

Ausgewählte Rechtsprobleme beim Einsatz von KI

RA Prof. Andreas Göbel
Fachanwalt für IT- Recht

GESCHÄFTSLEITERHAFTUNG FÜR IT-SICHERHEIT und AUSGEWÄHLTE RECHTSFRAGEN DER KÜNSTLICHEN INTELLIGENZ

ITQ

Future Solutions Day 04.09.2025

Prof. Andreas Göbel
Rechtsanwalt
Fachanwalt für Informationstechnologierecht

Begriff der IT- Sicherheit

§ 2 Abs. 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnologie (BSIG):

„Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen wie informationstechnischen Systemen, Komponenten oder Prozessen oder bei deren Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen“.

Cyberangriffe sind

„gezielte Maßnahmen gegen Infrastrukturen der Informationstechnologie, die entweder der Informationsbeschaffung-insbesondere von Kundendaten oder Geschäftsgeheimnissen- oder der Schädigung bzw. Sabotage des angegriffenen IT-Systems dienen“ (Definition des Bundesamtes für Verfassungsschutz, Stand Februar 2019).

Gefahren und Risiken

Man schätzt die Schäden durch Cyberangriffe mehr als 200 Milliarden EURO..

Keine vollständige Möglichkeit der Versicherung

Warren Buffett glaubt nicht, dass man das Risiko wirklich finanziell kalkulieren könne. Jedes Jahr bestehe ein zweiprozentiges Risiko einer Superkatastrophe mit einem Schaden von 400 Milliarden \$ oder mehr.

Die Frage ist nicht, ob, sondern wann man angegriffen wird.

In den nächsten Jahren wird jedes Unternehmen mindestens einmal erfolgreich angegriffen worden sein.

Schäden des Unternehmens

- Umsatzeinbußen
- Kosten Wiederherstellung der Betriebssysteme
- Ursachenfeststellung
- juristische und forensische Berater
- Reputationsschäden
- Beeinträchtigung des Unternehmenswerts (Kaufpreis Yahoo! In 2016 wegen Verlust von Millionen von Nutzerdaten um 350 Millionen \$ reduziert bei Kauf durch Verizon (FAZ 04.10.2017).
- Schadensersatzansprüche von Kunden gemäß § 280 BGB wegen Verzug von Leistungen und Datenverlust
- Problem § 280 Abs. 1 Satz 2 BGB: Beweislastumkehr: Unternehmen muss beweisen, die IT-Sicherheitspflichten erfüllt zu haben.
- Haftungsbeschränkungen in AGB nur in engen Grenzen möglich.

Risiko Datenschutz

Haftung des Unternehmens gegenüber Aufsichtsbehörden nach Art. 82 DSGVO mit den bekannten Bußgeldern bis zu 10 bzw. 20 Millionen, bzw. 2 % bzw. 4 % des Jahresumsatzes.

Die soll „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein.

Daneben: Immaterieller Schaden für die Betroffenen, deren Daten veröffentlicht wurden, Art. 82 DSGVO.

Haftung nur ausgeschlossen bei Nachweis, dass der Verantwortliche „in keinerlei Hinsicht“ verantwortlich ist.

Gesetzliche Vorgaben zur IT- Sicherheit

Was muss bei IT- Sicherheit beachtet werden?

Daten gelten nach dem IT- Sicherheitsgesetz und BSI-G als sicher, wenn Folgendes gewährleistet ist:

Verfügbarkeit – Schutz vor Verlust

Integrität – Schutz vor Veränderung

Authentizität – Nachweis der Herkunft/Urheberschaft und

Vertraulichkeit der Systeme – Schutz vor Kenntnisnahme durch Unbefugte.

- Verfügbarkeit
- ist der Schutz vor Informationsverlust, Informationsentzug, Informationsblockade und Informationszerstörung, Verfügbarkeit von Systemen, z.B. Wasserversorgung

Zum Beispiel : Produktionsstillstand

Verlust von Unterlagen (Angebote, Verträge, ...)

- Integrität

Ist der Schutz vor ungewollter Veränderung von Informationen

auch eine Pflicht nach den GOBD, § 147 Abgabenordnung

Mittel: Verschlüsselung und Einsatz elektronischer Signatur

Vertraulichkeit

Ist Schutz der Unternehmensinformationen gegen das Ausspähen durch Dritte

- Personenbezogene Daten
- Inhalt der Telekommunikation (Fernmeldegeheimnis)
- Geschäftsgeheimnisse

Mittel: Zugangsbeschränkungen, technische Schutzvorrichtungen, Rollenkonzepte

Schutz auch vor Datenmissbrauch eigener Mitarbeiter bedenken

Authentizität

Feststellbarkeit der handelnden Personen

Gefahr: Vertragspartner bestreitet, dass die E-Mail/Unterschrift von ihm ist.

Mittel: Verschlüsselung, elektronische Signatur

Zu berücksichtigen

- Europäische Vorgaben
- Datenschutz
- Deliktsrecht (§ 823 BGB, Produkthaftungsgesetz, Produktsicherheitsgesetze)
- Wettbewerbsrecht
- Vertragsrecht
- Bundes-IT-Sicherheitsgesetze: KRITIS, NIS-2, CRA, DORA, TDDDDG (Telekommunikations- und Digitale Dienste Datenschutzgesetz)

Jede dieser Vorschriften hat eigene Anwendungsbereiche, Adressaten, Voraussetzungen und Pflichten.

- Das sind also viele unterschiedliche Rechtsquellen, die teilweise auch noch sich teilweise auch noch stark unterscheiden. Stichwortartig seien hier Maßnahmen zur Cybersicherheit beispielhaft aufgeführt. Welche dieser Maßnahmen ergriffen werden muss ist individuell für das einzelne Unternehmen zu bestimmen (Risikomanagement).
- Schutz vor Hackern, Viren, Trojanern, Spyware, Botnets
- Schutz gegen Datenlecks
- Abwehr von Spionage (Geschäftsgeheimnisschutz)
- Datensicherung
- Investitionsschutz bei Programmen (lange Wartungsverträge)
- Hinterlegung eines Quellcodes
- Handlungsanweisungen im Unternehmen (Policies)
- Beachtung von Normen (ISO 27001, GOBD) und Prüfungsstandards (Wirtschaftsprüfer-Testat)

- Bei Verletzung von IT-Sicherheitspflichten kommen folgende Personen als Haftende in Betracht:

- Angreifer
- Unternehmen
- Dienstleister
- Geschäftsführer
- Aufsichtsrat
- Arbeitnehmer

Unternehmenshaftung aus Vertrag

- Kauf (§ 433), Werkvertrag (§ 633) und Miete (§ 535 BGB) verlangen Gebrauchstauglichkeit.
- Gebrauchstauglichkeit stets gegeben. IT-Sicherheit führt nur zum späteren Wegfall der
- Gebrauchstauglichkeit. Daher wohl keine IT Sicherheit als Hauptleistungspflicht. Und nur dann Rücktritt bzw. Kündigung.
- Anders bei Auftragsdatenverarbeitung, Art. 28 Absatz 3 lit. c DSGVO
- Beispiel: Cloud, Services, Outsourcing. Da ist IT- Sicherheit Hauptpflicht.
- Streitig für IT- Wartung und /-Pflege.
- Ansonsten vertraglich vereinbaren.
- Empfohlen: Individuelle Festlegung der Maßnahmen, sofern dies dem Kunden möglich.
- Rechtsfolge: Kündigung bzw. Rücktritt, Minderung, Schadensersatz

HAFTUNG VON UNTERNEHMENSORGANEN -GESCHÄFTSFÜHRER

Überblick:

§ 91 Abs. 2 AktG:

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“.

Hat auch „ Ausstrahlungswirkung „auf GmbH-Geschäftsführer, § 43 GmbH-Gesetz.

.Bei Delegation sorgfältige Auswahl, Überwachung, Ausrüstung, Unterstützung.

Bei Duldung und nicht Verfolgung von IT-Sicherheitsverstößen Risiko einer betrieblichen Übung (OLG Celle GWR 2011,433).

Haftung von Unternehmensorganen gegenüber Gesellschaft (+)

gegenüber Dritten (Außenhaftung) eher (-) Ausnahme: bei Complianceverstößen

(BGH NJW 2012,3439, 3442)

Pflichten der Geschäftsleitung bezüglich IT-Sicherheit

- § 93 Abs. 1 Satz 1 AG, § 43 Abs. 1 GmbH-Gesetz:
- „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt
- eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden“.
- Folgerungen:
 - - Risikoanalyse (Bewertung und Maßnahmen – auch Risiko akzeptieren möglich!)
 - Überwachungsmaßnahmen festlegen und
 - organisieren.

Landgericht München I (Siemens/Neubürger, 10.12.2013 Neue Zeitschrift für Gesellschaftsrecht 2014,345):

„Einer derartigen Organisationspflicht genügt der Vorstand bei entsprechender Gefährdungslage nur dann, wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet“.

Das gilt auch für die IT-Sicherheit.

Dabei Beweislastumkehr: Unternehmen muss beweisen:

Pflichtverletzung

Schaden

Geschäftsführer muss beweisen:

Mangelndes Verschulden.

Kollektive Haftung der Geschäftsleitung

Aufgaben:

Gemeinsame Einschätzung und Entscheidung, ob Gefährdungslage vorliegt und welche Maßnahmen notwendig.

Entscheidung über die notwendige Organisation zur Abwehr:

- unmissverständliche Zuständigkeiten

- engmaschiges Berichtswesen

- genaue Dokumentation

Übertragung auf ein Mitglied der Geschäftsleitung zulässig.

Dann bleibt Überwachungspflicht für die anderen Organmitglieder.

Bundesgerichtshof 06.01.2018

Auch eine für sich genommen zulässige Verteilung der Geschäftsführungsaufgaben entbindet denjenigen, dem hiernach nur bestimmte Aufgaben zu Erledigung zugewiesen sind, allerdings nicht von seiner eigenen Verantwortung für die ordnungsgemäße Führung der Geschäfte der Gesellschaft. „(BGH NJW 2019, 1067)

Der hier Verurteilte war nach Geschäftsverteilung nur für die künstlerischen Fragen zuständig ...

Vorgehen der Geschäftsleitung

Landgericht München I (Neue Zeitschrift für Gesellschaftsrecht 2008, 319):

Die Einrichtung eines solchen Systems fordert eine Organisation, die

- unmissverständliche Zuständigkeiten begründet,
- ein engmaschiges Berichtswesen aufbaut, das
- entsprechend dokumentiert ist.

Es ist sicherzustellen,

- dass vom verantwortlichen Sachbearbeiter über die jeweiligen Hierarchieebenen
bis hin zur Unternehmensleitung sämtliche relevanten Stellen von vorhandenen
Risiken Kenntnis erlangen, um die entsprechenden Maßnahmen zur

Beherrschung dieser Risiken einleiten zu können.

Daneben ist zu empfehlen, eine Dokumentation zu schreiben.

Sie hilft dem Organmitglied, seine ihm obliegende Beweislast für mangelndes Verschulden zu erfüllen.

Organisationspflichten

- GL kann nicht alles allein machen. Er kann und muss delegieren.
- Richtige Person auswählen
- Zeit, Material, Personal ausreichend zur Verfügung stellen
- Person schulen
- Aufgaben lückenlos zuordnen (sonst niemand verantwortlich)
- Überwachen:
 - Stichproben, ggf. durch externe Spezialisten
 - auch Geschäftsleiter untereinander, zumindest bei gegebenem Anlass (Grund zum Verdacht eines Pflichtverstoßes)
- -Verstöße sanktionieren: Ermahnung, Abmahnung, Kündigung, Schadensersatz

Versicherung

- Möglichkeiten des Versicherungsschutzes
- Einerseits eine Versicherung des Unternehmens gegen Cyber-Schäden
- andererseits D & O-Versicherung für den Geschäftsleiter
- (im Interesse des Unternehmens, denn der GL wird im Zweifel den Cyberschaden nicht bezahlen können)

Fazit

- Die Angriffe werden immer intelligenter und häufiger
- es drohen riesige Schäden
- nichts tun ist keine Alternative
- notwendige Maßnahmen ergreifen entspr. Risikoanalyse
- Belegschaft sensibilisieren
- Unternehmen versichern
- Geschäftsleiter versichern

- Definition in Art. 3 Nr. 1 KI- VO- EU:
- „System der künstlichen Intelligenz“ (KI-System) eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren;

- Schwache KI:
 - lernt (Deep Learning, Big Data) und kommt zu besseren, aber planmäßig gesuchten Ergebnissen
- Starke KI:
 - Verselbständigt sich, entscheidet selbst, entwickelt sich auch in nicht vorhersehbare Richtungen

Vertragsrecht

- Fall:
- Sven hat sich Paul, einen intelligenten Kühlschrank, gekauft. Paul soll Joghurt bestellen, wenn weniger als 2 Becher im Kühlschrank. Dabei soll er den besten Preis ermitteln. Durch Recherche im Internet ermittelt Paul einen sehr günstigen Preis eines Anbieters aus China und bestellt dort.
- Der Joghurt ist bei der Ankunft verdorben.
- Der Anbieter berechnet Fracht von 20.-€/Becher (stand im Kleingedruckten. Paul versteht kein Mandarin.)
- Muss Sven bezahlen?

- Sven hat nicht gehandelt.
- Zurechnung des autonomen Handelns von Paul zu Sven?
- Autonom bedeutet, dass die Entscheidungen des Systems nicht in jeder Hinsicht durch die Programmierung vorgegeben und daher nicht (vollständig) prognostizierbar sind. Das bedeutet eine echte Delegation der Entscheidung an das System entsprechend einer Stellvertretung, nicht nur Bote.
- Der Bote übermittelt lediglich die Erklärung eines Anderen. Der Stellvertreter gibt die Erklärung aufgrund eigener Entscheidung selbst – mit Wirkung für den Vertretenen - ab, wozu er von der vertretenen Person bevollmächtigt ist.
- Die Abgrenzung zwischen automatisierten Angeboten und autonomen Entscheidungen ist schwierig und ungeklärt. Denn auch die autonome Entscheidung ist herbeigeführt durch Voreinstellungen, wenn auch mit Spielraum. Und umgekehrt: Auch jedes automatische Angebot arbeitet teilweise autonom, weil es erst auf eingehende Anfragen reagiert.

- Entscheidend ist also der Grad der Selbstständigkeit. Wo da die Grenze liegt, ist zurzeit weder technisch noch rechtlich geklärt.
- Problem:
- KI handelt nur im Rahmen seiner Vorgaben. Sind die zu eng oder zu weit, kommt es zu Fehlern. Daher hohe Anforderungen an Testdaten und – verfahren.
- Ergebnis: Sven hat einen wirksamen Vertrag geschlossen, weil er die Voreinstellung zu verantworten hat.

- Anfechtung?
- Sven wollte den Vertrag nicht.
- Irrtum?
- Wer hat geirrt?
- Sven nicht. Keine Vorstellung...
- Paul auch nicht. Der hat keine Vorstellung.
- Können Kühlschränke irren?
- Übermittlungsfehler? Nein.

- Haftung des Arbeitgebers für das Handeln des Roboters
 - Zurechnung des Handelns des Roboters zum Arbeitgeber?
 - Parallele zum Arbeitnehmer?
- § 278 BGB Verantwortlichkeit des Schuldners für Dritte
- Der Schuldner hat ein Verschulden seines gesetzlichen Vertreters und der Personen, deren er sich zur Erfüllung seiner Verbindlichkeit bedient, in gleichem Umfang zu vertreten wie eigenes Verschulden.
- (-) es fehlt Schuldfähigkeit von R.; zugerechnet wird nicht nur das Handeln, sondern das Verschulden des R. (h.M.)
- Haftung des Arbeitgebers wegen eigenen Verschuldens
- Verletzung der Montage- oder Betriebsanleitung, Beobachtungspflicht, falsche Auswahl?
- Wenn nicht, keine Haftung des Arbeitgebers!!
- Deshalb wieder Diskussion : Roboterversicherung

Haftung des Herstellers/Programmierers

Produzentenhaftung:

Anknüpfungspunkte einer Haftung heute:

- Konstruktions- ,
- Fabrikations- ,
- Instruktionsfehler oder
- Produktbeobachtungsversäumnis.

Im Einzelfall prüfen.

Neue EU- Produkthaftungsrichtlinie für KI in der Bearbeitung

Urheberrecht



Haftung für KI

- Haftung für Schäden durch KI 1
- Fall:
- Roboter R arbeitet völlig normal in der Klinik Kund verteilt Tabletten. Eines Tages verwechselt er die Patienten. Der 25- jährige Fussballnationalspieler F stirbt. Seine Erben verlangen mehrere Millionen Schadensersatz.
- Haftung des Roboters?
- E- Person (-), die hat kein Geld.
- Versicherungslösung: verleitet zur Nachlässigkeit bei Herstellung und Betrieb

- Haftung des Arbeitgebers für das Handeln des Roboters
 - Zurechnung des Handelns des Roboters zum Arbeitgeber?
 - Parallele zum Arbeitnehmer?
- § 278 BGB Verantwortlichkeit des Schuldners für Dritte
- Der Schuldner hat ein Verschulden seines gesetzlichen Vertreters und der Personen, deren er sich zur Erfüllung seiner Verbindlichkeit bedient, in gleichem Umfang zu vertreten wie eigenes Verschulden.
- (-) es fehlt Schuldfähigkeit von R.; zugerechnet wird nicht nur das Handeln, sondern das Verschulden des R. (h.M.)
- Haftung des Arbeitgebers wegen eigenen Verschuldens
- Verletzung der Montage- oder Betriebsanleitung, Beobachtungspflicht, falsche Auswahl?
- Wenn nicht, keine Haftung des Arbeitgebers!!
- Deshalb wieder Diskussion : Roboterversicherung

- Kann KI Urheberrechte (selbst) haben?
- Für Naruto verneint
- Auch KI kein Urheber
- Urheber- wenn überhaupt – immer ein Mensch
- Programmierer oder Nutzer?
- Wenn KI auf Schaffung von Werken ausgerichtet, -> Programmierer
- Wenn konkreter Einsatz erst das Werk möglich macht, der Nutzer.

- Aber kann durch KI überhaupt ein urheberrechtlich relevantes Werk entstehen?



- „Portrait of Edmond de Belamy“.
- Das Gemälde wurde erstmals am 25. Oktober 2018 im Rahmen der Auktion Prints & Multiples vom Auktionshaus Christie's für 432.500 US-Dollar versteigert. Der geschätzte Wert wurde damit fast um das 45-fache übertroffen.

- § 1 Urheberrechtsgesetz:
- Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes.
- „ 2 Urheberrechtsgesetz
- (1) ...
- (2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen.
- Daher Voraussetzung menschliches Handeln.

- Ist es noch ein persönlicher schöpferischer Akt, 100 Bilder von Rembrandt einzugeben und dann die KI machen zu lassen?
- Kontra: keinerlei weitere Handlung eines Menschen.
- nur Rahmen vorgegeben (Daten)
- Pro: auch Mensch schöpft aus begrenzten Mitteln (Daten in seinem Kopf). Dann KI mehr Daten also sogar noch mehr schöpferisch?

- Jackson Pollock: Spannt Seil quer durch Raum, hängt Farbeimer dran und setzt das Seil in Bewegung. Urheberrecht an dem auf dem Boden (Leinwand) entstehenden Bild? Er gibt auch nur Rahmen (Seil, Eimer, Schwingung -> zufällig) vor (wie Daten bei KI). UrhR bejaht.
- Rehberger: Ausgestellt Hundehütte aus Pappe. Den Satz Pappe soll man an der Kasse kaufen und selbst beliebig zusammenfügen und ein Bild davon an Rehberger senden. Der nimmt das in sein Werkverzeichnis auf und macht es zu einem „echten Rehberger“. UrhR nach h.M. verneint.
- Ergebnis offen. M.E. Vom Einzelfall abhängig: wie stark ist die Gestaltungsleistung des Menschen – Ggf. durch Voreinstellung

- Urheberrechtsverletzungen durch KI – Training
- FAZ 11.11.2023, Seite 29:
- In einem Urheberrechtsverfahren von US-Autoren Gegen Metas Künstliche Intelligenz (KI) Llama hat der Facebook-Mutterkonzern zunächst einen Teilerfolg erzielt. Bundes Bezirksrichter Vince Chabria mit Sitz in San Francisco gab am Donnerstag einem Antrag von Meta statt, zahlreiche Klagepunkte der Komikerin Sarah Silverman und anderer Autoren abzuweisen. Er machte jedoch klar, dass er die meisten davon in einer überarbeiteten Form neu prüfen würde. „Ich verstehe den Kern ihrer Theorie“, sagte Chabria den Anwälten der Autoren. „Ihre übrigen Haftungstheorien verstehe ich nicht einmal ansatzweise.“
- Die im Juli gegen Meta und den ChatGPT-Betreiber OpenAI eingereichte Klage setzt sich aus zwei Teilen zusammen. Die Autoren argumentieren einmal, dass die Technik-Konzerne ihre Rechte verletzt hätten, als sie mithilfe der Bücher ihre KI-Modelle trainierten. Getrennt davon machen sie geltend, dass die Antworten dieser Systeme auf Anfragen der Nutzer ebenfalls gegen das Urheberrecht verstoßen würden. Meta hat das Gericht bislang nur gebeten, den zweiten Teil abzuweisen. Der Microsoft-Partner OpenAI hat das Gericht ebenfalls aufgefordert, die Klage einzuschränken. Dieser Antrag soll im kommenden Monat verhandelt werden.

- • Chabria zeigte sich am Donnerstag von dem zweiten Teil der Autoren-Klage ebenfalls wenig überzeugt. „Wenn ich eine Anfrage an Llama stelle, ist das keine Bitte um eine Kopie von Sarah Silvermans Buch“, sagte er. „Ich bitte nicht einmal um einen Auszug daraus.“ Auch das Argument der Autoren, Llama selbst würde schon das Urheberrecht verletzen, ließ er so nicht gelten. Aus der Argumentation würde folgen müssen, „dass sie das Lama-Sprachmodell und Sarah Silvermans Buch als ähnlich bezeichnen würden, wenn man sie nebeneinander hinstellen würde.“, sagte er. „Mein Kopf explodiert, wenn ich versuche, das zu verstehen.“
- • Die neuen KI Systeme werden als „generativ“ bezeichnet aufgrund ihrer Fähigkeit, auf der Grundlage von vergleichsweise einfachen Aufträgen- „Prompt“ – neue Inhalte zu erstellen. Gegen die Erschaffer und Betreiber derartiger Modelle laufen mehrere Klagen. So wurde im Juli der Alphabet-Tochtergesellschaft Google vorgeworfen, unerlaubt Daten aus dem Internet für die für ihr KI-Training verwendet zu haben. Im vergangenen Monat wies ein anderer Bundesrichter Ansprüche von bildenden Künstlern gegen StabilityAI, Midjourney und die Deviant Art ab. Demnach weisen die von ihren Systemen generierten Bilder vermutlich keine ausreichend große Ähnlichkeit zu den Werken der Künstler auf, um eine Verletzung von deren Rechten darzustellen.
- • Lösungsvorschlag Deutschland: § 44 b UrhG: maschinenlesbare Ablehnung

- Nach mehr als anderthalb Jahren hat der Richter nunmehr sein Urteil gesprochen. Er wies die Klage gegen Meta ab. Allerdings nicht, weil Meta grundsätzlich berechtigt sei, die Werke anderer zu verwenden. Es handele sich vielmehr um einen Einzelfall. Wörtlich schrieb er: „Dieses Urteil steht nicht für die Behauptung, dass die Verwendung urheberrechtlich geschützten Materials durch Meta zum Training seiner Sprachmodelle rechtmäßig ist.“ (Aktenzeichen 3:23-CEV-03417).
- Ein anderes US Gericht hat aber in einem Prozess gegen ANTHROPIC entschieden, dass das KI-Datentraining mit urheberrechtlich geschützten Büchern jedenfalls dann möglich sein soll, wenn die Werke selbst vorher legal erworben worden sind (Aktenzeichen C 24-05417WHA).

- Urheberrechte an Input ? Möglich
 - Urheberrechte an Input ? Möglich
 - Urheberrechte an Prompts ? denkbar
-
- In Vertrag regeln

- EU- VO KI
- VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISierter VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION.
- Inkrafttreten 9.12. 2024
- Übergangszeit zwei Jahre nach Veröffentlichung bis 9.12.2026.
- Zur Überbrückung: KI-Pakt auf freiwilliger Basis, die wichtigsten Verpflichtungen des Gesetzes bereits vor Ablauf der gesetzlichen Fristen umzusetzen.

- In dieser Verordnung wird Folgendes festgelegt:
- a) harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der künstlichen Intelligenz (im Folgenden „KI-Systeme“) in der Union;
- b) Verbote bestimmter Praktiken im Bereich der künstlichen Intelligenz;
- c) besondere Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für Betreiber solcher Systeme;
- d) harmonisierte Transparenzvorschriften für KI-Systeme, die mit natürlichen Personen interagieren sollen, für KI-Systeme zur Emotionserkennung und zur biometrischen Kategorisierung sowie für KI-Systeme, die zum Erzeugen oder Manipulieren von Bild-, Ton- oder Videoinhalten verwendet werden;
- e) Vorschriften für die Marktbeobachtung und Marktüberwachung.

- Die Verordnung unterscheidet wie folgt:
- Minimales Risiko: zum Beispiel KI gestützte Empfehlungssysteme oder Spamfilter:. Aber Transparenz- und Hinweispflichten
- hohes Risiko: strenge Anforderungen: Systeme zur Risikominderung, hohe Qualität der Datensätze, Protokollierung von Aktivitäten, ausführliche Dokumentation, klare Benutzerinformationen, Möglichkeit der menschlichen Aufsicht, hohes Maß an Robustheit, Genauigkeit und Cybersicherheit.
- unannehmbares Risiko: eindeutige Bedrohung für Grundrechte, zum Beispiel KI, die das menschliche Verhalten manipuliert oder Social Scoring ermöglicht. Auch einige Anwendungen biometrischer Systeme, zum Beispiel zur Erkennung von Emotionen an Arbeitsplatz und einige Systeme zur Kategorisierung von Personen oder zu biometrischen Fernidentifizierung in Echtzeit zu Strafverfolgungszwecken in öffentlich zugänglichen Räumen.
- Militärische KI ist gemäß Art. 2 Abs. 3 vom Geltungsbereich der Verordnung ausgenommen.

- KI- Modelle mit allgemeinem Verwendungszweck (General Purpose AI - GPAI), Artt. 53, 54
- KI- Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko, Art. 55
- KI- Kompetenz, Art. 4
- Transparenzpflichten, Art. 50

- Die Verordnung gilt für
 - – Anbieter, die KI-Systeme in der Union Inverkehrbringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;
 - – Nutzer
 - – Anbieter und Nutzer in einem Drittland, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird.
 - – Gilt für Hochrisiko-KI-Systeme
- es gelten die in Art. 2 Absatz 2a-h) genannten Ausnahmen.
- Gilt nicht für Behörden in Drittländern oder internationale Organisationen.

- Die Verordnung gilt für
 - – Anbieter, die KI-Systeme in der Union Inverkehrbringen oder in Betrieb nehmen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;
 - – Nutzer
 - – Anbieter und Nutzer in einem Drittland, wenn das vom System hervorgebrachte Ergebnis in der Union verwendet wird.
 - – Gilt für Hochrisiko-KI-Systeme
- es gelten die in Art. 2 Absatz 2a-h) genannten Ausnahmen.
- Gilt nicht für Behörden in Drittländern oder internationale Organisationen.

- – KI System mit Techniken der unterschwelligen Beeinflussung (Absatz 1 lit. a)
- – KI System, das eine Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund Alter oder körperlichen oder geistigen Behinderungen ausnutzt, wenn dies einen psychischen oder physischen Schaden zufügt oder zufügen kann.
- – KI zur Bewertung oder Klassifizierung von Vertrauenswürdigkeit natürlicher Personen durch Behörden auf Grundlage ihres sozialen Verhaltens oder vorhergesagte persönliche Eigenschaften, sofern dies zu den in Art. 5 Absatz 1c) genannten Folgen führt.
- – Verwendung biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zur Strafverfolgung (mit umfangreichen Ausnahmen in Artikel 5d) und Abs. 2 und 3.

- Immer ein Hochrisiko-System wenn
 - – Sicherheitskomponente eines in Anhang II aufgeführten Produktes verwendet wird oder selbst ein solches Produkt ist;
 - – das Produkt, dessen Sicherheitskomponente das KI-System ist, oder das KI System selbst als Produkt eine Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen dieses Produktes gemäß den in Anhang II aufgeführten Vorschriften braucht.
 - – Alle in Anhang III genannten KI Systeme

- 1. Biometrische Identifizierung und Kategorisierung natürlicher Personen:
- 2. Verwaltung und Betrieb kritischer Infrastrukturen:
- 3. Allgemeine und berufliche Bildung:
- 4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit:
- 5. Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen:
- 6. Strafverfolgung:
- 7. Migration, Asyl und Grenzkontrolle:
- 8. Rechtspflege und demokratische Prozesse
- Alle Punkte sind in Anhang III umfangreich weiter ausgeführt.

- Risikomanagementsystem
- Daten-Governance, Art. 10
- Technische Dokumentation, Art. 11
- Aufzeichnungspflichten, Art. 12
- Menschliche Aufsicht, Art. 14
- Genauigkeit, Robustheit und Cybersicherheit
- Qualitätsmanagement, Art. 17
- Transparenz, Art. 13
- KI- Kompetenz , Art. 4 – alle!

- „Ein Viertel unserer Ingenieure ist ausschließlich mit Vorschriften beschäftigt.“
- Stellantis- Chef John Elkann
- (lt. Frankfurter Allgemeine Sonntagszeitung 11.5.2025 in einem Interview mit „Le Figaro“)

- A fährt den LKW seiner Firma. Auf der Straße liegt ein Stein. A will ausweichen. Die KI sagt: „weiterfahren“. Er fährt auf den Stein. Schaden am LKW 5.000 €.
- Im toten Winkel war ein Fahrradfahrer.

Fall wie vor: da war keiner im toten Winkel.

Haftung A?

- Fall wie vor:
- A ignoriert KI- Anweisung und weicht aus und überfährt einen Radfahrer.
- Fahrlässige Tötung durch A?
- § 222 StGB Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe.

- Mai 2016:
- Der 40-jährige Joshua Brown fuhr mit seinem Tesla Model S vollautonom auf einer Autobahn in Florida. Ein 18-Rad-Lkw mit einem Anhänger voller Blaubeeren kreuzt seinen Weg. Das Wetter war ein strahlender Sonnentag. Das Radar des Tesla verwechselte das hochkantige Fahrzeug wahrscheinlich mit einem Verkehrsschild. Und die Kameras verwechselten vermutlich den weißen Anhänger mit dem Himmel. Infolgedessen sah das Auto den Lkw nicht, bremste nicht und fuhr mit voller Geschwindigkeit von 120 KM/h in den 16 m langen Kühltransporter. Und das mit überhöhter Geschwindigkeit von fast 15 km schneller als auf der Straße (105 km/h) erlaubt war.
- Bei dem Aufprall fuhr der Tesla unter den Lkw. Die Windschutzscheibe des Tesla prallte auf den Boden des Anhängers. Das Dach des Fahrzeugs wurde durch die Wucht des Aufpralls abgerissen. Der Wagen fuhr weiter und prallte gegen einen Strommast. Joshua Brown starb sofort an den Folgen stumpfer Gewalteinwirkung auf den Kopf.
- Die Hände des Fahrers waren während der letzten 37 Minuten seiner Fahrt nur 25 Sekunden lang am Steuer. Das Autopilot-System hatte ihn vor dem tödlichen Unfall siebenmal gewarnt, seine Hände wieder ans Steuer zu legen. Und siebenmal nahm er seine Hände vom Lenkrad. Nach Angaben der Nachrichtenagentur Associated Press berichtete der am Unfall beteiligte LKW-Fahrer, dass Brown zum Zeitpunkt des Unfalls gerade einen Harry-Potter-Film angeschaut habe. Die Polizei hatte einen tragbaren DVD-Player aus dem Auto geborgen.

- März 2018:
- In Arizona führte Elaine Herzberg zu Fuß ihr Fahrrad über die Straße und wurde von einem selbstfahrenden Uber-Testfahrzeug angefahren und getötet.
- Das selbstfahrende System von Uber erkannte die Frau fast 6 Sekunden vor dem Aufprall. Das System hatte sie jedoch nicht als Fußgängerin eingestuft. Sie überquerte die Straße nämlich an einer Stelle, an die es keinen Fußgängerüberweg gab, und das System war so eingestellt, dass es sogenannte „Jaywalker“, also Personen, die an unzulässigen Stellen die Straße überqueren, ignoriert, da das zu viele Fehlalarme gab. Außerdem änderte die Software ständig ihre Klassifizierung – war Elaine Herzberg ein Fahrzeug, ein Fahrrad, ein unbekanntes Objekt? – was das Auto daran hinderte, zu bremsen oder weg zu lenken.
- Als das selbstfahrende Auto schließlich Alarm schlug, um die Sicherheitsfahrerin von Uber zum Eingreifen aufzufordern, blieb der nur der Bruchteil einer Sekunde, um zu reagieren.
- Hier kommt nun der menschliche Faktor ins Spiel: Erschwerend kam nämlich hinzu, dass die Sicherheitsfahrerin, als der Alarm schließlich losging, gerade eine Folge von „The Voice“ auf ihrem Mobiltelefon anschaute. Sie wurde daraufhin wegen Mordes angeklagt.
- Die Ermittler des National Transportation Safety Board, die den Unfall untersuchten, übten scharfe Kritik an Uber. Sie stellten fest, dass dem Testprogramm in Arizona ein formeller Sicherheitsplan, Vollzeit-Sicherheitspersonal und angemessene Betriebsverfahren fehlten. Außerdem hatte Uber nur fünf Monate vor dem Unfall seine Testfahrer von zwei auf einen pro Fahrzeug reduziert.

- Beispiel:
- Sven G. fährt Auto. Plötzlich läuft ein Fußgänger vor ihm auf die Straße. Rechtzeitiges Bremsen ist nicht mehr möglich, sondern nur das Ausweichen. Ausgewichen werden kann nur auf den Bürgersteig. Dort geht gerade eine Frau mit Kinderwagen über den Bürgersteig, die sicherlich verletzt oder gar getötet werden würden.
- Beispiel:
- Wie vor: auf der Straße befinden sich drei, auf dem Bürgersteig dagegen nur eine Person.
- Strafbarkeit von Sven G.?

Datenschutz

- Problem Testdaten
- Werden personenbezogene Daten erfasst, müssen gemäß Art. 12-14 DSGVO die Betroffenen informiert werden. Ist bei Suche im Internet unmöglich.
- Wohl keine Rechtsgrundlage:
- Einwilligung (-)
- Berechtigte Interessen (-) , besondere Kategorien nicht vermeidbar.
- Folge : Bußgelder 10/20 Mio. ,2 oder 4 % Weltjahresumsatz
- Vgl. LfDI BW: Diskussionspapier Datenschutz bei KI (siehe Folie Datenschutz 4)

- <https://datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbots>
- Aspekte zum kontrollierten Umgang mit LLM-Chatbots
- 1. Compliance-Regelungen vorgeben
- 2. Datenschutzbeauftragte einbinden
- 3. Bereitstellung eines Funktions-Accounts
- 4. Sichere Authentifizierung
- 5. Keine Eingabe personenbezogener Daten
- 6. Keine Ausgabe personenbezogener Daten
- 7. Vorsicht bei personenbeziehbaren Daten
- 8. Opt-out des KI-Trainings
- 9. Opt-out der History
- 10. Ergebnisse auf Richtigkeit prüfen
- 11. Ergebnisse auf Diskriminierung prüfen
- 12. Keine automatisierte Letztentscheidung
- 13. Beschäftigte sensibilisieren
- 14. Datenschutz ist nicht alles
- 15. Weitere Entwicklung verfolgen

Weil es so lustig ist:

LfDI BW – Diskussionspapier. Version 1.0 vom 07.11.2023 –

„Insgesamt stellt Art. 6 Abs. 1 Buchst. f DS-GVO aufgrund des offenen Tatbestands für die meisten Verarbeitungsprozesse im KI-Kontext eine besonders geeignete Rechtsgrundlage dar. Aufgrund der obligatorischen Interessenabwägung kann die Norm allerdings nur bedingt eine Rechtssicherheit vermitteln, da es stets erforderlich sein wird, den konkreten Einzelfall umfassend zu bewerten.“

2. Prof. Dr. Rolf Schwartmann, Vorstand GDD:

Wohlverstandener Datenschutz ist ein Standortvorteil.

und:

Lebensschutz geht nicht vor Datenschutz.

- Trotzdem:

- Viel Erfolg mit KI!

Vielen Dank für Ihre Aufmerksamkeit!

Prof. Andreas Göbel

Rechtsanwalt

Fachanwalt für Informationstechnologierecht

Fachanwalt für Arbeitsrecht

Honorarprofessor der FH Südwestfalen

Aschenbergstr. 3

58097 Hagen

Tel.: 02331 348180

info@goebel.law

www.goebel.law