

§ 2

KI-Fibel – Eine kleine Werkzeugkunde für eine große Technik

A. Rollen und Regeln

I. Die Rollenverteilung im KI-Recht

Die KI-Verordnung legt insbesondere Pflichten für Anbieter und Betreiber von KI vor. 13
Aus dem vielfältigen Recht, das Menschen vor Verletzungen durch den Einsatz der KI als Werkzeug schützt, ergeben sich weitere Pflichten für die Nutzer von KI. Das KI-Gesetz regelt zunächst Pflichten für Anbieter von KI-Modellen und -Systemen.

1. Anbieter und Entwickler

Anbieter sind Hersteller und Entwickler von KI, setzen diese Produkte aber nicht 14
selbst ein. Das sind in der Regel große KI-Anbieter wie OpenAI, Meta und Google oder kleinere, wie Mistral oder andere staatliche oder private Einrichtungen. Darunter fallen auch KI-Systemanbieter wie Microsoft für den Copiloten, oder auch Anbieter von besonderen KI-Systemen mit besonderen Aufgaben und erweiterter Autonomie, sog. „KI-Agenten“.

2. Betreiber

Der Einsatz der Werkzeuge erfolgt durch Nutzer oder Verwender, die das KI-Gesetz 15
Betreiber nennt. Das ist faktisch jeder, der KI nicht ausschließlich zu privaten Zwecken eigenverantwortlich verwendet. Wer als Handwerker seine Mitarbeiter- oder Kunden per Sprach-KI anspricht oder sich einen Werbeflyer von einer Bild-KI erzeugen lässt, ist Betreiber, denn er verwendet ein KI-System für berufliche Zwecke. Betreiber von KI sind also in erster Linie Behörden und Unternehmen und Dienstleister. An sie richten sich die Pflichten für den Werkzeugeinsatz. Wer für ein Unternehmen oder eine Behörde oder einen Dienstleister arbeitet und im Auftrag des Arbeitgebers KI einsetzt, ist nicht Betreiber, sondern bloßer Anwender der KI. Das Gesetz nennt diesen Kreis „sonstige Dritte“. Als sonstiger Dritter ist man solange kein Betreiber von KI, wie man sich an den Auftrag des Arbeitgebers hält.

Das bedeutet: Der Chef legt als Betreiber der KI fest, ob und wozu das Werkzeug KI 16
im Unternehmen eingesetzt wird. Er legt auch fest, welche Aufgaben mit dem Werkzeug wahrgenommen werden dürfen und welche nicht. Dazu schaut er in die Betriebsanleitung und Nutzungsbedingungen des Werkzeugs KI und richtet den zulässigen Einsatz des Werkzeuges an dessen bestimmungsgemäßem Zweck aus. Diesen gibt er an die Beschäftigten weiter.

Beispiele. Mit dem Gabelstapler fährt man Paletten im Lager aus, aber nicht Tablett für 17
das Essen in der Kantine. Mit dem Dienstwagen werden nur Dienstfahrten erledigt, keine privaten Fahrten. Mit Allzweck-KI werden keine hochriskanten Aufgaben erledigt. Hochriskant sind etwa viele Aufgaben im Personalbereich. Nicht hochriskant und erlaubt ist es etwa, sich eine Anregung für eine Werbebotschaft geben zu lassen. Man darf aber keine Inhalte nutzen, die etwa gegen Datenschutz- oder Urheberrecht verstoßen.

3. Anwender

- 18 Die Beschäftigten sind nicht Betreiber, da sie KI nicht eigenverantwortlich nutzen. Das Gesetz bezeichnet sie als „sonstige Dritte“. Sie handeln für den Betreiber und in dessen Verantwortung. Nutzt ein Beschäftigter aber KI zu einem Zweck, den das Unternehmen untersagt hat, dann nutzt er KI eigenverantwortlich. Es wäre nicht fair, dem Chef die Verantwortung für den bewussten Missbrauch eines Werkzeuges anzulasten, obwohl er diesen Missbrauch verboten hat. Wenn ein Beschäftigter also eine Personalentscheidung mit einem GPAI-System vornimmt, obwohl das verboten ist, dann ist er und nicht mehr der Chef verantwortlich. Dann ist der Mitarbeiter Betreiber der KI.

4. Sonderproblem „Schatten-KI“

- 19 Es kommt vor, dass im Unternehmen keine Regelung zu KI getroffen wird, oder dass der Chef den Einsatz privater KI duldet, obwohl er die Software für das Unternehmen nicht angeschafft hat. In diesem Fall spricht man von Schatten KI. Duldet das Unternehmen den Einsatz privater KI, dann dürfte er Betreiber sein. Duldet er den Einsatz nicht, sondern hat ihn verboten und kann ihn nicht erkennen, dann ist der Beschäftigte Betreiber.

5. Private Tätigkeit unterfällt dem KI-Recht nicht

- 20 Wer KI für rein private Zwecke betreibt, ist nicht Betreiber von KI. Für ihn gilt das KI-Gesetz nicht. Wer sich als Privatperson medizinischen Rat per Sprachbot einholt, der handelt in jeder Hinsicht erlaubt, denn das KI-Recht gilt für ihn nicht und er ist auch nicht durch das sonstige Recht gebunden. Das Recht für Ärzte gilt nicht für ihn und auch die Pflicht nur Medizinprodukte zu verwenden, ist für Privatleute irrelevant.
- 21 Allerdings muss man als Privatperson aufpassen. Schulen, die Schülern die Verwendung eines Sprachbots zur Unterstützung bei den Hausaufgaben zur Verfügung stellen, sind Betreiber von KI-Systemen und müssen den Schülern KI-Kompetenz vermitteln. Schließlich sind Hausaufgaben keine Privatsache, sondern werden im Rahmen der staatlichen Schulpflicht erledigt.

II. Regeln und Fragen für den KI-Einsatz

1. Welche Zwecke darf man mit dem Werkzeug KI verfolgen?

- 22 Der grundlegende Ansatz für den KI-Einsatz und dessen Regeln sind nach der Risikopyramide denkbar einfach, fast ein Kinderspiel. Es ist wie am Strand. Im seichten Wasser schwimmen ist nicht riskant, da wo es tief ist, ist es hochriskant und nur für geübte Schwimmer erlaubt. In der Hai-Zone ist das Schwimmen verboten.

a) Verbote

- 23 Jeder, der KI nicht ausschließlich privat betreibt, prüft zunächst, ob der Zweck, den er mit der KI verfolgt, verboten ist. Diese Fälle fasst das KI-Gesetz in einem Artikel zusammen. Das wäre in einer Ampel Rot. Verbote finden sich in acht Bereichen:
1. schädigende unterschwellige Beeinflussung von Menschen,
 2. das Ausnutzen von schwachen und schutzbedürftigen Menschen,

3. die Benachteiligung wegen ihres Sozialverhaltens
4. das Auswerten des Verhaltens einer Person mit Blick auf deren künftige Strafbarkeit
5. das ungezielte Auslesen von Gesichtsbildern aus dem Internet
6. die Ableitung von Emotionen an Bildungseinrichtungen oder am Arbeitsplatz
7. die Kategorisierung nach sensiblen Eigenschaften, wie sexueller Ausrichtung
8. Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen – hier gibt es Ausnahmen zur Verbrechensbekämpfung

Betreiber müssen also darauf achten, nichts Verbotenes zu tun. Möchte eine Behörde etwa am Arbeitsverhalten eines Beschäftigten messen, ob dieser auf der Dienststelle zufrieden ist oder ob er traurig oder wütend ist, dann ist das grundsätzlich verboten. 24

b) Erlaubte, aber hochriskante Zwecke

Danach muss man schauen, ob der Zweck hochriskant ist. Wenn das so ist, dann braucht man ein besonderes Werkzeug. Die benutzte KI – das „One-Trick-Pony“ – muss in diesem Fall für den gefährlichen Einsatz entwickelt und angeboten sein und sie muss entsprechend der Vorgaben betrieben werden. Diese Zwecke benennt das KI-Gesetz in einer Anlage. Bei einer Ampel entspräche das Gelb. 25

Hochriskante Zwecke finden sich ebenfalls in acht Bereichen. Das sind Folgende: 26

1. KI zum Zwecke biometrischer Fernidentifizierung
2. KI-Systeme im Bereich der kritischen Infrastruktur, etwa im Straßenverkehr oder in der Energieversorgung
3. Zwecke im Bereich der beruflichen Bildung, insbesondere, wenn mit Hilfe von KI der Zugang zu Bildungseinrichtungen vermittelt werden soll oder wenn KI für die Bewertung von Lernergebnissen eingesetzt werden soll
4. KI für Entscheidungen, die Bedingungen von Beschäftigungsverhältnissen beeinflussen
5. KI zum Zugang zu grundlegenden privaten und öffentlichen Leistungen, etwa für Unterstützungsleistungen einschließlich Gesundheitsleistungen, Kreditwürdigkeit, Finanzbetrug, Preisbildung bei Versicherungen, Priorisierung von Rettungseinsätzen und Triage in der medizinischen Notfallversorgung
6. KI-Einsatz durch Strafverfolgungsbehörden
7. KI-Systeme zur Einreise von Migrant*innen
8. KI-Systeme zum Einsatz in Justizbehörden zur Unterstützung bei der Rechtsanwendung und zum Einsatz bei Wahlen

Aber Vorsicht wegen der Keule des Gesetzes. Nimmt man anstelle des hier erforderlichen „One-Trick-Pony“, also eines Spezialwerkzeugs, das „Schweizer Taschenmesser“, also eine KI für allgemeine Zwecke, die man per Sprachbefehl eigenständig zum Spezialwerkzeug gemacht hat, obwohl deren Anbieter das weder will noch weiß, entsteht ein unzumutbarer Zustand. Dann muss man die Pflichten des Anbieters des zweckveränderten Werkzeugs übernehmen. 27

c) Das Allermeiste ist erlaubt

Für alles, was weder für verbotene noch für hochriskante Zwecke eingesetzt wird, gelten wenige Vorgaben aus dem KI-Recht. Denn diese Zwecke, wohl die überwiegende Mehrzahl der Zwecke, sind risikolos. Hier kann ich das Taschenmesser GPAI nach Herzenslust nutzen. Die hier geltenden wenigen Pflichten dienen in erster Linie der Transparenz, so dass man etwa weiß, dass man mit einem Bot kommuniziert. Hier ist man im grünen Bereich. 28

- 29 Aber **Achtung**: Jeder – auch jeder private Betreiber – muss darauf achten, dass er mit dem Werkzeug KI kein sonstiges Recht verletzt. So ging es der Zeitschrift „Die Aktuelle“ noch bevor es das KI-Gesetz gab, als sie ein per Sprachbot geführtes Interview mit Michael Schumacher abdruckte.¹ Für das Persönlichkeitsrecht ist es belanglos, ob es mit KI oder auf andere Weise verletzt wird. Mit KI geht das nur sehr leicht.

2. Braucht man das Werkzeug KI für einen der Zwecke?

- 30 Deshalb sollte man sich gut überlegen, ob man KI als Werkzeug tatsächlich einsetzen muss, oder ob man darauf vielleicht verzichten soll, weil es ohne KI auch und vielleicht sogar besser geht. Viele Aufgaben, die eine Behörde oder ein Unternehmen verfolgt, können nämlich ohne KI erledigt werden. Manche Dinge kann KI zum Beispiel gar nicht. Dazu gehört etwa das schlichte Zählen von Zeichen, denn Zählen ist keine Frage der Wahrscheinlichkeit. Gab man frühen Versionen von Sprachmodellen auf, Zeichen in einem Dokument zu zählen, so variierten die Ergebnisse. Das ist nachvollziehbar, weil die hohe Wahrscheinlichkeit einer Anzahl von Zeichen in einem Text etwas anderes ist, als die präzise Zählung. Moderne Bots greifen unter der Oberfläche des Systems auf ein Programm zu, das nicht KI ist und deshalb zählen kann. Dann merkt man den Mangel nicht. Um das für den Einsatz passende Tool zu finden, sollte man folgende vier Fragen beantworten.

a) Welche Zwecke möchte man mit KI verfolgen?

- 31 Ist der Zweck im oben genannten Sinn nicht riskant, hochriskant oder verboten?
- 32 Geht es darum, am Arbeitsplatz, zum Beispiel im Callcenter, zu erfassen, ob die Beschäftigten emotional überlastet sind, ist das grundsätzlich verboten. Das KI-Recht verbietet die Ableitung von Emotionen am Arbeitsplatz nämlich grundsätzlich. Hier befindet man sich im Haifischbecken.
- 33 Geht es um Kunden, ist derselbe Zweck nur hochriskant, da sich das Verbot der Emotionserfassung nur auf den Arbeitsplatz und Bildungseinrichtungen bezieht. Möchte ich Emotionen von Kunden im Callcenter erfassen, etwa Wut, um sie besonders gut betreuen zu können, dann ist das nur hochriskant und unter strengen Voraussetzungen gestattet. Möchte man KI zur Auswahl oder Bewertung von neuem Personal für das Callcenter einsetzen, dann ist das auch nicht verboten, aber auch nicht risikolos, sondern hochriskant. In diesen Fällen befindet man sich in der Risikozone.
- 34 Soll die KI nur etwas übersetzen oder meine Produkte ordnen, eine Webeanzeige gestalten oder mir Strategien zur Kundengewinnung nennen, dann ist das auch mit Hilfe von GPAI erlaubt. Wir sind im risikoarmen Nichtschwimmerbecken.

b) Gibt es ein entsprechendes Tool?

- 35 Gibt es ein Tool, das hochriskante Aufgaben erfüllen kann. In vielen Fällen wird das Taschenmesser GPAI viele solcher Zwecke erfüllen können. Dennoch nimmt man das Produkt besser nicht dafür, denn dann schlägt die Keule des Gesetzes zu. Also muss man warten, bis das „One-Trick-Pony“ verfügbar ist.

1 Dazu <https://www.tagesschau.de/inland/die-aktuelle-fake-interview-schumacher-101.html> (zuletzt abgerufen am 15.9.2025).

c) Ist das Produkt für die ausgewählten Zwecke inhaltlich und rechtlich geeignet?

Wichtig ist es, sich klarzumachen, ob man KI auf eigenen Servern betreiben soll oder will. Das ist teuer, aber man ist Herr des Geschehens mit Blick auf die Daten, auf die das System zugreifen kann. Man vermeidet ungewollte Datentransfers, kann für die Einhaltung des Datenschutzes und der Datensicherheit geradestehen. Der Nachteil ist, dass man viel Fachwissen braucht. Die Alternative ist eine lizenzierte Version einer KI, bei der man die Einhaltung des Rechts durch den Anbieter vertraglich vereinbaren kann. Auf keinen Fall sollte man eine Version nutzen, die kostenlos ist, denn hier hat man in der Regel keine hinreichende Kontrolle. Ausnahmsweise kann eine vertrauenswürdige kostenlose Variante gut sein. Die EU bietet etwa einen KI-Übersetzer an, der gut und rechtlich einwandfrei ist. 36

d) Sind alle Pflichten als Betreiber und Anwender nach KI-Recht und sonstigem Recht erfüllt?

Im vierten Schritt muss man sich fragen, ob alle Pflichten für den Betrieb und Einsatz der konkreten KI erfüllt sind. Wer ein KI-System einsetzt, um im Call-Center das Wohlbefinden seiner Kunden per Biometrie-KI zu ermitteln, muss sich nicht nur fragen, ob er dafür ein geeignetes KI-System einsetzt. Die Frage lautet, ob eine angemessene Kundenbetreuung im Callcenter diese Datenverarbeitung wirklich erforderlich macht. Hier kann der Einsatz auch am Datenschutzrecht scheitern. 37



Abbildung 3: Sakurai, Kontrolle

B. Ein „einfacher“ Anwendungsfall

- 38 Der Einsatz von Sprachmodellen soll auch in der Verwaltung durch das KI-Gesetz mit einem beachtlichen Pflichtenheft versehen werden, das die Behörden rund um das neue Digitalministerium bei den genannten Aufgaben berücksichtigen müssen. Konstruieren wir einen lebensnahen Fall, den ich schon gemeinsam mit den KI-Experten Kristin Benedikt, Moritz Köhler und Markus Wünschelbaum in der F.A.Z. beschrieben habe.²
- 39 Was verlangt das Recht in der Praxis, wenn man zum Beispiel einen KI-Sprachassistenten in einer deutschen Verwaltungsbehörde einsetzen möchte, der aus einer Vielzahl von Anträgen auf Arbeitslosengeld weniger erfolgversprechende aussortieren soll? Der Assistent arbeitet auf Basis eines Sprachmodells, das von einem privaten Unternehmen in jahrelanger Arbeit entwickelt wurde. Das Modell wurde mit Texten trainiert. Mit jedem eingespielten Textbaustein hat es die Parameter seiner Wahrscheinlichkeitsberechnungen angepasst. Aufgrund dieser Berechnungen ist es nunmehr in der Lage, die in einem vorgegebenen Kontext wahrscheinlichste Wortfolge auszuspielen. Das Sprachmodell ist für keinen spezifischen Anwendungszweck entwickelt worden. Es ist von seinem Entwickler und Anbieter auch nicht als Wissensdatenbank konzipiert. Vielmehr soll das Modell als Basis einer Vielzahl von KI-Systemen Anwendung finden und für unbestimmt viele Einsatzzwecke sinnvoll klingende Wortfolgen erzeugen. Diese Simulation von Sprache erzeugt überzeugend anmutende Sinnzusammenhänge.
- 40 Der Entwickler des Sprachmodells bietet dieses nunmehr einem Softwareentwickler an, der es in eine konkrete Anwendung integriert, indem er ihm eine Prägung für den anvisierten Einsatzzweck auf den Weg gibt. In unserem Beispiel könnte der Softwareentwickler das Modell etwa darauf trainieren, Massen von Verwaltungsvorgängen zu Anträgen auf Arbeitslosengeld für die Agentur für Arbeit zu analysieren und Bewilligungs- und Ablehnungsmuster nachzuzeichnen. Hierzu füttert er das Modell mit einer Vielzahl entsprechender Dokumente und bringt ihm dadurch bei, welche Schlagworte es bei der Analyse zu beachten hat. Daneben entwickelt er eine Benutzeroberfläche für die Verwaltungsmitarbeiter. So entsteht ein generatives KI-System, also ein KI-System, das in der Lage ist, verschiedene Inhalte (z.B. Texte, Bilder, Videos) herzustellen.
- 41 Anbieter generativer KI-Systeme müssen nach der KI-VO stets besondere Transparenzpflichten erfüllen. Sie müssen dafür sorgen, dass ihre Systeme die künstliche Erzeugung der Inhalte erkennbar machen.
- 42 Das weitere Pflichtenprogramm ist abhängig von der Frage, ob das System im Einsatzkontext hochriskant ist. Der Katalog der Hochrisiko-KI-Systeme nennt unter anderem Systeme, die von Behörden eingesetzt werden sollen, um zu beurteilen, ob jemand Anspruch auf eine öffentliche Unterstützungsleistung, beispielsweise Arbeitslosengeld, hat. Trainiert der Softwareentwickler den Sprachassistenten auf einen der aufgelisteten Fälle und bietet ihn entsprechend auf dem Markt an, muss er zusätzliche Pflichten erfüllen. Er hat dann etwa bestimmte Vorgaben zu den Trainingsdatensätzen zu beachten und muss das System so programmieren, dass ein Mensch dessen Einsatz

2 Benedikt/Köhler/Schwartmann/Wünschelbaum F.A.Z. v. 18.3.2024, S. 18.

beaufsichtigen kann. Die Erfüllung dieser Pflichten ist mit erheblichen Kosten verbunden. Um diese Kosten zu sparen, können die Anbieter von Sprachassistenten deren Einsatz zu hochriskanten Zwecken in ihren Nutzungsbedingungen ausschließen. Dazu können sie etwa entsprechende Klauseln in die Lizenzverträge mit den Behörden oder Unternehmen aufnehmen, welche die Systeme als Betreiber einsetzen wollen.

Der Softwareentwickler im genannten Beispiel könnte also festlegen, dass sein System zwar auf die Analyse von Dokumenten programmiert, allerdings nicht dazu gedacht ist, Arbeitslosengeldanträge zu bearbeiten. Setzt die Behörde das System entgegen dieser Vorgabe doch zu einem solchen Zweck ein, geht die Anbieterrolle mit allen daran anknüpfenden Pflichten wegen der in Teil 3 beschriebenen „Keule des Gesetzes“ auf sie über. Das führt dazu, dass die Anbieterpflichten der KI-VO unter Umständen an Akteuren mit deutlich weniger Fachkenntnis und finanzieller Ausstattung hängen bleiben. Behörden sollten bei der öffentlichen Vergabe darauf achten, nur KI-Systeme zu beschaffen, die von den Anbietern hinsichtlich ihres Einsatzzwecks bereits spezialisiert und an die Anforderungen für Hochrisiko-KI-Systeme angepasst wurden. **43**

In die Leistungsbeschreibung gehören daher alle Anbieterpflichten nach der KI-VO. Die Anbieter werden sich ihre besondere Verantwortlichkeit von den Betreibern zwar teuer bezahlen lassen. Die Spezialisierung durch die Behörde ist aber mit Kosten und Mühen verbunden, die regelmäßig nicht mehr im Verhältnis zum Nutzen des Hochrisiko-KI-Systems stehen dürften. Alle Anwendungen, die oben beschrieben wurden müssen, müssen gewissenhaft daraufhin überprüft werden, dass ihre Anbieter gerade für den hochriskanten Einsatz einstehen und es sich bei dem Angebot nicht um ein GPAI System handelt. Hier gilt es, das Kleingedruckte der Nutzungsbedingungen der KI genau zu lesen. **44**

Unabhängig von den Anbieterpflichten treffen die Behörde aber insbesondere in ihrer Eigenschaft als Betreiberin eines Hochrisiko-KI-Systems Pflichten. Der größte Teil dieser Pflichten gilt für private und öffentliche Stellen gleichermaßen. So müssen Betreiber stets den Einsatz der KI durch die Beschäftigten überwachen und Vorfälle mit erheblichen Auswirkungen melden. Dabei ist sicherzustellen, dass der Sprachassistent nur nach Maßgabe seiner Gebrauchsanweisung verwendet wird. **45**

Das dürfte in der Praxis umfangreiche Maßnahmen der Behördenleitung erfordern. Insbesondere ist die zweckgemäße Verwendung schwer zu greifen. Sie ergibt sich aus den Maßgaben des Anbieters, einschließlich des spezifischen Kontexts und den Nutzungsbedingungen sowie der Gebrauchsanweisung im Werbe- oder Verkaufsmaterial. Wann stimmt die Verwendung eines KI- Systems nicht mehr mit dem beabsichtigten Zweck überein, der sich aus vernünftigerweise vorhersehbarem menschlichem Verhalten oder der Interaktion mit anderen Systemen, einschließlich anderen KI-Systemen, ergeben kann? **46**

Die hierzu erforderlichen umfangreichen Schulungen der Behördenmitarbeiter sind nicht nur zweckmäßig, sondern nach der KI-VO verpflichtend vorgesehen. Behörden, wie alle Betreiber von KI-Systemen, müssen für den Betrieb der generativen KI-Systeme einstehen, die sie in ihre behördlichen Anwendungen integrieren. Das heißt, sie müssen das komplexe und teilweise nicht einsehbare Gefüge eines Sprachassistenten verstehen und ihr Wissen sowie Nichtwissen transparent vermitteln. Das wirft weitere **47**

Fragen auf: Wie verantwortet man halluzinierendes „Verhalten“ der autonomen Maschine, wenn deren Ursache nicht erkennbar ist? Wie sollen Verwaltungsmitarbeiter diese nicht erlaubten Abweichungen des KI-Systems erkennen und einschätzen – wie soll eine Kontrolle durch den Arbeitgeber aussehen? Damit haben wir in den Teilen zwei bis vier dieses Buches befasst.

- 48** Die hinter diesen Vorgaben stehenden Fragen um den verantwortungsvollen, risikogerechten Einsatz von KI-Systemen gipfeln bei öffentlichen Stellen in einer weiteren Pflicht: der Grundrechte-Folgenabschätzung. Der Gesetzgeber fordert öffentliche Stellen auf, den Wald vor lauter Bäumen nicht aus den Augen zu verlieren. Die zahlreichen Dokumentations-, Berichts, und Meldepflichten über das „Wie“ des Einsatzes sollen öffentliche Stellen nicht davon ablenken, „ob“ der konkrete Einsatz grundrechtskonform ist. Die Grundrechte-Folgenabschätzung soll die Verwaltung nachdenklich stimmen, sie zum Innehalten bringen: Welche Risiken sind mit einem staatlichen KI-Einsatz verbunden?
- 49** Diese Pflicht trifft nicht ausschließlich Behörden, sondern den gesamten öffentlichen Sektor. Erfasst sind alle öffentlichen Stellen, Einrichtungen, öffentliche Unternehmen aber auch private Anbieter, die öffentliche Aufgaben erfüllen. Ob der KI-Einsatz zur öffentlichen Aufgabenerfüllung von einer Gemeinde, Hochschule, privatem Krankenhaus oder Energieversorger vorgenommen wird, ist nicht entscheidend. Zu prüfen sind potenzielle Folgen für Grundrechte, indem relevante Zielgruppen für die Anwendung festgelegt und Risiken für diese Zielgruppen bewertet werden. Wenn die Zielgruppe gefährdet sein könnte, muss ein System zur menschlichen Überprüfung der KI-Anwendung festgelegt werden. Für den Fall einer Realisierung der gelisteten Risiken muss schon vorab festgelegt sein, wie mit Grundrechtseingriffen umzugehen ist: Die öffentliche Stelle muss in der Lage sein, auf Beschwerden hin korrigierend einzugreifen und das KI-System präventiv zu übersteuern.
- 50** Sich Bewusstsein über die Risiken des KI-Einsatzes zu verschaffen bedeutet auch gewissenhafte Prüfung und für den grundrechtsgebundenen Staat im Zweifel Zurückhaltung: Behörden sind verpflichtet zu wissen, welche Risiken aus Nichtwissen folgen. Wir haben es schließlich mit einem autonomen Werkzeug zu tun. Gegenwärtige Sprachmodelle können nicht aufzeigen, wodurch ein bestimmtes Ergebnis verursacht worden ist. Weshalb die vom Sprachassistenten ausgegebene Wortfolge im konkreten Fall gerade so erfolgt ist, kann der Anwender nicht nachvollziehen – er sieht nur die Ausgabebox. Auch der Anbieter kann dies allenfalls begründet vermuten. Der Einsatz solcher Technologien bedarf daher einer gründlichen Abwägung und Expertise. Einerseits muss erwogen werden, ob bei einschneidenden Lebensereignissen wie staatlichen Prüfungen, der Beantragung sozialer Leistungen zur Existenzsicherung oder der Frage über den Zugang zur Daseinsvorsorge dieser Grad an Nichtwissen über die Entscheidungsursache akzeptabel ist. Andererseits muss sichergestellt sein, dass die KI Werkzeug bleibt und nicht die Entscheidung ersetzt – im Einzelfall durch den menschlichen Eingriff.
- 51** Letzteres ist auch datenschutzrechtlich geboten: Der Europäische Gerichtshof hat 2023 entschieden, dass Algorithmen nicht das letzte Wort haben dürfen: Trifft am Ende die Maschine und nicht der Mensch die maßgebliche Entscheidung, ist das unzulässig – Ausnahmen gibt es etwa, wenn der Betroffene dem ausdrücklich zustimmt oder ein Gesetz das vorsieht.

Ob alles richtig gemacht wurde, überprüfen insbesondere Gerichte. Hat der KI-Assistent den Antrag auf Arbeitslosengeld abgelehnt, hat der Bürger das Recht, diese Entscheidung gerichtlich überprüfen zu lassen. Das Gericht prüft dabei nicht nur, ob der Antrag zu Recht abgelehnt wurde, sondern auch den Weg zur Entscheidung. Denn es könnte sein, dass Antragsunterlagen fehlerhaft nicht geprüft wurden, ein atypischer Fall von der KI nicht erkannt wurde oder die Behördenentscheidung schlichtweg nicht begründet wurde. Behördliche KI-Systeme müssen daher sowohl für den Bürger als auch die Justiz transparent sein. Sind sie das nicht, geht dies zu Lasten der Behörde, die das intransparente KI-System einsetzt. Es wäre kontraproduktiv, wenn öffentliche Stellen KI-Systeme zur Entlastung einsetzen, die Gerichte hingegen belastet werden, weil die behördlichen KI-Entscheidungen massenhaft angefochten werden. **52**