Der Bayerische Landesbeauftragte
für den Datenschutz

Fotos veröffentlichen = KI trainieren?

Aktuelle Kurz-Information 55

Stichwörter: Künstliche Intelligenz: Trainingsdaten – Metadaten in Fotodateien: Trainingsdaten für Künstliche Intelligenz –Selfies: Trainingsdaten für Künstliche Intelligenz – Soziale Medien: Trainingsdaten für Künstliche Intelligenz – Trainingsdaten: Künstliche Intelligenz | **Stand:** 1. April 2024

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Das Training von KI-Modellen benötigt grundsätzlich viele Daten – auch personenbezogene.
- Jede Veröffentlichung personenbezogener Daten ist mit dem Risiko verbunden, dass diese als Trainingsdaten für KI-Modelle genutzt werden.
- Bayerische öffentliche Stellen müssen dieses Risiko in den Blick nehmen, wenn sie personenbezogene Daten etwa auf der eigenen Internetpräsenz, in Sozialen Netzwerken oder über die Medien offenlegen.
- Das gilt insbesondere für die Veröffentlichung von Fotos mit Beschreibungen – auch in den Metadaten.

Entwickler von Systemen Künstlicher Intelligenz (KI) sind auf eine Nutzung umfangreicher Datenbestände angewiesen, wenn sie auf statistische Verfahren gestützte Modelle effektiv trainieren möchten. Allgemein gilt der Grundsatz: Die Qualität der Ergebnisse steigt mit der Quantität der Trainingsdaten. Was liegt da näher, als den „Datenhunger“ der KI mit öffentlich verfügbaren Informationen zu stillen? 1

Das Internet bietet hier reichlich Nahrung: Die Bilddokumentation des eigenen Lebens unter Einschluss zahlreicher anderer Personen in Sozialen Medien ist längst keine Seltenheit mehr. Dabei sind in Fotos oft mehr Informationen gespeichert, als es den Beteiligten lieb ist: Kontexte, Bildbeschreibungen, auch die gern übersehenen, oftmals automatisiert angelegten Metadaten „plaudern“ darüber, wer wo wie abgebildet ist. Eine KI, die aus solchen Daten lernt, wird dann auch damit arbeiten. 2

Die vorliegende Aktuelle Kurz-Information ordnet die skizzierten Risiken ein und gibt Bürgerinnen und Bürgern wie auch bayerischen öffentlichen Stellen Empfehlungen für präventive Maßnahmen. 3

1. Um welche Risiken geht es?

Viele Nutzerinnen und Nutzer von internetbasierten Anwendungen, insbesondere Sozialen Medien, haben keine genauen Vorstellungen darüber, wie detailreich ihr digitales Abbild ausfällt – und welche „Schönheitsfehler“ es im Einzelnen (schon) zeigt. Manche vor Jahren geschriebenen Posts und hochgeladenen Fotos sind immer noch öffentlich, selbst wenn die Kennung und das Passwort für die betreffende Plattform längst vergessen sind und die Nutzerin oder der Nutzer auf andere Plattformen weitergezogen ist. Vielen Nutzenden war bei alldem auch nie so recht bewusst, dass moderne Smartphones gespeicherte Fotos häufig „von sich aus“ mit Metadaten wie dem Namen oder Geokoordinaten anreichern. **Nutzende können deshalb durchaus weit mehr von sich öffentlich preisgegeben haben, als ihnen aktuell bewusst und/oder erwünscht ist.** 4

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

5 Was einmal an zuordnungsfähigen Informationen, insbesondere an Fotos, öffentlich ist, kann grundsätzlich jedermann zu Gesicht bekommen – auch derzeitige (oder zukünftige) Vorgesetzte, Geschäftspartnerinnen, die Gegenpartei in einem Rechtsstreit, Mitschüler, (Ex-)Partner oder Verwandte. Ganz unscheinbar und zunächst einmal unbemerkt gesellt sich eine wachsende Anzahl von KI-Systemen hinzu, die öffentlich abrufbare Informationen zu unterschiedlichen, teils unbekannten oder sogar unerwünschten Zwecken sammeln („crawlen") und nutzen.

6 Initiativen wie das Large-scale Artificial Intelligence Open Network (LAION) kommen den KI-Entwicklern noch weiter entgegen: Nach ihren an sich positiv klingenden Grundsätzen von Transparenz und Offenheit bietet diese Non-Profit-Organisation eigenen Angaben zufolge Trainings-Datensätze, Werkzeuge und Modelle zum Experimentieren mit Machine Learning zur freien Verfügung an. Auf dieser Grundlage sollen KI-Anwendungen ohne hohe Investitionskosten für den Aufbau umfangreicher Datenbestände entwickelt werden können, damit – so das Ziel dieser Organisation – nicht ausschließlich finanzstarke Großunternehmen den Markt- und Forschungsbereich „KI" unter sich aufteilen. Wie ein bekannt gewordener Fall zeigt, können solche Trainingsdatensätze jedoch auch (ungewollt) sogar sensible personenbezogene Daten enthalten: Bei der Analyse des Trainingsdatensatzes für die KI-Bildgenerierung „LAION-5B"[1] haben Datenjournalistinnen des Bayerischen Rundfunks eine Vielzahl an Informationen entdeckt, mit denen Personen identifiziert werden könnten: Neben Gesichtern und Namen fanden sie Geokoordinaten, E-Mails und sogar Kontonummern.[2]

7 Das Beispiel zeigt: Angesichts des „Datenhungers" von KI und der bereits heute umfangreichen Verarbeitung öffentlich abrufbarer Informationen ist immer wieder zu überdenken, welche potenziellen Risiken mit einer Veröffentlichung personenbezogener Informationen einhergehen können. Unbeabsichtigt preisgegebene, zusätzliche Informationen in Form von Metadaten verschärfen das Problem zusätzlich.

8 Insbesondere trägt der internationale Datenhandel dazu bei, dass „das Internet" einmal veröffentlichte Daten oft nicht „vergisst" – selbst wenn personenbezogene Daten auf Löschungsanträge hin aus einzelnen Trainingsdatensätzen vielleicht eliminiert werden können. Sind die Daten einmal in ein KI-System eingeflossen, gestaltet sich die Situation noch komplizierter: Einzelne Daten können grundsätzlich nicht wieder „heraustrainiert" werden. Vielmehr müsste das jeweilige Modell mit einem aktualisierten Trainingsdatensatz „fortgebildet" werden (was mit erheblichen Kosten verbunden wäre). Zudem lässt sich an einem trainierten Modell in der Regel nicht nachweisen, dass bestimmte Daten Teil der Trainingsdaten waren.

9 Die Risiken für die Rechte und Freiheiten der Bürgerinnen und Bürger wachsen also. Werden etwa Personenfotos zum Training KI-gestützter Gesichtserkennung genutzt und wird dieses Instrument etwa in einem Urlaubsland für Fahndungszwecke eingesetzt, können sich bei einer „ahnungslosen" Einreise leicht nachteilige Konsequenzen ergeben – zumal im Fall falschpositiver Treffer.

2. Fotos: mehr als die Summe ihrer Pixel

10 Beim Speichern eines Fotos können der eigentlichen Aufnahme zusätzliche Informationen (sog. Metadaten) – meist automatisiert – hinzugefügt werden. Dabei fungiert etwa das

„Exchangeable Image File Format“ (kurz: „Exif“) als Standard für solche Metadaten und definiert eine ganze Reihe an Datenfeldern (sog. „Exif-Tags“) mit technischen Informationen,[3] wie etwa Kameramodell, Zeitpunkt der Aufnahme oder Kameraeinstellungen. Die Liste an Informationen wirkt auf den ersten Blick unauffällig, doch können gleich in mehreren Datenfeldern personenbezogene Daten hinterlegt werden. Besonders erwähnenswert sind hier die Felder „Autor/Fotograf“ sowie der Copyright-Vermerk, die ganz bewusst einen Personenbezug vorsehen, aber auch die geografische Position, die von Geräten mit integriertem GPS-Sensor hinzugefügt wird (fast jedes moderne Smartphone verfügt über einen solchen). Viele sind sich der Existenz dieser Datenfelder ebenso wenig bewusst wie der schädlichen Verwendungsmöglichkeiten für deren Inhalte. Werden Fotodateien mit Exif-Tags im Internet veröffentlicht, kann die Privatsphäre beispielsweise folgendermaßen beeinträchtigt werden:

11 – **Ortungsverfolgung:** Eine Person veröffentlicht ein Urlaubsfoto an einem Strand. Das Foto weist keine besonderen Landschaftsmerkmale auf, und die Person ist deshalb der Überzeugung, dass ihr konkreter Aufenthaltsort bei einer Veröffentlichung dieses Fotos unbekannt bleibt. Das für die Aufnahme genutzte Smartphone speichert jedoch im Hintergrund die Geokoordinaten mit ab. Wird diese Bilddatei auf ein Soziales Netzwerk hochgeladen, können die Metadaten ausgelesen werden, um den Standort des Benutzers zu erfahren. Dass es sich hierbei um kein rein theoretisches Szenario handelt, zeigt ein Fall, über den die Presse bereits im Jahr 2012 berichtete.[4]

12 – **Veröffentlichung privater Momente:** Angenommen, eine Person lädt ein Bild mit sensiblen Inhalten hoch, wie zum Beispiel ein freizügiges Foto oder eine private Versammlung – in der Annahme, dass sie selbst auf dem Foto nicht ohne weiteres identifizierbar ist (Gesicht nicht ausreichend gut erkennbar). Da die Metadaten aber den Namen des Benutzers enthalten können, ist mit diesen unbewusst mitgespeicherten Informationen unter Umständen doch eine Identifizierung möglich. Dies war zwar bereits vor der Existenz aktueller KI möglich, neueste Entwicklungen in der Bilderkennung und im gesamten Verarbeitungsprozess verschärfen das Problem aber deutlich. Fotos können automatisiert in sehr großer Zahl und sehr hoher Geschwindigkeit verarbeitet, verglichen und ganz allgemein mit anderen Fotos und Informationen zusammengeführt werden. Das ist betroffenen Personen beim Hochladen oder dem Festlegen der Privatsphäreeinstellungen oftmals kaum bewusst. Fotos, auf denen Gesichter zu erkennen sind, können schnell zur Quelle einer Rufschädigung werden.

13 In diesem Zusammenhang sorgte die US-amerikanische „Gesichtersuchmaschine“ Clearview AI bereits mehrfach für Aufsehen. Diese kostenpflichtige Software erlangte 2020 Bekanntheit, als die New York Times mit einer Recherche die eindrucksvolle Datensammlung des Unternehmens aufdeckte[5]. In der Suchmaschine kann neben dem Namen auch ein Foto als Suchkriterium genutzt werden[6]. Seine Datensammlung hatte das Unternehmen mutmaßlich aus Online-Quellen wie Sozialen Medien oder Nachrichten zusammengestellt. Da es sich bei Clearview AI um eine Software handelt, die auch von Strafverfolgungsbehörden (in den USA) eingesetzt wird, können die Folgen betroffenen Personen insbesondere in Fällen von Fehlzuordnungen, über die in den Medien bereits berichtet wurde,[7] nachhaltig schaden.

14 Social Media Plattformen entfernen Metadaten beim Upload von Fotos nicht immer automatisch von selbst. Dies mag zum einen an einem möglichen Eigeninteresse der Betreiber an diesen Daten liegen. Es können aber auch urheberrechtliche Gründe gegen die Entfernung sprechen.[8]

3. Zwischenfazit

15 Zusammenfassend lässt sich festhalten, dass die Fortschritte im Bereich KI die Risiken für die Rechte und Freiheiten von Bürgerinnen und Bürgern zunehmend anwachsen lassen. Die Abhängigkeit der KI-Systeme von großen Datensätzen und das daraus folgende Heranziehen öffentlich zugänglicher Informationen für das KI-Training bringen für die Internetveröffentlichung personenbezogener Daten neue, unter Umständen schwer kalkulierbare Risiken mit sich.

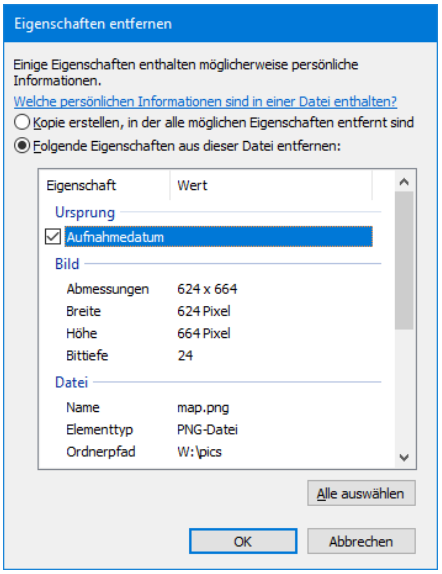
16 Angesichts der vielfältigen Möglichkeiten der Veröffentlichung personenbezogener Informationen insbesondere über Soziale Medien ist es daher Aufgabe einer und eines jeden Einzelnen, die eigenen Gewohnheiten insofern grundlegend zu überdenken.

4. Empfehlungen für Bürgerinnen und Bürger

17 Um persönliche Informationen zu schützen und potenzielle Risiken zu mindern, sollten Bürgerinnen und Bürger folgende Maßnahmen in Betracht ziehen:

18 **Bewusster Verzicht:** Überlegen Sie, ob Sie wirklich personenbezogene Daten – insbesondere Fotos oder Kurzvideos – veröffentlichen möchten. Nur weil es einfach und schnell geht, sind „ein paar Likes“ schwer kalkulierbare Risiken nicht wert. Verzichten Sie im Zweifel zu Ihrem eigenen Schutz auf eine Veröffentlichung.

19 **Entfernen von Bild-Metadaten:** Bevor Sie Bilder online teilen, können Sie Metadaten entfernen (oder modifizieren). Dafür gibt es zahlreiche (auch kostenlose) Tools und Anwendungen, die dabei helfen, Ihre Privatsphäre zu schützen. Auch der Windows Explorer kann nach einem „Rechtsklick“ auf ein Bild im „Details“-Reiter unten „Eigenschaften entfernen“, die Personenbezüge haben können (Abbildung rechts).



20 **Datenschutzeinstellungen und Bewusstsein:** Machen Sie sich mit den Datenschutzeinstellungen der von Ihnen genutzten Sozialen Medien vertraut. Dazu gehört insbesondere die Einstellung, wer welchen Beitrag, welches Foto oder Kurzvideo sehen darf – hier ist insbesondere die Einstellung „öffentlich“ problematisch.

Zu dieser „Öffentlichkeit“ haben sich nämlich nun möglicherweise KI-Firmen „hinzugesellt“, die zum Training ihrer Machine Learning-Modelle diese „frei verfügbaren Daten und Informationen“ auch auf Social Media-Plattformen sammeln. Die damit verbundenen Risiken für die oder den Einzelnen lassen sich aktuell noch nicht absehen. Selbst auferlegte wie auch gesetzliche Regelungen können mit den rasant wachsenden Fähigkeiten von KI nicht immer mithalten. 21

Auf den Medientagen Ende Oktober 2023 in München tauschten sich rund 5.000 Besucher drei Tage lang über die wichtigsten KI-Trends aus und sprachen insbesondere über Chancen und Risiken.[9] Neben bewusster Desinformation und unbewusster Falsch- und Fantasieinformation wurde hier die Sorge geäußert, „dass am Vorabend der Wahl irgendwelche Deepfakes auftauchen“. Bei Deepfakes handelt es sich um von KI generierte, täuschend echt aussehende Fotos oder sogar bewegte Videos mit Ton, in denen die betroffene Person Dinge tut oder sagt, die sie so eventuell nie wirklich getan oder gesagt hat. Moderne KI kann schon mit nur wenig Trainingsmaterial solche Deepfakes erstellen – **je mehr Fotos, Videos und Sprachaufnahmen einer Person öffentlich verfügbar sind, desto authentischer gelingt dies**. Bekannt geworden sind etwa täuschend echte „Fotos“, die eine Verhaftung von Donald Trump zeigen oder Papst Franziskus im neuen Designer-Daunenmantel,[10] ebenso ein gefaketes Statement des Bundeskanzlers zu einem Parteiverbot.[11] 22

Passen Sie also die Einstellungen zur Sichtbarkeit Ihrer Daten und Beiträge entsprechend Ihren Präferenzen an. Bleiben Sie wachsam und informiert. Üben Sie auch Selbstkritik: Sie wissen selbst am besten, was Sie schon alles öffentlich gepostet haben. Haben Sie schon einmal eine Veröffentlichung bereut? Gibt es von Ihnen Bilder, die heute nicht mehr zu Ihnen passen? Würden Sie die auf Social Media-Plattformen hochgeladenen Bilder auch mit Ihren aktuellen Kontakten teilen wollen? Was sagt die in Ihrem digitalen Leben bisher entstandene Sammlung von Texten, Bildern und Videoclips über Sie aus? Vermittelt sie das Bild, das andere von Ihnen haben sollen? Wenn Fragen dieser Art Ihnen ein „ungutes“ Gefühl bereiten: Werden Sie aktiv! 23

Überprüfen und Löschen: Überprüfen Sie am besten regelmäßig persönliche Informationen, die Sie eventuell auch schon vor längerer Zeit geteilt haben, auf ihre „Sichtbarkeit“, indem Sie die Beiträge betrachten, nachdem Sie sich aus dem jeweiligen Dienst abgemeldet haben. Löschen Sie sie im Bedarfsfall. Beachten Sie zudem, dass Sie auch auf Fotos erkennbar sein könnten, die andere gemacht oder hochgeladen haben. Bitten Sie hier um Löschung; Sie haben grundsätzlich ein Recht darauf (Art. 17 Datenschutz-Grundverordnung). 24

Um etwa bestimmte Informationen bei Facebook zu löschen, können Sie nach der Anmeldung zu den entsprechenden Abschnitten in den Einstellungen gehen. Beispielsweise können Sie unter „Profil und Tagging“ Ihre einzelnen Beiträge prüfen und löschen. Es ist jedoch wichtig zu beachten, dass selbst in diesem Fall möglicherweise Kopien der Daten auf den Servern von Facebook oder in den Konten anderer Personen vorhanden sind, wenn Sie Inhalte geteilt haben. 25

Ungenutzte Accounts löschen: Sie nutzen bestimmte Soziale Medien tatsächlich nicht mehr und konnten sich bisher nur nicht durchringen, Ihren Account zu löschen? Dann nehmen Sie die aktuellen Entwicklungen im Bereich von KI zum Anlass, vielleicht doch den einen 26

oder anderen Zugang aufzulösen oder zumindest zu sperren, sodass die darin gespeicherten Informationen nicht mehr öffentlich zugänglich sind.

27 Wenn Sie etwa Ihr Facebook-Konto deaktivieren möchten, können Sie dies unter „Deaktivierung und Löschung" in den Kontoeinstellungen tun. Beachten Sie, dass dies Ihr Konto nur vorübergehend deaktiviert und Sie es später reaktivieren können, wenn Sie sich erneut anmelden. Möchten Sie Ihr Konto dauerhaft löschen, wählen Sie die Option „Dein Konto und deine Informationen löschen". Befolgen Sie die Anweisungen, um den Löschvorgang abzuschließen. Bedenken Sie, dass dies irreversibel ist und alle Ihre Daten dauerhaft entfernt werden.

5. Hinweise für bayerische öffentliche Stellen

28 Auch bayerische öffentliche Stellen posten mitunter Fotos oder Videoclips, auf denen Personen zu erkennen sind, oder stellen Beiträge mit anderen personenbezogenen Daten ein. Einige Beispiele:

- Eine Gemeinde veröffentlicht auf einer Webseite Momente aus öffentlichen Veranstaltungen mit darauf erkennbaren Bürgerinnen und Bürgern.
- Ein Landratsamt teilt eine Liste von Bürgerinnen und Bürgern, die in bestimmten Programmen oder Projekten engagiert sind.
- Ein kommunales Kulturzentrum veröffentlicht Fotos von Veranstaltungen oder Konzerten, auf denen Einzelpersonen erkennbar sind.
- Eine Feuerwehr stellt eine Liste von Bürgerinnen und Bürgern online, die an Erste-Hilfe-Kursen teilgenommen haben.
- Eine öffentliche Schule teilt auf ihrer Website Bilder von Schulveranstaltungen, auf denen Schülerinnen und Schüler erkennbar sind.

29 Ungeachtet der Frage, ob die jeweilige Veröffentlichung in dieser Form überhaupt für bayerische öffentliche Stellen zulässig war, verweisen alle diese Beispiele auf mangelnde „KI-Disziplin": Machine Learning-Modellen Trainingsmaterial bereitzustellen ist nicht Aufgabe bayerischer öffentlicher Stellen. (Noch) mehr als bisher sollte bei der öffentlichen Bereitstellung insbesondere von Foto- und Videodateien Zurückhaltung geübt werden, wenn Personen erkennbar sind. Dies gilt gerade dann, wenn diese in begleitenden Texten auch noch namhaft gemacht werden.

30 Bayerische öffentliche Stellen sind grundsätzlich gut beraten, eine datensparsame Öffentlichkeitsarbeit zu betreiben. Auch wenn eine Rechtsgrundlage für eine Offenlegung personenbezogener Daten zur Verfügung stehen sollte: Nicht immer „braucht" die „Message" ein Gesicht – eine Gemeindehomepage darf ihre Stärke in guter Information haben. Das hilft den Bürgerinnen und Bürgern mehr als bunte Fotos von Beschäftigten.

31 Sollen dennoch Bilder mit Personen veröffentlicht werden, sollte eine „Verpixelung" geprüft werden; dies gilt insbesondere für Personen „im Hintergrund". Metadaten braucht es in den seltensten Fällen – also: weg damit! Apps bieten hier eine Vielzahl an Funktionen und Filtern, mit denen es etwa möglich ist, zu zeigen, dass eine Veranstaltung gut besucht war, ohne dass

dabei einzelne Besucherinnen und Besucher identifizierbar sind. Zurückhaltung ist auch bei Bildbeschreibungen angebracht –nicht jede oder jeder muss namhaft gemacht werden.

Ein weiterer Aspekt ist die Zugänglichmachung: Werden die Daten und Medien öffentlich gemacht oder kann der Personenkreis sinnvoll eingeschränkt werden -etwa auf einen „internen“ zugangsgeschützten Bereich. Neben diesem „harten“ Zugangsschutz, gibt es die „noindex“-Funktion, mit der Suchmaschinen und Indizierungstools angewiesen werden, die so markierten Inhalte oder Unterseiten nicht zu indexieren oder zu berücksichtigen.[12] 32

6. Fazit

Es passiert schnell, dass man mehr personenbezogene Daten und Informationen veröffentlicht, als man möchte. Das gilt für die oder den Einzelnen ebenso wie für bayerische öffentliche Stellen. Insbesondere die erst einmal nicht sichtbaren (weil von den gängigen Foto-Apps normalerweise nicht angezeigten) Exif-Daten sind in diesem Zusammenhang relevant. Neben diesem eher auf Fotos beschränkten Problem ist ganz allgemein vor Risiken zu warnen, die mit der Veröffentlichung personenbezogener Daten einhergehen. Diese zum Teil bereits seit längerem -etwa im Zusammenhang mit Suchmaschinen -bestehenden Risiken haben sich im Zuge des jüngsten Verbreitungsschubs von KI und insbesondere des „unkontrollierten“ Crawlings öffentlich zugänglicher Informationen zur Gewinnung von Trainingsdaten noch einmal verschärft. Insofern ist zu empfehlen, das „Ob“ neuer und bestehender Veröffentlichungen kritisch zu prüfen. Außer an Verzicht und Löschung sollte auch an eine Entfernung oder Minimierung von Personenbezügen gedacht werden. 33

1 Internet: https://laion.ai/blog/laion-5b.
2 Internet: https://www.br.de/nachrichten/netzwelt/trainingsdaten-fuer-ki-sind-voller-privater-informationen,TjDw2vh.
3 Ausführliche Liste unter: https://exiftool.org/TagNames/EXIF.html.
4 Internet: https://www.golem.de/news/vice-john-mcafee-mit-iphone-geolocation-geortet-1212-96131.html.
5 Internet: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
6 Internet: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
7 Internet: https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.
8 Dazu näher Oberlandesgericht Köln, Urteil vom 20. Januar 2017, 6 U 105/16, BeckRS 2017, 102365, Rn. 27 und Urteil vom 2. Juni 2023, 6 U 17/23, GRUR-RS 2023, 12243, Rn. 14 ff.
9 Der Bayerische Rundfunk (BR) berichtete: https://www.br.de/nachrichten/deutschland-welt/medientage-wo-die-chancen-von-ki-liegen-und-wo-die-risiken,TttxJQe.
10 Internet: https://www.heise.de/hintergrund/Der-KI-Papst-in-Daunenmantel-sollte-eine-Warnung-sein-8146920.html.
11 BR-Bericht: https://www.br.de/nachrichten/netzwelt/scholz-deepfake-sind-ki-faelschungen-verboten,TwzZ6nE.
12 Siehe etwa für OpenAI die Dokumentation zu ChatGPT: https://platform.openai.com/docs/gptbot.