ANWALTS
REVUE
DE L'AVOCAT

Stämpfli
Verlag

Anwaltsrevue|Revue de l'avocat 9/2024 |S. 360–365 **360**

Thema

KÜNSTLICHE INTELLIGENZ IN DER ANWALTSPRAXIS

David Schwaninger RA lic. iur., LL.M. Partner Blum&Grob Rechtsanwälte AG, Mitglied der Fachgruppe Digitalisierung des Schweizerischen Anwaltsverbandes (SAV)

Simon Fritsch RAass. iur. (RAK Berlin), LL.M. Associate Blum&Grob Rechtsanwälte AG

Stichworte: künstliche Intelligenz, Anwaltspraxis, Datenschutz, Immaterialgüterrecht, Berufsgeheimnis

I. Einleitung

Künstliche Intelligenz ist seit Monaten in aller Munde. Sie ist branchenübergreifendes Gesprächsthema und hält Einzug in alle Berufsfelder. Auch Anwältinnen und Anwälte sind davon betroffen. Als Juristinnen und Juristen und gerade bei der eigenen Nutzung gilt es jedoch, einige Grenzen und Herausforderungen zu bedenken, die es zum einen allgemein beim Einsatz von künstlicher Intelligenz im Arbeitsalltag und zum anderen speziell für die Anwaltschaft zu beachten gilt.

Künstliche Intelligenz stellt in diesem Zusammenhang ein weder juristisch noch technisch genau definiertes Gebiet dar, das jedoch aus Gründen der Verständlichkeit dieses Beitrags auf sogenannte Large Language Models[1] beschränkt und für diesen Beitrag synonym verwendet werden soll,[2] da diese für den absoluten Grossteil der Anwaltschaft am interessantesten sein dürften.[3]

Spätestens die jüngst verabschiedete EU-Verordnung zur künstlichen Intelligenz, gemeinhin als EU AI Act bezeichnet,[4] hat die rechtlichen Implikationen von künstlicher Intelligenz in den Fokus der Gesellschaft gerückt. Dabei regelt der EU AI Act nicht Rechtsbereiche, die bereits durch andere Gesetze abgedeckt sind, sondern schafft als Gesetz *sui generis* ein Regelwerk, das vor allem einen einheitlichen Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Nutzung schaffen soll.[5]

Auch wenn der Geltungsbereich des EU AI Act über die EU hinausgeht,[6] wird sich dieser Beitrag auf die hiesige Rechtslage konzentrieren und untersuchen, was Schweizer Anwältinnen und Anwälte beim Einsatz von künstlicher Intelligenz zu beachten haben. Dabei ist zu erwähnen, dass selbstverständlich bei der Implementierung und Nutzung aller neuen Werkzeuge, Mittel und Hilfsmittel das gesamte Recht zur Anwendung kommt und sich in einzelnen Spezialgebieten besondere Probleme ergeben können. In diesem Beitrag sollen jedoch die Problemfelder beleuchtet werden, die bei der Anwendung von künstlicher Intelligenz stets zu beachten sind. Dabei ist vorwegzunehmen, dass bei Beachtung der im Folgenden aufgezeigten Grenzen der Einsatz künstlicher Intelligenz weniger problematisch ist als gemeinhin angenommen.

II. Grundlagen

II. Grundlagen

Vor den rechtlichen Grenzen sind jedoch die tatsächlichen Grenzen zu beachten. Künstliche Intelligenz und insbesondere Large Language Models wie ChatGPT haben in den letzten Jahren erhebliche Fortschritte gemacht und werden zunehmend in juristischen Arbeitsprozessen eingesetzt.[7] Um die Möglichkeiten und Grenzen dieser Technologien zu verstehen, ist ein grundlegendes Verständnis ihrer Funktionsweise erforderlich.[8] Im Folgenden wird in

abstrakter Form erläutert, wie man sich die Funktionsweise von Large Language Models vorstellen kann und wie ihre Funktionsweise sie daher in mancher Hinsicht auch einschränkt.

Large Language Models basieren auf einem maschinellen Lernansatz namens «Deep Learning»[9], bei dem künstliche neuronale Netzwerke genutzt werden. Diese Netzwerke bestehen aus vielen miteinander verbundenen Knoten (den Neuronen), die in Schichten angeordnet sind. Das Modell wird mit riesigen Mengen an Textdaten trainiert und lernt dabei, Muster und Zusammenhänge in der Sprache zu erkennen. Der Trainingsprozess erfolgt durch «überwachtes Lernen», bei dem das Modell seine internen Parameter anhand von Trainingsdaten, die beschriftet sind,[10] anpasst, um Texte zu verstehen und zu generieren.

Ein Schlüsselmerkmal von Large Language Models ist ihre Fähigkeit, den Kontext von Texten zu berücksichtigen. Sie analysieren nicht nur einzelne Wörter, sondern den gesamten Kontext eines Satzes oder Dokuments. Dies ist auch besonders wichtig in der juristischen Praxis, wo die Bedeutung eines Begriffs stark vom Kontext abhängt. Large Language Models generieren Texte, indem sie Wahrscheinlichkeiten berechnen und das wahrscheinlichste nächste Wort bzw. den wahrscheinlich nächsten Wortbestandteil auswählen. Dies ermöglicht es, flüssige Texte zu erstellen, birgt jedoch auch das Risiko, dass ungenaue oder unzutreffende Informationen entstehen. Bei objektiv falschen Ergebnissen spricht man auch von Halluzinationen.

Wichtig ist, dass Large Language Models keine echten «Kenntnisse» oder kein echtes «Verständnis» im menschlichen Sinne haben. Sie basieren auf der Analyse von Mustern in den Trainingsdaten und besitzen keine Fähigkeit zur kritischen Reflexion oder ethischen Bewertung. Dies limitiert ihre Anwendung im juristischen Kontext derzeit noch erheblich.

Ein häufiges Missverständnis in Bezug auf den Einsatz von künstlicher Intelligenz ist, dass die Eingabe[11] notwendigerweise für das Training verwendet werde. Dies ist zumindest bei den gängigen Modellen meist nicht der Fall. Vor allem bei der Verwendung eines Large Language Models wird beispielsweise eine «eingefrorene», bereits vortrainierte Version des jeweiligen Modells verwendet.[12] Die eigene Eingabe wird vom Modell lediglich verarbeitet, verbleibt aber nicht im Modell. Allerdings ist hier Vorsicht geboten, da die Anbieter die Eingaben natürlich zumindest zur Verarbeitung auf ihren Servern zwischenspeichern müssen und viele sich auch vertraglich zusichern lassen, die Eingaben für zukünftiges Training ihrer Large Language Models verwenden zu dürfen.

Die Grenzen von Large Language Models liegen insbesondere in ihrer mangelnden Fähigkeit zur kritischen Analyse und ethischen Bewertung. Sie sind nicht für Aufgaben geeignet, die eine tiefgreifende juristische Interpretation oder eine kritische Auseinandersetzung mit einer Materie erfordern. Sie können jedoch für Aufgaben wie die Automatisierung einfacher Textverarbeitung oder (soweit das Berufsgeheimnis und der Datenschutz beachtet werden) auch zur Generierung von Texten nützlich sein. Juristen sollten Large Language Models daher eher als unterstützendes Werkzeug betrachten und nicht als Ersatz für fundierte juristische Fachkenntnisse.

Auch wenn viele aktuelle Versionen solcher Large Language Models inzwischen integrierte Lösungen für Rechenaufgaben anbieten, ist das Grundkonzept von Large Language Models nicht für das Rechnen ausgelegt. Soweit also in der juristischen Arbeit Rechenaufgaben anfallen, z.B. die Berechnung von Schadenshöhen, Zinsen, Fristen oder Prozesskosten, ist derzeit von der Verwendung eines Large Language Models eher abzuraten, es sei denn, das Modell gibt in nachvollziehbarer Weise einen überprüfbaren Rechenweg vor. Der Grund hierfür liegt in der bereits erwähnten wahrscheinlichkeitsbasierten Arbeitsweise und daran, dass der Schwerpunkt des Trainings auf dem Sprachverständnis und nicht auf der numerischen Genauigkeit liegt. Eine Rechenaufgabe oder Zahlen werden also primär als Text verstanden und die «Lösung» wird daher nur nach Wahrscheinlichkeit und Ähnlichkeit zu ähnlichen Texten dargestellt.

Bei den oben genannten Punkten ist daher immer Vorsicht geboten, zumal Large Language Models ungern zugeben, dass sie etwas nicht können oder falsch machen, und die Ergebnisse oft selbstbewusst und überzeugend klingen.

III. Rechtlicher Rahmen

1. Datenschutz

Durch die jüngste Novellierung des Datenschutzgesetzes ist der Datenschutz auch im Bereich der künstlichen Intelligenz eines der prominentesten Themen. Gerade im Arbeitsalltag liegt es auf der Hand, dass bei der Dateneingabe immer wieder Personendaten bearbeitet werden. Zur Erinnerung: Personendaten sind gemäss Art. 5 Abs. 1 DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Dies kann also beispielsweise auch bei E-Mail-Adressen oder Konto- und Steuernummern neben unzähligen anderen Daten der Fall sein. Enthält die Eingabe keine Personendaten, findet der Datenschutz zunächst keine Anwendung. Wenn Sie jedoch Personendaten in Ihrer Eingabe bearbeiten wollen, ist Folgendes zu beachten.

Ohne auf die technischen Details einzugehen, muss bei einem Large Language Model immer davon ausgegan-

gen werden, dass die Anbieter Personendaten bearbeiten, sofern solche in der Eingabe enthalten sind. [13]

Darüber hinaus gehen wir in der vorliegenden Analyse davon aus, dass die Mehrzahl der Anwältinnen und Anwälte zumindest derzeit noch Large Language Models von externen Anbietern nutzt.[14] Mit externen Anbietern sind hier all jene Anbieter gemeint, bei denen eine Kommunikation der Eingabe mit einem fremden (nicht eigenen) Server stattfindet, die in der Eingabe enthaltenen Daten also den eigenen Kontrollbereich verlassen und von einem Dritten (z.B. dem Anbieter des Large Language Models) bearbeitet werden.

Bei der Verwendung von Large Language Models externer Anbieter mit Personendaten ist daher darauf zu achten, dass der Anbieter des Large Language Models die Eingabe nicht für eigene Zwecke verwendet. Dies ist insbesondere immer dann der Fall, wenn eine Nutzung der Eingaben durch den Anbieter zu Trainingszwecken erlaubt ist[15], was jedoch in den meisten Fällen deaktiviert werden kann.[16] Darüber hinaus muss mit dem Anbieter des Large Language Models ein Vertrag zur Auftragsdatenbearbeitung abgeschlossen werden, in dem die Kriterien für eine angemessene und sichere Auftragsdatenbearbeitung festgelegt sind. Vielfach werden Verträge mit grossen Firmen wie OpenAI, Microsoft, Google oder anderen geschlossen, sodass man selten in der Position ist, verschiedene Vertragsdokumente anfordern zu können. Einige Subskriptionen enthalten jedoch entsprechende Verträge zur Auftragsdatenbearbeitung.[17] Sofern die Anbieter zudem in einem Land mit unzureichendem Datenschutzniveau ansässig sind, müssen zusätzlich zum Auftragsdatenbearbeitungsvertrag

entsprechende Absicherungen, z. B. in Form von Standardvertragsklauseln oder Garantien, getroffen werden.

Neben der Umsetzung der oben genannten Massnahmen ergeben sich noch weitere Aufgaben für den Datenschutz. Zum einen ist darauf zu achten, dass die Informationspflichten gegenüber den betroffenen Personen weiterhin korrekt erfüllt werden, beispielsweise in einer Datenschutzerklärung. Dies bedeutet insbesondere, dass die angegebenen Zwecke der Bearbeitung von Personendaten auch bei der Bearbeitung durch künstliche Intelligenz eingehalten bleiben. Aufgrund der Rechtsprechung des Bundesgerichts[18] ist zudem damit zu rechnen, dass die AGB-Kontrolle auch auf andere Vertragswerke und Datenschutzerklärungen ausgedehnt wird[19] und ein angemessener Zweck, der die Bearbeitung durch künstliche Intelligenz abdeckt, auch für die betroffenen Personen vorhersehbar sein muss. Schliesslich ist – wie auch schon ohne den Einsatz künstlicher Intelligenz – darauf zu achten, dass die Personendaten richtig und vollständig sind, die Rechte der Betroffenen weiterhin gewährleistet werden können und bei einem denkbaren hohen Risiko eine Datenschutzfolgeabschätzung durchgeführt wird.

Sofern man die zuvor beschriebenen Massnahmen nicht durchführen will oder kann, bedeutet dies in der Praxis, dass man sich selbst und alle Mitarbeitenden verpflichten muss, vor jeder Eingabe in ein Large Language Model sicherzustellen, dass diese Eingabe keine Personendaten enthält. Dabei ist auch dringend darauf zu achten, dass eine etwaige Bereinigung der Eingabe nicht im Eingabefeld des jeweiligen Large Language Model erfolgt und auch keine Anonymisierung durch ein solches Large Language Model vorgenommen wird. Abgesehen von der Problematik, dass automatisierte Anonymisierungssysteme nicht immer alle Personendaten erkennen, stellt eine Anonymisierung von Personendaten bereits eine Bearbeitung im Sinne des Datenschutzes dar.[20] Das Kopieren der späteren Eingabe in das Eingabefeld führt bei einigen Anbietern zu einer direkten Bearbeitung der Anfrage oder zumindest zu einer Speicherung auf dem Server oder im Cache.[21] Dies bedeutet, dass eine Anonymisierung innerhalb des Eingabefeldes sinnlos ist, da die entanonymisierte Eingabe bereits datenschutzrechtlich durch den Anbieter bearbeitet wurde.[22] Insofern sollte die Bereinigung auf dem eigenen System erfolgen, z.B. durch eine Word- oder txt-Datei, in der alle Personendaten manuell gelöscht werden, bzw. mit einer Software, die auf eigenen Systemen läuft.

2. Berufsgeheimnis

Neben dem Datenschutz ist das Berufsgeheimnis gemäss Art. 13 BGFA zu beachten. Dem Berufsgeheimnis unterstehen selbstverständlich alle Angaben, die auf ein Mandat oder dessen Inhalt schliessen lassen oder solche enthalten. Es betrifft also mehr Informationen als nach dem Datenschutzgesetz, da Letzteres nur Daten schützt, mit denen eine natürliche Person bestimmt oder bestimmbar ist.

In Analogie zu den Personendaten kann das Problem umgangen werden, indem die Eingabe von mandatsbezogenen Daten bereinigt wird. Sofern also die Eingabe als sol-

che von Dritten nicht auf ein Mandat oder auf Daten aus einem solchen Mandat zurückgeführt werden kann,[23] sind die nachfolgenden Empfehlungen nicht weiter zu beachten.

Sofern jedoch die volle Potenz von Large Language Models ohne vorherige Bereinigung von Mandatsdaten genutzt werden soll, so muss man einige der folgenden Massnahmen treffen:[24]

- Der Anbieter des Large Language Models muss sich zur Einhaltung der berufsrechtlichen Geheimhaltung verpflichten.[25]

- Es ist eine clientseitige Verschlüsselung zu empfehlen, sofern diese Option besteht. Denn für gewöhnlich haben die Anbieter von IT-Dienstleistungen (also potenziell auch KI-Anbieter) häufig auch Zugriff auf Ihre Dateien, Uploads oder Kommunikation. Eine clientseitige Verschlüsselung lässt dabei nur den Zugriff durch Sie als Nutzerin oder Nutzer (= Client) zu und schliesst den Anbieter aus.
- Der Anbieter des Large Language Models muss eine angemessene Datensicherheit (nicht nur für Personendaten) gewährleisten. Damit einhergehend sollten die technischen und organisatorischen Massnahmen sowie der Standard für Personendaten auf alle Daten erweitert werden.
- Der manuelle Providerzugriff sollte beschränkt oder vollständig unterbunden werden.
- Es ist ratsam auf eine Defend-your-Data-Klausel zu bestehen. Damit verpflichtet sich der Anbieter bei Zugriffen auf die Daten durch Behörden alle Rechtsmittel und den gesamten Rechtszug – soweit möglich – auszuschöpfen, um den Zugriff durch die Behörde abzuwehren.
- Man sollte vorher eine Risikoabschätzung eines ausländischen Behördenzugriffs durchführen. Grosse Anbieter teilen Zahlen dazu meist selbst mit, mit denen man die Abschätzung vornehmen kann.

Um zu prüfen, welche Anbieter und Abonnementsmodelle angemessene Regelungen zum Datenschutz und zum Berufsgeheimnis enthalten, gibt es im Internet bereits verschiedene Übersichten.[26] Dabei ist jedoch zu beachten, dass die Geschäftsbedingungen und Abonnementbezeichnungen der verschiedenen Anbieter derzeit noch ständigen Änderungen und Anpassungen unterliegen, weshalb auf die Aktualität solcher Übersichten zu achten ist.

Die Probleme des Berufsgeheimnisses und des Datenschutzes können auch einfach dadurch umgangen werden, indem man sich für die Nutzung von KI-Tools die Einwilligung des Mandanten holt, Mandats- und Personendaten bei der Nutzung von künstlicher Intelligenz nutzen zu dürfen.[27] Dies kann von einzelnen Mandanten aber auch abgelehnt werden.

3. Immaterialgüterrecht und weitere Rechte

Sowohl bei der Eingabe als auch bei der Ausgabe [28] ist das geistige Eigentum in seiner Gesamtheit zu beachten.[29] Dabei spielt das Urheberrecht wohl die grösste Rolle, aber auch Marken-, Design-, Patentrechte oder Geschäftsgeheimnisse können betroffen sein. Um beim Beispiel des Urheberrechts zu bleiben, könnte die Eingabe von urheberrechtlich geschütztem Material eine Verletzung des Urheberpersönlichkeitsrechts nach Art. 9 URG durch fehlende Namensnennung und auch seiner wirtschaftlichen Verwertungsrechte durch unbefugtes Verbreiten und Zugänglichmachen nach Art. 10 URG bedeuten. Es ist daher darauf zu achten, dass die Eingabe in eine künstliche Intelligenz eines Drittanbieters keine Inhalte enthält, die nicht aus der eigenen Feder stammen und, falls doch, durch übertragene Rechte, Genehmigungen oder Lizenzen für diese Nutzung in einem Large Language Model gedeckt sind.

Darüber hinaus muss die Ausgabe auf Plagiate überprüft werden, weil ein durch künstliche Intelligenz generiertes Ergebnis auch vorbestehende Werke oder Elemente daraus übernehmen kann. Die Prüfung der Ausgabe auf Übereinstimmung mit vorbestehenden Werken ist in der Praxis nicht immer einfach. Sucht man über die Eingabe in den Large Language Models gezielt nach Quellen oder versucht man gezielt eine Sprache oder einen Stil zu imitieren, ist jedenfalls erhöhte Vorsicht geboten. Ergänzend können frei verfügbare Plagiatchecker aus dem Internet helfen. Dazu sollte man sich die Frage stellen, wofür man die Ausgabe verwendet bzw. inwieweit man diese ohnehin noch verändert. Durch weitere Überarbeitung sinkt die in der Regel geringe Gefahr eines Plagiates nämlich weiter. Bei der direkten Übernahme einer Ausgabe kann ein Plagiat indes nicht mit absoluter Sicherheit ausgeschlossen werden.

Darüber hinaus sind sowohl bei der Eingabe als auch bei der Ausgabe das Lauterkeitsrecht, das Persönlichkeitsrecht und nicht zuletzt das Strafrecht zu beachten. Allen dreien liegt die Tatsache zugrunde, dass man für die Verwendung eines Large Language Models und sowohl für seine Eingabe als auch für seine Ausgabe

in erster Linie selbst verantwortlich ist.

Der folgende Anwendungsfall soll dem Lauterkeitsrecht dienen: Man verwendet eine Sprachvorlage für einen LinkedIn-Post oder einen Werbetext auf der eigenen Website. Hier muss man gerade bei der Ausgabe darauf achten, dass man beispielsweise keine Superlativwerbung nach § 3 S. 1 lit. e UWG kreiert[30] oder falsche Berufsbezeichnungen nach § 3 S. 1 lit. c UWG verwendet. Darüber hinaus ist auch berufsrechtlich darauf zu achten, dass bei einer solchen Verwendung die berufsrechtlichen Werberegelungen und die zulässigen Bezeichnungen nach dem BGFA eingehalten werden.[31]

Das Persönlichkeitsrecht ist z.B. betroffen, wenn unrichtige, z.B. ehrverletzende Angaben über Personen gemacht werden und diese Angaben in die Eingabe gelangen oder in der Ausgabe verwendet werden.[32] Das Strafrecht ist ferner betroffen, wenn der Inhalt einer Eingabe oder Ausgabe einen strafrechtlichen Tatbestand erfüllt.

Die von einer künstlichen Intelligenz generierten Ergebnisse sind daher immer auf Richtigkeit und Rechtmässigkeit zu prüfen. Dies wiederum setzt voraus, dass der Benutzer fachlich in der Lage ist, die Ergebnisse zu beurteilen.

4. Vertragliche Regelungen des Anbieters

Unabhängig davon, ob bei der Nutzung von künstlicher Intelligenz auf kostenfreie oder kostenpflichtige Angebote bzw. Versionen der verschiedenen Anbieter zugegriffen wird, unterliegt jede Nutzung vertraglichen Regeln, meistens den von den Anbietern zur Verfügung gestellten Allgemeinen Geschäftsbedingungen. Diese enthalten dabei meist unter anderem Regelungen zu den Rechten an Eingaben und Ausgaben sowie zur Verantwortung und Haftung bei der Nutzung von Large Language Models. Auch wenn nicht selten fraglich ist, ob die vertraglichen Regelungen von Anbietern in dieser Form rechtmässig sind und damit Bestand haben werden, ist es ratsam, sich bis zu einer gegenteiligen Entscheidung des Gesetzgebers oder der Gerichte – soweit sinnvoll – daran zu halten.

Beispiele für zu beachtende Regeln sind folgende.

Um das Haftungsrisiko des Anbieters zu reduzieren, weist ein Anbieter in der Regel die Verantwortung und das Eigentum an den Eingaben und Ausgaben dem Nutzer zu. Das (geistige) Eigentum an der Eingabe liegt zumindest nach Schweizer Recht zweifelsfrei beim Urheber und damit in der Regel beim Nutzer, ob ihm die Ausgabe nach hiesiger Rechtslage urheberrechtlich zugerechnet werden kann, ist jedoch eher zu verneinen, da ein urheberrechtlich geschütztes Werk zumindest nach Schweizer Recht nur von natürlichen Personen geschaffen werden kann.[33] Verbreitet sind auch Klauseln, wonach sich Anbieter eine zeitlich und räumlich unbeschränkte Lizenz an den Eingaben und Ausgaben durch den Nutzer einräumen lassen. Was für Inhalte bei der Nutzung einer künstlichen Intelligenz an den betreffenden Drittanbieter übermittelt werden, will daher überlegt sein.

Nicht selten finden sich in den Vertragsbedingungen auch weitgehende Haftungsausschlüsse. Nach Schweizer Recht ist ein vollständiger Haftungsausschluss nicht zulässig. Weil aber oft ausländisches Recht und die Zuständigkeit ausländischer Gerichte vertraglich vorgegeben wird, kann man sich nicht auf die Regelungen nach Schweizer Recht verlassen. Insbesondere ändert es nichts an der Tatsache, dass der Nutzer gegenüber Dritten haftbar bleibt. Demnach ist davon auszugehen, dass bei der Verwendung der Ausgaben unter eigenem Namen, die sich daraus ergebenden Haftungsfragen auf einen selbst zurückfallen und es wenig überzeugend sein dürfte, sich entweder (a) durch die Verwendung eines Large Language Models zu exkulpieren oder (b) die Anbieter des

Large Language Models in Regress zu nehmen.[34] Letzteres käme insbesondere nur dann in Betracht, wenn die Anbieter eine Zusicherung für die Ergebnisse ihres Large Language Models übernehmen.

Anbieter setzen oft auch voraus, dass die Nutzer die Ausgaben fachlich beurteilen können. Bezogen auf die Anwaltschaft würde dies bedeuten, dass juristischer Rat oder Inhalt nur verwendet werden soll, wenn er von dafür qualifizierten Personen geprüft und verifiziert wurde.

Als letztes erwähnenswertes Beispiel sei die Regelung erwähnt, wonach Nutzern vorgeschrieben wird, die Ausgaben – auch in manuell veränderter Form – immer als von künstlicher Intelligenz generiert zu kennzeichnen. Auch wenn wohl davon ausgegangen werden kann, dass in den meisten Fällen eine diesbezügliche Rechteverfolgung durch die Anbieter nicht vorgenommen wird, sollte man sich auch hier immer überlegen, in welchem Kontext man den Output nutzt und an wen er sich richtet.

Die oben genannten Beispiele zeigen, wie Anbieter von Large Language Models versuchen, Verantwortung und Haftung von sich zu weisen und so ihr eigenes Risiko zu minimieren. Nicht nur aus diesem Grund ist bei der Verwendung einer Ein- oder Ausgabe immer Vorsicht geboten.

IV. Fazit

Der Einsatz von künstlicher Intelligenz bedingt auch ohne eigene gesetzliche Regelung die Beachtung verschiedener Vorschriften, sei es aus den Gesetzen oder mit der Nutzung verbundenen Vertragsbestimmungen. Es ist aber wichtig, trotz der vermeintlichen Komplexität nicht die Augen vor diesem wachsenden Markt und den Möglichkeiten zu verschliessen. Ebenso bedeutend ist es, seine Mitarbeiter und Mitarbeiterinnen – und damit sind alle gemeint, auch Nichtjuristen – im Umgang mit künstlicher

Intelligenz zu schulen. Natürlich kann man den Einsatz von künstlicher Intelligenz in der eigenen Kanzlei verbieten. Dies führt jedoch in der Regel dazu, dass manch einer die gängigen Tools ohne Schulung dennoch nutzt. Diese Konstellation führt viel eher zu einer möglichen Verletzung insbesondere des Datenschutzrechts oder des Berufsgeheimnisses. Eine bessere Strategie ist es daher, für sich und die Mitarbeiter und Mitarbeiterinnen einen praktikablen Rahmen zu schaffen, in dem künstliche Intelligenz eingesetzt werden kann.[35]

In diesem Zusammenhang kann und sollte auch eine Risikobewertung in Bezug auf alle oben beschriebenen möglichen betroffenen Rechtsbereiche vorgenommen werden, bei der überlegt wird, wie wahrscheinlich (a) Verstösse sind, (b) diese Verstösse aufgedeckt werden und wie wahrscheinlich es (c) ist, dass eine mögliche Aufdeckung tatsächlich rechtliche Konsequenzen hat.

Ein üblicher und praktikabler Mittelweg wäre, den Mitarbeitenden die Nutzung bestimmter Tools zu erlauben, mit der Auflage, dass vor der Nutzung keine Personendaten, Berufsgeheimnisse und eindeutig fremde Inhalte als Eingaben verwendet werden dürfen und dass die Ausgaben stets auf Korrektheit und mögliche Plagiate überprüft werden müssen. Für Letzteres können die oben genannten Indizien herangezogen werden, da eine vollständige immaterialgüterrechtliche Prüfung unverhältnismässig sein dürfte.

1 Für den Beitrag werden die Begriffe «Large Language Model» und «Sprachmodel» sowie auch die Abkürzung «LLM» synonym verwendet und als gleichwertig betrachtet.

2 Zwar hat die EU im EU AI Act in Art. 3 Abs. 1 mittlerweile eine Legaldefinition geschaffen. Diese ist jedoch für das schweizerische Recht nicht verbindlich und stellt lediglich den ersten Versuch einer gültigen gesetzlichen Definition von KI dar; ferner Selman/Burrichter/Hubli, Anwaltsrevue 6/7 2023, S. 289;Catherine Reiter, Künstliche Intelligenz im Verwaltungsverfahren, AJP 2022, S. 984, 985 f.

3 Es darf darauf hingewiesen werden, dass es noch andere Modelle und Bereiche der künstlichen Intelligenz gibt (je nach Auslegung des Begriffs KI) z.B. Logik, Problemlösen durch Suche, Robotik, Spam-Filter usw.

4 VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), im Folgenden EU AI Act.

5 Erwägungsgrund 1 des EU AI Act.

6 Beispielsweise das Inverkehrbringen oder Verwenden einer KI in der EU durch ein Unternehmen in einem Drittstaat.

7 Mit Beispielen zur Anwendung: Selman/Burrichter/Hubli, Anwaltsrevue 6/7 2023, S. 289ff.

8 Heinze/Wendorf, in Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, S. 328;Ehinger/Stiemerling, «Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen – Welche Strukturelemente und welche Entwicklungsphasen sind urheberrechtlich geschützt?» in CR 2018, S. 762.

9 M.w.N. Goodfellow/Bengio/Courville, Deep Learning 2016, Shalev-Shwartz/Ben-David, Understanding Machine Learning 2014.

10 D.h. mit einem «Label» versehen sind, auf dem steht, was sich in den jeweiligen Daten befindet und was somit vom Modell zu erlernen ist.

11 Für den Beitrag werden die Begriffe «Eingabe» und «Input» synonym verwendet und als gleichwertig betrachtet.

12 Stiemerling, in Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, S. 27.

13 BSK DSG-Bühlmann/Reinle, Art. 6 N. 418; anders zu betrachten ist die Frage, ob Sprachmodelle Personendaten enthalten. Dazu sagte der Hamburger Datenschutzbeauftragte Fuchs am 3. Hamburger Datenschutzforum,, dass dem nicht so sei (›https://www.datenschutz-notizen.de/3-hamburger-datenschutz forum-ein-rueckblick-0948366/#:~:text=Unter%20anderem%20wurde%20dabei%20diskutiert,Fuchs%20seine%20Interpretation%20des%20Datenschutzrechts‹.) (Stand: 2.9.2024, 20:31 CET), a.A. Rosenthal auf ›https://www.vischer.com/know-how/blog/teil-19-sprachmodelle-mit-und-ohne-personenbezogene-daten/‹ (Stand: 2.9.2024, 20:31 CET).

14 Wenn die büroeigene Hardware potenter wird und/oder die Sprachmodelle weniger Hardware-hungrig sind, kann es sein, dass sich das in (naher) Zukunft ändert.

15 BSK DSG-Bühlmann/Reinle, Art. 6 N. 418.

16 Bei ChatGPT von Open AI kann dies unter den Einstellungen bei «Datenkontrolle» – «Das Modell für alle verbessern» per Regler deaktiviert werden (Stand: 2.9.2024, 20:31 CET).

17 Rosenthal auf ›https://www.rosenthal.ch/downloads/VISCHER_ ki-tools.pdf‹ (Stand: 2.9.2024, 20:31 CET).

18 Vergleiche zur Ausdehnung des AGB-Rechts: BGE 4A_330/2021 vom 5.1.2022.

19 BSK-DSG Bühlmann/Reinle, Art. 6 N. 309.

20 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 N. 34 m.w.N.

21 Am Beispiel von DeepL erkennt man die Problematik am besten: Eine Eingabe in das Eingabefeld führt ohne weiteren Zwischenschritt direkt zur Bearbeitung der eingegebenen Daten. Das ist zu spät um die Eingabe noch von Personendaten zu bereinigen.

22 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 N.105.

23 Brunner/Henn/Kriesi, Anwaltsrecht, S. 185 ff.

24 Zwar ist gesetzlich nicht vorgeschrieben, dass alle Massnahmen implementiert werden müssen, die Autoren empfehlen jedoch aus Gründen der Rechtssicherheit, so viele wie möglich und zumutbar zu implementieren, sofern man die KI mit Mandatsdaten verwenden will. Weitere Hinweise im Umgang mit KI durch den SAV (›https://www.sav-fsa.ch/documents/672183/2025869/SAV_KI+Guidelines+2024.pdf/ee0ba86a-6a1d-dda1-c6bc-b796115e08e9?t=1721047978375‹), die sich ihrerseits an den Grundgedanken der Nutzung von Cloud-Lösungen des SAV orientiert (›https://digital.sav-fsa.ch/digitale-kanzlei-nutzung- von-clouddiensten‹) (beide Stand: 2.9.2024, 20:31 CET).

25 Diese Implementierung gilt als absolute Pflicht, vgl. auch Art. 38 SSR.

26 So z.B. Rosenthal auf ›https://www.rosenthal.ch/downloads/VISCHER_ki-tools.pdf‹ (Stand: 2.9.2024, 20:31 CET).

27 Auch als gangbar in der SAV-Wegleitung für den Umgang mit künstlicher Intelligenz erwähnt (›https://www.sav-fsa.ch/documents/672183/2025869/SAV_KI+Guidelines+2024.pdf/ee0ba86a-6a1d-dda1-c6bc-b796115e08e9?t=1721047978375‹) (Stand:

2.9.2024, 20:31 CET).

28 Für den Beitrag werden die Begriffe «Ausgabe» und «Output» synonym verwendet und als gleichwertig betrachtet.

29 Eine detaillierte Betrachtung m.w.N. bei Berger, «Künstliche Intelligenz und Immaterialgüterrecht – Eine Übersicht über die Schweizer Rechtslage», in: Jusletter IT 4.7.2024.

30 Superlativwerbung ist unter diesem Tatbestand miterfasst, BSK UWG-Schmid, Art. 3 Abs. 1 lit. e N. 30.

31 Art. 11 und 12 lit. D BGFA.

32 Vgl. ›https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/‹ (Stand: 2.9.2024, 20:31 CET).

33 BGE 130 III 168, 173/4.

34 So auch die SAV-Wegleitung für den Umgang mit künstlicher Intelligenz (›https://www.sav-fsa.ch/documents/672183/2025869/SAV_KI+Guidelines+2024.pdf/ee0ba86a-6a1d-dda1-c6bc-b796115e08e9?t=1721047978375‹) (Stand: 2.9.2024, 20:31 CET).

35 Eine Hilfestellung bietet dabei die SAV-Wegleitung für den Umgang mit künstlicher Intelligenz (›https://www.sav-fsa.ch/documents/672183/2025869/SAV_KI+Guidelines+2024.pdf/ee0ba86a-6a1d-dda1-c6bc-b796115e08e9?t=1721047978375‹) (Stand: 2.9.2024, 20:31 CET).