Die KI- Revolution – Fluch oder Segen?

Es gibt kaum noch ein Superlativ, das nicht mit Künstlicher Intelligenz (KI) oder im englischen Original Artificial Intelligence (AI), in Verbindung gebracht wird. KI wird oft als Lösung all unserer Probleme und als Motor zukünftiger Entwicklungen gesehen.

Was zeichnet aber künstliche Intelligenz aus?

Es handelt sich um ein maschinenbasiertes System, welches autonom arbeitet, sich nach der Einführung anpassen und aus Eingaben ableiten kann, wie Ergebnisse erzeugt werden können. Vereinfacht gesagt ist es die Fähigkeit, aus Erfahrungen zu lernen, um damit Anfragen zu lösen.

Insbesondere die Anpassungsfähigkeit spielt eine wesentliche Rolle und kann in unterschiedliche Ausprägungen unterteilt werden.

Die Anwendungsmöglichkeiten sind unendlich, und reichen von Chatbots, über Transkriptionen bis hin zu E-Mail Posteingangsmanager. Die Hauptanwendungsbereiche im unternehmerischen Alltag sind im Moment die Generierung von Texten, Bildern und Videos.

Was bedeutet das für uns als Individuum, Unternehmen und Gesellschaft?

Viele Menschen sind im Alltag überfordert mit digitalen Tools, die sich schnell weiterentwickeln. Unsere Einstellung zu Cyber-Security und Datenschutz ist oft nachlässig. Schutzmaßnahmen werden als bürokratischer Aufwand abgetan.

Das könnte uns deshalb Probleme bescheren, wenn wir bedenken, wie fehlerhaft und hilflos zahlreiche Anwender im Alltag mit digitalen Tools umgehen, weil sie durch die rasende technologische Entwicklung überrollt wurden.

„Datenschutz verkompliziert alles und kostet Geld", sagen viele. Cyber-Security wird vernachlässigt, weil sie „keinen Umsatz bringt" und man glaubt, „es trifft mich nicht". In diesem kurzsichtigen Umfeld wird KI als Heilsbringer angesehen, ohne die Gefahren zu verstehen. Tools wie „ChatGPT" werden unkontrolliert und gratis genutzt, von Schülern bis zu Mitarbeitern: Ob Protokolle, Übersetzungen, kreative Texte oder Vertragsentwürfe – KI wird vielfach eingesetzt. Ohne jeglichem Verständnis für Gefahrenabwehr, Schulungsbedarf und Transparenz.

Zu erwartende Probleme/Risiken?

Beispielsweise werden ungefiltert komplette Vertragstexte zur Übersetzung oder Analyse in Gratisversionen von KI-Apps eingegeben. Dadurch werden diese Texte auch für das weitere Anlernen verwendet. Bei Prompts von (anderen) Usern werden dann diese Eingaben auch genutzt und herangezogen, was zu Datenschutzbedenken führen sollte.

Ein weiteres, sehr großes Problem stellen die ungenauen Prompts dar. Als solche bezeichnet man die Eingabe, welche als Anweisung, ergänzt durch möglichst relevante und nützliche Informationen, zur KI-generierten Antwort führen soll.

Einerseits können hier ungenaue, zweideutige oder gar falsche Antworten folgen. Darüber hinaus ergibt sich hier ein neues Feld der Inumlaufbringung von Fake-News. Eine Filterung von Informationen wird dadurch immer schwieriger, wie es uns der letzte US-Präsidentenwahlkampf gezeigt hat. Die Qualität der generierten Bilder oder Videos hat ein neues Level erreicht und ist für den Durchschnittsuser nicht mehr verifizierbar. Erinnern Sie sich nur an die „Verhaftung" von Donald Trump oder Kamal Harris in diktatorischer Uniform.

Leider: Die intuitive Anwendung der KI ist bequemer als das Einrichten von Sicherheitseinstellungen oder der Erwerb eines generellen Rüstzeugs. Ergebnisorientiert werden solche „Nebensächlichkeiten" als unwichtig beiseitegeschoben.

Folgen unbedachten Handelns

Aber gerade das ist der unabdingbare Hebel. Wir dürfen nicht nur aus Angst vor möglichen Strafzahlungen

durch AI-Act oder Datenschutzgesetze Problembewusstsein entwickeln. Sondern müssen uns über die Folgen unseres unbedachten Handelns bewusstwerden.

Problemgebiete durch einen unsachgemäßen Einsatz im Zusammenhang mit Produkthaftung, Urheber- und Datenschutzrecht liegen auf der Hand.

Der richtige Umgang ist immens wichtig. Abzuklären gilt es...

Vor dem Einsatz einer entsprechenden Software müssen unbedingt einige Punkte abgeklärt werden: Wie sehen die Nutzungsbedingungen aus? Wozu gebe ich meine Zustimmung? Welche Rechte und Pflichten kommen mir zu, welche dem Softwareanbieter? Gibt es einen Haftungsausschluss des Anbieters? Erwerbe ich Exklusivrechte am Ergebnis? Etc., etc.

Aber auch die Einstellungen in den Programmen spielen eine große Rolle: Durch Anpassungen können zahlreiche Fallstricke und Stolpersteine vermieden werden. Verwende ich beispielsweise im unternehmerischen Einsatz Daten, welche personenbezogen sind oder aber nicht öffentliche, unternehmerische Daten betreffen, kann bereits ein Verstoß gegeben sein. Zusätzlich ist relevant, ob die vom User eingegebenen Daten für weiteres maschinelles Anlernen herangezogen werden (dürfen). Dies kann häufig in den Einstellungen deaktiviert werden, was aber kaum Jemand weiß oder tut. Hier zeigen sich deutlich Unterschiede zwischen Gratis- und Bezahlversionen. Bei Letzteren sind weit mehr Einstellungen möglich, die helfen, rechtliche Fallstricke zu vermeiden.

Wie RA Mag. Stephan Novotny kürzlich im einem Artikel feststellte, müssen Personen im Versicherungsvertrieb, die mit KI-Systemen arbeiten, seit Februar 2025 verpflichtend an KI-Schulungen teilnehmen.

Also sollte in Unternehmen neben der verpflichtenden Schulung, vorab der Einsatz aller KI-Anwendungen im Zusammenhang mit Datenschutz überprüft und die wesentlichen Informationen von Herstellerseite recherchiert werden.

Weiters sollte es eine interne Richtlinie geben, die die Rahmenbedingungen im Unternehmen festlegen.

Basis dafür ist die EU-KI-Verordnung, deren Zweck die Einführung und ein gleichmäßiges, hohes Schutzniveau im Zusammenhang mit künstlicher Intelligenz im Binnenmarkt ist.

Ziel ist es, sichere Produkte in Verkehr zu bringen, welche auch unter Einhaltung höchster Standards den DSGVO-konformen-Umgang mit personenbezogenen Daten gewährleisten. Es soll dadurch auch ein höheres Vertrauen der Nutzer in diese Produkte erreicht werden.

Dabei orientiert sich die Intensität der Vorgaben unter anderem an vier Risikostufen, wobei Stufe 4 (= inakzeptables Risiko) verboten ist. Dabei handelt es sich um KI-Systeme, die das menschliche Verhalten manipulieren oder Schwachstellen ausnutzen. Diese sind unter dem Begriff „Social Scoring“ bekannt, wie sie in China Verwendung finden. Das steht im krassen Widerspruch zu den Werten der EU und ist daher verboten.

Mag. Günther Zikulnig
(© Tanja Guettersberger_GT Medien und IT-Service KG)

Die anderen drei Kategorien reichen von minimalem bzw. geringem Risiko über begrenztes Risiko (Chatbots) bis hin zu einem hohen Risiko (Biometrik etc.). Im Gegenzug dazu ist das US-Regulativ viel intensiver auf die Bestärkung von Investitionen und Forschung in diesem Bereich ausgelegt und erforderlicher Regulierungsbedarf weitgehend auf Freiwilligkeit aufgebaut. Es zeigt sich ein ähnliches Bild wie im Datenschutz, bei welchem die US-Rahmenbedingungen ebenfalls nicht annähernd mit den europäischen Standards mithalten können.

Zum Abschluss darf ich einen Spruch einfügen, der meinen Wunsch für dieses Thema beinhaltet: „Ich glaube, künstliche Intelligenz wird unser Partner sein. Wenn wir sie missbrauchen, wird sie ein Risiko sein. Wenn wir sie richtig einsetzen, kann sie unser Partner sein.“ – Masayoshi Son, Japanischer Tech-Unternehmer.

PS: Glauben Sie es oder nicht: Dieser Text wurde tatsächlich ohne KI erstellt. Inzwischen fällt dies aber schon auf, da selbstverfasste Texte an Eleganz und Wortgewandtheit mit KI-unterstützten Texten kaum mehr mithalten können. •

Von Mag. Iur. Günther Zikulnig

Mag. iur. Günther Zikulnig ist Jurist und Geschäftsführer der DDSB.AT Beratung GmbH mit den Schwerpunkten Digitalisierung, Datenschutz und Compliance. Er berät einerseits Unternehmen bei strategischen Fragen bzw. schult Mitarbeiter, Vorstände und Aufsichtsräte. Auch als AFPA-Lotse für Digitalisierung gibt er sein Fachwissen in Form von Webinaren, Lotsenberichten und Fachbeiträgen weiter.