Riemenschneider, Louisa (2021): Urheberrechtlicher Schutz für Algorithmenerzeugnisse? Phasenmodell de lege lata, Investitionsschutz de lege ferenda? In: Wettbewerb in Recht und Praxis 18 (3), S. 273–275.

Statista Research Department (2020): Umfrage zum Umgang mit Cookie-Hinweisen in Deutschland 2020. Online verfügbar unter https://de.statista.com/statistik/daten/studie/1121071/umfrage/umgang-mit-cookie-hinweisen-in-deutschland/, zuletzt geprüft am 13. 10. 2021.

Wedde, Peter (2021: Anmerkung – Streit um Einigungsstellenspruch zur Einführung eines IT-Sicherheitssystems. Anlasslose präventive Verarbeitung von Beschäftigtendaten durch KI-Software zulässig, LArbG München v. 23. 07. 2020–2 TaBV 126/19, jurisPR-ArbR 17/2021 Anm. 6. In: Juris – Das Rechtsportal.

Zech, Herbert (2019): Künstliche Intelligenz und Haftungsfragen. In: Zeitschrift für die gesamte Privatrechtswissenschaft 5 (2), S. 198–219.

PROF. DR. THOMAS WILMER
ist seit 2002 Professor für Informationsrecht an der Hochschule Darmstadt und leitet dort das Institut für Informationsrecht. Er befasst sich mit Fragen des Lizenz- und Datenschutzrechts und verwandter Bereiche des Informationsrechts.