

# Rechtlich gesehen

## Herausforderungen beim Einsatz von KI in Organisationen

Susanne Grimm

*Viele Organisationen setzen künstliche Intelligenz (KI) bereits in ihrem Arbeitsalltag ein, andere stehen vor einer Einführung von KI-Systemen. Dieser Schritt wirft rechtliche Fragen auf, die für Unternehmen von weitreichender Bedeutung sind – unabhängig davon, ob Software und Algorithmen dabei folgenschwere autonome Entscheidungen übernehmen oder lediglich «einfache» Anwendungen wie das Sprachmodell ChatGPT als Arbeitsmittel eingesetzt werden.*

Wer für die Gestaltung von Organisationen Verantwortung trägt oder diese berät, sollte die unterschiedlichen Rechtsgebiete im Blick haben, die beim Einsatz von KI potenziell betroffen sind. Dies gilt umso mehr, als viele diesbezügliche Rechtsfragen – datenschutzrechtlicher, urheberrechtlicher oder gar arbeitsrechtlicher Natur – noch nicht abschließend geklärt sind und sich aktuell dynamisch entwickeln. Unternehmen, die vermehrt auf den Einsatz von KI-Systemen setzen möchten, sollten daher die Risiken prüfen und auch ihren Mitarbeitenden klare Vorgaben machen, die arbeitsrechtlich fundiert sind.

### Haftungsfragen

Grundsätzlich stellen sich beim Einsatz künstlicher Intelligenz in Unternehmen zunächst Haftungsfragen. KI-Systeme können auf verschiedene Weise zu Schäden führen. Zum einen können sie Fehler bei der Verarbeitung von Daten machen, die sich auf ihre autonomen Entscheidungsfindungen und die erstellten Ergebnisse durchschlagen. Zum anderen können sie durch Manipulation der Lerndaten oder des Lernprozesses Schäden verursachen – damit sind Haftungsfragen gerade auch für Organisationen unmittelbar relevant, die KI-Systeme einsetzen, die mit eigenen Daten trainiert oder angelernt werden. Schließlich können KI-Systeme bei der weiteren Umsetzung von Entscheidungen Schäden verursachen. In allen Fällen stellt sich die Frage, wer für den entstandenen Schaden verantwortlich ist.

Wenn es um die Haftung für Entscheidungen von KI-Systemen geht, stößt das etablierte Haftungssystem des gesetzlichen Deliktsrechts an seine Grenzen. Denn KI-Systeme treffen ihre Ent-



Dr. Susanne  
Grimm

Rechtsanwältin und Fachanwältin  
für gewerblichen Rechtsschutz.  
Leiterin der Praxisgruppe IP & Media  
bei Rödl & Partner

**Kontakt:**  
susanne.grimm@roedl.com

scheidungen zwar auf der Grundlage von Daten und Algorithmen, die von Menschen erstellt wurden, aber sie treffen ihre Entscheidung autonom, also gerade ohne menschliche Einwirkung. Weil der fehlerhafte Einsatz von Systemen künstlicher Intelligenz zugleich schwerwiegende Folgen haben kann – man denke nur an Fehler beim autonomen Fahren – ist es unerlässlich, klare Regeln für die Haftung für Entscheidungen von KI-Systemen zu treffen. Nur so schafft man Rechtssicherheit. Die Europäische Union hat dazu verschiedene Gesetzesvorhaben auf den Weg gebracht, die noch 2024 in Kraft treten werden (siehe Kasten).

Im gegenwärtigen Haftungssystem ist es daher für den zu nächst beweibelasteten Geschädigten oft schwierig oder gar unmöglich, die ihm zustehenden Ansprüche durchzusetzen. Das fängt bereits bei der Benennung des richtigen Anspruchsgegners an und setzt sich über den Nachweis einer Sorgfaltpflichtverletzung bis hin zur Kausalität des erlittenen Schadens fort. Unternehmen, die KI-Systeme einsetzen, sollten daher die unterschiedlichen Haftungsperspektiven beachten:

Eine Möglichkeit, die Haftung für Schäden durch KI-Systeme durchzusetzen, ist den Hersteller des KI-Systems haftbar zu machen. Das entspricht dem Haftungsgrundsatz der Produkthaftung, also der Haftung des Herstellers oder Lieferanten für einen Schaden, der durch ein fehlerhaftes Produkt entsteht.

Sind an der Herstellung des KI-Systems mehrere Parteien beteiligt, etwa weil mehrere Unternehmen gemeinsam das System entwickelt und implementiert haben, kann es schwierig werden, den verantwortlichen Hersteller zu identifizieren. So erscheint es unbillig den Hersteller für einen Fehler im System haften zu lassen, der nicht durch ihn, sondern durch falsches Training der KI beim Betreiber verursacht wurde. Die Gründe für Schäden durch KI-Systeme können also vielfältig sein und erschweren oft eine klare Abgrenzung der Verantwortlichkeiten der Beteiligten.

Eine andere Möglichkeit besteht darin, den Benutzenden des KI-Systems haftbar zu machen. Die Haftung für unsachgemäße Verwendung von KI-Systemen kann dabei auf verschiedenen Ebenen auftreten. Dabei ist zunächst an das fehlerhafte Anlernen des Systems durch den Benutzenden zu denken. Daneben gibt es aber natürlich auch den Fall der Fehlentscheidung des KI-Systems. Als Beispiel sei auf die Verwendung von KI-Systemen in der medizinischen Diagnose verwiesen. Wenn ein Arzt/ eine Ärztin ein KI-System verwendet, um eine Diagnose zu stellen, und das System falsche Ergebnisse liefert, könnte der Arzt/ die Ärztin für den daraus resultierenden Schaden haftbar sein. Hier stellt sich allerdings für Organisationen die Frage, ob der Benutzende des KI-Systems überhaupt in der Lage ist, die möglichen Risiken und Schäden aus der Rückmeldung der KI zu erkennen und zu vermeiden. Das ist vor allem dann fraglich, wenn die Benutzenden die Entscheidungen des Systems nicht vollständig verstehen oder kontrollieren können, was bei komplexen KI-Entscheidungen in der Regel der Fall ist. Es ist daher wichtig, dass die Benutzenden von KI-Systemen ausreichend geschult wer-

den, und dass klare Richtlinien für die Verwendung von KI-Systemen in verschiedenen Branchen festgelegt werden, um die Haftungsfrage im Interesse aller Beteiligten rechtssicher zu regeln.

**Sie wollen den Artikel gerne weiterlesen?**

**Hier können Sie die komplette Ausgabe als ePaper lesen.**

## Neue Haftungsregeln für KI-Systeme



Die Europäische Union hat in den vergangenen Jahren verschiedene Gesetzesvorhaben auf den Weg gebracht, um den Einsatz von KI-Systemen weltweit zum ersten Mal gesetzlich zu regeln. Darunter den «Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz» (sog. **AI Act**) sowie eine Überarbeitung der Produkthaftungsrichtlinie und den Entwurf einer neuen Richtlinie zur KI-Haftung (sog. **AI Liability Directive**).

Bei der Richtlinie zur KI-Haftung handelt es sich, anders als der Name vermuten lässt, nicht um die Regelung von Haftungsansprüchen. Die Richtlinie fixiert vielmehr weitreichende Offenbarungspflichten für Beweismittel und etabliert ein System der Beweiserleichterung, um Anbieter und Betreiber von KI-Systemen mehr in die Pflicht zu nehmen. Nach den Vorschlägen der EU-Kommission sollen zwei Regelungen im Deliktsrecht verankert werden, nach denen die Sorgfaltpflichtverletzung und die Kausalität für den Eintritt des Schadens vermutet werden. Die Richtlinie sieht eine Umsetzungsfrist von 24 Monaten nach Inkrafttreten vor. Allerdings ist ein genauer Zeitpunkt des Inkrafttretens momentan noch nicht absehbar, sodass frühestens im Jahr 2026 mit der Geltung der KI-Haftungsrichtlinie gerechnet werden kann.

Der AI Act hat ein anderes Regelungsziel. Er dient als Grundlage der Regulierung von künstlicher Intelligenz und soll die Entwicklung, das Inverkehrbringen und die Verwendung von KI-Systemen in der EU regeln. Dabei wird ein risikobasierter Ansatz verfolgt. KI-Systeme werden in vier Kategorien unterteilt. Je höher die Kategorie ist, um so weitreichendere Regulierung erfährt das jeweilige KI-System. Der AI Act soll damit das Vertrauen der Gesellschaft in KI-Systeme stärken und gleichzeitig deren technische Entwicklung nicht blockieren. Nach zähem Ringen in den Trilog-Verhandlungen zwischen Europäischer Kommission, Europäischem Rat und Europäischem Parlament haben sich die Unterhändler am 8.12.2023 auf einen abschließenden Entwurf geeinigt, dem das Europäische Parlament und die Mitgliedsstaaten im Februar 2024 zugestimmt haben. In einer finalen Abstimmung im Europäischen Parlament im März 2024 wurde der Entwurf verabschiedet. Als nächsten Schritt wird die Verordnung voraussichtlich zwischen Mai und Juli 2024 im Amtsblatt der EU veröffentlicht und tritt 20 Tage später in Kraft. Sie gilt dann aber noch nicht in allen Punkten sofort, sondern mit Ausnahme bestimmter Verbote und Vorschriften für KI mit allgemeinem Verwendungszweck erst nach 24 Monaten.