DIE VERWALTUNG, 58 (2025) 2: 19 – 52
https://doi.org/10.3790/verw.2025.411108

EIN KI-TRANSPARENZREGISTER FÜR DIE ÖFFENTLICHE VERWALTUNG

Unions- und verfassungsrechtliche Rahmenbedingungen

Von Jonas Botta, Berlin*

I. Digitale Transformation der öffentlichen Verwaltung

Nur eine digitale Verwaltung ist eine zukunftsfähige Verwaltung. Ohne eine stärkere Automatisierung und Vernetzung der Behördenarbeit lässt sich weder die stetig wachsende Aufgabenlast noch der gleichzeitige Personalmangel im Öffentlichen Dienst bewältigen[1]. Folglich hängt vom Gelingen der digitalen Verwaltungstransformation auch das gesellschaftliche Vertrauen in die Leistungsfähigkeit öffentlicher Institutionen und damit in den freiheitlichen Verfassungsstaat insgesamt ab[2]. Es ist daher zu begrüßen, dass der Gesetzgeber den relevanten Rechtsrahmen jüngst umfassend reformiert hat (OZG-Änderungsgesetz[3])[4]. So soll es Bürgern (perspekti-

* Dr. Jonas Botta, Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung und Habilitand an der Deutschen Universität für Verwaltungswissenschaften Speyer. Er dankt der VolkswagenStiftung, die das Projekt „AI used by the state: Safeguarding autonomy and human rights with transparency to citizens and support for public servants“ gefördert hat. Die im Beitrag zitierten Internetquellen wurden zuletzt am 10. 6. 2025 aufgerufen.

1 Vgl. *Pilniok*, DÖV 2024, S. 581 (582); *Weeke*, Transparente digitale Verwaltung: Umsetzbarkeit eines KI-Registers in Deutschland, 2023, S. 5.

2 Vgl. *Initiative D21 e. V./Technische Universität München*, eGovernment MONITOR 2023, 2023, S. 15.

3 Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz), BGBl. 2024 I Nr. 245. Weiterführend dazu z. B. *Guckelberger*, DÖV 2024, S. 849 (849 ff.); *Schulz*, NVwZ 2024, S. 1703 (1703 ff.).

4 Bislang schritt die digitale Verwaltungstransformation in Deutschland nur langsam voran, was insbesondere dem föderalen Staatsaufbau geschuldet ist, der Parallelentwicklungen begünstigt und Kooperationen erschwert (*Martini*, DÖV 2017, S. 443 (447); *Schliesky/Hoffmann*, DÖV 2018, S. 193 (194)). Als Befreiungsschlag sollte ursprünglich das 2017 verabschiedete Onlinezugangsgesetz (OZG) dienen, für dessen Beschluss der Bund eine neue Gesetzgebungskompetenz erhalten hatte (Art. 91c Abs. 5 GG). Es verpflichtete beide Staatsebenen dazu, ihre Verwaltungsleistungen bis Ende 2022 auch elektronisch verfügbar zu machen (§ 1 Abs. 1 OZG a. F.). Eine Zielvorgabe, die zwar viele Fortschritte bewirkt hat, aber letztendlich nicht einzuhalten war (*Botta*, NVwZ 2022, S. 1247 (1247); *Schulz*, RDi 2023, S. 518 (518); *Wißmann*, DVBl. 2023, S. 200 (201)). Eine Übersicht über den OZG-Umsetzungsstand bietet das Dashboard Digitale Verwaltung (https://dashboard.digitale-verwaltung.de/). Seine (teilweise irreführende) Darstellungsweise verhindert jedoch eine umfassende Transparenz (kritisch dazu *Botta*, CERIDAP Journal 2022, S. 109 (112 f.); vgl. auch *Bundesrechnungshof*, Ergänzungs-

Duncker & Humblot · Berlin

visch) freistehen, ihre Daten und Nachweise der Verwaltung nur noch einmalig zu übermitteln, wofür der behördenübergreifende Datenaustausch erleichtert wird (Once-Only-Prinzip, § 5 Abs. 1 Nr. 1 E-Government-Gesetz Bund n. F. [5])[6]. Der Bund hat sich außerdem dazu verpflichtet, seine wesentlichen Verwaltungsleistungen vollständig elektronisch abzuwickeln (Ende-zu-Ende-Digitalisierung, § 6 Abs. 1 E-Government-Gesetz Bund n. F.)[7]. Die gesetzliche Digitalisierungspflicht stoppt mithin nicht mehr an der sinnbildlichen Amtspforte (Frontend)[8], sondern erfasst auch die verwaltungsinternen Abläufe (Backend). Zukünftig könnten medienbruchfreie Verfahren zum neuen Standard in der öffentlichen Verwaltung werden. Dafür braucht es indes nicht nur gesetzliche, sondern auch technologische Innovationen.

1. KI als Schlüsseltechnologie

Eine Schlüsselrolle bei der digitalen Verwaltungstransformation dürfte dem Einsatz von KI-Systemen zukommen, da sie insbesondere zur Prozessautomatisierung prädestiniert sind (zum KI-Begriff siehe unten II. 1. a) aa)). Sie sind in der Lage, selbst größte Datenmengen zu analysieren, Muster zu erkennen und Prognosen abzuleiten[9].

a) Chancen der Automatisierung. KI-Systeme können sowohl den Zugang zu Verwaltungsleistungen (z. B. intelligente Chatbots, die bei der Antragssuche und -erstellung behilflich sind) als auch verwaltungsinterne Tätigkeiten (z. B. Programme, die Behördenschreiben erstellen oder übersetzen) optimieren[10]. Dadurch kann es zum einen gelingen, dass Bürger zielgenauer von staatlichen Angeboten profitieren, die sie bislang aufgrund der hohen bürokratischen Hürden zu selten erreicht haben. So ruft bspw. nur eine Minderheit der Leistungsberechtigten die Mittel des Bildungs- und

band zu den Bemerkungen 2021, Bemerkung Nr. 43, Verwaltungsdigitalisierung: BMI beschönigt Fortschritt, 2022, S. 3 ff.).

5 Weiterführend zum Once-Only-Prinzip siehe z. B. *Botta*, DÖV 2023, S. 421 (422); *Martini/Wenzel*, DVBl. 2017, S. 749 (749); *Schulz*, RDi 2023, S. 518 (518). Der § 5 EGovG Bund erfasst die öffentlich-rechtliche Verwaltungstätigkeit der Bundesbehörden und auch der Behörden der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen (vgl. § 1 Abs. 1 und Abs. 2 EGovG Bund). Für die flächendeckende Umsetzung des Once-Only-Prinzips wären daher entsprechende Rechtsgrundlagen im Landesrecht erforderlich (dazu *Botta*, Stellungnahme zum Entwurf eines OZG-Änderungsgesetzes (OZGÄndG), A-Drs. 20(4)303 C, 2023, S. 27).

6 Der behördenübergreifende Datenaustausch setzt die sog. Registermodernisierung voraus. Hinter diesem Begriff verbirgt sich ein Vorhaben, das in seiner Tragweite nicht hinter der OZG-Umsetzung zurücksteht: die Digitalisierung und Vernetzung aller wesentlichen Datenbestände der öffentlichen Verwaltung (dazu *Botta*, DÖV 2023, S. 421 (422); *Ehmann*, ZD 2021, S. 509 (509); *Knauff/Lehmann*, DÖV 2022, S. 159 (159)).

7 Entscheidend für das Transformationspotenzial dieser Regelung ist, welche bzw. wie viele Verwaltungsleistungen als wesentlich gelten (kritisch dazu *Botta* (FN 5), S. 27).

8 *Kemmer/Glauner*, Für eine KI-Offensive in der öffentlichen Verwaltung, FAZ.net vom 23. 1. 2024, https://www.faz.net/pro/digitalwirtschaft/kuenstliche-intelligenz/fuer-eine-ki-offensive-in-der-oeffentlichen-verwaltung-19468627.html.

9 *Botta*, ZfDR 2022, S. 391 (393); *Siegel*, NVwZ 2024, S. 1127 (1127 f.).

10 Weiterführend z. B. *Schneeberger*, Machine Learning in der Verwaltung, 2024, S. 17 ff.

Teilhabepaketes ab, obwohl diese zum menschenwürdigen Existenzminimum von Kindern und Jugendlichen beitragen sollen[11]. Zum anderen kann KI neue Ressourcen in den Behörden freisetzen, die derzeit z. B. bei der persönlichen Beratung von Bürgern und Unternehmen fehlen. Auf diese Weise könnte die Verwaltungsdigitalisierung sogar zu mehr analogen Kontaktmöglichkeiten führen.

b) Risiken der Intransparenz. Bis der Staat durch und durch „intelligent" geworden ist, mögen zwar noch etliche Jahre vergehen, aber schon jetzt finden sich in der Bundesverwaltung über 200 KI-Projekte und Anwendungen[12]. Das verpflichtet den Gesetzgeber dazu, sich besser heute als morgen auch mit den Risiken dieser Technologien auseinanderzusetzen. Denn der Einsatz von KI-Systemen birgt ernstzunehmende Gefahren für die Grundrechte der betroffenen Bürger (und Behördenmitarbeiter), insbesondere Diskriminierung und informationelle Fremdbestimmung. Dies folgt sowohl aus dem Umstand, dass die Systeme nicht frei von den (unbewussten) Vorurteilen ihrer Entwickler (und Anwender) sind, als auch daraus, dass ihre Analyseschritte oftmals nicht ausreichend verständlich bzw. nachvollziehbar sind[13]. Um einen Eindruck davon zu gewinnen, welche Konsequenzen aus diesen Risiken erwachsen können, reicht ein Blick in die Staaten, die schon länger auf eine digitale Verwaltung setzen. So ermittelte bspw. in den Niederlanden ab 2013 ein selbstlernender Algorithmus das Betrugsrisiko von Kindergeldbeziehern. Dies führte zu zehntausenden Rückzahlungsforderungen, die jedoch überwiegend unberechtigt waren. Besonders betroffen waren Familien mit nicht-niederländischer Nationalität, da der Algorithmus diese als Risikofaktor eingestuft hatte[14]. Dieses staatliche *Racial Profiling* kam erst Ende 2019 ans Licht und führte als *Toeslagenaffaire* (Kindergeldaffäre) zum Regierungsrücktritt. Noch weitreichender können die Folgen sein, wenn sich der Einsatz von KI-Systemen nicht nur auf die klassische Leistungsverwaltung begrenzt, sondern auch die Eingriffsverwaltung umfasst[15]. Als besonders grundrechtssensibel gelten z. B. Gesichtserkennungsprogramme zur Überwachung des öffentlichen Raumes bzw. zum Grenzschutz[16] oder Prognosesoftware zur Steuerung polizeilicher Maßnahmen (sog. *Predictive Policing*)[17]. Es ist daher wenig

11 *Deutscher Paritätischer Wohlfahrtsverband*, Empirische Befunde zum Bildungs- und Teilhabepaket: Teilhabequoten im Fokus, 2020, S. 7.

12 Für einen Überblick über den KI-Einsatz im Geschäftsbereich der Bundesregierung siehe BT-Drs. 20/12191, S. 1 ff.

13 *Botta*, ZfDR 2022, S. 391 (394); *Martini*, JZ 2017, S. 1017 (1018 f.); *Schneeberger* (Fn. 10), S. 327 ff.; vgl. *Eichenhofer*, DÖV 2023, S. 93 (96); *Linhart*, Information aus der Blackbox, 2023, S. 55.

14 *Bortnikov/Dukart*, ZD 2024, S. 558 (558 f.).

15 *Krönke*, Die Verwaltung 56 (2023), S. 31 (48); *Siegel*, NVwZ 2024, S. 1127 (1135).

16 Weiterführend zur Gesichtserkennung z. B. *Heldt*, MMR 2019, S. 285 (285 ff.); *Martini*, NVwZ-Extra 1 – 2/2022, S. 1 (2 ff.); *Mysegades*, NVwZ 2020, S. 852 (852 ff.).

17 Weiterführend zum Predictive Policing z. B. *Rademacher*, AöR 142 (2017), S. 366 (366 ff.); *Schneeberger* (Fn. 10), S. 320 ff.; *Singelnstein*, NStZ 2018, S. 1 (1 ff.); *Trute/Kuhlmann*, GSZ 2021, S. 103 (103 ff.).

verwunderlich, dass in der deutschen Bevölkerung noch eine erhebliche Skepsis gegenüber dem staatlichen KI-Einsatz herrscht[18].

Um den aufgezeigten Risiken vorbeugen zu können, dürfte es vor allem darauf ankommen, öffentlich zu machen, ob und wie Behörden KI-Systeme verwenden. Noch fehlt es jedoch oftmals an einem entsprechenden Informationsstand – auch innerhalb der Verwaltung selbst. Fehlende Transparenz wirkt sich indes nicht nur für die Bürger, sondern auch für den Staat nachteilhaft aus. Denn sie erschwert den zwischenbehördlichen Austausch von Entwicklungs- bzw. Nutzungserfahrungen und eine gezielte KI-Strategie für den gesamten Bundesstaat. Angesichts der hohen Summen, die die öffentliche Hand in KI investiert, ein gegenüber den Steuerzahlern nur schwer zu rechtfertigender Zustand. Denn er führt zu ineffizienten Parallelentwicklungen, wie sie schon der fristgerechten OZG-Umsetzung im Wege standen[19].

2. Transparenz als Gelingensbedingung

Damit wird Transparenz zur Gelingensbedingung der digitalen Verwaltungstransformation.

a) Von der Holschuld der Bürger zur Bringschuld des Staates. Transparentes Verwaltungshandeln ist im demokratischen Rechtsstaat nicht nur allgemein von hoher Bedeutung, sondern gewinnt angesichts des beschriebenen „Blackbox"-Phänomens von KI-Systemen eine besondere Signifikanz. KI-Transparenz setzt sowohl eine Kennzeichnungspflicht des KI-Einsatzes als auch eine betroffenenzentrierte Erläuterung der grundsätzlichen Funktionsweise des jeweiligen Systems voraus, die nicht nur seine technischen Grundlagen, sondern auch seinen sozialen Kontext berücksichtigt[20].

Dabei ist zwischen Transparenz i. w. S. und Transparenz i. e. S. zu unterscheiden. Zum einen können Bürger Behörden mittels Informationsfreiheitsanträgen[21] grundsätzlich dazu verpflichten, über die von ihnen verwendeten KI-Systeme zu informieren (Transparenz i. w. S.)[22]. Soweit dem keine öffentlichen oder privaten Belange entgegenstehen (siehe unten III. 2. b)), lässt sich auf diesem Weg zumindest die Offenlegung der wesentlichen Parameter eines Algorithmus durchsetzen[23]. Zum anderen kann der Staat aber auch einen einheitlichen Zugang zu diesen Informationen proaktiv zur Verfügung stellen (Transparenz i. e. S.). Ein derartiger Open-Govern-

18 *Initiative D21 e. V./Technische Universität München* (Fn. 2), S. 20.

19 Vgl. *Botta*, CERIDAP Journal 2022, S. 109 (114 f.).

20 Weiterführend z. B. *Martini*, Blackbox Algorithmus, 2019, S. 177 ff.; *Olsen/Hildebrandt et al.*, Digital Government: Research and Practice 5 (2024), S. 1 (3 ff.); *Wischmeyer*, AöR 143 (2018), S. 1 (42 ff.); vgl. *Braun Binder/Obrecht*, AJP 2024, S. 1069 (1072).

21 Zusätzlich können die Behörden auch datenschutzrechtliche Auskunfts- und Informationspflichten (insbesondere nach Art. 13 ff. DSGVO) treffen, die jedoch ebenfalls nur Individualrechtsschutz bieten.

22 In Bayern und Niedersachsen existiert indes kein Informationsfreiheitsgesetz.

23 *Martini* (Fn. 20), S. 342.

ment-Ansatz[24] verheißt ein höheres Transparenzniveau, da er die informationsfreiheitsrechtliche „Holschuld" der Bürger durch eine „Bringschuld" des Staates ersetzt und dadurch ein niedrigschwelligeres Informationsangebot eröffnet[25]. Dieses Angebot erlaubt nicht nur eine Kontrolle durch Einzelpersonen, sondern vor allem auch durch die (organisierte) Öffentlichkeit[26]. Wie KI-Transparenz i. e. S. konkret erreicht werden kann, ließ sich bislang vor allem im europäischen Ausland studieren.

b) Konzept eines KI-Transparenzregisters. Ende 2022 haben die Niederlande in Reaktion auf die *Toeslagenaffaire* ein zentrales[27] Register eingeführt, in dem öffentliche Stellen die algorithmischen Systeme, die sie einsetzen, vermerken können (*Algoritmeregister*)[28]. Es informiert über den Entwicklungszweck, den Einsatzbereich und die Auswirkungen des jeweiligen Systems auf Bürger und Unternehmen. Dafür können die öffentlichen Stellen zahlreiche Informationen bereitstellen: z. B. eine Abwägung der Vor- und Nachteile des Systems, die Verwendung und Überprüfung seiner Ergebnisse durch Menschen, einen Überblick über das Risikomanagement, die Rechtsgrundlagen des Algorithmus, die durchgeführten Folgenabschätzungen (neben der Datenschutz- auch eine Menschenrechtsfolgenabschätzung), einen Überblick über die Daten, die vom Algorithmus verwendet werden und/oder ursprünglich zur Erstellung des Algorithmus verwendet wurden und eine Erläuterung der Funktionsweise des Algorithmus. Damit liegt dem Register ein menschenzentrierter Transparenzansatz zugrunde, der nicht nur die technischen Grundlagen eines algorithmischen Systems, sondern vor allem auch seine sozialen Auswirkungen in den Fokus nimmt[29]. Bislang ist das Register freiwillig, es soll perspektivisch aber verpflichtend werden[30]. In ihm sind bereits über 900 Algorithmen vermerkt[31].

Griechenland widmet sich ebenfalls verstärkt dem Einsatz algorithmischer Systeme in der öffentlichen Verwaltung. Das Gesetz 4961/2022[32] hat eine algorithmische Folgenabschätzung eingeführt, die sich am US-amerikanischen *Algorithmic Accountability Act of 2022 (H.R. 6580)*[33] und an der kanadischen *Directive on Automated Decision-Making*[34] orientiert[35]. Vor der Inbetriebnahme müssen öffentliche Stellen nun-

---

24 Weiterführend zum Leitbild des Open Government z. B. *Guckelberger*, Öffentliche Verwaltung im Zeitalter der Digitalisierung, 2019, S. 66 ff.

25 Vgl. *Bäumer*, ZGI 2022, S. 270 (270); *Brink*, ZGI 2024, S. 197 (198); *Hill*, DÖV 2014, S. 213 (214).

26 Vgl. *Braun Binder/Obrecht*, AJP 2024, S. 1069 (1073).

27 Zuvor hatte es auf kommunaler Ebene bereits entsprechende Register gegeben. Das weltweit erste KI-Register hatte die Stadt Amsterdam im Jahr 2020 eingerichtet (https://algoritmeregister.amsterdam.nl/en/ai-register/). Siehe dazu z. B. *Weeke* (Fn. 1), S. 11 f.

28 Online abrufbar unter https://algoritmes.overheid.nl/en.

29 Vgl. *Olsen/Hildebrandt et al.*, Digital Government: Research and Practice 5 (2024), S. 1 (5 f.).

30 *Weeke* (Fn. 1), S. 12.

31 *Autoriteit Persoonsgegevens*, AI & Algorithmic Risks Report, 2024, S. 50.

32 GG 146/A/27-07-2022.

33 Online abrufbar unter: https://www.congress.gov/bill/117th-congress/house-bill/6580.

34 Online abrufbar unter: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592.

mehr u. a. prüfen, welche Risiken sich für die Rechte, Freiheiten und rechtmäßigen Interessen betroffener Personen ergeben können und ob der erwartete gesellschaftliche Nutzen des Systems im Verhältnis zu diesen Risiken steht (Art. 5 Gesetz 4961/2022). Die dabei erfassten Informationen hat jede öffentliche Stelle in einem KI-Register zu vermerken, das jedoch nicht dauerhaft allgemein zugänglich ist, sondern nur auf Aufforderung vorzulegen ist (Art. 8 Gesetz 4961/2022).

In der Schweiz existieren hingegen jederzeit einsehbare Transparenzverzeichnisse[36]. Auf Bundesebene führt das Kompetenznetzwerk für künstliche Intelligenz (CNAI) eine Datenbank von KI-relevanten Projekten in der Bundesverwaltung[37]. Auf Kantonsebene ist Appenzell Innerrhoden Vorreiter. Als erster Kanton hat er im Sommer 2024 ein Verzeichnis algorithmischer Systeme eingeführt[38]. Die zur Verfügung gestellten Informationen (zu vier Systemen) sind jedoch sehr überschaubar. Relevanter könnte das geplante Verzeichnis des Kantons Zürich werden. Gegenwärtig hat der dortige Kantonsrat über einen Regierungsvorschlag zu entscheiden, nach dem jedes öffentliche Organ ein allgemein zugängliches Verzeichnis der von ihm verwendeten algorithmischen Entscheidungssysteme, die sich auf die Grundrechte von Personen auswirken können, führen müsste (§ 13 Abs. 3 revidiertes Gesetz über die Information und den Datenschutz)[39]. Der nähere Verzeichnisinhalt soll durch eine Verordnung geregelt werden.

Die Idee eines KI-Transparenzregisters für die öffentliche Verwaltung trägt mithin europaweit Früchte, ohne dass dabei ein einheitliches Konzept verfolgt wird. Seit Anfang 2025 gibt es auch in Deutschland – zumindest dem Namen nach[40] – ein derartiges Register für die Bundesverwaltung[41]. Das Beratungszentrum für Künstliche Intelligenz (BeKI) im Bundesministerium des Innern und für Heimat (BMI) hat es i. R. d. „Marktplatzes der KI-Möglichkeiten" errichtet[42]. Das Register ist bislang freiwillig und seine Informationstiefe ist begrenzt. Zu den 186 verzeichneten KI-Syste-

35 Weiterführend dazu z. B. *Broumas/Charalampous*, JIPITEC 2023, S. 594 (594 ff.); *Chatzipanagioti*, MMR-Aktuell 2024, 01543.

36 Weiterführend dazu z. B. *Braun Binder/Obrecht*, AJP 2024, S. 1069 (1069 f.).

37 Online abrufbar unter: https://cnai.swiss/dienstleistungen/projektdatenbank/.

38 Online abrufbar unter: https://www.ai.ch/themen/staat-und-recht/digitale-verwaltung/verzeichnis-algorithmischer-systeme.

39 *Regierungsrat des Kantons Zürich*, Antrag vom 5. 7. 2023, Vorlage 5923, Gesetz über die Information und den Datenschutz (IDG), online abrufbar unter: https://parlzhcdws.cmicloud.ch/parlzh5/cdws/Files/b5722262463b471a9bb0b9ffac3231cb-332/2/pdf.

40 Zur Kritik am deutschen KI-Transparenzregister *Rudl*, Marktplatz statt Transparenzregister, Netzpolitik.org vom 29. 1. 2025, https://netzpolitik.org/2025/kuenstliche-intelligenz-marktplatz-statt-transparenzregister/.

41 Bislang war es in Deutschland vorrangig parlamentarischen Anfragen zu verdanken, dass eine allgemeinzugängliche Übersicht über den KI-Einsatz in der Bundesverwaltung zumindest in gewissem (thematisch und zeitlich beschränktem) Umfang bestand. Erwähnenswert ist in diesem Zusammenhang das Engagement der ehemaligen linken Bundestagsabgeordneten *Anke Domscheit-Berg*; https://mdb.anke.domscheit-berg.de/bundestag/parlamentarische-initiativen/kleine-anfragen/.

42 Online abrufbar unter: https://maki.beki.bund.de/a/bmi-makimo-app/tabelle. Dazu schon *Bundesministerium des Innern und für Heimat*, KI-Leitbild für das Ressort BMI, 2024, S. 22; *IT-Planungsrat*, Marktplatz der KI-Möglichkeiten, Beschluss 2024 – 01 vom 4. 7. 2024.

men sind nur Kurzbeschreibungen verfügbar, die teilweise inhaltsgleich mit dem jeweiligen Projekttitel sind. Für die verwendeten Risikoklassifizierungen fehlt eine Erläuterung, was die Nachvollziehbarkeit erschwert. Das Register dient damit vor allem dem behördenübergreifenden Informationsaustausch und gewährt den Bürgern gegenwärtig nur einen oberflächlichen Einblick in die staatliche KI-Praxis. Insbesondere fehlt die Landes- und Kommunalebene noch gänzlich[43]. Gleichwohl erfordert diese Entwicklung bereits jetzt eine vertiefte Auseinandersetzung mit den Rechtsfragen, die sich aus der Errichtung eines KI-Transparenzregisters für die öffentliche Verwaltung ergeben. Dies umfasst sowohl die Frage nach seiner allgemeinen Zulässigkeit als auch nach seiner konkreten Ausgestaltung. Dafür müssen die (neuen) Grundlagen der KI-Regulierung im europäischen Mehrebenensystem näher betrachtet werden. Während das Unionsrecht für das „Ob" eines nationalen KI-Transparenzregisters maßgeblich ist (II.), gibt das mitgliedstaatliche Verfassungsrecht das „Wie" vor (III.).

II. Unionsrechtlicher Rahmen eines KI-Transparenzregisters

Im August 2024 ist das weltweit erste umfassende Gesetz zur Regulierung künstlicher Intelligenz in Kraft getreten: die Verordnung über künstliche Intelligenz (KI-VO)[44]. Mit ihr hat der Unionsgesetzgeber das bereits 2020 im KI-Weißbuch niedergelegte Ziel verwirklicht, einen Rechtsrahmen für vertrauenswürdige KI zu schaffen[45]. Die KI-VO soll sowohl der Fortentwicklung des digitalen Binnenmarktes als auch dem Schutz der Grundrechte, Demokratie und Rechtsstaatlichkeit dienen (ErwGr. 1 S. 1 KI-VO). Sie verfolgt einen risikobasierten Regelungsansatz und konzentriert sich vornehmlich auf Hochrisiko-KI-Systeme[46/47]. Gleichzeitig beschränkt sie sich auf keinen speziellen Anwendungssektor, sondern ist ein horizontales Regelungswerk[48].

Für ein nationales KI-Transparenzregister ist die KI-VO in zweifacher Hinsicht von Bedeutung. Zum einen enthält sie zahlreiche Transparenzvorgaben[49] und könnte

43 Der „Marktplatz der KI-Möglichkeiten" soll sich perspektivisch auch für die Landes- und Kommunalverwaltung öffnen (*IT-Planungsrat*, Pilotprojekt KI-Marktplatz, Beschluss 2024/56 vom 13.11.2024). Bereits jetzt existiert bspw. in Nordrhein-Westfalen eine sog. „KI.Landkarte", die Informationen über KI-Anwendungen inner- und außerhalb der Verwaltung bereitstellt (https://www.ki.nrw/ki-landkarte/#/). Diese richtet sich jedoch primär nicht an die betroffenen Personen, sondern an KI-interessierte Unternehmen, Hochschulen und Forschungseinrichtungen.

44 *Martini/Botta*, MMR 2024, S. 630 (630); *Seitz*, EuZW 2024, S. 836 (836 f.). Kritisch zur Einordnung als erstes KI-Gesetz äußert sich hingegen *Vasel*, EuZW 2024, S. 829 (829).

45 Vgl. *Botta*, ZfDR 2022, S. 391 (396); *Seckelmann*, Die Verwaltung 56 (2023), S. 1 (14).

46 Zu deren Definition siehe unten II. 1. b) aa).

47 *Botta*, ZfDR 2022, S. 391 (397); *Seckelmann*, Die Verwaltung 56 (2023), S. 1 (2). Weiterführend zum risikobasierten Ansatz siehe z. B. *Martini*, § 4. Hochrisiko-KI-Systeme: Risikobasierter Ansatz, in: Hilgendorf/Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, 2023, S. 51 (51 ff.).

48 *Martini/Botta*, MMR 2024, S. 630 (630); *Ruschemeier*, ZG 2023, S. 337 (344).

49 Vgl. weiterführend *Linhart* (Fn. 13), S. 67 ff.

daher einen zusätzlichen mitgliedstaatlichen Transparenzmechanismus entbehrlich machen (1.). Zum anderen könnte sie aufgrund ihres Anwendungsvorrangs[50] den Regelungsspielraum des mitgliedstaatlichen Gesetzgebers derart einschränken, dass ein nationales Register unionswidrig wäre (2.).

1. Vorgaben der KI-VO

Transparenz i. S. d. KI-VO erfordert, dass KI-Systeme so entwickelt und verwendet werden, dass sie angemessen nachvollziehbar und erklärbar sind, wobei den Menschen bewusst gemacht werden muss, dass sie mit einem KI-System kommunizieren oder interagieren, und dass die betroffenen Personen ordnungsgemäß über die Fähigkeiten und Grenzen des KI-Systems informiert und über ihre Rechte in Kenntnis gesetzt werden (ErwGr. 27 S. 8 KI-VO). Bevor sich die konkreten Transparenzvorgaben der KI-VO näher untersuchen lassen, ist zunächst klärungsbedürftig, inwieweit der Einsatz von KI-Systemen in der öffentlichen Verwaltung überhaupt ihrem Anwendungsbereich unterfällt.

a) Anwendungsbereich (Art. 2 und Art. 3 KI-VO). Die Vorschriften der KI-VO zielen überwiegend auf die Anbieter von KI-Systemen bzw. KI-Modellen[51] (Art. 2 Abs. 1 lit. a KI-VO) sowie auf deren Betreiber (Art. 2 Abs. 1 lit. b KI-VO)[52]. Diese Begriffe hat der Unionsgesetzgeber in Art. 3 KI-VO definiert.

aa) KI-Systeme (Art. 3 Nr. 1 KI-VO). Mangels eines einheitlichen KI-Verständnisses bietet bereits die Definition von KI-Systemen in Art. 3 Nr. 1 KI-VO juristischen Zündstoff[53]. Die Verordnung soll einerseits keine herkömmlichen Softwaresysteme und Programmierungsansätze erfassen (ErwGr. 12 S. 2 KI-VO) und andererseits nicht nur für Hochrisiko-KI-Systeme gelten. Konkret nennt Art. 3 Nr. 1 KI-VO drei Voraussetzungen für ein KI-System[54]. Erstens muss es sich um ein maschinen-

50 Vgl. EuGH, NJW 1964, S. 2371 (2372); NJW 1978, S. 1741 (1741 f.).

51 Neben dem Begriff des KI-Systems kennt die KI-VO auch das KI-Modell mit allgemeinem Verwendungszweck. Dabei handelt es sich um ein KI-Modell – einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden (Art. 3 Nr. 63 KI-VO). Weiterführend dazu z. B. *Wendehorst*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 3 Rn. 395 ff.

52 Zusätzlich ist ein Unionsbezug erforderlich, der bei deutschen Behörden gegeben ist.

53 Der ursprüngliche Kommissionsentwurf war dafür kritisiert worden, dass er letztendlich für fast alle Softwaresysteme gegolten hätte (*Bomhard/Merkle*, RDi 2021, S. 276 (277); *Botta*, ZfDR 2022, S. 391 (397); *Engelmann/Brunotte/Lütkens*, RDi 2021, S. 317 (318)). Für die finale Begriffsklärung hat sich der Verordnungsgeber an der KI-Definition der OECD orientiert (vgl. *OECD*, Explanatory memorandum on the updated OECD definition of an AI system, OECD Artificial Intelligence Papers, No. 8, 2024, https://doi.org/10.1787/623da898-en).

54 Die EU-Kommission hat die KI-Definition (unverbindlich) in sieben verschiedene Bestandteile unterteilt. Siehe *Europäische Kommission*, Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), 5. 2. 2025, S. 2.

gestütztes System handeln, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist. Das bedeutet, dass das System zu einem gewissen Grad unabhängig von menschlichem Zutun agiert und in der Lage ist, ohne menschliches Eingreifen zu arbeiten (ErwGr. 12 S. 11 KI-VO). Diesem Erfordernis dürfte in der öffentlichen Verwaltung kein hohes Abgrenzungspotenzial zukommen[55]. Denn jedes algorithmische System kann gewisse Abläufe autonom ausführen[56]. Zweitens kann ein KI-System i. S. d. Art. 3 Nr. 1 KI-VO nach seiner Betriebsaufnahme anpassungsfähig sein. Diese Voraussetzung dürfte die meisten Fragen in der Rechtsanwendung aufrufen. Entscheidend ist die Auslegung von „kann […] anpassungsfähig sein". Während die deutsche Sprachfassung darauf hindeutet, dass es sich um eine obligatorische Vorgabe handelt, legt bspw. die englische Sprachfassung („*that may exhibit adaptiveness after deployment*") eine lediglich fakultative Vorgabe nahe[57]. Wäre die Lernfähigkeit entscheidend für die Eröffnung des Anwendungsbereichs der KI-VO, dürften (nicht nur) in der öffentlichen Verwaltung zahlreiche Systeme nicht ihrem Regelungsregime unterfallen[58]. Dafür spricht, dass eine bloß fakultative Verankerung letztendlich überflüssiger Normtext wäre[59]. Dagegen lässt sich indes zusätzlich zum Wortlaut des ErwGr. 12 S. 12 KI-VO („Anpassungsfähigkeit, die ein KI-System nach Inbetriebnahme aufweisen könnte") überzeugend anführen, dass Art. 15 Abs. 4 UAbs. 3 und Art. 43 Abs. 4 UAbs. 2 KI-VO spezielle Regelungen für Hochrisiko-KI-Systeme treffen, „die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen"[60]. Im Umkehrschluss daraus gilt die KI-VO auch für KI-Systeme, die das nicht tun[61]. Drittens muss ein KI-System aus den erhaltenen Eingaben Ableitungen vornehmen können. Diese Fähigkeit bezieht sich auf den Prozess der Erzeugung von Ausgaben, wie Vorhersagen, Inhalten, Empfehlungen oder Entscheidungen, die physische und virtuelle Umgebungen beeinflussen können (ErwGr. 12 S. 4 KI-VO). Auch dieses Kriterium ist somit relativ offen formuliert und erfasst letztendlich alle algorithmischen Systeme, die Ausgaben erzeugen[62]. Damit dürften alle Systeme in der öffentlichen Verwaltung, die schon bislang als KI galten, auch als KI i. S. v. Art. 3 Nr. 1 KI-VO gelten.

bb) Anbieter (Art. 3 Nr. 3 KI-VO). Anbieter sind alle Stellen, die ein KI-System (oder ein KI-Modell mit allgemeinem Verwendungszweck) entwickeln (oder entwickeln lassen) und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen, sei es entgeltlich oder unentgeltlich (Art. 3 Nr. 3 KI-VO)[63]. Dazu können ausdrücklich auch Behörden zählen. Damit folgt die KI-VO dem

55 Wohl a. A.: *Pilniok*, DÖV 2024, S. 581 (585).

56 *Wendehorst* (Fn. 51), Art. 3 Rn. 29; vgl. *Europäische Kommission* (Fn. 54), S. 3.

57 *Pilniok*, DÖV 2024, S. 581 (585); *Wendehorst* (Fn. 51), Art. 3 Rn. 32.

58 *Guckelberger*, DÖV 2025, S. 45 (47); *Pilniok*, DÖV 2024, S. 581 (585); vgl. *Wendehorst* (Fn. 51), Art. 3 Rn. 33.

59 *Wendehorst* (Fn. 51), Art. 3 Rn. 33.

60 Vgl. *Wendehorst* (Fn. 51), Art. 3 Rn. 3.

61 Ebenso *Guckelberger*, DÖV 2025, S. 45 (46); *Europäische Kommission* (Fn. 54), S. 4.

62 Vgl. *Wendehorst* (Fn. 51), Art. 3 Rn. 50; a. A.: *Steen*, KiR 2024, S. 7 (9 f.).

63 Die Vorgaben der KI-VO greifen erst mit dem Inverkehrbringen bzw. der Inbetriebnahme eines KI-Systems. Dies folgt sowohl aus Art. 2 Abs. 1 KI-VO als auch klarstellend aus Art. 2

für die gesamte unionale Digitalgesetzgebung kennzeichnenden Regelungsansatz, grundsätzlich nicht zwischen dem privaten und dem öffentlichen Sektor zu unterscheiden[64].

Deutsche Behörden dürften sich gleichwohl nur dann als Anbieter qualifizieren, wenn sie ein KI-System entwickeln (lassen) und dieses selbst verwenden oder direkt einer anderen (öffentlichen) Stelle zum Erstgebrauch bereitstellen (vgl. Art. 3 Nr. 11 KI-VO)[65]. Denn die Tatbestandsalternative des Inverkehrbringens setzt die erstmalige Bereitstellung eines KI-Systems auf dem Unionsmarkt i. R. e. Geschäftstätigkeit (Art. 3 Nr. 9 und Nr. 10 KI-VO) voraus. Selbst wenn öffentliche Stellen KI-Systeme entwickeln (lassen), dürfte es aktuell sehr unwahrscheinlich sein, dass sie diese anschließend dem freien Markt zur Verfügung stellen.

cc) Betreiber (Art. 3 Nr. 4 KI-VO). Auch wenn öffentliche Stellen zumeist (noch) keine Anbieter sind[66], sind sie nicht vom Regelungsregime der KI-VO entbunden. Denn sie lassen sich problemlos unter den Betreiberbegriff subsumieren. Betreiber sind Stellen, die ein KI-System in eigener Verantwortung verwenden (Art. 3 Nr. 4 KI-VO), m. a. W.: die ein KI-System auf eigene Rechnung und auf eigenes Risiko einsetzen[67]. Dies setzt voraus, dass alle wesentlichen Schritte von der Dateneingabe in das KI-System bis hin zur Ausgabe der erzeugten Daten im Herrschaftsbereich der jeweiligen öffentlichen Stelle erfolgen. Auch bei Software-as-a-Service-Lösungen lässt sich dieses Erfordernis bejahen, solange die öffentliche Stelle über das „Ob" und „Wie" des KI-Einsatzes entscheidet[68].

dd) Ausnahmen. Der grundsätzlich weite Anwendungsbereich des Art. 2 Abs. 1 KI-VO erfährt Einschränkungen, von denen insbesondere zwei für den KI-Einsatz in der öffentlichen Verwaltung relevant sind.

(1) Nationale Sicherheit (Art. 2 Abs. 3 KI-VO). Die KI-VO gilt nur in den Bereichen, die dem Unionsrecht unterfallen (Art. 2 Abs. 3 UAbs. 1 Hs. 1 KI-VO). Dies ergibt sich freilich nicht erst aus dem Sekundärrecht, sondern folgt schon aus dem Primärrecht, vornehmlich Art. 4 Abs. 2 EUV[69]. Danach hat die Union die grundlegenden Funktionen des Staates, insbesondere die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit zu achten (Art. 4 Abs. 2 S. 2 KI-VO). Für die nationale Sicherheit

Abs. 8 KI-VO (*Wendehorst*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 2 Rn. 90). Während Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen müssen öffentliche Stellen die Einhaltung der KI-VO nur insoweit beachten, als dass aus diesen Tätigkeiten keine rechtswidrigen Systeme resultieren.

64 Vgl. *Botta*, Datenschutz bei E-Learning-Plattformen, 2020, S. 81.

65 Zusätzlich können öffentliche Stellen auch nach Art. 25 KI-VO als Anbieter gelten, wenn sie z. B. die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System i. S. v. Art. 6 KI-VO wird.

66 Vgl. *Hornung*, AöR 147 (2022), S. 1 (62 f.); *Pilniok*, DÖV 2024, S. 581 (584).

67 *Wendehorst* (Fn. 51), Art. 3 Rn. 83 f.

68 Vgl. *Wendehorst* (Fn. 51), Art. 3 Rn. 88 f.

69 *Calliess*, in: Calliess/Ruffert (Hrsg.), 6. Aufl. 2022, Art. 4 EUV Rn. 8.

besteht sogar ein ausdrücklicher Kompetenzvorbehalt (Art. 4 Abs. 2 S. 3 KI-VO)[70]. Dementsprechend hat der unionale Verordnungsgeber festgehalten, dass die KI-VO keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die nationale Sicherheit berührt (Art. 2 Abs. 3 UAbs. 1 Hs. 2 KI-VO).

Damit eng verknüpft sind die Regelungen der Art. 2 Abs. 3 UAbs. 2 und UAbs. 3 KI-VO. So gilt die Verordnung nicht für KI-Systeme, wenn und soweit sie ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit in Verkehr gebracht, in Betrieb genommen oder, mit oder ohne Änderungen, verwendet werden (Art. 2 Abs. 3 UAbs. 2 KI-VO). Sie findet auch dann keine Anwendung, wenn die KI-Systeme zwar nicht in der Union in Verkehr gebracht oder in Betrieb genommen werden, aber ihr Output in der Union ausschließlich für die zuvor genannten Zwecke verwendet wird (Art. 2 Abs. 3 UAbs. 3 KI-VO), was der Zusammenarbeit mit Drittstaaten dient. Es hängt somit von der Reichweite dieser Zwecke ab, inwieweit so grundrechtssensible Bereiche der öffentlichen Verwaltung wie die Bundeswehr, die Polizei und die Nachrichtendienste des Bundes und der Länder überhaupt der KI-VO unterfallen[71].

Historisch betrachtet sind die innere und die äußere Sicherheit ureigene Domänen des Nationalstaates, in einer globalisierten Welt lässt sich die mitgliedstaatliche Sicherheit indes nicht mehr ohne eine unionale Dimension denken. Dies gilt vor allem angesichts fehlender Binnengrenzen[72]. Diese Erkenntnis hat auch in das Primärrecht Einzug gehalten. So heißt es in Art. 67 Abs. 1 AEUV, dass die EU einen Raum der Freiheit, der Sicherheit und des Rechts bildet, in dem die Grundrechte und die verschiedenen Rechtsordnungen und -traditionen der Mitgliedstaaten geachtet werden. Dies legt nahe, den Begriff der nationalen Sicherheit nicht mit dem gesamten Politikfeld der Sicherheit gleichzusetzen.

Auch der EuGH legt den Begriff der nationalen Sicherheit eng aus, wie sich aus seiner Rechtsprechung auf dem Gebiet des Datenschutzrechts ergibt[73]. Danach dient die nationale Sicherheit dem Schutz der wesentlichen Funktionen des Staates und der grundlegenden Interessen der Gesellschaft und umfasst daher die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten[74]. Insoweit grenzt der EuGH die nationale Sicherheit von der öffentlichen Sicherheit ab, zu deren Zielen er insbesondere die Bekämpfung (schwerer) Kriminalität zählt[75]. Der Begriff der nationalen Sicherheit beschränkt sich folg-

70 *Karpenstein/Sangi*, GSZ 2020, S. 162 (163 f.).

71 Vgl. *Pilniok*, DÖV 2024, S. 581 (584).

72 *Calliess* (Fn. 69), Art. 4 EUV Rn. 47; vgl. auch *Peuker*, EuR 2023, S. 535 (536 f.).

73 Grundlegend EuGH, ZGI 2021, S. 16 (17); bestätigt etwa durch EuGH, BeckRS 2022, S. 34896 Rn. 79; ZD 2023, S. 610 (611); NJW 2023, S. 1639 (1640); EuZW 2024, S. 214 (215). Dazu *Peuker*, EuR 2023, S. 535 (548 f.); *Pfeffer*, NVwZ 2023, S. 1286 (1288); *Pilniok*, DÖV 2024, S. 581 (584); *Wendehorst* (Fn. 63), Art. 2 Rn. 61.

74 EuGH, EuZW 2021, S. 209 (215).

75 EuGH, EuZW 2021, S. 209 (215); *Peuker*, EuR 2023, S. 535 (549).

lich auf die Sicherheit bzw. den Bestand des Staates[76]. Daher findet die KI-VO im Regelfall zwar keine Anwendung auf die nachrichtendienstliche Tätigkeit[77], sehr wohl aber auf die Gefahrenabwehr und Strafverfolgung (vgl. Art. 3 Nr. 46 KI-VO). In der Folge richtet sich der KI-Einsatz nicht nur in der Leistungs-, sondern auch in der Eingriffsverwaltung überwiegend nach den unionalen Vorgaben.

Inwieweit in Art. 2 Abs. 3 KI-VO den „militärischen Zwecken" und den „Verteidigungszwecken" neben den „Zwecken der nationalen Sicherheit" eine eigenständige Bedeutung für den KI-Einsatz in der öffentlichen Verwaltung zukommt, ist fraglich. Einerseits legt die Entstehungsgeschichte des Art. 4 Abs. 2 EUV nahe, dass der Begriff der nationalen Sicherheit auch die Landesverteidigung und die Organisation der Streitkräfte umfasst[78]. Andererseits unterscheidet Art. 4 Abs. 2 S. 2 EUV zwischen der Wahrung der territorialen Unversehrtheit und der nationalen Sicherheit, was dafür sprechen könnte, beide Begriffe in Abgrenzung zueinander als äußere und innere Sicherheit zu verstehen. Auch der EuGH scheint derart zwischen den beiden Termini zu differenzieren, legt beide jedoch gleich eng aus[79]. Daher scheidet jedenfalls nicht schon jedes KI-System aus dem Anwendungsbereich der KI-VO aus, das z. B. im Bundesministerium der Verteidigung oder in der Bundeswehr zum Einsatz kommt (z. B. bei der Personalauswahl)[80]. Es ist vielmehr stets im konkreten Einzelfall zu prüfen, ob der Einsatzzweck unmittelbar dem Schutz der äußeren oder inneren Sicherheit des Staates verpflichtet ist und ob nicht nur ein Zweckbündel vorliegt (vgl. ErwGr. 24 S. 6 KI-VO).

(2) Wissenschaft (Art. 2 Abs. 6 KI-VO). Eine Ausnahme vom Anwendungsbereich der KI-VO gilt auch für die Wissenschaft[81]. KI-Systeme oder KI-Modelle, einschließlich ihrer Ausgabe, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, unterliegen der Verordnung nicht (Art. 2 Abs. 6 KI-VO). Von diesem Privileg können in Deutschland die zahlreichen staatlichen Hochschulen und Forschungseinrichtungen profitieren[82]. Wie weit die Ausnahme konkret reicht, hängt vom Begriff der wissenschaftlichen Forschung und Entwicklung ab. Da sich in der KI-VO keine gesonderte Definition findet, ist auf das allgemeine Begriffsverständnis von Wissenschaft abzustellen. Danach bezieht sich Wissenschaft auf jede Tätigkeit, die darauf abzielt, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen[83]. Nicht entscheidend ist, dass dieses Erkenntnisinteresse auf KI gerichtet ist.

---

76 EuGH, CR 2008, 381 (382); *Botta*, CR 2020, S. 82 (85); *Pilniok*, DÖV 2024, S. 581 (584).

77 *Wendehorst* (Fn. 63), Art. 2 Rn. 63.

78 *Karpenstein/Sangi*, GSZ 2020, S. 162 (165); vgl. auch *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 254 im Kontext von Art. 2 Abs. 3 lit. a JI-RL.

79 Vgl. EuGH, BeckRS 2021, S. 18433 Rn. 40.

80 *Pilniok*, DÖV 2024, S. 581 (587); vgl. auch EuGH, BeckRS 2021, S. 18433 Rn. 40.

81 Diese fand sich im ursprünglichen Kommissionsentwurf noch nicht, was z. B. *Becker*, ZfDR 2023, S. 164 (180) kritisiert hatte.

82 Das Wissenschaftsprivileg gilt darüber hinaus auch für die private Forschung. Siehe *Becker*, ZfDR 2023, S. 164 (167); vgl. *Botta* (Fn. 64), S. 305.

83 *Botta* (Fn. 64), S. 305; *Jarass*, in: ders. (Hrsg.), 4. Aufl. 2021, Art. 13 Rn. 8.

Vielmehr darf KI ein bloßes Mittel zum Zweck sein[84]. Die Ausnahmeregelung dürfte jedoch dort an ihre Grenzen kommen, wo sich die wissenschaftliche Tätigkeit nachteilhaft auf unbeteiligte Dritte auswirkt[85]. Daher ist es bspw. der Polizei versagt, KI-Systeme unter dem Deckmantel der wissenschaftlichen Forschung in der Praxis zu erproben, ohne dabei die KI-VO zu beachten (sofern nicht Art. 2 Abs. 3 KI-VO greift).

ee) Zwischenfazit. Im Ergebnis zeigt sich, dass der KI-Einsatz in der öffentlichen Verwaltung – mit eng umgrenzten Ausnahmen zum Schutz der nationalen Sicherheit und der Wissenschaftsfreiheit – dem Anwendungsbereich der KI-VO unterliegt. Schlüsselnormen für die Unionskonformität eines nationalen KI-Transparenzregisters bzw. für das Bedürfnis nach einem derartigen Instrument sind daher Art. 71 und Art. 27 KI-VO. Mit den beiden Normen hat der Unionsgesetzgeber erkennbar an die mitgliedstaatlichen Strategien zur Steigerung der KI-Transparenz angeknüpft.

b) EU-Datenbank für Hochrisiko-KI-Systeme (Art. 71 KI-VO). Um den Vollzug der KI-VO zu erleichtern und die Transparenz gegenüber der Öffentlichkeit zu erhöhen, muss die EU-Kommission bis zum 2. 8. 2026 eine Datenbank für Hochrisiko-KI-Systeme einrichten (Art. 71 Abs. 1, ErwGr. 131 S. 1 KI-VO). Diese Datenbank soll sowohl den Aufsichtsbehörden als auch der Zivilgesellschaft Klarheit über die Verfügbarkeit, den Einsatz und die grundlegenden Funktionsweisen der Hochrisiko-KI-Systeme auf dem Unionsmarkt verschaffen[86]. Dafür etablieren Art. 49 und Art. 60 KI-VO Registrierungspflichten für die Anbieter und Betreiber von KI-Systemen.

Die daraus resultierende Produktdatenbank fungiert als unionsweiter Transparenzmechanismus. Die abgespeicherten Informationen[87] müssen grundsätzlich auf benutzerfreundliche Weise zugänglich und öffentlich verfügbar sein (Art. 71 Abs. 4 S. 1 KI-VO). Die Datenbank beinhaltet jedoch auch einen nicht öffentlichen Teil mit beschränkten Zugangsrechten. In letzteren sind alle Hochrisiko-KI-Systeme einzutragen, die in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle zum Einsatz kommen sollen (Art. 49 Abs. 4 UAbs. 1 KI-VO). Auf diesen Datenbankbestand haben nur die EU-Kommission und die in Art. 74 Abs. 8 KI-VO genannten nationalen Behörden – insbesondere die Datenschutzbehörden[88] – Zugriff

84 *Wendehorst* (Fn. 63), Art. 2 Rn. 74.

85 *Wendehorst* (Fn. 63), Art. 2 Rn. 85.

86 *Kolain*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 71 Rn. 1.

87 Da in die Datenbank personenbezogene Daten (zu diesen Informationen gehören die Namen und Kontaktdaten der natürlichen Personen, die für die Registrierung des Systems verantwortlich sind und die rechtlich befugt sind, den Anbieter oder ggf. den Betreiber zu vertreten; Art. 71 Abs. 5 S. 2 KI-VO) einfließen sollen, hat der Verordnungsgeber mit Art. 71 Abs. 5 KI-VO eine Verarbeitungsgrundlage i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO geschaffen (*Kolain* (Fn. 86), Art. 71 Rn. 39). Die EU-Kommission gilt zudem nicht nur als datenschutzrechtlich verantwortliche Stelle für die Datenbank (Art. 4 Nr. 7 DSGVO, Art. 71 Abs. 6 S. 1 KI-VO; siehe dazu *Kolain* (Fn. 86), Art. 71 Rn. 40), sondern muss den Anbietern und Betreibern auch angemessene technische und administrative Unterstützung bereitstellen (Art. 71 Abs. 6 S. 2 KI-VO). Des Weiteren muss sie sicherstellen, dass die Datenbank den geltenden Barrierefreiheitsanforderungen entspricht (Art. 71 Abs. 6 S. 3 KI-VO).

88 *Hartmann*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 74 Rn. 15.

(Art. 49 Abs. 4 UAbs. 2 KI-VO). In der gesamten Datenbank sollen die Informationen leicht handhabbar und maschinenlesbar sein (Art. 71 Abs. 4 S. 2 KI-VO).

aa) Erfasste KI-Systeme (Art. 71 Abs. 1 S. 1 KI-VO). Die Datenbank wird nicht alle KI-Systeme auf dem Unionsmarkt beinhalten[89]. Sie wird noch nicht einmal alle Hochrisiko-KI-Systeme erfassen. Vielmehr liegt Art. 71 Abs. 1 S. 1 KI-VO die der ganzen Verordnung inhärente Unterscheidung zwischen zwei verschiedenen Kategorien von Hochrisiko-KI-Systemen zugrunde. Die erste Kategorie umfasst KI-Systeme, die bereits in den Anwendungsbereich anderer Harmonisierungsrechtsvorschriften (z. B. der Medizinprodukteverordnung (EU) 2017/745) fallen (Art. 6 Abs. 1 KI-VO). Sie müssen nicht in die Datenbank eingetragen werden (ErwGr. 131 S. 1 KI-VO)[90]. Zur zweiten Kategorie gehören alle übrigen KI-Systeme, die in einem der acht Bereiche zum Einsatz kommen sollen, die in Annex III KI-VO abschließend aufgeführt sind (Art. 6 Abs. 2 KI-VO)[91]. Sie sind in die Datenbank einzutragen (Art. 71 Abs. 1 S. 1 KI-VO). Die acht Einsatzbereiche des Annex III KI-VO sind für die öffentliche Verwaltung allesamt von erheblicher Bedeutung[92]: Biometrie (Nr. 1), Kritische Infrastruktur (Nr. 2), allgemeine und berufliche Bildung (Nr. 3), Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit (Nr. 4), Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen (Nr. 5), Strafverfolgung (Nr. 6), Migration, Asyl und Grenzkontrolle (Nr. 7) sowie Rechtspflege und demokratische Prozesse (Nr. 8). Gleichzeitig gilt, dass nicht die gesamte öffentliche Verwaltung ein Hochrisiko-Bereich ist[93]. Insbesondere bezieht sich Annex III Nr. 5 KI-VO nur auf grundlegende staatliche Unterstützungsleistungen und -dienste (insbesondere Gesundheitsdienste und soziale Dienste, die Schutz bei Arbeitsplatzverlust, Arbeitsunfällen, Krankheit, Mutterschaft oder Pflegebedürftigkeit etc. bieten) und nicht auf alle Verwaltungsleistungen (vgl. ErwGr. 58 S. 1 KI-VO). Außerdem war der Parlamentsvorschlag erfolglos, Annex III Nr. 8 KI-VO dahingehend zu ergänzen, dass er auch solche KI-Systeme erfasst, die bestimmungsgemäß von Verwaltungsbehörden bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften sowie bei der Anwendung des Rechts auf konkrete Sachverhalte verwendet werden.

bb) Informationspflichten des Anbieters (Art. 71 Abs. 2 KI-VO). Welche Informationen der Anbieter vor dem Inverkehrbringen oder der Inbetriebnahme eines Hochrisiko-KI-Systems i. S. d. Art. 6 Abs. 2 i. V. m. Annex III KI-VO in die Datenbank gemäß Art. 71 Abs. 2 KI-VO eintragen muss, richtet sich danach, ob er der allgemeinen Registrierungspflicht nach Art. 49 Abs. 1 KI-VO oder der speziellen nach

89 *Kolain* (Fn. 86), Art. 71 Rn. 16.

90 Für die KI-Transparenz in der öffentlichen Verwaltung ist dies weitgehend unbeachtlich, da dort nur selten Hochrisiko-KI-Systeme i. S. d. Art. 6 Abs. 1 KI-VO zum Einsatz kommen dürften. Siehe *Schneeberger* (Fn. 10), S. 420 f.

91 Zum Ausnahmetatbestand des Art. 6 Abs. 3 KI-VIO weiterführend *Guckelberger*, DÖV 2025, S. 45 (48 f.); *Ruschemeier*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 6 Rn. 90 ff.

92 *Schneeberger* (Fn. 10), S. 421 f.

93 Ebenso *Guckelberger*, DÖV 2025, S. 45 (47).

Art. 49 Abs. 2 KI-VO unterliegt[94]. Dafür ist maßgeblich, ob er der Auffassung ist, dass das grundsätzlich von Art. 6 Abs. 2 i. V. m. Annex III KI-VO erfasste System hochriskant ist oder nicht. Stellt er das hohe Risiko des KI-Systems nicht in Frage, muss er die Informationen aus Abschnitt A des Anhang VIII KI-VO bereitstellen und auf dem neusten Stand halten[95]. Hält er das KI-System hingegen nicht für hochriskant, muss er den – im Vergleich beschränkteren – Informations- bzw. Aktualisierungspflichten aus Abschnitt B des Anhang VIII KI-VO nachkommen. Dafür muss er insbesondere darlegen, warum er das KI-System nicht als Hochrisiko-KI-System einstuft[96].

cc) Informationspflichten des Betreibers (Art. 71 Abs. 3 KI-VO). Auch wenn öffentliche Stellen keine Anbieter sind[97], kann sie gleichwohl eine Registrierungs- bzw. Informationspflicht treffen. Denn Betreiber, bei denen es sich um Behörden oder sonstige öffentliche Stellen handelt, müssen sich vor der Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems i. S. d. Art. 6 Abs. 2 i. V. m. Annex III KI-VO in der Datenbank registrieren (Art. 49 Abs. 3 KI-VO). Entgegen dem missverständlichen deutschen Wortlaut des Art. 49 Abs. 3 KI-VO („Betreiber, bei denen es sich um Behörden oder Organe, Einrichtungen oder sonstige Stellen der Union oder in ihrem Namen handelnde Personen handelt") bezieht sich diese Regelung nicht nur auf öffentliche Stellen der EU, sondern auch der Mitgliedstaaten (vgl. die englische Sprachfassung: „deployers that are public authorities, Union institutions,

94 Art. 60 Abs. 4 lit. c KI-VO begründet zudem für in Annex III KI-VO gelistete Hochrisiko-KI-Systeme eine spezielle Registrierungspflicht, wenn ihre Anbieter sie unter Realbedingungen außerhalb von KI-Reallaboren testen wollen (siehe dazu *Botta*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 60 Rn. 24 ff.). Auf die Informationen, die Anbieter für Tests unter Realbedingungen nach Art. 60 KI-VO in die Datenbank eintragen, können nur die Marktüberwachungsbehörden und die EU-Kommission zugreifen, es sei denn, der (zukünftige) Anbieter hat seine Zustimmung dafür erteilt, dass diese Informationen öffentlich zugänglich sind (Art. 71 Abs. 4 S. 3 KI-VO).

95 Der Name, die Anschrift und die Kontaktdaten des Anbieters (1.), bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: der Name, die Anschrift und die Kontaktdaten dieser Person (2.), ggf. der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten (3.), der Handelsnamen des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen (4.), eine Beschreibung der Zweckbestimmung des KI-Systems und der durch dieses KI-System unterstützten Komponenten und Funktionen (5.), eine grundlegende und knappe Beschreibung der vom System verwendeten Informationen (Daten, Eingaben) und seiner Betriebslogik (6.), der Status (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen) des KI-Systems (7.), die Art, die Nummer und das Ablaufdatum der von der notifizierten Stelle ausgestellten Bescheinigung und ggf. Name oder Identifizierungsnummer dieser notifizierten Stelle (8.), ggf. eine gescannte Kopie der in Nr. 8 genannten Bescheinigung (9.), alle Mitgliedstaaten, in denen das KI-System in Verkehr gebracht, in Betrieb genommen oder in der Union bereitgestellt wurde (10.), eine Kopie der in Art. 47 KI-VO genannten EU-Konformitätserklärung (11.), elektronische Betriebsanleitungen; dies gilt nicht für Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung oder Migration, Asyl und Grenzkontrolle gemäß Anhang III Nr. 1, 6 und 7 KI-VO (12.) und fakultativ eine URL-Adresse für zusätzliche Informationen (13.).

96 *Kolain* (Fn. 86), Art. 71 Rn. 27.

97 Siehe oben II. 1. a) bb).

bodies, offices or agencies or persons acting on their behalf")[98]. Eine Ausnahme von der Registrierungspflicht gilt für den Bereich der Kritischen Infrastrukturen. Derartige Hochrisiko-KI-Systeme sind auf nationaler Ebene zu registrieren (Art. 49 Abs. 5 KI-VO).

Die Informationspflichten öffentlicher Betreiber ergeben sich aus Abschnitt C des Anhang VIII KI-VO (Art. 71 Abs. 3 KI-VO). Zwar bezieht sich dieser Abschnitt unmittelbar nur auf Eintragungen in den öffentlichen Teil der Datenbank (Art. 49 Abs. 3 KI-VO). Aber Art. 71 Abs. 3 verweist auch für den nicht öffentlichen Teil nach Art. 49 Abs. 4 KI-VO auf Abschnitt C. Erforderliche (und zu aktualisierende) Informationen sind der Name, die Anschrift und die Kontaktdaten des Betreibers (1.), der Name, die Anschrift und die Kontaktdaten der Person, die im Namen des Betreibers Informationen übermittelt (2.), die URL des Eintrags des KI-Systems in der EU-Datenbank durch seinen Anbieter (3.), eine Zusammenfassung der Ergebnisse der gemäß Art. 27 KI-VO durchgeführten Grundrechte-Folgenabschätzung (4.) und ggf. eine Zusammenfassung der im Einklang mit Art. 35 DSGVO oder Art. 27 JI-RL Richtlinie (EU) 2016/680 gemäß Art. 26 Abs. 8 KI-VO durchgeführten Datenschutz-Folgenabschätzung (5.). Zentrale Informationsgehalte sind demnach die Zusammenfassungen der Folgenabschätzungen.

c) Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme (Art. 27 KI-VO). Die Idee einer Grundrechte-Folgenabschätzung (GRFA) für KI-Systeme geht im Unionsrecht maßgeblich auf die Hochrangige Expertengruppe KI zurück, die die EU-Kommission im Jahr 2018 eingesetzt hatte[99]. Folgenabschätzungen sind gleichwohl keine neue Erfindung, sondern seit Jahrzehnten geübte Praxis im Umweltrecht[100]. Auch im Bereich des Menschenrechtsschutzes finden Folgenabschätzungen bereits länger Anwendung[101]. So ist das „Human Rights Impact Assessment" fester Bestandteil der UN-Leitprinzipien für Wirtschaft und Menschenrechte[102].

Das Instrument der GRFA verfolgt zwei Ziele: Zum einen zwingt es vor dem Einsatz eines Hochrisiko-KI-Systems zur Selbstreflexion über dessen Schadenspotenziale (im konkreten Einsatzkontext)[103]. Zum anderen erhöht es die Nachvollziehbarkeit algorithmischer Prozesse und Entscheidungen[104]. Im Kommissionsentwurf der KI-VO fand sich indes trotz des selbst erklärten Verordnungsziels des Grundrechts-

98 Vgl. im Ergebnis übereinstimmend *Gerdemann*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 49 Rn. 21.

99 *Hochrangige Expertengruppe für künstliche Intelligenz*, Ethik-Leitlinien für vertrauenswürdige KI, 2019, S. 19.

100 *Dollinger*, Folgenabschätzungen für Verwaltungs-Algorithmen, 2023, S. 38; *Wernick*, Digital Society 3 (2024), S. 1 (5).

101 *Mantelero*, CLSR 54 (2024), S. 1 (3).

102 *Human Rights Council*, Guiding Principles on Business and Human Rights: Implementing the United Nations „Protect, Respect and Remedy" Framework, UN doc A/HRC/17/31, 2011, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

103 *Eisenberger*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 27 Rn. 13; *Pilniok*, DÖV 2024, S. 581 (589).

104 *Müller/Schneeberger*, juridikum 2024, S. 265 (266).

schutzes[105] keine GRFA wieder. Vielmehr setzte sich erst das EU-Parlament erfolgreich dafür ein, dass die KI-VO nunmehr ein derartiges Instrument vorsieht (vgl. Art. 29a KI-VO-E-EP). Neben dem Beschwerderecht nach Art. 85 KI-VO ist die GRFA die einzige Vorgabe in der KI-VO, die tatsächlich unmittelbar dem Grundrechtsschutz dient[106].

Prüfungsmaßstab ist die Charta der Grundrechte der EU (GRCh), auch wenn deutsche Behörden die GRFA durchführen[107]. Denn bei der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen (d. h. Verordnungen im Unterschied zu Richtlinien) sind nach dem Grundsatz des Anwendungsvorrangs des Unionsrechts in aller Regel nicht die Grundrechte des Grundgesetzes, sondern allein die Unionsgrundrechte maßgeblich[108].

aa) Verpflichtete Betreiber (Art. 27 Abs. 1 S. 1 KI-VO). Die finale Fassung der GRFA ist hinter dem Parlamentsvorschlag zurückgeblieben und hat einen beschränkteren Adressatenkreis[109]. Während der Parlamentsvorschlag noch alle Betreiber von Hochrisiko-KI-Systemen nach Art. 6 Abs. 2 i. V. m. Anhang III KI-VO vor der Inbetriebnahme des jeweiligen Systems zur Durchführung einer GRFA verpflichten wollte, müssen dies nach Art. 27 Abs. 1 S. 1 KI-VO nur noch drei Betreibergruppen. In erster Linie sind dies öffentliche Stellen[110]. Aufgrund des Wortlauts („Betreiber, bei denen es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt") ließe sich erwägen, dass nur solche öffentliche Stellen eine GRFA durchführen müssen, die zur Leistungsverwaltung zählen. Dagegen spricht jedoch schon, dass in diesem Fall der besonders grundrechtssensible Bereich der Eingriffsverwaltung keiner GRFA-Pflicht unterläge. Naheliegender ist es, das Erfordernis der Erbringung öffentlicher Dienste nur auf private Einrichtungen zu beziehen, die dann ebenfalls der GRFA-Pflicht unterliegen[111].

bb) Prüfungselemente. Die GRFA umfasst sechs Prüfungselemente (Art. 27 Abs. 1 S. 2 lit. a bis e KI-VO). Damit stellt der Verordnungstext (scheinbar) ein weiteres Minus zum Parlamentsvorschlag dar (dazu nachfolgend)[112].

---

105 ErwGr. 1 KI-VO-E-KOM.

106 *Vasel*, EuZW 2024, S. 829 (831); vgl. *Palmstorfer*, NLMR 2024, S. 281 (285 ff.).

107 Vgl. *Eisenberger* (Fn. 103), Art. 27 Rn. 32; *Seitz*, EuZW 2024, S. 836 (843).

108 BVerfGE 152, 216 (236). Siehe dazu z. B. *Botta*, NVwZ 2022, S. 1247 (1249); *Karpenstein/Kottmann*, EuZW 2020, S. 185 (186 f.); *Kühling*, NJW 2020, S. 275 (277).

109 *Eisenberger* (Fn. 103), Art. 27 Rn. 19; *Müller/Schneeberger*, juridikum 2024, S. 265 (266 ff.).

110 Zusätzlich müssen auch die Betreiber von Hochrisiko-KI-Systemen gemäß Anhang III Nr. 5 lit. b und c KI-VO eine GRFA durchführen: KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden und KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen.

111 *Eisenberger* (Fn. 103), Art. 27 Rn. 27.

112 *Mantelero*, CLSR 54 (2024), S. 1 (8).

(1) Verfahren (Art. 27 Abs. 1 S. 2 lit. a KI-VO). Erstens muss der Betreiber die Verfahren beschreiben, bei denen er das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung einsetzen will (Art. 27 Abs. 1 S. 2 lit. a KI-VO). Dabei muss der Betreiber die durch den Anbieter getroffenen Festlegungen beachten[113]. Zum Detailgrad der Verfahrensbeschreibung schweigt sich der Normtext aus. Da sich aus der geplanten Verwendung der Einsatzkontext ergibt, ist jedoch Wert auf eine besondere Genauigkeit zu legen. Anderenfalls fehlte es an einer Grundlage dafür, um die nachfolgenden Informationen bewerten zu können. Dem steht auch nicht die (partielle) Veröffentlichungspflicht der GRFA entgegen[114], da sich diese nur auf die Zusammenfassung bezieht und nur die zuständigen Aufsichtsbehörden Zugriff auf die ausführliche GRFA haben[115].

(2) Zeitraum und Verwendungshäufigkeit (Art. 27 Abs. 1 S. 2 lit. b KI-VO). Zweitens muss der Betreiber beschreiben, in welchem Zeitraum und wie häufig er das Hochrisiko-KI-System verwenden will (Art. 27 Abs. 1 S. 2 lit. b KI-VO). Die zeitlichen Angaben müssen geeignet sein, um aus ihnen auf spezifische Schadensrisiken schließen zu können. Unzureichend dürften daher bspw. Angaben wie „regelmäßig" oder „selten" sein.

(3) Betroffene Personen und Personengruppen (Art. 27 Abs. 1 S. 2 lit. c KI-VO). Drittens muss der Betreiber die Kategorien der natürlichen Personen und Personengruppen nennen, die von dem KI-Einsatz im spezifischen Verwendungskontext betroffen sein könnten (Art. 27 Abs. 1 S. 2 lit. c KI-VO). Aufgrund ihres besonderen grundrechtlichen Schutzes ist insbesondere in den Blick zu nehmen, ob vulnerable Personen(gruppen) betroffen sein könnten. Dazu zählen vor allem Kinder (Art. 24 GRCh), ältere Menschen (Art. 25 GRCh) und Menschen mit Behinderung (Art. 26 GRCh)[116]. Da nur die Kategorien von Personen(gruppen) zu ermitteln sind, sind keine konkreten Personen zu nennen.

(4) Maßnahmen der menschlichen Aufsicht (Art. 27 Abs. 1 S. 2 lit. e KI-VO). Viertens muss der Betreiber beschreiben, inwieweit er Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen umgesetzt hat (Art. 27 Abs. 1 S. 2 lit. e KI-VO)[117]. Diese Informationspflicht spiegelt die Anbieterpflichten des Art. 14 KI-VO, die darauf zielen, dass Hochrisiko-KI-Systeme so gestaltet und entwickelt werden, dass natürliche Personen ihre Funktionsweise überwachen und sicherstellen können, dass sie bestimmungsgemäß verwendet werden und dass ihre

113 Denn Zweckbestimmung meint die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation (Art. 3 Nr. 12 KI-VO).

114 Siehe oben II. 1. b) cc).

115 Siehe unten II. 1. c) ee).

116 Vgl. *Müller/Schneeberger*, juridikum 2024, S. 265 (271).

117 Die Maßnahmen der menschlichen Aufsicht sind vor der Ermittlung spezifischer Schadensrisiken zu ermitteln, da sie in die dafür erforderliche Risikoprognose einfließen müssen.

Auswirkungen während des Lebenszyklus des Systems berücksichtigt werden (ErwGr. 73 S. 1 KI-VO).

(5) Spezifische Schadensrisiken (Art. 27 Abs. 1 S. 2 lit. d KI-VO). Fünftens muss der Betreiber die spezifischen Schadensrisiken, die sich auf die ermittelten natürlichen Personen(gruppen) auswirken könnten – unter Berücksichtigung der vom Anbieter bereitgestellten Informationen aus den Betriebsanleitungen (Art. 13 KI-VO) – nennen (Art. 27 Abs. 1 S. 2 lit. d KI-VO).

(a) Begriff des Schadensrisikos. Um sich den Regelungsgehalt dieser Pflicht erschließen zu können, ist das Schadensverständnis in Art. 27 KI-VO entscheidend. Zunächst handelt es sich beim Begriff des Schadensrisikos um eine Tautologie. Denn der Verordnungsgeber hat „Risiko" als die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens definiert (Art. 3 Nr. 2 KI-VO). Damit geht die Grundannahme einher, dass sich sowohl die Schadenswahrscheinlichkeit als auch die Schadensschwere quantifizieren lässt. Denn das Ziel des Produktsicherheitsrechts ist es, zumindest einen oder beide Faktoren auf ein akzeptables Level zu reduzieren (vgl. das Risikomanagementsystem des Art. 9 KI-VO[118])[119]. Ob ein KI-System dieses Level gerade noch einhält oder deutlich übertrifft, ist bedeutungslos.

Dieses Schadens- und Risikoverständnis lässt sich indes nicht eins zu eins auf die Grundrechte übertragen[120]. Zum einen beschränkt sich der Grundrechtsschutz nicht auf die Abwehr quantifizierbarer – insbesondere gesundheitlicher oder wirtschaftlicher – Nachteile und greift auch schon im Vorfeld solcher Schäden[121]. Zum anderen zielt der Grundrechtsschutz nicht nur auf ein akzeptables Level, sondern auf die größtmögliche Freiheitsgewährleistung[122]. Ein rein produktsicherheitsrechtliches Schadensverständnis höhlte die GRFA daher inhaltlich aus. Art. 27 Abs. 1 lit. d KI-VO ist folglich so auszulegen, dass das Schadensrisiko die Möglichkeit einer Grundrechtsverletzung der betroffenen Personen(gruppen) meint[123]. Eine derartige Auslegung überdehnt auch weder den Wortlaut der Norm noch widerspricht sie dem Willen des Verordnungsgebers. Denn dieser hat (an anderer Stelle) ausdrücklich festgehalten, dass ein Risiko i. S. d. KI-VO auch ein Risiko für die Grundrechte allgemein und nicht nur speziell für die (ebenfalls grundrechtlich geschützte) Gesundheit und Sicherheit bedeuten kann (vgl. Art. 79 Abs. 1 KI-VO).

(b) Risikoprognose. Da das Vorliegen einer Grundrechtsverletzung eine Wertungsfrage ist, bedarf die Schadensprognose einer vornehmlich qualitativen Analyse[124].

118 Siehe dazu z. B. *Braun Binder/Egli*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 9 Rn. 33 f.

119 *Almada/Petit*, The EU AI Act: A Medley of Product Safety and Fundamental Rights?, 2023, S. 19.

120 *Palmstorfer*, NLMR 2024, S. 281 (285); vgl. *Malgieri/Santos*, CLSR 56 (2025), S. 1 (4); *Seitz*, EuZW 2024, S. 836 (843).

121 *Malgieri/Santos*, CLSR 56 (2025), S. 1 (4); *Mysegades*, NVwZ 2020, S. 852 (854 f.); *Ruschemeier*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 7 Rn. 15; vgl. EuGH, NJW 2021, S. 531 (535); NJW 2024, S. 2099 (2101).

122 *Almada/Petit* (Fn. 119), S. 20.

123 *Eisenberger* (Fn. 103), Art. 27 Rn. 39; vgl. auch *Ruschemeier* (Fn. 91), Art. 6 Rn. 103.

124 *Eisenberger* (Fn. 103), Art. 27 Rn. 41.

Dafür ist eine umfassende Grundrechtsprüfung vorzunehmen[125]. Zwar haben die grundrechtsspezifischen Prüfungselemente keinen Eingang in die finale Fassung des Art. 27 KI-VO gefunden. Der Parlamentsentwurf hatte noch ausdrücklich vorgesehen, dass die Verwendung des jeweiligen Hochrisiko-KI-Systems den Grundrechten entsprechen muss (Art. 29a Abs. 1 S. 2 lit. d KI-VO-E-EP) und dass die vernünftigerweise vorhersehbaren Auswirkungen der Inbetriebnahme des Hochrisiko-KI-Systems auf die Grundrechte zu berücksichtigen sind (Art. 29a Abs. 1 S. 2 lit. e KI-VO-E-EP). Aber auch die Streichung dieser Prüfungselemente ändert nichts daran, dass nur eine Grundrechtsprüfung dem Betreiber Klarheit darüber verschaffen kann, ob ungerechtfertigte Grundrechtseingriffe drohen. Dass der Unionsgesetzgeber dies nicht ausdrücklich festgehalten hat, entlastet die Betreiber mithin nicht durch eine „GRFA light", sondern erhöht vielmehr ihren Prüfungsaufwand, da sie sich nicht ausschließlich am Gesetzeswortlaut orientieren können[126]. Soweit sich im Schrifttum der Vorschlag findet, die GRFA in drei Schritte – Risikoidentifikation, Risikoanalyse und Risikomanagement – zu untergliedern[127], spiegelt sich diese Vorgehensweise auch in der klassischen Grundrechtsprüfung wider. In ihr werden die zuvor erlangten Informationen zusammengeführt und auf etwaige Schutzlücken untersucht. Eine Modifikation folgt freilich insoweit, dass lediglich die Möglichkeit einer Grundrechtsverletzung und nicht das Bestehen einer Grundrechtsverletzung festzustellen ist.

Eingangs ist zu ermitteln, welche Grundrechte von der Verwendung des Hochrisiko-KI-Systems betroffen sein könnten. Zu berücksichtigende Grundrechte sind insbesondere die Menschenwürde (Art. 1 GRCh)[128], die Achtung des Privat- und Familienlebens (Art. 7 GRCh), der Schutz personenbezogener Daten (Art. 8 GRCh), die Gleichheit vor dem Gesetz (Art. 20 GRCh), die Nichtdiskriminierung (Art. 21 GRCh) und das Recht auf eine gute Verwaltung (Art. 41 GRCh)[129]. Es ist für jedes Grundrecht separat zu prüfen, ob sein Schutzbereich durch die Verwendung des Hochrisiko-KI-Systems (wahrscheinlich) eröffnet wird. Dafür ist maßgeblich auf die Zweckbestimmung des Systems und das Verfahren, bei dem es zum Einsatz kommen soll, abzustellen. Aufschlussreich können auch die betroffenen Personen(gruppen) sein. Entscheidend ist oftmals, ob bzw. welche personenbezogenen Daten in den

125 Aus der Gegenansicht dazu folgte ein doppeltes Prüfungserfordernis für öffentliche Stellen. Diese müssten dann sowohl eine GRFA durchführen als auch eine Recht- und insbesondere Verhältnismäßigkeitsprüfung vornehmen. Denn eine rein produktsicherheitsrechtlich verstandene GRFA ersetzte keine Grundrechtsprüfung (vgl. dazu *Seitz*, EuZW 2024, S. 836 (844)). Eine „GRFA light" wäre daher mitnichten eine bürokratische Entlastung für die öffentliche Verwaltung.

126 *Mantelero*, CLSR 54 (2024), S. 1 (8).

127 Vgl. *Mantelero*, CLSR 54 (2024), S. 1 (11).

128 Zum Verhältnis von Menschenwürde und KI z. B. *Golla*, DÖV 2019, S. 673 (675 ff.); vgl. auch *Botta*, Industrie 4.0: Menschenwürde und verfassungsrechtliche Perspektiven, in: Schroeder/Bitzegeio/Fischer (Hrsg.), Digitale Industrie, algorithmische Arbeit, gesellschaftliche Transformation, 2020, S. 102 (102 ff.).

129 Der Parlamentsentwurf hatte zusätzlich ausdrücklich die Einbeziehung von Allgemeininteressen vorgesehen, konkret den Umweltschutz (Art. 29a Abs. 1 S. 2 lit. g KI-VO-E-EP). Diese sind nunmehr nur mittelbar über die Grundrechte zu berücksichtigen, soweit sie von diesen miterfasst sind.

Algorithmus einfließen sollen. So ruft bspw. die Verarbeitung besonders sensibler Merkmale wie Geschlecht oder Religionszugehörigkeit neben Art. 7 und Art. 8 GRCh auch Art. 21 GRCh auf den Plan. Gleichzeitig kann die Nichtberücksichtigung relevanter Informationen mit Art. 41 GRCh kollidieren[130].

Des Weiteren muss der Betreiber untersuchen, inwieweit die Verwendung des Hochrisiko-KI-Systems in den Schutzbereich der ermittelten Grundrechte eingreift. Es kommt somit darauf an, ob eine grundrechtlich geschützte Verhaltensweise erschwert oder unmöglich gemacht wird[131]. Auch das Bestehen einer Ungleichbehandlung (aufgrund bestimmter Merkmale) ist in den Fokus zu nehmen. In diesem Prüfungsschritt sind zwei Faktoren von besonderer Bedeutung: die Wahrscheinlichkeit und die Schwere des Eingriffs bzw. der Ungleichbehandlung. Dabei ist insbesondere auf den Zeitraum und die Häufigkeit der Verwendung des KI-Systems sowie die Anzahl der betroffenen Personen(gruppen) zu achten. Die Intensität des Eingriffs bzw. der Ungleichbehandlung bestimmt sich zudem nach seiner bzw. ihrer Reversibilität[132].

Schlussendlich muss der Betreiber ergründen, ob sich die ggf. festgestellten Eingriffe bzw. Ungleichbehandlungen rechtfertigen lassen. Dies setzt eine Verhältnismäßigkeitsprüfung voraus. Es ist insoweit unschädlich, dass Art. 27 KI-VO im Unterschied zu Art. 35 Abs. 7 lit. b DSGVO, der die Datenschutz-Folgenabschätzung regelt, eine derartige Prüfung nicht explizit einfordert. Die anvisierte Verwendung des Hochrisiko-KI-Systems ist darauf zu untersuchen, ob sie einen legitimen Zweck verfolgt, geeignet, erforderlich und angemessen ist. Dafür sind vornehmlich die Erkenntnisse aus den Betriebsanleitungen des Anbieters und aus den anderen Prüfungselementen des Art. 27 Abs. 1 S. 2 KI-VO fruchtbar zu machen. Rechtfertigung kann der staatliche KI-Einsatz insbesondere aus der Sicherstellung einer funktionsfähigen und zeitgemäßen Verwaltung erfahren[133]. Im Rahmen der Erforderlichkeitsprüfung ist kritisch in den Blick zu nehmen, ob das angestrebte Ziel nicht auch durch die Verwendung eines KI-Systems mit geringerem Risiko oder ganz ohne KI erreicht werden kann. Es muss folglich nicht nur nach dem „Wie", sondern auch nach dem „Ob" gefragt werden. Inwieweit die Verwendung des Hochrisiko-KI-Systems angemessen ist, hängt u. a. davon ab, welche risikovermeidenden und risikominimierenden Maßnahmen der Betreiber beabsichtigt hat. Dabei sind auch die Maßnahmen der menschlichen Aufsicht zu berücksichtigen.

(*6) Maßnahmen im Falle eines Risikoeintritts (Art. 27 Abs. 1 S. 2 lit. f KI-VO).* Sechstens muss der Betreiber die Maßnahmen benennen, die im Falle des Eintretens der ermittelten Risiken zu ergreifen sind, einschließlich der Regelungen für die inter-

130 EuGH, EuZW 2002, 721 (723); *Ruffert*, in: Calliess/Ruffert (Hrsg.), 6. Aufl. 2022, Art. 41 GRCh Rn. 10.

131 *Jarass*, in: ders. (Hrsg.), 4. Aufl. 2021, Art. 52 Rn. 11; *Kingreen*, in: Calliess/Ruffert (Hrsg.), 6. Aufl. 2022, Art. 52 GRCh Rn. 55 f.; *Pache*, in: Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar EUV/GRC/AEUV, 2. Aufl. 2023, Art. 52 GRCh Rn. 15.

132 Vgl. *Mantelero*, CLSR 54 (2024), S. 1 (15).

133 Vgl. *Botta*, NVwZ 2022, S. 1247 (1250).

ne Unternehmensführung[134] und Beschwerdemechanismen (Art. 27 Abs. 1 S. 2 lit. f KI-VO). Aus dieser Vorgabe ließe sich schlussfolgern, dass die GRFA nicht bezweckt, das Schadensrisiko zu mindern, sondern nur seine Folgen abzumildern[135]. Dafür spricht, dass die finale Fassung des Art. 27 KI-VO im Gegensatz zum Parlamentsentwurf (Art. 29a Abs. 1 S. 2 lit. h und Abs. 2 KI-VO-E-EP) tatsächlich an keiner Stelle ausdrücklich Maßnahmen zur Schadensminderung erwähnt. Dagegen lässt sich indes anführen, dass der Risikoeintritt eine Grundrechtsverletzung bedeutet. Art. 27 KI-VO zielt vornehmlich auf öffentliche Stellen, die grundrechtsgebunden sind und daher nicht sehenden Auges grundrechtswidrige Zustände abwarten dürfen. Ein bloßer ex-post-Grundrechtsschutz liefe außerdem dem ex-ante-Ansatz des Art. 27 KI-VO und der gesamten Verordnung zuwider[136].

Kommt der Betreiber i. R. d. Grundrechtsprüfung zu dem Ergebnis, dass sich der beabsichtigte KI-Einsatz nicht (durch ergriffene Schutzmaßnahmen) rechtfertigen lässt, darf er mit diesem gar nicht erst beginnen. Ein solches Szenario tritt bspw. dann ein, wenn das KI-System umfassende Persönlichkeitsprofile der betroffenen Personen erstellen soll, was eine grundrechtswidrige Totalerfassung zur Folge hätte[137]. Ergibt sich die Grundrechtsverletzung erst nach der Inbetriebnahme des Hochrisiko-KI-Systems, muss der Betreiber die Verwendung sofort beenden und etwaigen Folgeschäden angemessen begegnen. Der Betreiber muss in der GRFA daher auch Szenarien abwägen, in denen die von ihm getroffenen Maßnahmen zur Risikovermeidung oder Risikominimierung versagen.

cc) Einbeziehung relevanter Interessenträger (ErwGr. 96 S. 11 KI-VO). Grundsätzlich hat der Unionsgesetzgeber den Betreiber i. R. d. GRFA nur dazu verpflichtet, auf bestimmte Informationen des Anbieters zurückzugreifen. Es steht ihm jedoch frei, relevante Interessenträger, u. a. Vertreter von Personengruppen, die von dem KI-System betroffen sein könnten, unabhängige Sachverständige und Organisationen der Zivilgesellschaft, sowohl in die Durchführung der GRFA als auch in die Gestaltung von Abhilfemaßnahmen einzubeziehen (ErwGr. 96 S. 11 KI-VO).

dd) Fortwirkung und Aktualisierungspflicht (Art. 27 Abs. 2 KI-VO). Die Durchführung einer GRFA ist grundsätzlich nur vor der ersten Verwendung eines Hochrisiko-KI-Systems verpflichtend (Art. 27 Abs. 2 S. 1 KI-VO). Der Betreiber kann sich in ähnlichen Fällen auf zuvor durchgeführte GRFA oder bereits vorhandene Folgenabschätzungen des Anbieters stützen (Art. 27 Abs. 2 S. 2 KI-VO). Letzteres dürfte sich insbesondere auf die Erkenntnisse aus dem Risikomanagementsystem des Anbieters beziehen (vgl. Art. 9 KI-VO)[138].

Gelangt der Betreiber während der Verwendung des Hochrisiko-KI-Systems zur Auffassung, dass die Informationen, die der GRFA zugrunde lagen, sich geändert ha-

134 Dies setzt in der öffentlichen Verwaltung eine entsprechende Governance-Struktur voraus. Siehe dazu *Eisenberger* (Fn. 103), Art. 27 Rn. 47.

135 *Eisenberger* (Fn. 103), Art. 27 Rn. 14; *Müller/Schneeberger*, juridikum 2024, S. 265 (268).

136 *Mantelero*, CLSR 54 (2024), S. 1 (9).

137 Vgl. EuGH, NJW 2024, 2099 (2107) m. Anm. *Hartl/Vogel*; BVerfGE 27, 1 (6); 65, 1 (53); *Botta*, DÖV 2023, S. 421 (424 f.).

138 *Mantelero*, CLSR 54 (2024), S. 1 (6).

ben oder sich nicht mehr auf dem neuesten Stand befinden, so unternimmt er die erforderlichen Schritte, um die Informationen zu aktualisieren (Art. 27 Abs. 2 S. 3 KI-VO)[139].

ee) Mitteilung an Marktüberwachungsbehörde (Art. 27 Abs. 3 KI-VO). Sobald der Betreiber die GRFA durchgeführt hat, teilt er ihre Ergebnisse der zuständigen Marktüberwachungsbehörde mit, indem er den ausgefüllten Musterfragebogen[140] übermittelt (Art. 27 Abs. 3 S. 1 KI-VO). Die Mitteilungspflicht ist nur entbehrlich, wenn außergewöhnliche Gründe der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit von Personen, des Umweltschutzes oder des Schutzes wichtiger Industrie- und Infrastrukturanlagen vorliegen (Art. 27 Abs. 3 S. 2 i. V. m. Art. 46 Abs. 1 KI-VO).

ff) Verhältnis zur Datenschutz-Folgenabschätzung (Art. 27 Abs. 4 KI-VO). Zwischen der GRFA und einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO bzw. Art. 27 JI-RL besteht ein Spezialitätsverhältnis zugunsten letzterer[141]. Umfasst eine DSFA bereits einen Bestandteil der GRFA, so ergänzt die GRFA die DSFA lediglich (Art. 27 Abs. 4 KI-VO). Aufgrund des engeren Anwendungsbereichs der DSFA dürfte dies freilich nur dann der Fall sein, wenn sie sich den Verarbeitungsfolgen für Art. 7 und Art. 8 GRCh widmet[142]. Dass eine DSFA darüber hinaus noch andere Grundrechte in den Fokus nimmt, ist trotz des Wortlauts des Art. 35 DSGVO bzw. Art. 27 JI-RL („Rechte und Freiheiten natürlicher Personen") die Ausnahme[143].

gg) Musterfragebogen (Art. 27 Abs. 5 KI-VO). Das Büro für Künstliche Intelligenz[144] ist beauftragt, einen (automatisierten) Musterfragebogen zu erarbeiten, um die Betreiber in die Lage zu versetzen, ihrer Pflicht zur GRFA-Durchführung in vereinfachter Weise nachzukommen (Art. 27 Abs. 5 KI-VO)[145]. Entgegen dem Wortlaut dieser Regelung („die Betreiber in die Lage zu versetzen") ist das Ausfüllen des Musterfragebogens obligatorisch und kein fakultatives Angebot. Dies ergibt sich aus der Übermittlungspflicht nach Art. 27 Abs. 3 KI-VO[146]. Eine Grundrechtsprüfung lässt sich indes nur begrenzt standardisieren, da sie auf einer vornehmlich qualitativen

139 Die Aktualisierungspflicht hängt somit vom Kenntnisstand des Betreibers ab. Siehe *Eisenberger* (Fn. 103), Art. 27 Rn. 51.

140 Siehe unten II. 1. c) gg).

141 Vgl. *Hüger*, ZfDR 2024, S. 263 (284).

142 Vgl. *Eisenberger* (Fn. 103), Art. 27 Rn. 58; *Müller/Schneeberger*, juridikum 2024, S. 265 (267).

143 *Mantelero*, CLSR 54 (2024), S. 1 (4); wohl a. A.: *Gaden*, PinG 2024, S. 189 (189).

144 Das Büro für Künstliche Intelligenz ist Bestandteil der EU-Kommission (Art. 3 Nr. 47 KI-VO).

145 Dabei kann das Büro z. B. auf die Vorarbeiten des European Law Institute (*European Law Institute*, ELI Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration, 2022) zurückgreifen. Dazu weiterführend *Dollinger* (Fn. 100), S. 76 ff.; *Merli*, Eine Folgenabschätzung für Algorithmen in der staatlichen Verwaltung. Der Gesetzgebungsvorschlag des European Law Instituts, in: Hoffberger-Pippan/Ladeck/Ivankovics (Hrsg.), Digitalisierung und Recht, 2022, S. 275 (275 ff.).

146 *Eisenberger* (Fn. 103), Art. 27 Rn. 60.

Analyse beruht und einzelfallabhängig ist[147]. Der Musterfragebogen birgt daher sowohl die Chance auf ein einheitliches Prüfungsniveau als auch das Risiko einer unterkomplexen und damit bedeutungslosen Folgenabschätzung.

d) Zwischenfazit. Die EU-Datenbank für Hochrisiko-KI-Systeme (Art. 71 KI-VO) dürfte das KI-Transparenzniveau in der öffentlichen Verwaltung deutlich erhöhen. Einen neuen Goldstandard etabliert sie gleichwohl nicht. Insbesondere bleibt sie hinter der Informationsdichte des niederländischen Registers zurück. Zum einen erfasst die Datenbank nicht alle KI-Systeme und zum anderen kann auch die GRFA (Art. 27 KI-VO) als ihr zentraler Informationsgehalt nur eine beschränkte Transparenzwirkung entfalten, da lediglich deren Zusammenfassung veröffentlicht werden muss[148]. Eine generelle Veröffentlichungspflicht fehlt[149]. Außerdem ist die Prüfungstiefe der GRFA noch mehr als ungewiss. Vor diesem Hintergrund stellt sich die Frage, ob die mitgliedstaatlichen Gesetzgeber für ihren Verwaltungsbereich auch eigene (umfassendere) KI-Transparenzregister auf den Weg bringen oder fortführen dürfen.

2. Mitgliedstaatlicher Regelungsspielraum

Dafür ist entscheidend, welcher Regelungsspielraum den Mitgliedstaaten nach Inkrafttreten der KI-VO verblieben ist.

a) Öffnungsklauseln? Im Unterschied zur DSGVO enthält die KI-VO nur wenige[150] Öffnungsklauseln[151]. Im Zusammenhang mit der EU-Datenbank besteht ein ausdrücklicher Regelungsspielraum allein für KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteile i. R. d. Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen (Anhang III Nr. 2 KI-VO). Derartige Hochrisiko-KI-Systeme sind auf nationaler Ebene zu registrieren (Art. 49 Abs. 5 KI-VO). Vorgaben für die nationalen Datenbanken beinhaltet die KI-VO nicht[152].

Auch die Öffnungsklausel des Art. 2 Abs. 11 KI-VO schafft keine Grundlage für ein umfassendes KI-Transparenzregister. Danach hindert die KI-VO die Mitgliedstaaten nicht daran, Rechts- oder Verwaltungsvorschriften beizubehalten oder einzuführen, die für Arbeitnehmer im Hinblick auf den Schutz ihrer Rechte bei der Verwendung von KI-Systemen durch die Arbeitgeber vorteilhafter sind, oder die Anwendung von Kollektivvereinbarungen zu fördern oder zuzulassen, die für die Arbeitnehmer vorteilhafter sind. Der nationale Gesetzgeber kann daher zum Schutz der

147 Kritisch dazu *Mantelero*, CLSR 54 (2024), S. 1 (7).

148 *Mantelero*, CLSR 54 (2024), S. 1 (10); vgl. *Wernick*, Digital Society 3 (2024), S. 1 (24 f.).

149 *Müller/Schneeberger*, juridikum 2024, S. 265 (267). Stattdessen ist der Umweg über Informationsfreiheitsansprüche zu gehen. Siehe dazu *Pilniok*, DÖV 2024, S. 581 (590).

150 Eine Öffnungsklausel beinhaltet z. B. Art. 5 Abs. 5 KI-VO für den Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken.

151 Weiterführend zu Öffnungsklauseln in der DSGVO siehe z. B. *Kühling/Martini et al.*, Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 2 ff.; *Sandhu*, Grundrechtsunitarisierung durch Sekundärrecht, 2021, S. 238 ff.

152 *Gerdemann* (Fn. 98), Art. 49 Rn. 39.

Beschäftigten im Öffentlichen Dienst eigene Transparenzmechanismen einführen. Die staatlich eingesetzten KI-Systeme dürften oftmals jedoch auch (in größerer Zahl) Personen außerhalb der Verwaltung betreffen, deren Schutz nicht von der Öffnungsklausel erfasst ist.

b) Sperrwirkung der KI-VO? Die Unionskonformität eines nationalen KI-Transparenzregisters für die öffentliche Verwaltung hängt mithin maßgeblich davon ab, ob bzw. inwieweit die KI-VO abschließend für die KI-Regulierung ist. Dafür ist zunächst ein Blick auf die kompetenziellen Grundlagen der Verordnung zu werfen. Wie auch bei anderen Daten- und Digitalrechtsakten hat sich der Unionsgesetzgeber vornehmlich auf die Binnenmarktkompetenz (Art. 114 Abs. 1 AEUV) berufen[153]. Die Regulierung des Binnenmarktes stellt eine geteilte Zuständigkeit zwischen der Union und ihren Mitgliedstaaten dar (Art. 4 Abs. 2 lit. a AEUV). Insoweit der Unionsgesetzgeber diese Zuständigkeit wahrnimmt, sind mitgliedstaatliche Regelungen grundsätzlich gesperrt (Art. 2 Abs. 2 S. 2 AEUV)[154]. Erlässt ein Mitgliedstaat dennoch eigene Vorschriften, sind diese unanwendbar und stellen einen Verstoß gegen Art. 2 Abs. 2 AEUV i. V. m. Art. 114 AEUV dar[155].

Die Reichweite der Sperrwirkung bestimmt sich nach dem Regelungsgehalt des jeweiligen Sekundärrechtsaktes[156]. Die KI-VO ist in erster Linie Produktsicherheitsrecht[157]. Sie soll das Funktionieren des Binnenmarktes durch einen einheitlichen Rechtsrahmen verbessern, der einen grenzüberschreitenden freien Verkehr KI-gestützter Waren und Dienstleistungen gewährleistet und verhindert, dass die Mitgliedstaaten die Entwicklung, Vermarktung und Verwendung von KI-Systemen beschränken (ErwGr. 1 KI-VO). Dafür verpflichtet sie vorrangig die Anbieter von Hochrisiko-KI-Systemen dazu, ein Konformitätsbewertungsverfahren durchzuführen, um die Risiken ihrer Systeme vor dem Inverkehrbringen bzw. der Inbetriebnahme zu minimieren[158]. Außerdem regelt sie die staatliche Notifizierung unabhängiger Konformitätsstellen und die Marktüberwachung und damit ihren direkten bzw. indirekten Vollzug[159/160]. Damit zielt sie im Produktsicherheitsrecht für Hochrisiko-KI-Systeme erkennbar auf eine Vollharmonisierung.

---

153 Daneben hat sich der Unionsgesetzgeber auch auf die Datenschutzkompetenz (Art. 16 Abs. 2 AEUV) gestützt. Diese Kompetenz soll ausweislich ErwGr. 3 S. 5 KI-VO aber nur die Regelungen der Verwendung von KI-Systemen zur biometrischen Fernidentifizierung zu Strafverfolgungszwecken, der Verwendung von KI-Systemen für die Risikobewertung natürlicher Personen zu Strafverfolgungszwecken und der Verwendung von KI-Systemen zur biometrischen Kategorisierung zu Strafverfolgungszwecken stützen. Siehe dazu z. B. *Palmstorfer*, NLMR 2024, S. 281 (284).

154 Weiterführend dazu z. B. *Bauerschmidt*, EuR 2014, S. 277 (285); *Bieber/Kotzur*, § 3 Strukturprinzipien der EU-Verfassung, in: Bieber/Epiney/Haag/Kotzur (Hrsg.), Die Europäische Union, 13. Aufl. 2019, S. 100 (112).

155 *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, 7. Aufl. 2015, Art. 2 AEUV Rn. 29.

156 Protokoll 25, ABl. 2007 C 306/158.

157 *Pilniok*, DÖV 2024, S. 581 (584); vgl. *Martini/Botta*, MMR 2024, S. 630 (630).

158 Weiterführend dazu *Gerdemann*, NJW 2024, S. 2209 (2209 ff.).

159 Zur Unterscheidung zwischen dem direkten und dem indirekten Vollzug des Unionsrechts siehe z. B. *Ruffert*, DÖV 2007, S. 761 (763).

Mit den Art. 71 und Art. 27 KI-VO könnte der Unionsgesetzgeber auch das Konzept eines KI-Transparenzregisters (für die öffentliche Verwaltung) abschließend geregelt haben. Schließlich beziehen sich die Vorschriften nicht nur auf private, sondern vor allem auch auf öffentliche Stellen und sehen für die Mitgliedstaaten lediglich überschaubare Regelungsspielräume vor. Ihre Sperrwirkung kann indes nicht weiter reichen als die ihnen zugrunde liegende Binnenmarktkompetenz[161]. Eine allgemeine Zuständigkeit für das Verwaltungsrecht steht dem Unionsgesetzgeber nicht zu (vgl. Art. 291 Abs. 1 AEUV)[162]. Etabliert ein mitgliedstaatlicher Gesetzgeber daher Vorgaben mit einer anderen Zielsetzung – vorliegend die Transparenz der öffentlichen Verwaltung –, ist es unschädlich, wenn sie denselben Adressatenkreis betreffen und vergleichbare Instrumentarien vorsehen[163]. Eine Grenze besteht allein insoweit, als dass das mitgliedstaatliche Recht kein Hemmnis für den freien Waren- und Dienstleistungsverkehr verursachen darf[164]. Bei der Regelung des KI-Einsatzes in der öffentlichen Verwaltung liegen Kollisionen mit den Grundfreiheiten oder Wettbewerbsverfälschungen schon allgemein eher fern[165]. Insbesondere ein mitgliedstaatliches KI-Transparenzregister für die öffentliche Verwaltung stellt kein Hindernis für die Umsetzung der KI-VO dar, solange es nicht die Pflichten aus Art. 71 und Art. 27 KI-VO erschwert oder unmöglich macht. Während die KI-VO somit im Produktsicherheitsrecht eine relevante Sperrwirkung entfaltet, bindet sie den mitgliedstaatlichen Gesetzgeber bei der Gestaltung seines Verwaltungsrechts deutlich geringer[166].

III. Verfassungsrechtlicher Rahmen eines KI-Transparenzregisters

Die Errichtung eines KI-Transparenzregisters für die öffentliche Verwaltung ruft nicht nur das Unionsrecht, sondern auch das nationale Verfassungsrecht auf den Plan.

160 Weiterführend dazu *Martini/Botta*, MMR 2024, S. 630 (630 ff.); *Roth-Isigkeit*, ZRP 2022, S. 187 (187 ff.).

161 *Härtel*, § 6 Die Zuständigkeiten der Union, in: Niedobitek (Hrsg.), Europarecht, 2019, S. 447 (483). Zudem lässt sich der Binnenmarktbezug und damit die Unionskonformität des Art. 27 KI-VO generell kritisch hinterfragen (siehe *Krönke*, NVwZ 2024, S. 529 (533)).

162 *Kahl*, NVwZ 1996, S. 865 (869). Indes darf der Unionsgesetzgeber über die Binnenmarktkompetenz den indirekten Vollzug des Unionsrechts durch die Mitgliedstaaten regeln und z. B. Vorgaben für die Organisation der zuständigen nationalen Behörden aufstellen. Es ist dem mitgliedstaatlichen Gesetzgeber daher bspw. versagt, die Unabhängigkeit der Marktüberwachungsbehörde(n) anzutasten (vgl. Art. 70 Abs. 1 S. 2 KI-VO).

163 Vgl. *Cole/Ukrow*, Der EU Digital Services Act und verbleibende nationale (Gesetzgebungs-) Spielräume, 2023, S. 14.

164 *Bauerschmidt*, EuR 2014, S. 277 (294); vgl. *Kahl*, NVwZ 1996, S. 865 (867); *Korte*, in: Calliess/Ruffert (Hrsg.), 6. Aufl. 2022, Art. 114 Rn. 40.

165 Vgl. *Gless/Janal*, § 2 Anwendungsbereich und Adressaten, in: Hilgendorf/Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, 2023, Rn. 35; *Pilniok*, DÖV 2024, S. 581 (583); *Wendehorst* (Fn. 63), Art. 2 Rn. 157.

166 *Heckmann/Rachut*, Kapitel 5: Digitale Verwaltung, in: Heckmann/Paschke (Hrsg.), juris PraxisKommentar Internetrecht, 8. Aufl. 2024, Rn. 1223; *Pilniok*, DÖV 2024, S. 581 (583); vgl. *Dollinger* (Fn. 100), S. 276 ff.; zurückhaltender *Korte*, DÖV 2024, S. 770 (771); offen lassend *Guckelberger*, DÖV 2025, S. 45 (46).

1. Anforderungen an die Registergrundlage

Zunächst ist klärungsbedürftig, auf welcher Rechtsgrundlage ein KI-Transparenzregister in Deutschland basieren muss, um verfassungskonform zu sein.

a) Vorbehalt des Gesetzes (Art. 20 Abs. 3 GG). Da das Register einen Einblick in die Arbeitsweise der Verwaltung verschaffen soll, ließe sich erwägen, es durch bloßes Exekutivrecht, d. h. mittels einer Rechtsverordnung oder sogar nur mittels einer Verwaltungsvorschrift, zu errichten. In diesem Zusammenhang könnte es auch naheliegend erscheinen, ein KI-Transparenzregister mithilfe des IT-Planungsrates einzuführen (in diese Richtung weisen die bisherigen Bestrebungen)[167]. Er ist das zentrale politische Steuerungsgremium von Bund und Ländern für die Verwaltungsdigitalisierung und kann verbindliche Beschlüsse fassen, die als Innenrecht wirken[168].

aa) Wesentlichkeit eines KI-Transparenzregisters. Nach der ständigen Rechtsprechung des BVerfG ist der Gesetzgeber indes verpflichtet, in grundlegenden normativen Bereichen alle wesentlichen Entscheidungen selbst zu treffen[169]. Zu diesen Bereichen zählt insbesondere die Grundrechtsausübung, wobei es nicht zwingend auf einen staatlichen Eingriff ankommt[170].

Zwar folgt aus der Informationsfreiheit des Art. 5 Abs. 1 S. 1 Alt. 2 GG keine Verpflichtung zur staatlichen Informationsbereitstellung, sondern nur ein Zugangsrecht zu bereits allgemein zugänglichen Informationsquellen[171]. Aber ein KI-Transparenzregister nach niederländischem Vorbild diente insbesondere dem offenen Prozess politischer Meinungs- und Willensbildung als Voraussetzung demokratischer Legitimation und konkretisierte so das Demokratieprinzip (Art. 20 Abs. 2 GG) und zugleich die Informationsfreiheit in ihrer Funktion für die politische Willensbildung[172]. Außerdem können KI-Systeme in der öffentlichen Verwaltung insbesondere die informationelle Selbstbestimmung und die Gleichheitsrechte – sowohl der Behördenmitarbeiter als auch der Bürger – berühren. Ohne eine ausreichende Informationsgrundlage lässt sich darüber hinaus schon gar nicht überprüfen, ob die eigenen Grundrechte tatsächlich betroffen sind, was ihrer Ausübung und ihrem Schutz entgegensteht. Ein Transparenzregister ist daher ein wichtiger Baustein für einen effektiven Grundrechtsschutz im digitalen Staat, m. a. W.: Grundrechtsvoraussetzungsschutz[173]. Gleichzeitig können aus einem Transparenzregister auch Eingriffe in die Grundrechte Dritter erfolgen, insbesondere durch die Veröffentlichung von perso-

167 Vgl. *IT-Planungsrat*, Marktplatz der KI-Möglichkeiten, Beschluss 2024-01 vom 4. 7. 2024.

168 *Schulz/Tallich*, NVwZ 2010, S. 1338 (1341); *Siegel*, § 157 Verwaltungshandeln sui generis, in: Kahl/Ludwigs (Hrsg.), Handbuch des Verwaltungsrechts, 2023, Rn. 49; vgl. *Steinmetz*, NVwZ 2011, S. 467 (468 ff.).

169 StRspr. des BVerfG, siehe z. B. BVerfGE 49, 89 (126 f.); 53, 30 (56); 88, 103 (116).

170 Ebenda; *Kalscheuer/Jacobsen*, DÖV 2018, S. 523 (528).

171 BVerfGE 66, 116 (137); 103, 44 (60); *Caspar*, DÖV 2013, S. 371 (372); *Nolte*, NVwZ 2018, S. 521 (522).

172 Vgl. BVerwG NVwZ 2018, S. 1401 (1404).

173 Vgl. *Schoch*, in: ders. (Hrsg.), 3. Aufl. 2024, Einleitung, Rn. 53; *Wehrmann*, ZGI 2022, S. 205 (209).

nenbezogenen Daten oder Betriebs- und Geschäftsgeheimnissen (siehe unten III. 2. b)). Auch dies ruft den Vorbehalt des Gesetzes auf den Plan[174].

Selbst wenn man die Grundrechtsrelevanz des Registers verneinen wollte, stünde dies der Wesentlichkeit seiner Einführung nicht entgegen. Denn gesetzlicher Regelung bedürfen auch Fragen, die für Staat und Gesellschaft von erheblicher Bedeutung sind[175]. Zu derartigen für das Allgemeinwohl relevanten Fragen gehört aufgrund seiner großen Chancen – aber auch seiner großen Risiken – der staatliche KI-Einsatz und das Wissen über diesen. Die Entscheidung über das Ausmaß der Informationsgewährung entfaltet in zweifacher Hinsicht eine erhebliche Bedeutung. Einerseits ist das Transparenzniveau bestimmend für die Kontrolldichte des KI-Einsatzes durch Parlament und Öffentlichkeit. Andererseits ermöglicht ein einmal offengelegtes KI-System einen Einblick in die Behördenarbeit, der nicht nur positive, sondern auch negative Effekte wie z. B. eine erhöhte technische Vulnerabilität und damit eine Gefahr für die Funktionsfähigkeit der Verwaltung mit sich bringen kann[176]. Es ist die Aufgabe des Gesetzgebers, diese gegenläufigen Aspekte miteinander abzuwägen und in einen schonenden Ausgleich zu bringen. Die Errichtung eines KI-Transparenzregisters muss somit auf Grundlage eines formellen Gesetzes erfolgen[177].

bb) KI-Transparenz de lege lata. Auf Landesebene existieren bereits gesetzliche Vorgaben zur KI-Transparenz, an die sich anknüpfen ließe. So schreibt Art. 5 Abs. 2 S. 2 Bayerisches Digitalgesetz vor, dass der Einsatz von KI in der Verwaltung durch geeignete Kontroll- und Rechtsschutzmaßnahmen abzusichern ist. Zu derartigen Maßnahmen zählt auch die Information über die Verwendung des jeweiligen KI-Systems. Noch konkreter sind die Transparenzpflichten für Schleswig-Holsteinische Behörden[178]. Diese müssen den Algorithmus von datenbasierten Informationstechnologien und die zugrunde liegende Datenbasis offenlegen, sofern dem nicht der Schutz personenbezogener Daten, sonstige Rechte Dritter oder öffentliche Interessen an der Geheimhaltung entgegenstehen (§ 6 Abs. 1 S. 1 IT-Einsatz-Gesetz Schleswig-Holstein). Zusätzlich zur Offenlegung bedarf es einer in allgemeinverständlicher Form und Sprache formulierten Beschreibung, aus der sich die grundsätzliche Funktionsweise und die Entscheidungslogik des Algorithmus ergeben (§ 6 Abs. 1 S. 3 IT-Einsatz-Gesetz Schleswig-Holstein).

b) Kompetenzordnung (Art. 70 ff. und 83 ff. GG). Um den Bürgern einen möglichst niedrigschwelligen und umfassenden Informationsstand über den KI-Einsatz in der öffentlichen Verwaltung zu bieten, wäre es empfehlenswert, eine einheitliche, ebenenübergreifende Datenbank zu errichten. Die Zulässigkeit einer zentralen Register-

174 Vgl. BayVGH ZD 2017, S. 487 (388).

175 BVerfGE 150, 1 (97); 166, 196 (253); *Jarass*, in: Pieroth/Jarass (Hrsg.), 18. Aufl. 2024, Art. 20 Rn. 76; *Kalscheuer/Jacobsen*, DÖV 2018, S. 523 (525).

176 *Bundesamt für Sicherheit in der Informationstechnik*, Transparenz von KI-Systemen, 2024, S. 14 f.

177 Mit Blick auf die Schweizer Rechtslage empfehlen auch *Braun Binder/Obrecht*, AJP 2024, S. 1069 (1078 f.) eine formell-gesetzliche Grundlage, z. B. im Schweizer Bundesgesetz über den Datenschutz (DSG).

178 Dazu *Siegel*, NVwZ 2024, S. 1127 (1134).

lösung richtet sich nach der grundgesetzlichen Kompetenzordnung (Art. 70 ff. und 83 ff. GG).

aa) Grundsatz der getrennten Verwaltungsräume. Eine spezielle Gesetzgebungskompetenz für die Regulierung informationstechnischer Systeme findet sich im Grundgesetz nicht[179]. Art. 91c Abs. 5 GG adressiert die digitale Verwaltungstransformation im föderalen Staat. Die Regelungsbefugnis des Bundes lässt sich für die Errichtung eines KI-Transparenzregisters jedoch allenfalls beschränkt nutzbar machen. Denn sie bezieht sich nur auf den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern und nicht auf die daran anschließenden Verfahren. Die Gesetzgebungskompetenz erlaubte es somit lediglich, den KI-Einsatz i. R. d. Antragsverfahren über den Portalverbund zu regulieren und deckte damit nur einen kleinen Ausschnitt der KI-Potenziale in der öffentlichen Verwaltung ab.

Folglich ist entscheidend, wer allgemein für die Regelung der Organisation und der Verfahren innerhalb der Verwaltung zuständig ist. Grundsätzlich sind die Verwaltungsräume von Bund und Ländern getrennt[180]. Zwar kann der Bund nicht nur für seine eigene Verwaltung Vorgaben aufstellen[181]. Aber für die Landesebene kann er lediglich Regelungen erlassen, insoweit die Landesbehörden Bundesrecht in landeseigener Verwaltung oder in Bundesauftragsverwaltung vollziehen und sich dies aus Art. 84 Abs. 1 und Art. 85 Abs. 1 S. 1 GG oder als Annexkompetenz aus den Art. 72 ff. GG ergibt[182]. Dem Bund ist es mithin *de constitutione lata* versagt, ein zentrales KI-Transparenzregister zu schaffen, das für die gesamte öffentliche Verwaltung verpflichtend ist.

bb) Staatsvertrag als Registergrundlage. Ohne Verfassungsänderung wäre ein ebenenübergreifendes Pflichtregister nur auf Grundlage eines Staatsvertrags zwischen Bund und Ländern möglich[183]. Dieser genügte im Gegensatz zu einer bloßen Verwaltungsvereinbarung dem Vorbehalt des Gesetzes. Die Zustimmung zu einem Staatsvertrag erfolgt zwar nur durch Parlamentsbeschluss und nicht durch ein förmliches Gesetz, aber erhebt dessen normativen Teil in Gesetzesrang[184]. Über einen Staatsvertrag ließe sich sowohl ein einheitliches Register als auch ein Registerportal errichten. Letzteres setzte dann voraus, dass Bund und Länder zugleich eigene Register einführten. Kommt weder eine Verfassungs-

179 *Martini/Botta*, MMR 2024, S. 630 (634).

180 *Schliesky*, NVwZ 2019, S. 693 (695); *Siegel*, § 50 Trennung der Verwaltungsräume, Verwaltungszusammenarbeit, Gemeinschaftsaufgaben, in: Stern/Sodan/Möstl (Hrsg.), Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, Band 2, 2. Aufl. 2022, Rn. 1.

181 Diese Kompetenz folgt aus den Art. 70 ff. i. V. m. Art. 86 ff. GG und den Grundsätzen über die Zuständigkeit kraft Sachzusammenhangs. Siehe *Schmitz*, in: Stelkens/Bonk/Sachs (Hrsg.), 10. Aufl. 2023, § 1 Rn. 34; *Schwarz*, in: Fehling/Kastner/Störmer (Hrsg.), 5. Aufl. 2021, Einleitung zum VwVfG, Rn. 38; vgl. BVerfGE 26, 338 (369).

182 *Schmitz* (Fn. 181), § 1 Rn. 35 f.; *Schwarz* (Fn. 181), Einleitung zum VwVfG, Rn. 38.

183 Ob Bund und Länder einen derartigen Staatsvertrag schließen wollen, obliegt ihrer freien Entscheidung und ist nicht erzwingbar. Vgl. *König*, DÖV 2022, S. 189 (192).

184 BVerfGE 37, 191 (197); *Jarass* (Fn. 175), Art. 20 Rn. 77; vgl. *Böllhoff/Botta*, NVwZ 2021, S. 425 (429 f.); *Schulz/Tallich*, NVwZ 2010, S. 1338 (1339).

änderung noch ein Staatsvertrag zustande, kann ein zentrales Register nur ein freiwilliges Angebot sein.

2. Anforderungen an den Registerinhalt

Das Verfassungsrecht stellt nicht nur Anforderungen an die rechtliche Grundlage eines KI-Transparenzregisters, sondern auch an seinen Inhalt.

a) Klarheitsgebot. Aus dem Rechtsstaatsprinzip des Art. 20 Abs. 3 GG folgt, dass der Staat, wenn er seine Bürger informiert, dies klar und verständlich tun muss[185]. Es ist zwar nicht erforderlich, dass wirklich jeder Bürger den Inhalt des KI-Transparenzregisters abschließend erfassen kann. Das im Register zur Verfügung gestellte Wissen muss aber jedenfalls dem Bevölkerungsdurchschnitt verständlich sein[186]. Die Informationsdarstellung darf daher keine Fehlinterpretationen begünstigen (z. B. durch eine undurchsichtige Kategorisierung der KI-Systeme oder eine irreführende Zweckbeschreibung). Auch ein „Information Overload", d. h. eine intellektuelle Überforderung durch ein Zuviel an Informationen[187], kann mit dieser Anforderung kollidieren, wenn er es dem Durchschnittsempfänger unmöglich macht, den wesentlichen Informationsgehalt des Registers zu erfassen[188].

b) Grenzen der Transparenz. Bei der Ausgestaltung des KI-Transparenzregisters ist zu beachten, dass den Veröffentlichungsmöglichkeiten auch Grenzen gesetzt sind. Der parlamentarische Gesetzgeber kann insbesondere keinen Zugang zu Informationen eröffnen, die ihm selbst vorenthalten sind[189].

Zum einen sind öffentliche Belange – insbesondere das Staatswohl – zu beachten. Eine Legaldefinition des Staatswohls fehlt zwar[190]. Darunter fallen aber insbesondere der Schutz der Wehr- und Bündnisfähigkeit sowie der Schutz der Funktionsfähigkeit der Nachrichtendienste[191]. Gerade im Zuständigkeitsbereich der Innen- und Verteidigungsressorts sind der KI-Transparenz folglich Grenzen zu setzen. Das gilt auch vor dem Hintergrund, dass gegenüber Bürgern ein strengerer Geheimschutz als gegenüber dem Parlament geboten ist, da sich nur letzteres darauf berufen kann, sich das Staatswohl mit der Regierung zu teilen[192]. Gleichzeitig können derartige Arkanbereiche im freiheitlichen Verfassungsstaat nur Ausnahmen darstellen und sind daher eng zu begreifen[193].

---

185 Siehe grundlegend zum Klarheitsgebot *Mast*, Staatsinformationsqualität, 2020, S. 295 ff.

186 Vgl. *Mast* (Fn. 185), S. 308; *Schoch*, § 37 Entformalisierung staatlichen Handelns, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik, Band III, 3. Aufl. 2005, Rn. 143.

187 *Botta*, DÖV 2023, S. 421 (428).

188 Vgl. *Hill*, DÖV 2014, S. 213 (213 ff.); *Mast* (Fn. 185), S. 322.

189 *Schnabel/Freund*, DÖV 2012, S. 192 (195).

190 *Holzner*, DÖV 2016, S. 668 (671); *Manns*, ZRP 2024, S. 54 (54); vgl. BVerfGE 124, 78 (123).

191 *Warg*, NVwZ 2014, S. 1263 (1267); vgl. *Holzner*, DÖV 2016, S. 668 (671).

192 Vgl. BVerfGE 124, 78 (124); 137, 185 (241); *Warg*, NVwZ 2014, S. 1263 (1268).

193 *Barczak*, DÖV 2020, S. 997 (1000).

Zum anderen können auch grundrechtlich geschützte Interessen (neben dem Schutz personenbezogener Daten insbesondere auch Betriebs- und Geschäftsgeheimnisse) der Veröffentlichung im Transparenzregister entgegenstehen[194]. Folglich ist es (auch) aus Transparenzgründen empfehlenswert, wenn die öffentliche Verwaltung vorrangig auf Open-Source-Software setzt. Allerdings begründen die Interessen Dritter keine absoluten Hürden für eine Informationsgewährung[195]. Dass der Gesetzgeber in § 6 S. 2 IFG Bund für Betriebs- und Geschäftsgeheimnisse eine abweichende Regelung getroffen hat (kein Informationszugang ohne Einwilligung des Betroffenen), ist grundrechtlich nicht zwingend[196]. Im Sinne eines möglichst hohen KI-Transparenzniveaus sollte der Gesetzgeber in der Registergrundlage Abwägungsvorbehalte verankern, um Interessenkollisionen einzelfallabhängig lösen zu können. Dabei kann er sich am Transparenzrecht der Länder orientieren[197].

IV. Aufsicht über ein KI-Transparenzregister

Die Errichtung eines nationalen KI-Transparenzregisters für die öffentliche Verwaltung ist untrennbar mit der Frage verbunden, welche Stelle künftig für die Überprüfung seiner ordnungsgemäßen Führung verantwortlich sein soll.

Auf Unionsebene verwaltet grundsätzlich die EU-Kommission die Datenbank (Art. 71 Abs. 1 S. 1 KI-VO). Zudem verfügt der Europäische Datenschutzbeauftragte als zuständige Marktüberwachungsbehörde (Art. 70 Abs. 9 KI-VO) über Aufsichts- bzw. Sanktionsbefugnisse, insoweit unionale Stellen ihren Registrierungspflichten nicht nachkommen. So kann er bspw. die Verwendung des KI-Systems (vorübergehend) untersagen und/oder Geldbußen verhängen (vgl. Art. 100 i. V. m. Art. 26 Abs. 8 S. 1 KI-VO). Auch mitgliedstaatliche Behörden müssen mit Reaktionen der nationalen KI-Aufsicht rechnen, wenn sie die Registrierungspflichten nicht erfüllen, wozu ebenfalls Sanktionen zählen (Art. 99 Abs. 4 lit. e i. V. m. Art. 26 Abs. 8 S. 1 KI-VO)[198]. Die Ausgestaltung der Sanktionen und Durchsetzungsmaßnahmen liegt indes beim nationalen Gesetzgeber. Im Unterschied zum Datenschutzrecht (vgl. Art. 83 Abs. 7 DSGVO) kann dieser allerdings nur über das „Wie" und nicht das „Ob" von Geldbußen gegen Behörden entscheiden[199].

Diese Aufgabenteilung ließe sich für ein nationales KI-Transparenzregister nachbilden. Danach wäre die Exekutive – auf Bundesebene z. B. das BMI – dafür verant-

194 *Schoch*, ZGI 2023, S. 251 (251 f.); vgl. *Holzner*, DÖV 2016, S. 668 (671); *Schwill*, NVwZ 2019, S. 109 (110 ff.).

195 *Kloepfer/Greve*, NVwZ 2011, S. 577 (578); *Martini* (Fn. 20), S. 342.

196 Vgl. *Guckelberger*, in: Gersdorf/Paal (Hrsg.), BeckOK InfoMedienR, 46. Ed. (Stand: 1. 11. 2024), § 6 IFG Rn. 15.

197 Verwiesen sei z. B. auf die §§ 4 bis 7 Hamburgisches Transparenzgesetz.

198 Der deutsche Wortlaut des Art. 26 Abs. 8 S. 1 KI-VO ist irreführend, da er fälschlicherweise nahelegt, dass die Registrierungspflichten nur für Stellen der Union gelten. Siehe oben II. 1. b) aa).

199 *Nemitz*, in: Martini/Wendehorst (Hrsg.) 2024, Art. 99 Rn. 85. Im Datenschutzrecht hat der deutsche Gesetzgeber entschieden, dass Aufsichtsbehörden keine Geldbußen gegen andere Behörden verhängen können (§ 43 Abs. 3 BDSG).

wortlich, das Register zu errichten und zu führen. Gleichzeitig könnte eine unabhängige Aufsichtsstruktur zur Registerüberwachung geschaffen werden[200]. Dies dürfte das Vertrauen in das Register und damit den staatlichen KI-Einsatz zusätzlich stärken. Für die Registeraufsicht sollten dieselben nationalen Behörden zuständig sein, die auch für die Einhaltung des Art. 26 Abs. 8 S. 1 KI-VO durch staatliche Stellen Sorge tragen müssen.

Eine unabhängige Registeraufsicht kann indes *de constitutione lata* mit der föderalen Staatsordnung kollidieren. Denn verständigten sich Bund und Länder tatsächlich mittels Staatsvertrags darauf, dass der „Marktplatz der KI-Möglichkeiten" als zentrales Transparenzregister dienen soll[201], läge es auf den ersten Blick nahe, auch die Registeraufsicht bei einer Bundesbehörde zu bündeln. Bei näherem Hinsehen offenbart sich jedoch, dass die damit einhergehenden Kontrollbefugnisse, die sogar die Verhängung von Bußgeldern für nicht oder fehlerhaft registrierte KI-Systeme umfassen könnten, eklatant in die Staatlichkeit der Länder eingriffen[202]. Das KI-Transparenzregister müsste daher als Verbundlösung ausgestaltet werden, um eine föderal organisierte Registeraufsicht zu ermöglichen und verfassungsrechtliche Fallstricke zu vermeiden. Jedes der (siebzehn) miteinander verknüpften Register ließe sich dann einer eigenen unabhängigen (Bundes- bzw. Landes-)Behörde unterstellen, sodass die Hoheitsrechte aller Beteiligten gewahrt blieben.

V. Fazit und Ausblick

Künstliche Intelligenz hat das Potenzial, zur Schlüsseltechnologie für die digitale Verwaltungstransformation zu werden. Wenn aus Leuchtturmprojekten Standardanwendungen werden, verspricht dies jedoch nicht nur eine effizientere Verwaltung, sondern birgt auch immer größere Risiken für die Bürger. Eine besondere Gefahr geht dabei vom bestehenden Transparenzdefizit – sowohl für die Bevölkerung als auch für die Verwaltung selbst – aus. Außerhalb der jeweiligen Behörde ist oftmals nicht (ausreichend) bekannt, wo und zu welchem Zweck ein KI-System zum Einsatz kommt. Das Wissen über die verwendeten Systeme und ihre Funktionsweise ist indes zentral für die Akzeptanz ihres Einsatzes, ihre Kontrolle, den Grundrechtsschutz und einen zwischenbehördlichen Erfahrungsaustausch.

Um die Transparenz über den staatlichen KI-Einsatz zu erhöhen, empfiehlt sich die Einführung eines öffentlichen Registers, wie es z. B. in den Niederlanden schon existiert. Auch auf Unionsebene entsteht mit der Datenbank nach Art. 71 KI-VO ein vergleichbares Instrument. Öffentliche Stellen müssen in der Datenbank über den Einsatz bestimmter Hochrisiko-KI-Systeme informieren und insbesondere eine Zusammenfassung der Grundrechte-Folgenabschätzung (GRFA) nach Art. 27 KI-VO zur Verfügung stellen. Ein abschließendes Bild vom staatlichen KI-Einsatz kann die Datenbank jedoch nicht vermitteln. Neben ihrem begrenzten Anwendungs-

200 Empfehlenswert wäre zudem ein jährlicher Bericht, der die Entwicklung der Registereinträge und damit auch des KI-Einsatzes aufzeigt.

201 Siehe oben III. 1. b) bb).

202 Vgl. *Martini/Botta*, MMR 2024, S. 630 (634).

bereich folgt dies insbesondere aus der fraglichen Relevanz der GRFA. Zwar setzt diese (nach der hier vertretenen Ansicht) eine vollständige Grundrechtsprüfung voraus, aber es ist zu befürchten, dass das Büro für Künstliche Intelligenz ihren Inhalt auf ein Minimum reduzieren wird. Einem höheren Transparenzniveau steht die KI-VO derweil nicht entgegen, da sie nicht abschließend vorgibt, wie die Mitgliedstaaten die Verwendung von KI-Systemen in ihrer Verwaltung zu regeln haben. Dafür fehlt der Union schon die Kompetenz.

Es steht dem deutschen Gesetzgeber daher frei, ein eigenes KI-Transparenzregister zu errichten[203]. Erste (zaghafte) Schritte in diese Richtung ist das BMI mit seinem „Marktplatz der KI-Möglichkeiten" gegangen. Das darin integrierte Register weist jedoch nicht nur erhebliche Mängel in seiner rechtlichen Ausgestaltung auf (siehe oben III. 1. a)), sondern auch in Bezug auf sein Transparenzniveau (siehe oben I. 2. b)). Für seine Fortentwicklung ließe sich ein Vorbild an den Niederlanden nehmen[204]. Auch in Deutschland sollte eine (möglichst) zentrale und inhaltsreiche Datenbank entstehen, die nach einer Übergangszeit obligatorisch wird. Gleichzeitig zieht das geltende Verfassungsrecht einer umfassenden (und verpflichtenden) Zentralisierung klare Grenzen. Ein gemeinsames Pflichtregister von Bund und Ländern könnte *de constitutione lata* nur auf Grundlage eines Staatsvertrages entstehen. Um eine unabhängige Aufsicht über dieses Register zu ermöglichen, müsste ihm zudem eine föderale Verbundstruktur zugrunde liegen: d. h. Bund und Länder müssten jeweils eigene Register errichten und diese miteinander verknüpfen. Effizient wäre eine derartige Vorgehensweise allenfalls, wenn beide Staatsebenen die Register gemeinsam auf Open-Source-Basis (wie in den Niederlanden) entwickelten.

In Deutschland steht die Errichtung eines KI-Transparenzregisters damit unweigerlich vor denselben föderalen Herausforderungen wie die digitale Verwaltungstransformation insgesamt[205]. Perspektivisch sollten Bund und Länder daher nicht vor einer Verfassungsreform zurückschrecken[206]. Überlegenswert wäre es z. B., den Regelungsbereich des Art. 91c Abs. 5 GG zu erweitern[207]. Fest steht jedenfalls, dass der deutsche Bundesstaat nicht nur in Sachen Digitalisierung, sondern auch in Sachen Transparenz ein Update benötigt, wenn er die Funktionsfähigkeit seiner Verwaltung und das Vertrauen seiner Bürger gleichermaßen erhalten will.

---

203 Zugleich ist es empfehlenswert, die Register auf nationaler und unionaler Ebene zu vernetzen, um den Mehraufwand in den Behörden zu reduzieren und die Transparenz für die Bürger zu erhöhen.

204 Bei der Darstellung der Registerinformationen könnte Deutschland sogar neue Maßstäbe setzen. Das niederländische Register ist gegenwärtig ausschließlich textbasiert und dürfte daher für viele Bürger keinen niedrigschwelligen Informationszugang darstellen. Für einen schnellen Wissensgewinn könnten zusätzlich z. B. *Icons* helfen (vgl. *Botta*, DÖV 2023, S. 421 (428); *Martini* (Fn. 20), S. 188 f.). Bildliche Darstellungen können der Verständlichkeit jedoch auch entgegenwirken, wenn sie zu unbestimmt sind (*Mast* (Fn. 185), S. 316).

205 Siehe oben Fn. 4 und die Ausführungen unter III. 1. b).

206 Ebenso *Schulz*, NVwZ 2024, S. 1703 (1709).

207 Weitere Reformvorschläge finden sich bspw. bei *Martini/Botta*, NJW 2025, S. 1464 (1469).

Abstract

Artificial intelligence (AI) holds the potential to become the cornerstone of digital transformation in public administration. While the use of AI systems promises more efficient operations through automation, it also introduces significant risks, particularly concerning data protection and the equal treatment of individuals. One of the most pressing challenges is the existing lack of transparency – both for citizens and for the administration itself. Outside the responsible government agencies, it is often unclear where and for what purposes AI systems are used. However, awareness of the systems in use and their functioning is critical to fostering public acceptance, ensuring effective oversight, protecting fundamental rights, and facilitating cross-agency knowledge sharing.

To enhance transparency regarding state usage of AI, the introduction of a public register is advisable – similar to the system already in place in the Netherlands. In the Dutch "Algoritmeregister", government agencies are required to record the AI systems they use. The register provides key details such as the system's intended purpose, its application domain, and the potential impacts on citizens and businesses. In early 2025, the German Federal Ministry of the Interior and Community took the first tentative steps toward this direction with the "Marktplatz der KI-Möglichkeiten".

However, the establishment of a national AI transparency register for public administration raises significant legal considerations. The EU's AI Act establishes its own framework for AI transparency, which takes precedence over national laws. According to the AI Act, public authorities must disclose the use of specific high-risk AI systems in a central database (Article 71 AI Act) and, notably, provide a summary of the fundamental rights impact assessment (Article 27 AI Act). If the AI Act comprehensively regulates AI transparency within public administration, the creation of a national register could conflict with EU law. Even if EU law does not completely preclude the creation of such a register, the approach to its implementation must be in line with German constitutional law. Specifically, the principle of the "Vorbehalt des Gesetzes" (reservation of the law) and Germany's federal system of competences must be considered. This article explores these issues and outlines how the concept of a national AI transparency register can be legally implemented within the European multi-level system.