Deep Fakes – Täuschend echt?!
Hintergrundinfos für Lehrpersonen

Begriffserklärung
Deep Fake setzt sich zusammen aus „Deep Learning“ (eine Methode, durch die eine Künstliche Intelligenz lernt) und dem Begriff „Fake“.

Seit wann gibt es Deep Fakes?
Die Manipulation von Medieninhalten ist bekanntlich kein neues Phänomen und hat seine Ursprünge in der politischen Propaganda. Doch im Vergleich zu früher kann heutzutage auf Künstliche Intelligenz und enorme Rechenleistung zurückgegriffen werden, die Deep Fakes nahezu realistisch wirken lassen, was vor allem die Filmbranche sich mehr und mehr zunutze macht. In den letzten Jahren verbreiten sich jedoch immer mehr kostenlose Apps, Webseiten und integrierte Filter auf Social Media, mit denen sich innerhalb von Sekunden ein Deep Fake erzeugen lässt.

Wer kann Deep Fakes erstellen?
Nahezu realistische Deep Fakes benötigen einen leistungsstarken Computer, komplexe Software, Kenntnisse im Umgang mit Künstlicher Intelligenz und maschinellem Lernen sowie Editing-Skills. Ungeübte können auf die oben genannten Methoden zurückgreifen und innerhalb weniger Klicks und Sekunden ein Deep Fake generieren, der sich jedoch relativ einfach als Täuschung enttarnen lässt. Eine bekannte Methode der Manipulation ist der Face Swap, bei der Gesichter ausgetauscht werden. Vor allem im pornografischem Kontext wird die Methode des Deep Fakes dafür verwendet, Gesichter von Schauspieler:innen in pornografische Inhalte einzufügen.

Welche Gefahren gehen von Deep Fakes aus?
Einzelne Individuen können durch das Verbreiten von Deep Fakes erheblich geschädigt werden, wenn von ihnen Video-, Audio oder Bildinhalte erstellt werden, die so nie geschehen sind. Ein weiteres Gefahrenpotenzial von Deep Fakes besteht darin, dass das Gefühl entsteht, keiner Quelle mehr vertrauen zu können oder dass Menschen echte Aufnahmen für eine Manipulation halten, wie zum Beispiel die Behauptung von Trump-Anhänger:innen, das Video, in dem Donald Trump den Wahlsieg seines Kontrahenten Joe Biden anerkennt, sei lediglich ein Deep Fake gewesen. Auch das Verwenden von kostenlosen Apps und Webseiten im privaten Bereich birgt die Gefahr des Missbrauchs der hochgeladenen Daten. Vor einer Verwendung solcher Apps sollte stets geprüft werden, wer die Daten erhebt, welche Rechte an den eigenen Bildern abgetreten werden und wo die Daten gespeichert werden.

Wie erkenne ich Deep Fakes?
Die meisten Deep Fakes lassen sich noch mit bloßem Auge erkennen, da die Technik zwar oftmals gut aber noch lange nicht perfekt ist. Typische Erkennungsmerkmale von Deep Fakes sind eine unnatürliche Mimik, ein leerer Blick, nicht korrekte Schattenwürfe im Gesicht oder Pixelfehler an den Außenkanten des Gesichts. Um die Fehler besser zu erkennen, hilft es, sich die betreffenden Videos im Vollbildmodus anzuschauen. Mittlerweile werden auch KI-Systeme entwickelt und angewandt, die Deep Fakes schneller aufspüren und entlarven sollen. Oft reicht schon ein minimaler Pixelfehler im Video, um den Versuch einer Täuschung zu überführen. Somit wird es Erzeuger:innen von Deep Fakes immer schwerer gemacht, ihre manipulierten Inhalte zu veröffentlichen und zu verbreiten. Grundsätzlich helfen folgende Fragen beim Prüfen auf Echtheit von Deep Fakes:

- Ist das Material auf einer seriösen Informationsquelle aufgetaucht oder befinden sich die Inhalte auf einer eher dubiosen Webseite?
- Wann und wo ist das Video zum ersten Mal aufgetaucht?
- Ist das Video-, Bild-, oder Audiomaterial auf mehreren Webseiten zu finden?
- Stehen die Aussagen und das Verhalten der gezeigten Person im Gegensatz zu dem, was sie üblicherweise sagt oder tut?