Berlin, 3. August 2020

Deutscher Industrie- und Handelskammertag

Rückmeldung des Deutschen Industrie- und Handelskammertags (DIHK) zu einer Folgenabschätzung der Kommission

„Artificial intelligence – ethical and legal requirements“

1. Opportunität eines Regulierungsrahmens für KI

Der DIHK unterstützt die Idee der EU-Kommission, einen Regulierungsrahmen zu schaffen, der aber offen sein muss für weitere Entwicklungen. Die Fortschritte und weitere Marktdurchdringung sind bei KI-Anwendungen momentan nicht einzuschätzen. Daher dürfen gesetzliche Regelungen keine unnötigen Hemmnisse für die Weiterentwicklung bei KI aufbauen und sollten vielmehr innovationsfördernd wirken. Die Gefahr einer Fragmentierung des Binnenmarkts durch nationale KI-Regelungen in grenzüberschreitenden Sektoren spricht auch für eine Harmonisierung auf EU-Ebene. Es darf sich allerdings lediglich um einen Rahmen handeln, der klare und allgemeinen Leitplanken für KI regelt.

Bei der KI-Regulierung sollte besonders für KMU vermieden werden, dass komplexe und bürokratische Regeln entstehen. Die Rechtssicherheit der Unternehmen sollte bei der Regulierung eine Priorität sein – und nicht vor allem auf den Schutz der Verbraucher fokussiert sein, wie das KI-Weißbuch an mehreren Stellen zu verstehen gibt. Dabei sollten die rechtlichen Regelungen die Risiken, die KI-Anwendungen verursachen können, berücksichtigen. Das betrifft einmal die Höhe des Risikos, aber andererseits auch die Frage der ungleichen Marktmacht im B2B-Bereich.

Bei der Überlegung einer Differenzierung zwischen B2B und B2C muss berücksichtigt werden, dass gerade viele kleinere und mittlere Unternehmen genauso „schutzwürdig“ im Bereich KI sein können wie Verbraucher.

2. Risikobasierten Ansatz verfolgen

Der von der EU-Kommission gewählte risikobasierte Ansatz ist im Sinne eines verhältnismäßigen regulatorischen Eingriffs sinnvoll. Auch die Datenethikkommission in Deutschland hat einen solchen ihrem Bericht zugrunde gelegt. Die Kommission schlägt vor, KI-Anwendungen als „hohes Risiko“ einzustufen, wenn sowohl der Sektor als auch die beabsichtigte Verwendung erhebliche Risiken bergen. Dennoch scheint dieser Ansatz keine bessere Risikoeinschätzung im Einzelfall zu ermöglichen, denn die Risiken und Risikobereiche werden nicht vorhersehbar sein – dadurch könnten nicht alle Risiken erfasst werden.

Teilweise wird vorgebracht, dass risikobehaftete Sektoren in einer Liste aufgezählt werden sollten, umso mehr Rechtssicherheit zu erhalten. Allerdings könnte eine Liste von „risikoreichen Sektoren“

ganze Sektoren unter Verdacht stellen, obwohl in jedem Sektor Anwendungen, Produkte und Dienste mit unterschiedlichsten Risikoanforderungen bestehen. Eine Liste von „risikoreichen Sektoren“ würde damit allen gelisteten Sektoren die Nutzung von KI auch für unkritische Funktionen/Dienste erheblich erschweren, etwa durch erhöhten Trainingsaufwand von ethisch unbedenklichen Anwendungsfällen. Dies wäre mit erheblichen Schäden für die Konkurrenzfähigkeit und Beschäftigung des EU-Standorts verbunden. Eine Bestimmung der risikoreichen Anwendungen nach Sektoren erscheint also nicht geeignet, um die Vielfalt der KI zu erfassen. Daher sollte eine Beurteilung des Risikos anhand allgemeiner Kriterien erfolgen. Sie sollten allerdings sehr klar festgelegt, eng gefasst und zukunftsfest sein.

3. Zertifizierung/Standardisierung

Die Entwicklung von KI sollte grundsätzlich den gleichen Sicherheitsstandards genügen, wie dies bei anderen Industriegütern oder Dienstleistungen heute schon geregelt ist. Um Schutzziele mit den Entwicklungszielen in Einklang zu bringen, muss auch hier das Grundprinzip Wettbewerb unter Einhalten von Sicherheitsstandards gelten. Eine Möglichkeit wäre, grundsätzliche Anforderungen ähnlich dem Prinzip der CE-Kennzeichnung für KI-Anwendungen und KI-Produkte zu definieren und Unternehmen diese nach dem Selbstverpflichtungsprinzip (Konformitätsbewertungsverfahren) unter behördlicher Überwachung umsetzen zu lassen.

Ob die Prüfung, Zertifizierung oder auch Standardisierung von Algorithmen jedoch möglich ist, erscheint fraglich. Das Ergebnis wäre eine Momentaufnahme, die bei der schnellen technischen Entwicklung regelmäßig angepasst werden müsste. Zudem ist zu berücksichtigen, dass insbesondere für Start-ups und KMU Zertifizierungen eine enorme finanzielle Belastung bedeuten. Hier sind Nutzen und Mehrwert einer Zertifizierung sorgfältig gegenüber dem Aufwand abzuwägen.

Großer Handlungsbedarf besteht bei der Anonymisierung von Daten. Denn dies könnte helfen, die Datennutzung zu verbessern und das Zusammenführen von Daten verschiedener Anbieter zu ermöglichen. Europäische Standards für die technische Umsetzung der Anonymisierung personenbezogener Daten wären ein großer Schritt in die richtige Richtung. Die zur Verfügungsstellung eines Prüfsystems, dass automatisch die Stabilität, Sicherheit und den Bias überprüft, könnte Unternehmen einiges an Last abnehmen. Denn schließlich muss beim Einsatz von KI das Recht der Betroffenen "nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung" gewahrt werden. Fraglich ist, wann eine Entscheidung ausschließlich auf einer automatisierten Entscheidung beruht.

Die (verlässliche und tatsächliche) Umsetzbarkeit von gesetzlichen Auflagen durch Unternehmen hängt auch stark von den staatlichen Stellen ab, die die Vorgaben/Regelungen (glaubwürdig) kommunizieren, deren Einhaltung überprüfen und gleichzeitig unternehmensfreundliche Hilfestellungen/Umsetzungs- bzw. Einhaltungswerkzeuge bereitstellen. Zur Unterstützung der

Unternehmen sollten entsprechende Entwicklungsleitfäden, eventuell sogar ein neuartiger Entwicklungsprozess für KI-Anwendungen, erarbeitet werden.

Daraus ergeben sich folgende Fragen: Wird es eine zentrale Stelle auf EU geben, die in enger Abstimmung mit landesspezifischen Einrichtungen (wie dem BSI) eine Operationalisierung und Koordinierung vornimmt? Und kann dieses hochanspruchsvolle Wissen, was in gesetzliche Regelungen übersetzt werden soll, überhaupt von jedem EU-Land einzeln geleistet werden – oder macht eine EU-weite Bündelung Sinn? Wie sollen Daten im Rahmen von Edge Computing Lösungen effizient vorgehalten werden, wenn sie nicht zentral verfügbar sind? Wie werden bei einer externen Prüfung Unternehmensgeheimnisse und Datenschutz gewahrt? Wie soll mit KI-Anwendungen umgegangen werden, die bereits entwickelt sind?

4. Datenschutz und KI zum Ausgleich bringen

Aus datenschutzrechtlicher Sicht zeigt sich, dass die DSGVO die Nutzung von KI vor Herausforderungen stellt. So hat die EU selbst mit ihrer Verordnung (EU) 2018/1807 vom 14.11.2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union deutlich gemacht, wie schwierig die Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten ist. In der Realität gibt es einen hohen Prozentsatz an gemischten Daten, die aber für KI-Anwendungen notwendig sind, wegen des Personenbezugs aber der DSGVO unterliegen. Ob eine stärkere Anwendungsmöglichkeit von Pseudonymisierung und Anonymisierung von Daten bei der Verarbeitung für und durch KI möglich ist, wäre ein wichtiger Aspekt, um zumindest teilweise nicht dem strengen Regime der DSGVO zu unterliegen.

Die EU-Kommission sieht zurecht eine generelle Sektor-Überwachung bei der Frage eines höheren Risikos als kritisch an. Denn nicht jede KI-Anwendung in einem risikohaften Sektor ist an sich ebenfalls risikoreich. So beinhaltet z. B. die Auswertung von abstrakten, anonymisierten Daten für die Überprüfung von Verkehrsflüssen keinerlei Risiko für die Verkehrsteilnehmer. KI-Anwendungen mit einem hohen Risiko müssen wohl ohnehin, wenn sie personenbezogene Daten verarbeiten, z. B. einer Datenschutz-Folgenabschätzung unterliegen. Zudem unterliegen sie entsprechenden Informationspflichten nach der DSGVO. Insofern ist nicht ersichtlich, welche weiteren Kennzeichnungen notwendig wären. Werden keine personenbezogenen Daten verarbeitet, ist nicht erkennbar, worin dann ein hohes Risiko für Verbraucher/Bürger liegen soll.

Im Bereich des Deep Learning – eine spezielle Machine-Learning-Technik - lernt die KI selbst und direkt aus Beispielen. Zwangläufig ergibt sich die Frage, wie den Anforderungen der DSGVO nachgekommen werden kann bzw. ob der von der DSGVO vorgebebene Rahmen kompatibel mit Anwendungsszenarien sich weiter entwickelnder KI ist. Konkrete Unklarheiten sind: (i) Der Zweckbindungsgrundsatz (dynamischer Prozess; eine KI entwickelt sich nicht starr nach vorgebebenen Kriterien), (ii) Voraussetzungen informierter Einwilligung (wie möglich, wenn die Zwecke nicht ausreichend feststehen; Umsetzung des Widerrufs bei bereits verarbeiteten Daten in

der KI schwierig), (iii) Informationspflichten (keine Darstellung der Verarbeitungszwecke im Detail möglich).

Auch das Löschen von Daten in der KI dürfte schwierig sein. Wie sollen die verarbeiteten Daten herausgelangen und kann die KI ihren Zweck, aus Datensätzen zu lernen, dennoch weiterverfolgen? Tatbestände der DSGVO müssten im KI-Anwendungsfeld wohl weit ausgelegt werden, um KI und DSGVO zum Ausgleich zu bringen und die DSGVO nicht zum Innovationshemmnis für die Entwicklung neuer Technologien werden zu lassen. Darüber hinaus braucht es weitere Präzisierungen und eine einheitliche, europaweite Auslegung der DSGVO.

5. Transparenz

Grundsätzlich ist die Forderung nach Transparenz zu unterstützen. Es muss zumindest im B2C-Bereich deutlich gemacht werden, dass KI-Lösungen angewendet werden. Eine transparente KI kann für Beweisführungen und Haftungsfragen ggf. Vorteile mit sich bringen. Allerdings findet die Transparenz dort ihre Grenzen, wo es um Geschäftsgeheimnisse geht. Hier sei auf die Richtlinie (EU) 2016/943 verwiesen. Algorithmen und KI-Anwendungen gehören eindeutig zu den schützenswerten Geschäftsgeheimnissen von Unternehmen.

Mit der geforderten Datentransparenz können Geschäftsgeheimnisse tangiert werden. Deshalb sollten Unternehmen die bereitzustellenden Informationen über Fähigkeiten, Grenzen und ordnungsgemäße Funktionalität auf höherem Abstraktionsgrad bereitstellen können. Vermieden werden muss, dass Datentransparenz zum Einfallstor für Spionage wird und ggf. so zu Wettbewerbsverzerrungen zwischen First und Late-Mover führt.

Dass die Transparenz bzw. das Auskunftsrecht der betroffenen Personen nicht schrankenlos sind, sondern die Geschäftsgeheimnisse oder Rechte des geistigen Eigentums nicht beeinträchtigen darf, sieht bereits Erwägungsgrund 63 vor. Auch hier wäre - für KI-basierte Entscheidungen - eine Klarstellung dahingehend sinnvoll, dass Algorithmen nicht offengelegt werden müssen, weil nach Erwägungsgrund 58 die Möglichkeit besteht, „präzise, leicht zugänglich und verständlich" zu informieren.

6. Haftung

a. Opportunität eines Haftungsrechtsrahmens für KI

Die Digitalisierung ermöglicht in nahezu allen Wirtschaftszweigen und Branchen KI-Lösungen. Geschäftsmodelle bauen zunehmend auf KI-Lösungen auf. Bisherige ordnungs- und rechtspolitische Paradigmen werden dadurch dennoch nicht obsolet.

Die Fragen, wer die Verantwortung für Schäden, die aus KI-Anwendungen hervorgehen, zu tragen hat, sollten durch Herausbildung europaweit einheitlicher Regeln, insbesondere bei

Produktsicherheits- und Haftungsfragen erfolgen. Dabei sollte auch der Begriff „Verantwortung“ europäisch definiert werden. Die Ausführungen unter B.2 zur KI-Definition gelten hier entsprechend.

Zugleich gilt, dass vor jeder neuen Regulierung eine Regelungs- oder Rechtsdurchsetzungslücke nachgewiesen sein sollte. Regulierung darf kein Selbstzweck sein und in Überregulierung münden. Sie sollte Innovationen fördern, also innovationsoffen sein, und eine leistungsstarke und international wettbewerbsfähige Wirtschaft ermöglichen.

Wo werden Regelungslücken gesehen? Das Aufkommen neuer digitaler Technologien wie KI, Internet der Dinge und Robotik birgt in Bezug auf rechtliche Fragen, z. B. für die Produktsicherheit und -haftung, neue Herausforderungen wie Konnektivität, Autonomie, Datenabhängigkeit, Opazität, Komplexität von Produkten und Systemen, Softwareaktualisierungen sowie ein komplexeres Sicherheitsmanagement und komplexere Wertschöpfungsketten. Diese Probleme sind auch bisher nicht unbekannt.

Beim Einsatz von KI wird es aber gegebenenfalls noch schwieriger, die Risiken zu beschreiben und zu quantifizieren. Insbesondere die Nachvollziehbarkeit von KI-Systemen und die von diesen oder mit deren Hilfe getroffenen Entscheidungen müssen beurteilt und ggf. entschlüsselt werden. Konnektivität darf nicht mit Kausalität gleichgesetzt werden.

Ob vor diesem Hintergrund eine Notwendigkeit besteht, dass für KI neue rechtliche Regelungen eingeführt werden oder bestehende angepasst werden sollten, ist vorsichtig zu beurteilen.

b. Produkthaftung

Im Rahmen von Industrie 4.0 können, wie bei der industriellen Fertigung auch, im Herstellungsprozess Fehler auftreten, die sich in der Produktnutzung fortsetzen. Der Schaden, der bei der Nutzung des fehlerhaften Produkts entsteht, ist dann auf das fehlerhafte Produkt selbst zurückzuführen. Beim Einsatz autonomer oder selbstlernender Systeme können Schäden durch ein Fehlverhalten dieser Systeme auftreten.

Das Produkthaftungsgesetz und das Deliktsrecht sind nur dann „fit“ für die Digitalisierung, wenn sowohl die Produkte selbst als auch Dienstleistungen mitumfasst werden. KI wird üblicherweise aus dem Bereich der Dienstleistungen generiert. Im Dienstleistungsbereich können auch Fragen der genügenden Cybersicherheit zu Problemen führen. Der Hauptfokus dürfte im Bereich des Nachweises bzw. der Kausalität liegen . Hier könnte daher möglicherweise eine Beweislastumkehr oder zumindest Beweislasterleichterungen entsprechend der Verantwortungs- und Risikosphären angedacht werden.

c. Deliktsrecht

Verursachen autonome oder selbstlernende Systeme Schäden, ist es insbesondere schwierig, den Anspruchsgegner zu identifizieren. Dieses Rechtsrisiko unterscheidet sich strukturell nicht von anderen Situationen, in denen der Verursachungshergang nicht oder nur schwer aufklärbar ist.

Es ist zu überlegen, ob die Haftung für autonome Systeme sich am Beispiel der Halterhaftung (ähnlich der Regelungen im Straßenverkehr), verbunden mit einer Versicherungspflicht, orientieren sollte. Eine in diesem Zusammenhang diskutierte gesetzliche Erweiterung um eine reine Gefährdungshaftung geht allerdings zulasten der Unternehmen. Denn die Gefährdungshaftung geht davon aus, dass sie ohne jeden Bezug auf ein Verschulden oder auf einen Verursachungsbeitrag zur Anwendung kommt. Dies würde sich nachteilig auf die internationale Wettbewerbsfähigkeit auswirken und Unternehmern die Entwicklung und Etablierung innovativer Produkte erschweren. In diesem Zusammenhang ist darauf hinzuweisen, dass schon heute viele Produkte einer besonderen Zulassung vor dem Inverkehrbringen bedürfen, z. B. im Medizin-/Pharma- oder KFZ-Bereich.

d. Zurechnung von Willenserklärungen

Automatisiert agierende Systeme handeln nach voreingestellten Bedingungen, wie Drucker, die ab einem vorgegebenen Füllstand der Druckerpatrone eine neue nachbestellen. Virtuelle Assistenten, wie „Siri“ oder „Alexa“, führen sprachgesteuerte Bestellungen durch. Autonom agierende Systeme sind in der Lage, aufgrund der ihnen zur Verfügung stehenden Datensätze selbstständig zu lernen und damit „Willenserklärungen“ abzugeben.

Für Deutschland gilt gemäß dem Bürgerlichen Gesetzbuch (BGB) der Grundsatz, dass Erklärungen demjenigen zuzurechnen sind, aus dessen Sphäre sie tatsächlich stammen. Viele Fragen zum Vertragsschluss lassen sich daher bereits mit den Auslegungsregeln §§ 133, 157 BGB lösen. Automatisiert agierende Systeme handeln, wie in den Beispielen oben dargelegt, nach voreingestellten Bedingungen und folgen einem vom Menschen vorgegebenen Algorithmus. Die Person, die die KI nutzt, hat den generellen Willen, zu einem zuvor definierten Zeitpunkt oder bei Eintritt bestimmter Bedingungen eine Willenserklärung abzugeben. Die Willenserklärung kann dieser Person zugerechnet werden. Die Erklärungen eines autonom agierenden Systems sind zwar nicht vorhersehbar, aber auch dieses System kann Willenserklärungen erst generieren, wenn die Nutzer dies so wollen. Dieser Person ist bewusst, dass das System Erklärungen abgeben könnte. Erklärungen des Systems lassen sich daher der Person zurechnen aus deren Sphäredie Erklärungen stammen.

Für die Frage der Zurechnung von Willenserklärungen, die von automatisiert oder autonom agierenden Systemen abgegeben werden, bieten Regelungen wie im deutschen BGB bereits einen passenden Rechtsrahmen. Eine Regelungslücke erscheint uns daher nicht zu bestehen.

Berlin, 3. August 2020

Deutscher Industrie- und Handelskammertag

Wer wir sind:

Unter dem Dach des Deutschen Industrie- und Handelskammertags (DIHK) haben sich die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich der DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Darüber hinaus koordiniert der DIHK das Netzwerk der 140 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 92 Ländern.
Er ist im Register der Interessenvertreter der Europäischen Kommission registriert (Nr. 22400601191-42).

Ansprechpartner im DIHK

Annette Karstedt-Meierrieks
Bereich Recht
Referatsleiterin Datenschutz
Tel.: +49 30 20308- 2706
E-Mail: karstedt-meierrieks.annette@dihk.de

Doris Möller
Bereich Recht
Leiterin des Referats Recht des Geistigen Eigentums
Tel.: +49 30 20308- 2704
E-Mail: moeller.doris@dihk.de

Annelise Badinand
Legal Affairs
Director European Economic Law, German and International Commercial Law
Tel.: +32-2-286-1663
E-Mail: badinand.annelise@dihk.de