Bitte glauben Sie Ihren Augen nicht!

Identitätsklau mit gefälschten Videos im Internet wird mit der rasend schnellen Entwicklung der künstlichen Intelligenz immer leichter. Die Palette von Deep Fake reicht von gutgemeinten PR-Kampagnen bis zu Cybercrime

BERICHT: TESSA SZYSZKOWITZ

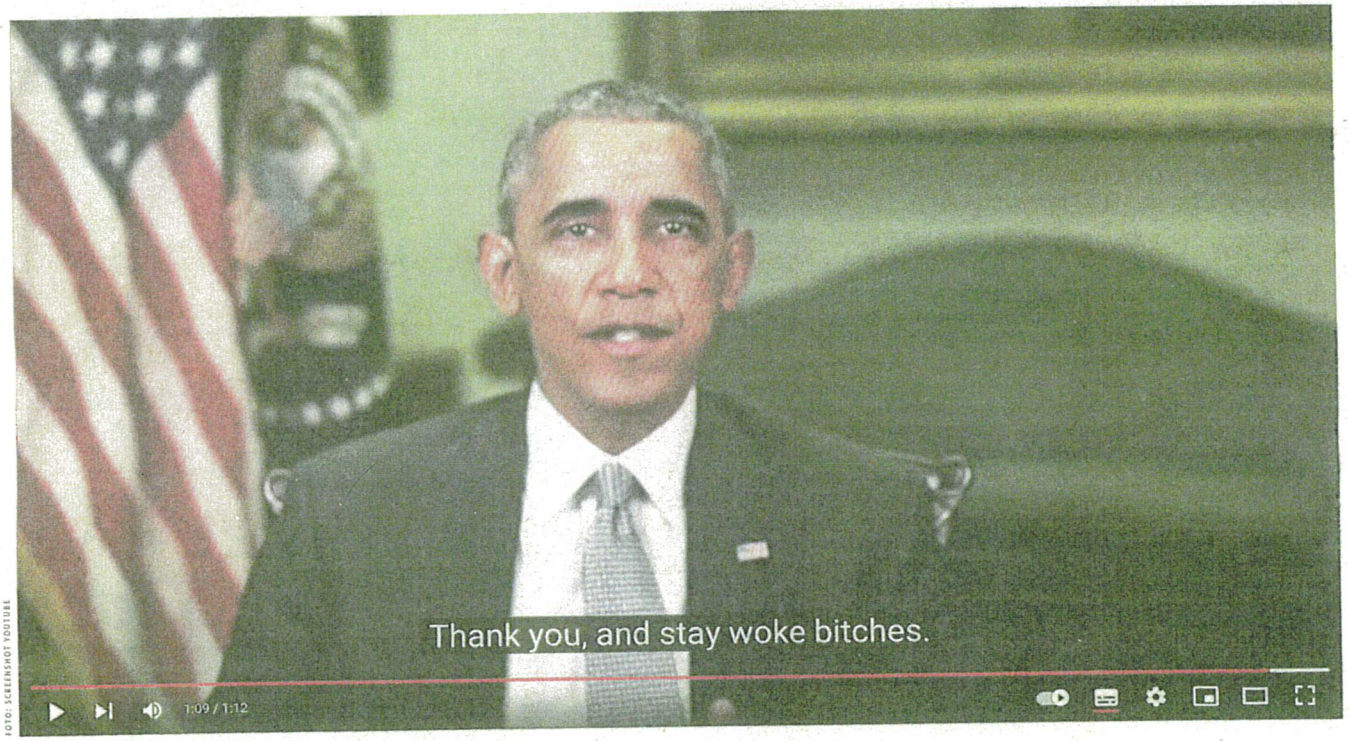

FOTO: SCREENSHOT YOUTUBE

Hier spricht Barack Obama. Oder auch nicht. Ein Deep-Fake-Video als Weckruf aus dem Jahre 2018

Im April 2021 trat Alexei Nawalny aus Protest gegen seine Behandlung im russischen Kerker in den Hungerstreik. Die rechte Hand des russischen Oppositionsführers, Leonid Wolkow, führte derweil den Widerstand gegen Wladimir Putins Regime an. Dazu trat er per Videocall mit europäischen Parlamentariern in Kontakt. Auch der lettische Politiker Rihards Kols sprach damals mit Wolkow.

Angeblich. Denn schnell war klar: Kols hatte mit einem Doppelgänger telefoniert.

Kurze Zeit später meldete sich Wolkow, im Zivilberuf Computer-Ingenieur, auf Facebook zu Wort: „Das bin nicht ich. Aber wie haben die mein Gesicht auf den Zoom-Call bekommen? Welcome to the Deep Fake Age."

Leonid Wolkow sieht die Affäre im Gespräch mit dem *Falter* heute etwas entspannter: „Das war am Ende ja kein Deep Fake, sondern ein Fall von schlechtem Make-up." Die Identitätsfälscher hatten nicht hochkomplizierte Artificial Intelligence eingesetzt, um Wolkows Identität zu klauen. Ein Komiker hatte sich bloß einen Vollbart aufgeklebt und sich einen schlechten Scherz erlaubt. Sein Name und der seines Komplizen sind inzwischen auch im Wiener Rathaus bekannt. Das russische Prankster-Pärchen Vovan und Lexus alias Wladimir Kutsnetsow und Alexei Stoliarow haben vor kurzem den Wiener Bürgermeister Michael Ludwig reingelegt. Die beiden putinistischen Witzbolde machten den Stadtvater glauben, er unterhalte sich mit seinem Kollegen aus Kiew, dem ehemaligen Boxer Witali Klitschko. Und das minutenlang.

Obwohl es sich in keinem Fall um Deep Fakes handelte, wurde sofort vielerorts darüber spekuliert, wie gefährlich diese neuen Technologien in Zeiten des digitalen Kriegs werden könnten. Vor allem in sozialen Medien, in denen oft erst spät auf Fälschungen reagiert wird. Auch Fake-Accounts werden viel zu spät gelöscht. Hinter den Bots sitzen oft nicht Menschen, sondern Maschinen, die teilweise von sinistren politischen Akteuren gesteuert Desinformation streuen. Twitter löscht jeden Tag eine Million dieser

Fortsetzung nächste Seite

Fortsetzung von Seite 21

Konten. Elon Musk hat deshalb gerade seinen Twitter-Deal platzen lassen.

Die Bot-Armeen sind das Sprungbrett für die neuere und kompliziertere digitale Bedrohung durch Deep Fakes. Der Multiplikationsfaktor von Fälschungen ist nicht zu unterschätzen. Vor allem, weil digitale Manipulationen immer leichter zugänglich werden.

Der Begriff Deep Fake entstand ursprünglich als eine Zusammenziehung aus „Deep Learning" und „Fake". Künstliche Intelligenz trifft auf Photoshop. Machine-Learning-Algorithmen – sogenannte neuronale Netzwerke – werden von Wissenschaftlern anhand von echten Videoaufzeichnungen auf verschiedene Aspekte menschlichen Ausdrucks trainiert: Stimmen, Gesichter, Mimik, Gestik. Dann zeichnet das Computerprogramm ein Gesicht digital nach – der englische Fachausdruck lautet „mapping" – und setzt es in einen anderen Film auf eine andere Person auf. Um Schwächen auszugleichen, verwenden die Techniker dann noch ein GAN-Programm (Generative Adversarial Network).

> *Es besteht durchaus eine reale Gefahr, dass man von einem Deep-Fake-Videoanruf getäuscht wird*
>
> CLEMENS HEITZINGER

Der Comedian Jordan Peele schlüpft mittels künstlicher Intelligenz in Barack Obama

An amerikanischen Universitäten wird seit Jahren mit Deep Fake experimentiert. Mit der richtigen Software ist der Unterschied zwischen echt und falsch inzwischen nicht mehr zu erkennen. 2018 sorgte ein Deep-Fake-Video von Barack Obama für Aufsehen. Der ehemalige US-Präsident bezeichnete seinen Nachfolger Donald Trump als Vollidioten. Bloß: Es war ein künstlich geschaffener ehemaliger US-Präsident, der da auf Youtube herumschimpfte. Comedian Jordan Peele hatte in Kooperation mit Buzzfeed Fake Barack seinen Mund und seine Worte geliehen, um vor Fake News und den neuen Technologien zu warnen, die sie möglich machen.

Solche gutwilligen Deep Fakes werden von ihren Erschaffern dazu genutzt, um auf die Errungenschaften von künstlicher Intelligenz hinzuweisen. Wissenschaftler, die auf Artificial Intelligence spezialisiert sind, betonen stets und nicht zu Unrecht die Vorteile der Gesichtserkennungstechnologie und des Machine Learning. Etwa auch Clemens Heitzinger, der an der TU Wien die Forschungsgruppe Maschinelles Lernen leitet: „Dadurch kann die Früherkennung und Behandlung von Krankheiten verbessert und die Zuverlässigkeit von Software und Algorithmen verstärkt werden." Sogar bei der Steuerung von Geräten und Anlagen ließe sich damit Energie sparen.

Auch gesellschaftspolitisch sind Deep Fakes durch ihren Verfremdungseffekt ein interessantes Instrument. In der Filmindustrie werden Deep Fakes nicht nur zum Spaß eingesetzt, wenn etwa statt der Schauspielerin Amy Adams plötzlich Nicholas Cage „I will survive" singt. Filmemacher setzen sie auch zum sogenannten „queering" ein, dem Reframing von Geschlechterrollen. Es entstehen erstaunlich vielfältige Gesichtszüge, wenn zwei Menschen digital vermischt werden – traditionelle Rollenbilder können damit aufgebrochen werden.

Selbstversuch der Autorin: Wie man per App einen Mafiaboss in der Serie „Peaky Blinders" spielen kann

Da die Technologie jedoch bereits publiziert wurde, können viele Akteure Deep Fakes herstellen: „Insofern besteht durchaus eine reale Gefahr, dass man von einem Deep-Fake-Videoanruf getäuscht wird", erklärt Heitzinger. Unter seiner Leitung wurde 2021 das CAIML eröffnet – das Center for Artificial Intelligence and Machine Learning. „Die größten Gefahren entstehen, wenn diese Technologie für kriminelle Zwecke oder für Täuschungen verwendet wird – also etwa Identitätsdiebstahl, Finanzbetrug, automatisierte Desinformationsangriffe, Verleumdung und Falschmeldungen."

96 Prozent aller Deep Fakes finden sich in der Pornoindustrie. Wie Alyssa Muck vom University College London (UCL) in einem Video erklärt: „Diese Videos sind mit hoher Wahrscheinlichkeit nicht mit Zustimmung der jeweiligen Person zustande gekommen. Die Opfer des Identitätsbetrugs haben wenig Handhabe, um den Verbrechern juristisch beizukommen." Deep Fakes werden besonders oft in gefälschten Pornovideos mit Prominenten eingesetzt. Vor allem Schauspielerinnen werden mit kaum als Fälschungen zu erkennenden Filmen unter Druck gesetzt.

Hochproblematisch sind Deep Fakes aber auch im großen, grauen Bereich der Desinformation in den sozialen Medien. Extinction Rebellion produzierte 2020 ein Deep-Fake-Video der damaligen belgischen Premierministerin Sophie Wilmès, in dem sie sich gegen Klimawandel ausspricht. Diese Fälschung sollte Aufmerksamkeit erregen und tat nicht einmal so, als wäre sie echt.

Allein das Wissen aber, dass Deep Fake existiert, untergräbt das bisherige Vertrauen in Bild und Ton. Josef Stalin ließ noch auf Fotografien mühsam die Köpfe jener Mitstreiter wie Leo Trotzki herausretuschieren, die er gerade hatte umbringen lassen.

Heute kann man sich nicht mehr sicher sein, ob der nordkoreanische Diktator Kim Jong-un tatsächlich per Video zu seinem Volk spricht oder ob es sich um eine Computeranimation handelt. Ein Kim, der ganz gegen seine Gewohnheit warnt: „Demokratie ist eine fragile Sache", stellte sich 2020 schnell als Deep Fake der NGO Represent Us heraus, die damit zu höherer Wahlbeteiligung im Westen aufrufen wollte.

„Deep-Fake-Videos können schon in Echtzeit erstellt werden", warnt Clemens Heitzinger. Je besser Kriminelle bei der Erstellung von Deep Fakes werden, umso schneller ziehen jene nach, die genau diese Verbrechen bekämpfen: Verbrechen und Strafe halten sich die Waage. Was Heitzinger auch gleich betont: „Es kommt zu einem Technologiewettlauf zwischen Software zum Erstellen von Deep Fakes und Software zur Erkennung derselben."

Die Gesetzgeber müssen sich beeilen, um mit der Entwicklung Schritt zu halten. So durfte man ja auch schon vor der Verbreitung von Deep Fakes in sozialen Medien jemandem nicht ungestraft die Identität stehlen. Wer etwa alte – oder nicht so alte – Damen und Herren anruft, sich als Angestellter ihrer Bank ausgibt und ihnen Geld aus der Tasche zieht, machte sich auch schon vor dem digitalen Stimmendiebstahl strafbar.

Inzwischen gibt es aber Fälle, wo gefälschte Enkel es per Videoanruf bei Großeltern versuchen – ein perfider Betrug, der noch schwerer zu durchschauen ist. Für diese Art krimineller Aktivität braucht es allerdings komplizierte technische Vorbereitungen. Sehr verbreitet sind Deep-Fake-Crimes deshalb noch nicht.

Für einfache Anwendungen dagegen können sich auch Amateure schon erstaunlich schnell in die wilde Welt der Deep Fakes versetzen. Unzählige Apps bieten inzwischen Witzvideo-Installationen an, in denen man mit dem Hochladen eines Selfies schnell zur Hauptdarstellerin in einer Fernsehserie werden kann. Ihre Autorin verwandelte sich beim Selbstversuch innerhalb weniger Minuten in Tommy Shelby aus der englischen Hitserie „Peaky Blinders".

Stand 2022 sind die meisten Deep Fakes noch unschuldig – und in ein paar Sekunden ist der Spaß vorbei. Mit der rasenden Entwicklung von AI-Technologie und Cybercrime aber steigen die Optionen für bösartige Verwendung minütlich. Desinformation ist besonders perfide, weil sie das Vertrauen in die politischen Institutionen untergräbt. Wenn Joe Biden demnächst auf Twitter verkündet, er habe Donald Trump eingeladen, ihn als Präsident für ein paar Monate zu vertreten, dann erkennen das die meisten hoffentlich als Deep Fake. Aber wer weiß. Unser Tipp: Glauben Sie Ihren Augen nicht.

FOTO: SCREENSHOT YOUTUBE, REFACE, FACE SWAP VIDEO APP