TAGESSPIEGEL BACKGROUND

„Die Zertifizierbarkeit von KI kann ein Exportschlager werden“

von ***Miriam Schröder***

veröffentlicht am 30.11.2020

Beim Digitalgipfel wird heute auch die Normungsroadmap KI vorgestellt. Entwickelt wurde sie beim Deutschen Institut für Normung (DIN), Vorsitzende der Steuerungsgruppe war der KI-Forscher Wolfgang Wahlster. Er hoffe, dass bis Ende des nächsten Jahres die ersten KI-Zertifikate ausgestellt werden können, sagt er im Interview mit Miriam Schröder.

Herr Wahlster, Sie arbeiten seit einem Jahr im Auftrag des Bundeswirtschaftsministeriums an einer Normungsroadmap für KI. Heute legen Sie Ihren Bericht vor. Was hat das Gremium erreicht?

Wir haben zunächst eine Bestandsaufnahme gemacht und untersucht, welche Normen und Standards international auf dem Gebiet der KI bereits verfügbar sind. Wir geben auch einen Überblick darüber, in welchen Teilen der Welt welche Organisationen an neuen Normen und Standards arbeiten und welches die weißen Flecken sind, also KI-Gebiete, in denen bislang noch gar keine Standardisierung begonnen wurde und wo in den nächsten Jahren Handlungsbedarf besteht.

Wie dick ist das Papier geworden?

Es umfasst 236 Seiten. Aber es ist klar, dass das nur eine Momentaufnahme sein kann, die immer wieder aktualisiert werden muss, quasi ein lebendes Dokument. Schließlich schreiten die Forschung und Entwicklung in der KI sehr schnell voran.

Und wo besteht Ihrer Ansicht nach der größte Handlungsbedarf?

Was wir jetzt brauchen, sind Prüfprofile und die dazu passenden Prüfverfahren. Die Unternehmen wünschen sich ja ein Zertifikat oder ein Prüfsiegel für ihre KI-Produkte. Davon sind wir noch weit entfernt. Dazu müssen wir ja die Prüfkriterien technisch eindeutig definieren und auch festlegen, wie unabhängige Prüforganisationen diese testieren können. Das ist ja nicht wie bei einer Abgasuntersuchung, wo einfach die über eine Sonde im Auspuff ermittelten Werte mit der vorgeschriebenen Norm verglichen werden. Gerade wenn man selbstlernende KI-Systeme mit komplexer Sensorfusion etwa beim hochautomatisierten Fahren oder autonomen Zügen und Schiffen einsetzt, sind komplexe Prüfprofile und wissenschaftlich sehr anspruchsvolle Prüfverfahren notwendig.

Wir empfehlen daher der Bundesregierung, nach der Normungsroadmap jetzt zügig ein Umsetzungsprogramm für die Entwicklung konkreter Prüfverfahren für wichtige KI-Anwendungsfälle zu starten, so dass Ende nächsten Jahres hoffentlich schon erste Zertifikate für einfache KI-Produkte ausgestellt werden können. Andererseits sind aber für die neuste Generation hybrider KI-Systeme noch Forschungen notwendig, um auch für diese Zertifizierungsverfahren zu entwickeln.

Wozu braucht es Normen und Standards überhaupt?

Es gibt zwei Hauptfunktionen: Zum einen müssen die verschiedenen KI-Komponenten interoperabel sein. Stellen Sie sich zwei mobile Logistik-Roboter von unterschiedlichen Herstellern vor, die in einer Fabrik eigenständig unterwegs sind. Die müssen sich miteinander abstimmen können, um Kollisionen zu vermeiden, ohne dass Menschen zwischen ihnen vermitteln. Dafür muss ihre Sprache standardisiert sein. Noch wichtiger für den Endkunden ist die Vertrauenswürdigkeit: Ein datengetriebener Lernalgorithmus etwa in einer Diabetes-App, der auf Basis von Blutzuckerdaten individuell errechnet, wieviel Insulin einem Patienten über eine automatische Insulinpumpe zugeführt wird, braucht natürlich ein Zertifikat, damit die Nutzer darauf vertrauen können, dass das Produkt medizinischen Standards genügt.

Kann es allgemein gültige Normen für KI geben oder müssen die Algorithmen branchenspezifisch normiert werden?

Ganz allgemein gültig geht das nicht. Je nachdem wie hoch das Risiko ist, müssen wir andere Maßstäbe anlegen. Eine Software, die Karies in Röntgenbildern erkennt, birgt natürlich keine lebensbedrohlichen Risiken, im Gegensatz zur KI-Steuerung einer Insulinpumpe. Oder nehmen Sie KI-Systeme, die Verkehrszeichen erkennen sollen – die sind erst dann wirklich kritisch, wenn sie als Teil einer Software zum autonomen Fahren verwendet werden. Die Kritikalität ergibt sich jeweils aus dem Anwendungskontext. Wir gehen darum davon aus, dass wir Prüfprofile für bestimmte Anwendungsklassen festlegen müssen. Hinzu kommen die verschiedenen KI-Methoden. Wir haben die KI in unserer Roadmap in 41 KI-Methoden untergegliedert, in 17 Teilgebieten und vier methodischen Dimensionen.

Und die müssen alle einzeln normiert werden?

Selbstverständlich. Nehmen Sie das Beispiel der maschinellen Übersetzung. Bei Gerichtsverhandlungen dürfen KI-basierte Übersetzungen grundsätzlich nicht verwendet werden. Es gibt nämlich bislang kein Übersetzungssystem, das garantiert niemals eine verdeckte Negation übersieht. Bei juristischen Verträgen,

die aus anderen Sprachen übersetzt werden, braucht man etwas weniger, aber immer noch hohe Anforderungen, das gleiche gilt für journalistische Nachrichten. Dann gibt es eine große Menge an unproblematischen Übersetzungsaufgaben.

Wie misst man die Güte eines maschinellen Übersetzungssystems?

Man verwendet als ersten Ansatz den sogenannten Bleu-Wert, der den Unterschied zwischen menschlichen und maschinellen Übersetzungen sehr grob misst. Den Bleu-Wert kann man maschinell ermitteln. Also kann man festlegen: Für eine bestimmte KI-Anwendung im Übersetzungsbereich muss der Bleu-Wert des verwendeten Systems den jeweils gültigen normierten Minimalwert überschreiten.

Wie wichtig ist die Datenbasis, auf der ein Algorithmus basiert? Beim maschinellen Lernen hängt die Qualität der Ergebnisse ja von der Qualität der Daten ab.

Die ist sehr wichtig, die Systeme lernen ja aus Datenströmen und verändern sich ständig. Bei selbstlernenden Systemen aus parallelen Datenströmen muss es darum eine Live-Schnittstelle geben, so dass etwa die Prüfung der Zulässigkeit von KI-gesteuerten Transaktionen an der Börse laufend erfolgen kann. Die Zertifizierbarkeit von KI-Systemen, die in Echtzeit operieren, ist noch ein offenes Forschungsthema, zu dem wir ein großes Verbundprojekt bräuchten.

Was ist mit der Qualität der Trainingsdatendaten selbst?

Auch die Ordnungsmäßigkeit der Datenkuratierung kann und muss man überprüfen. Man muss hier ja unterscheiden zwischen Rohdaten und den sogenannten annotierten Trainingsdaten für das überwachte maschinelle Lernen, die zuvor eine manuelle Zuweisung erfahren haben. Auch dafür gibt es Werte, etwa den Kappa-Wert, der misst, wie einstimmend diese Zuschreibungen für die Trainingsdatensätze waren, oder ob es große Unterschiede zwischen den verschiedenen menschlichen Klassifikationen gab. Die Annotationsqualität kann man also standardisiert messen. Dazu müssen die Prüfer aber auch auf Dokumente zum Annotationsverfahren zugreifen können.

Es wird oft kritisiert, dass die Normierungsprozesse zu lange dauern, während sich die Technologie schneller entwickelt.

Das Problem sehe ich heute weniger. In den letzten Jahren ist die Normungsarbeit stark beschleunigt worden, so dass Normen nun rascher und auch maschinenlesbar geschrieben werden. Der Rekord liegt bei einem halben Jahr, wo man früher drei bis vier Jahren gebraucht hat. Man kann im Übrigen auch die IT-Technologie selbst nutzen, um diesen Prozess zu beschleunigen. Wir wollen mittelfristig auch KI dafür einsetzen, bei der Prüfung der Normen zu helfen. Die KI-Prüfstelle der Zukunft prüft mit Hilfe von Software die zu zertifizierenden Systeme.

Normen und Standards sollen geltendes Recht in die Anwendung bringen. Die EU entwickelt aber gerade erst ein KI-Gesetz, bis es verabschiedet wird, kann es noch dauern. Inwiefern laufen die Prozesse hier synchron ab?

Die EU setzt ethische, gesellschaftlichen und rechtliche Rahmenbedingungen. Das findet auf einer Metaebene statt und geht nicht auf die konkrete Ebene der technischen Prüfprofile für die funktionale Sicherheit der einzelnen Anwendungsfälle. Wir sind aber in unseren DIN/DKE Arbeitskreisen zur KI-Normungsroadmap aber ja auch personell querverbunden, etwa mit der Enquete-Kommission KI des

Deutschen Bundestags, in der zwei Forscher des DFKI saßen oder mit der Datenethikkommission, der ich angehört habe. Wir haben auch die Ergebnisse der High-Level-Expert-Group on AI in unsere Diskussion mit aufgenommen. Aber bisher wurden in all diesen Kommissionen keine konkreten Werte für Qualitätsmetriken oder eindeutige Risikoeinstufungen mit exakten Grenzwerten festgelegt, so dass noch weitere Detailarbeit zu leisten ist, um eine risikoadaptive Regulierung auch praktisch durchführbar zu machen.

Das heißt, über die Frage, wann ein Algorithmus diskriminierend ist und wann nicht, entscheiden jetzt nicht mehr die Politik, sondern die Normierungsgremien. Etwa bei der Personalsoftware.

Nein, natürlich nicht: die Politik muss den Rahmen setzen. Aber für konkrete Einzelfallprüfungen sind deren Vorgaben noch zu undifferenziert. Wir müssen uns aber auch vor einer Überregulierung hüten, die europäischen KI-Anbietern den Marktzugang für völlig harmlose KI-Anwendungen durch zu viele Hürden erschwert, während amerikanische und chinesische Hyperscaler diese Hürden einfach nicht beachten, so dass eine Wettbewerbsverzerrung entsteht.

Ist die Festlegung von Standards nicht aber hauptsächlich industriegetrieben?

Nein, wir versuchen, alle relevanten gesellschaftlichen Gruppen in diesen Prozess einzubeziehen. Bei der Normungsroadmap haben 300 ehrenamtliche Experten in sieben Arbeitsgruppen mitgearbeitet, 42 Prozent davon aus der Wirtschaft, 32 Prozent aus der Wissenschaft, 26 Prozent von NGOs, Gewerkschaften, Verbänden und Behörden. Die Arbeiten an der Normungsroadmap sind offen und transparent und wir sind dankbar für jede Expertise, die zusätzlich eingebracht wird.

Ziel von Standardisierung ist ja, möglichst auch international kompatibel zu sein. Wie früh ist Deutschland dran mit dem Prozess, wie hoch ist die Chance, dass wir international die Standards setzen können?

Das kommt auf die Teilgebiete an. Wir können keine Methoden normieren, die im Wesentlichen im Ausland entwickelt wurden. Wir müssen uns auf die konzentrieren, die hier entwickelt wurden und wofür wir Leitanbieter sind. Deutschland ist derzeit weltweit führend in der industriellen KI, also Anwendungen für Industrie 4.0. Das Deutsche Institut für Normung ist in den internationalen Gremien wie ISO sehr anerkannt, so dass hier gute Chancen bestehen. Andererseits können wir etwa beim Deep Learning in Europa ohne Einbindung der USA, Kanada und China natürlich kaum Normen erfolgreich durchsetzen.

Wenn es um ethische Standards geht, dürften diese Diskussionen langwierig werden.

Annette Schavan hat kürzlich bei einer internationalen Konferenz mit dem Bundespräsidenten zur Ethik in der Digitalisierung vorgeschlagen, man solle jetzt zügig einen weltweiten ethischen Minimalkonsens für KI-Anwendungen finden. Das halte ich für sinnvoll. Wir arbeiten zwar zunächst an Standards für Europa. Es ist aber eine Illusion, dass wir diese ohne weiteres weltweit ausrollen können. Andererseits hat die DSGVO gezeigt, dass unsere Standards sehr wohl respektiert und auch übernommen werden, wenn wir uns frühzeitig mit Thematiken beschäftigen, die anderswo erst später erkannt werden. Privacy by design, security by design, das sind Ansätze, für die unsere Produkte inzwischen auch in anderen Teilen der Welt geschätzt werden. Zertifizierbarkeit by design, das könnte der nächste Exportschlager für vertrauenswürdige KI werden.

Das Interview führte Miriam Schröder.