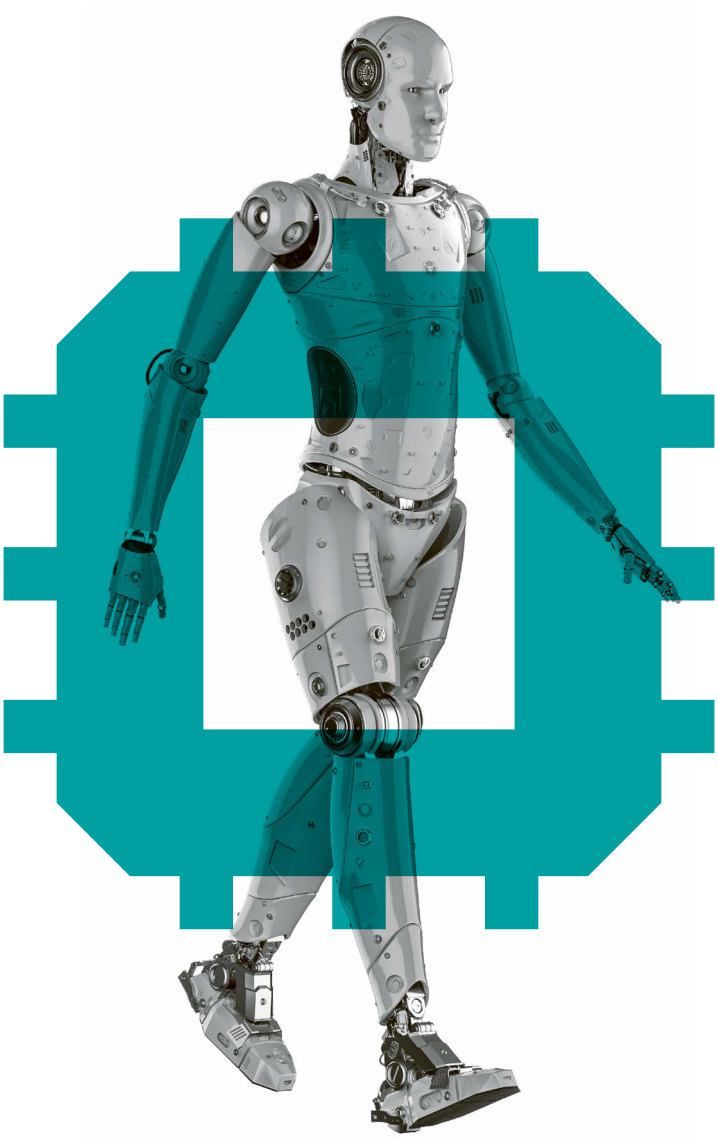
N

Newsletter
10/2019

Information and Communication Technology

Schellenberg Wittmer



Rechtliche Aspekte "Künstlicher Intelligenz" (KI)

Samuel Klaus und Claudia Jung

Key Take-aways

1.
Die Funktionsweise von KI besteht darin, aus unstrukturierten Daten mit einem auf den konkreten Verwendungszweck zugeschnittenen Algorithmus gewisse Muster zu erkennen, um daraus eine Schlussfolgerung abzuleiten.

2.
Unabhängig davon, in welchem Bereich und für welchen Zweck eine KI-Anwendung eingesetzt wird, stellen sich rechtliche Fragen bei der Erstellung, der Parametrisierung und dem Einsatz von KI-Anwendungen.

3.
Da die Gesetzgebung der Komplexität von KI (noch) nicht Rechnung trägt, sollten die rechtlichen Risiken durch organisatorische Massnahmen und vertragliche Regelungen adressiert werden.

1 Was ist "Künstliche Intelligenz"?

1.1 Begriff

Der Begriff "**Künstliche Intelligenz**" (KI) bzw. *"Artificial Intelligence" (AI)* bezeichnet keine bestimmte Technologie. KI ist ein Sammelbegriff für eine Vielzahl von Methoden, bei denen kognitive Fähigkeiten mit mathematisch-statistischen Modellen simuliert werden.

1.2 Funktionsweise

Das Prinzip von KI besteht darin, aus einer grossen Menge unstrukturierter Daten (***Big Data***) mit Hilfe eines auf den konkreten Verwendungszweck zugeschnittenen Algorithmus gewisse Muster zu erkennen, um daraus eine Schlussfolgerung abzuleiten. Dazu werden sogenannte **neuronale Netze** *(Neural Networks)* eingesetzt, deren Algorithmen und Struktur sich an der Funktionsweise des menschlichen Gehirns orientieren: Viele einzelne Algorithmen arbeiten dabei in einer vernetzten Weise zusammen, die der Vernetzung der Synapsen im Gehirn nachempfunden ist. Bei komplexen neuronalen Netzen mit mehreren Verarbeitungsschichten (d.h. mit vielen hintereinandergeschalteten und sich gegenseitig beeinflussenden Algorithmen) spricht man von ***Deep Neural Networks***.

Die Art und Weise, in der die Algorithmen miteinander interagieren, wird bei komplexen ("tiefen") neuronalen Netzen nicht mehr vom Entwickler vorgegeben, da die Zahl der festzulegenden Parameter viel zu gross ist. Stattdessen werden dem neuronalen Netz geeignete (d.h. auf den konkreten Verwendungszweck ausgerichtete) **Trainingsdaten** vorgelegt (z.B. Röntgenbilder mit diagnostizierten Tumorherden), welche dieses in einer Vielzahl automatisierter Trainingszyklen verarbeitet. Dabei sucht das neuronale Netz durch **statistische Optimierungsprozesse** die bestmögliche Einstellung *(Parametrisierung)*, z.B um danach auf neuen Röntgenbildern selbständig Tumorherde zu erkennen. Dieser Vorgang der automatisierten Einstellung des neuronalen Netzes wird als ***Deep Learning*** bezeichnet.

Die Qualität einer KI-Anwendung hängt von ihrer Architektur, ihrem Training und der Qualität der Trainingsdaten ab.

Sowohl die Struktur des neuronalen Netzes wie auch dessen Einstellung müssen auf den **konkreten Anwendungszweck** ausgerichtet sein, den die KI-Anwendung erfüllen soll (z.B. Sprach- oder Bilderkennung, Textgenerierung etc.). Im Idealfall ist die KI-Anwendung dann in der Lage, aus einer grossen Datenmenge (z.B. dem Datenstrom einer Überwachungskamera) in kürzester Zeit diejenige Art von Mustern zu erkennen, auf die sie trainiert wurde (z.B. Gesichter, Autokennzeichen, etc.). Wie erfolgreich sie dabei ist, hängt von der Architektur des neuronalen Netzes, der Art und Weise des Trainings sowie der Qualität der Trainingsdaten ab.

1.3 Einsatzbereiche

KI-Anwendungen eignen sich, um in kurzer Zeit viele, hochkomplexe oder dynamisch ändernde Daten auf gewisse Muster hin zu analysieren (z.B. Kreditkartendaten zur Betrugsbekämpfung, Sprach- und Bilderkennung in Echtzeit, Umgebungsorientierung autonomer Fahrzeuge).

2 Rechtliche Aspekte

Unabhängig davon, in welchem Bereich und für welchen Zweck eine KI-Anwendung eingesetzt wird, stellen sich rechtliche Fragen zur **Erstellung** (Ziff. 2.1), zur **Parametrisierung** (Ziff. 2.2), und zum **Einsatz** (Ziff. 2.3) von KI-Anwendungen.

2.1 Bei der Erstellung

Bei der Erstellung von KI-Anwendungen sind für Eigenersteller wie für Dritthersteller Fragen zum Schutz der KI-Anwendung sowie zur Integration in physische Produkte relevant.

Software ist urheberrechtlich geschützt, Algorithmen und Parametrisierungen hingegen nicht. Eine KI-Anwendung wird zwar softwaretechnisch umgesetzt, basiert aber grösstenteils auf Algorithmen und deren Parametrisierung. Für eine Patentierung fehlt es zumeist am technischen Charakter. Das *Herzstück* einer KI-Anwendung lässt sich somit **weder urheber- noch patentrechtlich schützen**. Der Ersteller eine KI-Anwendung sollte deshalb alternative Schutzmassnahmen treffen, wie z.B. vertragliche Vorgaben zur Geheimhaltung.

Oft werden **KI-Anwendungen in physische Produkte integriert** (z.B. in "smarte" Geräte, Maschinen, Roboter), die der Gesetzgebung zur Produktehaftpflicht (PrHG) und Produktesicherheit (PrSG) unterliegen. Diesfalls ist der zusätzlichen Komplexität Rechnung zu tragen, die sich durch den Einsatz von KI ergibt (z.B. bei der Produktbeobachtung, wenn sich KI-basierte Produkte nach Inverkehrsetzung durch Interaktion mit den Nutzern weiterentwickeln).

Entwickler, die KI-Anwendungen für Dritte erstellen, sind mit den **üblichen Fragen bei ICT-Verträgen** konfrontiert: Ein Vertrag über die Erstellung einer KI-Anwendung ist ein Werkvertrag, bei dem sich insbesondere Fragen zur Leistungs- und Mängeldefinition stellen (Wie sind die Anforderungen an eine KI-Anwendung zu spezifizieren, und wann liegt ein Mangel vor?) und zur Haftung. Der Entwickler kann z.B. gegenüber dem Kunden haften, wenn er einen für den gewünschten Anwendungszweck ungeeigneten Algorithmus oder eine für diesen Zweck ungeeignete Struktur des neuronalen Netzes wählt. Hier ist den Parteien zu raten, im Vertrag die definierten Anwendungszwecke und Vorgaben des Kunden genau festzuhalten. Einer präzisen Regelung bedarf es zudem, wenn der Kunde die KI-Anwendung selbst trainiert oder die Trainingsdaten stellt (vgl. dazu Ziff. 2.2), die KI-Anwendung selbst weiterentwickelt oder für andere Zwecke einsetzen will als für die ursprünglich angedachten.

2.2 Beim Training (Parametrisierung)

Das neuronale Netz einer KI-Anwendung muss anhand möglichst vieler und möglichst zweckmässiger Trainingsdaten **parametrisiert ("trainiert")** werden. Im Training durchläuft es eine Vielzahl von Optimierungszyklen, bis schliesslich die für den vorgesehenen Zweck optimale Einstellung ("Parametrisierung") der einzelnen Algorithmen erreicht ist, aus denen das neuronale Netz besteht. Hier stellen sich Fragen zur Qualität und rechtlichen Schützbarkeit der Trainingsdaten sowie zum Datenschutz.

Die **Auswahl und Qualität der Trainingsdaten** beeinflussen die Ergebnisse, die die KI-Anwendung im produktiven Einsatz erbringt: Werden ungeeignete Daten ausgewählt oder sind diese von schlechter Qualität (z.B. im Aufbau, Inhalt und Informationsgehalt nicht vergleichbar mit den späteren Input-Daten), so wird die KI-Anwendung im produktiven Einsatz kaum die gewünschten Resultate liefern.

Zudem sind an die Auswahl der Trainingsdaten hohe Anforderungen zu stellen, um nicht vorbestehende (unerwünschte) Tendenzen in die KI-Anwendung zu übertragen. Wie bisherige Erfahrungen gezeigt haben, ist dies gerade bezüglich **Gleichstellungs- und Diskriminierungsaspekten** relevant: Sind die Trainingsdaten unausgeglichen zusammengesetzt (z.B. bezüglich Geschlecht oder Hautfarbe), so wird auch die damit trainierte KI-Anwendung diese Unausgeglichenheit übernehmen (sog. ***"Machine Bias"*** oder "automatische Voreingenommenheit"). Setzt ein Unternehmen eine KI-Anwendung mit einem solchen *Machine Bias* ein, läuft es Gefahr, gegen gesetzliche Gleichstellungsvorgaben und Diskriminierungsverbote zu verstossen (vgl. Ziff. 2.3).

Wer für das Training einer KI-Anwendung Dritte beizieht, ist gut beraten, sich **vertragliche Zusicherungen** zur Zusammensetzung und Qualität der Trainingsdaten und zur Angemessenheit des Trainings einräumen zu lassen. Wer das Training mit eigenen Daten durchführt, sollte diese auf deren Qualität und Angemessenheit hin prüfen.

Das Training einer KI-Anwendung und die dazu nötigen Trainingsdaten sind mindestens so relevant wie die Wahl der geeigneten Struktur und Algorithmen. Damit stellt sich die Frage nach der **Schützbarkeit der Trainingsdaten**. Unter Schweizer Recht sind reine Datensammlungen immaterialgüterrechtlich nicht schützbar. Umso wichtiger sind deshalb vertragliche Absicherungen zur Berechtigung, Geheimhaltung und Exklusivität der Trainingsdaten.

Oft enthalten Trainingsdaten auch Personendaten (z.B. können auf Bildern Personen erkennbar sein). Diesfalls sind die Vorgaben des **Datenschutzes** zu beachten, d.h. bei rein schweizerischen Verhältnissen das Datenschutzgesetz (DSG), bei EU-Bezug zusätzlich die Datenschutz-Grundverordnung (DSGVO). Werden Daten von Dritten bezogen, so sind vertragliche Zusicherungen vorzusehen. Werden eigene Daten verwendet, ist zu prüfen, ob deren Verwendung zulässig ist: Liegt keine Einwilligung der Betroffenen vor, so reicht die Absicht, eine KI-Anwendung zu erstellen, in der Regel nicht als Rechtfertigungsgrund. Allenfalls kann hier eine Anonymisierung der Trainingsdaten Abhilfe schaffen.

2.3 Beim Einsatz

Für **negative Folgen des Einsatzes einer KI-Anwendung** ist das einsetzende Unternehmen genauso verantwortlich wie für andere Hilfsmittel. Selbst wenn der KI-Anwendung eine gewisse Autonomie zugestanden wird und sie infolge einer autonomen Entscheidung einen Schaden verursacht, so kann das einsetzende Unternehmen daraus nichts zu seiner Verteidigung ableiten: Einer KI-Anwendung kommt keine rechtliche Selbständigkeit zu, **das "Handeln" einer KI-Anwendung wird stets dem einsetzenden Unternehmen zugerechnet**. Es stellt sich somit die Frage nach der Haftung für KI-basierte Entscheidungen und allfälligen Regressmöglichkeiten.

Bei Haftungsfragen kommt der Nachvollziehbarkeit des Entscheidungsprozesses der KI-Anwendung grosse Bedeutung zu.

Führt der Einsatz einer KI-Anwendung zu einem Schaden, so stellt sich die Frage nach dem Grund dafür: Lag es an der unpassenden Struktur des neuronalen Netzes? An unzureichend ausgeführtem Training? Oder an den Trainingsdaten? In diesen Fällen läge die Schadensursache im Verantwortungsbereich des Herstellers. Falls der Grund aber in einem Bedienungsfehler lag (z.B. Eingabe ungeeigneter Daten), oder daran, dass die KI-Anwendung für einen anderen Zweck eingesetzt wurde als den, für den sie ursprünglich konzipiert wurde, läge dies im Verantwortungsbereich des einsetzenden Unternehmens. Voraussetzung für die Identifikation der Fehlerquelle bildet in jedem Fall die **Nachvollziehbarkeit** des Verarbeitungs- und Entscheidungsprozesses der KI-Anwendung (sogenannte ***"Algorithmic Explainability"***). Ein Unternehmen, das von Dritten erstellte/trainierte KI-Anwendungen einsetzt, sollte deshalb auch hierzu entsprechende Zusicherungen einholen und sich umfassend dokumentieren lassen.

Eine unpassend programmierte/trainierte KI-Anwendung kann zu Verstössen gegen Gleichstellungsgebote und Diskriminierungsverbote führen: Werden z.B. aufgrund eines Machine Bias durch KI-basierte Entscheidungen systematisch Frauen benachteiligt (z.B. bei Einstellungs- oder Lohnfragen), so kann eine Verletzung des Gleichstellungsgesetzes (GIG) vorliegen.

Je nach Einsatzbereich müssen **zwingende sektorspezifische Vorschriften** beachtet werden (z.B. im Strassenverkehr bei selbstfahrenden Autos, im Gesundheitswesen bei KI-basierten Medizinalprodukten oder im Finanzbereich bei der automatisierten Portfolioverwaltung). Eine KI-Anwendung ist deshalb so zu implementieren, dass sie derartige Vorgaben in jedem Fall berücksichtigt. Wer eine KI-Anwendung von einem Dritthersteller beschafft, sollte hierzu entsprechende Zusicherungen vorsehen.

Werden KI-Anwendungen nicht bloss als Hilfsmittel zur Entscheidvorbereitung eingesetzt, sondern für **automatisierte Entscheidungen** selbst (z.B. zur automatischen Bewilligung/Ablehnung eines Kredits aufgrund einer KI-basierten Prüfung

der Kreditwürdigkeit), so müssen allenfalls auch **datenschutzrechtliche Pflichten** beachtet werden: Im Anwendungsbereich der DSGVO ist ein Recht der Betroffenen vorgesehen, nicht einer Entscheidung unterworfen zu sein, die ausschliesslich auf einer automatisierten Entscheidfindung basiert. Im DSG ist dies derzeit noch nicht der Fall, soll aber im Rahmen dessen Revision in ähnlicher Weise eingeführt werden.

Werden KI-Anwendungen für **kreative Prozesse** eingesetzt (z.B. zur Gestaltung neuer Produkte), stellt sich die Frage, wie Resultate geschützt werden können, die autonom von einer KI-Anwendung geschaffen wurden. Mangels eines menschlichen *Schöpfers* sind solche Arbeitsergebnisse **urheberrechtlich nicht schützbar** und beim Schutz nach Designgesetz (DesG) stellt sich die Frage, wer als *Designer* gilt: Der Hersteller der KI-Anwendung, deren Trainer, der Lieferant der Input-Daten, oder derjenige, der die KI-Anwendung einsetzt? Umso wichtiger sind auch hier passende **vertragliche Regelungen** zum Einsatz der KI-Anwendung und zur Verwendung der damit erstellten Arbeitsergebnisse.

3 Fazit

KI-Anwendungen sind vielseitig einsetzbar und bergen grosses Potential, bringen aber auch zahlreiche **rechtliche Risiken** mit sich. Da die Gesetzgebung der durch KI-Anwendungen geschaffenen Komplexität und den damit verbundenen speziellen Fragen (noch) nicht Rechnung trägt, sollten die rechtlichen Risiken durch **organisatorische Massnahmen** und **vertragliche Regelungen** mit den involvierten Parteien adressiert werden.

Roland Mathys, LL.M.
Partner Zürich
roland.mathys@swlegal.ch

Dr. Samuel Klaus, LL.M.
Senior Associate Zürich
samuel.klaus@swlegal.ch

Louis Burrus
Partner Genf
louis.burrus@swlegal.ch

Prof. Dr. Olivier Hari
Of Counsel Genf
olivier.hari@swlegal.ch

Schellenberg Wittmer AG ist Ihre führende Schweizer Wirtschaftskanzlei mit mehr als 150 Juristinnen und Juristen in Zürich und Genf sowie einem Büro in Singapur. Wir kümmern uns um alle Ihre rechtlichen Belange – Transaktionen, Beratung, Prozesse.

Schellenberg Wittmer AG
Rechtsanwälte

Zürich
Löwenstrasse 19
Postfach 2201
8021 Zürich / Schweiz
T +41 44 215 5252
www.swlegal.ch

Genf
15bis, rue des Alpes
Postfach 2088
1211 Genf 1 / Schweiz
T +41 22 707 8000
www.swlegal.ch

Singapur
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapur 049909
T +65 6580 2240
www.swlegal.sg