

Ursula Sury

Künstliche Intelligenz und Datenschutz

KÜNSTLICHE INTELLIGENZ

Künstliche Intelligenz oder artificial intelligence (AI) ist ein heute sehr berühmtes und prominentes Anwendungsgebiet der Informatik. Computer oder Roboter scheinen sich wie Menschen verhalten zu können oder scheinen sogar menschlicher Intelligenz überlegen zu sein. Dies lässt sich am bekannten Beispiel von Watson, beim Wettstreit zwischen Computerprogramm und Mensch in der Quizsendung „Jeopardy“, aufzeigen. Dort siegte das Computerprogramm Watson überlegen gegen zwei menschliche Gegner, welche in diesem Quiz zuvor Rekordsummen gewonnen hatten. Dies ist umso bemerkenswerter, weil die als Antworten gestellten Aufgaben in „Jeopardy“ meist bewusst mehrdeutig formuliert sind und häufig die Verknüpfung mehrerer Fakten erforderlich machen. Zu erwähnen ist, dass Watson keine Verbindung zum Internet hatte und somit wie seine menschlichen Gegenspieler auf sich alleine gestellt war.

Auch beim Einsatz von Expertensystemen scheinen Computer oder Softwareprogramme menschlicher Intelligenz überlegen zu sein. Programme künstlicher Intelligenz werden heute auch für die Steuerung des Verhaltens von Robotern eingesetzt.

Computerprogramme, welche dank diverser Algorithmen sehr viel aufgenommene Informationen verschieden verknüpfen und selber neue Informationen aufnehmen, zuordnen und wieder verknüpfen können, werden für zukünftige Entwicklungen zur Digitalisierung der Gesellschaft immer wichtiger werden. Diejenigen, welche die Programmierung vornehmen, geben nur die Prinzipien und Strukturen des Aufnehmens und der Varianten der Verknüpfungen von Informationen vor. Welche konkreten Zwischenresultate und Resultate daraus resultieren, hängt massgeblich auch von äusseren Umständen, d.h. den konkreten zugegangenen Informationen ab.

DATENSCHUTZ

Der Datenschutz fordert grundsätzlich, dass Daten einer Person nur mit gesetzlicher Grundlage oder Einwilligung bearbeitet werden dürfen (Zweckmässigkeit). Sofern ein genügender Zweck vorliegt, müssen dann die konkreten Datenbearbeitungen verhältnismässig sein, d.h. sie dürfen nur soweit gehen wie unbedingt notwendig, um den zulässigen Zweck erreichen zu können. Die Verhältnismässigkeit umfasst insbesondere die Themenbereiche der Zugriffe (wer kann auf was zugreifen), die Dauer der Aufbewahrung und Archivierung und Fragen der weiteren zukünftigen Datenverknüpfungen.

Wenn nun Computer / Computerprogramme oder Roboter aus dem Bereich der künstlichen Intelligenz gemäss den ihnen implementierten Algorithmen und Methodologien Informationen anreichern, verknüpfen und dann Schlüsse daraus ziehen, kann es sich durchaus auch um Informationen handeln, die einen Personenbezug haben. Mit dem Einsatz von Systemen künstlicher Intelligenz lässt sich aber, und das liegt in der Natur der Sache, schwer voraussehen, welche künftigen Erkenntnisse sich ergeben werden. Es ist also unwahrscheinlich, dass bei einer betroffenen Person eine konkrete Einwilligung für diese Art von Datenbearbeitung überhaupt eingeholt werden könnte. Dies insbesondere, weil die betroffene Person wissen muss, zu was sie genau einwilligt. Was den Bereich der gesetzlichen Grundlage anbelangt, so sind Datenbearbeitungen gemäss gesetzlicher Grundlage Businessprozessunterstützungen. Es handelt sich also um die Umsetzung schon vorgegebener und durchdachter Vorgehensweisen und nicht um exploratives tätig sein.

Für den privatrechtlichen Bereich der Einwilligung könnte man sich die Überlegung anstellen, ob man auch eine Einwilligung für Methodologien und Zukünftiges, welches sich aus der Anwendung von Algorithmen ergibt, einholen könnte. Dies natürlich verbunden mit einem jederzeitigen Informations- und Auskunftsrecht der betroffenen Person und natürlich dann nachfolgend der Möglichkeit einer Löschung dieser Daten.

Was den Bereich der Einwilligung anbelangt, so wird dies dadurch erschwert, dass die Formulierung, wie die Daten bearbeitet werden, aus Konsumentenschutzgründen

ganz einfach und zielpublikumorientiert sein müssen, also so, dass es z.B. auch ein Kind verstehen könnte.

PRIVACY BY DESIGN UND PRIVACY BY DEFAULT

Die anfangs 2018 in Kraft tretende Datenschutzgrundverordnung der EU verlangt, dass bei der Einführung von neuen Dienstleistungen, Services etc. technisch und organisatorisch maximal sichergestellt ist, dass keine Datenschutzverletzungen vorliegen. Dies würde bedeuten, dass ohne entsprechende eher generische Einwilligung von Seiten der betroffenen Personen die Implementierung von Softwareprogrammen der künstlichen Intelligenz häufig illegal wäre. Dies ist nämlich der Fall, sobald ein Programm Aktivitäten entwickelt, welche nicht genau *im Vorherein* durch eine gesetzliche Grundlage abgedeckt sind.

ZUSAMMENFASSUNG

- Programme und Roboter weisen immer mehr menschliche Verhaltensmuster auf und scheinen der menschlichen Intelligenz teilweise sogar überlegen zu sein.
- Selbstlernende Computerprogramme gewinnen für zukünftige Entwicklungen zur Digitalisierung der Gesellschaft immer mehr an Bedeutung.
- Für die (zulässige) Bearbeitung von Personendaten bedarf es der Einhaltung verschiedener Regeln. So werden eine gesetzliche Grundlage oder eine Einwilligung der betroffenen Personen sowie die Verhältnismässigkeit der Datenbearbeitung vorausgesetzt.
- Welche Schlüsse Systeme künstlicher Intelligenz ziehen, lässt sich schwer vorhersehen. Eine Einwilligung einzuholen ist schwierig, weil die betroffene Person für eine wirksame Einwilligung wissen muss, in was sie einwilligt.
- Es stellt sich die Frage, ob es möglich ist, die Einwilligung für die Methodologie und die Anwendung des Algorithmus einzuholen verbunden mit einem jederzeitigen Informations- und Auskunftsrecht und der Möglichkeit auf Löschung dieser Daten.
- Durch die 2018 in Kraft tretende Datenschutzverordnung der EU sind Aktivitäten von Softwareprogrammen, welche im Vorherein nicht genau durch eine gesetzliche Grundlagen abgedeckt sind, illegal.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern - Informatik. Sie ist zudem Dozentin für Informatikrecht an verschiedenen Nachdiplomstudien. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.

23.09.2016 / Ursula Sury