Deep Learning und Rechtsrisiken

Ursula Sury

Mehrere Beteiligte

Deep Learning ist eine Anwendung oder auch Weiterentwicklung von künstlicher Intelligenz. Es geht darum, dass die Software Daten intelligent miteinander verknüpft und daraus Rückschlüsse gezogen werden. Die Software ist so angelegt, dass sie sich selber weiterentwickelt. Dies sowohl durch die Verbreiterung der Datenbasis als auch durch die Varianz der Verknüpfungen. Der Computer lernt also auch durch Erfahrung.

Wenn man die Entstehung einer Deep Learning Anwendung analysiert, so stellt man fest, dass es mehrere Beteiligte gibt, die dazu beitragen. Zuerst sind es einmal die Softwareentwickler, dann aber auch die jeweiligen Fachexperten, die die Datenbasis und bekannte Kombinationen/Reaktionsmuster zur Verfügung stellen. Aber auch der (End)Anwender selber trägt zur Weiterentwicklung mit der Art seiner Verwendung bei.

Die Verantwortung für sinnvolle, brauchbare und somit ungefährliche Resultate liegt somit bei mehreren Parteien. Softwareersteller, Experten und Anwender.

Falls das Deep Learning Produkt als Produkt im Sinne des Produktehaftpflichtgesetzes angeschaut würde (was bei NurSoftware kaum der Fall ist), haben wir also verschiedene Produzenten und bei anderer Form der Haftpflicht, mehrere gemeinsam Haftpflichtige.

Nachvollziehbarkeit

Wenn solche Deep Learning Produkte in der Praxis eingesetzt werden, zum Beispiel bei der Erkennung von Krebszellen, so ist es für den Anwender nicht nachvollziehbar, warum der Computer auf welche Resultate kommt. Das ist eine gewisse Schwierigkeit, aber nicht ganz neu. Wenn ich den vorliegenden Artikel schreibe, weiss ich auch nicht, was im Hintergrund im Betriebssystem und im Word technisch alles abläuft, aber ich verwende es wie Millionen andere Menschen trotzdem. Dasselbe haben wir beim Einsatz heutiger Haushaltsmaschinen, wie Staubsaugerroboter, Softwaregesteuerte, Backöfen, intelligenten Haussteuerungen etc.

Der Unterschied liegt aber in der Dimension der Nichtnachvollziehbarkeit. Beim Backofen, gibt es viele Maschinenbauingenieure, die genau erklären können, warum es funktioniert, weil das System klarere Grenzen hat und

nicht Inputs aus verschiedenen Quellen auf verschiedene Arten kombiniert und in diesen zwei Dimensionen «eigenständig» neue Kombinationen schafft.

Die Nachvollziehbarkeit der Resultate rückblickend (wie ist denn das gegangen) ist bei Deep Learning Produkten schwierig.

Arbeitsteilung Mensch-Maschine

Der Einsatz von Deep Learning Produkten verlangt vom Menschen, dass er die entstandenen Resultate trotz der fehlenden Nachvollziehbarkeit aufgrund seiner Expertise und seiner Intuition (genau das fehlt nämlich der Maschine sic!) auf deren Brauchbarkeit einschätzen und überprüfen kann.

Ziel des Einsatzes ist es ja weiter zu kommen, als ohne Maschine, und die Vorteile der Maschine mit den Aktivitäten des Menschen zu ergänzen. Es ist ein grosser Vorteil, dass ich einen Roboter habe, der mir den Küchenboden nass putzt, aber ich kann und muss ihn zu einem gewissen Grad überwachen, denn er könnte die Virtual Wall durchbrechen und auf dem Parkett Schaden anrichten. Zudem muss ich die Ränder noch von Hand putzen.

Wo und wie es sinnvoll ist, die Maschine einzusetzen und wo nicht, ist eine menschliche Entscheidung. Diese muss sorgfältig getroffen werden.

Test, Riskmanagement und Vollzugsprobleme

Der unsachgemässe Einsatz oder der Einsatz von fehlerhaften Deep Learning Produkten kann grosse Schäden generieren. Dies muss unter allen Umständen vermieden werden. Deshalb müssen die Anwender entsprechend geschult sein, aber auch die Produkte immer wieder getestet werde. Eine gute Idee ist auch immer ein Framing, d.h. anzugeben, in welchem Kontext und mit welchem Know-how das Produkt angewendet werden kann, und wo eben nicht.

Sollte dann einmal tatsächlich ein Problem auftauchen, dann ist es in so komplexen und vergemeinschafteten Projekten schwierig den Schadenverursacher beweisbar ausfindig zu machen. Und selbst wenn dies möglich wäre, ist es in der heutigen internationalen Welt schwierig, die Rechtsansprüche effizient und effektiv durchzusetzen.

Aus diesem Grund wird zum Framing unbedingt eine realistisches Bussiness Continuity Management vorzukehren sein.

Fazit

- Bei Deep Learning sind immer mehrere Personen beteiligt.
- Die Ergebnisse des Systems sind nur schwer nachvollziehbar.

- Man muss sich den Risiken von Deep Learning bewusst sein und sollte Vorkehrungen treffen, um eine einigermassen sichere Anwendung garantieren zu können.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern - Informatik. Sie ist zudem Dozentin für Informatikrecht, Datenschutzrecht und Digitalisierungsrecht.