**Kurs 4: Deepfakes und Urheberrecht in der KI**

***[Bildschirminhalt] Eingeblendeter Videotitel " Deepfakes und Urheberrecht in der KI"***

Voice over: - Deepfakes und Urheberrecht in der KI. Stellen Sie sich vor, Sie scrollen durch Ihren Social Media-Feed und Sie stoßen auf ein Video einer berühmten Person, die etwas Kontroverses sagt. Sie sind erst verwundert, doch dann fällt Ihnen ein – es könnte ein sogenannter Deepfake sein.

***[Bildschirminhalt] Ein Mobiltelefon zeigt ein Video mit Untertiteln.***

Ein Deepfake ist ein gefälschter Medieninhalt, der verändert oder erstellt wurde. Deepfakes sind normalerweise gefälschte Audio- oder Videoinhalte, bei deren Erstellung auch KI eingesetzt werden kann.

Deepfakes setzen mittlerweile häufig fortschrittliche KI-Techniken ein, um die Stimme, das Bild einer realen Person oder beides durch erschreckend ähnliche künstliche Nachbildungen zu ersetzen. Diese Technologie hat dazu geführt, dass es zunehmend schwieriger wird, zu erkennen, ob etwas, das Sie im Internet sehen oder hören, real ist.

Deepfakes werden häufig zur Verbreitung von Desinformationen eingesetzt und können bei Betrügereien, Wahlmanipulationen, Social Engineering-Angriffen und anderen Arten von Betrug eingesetzt werden.

***[Bildschirminhalt] Eine Person mit einer Maske, Geld, Akten und einer ID-Karte.***

Angesichts der dringenden Notwendigkeit, Deepfakes zu bekämpfen, ergreift der Technologiesektor Gegenmaßnahmen, darunter auch Unternehmen, die an der Erstellung von KI-Modellen und Consumer Services beteiligt sind, wie Microsoft.

Diese Bemühungen haben sich im Laufe der Zeit weiterentwickelt, von der Einführung von Funktionen zur Fälschungssicherheit bis hin zu fortschrittlichen digitalen Schutztechnologien.

Im Folgenden erfahren Sie, was der Tech-Sektor unternimmt: Schaffung einer sicheren Umgebung: Es werden Sicherheitsmaßnahmen getroffen, um reibungslose und sichere Abläufe zu gewährleisten. Dazu gehören Dinge wie ständige Kontrollen, das Blockieren von Fehlverhalten und schnelles Handeln gegen diejenigen, die das System missbrauchen.

***[Bildschirminhalt] KI in einem Kreis mit Symbolen, die es umkreisen.***

Inhaltsnachweise: Um gefälschte Videos, Bilder oder Audio zu bekämpfen, werden spezielle Markierungen oder Symbole zu KI-erstellten Inhalten hinzugefügt. So lässt sich feststellen, woher der Inhalt stammt und wie er entstanden ist.

Sichere Dienste: Es werden Anstrengungen unternommen, um schädliche und irreführende Inhalte auf Online-Plattformen zu erkennen und sie zu entfernen. Dies trägt dazu dabei, den digitalen Raum generell für alle sicher und vertrauenswürdig zu halten.

Zusammenarbeit: So wie Zusammenarbeit der Schlüssel zum Erreichen gemeinsamer Ziele ist, können Einzelpersonen aus der Technologiebranche, Organisationen, die sich dem Gemeinwohl widmen, und Verwaltungseinrichtungen gemeinsam dazu beitragen, eine sicherere Online-Umgebung zu schaffen.

Dieser gemeinschaftliche Ansatz kann zu innovativen Lösungen und stärkeren Schutzvorrichtungen für alle im digitalen Raum führen.

***[Bildschirminhalt] KI in einem Kreis mit Symbolen, die es umkreisen.***

Aktualisierung von Gesetzen für neue Herausforderungen: Angesichts neuer Herausforderungen werden Anstrengungen unternommen, um neue Gesetze und Initiativen zu entwickeln, die Personen vor Missbrauch schützen sollen.

Aufklärung der Öffentlichkeit: Es ist für alle wichtig, gut informiert zu sein. Initiativen sind angelaufen, um die Öffentlichkeit in die Lage zu versetzen, echte Inhalte von gefälschten Inhalten zu unterscheiden. Dazu gehört auch die Entwicklung neuer Hilfsmittel und Programme zur Aufklärung der Öffentlichkeit. Diese Strategien zielen darauf ab, die Transparenz zu erhöhen und die Gesellschaft widerstandsfähiger gegenüber Deepfakes zu machen.

Während Deepfakes aufgrund ihres möglichen Missbrauchs zur Verbreitung von Fehlinformationen und Identitätsdiebstahl weiterhin ethische und Sicherheitsbedenken aufwerfen, machen KI-Technologien Fortschritte bei der treffsicheren Erkennung von Deepfakes.

***[Bildschirminhalt] KI in einem Kreis mit echten und Deepfake-Videos, die überprüft werden.***

Dies führt uns zu einem weiteren wichtigen Thema – der Zunahme von und dem Bewusstsein für KI-generierte Inhalte.

Das Urheberrecht ist ein rechtliches Konzept, das Urheber(inne)n und Autor(inn)en von Originalwerken ausschließliche Rechte für deren Nutzung und Verbreitung gewährt, um sicherzustellen, dass sie Anerkennung für und finanziellen Nutzen aus ihren Werken erhalten.

Aber was passiert, wenn der Urheber ein KI-Dienst oder -Werkzeug ist?

Da wir wissen, dass Urheberrechte bei KI-generierten Inhalten ein wichtiges Thema sind, wurden Initiativen wie das „Microsoft Copilot Copyright Commitment“ ins Leben gerufen, um die bestehende Unterstützung für den Schutz des geistigen Eigentums auf kommerzielle Copilot-Dienste auszuweiten.

***[Bildschirminhalt] Das Copilot-Logo.***

Diese Verpflichtung befasst sich mit der möglichen Haftung für Verletzungen des Urheberrechts, die sich aus der Verwendung der Ergebnisse von Microsofts Copilot und Azure OpenAI Service ergeben könnte.

Um das Vertrauen in KI-generierte Inhalte weiter auszubauen, hat Microsoft Inhaltsnachweise (Content Credentials) entwickelt. Diese Funktion verwendet kryptografische Methoden, um allen KI-generierten Bildern in Bing ein unsichtbares digitales Wasserzeichen hinzuzufügen, einschließlich Zeit und Datum der ursprünglichen Erstellung.

***[Bildschirminhalt] Ein Bild mit einer KI-Flagge.***

Auf diese Weise lässt sich feststellen, woher der Inhalt stammt und diejenigen, die Inhalte erstellen und weitergeben, haben bessere Möglichkeiten zu entscheiden, welchen Inhalten sie vertrauen können. Dies ist ein entscheidender Schritt, um die verantwortungsvolle und ethische Nutzung der KI-Technologie zu gewährleisten.

***[Bildschirminhalt] Eine Person verbunden mit Bildern und KI, mit einem Häkchen in einer Gedankenblase in der Mitte.***

Es ist wichtig, informiert zu bleiben. Denken Sie daran, dass nicht alles, was Sie sehen oder hören, unbedingt der Wahrheit entspricht. Wenn es also um KI-generierte Inhalte geht, ist es wichtig, dass Sie Ihre Rechte und die Maßnahmen kennen, die zu deren Schutz vorgesehen sind.