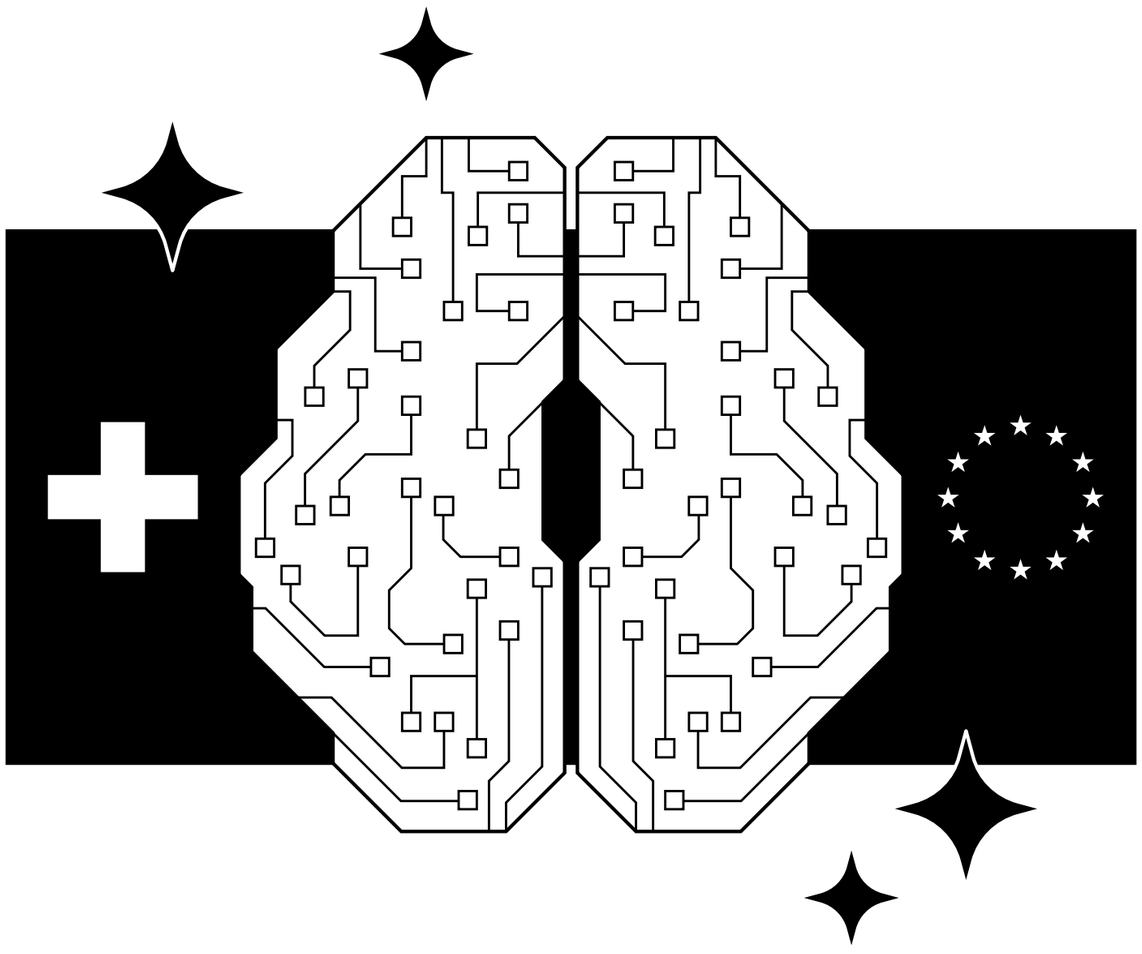
Rechtliche Rahmenbedingungen



für künstliche Intelligenz

Schon seit Jahren filtert KI unsere Spam-Mails, übersetzt auf DeepL unsere Texte und entscheidet auf Social Media, was uns angezeigt wird. Mit ChatGPT wurde Ende November 2022 eine generative KI veröffentlicht, die einfach in der Anwendung ist und auf sämtliche Fragen eine Antwort weiss – oftmals sogar eine korrekte. Seither wurde generative KI in Windeseile Teil des Alltags und es scheint, als seien generativer KI keine Grenzen gesetzt.

Regulierung in der Schweiz

Obwohl es in der Schweiz bisher kein «KI-Gesetz» gibt, muss künstliche Intelligenz bereits den jetzt geltenden – in der Regel technologieneutral verfassten – Gesetzen entsprechen.

Zur Prüfung des Gesetzgebungsbedarfs hat der Bundesrat dem eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK am 22. November 2023 den Auftrag gegeben, bis Ende 2024 eine Übersicht möglicher Regulierungsansätze zu erstellen. Am 12. Februar 2025 legte das UVEK dem Bundesrat seine Auslegeordnung zur Regulierung von künstlicher Intelligenz vor. Darin skizziert das UVEK die unterschiedlichen Möglichkeiten einer Regulierung von KI und weist insbesondere auf die KI-Konvention des Europarats hin. Der Bundesrat hat sich für folgenden Regulierungsansatz entschieden:

- Die Schweiz soll die KI-Konvention ratifizieren und in das Schweizer Recht übernehmen.
- Die Schweiz soll, wo Gesetzesanpassungen nötig sind, einen möglichst sektorbezogenen Ansatz verfolgen. In zentralen, grundrechtsrelevanten Bereichen wie dem Datenschutz werden jedoch auch allgemeine Regulierungen angestrebt.
- Neben der Gesetzgebung sollen auch rechtlich nicht verbindliche Massnahmen zur Umsetzung der KI-Konvention erarbeitet werden, beispielsweise Selbstdeklarationsvereinbarungen oder Branchenlösungen.

Insgesamt soll KI so reguliert werden, dass ihr Potential für den Wirtschafts- und Innovationsstandort Schweiz nutzbar gemacht wird und die Risiken für die Gesellschaft möglichst klein bleiben. Der Bundesrat hat einen pragmatischen Mittelweg gewählt und will nur in wenigen Bereichen auf eine horizontale Regelung setzen.

Das Ziel der KI-Konvention ist, dass KI-Systeme während ihres gesamten Lebenszyklus mit den Menschenrechten, der Demokratie und der Rechtsstaatlichkeit vereinbar sind, wofür die KI-Konvention einige Grundsätze festsetzt. Zu diesen Grundsätzen gehören Menschenwürde und Selbstbestimmung, Transparenz und Überwachung, Gleichstellung und Nichtdiskriminierung sowie Privatsphäre und Datenschutz. Die KI-Konvention ist vorab auf Staaten und deren Institutionen ausgerichtet, ebenso wie auf private Akteure, welche im Namen von Staaten handeln.

RECHT

«Es gilt der Grundsatz: so viel wie nötig, so wenig wie möglich. Weiter betont der EDÖB die Wichtigkeit der Transparenz.»

Regulierung der EU

Anders als die Schweiz hat sich die EU für eine gesamtheitliche, horizontale Regelung von KI entschieden. Sie hat sehr schnell auf die Entwicklung von KI reagiert und bereits am 1. August 2024 den «AI-Act» in Kraft gesetzt.

Der Anwendungsbereich des AI-Acts ist extraterritorial. Für die Anwendbarkeit des AI-Acts genügt es, wenn die entsprechende KI-Anwendung in der EU in Verkehr gebracht oder in Betrieb genommen wird, ohne dass der Anbieter in der EU niedergelassen sein muss. Der AI-Act ist zudem für Anbieter und Betreiber von KI-Systemen auch dann anwendbar, wenn die vom KI-System hervorgebrachte Ausgabe, beziehungsweise das Resultat, in der EU verwendet wird. Zur Prüfung, ob die von Schweizer Unternehmen eingesetzten KI-Anwendungen unter den AI-Act fallen, stellt economiesuisse in Zusammenarbeit mit Kellerhals Carrard ein KI-Selbsteinschätzungstool zur Verfügung. Trotz EU-Bezug den AI-Act zu ignorieren, empfiehlt sich nicht: Je nach Verstoss drohen Sanktionen in der Höhe von bis zu CHF 35 000 000.00 oder 7% des weltweiten Jahresumsatzes.

AI Act Self-Assessment Tool

Einzelfragen aus dem Schweizer Recht

Datenschutzrecht

Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat am 9. November 2023 kommuniziert, dass das (damals noch sehr neue) Datenschutzgesetz direkt auf KI-gestützte Datenbearbeitungen anwendbar ist.

Der EDÖB nimmt vorab die Hersteller, Anbieter und Verwender von KI-Anwendungen in die Pflicht, bereits bei der Entwicklung neuer Technologien und bei der Planung ihres Einsatzes sicherzustellen, dass den betroffenen Personen (also den Personen, deren Personendaten mittels KI bearbeitet werden) ein möglichst hohes Mass an digitaler Selbstbestimmung zukommt. Es gilt der Grundsatz «so viel wie nötig, so wenig wie möglich». Weiter betont der EDÖB die Wichtigkeit der Transparenz. Den von der Datenbearbeitung betroffenen Personen soll es ermöglicht werden, einer automatischen Datenbearbeitung zu widersprechen oder eine automatisierte Einzelentscheidung von einem Menschen überprüfen lassen zu können. Zudem haben Benutzer von intelligenten Sprachmodellen (wie beispielsweise Chatbots) ein Recht darauf zu wissen, ob sie mit einem Menschen oder einer Maschine sprechen und ob die eingegebenen Daten verwendet werden, beispielsweise zur Verbesserung der selbstlernenden Programme. Schliesslich weist der EDÖB im Rahmen seinen Ausführungen noch darauf hin, dass die Verwendung von Deep Fakes deutlich erkennbar sein muss.

Der EDÖB geht auch auf KI-gestützte Datenbearbeitungen mit hohem Risiko ein. Diese seien zulässig, wenn angemessene Massnahmen ergriffen und eine Datenschutz-Folgenabschätzung durchgeführt werde. Der EDÖB hat sich wohl vom AI-Act inspirieren lassen, denn er erwähnt an dieser Stelle einige Anwendungen, welche datenschutzrechtlich verboten seien. Dazu gehören die flächendeckende Gesichtserkennung in Echtzeit und das Social Scoring, welche auch unter dem AI-Act verboten sind.

Auf die Frage, inwiefern Personendaten für das Maschinenlernen verwendet werden dürfen, geht der EDÖB nicht ein. KI benötigt eine riesige Menge an Daten, um zu funktionieren, beziehungsweise um zu «lernen». An dieser Stelle sei lediglich darauf hingewiesen, dass bei der Zusammenarbeit mit Auftragsbearbeitern, welche KI-Tools anbieten oder entwickeln, die Vertragsbestimmungen des Auftragsbearbeiters genau geprüft werden sollten. Wenn darin vorgesehen ist, dass die Daten weiterverwendet werden, sind die notwendigen Massnahmen (insb. die Anpassung der Datenschutzerklärung) zu ergreifen, sofern der Vertrag trotzdem abgeschlossen wird.

In datenschutzrechtlicher Hinsicht steht KI vor verschiedenen praktischen Herausforderungen: Wie kann geprüft und dargelegt werden, dass automatisch getroffene Entscheidungen einer KI korrekt sind? Wie wird verhindert, dass die KI-Verzerrungen oder blinden Flecken ausgesetzt ist und deshalb Personen vor- oder nachteilig behandelt? Und wie kann sichergestellt werden, dass sich die für das Training von KI-Modellen verwendeten Personendaten nicht aus diesen Modellen extrahieren lassen? Werden diese Fragen sorgfältig geprüft und entsprechende Massnahmen umgesetzt, ist die Verwendung von KI datenschutzrechtlich nicht problematischer oder an höhere Voraussetzungen gebunden als eine «normale» Bearbeitung von Personendaten.

Urheberrecht

Die zentralen urheberrechtlichen Fragen im Zusammenhang mit KI sind: Darf ich urheberrechtlich geschützte Werke für das Training der KI benutzen? Und wem gehört, was die KI erstellt hat?

Das Urheberrechtsgesetz gewährt dem Urheber ein absolutes Ausschliesslichkeitsrecht an seinem Werk. Der Urheber hat unter anderem das ausschliessliche Recht zu bestimmen, ob wann und wie das Werk verwendet wird (Art. 10 Abs. 1 URG). Die juristische Lehre geht mehrheitlich davon aus, dass die Verwendung von urheberrechtlichen Werken für das KI-Training einen Eingriff in das Vervielfältigungsrecht darstellt. Für die Verwendung von urheberrechtlich geschützten Werken ist vor diesem Hintergrund entweder die Zustimmung des Urhebers oder die Anwendbarkeit einer urheberrechtlichen Ausnahme notwendig. Die urheberrechtlichen Ausnahmen werden jedoch eng ausgelegt und keine erscheint für das KI-Training einschlägig. Das Training von KI mit urheberrechtlich geschützten Werken ist folglich problematisch. Es gibt deshalb Bemühungen, Lizenzverträge abzuschliessen, um das KI-Training urheberrechtlich abzusichern und die Urheber zu vergüten.

Betreffend urheberrechtlichen Schutz von KI-generiertem Inhalt ist vorab festzuhalten, dass der urheberrechtliche Schutz auch für den Output gilt, wenn urheberrechtlich geschützte Werke für das KI-Training oder den Prompt verwendet werden, und die Werke im Output (also im KI-generierten Inhalt) erkennbar sind. Weitergehend ist ein Werk urheberrechtlich in der Schweiz nur geschützt, wenn es eine «geistige Schöpfung» ist (Art. 2 Abs. 1 URG). Das Urheberrecht geht von einer menschlichen Schöpfung aus – für nicht menschengeschaffene Inhalte besteht kein Urheberrechtsschutz. Ein urheberrechtlicher Schutz kommt vor diesem Hintergrund nur dann in Frage, wenn die KI als «Werkzeug» verwendet wird, ähnlich einer Kamera oder eines Stifts. Dies kann insbesondere dann der Fall sein, wenn der Mensch erheblich zum Output beigetragen hat (bspw. sich die Kreativität eines Prompts sich im Output niederschlägt) oder er den Output abgeändert hat (Output nur als Grundlage für das danach entstehende Werk). Ein Urheberrechtsschutz für den Output von KI kann somit nur bei einer Bearbeitung oder erheblichen Beeinflussung des Outputs durch den Menschen im Einzelfall bejaht werden.

«Stand heute gilt für künstliche Intelligenz die sogenannte ‹Werkzeugtheorie›: **Die Entscheidungen und Handlungen der Maschine gelten als diejenigen des Anwenders.»**

Haftung

Da KI sehr unterschiedlich ausgestaltet und angewendet werden kann, gibt es auch keine allgemeine Antwort auf die Frage, wer für die KI und deren Fehler haftet.

Obwohl Schweizer Gesetze grundsätzlich technologieneutral ausgestaltet sind, werden teilweise neue Entwicklungen erst verzögert abgebildet. So ist das Schweizer Produkthaftpflichtgesetz bis heute gemäss Wortlaut nur auf bewegliche Sachen und Elektrizität anwendbar (Art. 3 Abs. 1 PrHG). Ob und inwiefern eine Software als Produkt gilt, ist umstritten und wird in der Lehre stark diskutiert. Da zwischen Hersteller und Anwender in der Regel ein Vertragsverhältnis besteht, ist neben der produkthaftpflichtgesetzlichen auch an die vertragsrechtliche Haftung zu denken. So muss der Hersteller sicherstellen, dass bei der Entwicklung des KI-Systems mit der angemessenen Sorgfalt gearbeitet wurde. Ist eine KI fehlerhaft, beziehungsweise kann einem Hersteller eine Verletzung der Sorgfaltspflicht bewiesen werden, ist die Haftung des Herstellers eines KI-Systems denkbar.

In der Praxis wohl relevanter wird die Frage sein, ob der Anwender einer KI für die Resultate der KI haftet. Stand heute gilt für künstliche Intelligenz die sogenannte «Werkzeugtheorie»: Die Entscheidungen und Handlungen der Maschine gelten als diejenigen des Anwenders. Sofern also ein vertragliches Verhältnis zwischen dem Anwender und der geschädigten Person vorliegt, muss geprüft werden, ob der Anwender bei der Erfüllung seines Vertrages die angemessene Sorgfalt gewahrt hat. Gerade bei generativer KI im Dienstleistungsbereich (Rechtsberater, Architekten, Ingenieure) dürfte mit einer direkten Weiterverwendung des Outputs einer KI zum heutigen Stand die Sorgfaltspflicht in jedem Fall verletzt werden. Der Output ist stets kritisch zu prüfen und wo notwendig anzupassen, bevor er der Kundschaft vorgelegt wird.

Rechtlich komplizierter wird es bei der ausservertraglichen Haftung, weil KI äusserst flexibel angewendet werden kann. Eine gewisse Fehleranfälligkeit liegt deshalb in der Natur einer KI. Mit diesen Überlegungen lässt sich argumentieren, dass die Verwendung einer KI naturgemäss ein Gefährdungspotential mit sich bringt und den Anwender deshalb eine Schadenminderungspflicht trifft. Es sind deshalb beim Einsatz von KI die für das betroffene System angemessenen Sicherheitsmassnahmen zu treffen.

Das wichtigste in Kürze

KI ist aus dem Alltag nicht mehr wegzudenken. Beim beruflichen Umgang damit gilt es jedoch, einige Kernfragen zu beachten:

- Ist der AI-Act anwendbar und wenn ja, halten wir die entsprechenden Vorschriften ein?
- Wissen wir, welche Daten unsere KI-Anbieter für das KI-Training verwenden und ob sie das Datenschutzrecht einhalten?
- Verwendet der KI-Anbieter unsere Daten für das KI-Training? Wenn ja, wird dies in unserer Datenschutzerklärung abgebildet?
- Welche Daten und vor allem welche Personendaten dürfen wir für welche KI-Systeme verwenden?
- Haben wir den Output der KI auf dessen Richtigkeit hin geprüft und bei Bedarf angepasst?
- Entspricht der Output einem urheberrechtlichen Werk und verletzt er dadurch das Urheberrecht?

●

Dr. Mario Marti, Rechtsanwalt, Geschäftsführer suisse.ing
Leandra Gafner, Rechtsanwältin, Kellerhals Carrard