Datenschutz und KI – Wunschdenken?

Buzzwords wie ChatGPT, OpenAI, DALL-E 2 sorgten in den letzten Monaten für großes Aufsehen. Auch im Bankensektor ist Künstliche Intelligenz nicht mehr wegzudenken. Doch was ist Künstliche Intelligenz eigentlich? Und ist eine datenschutzkonforme Anwendung überhaupt möglich?

Die digitalen und physischen Bereiche der Industrie und Wirtschaft vernetzen sich immer weiter und intensiver aufgrund der rasanten Entwicklung der Technik und der unaufhaltsamen Dynamik der Digitalisierung. Dabei spielt der Einsatz der Künstlichen Intelligenz zunehmend eine signifikante Rolle in der Industrie 4.0, Wirtschaft und im Alltag eines jeden. Auch im Bankensektor hat Künstliche Intelligenz einen nicht mehr wegzudenkenden Platz eingenommen. Doch Künstliche Intelligenz ist weit vielschichtiger, als gemeinhin angenommen wird. Und – die Frage, ob eine datenschutzkonforme Anwendung möglich ist, muss differenziert beantwortet werden.

Prozesse werden immer mehr in autonome Systeme verlagert. Hierfür benötigen die Maschinen Daten und Information, auf die sie zurückgreifen können.

Gleichzeitig ist der Schutz der Daten in Deutschland und zumindest ganz Europa eine hochsensible Thematik.

Mit Hinblick auf die am 24. Mai 2016 in Kraft getretene und seit Mai 2018 wirksam anzuwendende europäische Datenschutzgrundverordnung und das neue Bundesdatenschutzgesetz stellt sich daher die Frage, inwieweit der Einsatz von Künstlicher Intelligenz rechtlich, unter Betrachtung der europäischen Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes, möglich ist.

Durch die Komplexität der Systeme wird die Einhaltung der Ziele der Datenschutzgrundverordnung (DSGVO) jedoch schwierig. Kernprobleme sind u. a. die Einhaltung der Transparenzanforderungen der europäischen Datenschutzgrundverordnung sowie die Nachvollziehbarkeit, was konkret mit den persönlichen Daten im Netz und im System dahinter passiert. Doch was ist Künstliche Intelligenz?

Eine eindeutige Definition gibt es in der Wissenschaft nicht. Grund hierfür ist, dass sich der Begriff seit der Begriffsbildung Ende der 50er Jahre als interdisziplinäre Forschungsrichtung entwickelt. Dadurch passt sich die Begriffsdeutung an die immer weiter fortschreitenden technischen Möglichkeiten an.[1]

Künstliche Intelligenz (kurz KI) lässt sich als ein Teilgebiet der Informatik beschreiben, das sich mit der Erforschung von intelligentem menschlichem Verhalten befasst[2] und versucht, dieses zu adaptieren.[3]

Die Künstliche Intelligenz ist somit die „Erforschung eines intelligenten Problemlösungsverhaltens und die Erstellung von intelligenten Computersystemen".[4]

Welche Arten von Künstlicher Intelligenz gibt es?

Grundsätzlich kann man die Künstliche Intelligenz in vier Bereiche einteilen.[5] Die Einstufung bemisst sich dabei nach der Stärke der Künstlichen Intelligenz.

1. **Rein reaktive KI (reactive machine)[6]**
   Das System erkennt seine Umwelt und reagiert entsprechend darauf. Da es keinerlei Vorstellung von seiner Umwelt und auch keine Gedächtnisfunktion hat, um auf diese Erlebnisse in seiner Handlung zurückgreifen zu können, stellt es den Basis-Typ dar. In der Regel ist diese Form der KI darauf programmiert, eine ganz bestimmte Aufgabe zu erfüllen. Somit ist sie keine selbstlernende KI.

Beispiele hierfür sind IBMs Deep Blue, Schachcomputer, der lediglich mit Hilfe von Algorithmen bestmöglichst Schach spielen kann, oder auch das digitale Brettspiel AlphaGo von Google.[7]

2. Systeme mit begrenztem Gedächtnis (limited memory)

Wie bereits die Bezeichnung beschreibt, hat diese Form der Künstlichen Intelligenz ein Gedächtnis, das jedoch begrenzt ist. Sie kann Erfahrungen der Vergangenheit in die vorprogrammierte Darstellung ihrer Umwelt integrieren und ist nicht nur auf eine Aufgabe begrenzt.

Jedoch werden trotz begrenzter Speicherkapazität große Mengen von Daten verarbeitet. Bei dieser Art wird über Machine Learning die KI mit Daten gefüttert. Über neuronale Netze und durch überwachtes Lernen kann sie dann eine große Menge an Daten und Vorgehensweisen entwickeln. Jedoch kann sie nur auf begrenzte Informationen zurückgreifen.

Beispiele hierfür sind Sprachassistenten wie Siri oder OK-Google. Diese Sprachassistenten können aufgrund eines Sprachbefehls Informationen aus dem Internet suchen, Kalender verwalten oder einfach Handlungen ausführen wie die Telefonwahl. Auch beim autonomen Fahren handelt es sich um eine KI der zweiten Art, da sie neben den Verkehrsregeln auch auf unerwartete Situationen im Straßenverkehr reagieren kann. Auch Chat-GPT gehört in diese Kategorie, da sie im Vergleich zur dritten Art keine Emotionen verstehen und verarbeiten, geschweige denn etwas fühlen kann.

3. Systeme mit eigenem Bewusstsein (theory of mind)

In dieser Kategorie handelt es sich bereits um die nächste Stufe der Künstlichen Intelligenz. Diese Form der KI kann Emotionen, Absichten und Gedanken verstehen, sich ein eigenes Bild der Umwelt machen und entsprechend interagieren.

Diese Art von KI existiert derzeit noch nicht. Jedoch wären Beispiele für diese Kategorie der KI der knuffige Roboter R2-D2 oder sein goldener Freund C-3PO aus dem Filmklassiker Star Wars.

4. Sich „ihrer selbst" bewusste Systeme (self-aware)

Diese Art der selbstbewussten KI hat ein umfassendes Verständnis von sich selbst und kann über das hinausgehen, wofür sie ursprünglich entwickelt wurde. Sie verfügt über eine Superintelligenz, Empathie und Bewusstsein. Ihr äußeres Erscheinungsbild ist vom Menschen nicht mehr zu unterscheiden. Auch diese Form der KI existiert derzeit lediglich in Science-Fiction-Filmen wie M3GAN oder Ex Machina.

Ist KI nun mit geltendem Datenschutz vereinbar?

Eine KI benötigt, um effizient eingesetzt werden zu können, Daten. Dies teilweise in nicht geringen Mengen. (Wie eine Künstliche Intelligenz im Grundsatz funktioniert, wird in einem gesonderten Artikel in einer der nächsten PoC-Ausgaben ausführlich erörtert.)

Um der Angst entgegenzuwirken, ein sogenannter gläserner Kunde zu sein und durch die vermeintliche Datensammelwut die Kontrolle über die eigenen Daten zu verlieren, bedarf es eines klaren rechtlichen Rahmens und der Transparenz gegenüber der betroffenen Person.[8]

Aufgrund des hohen Stellenwerts der DSGVO und der steigenden Relevanz von Künstlicher Intelligenz, insbesondere für Wirtschaftsunternehmen, ist deren Zusammenspiel und die gesetzeskonforme Begutachtung der überschneidenden Themenbereiche von signifikanter Bedeutung.

Dabei ist zwischen zwei Phasen der datenschutzrechtlichen Begutachtung der Künstlichen Intelligenz zu unterscheiden. In der ersten Phase geht es um die Generierung von Künstlicher Intelligenz auf Grundlage von automatisierten Big-Data-Analysen (Analysen von großen Datamengen). Die zweite Phase beinhaltet die tatsächliche Implementierung von Künstlicher Intelligenz im Alltag, wie beispielsweise durch digitale Assistenten und automatisierte Entscheidungssysteme (vgl. Abb. 1[9]).

Beim Einsatz von KI, bei der personenbezogene Daten verarbeitet werden, handelt es sich um den Einsatz einer neuen Technologien. Daher bestehen kaum gerichtliche Entscheidungen oder Leitlinien. Es ist daher auch zu beachten, dass der Einsatz solcher Systeme stets mit einem Risiko verbunden ist.

Beispielsweise stellt sich die Frage, wer als Verantwortlicher eines eingesetzten KI-Systems gilt. Dies ist in der Regel derjenige, der das System in die unternehmensinternen Prozesse integriert und daher über den Zweck und die Mittel der Datenverarbeitung gem. Art. 4 Nr. 7 DSGVO entscheidet. Doch was ist mit dem Anbieter des KI-Systems? In den meisten Fällen erfolgt die Datenverarbeitung auf den Servern des Anbieters. Daher liegt es nahe, dass es

Abb. 1. **Zwei Phasen der KI bzw. automatisierten Entscheidung im Einzelfall**

Quelle: eigene Darstellung

sich hierbei um eine Auftragsdatenverarbeitung gem. Art. 28 DSGVO handelt. Dabei sollte durch den Verantwortlichen vor Abschluss geprüft werden, ob der Auftragsdatenverarbeiter die zugesicherten technisch-organisatorischen Maßnahmen auch tatsächlich einhalten kann. Das ist wichtig, da auch die Anbieter einen bestimmten Teil des KI-Sytems nicht selbst beherrschen können – Stichwort Blackbox.

Werden jedoch die durch die KI-Systeme erhobenen Daten für die Weiterentwicklung des Systems genutzt, könnte dies die Grenzen der Auftragsdatenverarbeitung verlassen und der Anbieter selbst, je nach Fallkonstellation, als Verantwortlicher oder aber auch als gemeinsam mit dem Anwender Verantwortlicher einzuordnen sein. Hieran sind weitere rechtliche Probleme gekoppelt, weshalb bei einer Vertragsanbahnung die datenschutzrechtliche Fachexpertise des Datenschutzbeauftragten unentbehrlich ist.

Für eine datenschutzkonforme Verarbeitung von personenbezogenen Daten durch KI-Systeme kommt in der Regel die Rechtsgrundlage der Einwilligung gem. Art 6 Abs. 1 lit. a DSGVO in Betracht.

Eine Begründung der Verarbeitung auf der Rechtsgrundlage des berechtigten Interesses gem. Art 6 Abs. 1 lit. f DSGVO ist aufgrund des sehr hohen Risikos der Verarbeitung durch KI-Systeme und der überwiegenden Interessen der Betroffenen häufig nicht gegeben.

Ein weiterer Punkt ist die Informationspflicht gem. Art. 13 DSGVO. Hierbei ist neben den bekannten Informationspflichten aber auch die Informationen über automatisierte Entscheidungsfindung gem. Art 22 DSGVO einzuhalten.

Gleichzeitig besteht die Pflicht, geeignete Prozesse zu haben, um als Betroffener die Ansprüche gem. der DSGVO auch ausführen zu können. In Anbetracht der Komplexität der KI wird es beispielsweise schwer sein, eine vollständige Löschung der Daten durchsetzen zu können, ohne dabei das Modell zu beeinträchtigen: Die Daten sind direkt in das KI-Modell eingeflossen und haben dieses verändert.[10]

Fraglich ist auch, inwieweit der Grundsatz des Transparenzgebotes gem. Art 5 DSGVO eingehalten und gelebt werden kann.

Transparenz i.S.v. Art. 5 DSGVO setzt nach dem Erwägungsgrund 58 der DSGVO grundsätzlich voraus, dass eine Information präzise, leicht zugänglich und verständlich ist und ggf. zusätzliche und verständliche visuelle Elemente eingesetzt werden.[11]

Der Grundsatz der Transparenz wird hinsichtlich der Gestaltung und des Verfahrens der Informationspflicht durch Art. 12 Abs. 1 DSGVO konkretisiert.[12] Damit werden durch Art. 12 DSGVO formale Anforderungen an die Informationspflichten aus Art. 13 ff. DSGVO normativ festgelegt.

Dies bedeutet für die Anwendung von KI-Systemen, dass nicht nur die Datenverarbeitungsprozesse und die Logik der datenbasierten Entscheidungen für die betroffene Person nachvollziehbar[13], sondern auch die Trainingsdaten leicht zugänglich und stringent im Sinne des Art. 12 Abs. 1 Satz 1 DSGVO sein müssen.[14] Somit muss der Betroffene beim Einsatz von personenbezogenen Daten für KI-Systeme auch darüber informiert werden: Erst durch diese Mitteilung kann der Betroffene selbst entscheiden, ob er einen solchen Dienst nutzen möchte oder nicht.

Dabei gilt für die Beschreibung der Verarbeitung nicht, dass tiefgreifende und ausführliche Informationen über den Verarbeitungsprozess erfolgen müssen.[15] Es sind viel-

mehr wesentliche, prägnante und beschränkte Erläuterungen gefordert, ohne den objektiven Empfänger zu überfordern.[16]

Hinsichtlich der auf Künstlicher Intelligenz basierenden Entscheidungen wird eine Datenschutzfolgeabschätzung jedoch nicht unproblematisch sein, da insbesondere bei selbstlernenden Prozessen die Risikoreichweite kaum bis überhaupt nicht abschätzbar ist.[17] Es wird jedoch grundsätzlich immer eine Datenschutzfolgeabschätzung erfolgen müssen.

Fazit

Zusammenfassend ist festzuhalten, dass eine datenschutzrechtskonforme Anwendung von sogenannten „schwachen" KI-Systemen (siehe oben „reactive machine" und „limited memory") nicht ausgeschlossen ist. Jedoch stellt sie Unternehmen gleichzeitig vor große Herausforderungen, die durch die DSGVO derzeit nicht völlig gelöst sind. Es bleibt daher offen, inwiefern eine KI-Verordnung dem Einsatz von KI-Systemen eine rechtliche Sicherheit geben kann.

Auch angesichts der wirtschaftlichen und gesellschaftlichen Bedeutung von algorithmenbasierten Entscheidungen und der rasanten Entwicklung der technischen Möglichkeiten, wird die Bedeutung von automatisierten Entscheidungen auch in Zukunft immer stärker zunehmen. So wird auch die DSGVO, in Anbetracht der fortschreitenden Technik, sich weiterentwickeln und weiter auslegen lassen müssen.

Dies ist ein Zeichen dafür, dass mit Blick in die Zukunft und angesichts der Entwicklungsprognose der Technik der Künstlichen Intelligenz mehr Raum eingeräumt werden muss. ▬

Derya Isikli
Beauftragte Informationssicherheit & Datenschutz,
E-Mail: derya.isikli@dz-cp.de

[1] Bitkom, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderung, menschliche Verantwortung, 2017, S. 28 ff.

[2] Gruhn, Volker, Künstliche Intelligenz verleiht Cyber Physical Systems Flügel, in: Industrie 4.0 Management 34, Jg. 2018, S. 45-48 (45)

[3] Söbbing, Thomas, Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law), Frankfurt am Main, dfv Mediengruppe 2019, S. 3

[4] Andresen, Maja (21. Oktober 2019), Wie funktioniert Künstliche Intelligenz, abgerufen am 25.08.2023 von https://www.zeitakademie.de/elearning/wie-funktioniert-kuenstliche-intelligenz/

[5] Möhring, Cornelia, Diese vier Arten von KI gibt es, auf Heise.de, abgerufen am 25.08.2023 von https://www.heise.de/tipps-tricks/Diese-vier-Arten-von-KI-gibt-es-9076579.html

[6] Dusold, Julia (10. Dezember 2019), Künstliche Intelligenz verständlich erklärt, abgerufen am 25.08.2023 von https://www.produktion.de/technik/kuenstliche-intelligenz-verstaendlich-erklaert-243.html#wiefunktioniert-kuenstliche-intelligenz

[7] Leichsenring, Dr. Hansjörg, Vier unterschiedliche Arten Künstlicher Intelligenz – Infografik, auf Der Bank Blog, abgerufen am 25.08.2023 auf https://www.der-bank-blog.de/typologie-kuenstliche-intelligenz/technologie/29269/

[8] Bitkom, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderung, menschliche Verantwortung, 2017, S. 35.

[9] Gausling, Tina, Künstliche Intelligenz und DSGVO, in: DSRITB 2018, S. 519-545 (526)

[10] Globocnik in: ActiveMind.AG: Künstliche Intelligenz (KI) und Datenschutz, abgerufen am 21.08.2023 von https://www.activemind.de/magazin/kuenstliche-intelligenz/

[11] BeckOK DatenschutzR/ Spoerr, 32. Ed. 01.05.2020, DS-GVO Art. 26, RN 28,29

[12] Strassemeyer, Laurenz, Datenschutzrechtliche Transparenz von Algorithmischen Entscheidungen und Verarbeitungen mittels Gamification, Ablaufdiagramme und Piktogramme, in: Taeger, Jürgen (Hrsg.), Die Macht der Daten und Algorithmen – Regulierung von IT, IoT und KI, DSRI, Deutsche Stiftung für Recht und Informatik, München, Oldenbourg Verlag, 2019, S. 34

[13] DSGVO Fluch oder Segen für Europas Wettrennen um Künstliche Intelligenz? Erschienen Algorithmenethik 18.Oktober 2019 / Pierre Adrien Hanania, Dr. Nikolai Horn, Dr. Tobias Knobloch, abgerufen am 25.08.2023 von https://algorithmenethik.de/2019/10/18/datenschutzgrundverordnung-fluch-oder-segen-fuereuropas-wettrennen-um-kuenstliche-intelligenz/

[14] Hambacher Erklärung zur Künstlichen Intelligenz, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörde des Bundes und der Länder, Hambacher Schloss 3. April 2019// So auch Erwägungsgrund 39 zur DSGVO

[15] Eßer in: Eßer/ Kramer/ von Lewinski, DSGVO/ BDSG, Köln, Carl Heymann Verlag, 6. Auflage, 2018, Art. 12 Rn. 6

[16] Strassemeyer, Laurenz, Datenschutzrechtliche Transparenz von Algorithmischen Entscheidungen und Verarbeitungen mittels Gamification, Ablaufdiagramme und Piktogramme, in: Taeger, Jürgen (Hrsg.), Die Macht der Daten und Algorithmen – Regulierung von IT, IoT und KI, DSRI, Deutsche Stiftung für Recht und Informatik, München, Oldenbourg Verlag, 2019, S. 36

[17] Conrad, C.S., Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017, S. 744