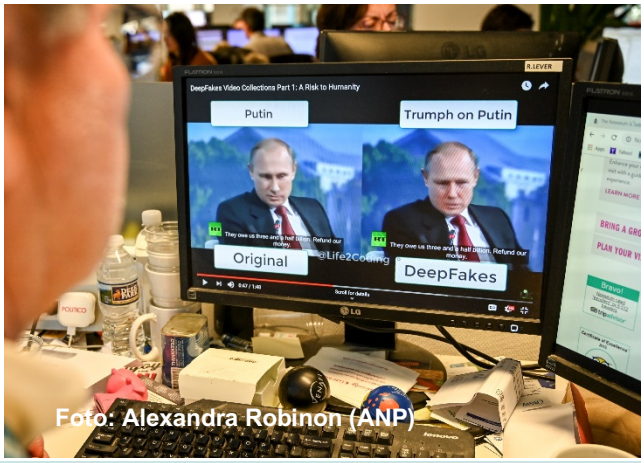
Moeten we bang zijn voor deepfake video's?

Tv-maker Arjen Lubach die in de trailer voor zijn nieuwe tv-programma al pratend verandert in respectievelijk Thierry Baudet, koning Willem-Alexander, Martien Meiland en Yvon Jaspers. Het kan allemaal door de techniek van kunstmatige intelligentie. Dit soort video's worden ook wel *deepfake video's* genoemd en zijn niet of nauwelijks meer van echt te onderscheiden. Zijn ze daarmee alleen maar grappig, of kunnen ze ook een bedreiging zijn als ze bijvoorbeeld als nepnieuws ingezet worden?



Journalist bekijkt deepfake video

Deepfake

Deepfake is een verzamelnaam voor software waarmee je nepvideo's kunt maken die bijna niet van echt te onderscheiden zijn. Met deze software kun je iemand dingen laten zeggen of doen die hij of zij in werkelijkheid nooit gezegd of gedaan heeft. Deepfake kan het in de toekomst steeds moeilijker maken om te zien of een video echt of nep is.

De naam deepfake is een combinatie van de woorden *deep learning* en *fake* (nep). Deep learning is een techniek die valt onder kunstmatige intelligentie. Het zorgt ervoor dat computers nieuwe dingen kunnen leren op basis van grote hoeveelheden getallen, tekst, geluiden of beelden. Deepfake software gebruikt kunstmatige intelligentie om nepvideo's te maken die echt lijken. Dit soort software was vroeger alleen te vinden in dure filmstudio's in Hollywood, maar is nu steeds vaker gratis te downloaden en te gebruiken.

Slimme software

Stel dat iemand een deepfake video van premier Mark Rutte wil maken. In dat geval gaat de software video's waarop Rutte te zien is beeld voor beeld analyseren. Zo leert de software wat de omvang en vorm is van Rutte's gezicht, hoe de verhoudingen van zijn neus en mond zijn en hoe zijn gezicht beweegt als hij praat. Zo ontstaat een datamodel van een pratende premier. Dit model kan vervolgens worden gebruikt in een nepvideo waarin Rutte bijvoorbeeld zou kunnen zeggen dat de Friezen begonnen zijn om de provincie Groningen binnen te vallen. Dat terwijl hij dit nooit echt heeft gezegd.

Een goed voorbeeld van een overtuigende deepfake video werd gemaakt door de Amerikaanse nieuwssite *Buzzfeed* en comedian Jordan Peele. Samen produceerden zij een deepfake video waarin voormalig president van de Verenigde Staten Barack Obama de wereld toespreekt over de gevaren van nepnieuws en dingen die echt lijken, maar het niet zijn.

Nepnieuws

Voorlopig zijn er geen bekende voorbeelden van deepfakes die voor grote verwarring zorgden. De toepassing beperkt zich voorlopig tot experimenten van journalisten, media en universiteiten. De ontwikkeling van deepfake software kan echter snel gaan. De kwaliteit zal steeds beter worden en de kosten om de software te maken steeds lager.

De meest voor de hand liggende toepassing van deepfake ligt in nepnieuws. Nepnieuws draait om het verspreiden van misleidende informatie. Daar kunnen deepfake video's zich goed voor lenen. Misbruik van de technologie kan voor verwarring en onrust zorgen.

Ook zijn er meer onschuldige toepassingen. Zo kan de technologie ingezet worden in de productie van films om (een overleden) acteur een rol in een film te geven. Filmfans gingen al aan de slag met de technologie door acteur Nicolas Cage allemaal rollen te geven in films waar hij nooit in speelde. Dat deepfake ook gebruikt kan worden voor een goed doel, blijkt ook uit een filmpje waarin oud-profvoetballer David Beckham aandacht vraagt voor de ziekte malaria. Dankzij de technologie deelt hij zijn boodschap in wel negen talen.

Risico's

De technologie roept veel vragen op over de gevaren voor de journalistiek en de democratie. Hoe weet je nog wat echt of nep is? Dit kan ervoor zorgen dat mensen de media, politici en de democratie niet meer vertrouwen. Immers, deepfake kan bekende mensen, van acteurs tot wereldleiders, allerlei uitspraken in de mond leggen die ze nooit hebben gedaan. Beeldvorming, gebeurtenissen en gesprekken kunnen worden beïnvloed en tot grote verwarring over de waarheid leiden. 'Zien is geloven' is dan niet meer vanzelfsprekend. Nieuwsmedia, zoals het NOS-journaal of NU.nl, maken in hun verslaggeving veel gebruik van video's. Als live-beelden of reportages overtuigend kunnen worden bewerkt met deepfake, kan de betrouwbaarheid van de journalistiek daaronder lijden. Deepfakes, en nepnieuws, zorgen ervoor dat je mensen kunt overtuigen van iets dat nooit heeft plaatsgevonden of iemand nooit heeft gezegd. In het ergste geval zorgt het ervoor dat alles nep zou kunnen zijn. Media, politiek en democratie zijn in Nederland gebaseerd op hun geloofwaardigheid. Daarom is het belangrijk om te weten hoe je deepfake (en nepnieuws) kunt herkennen.

Verbod?

In Nederland is er nog geen officiële wetgeving over de verantwoordelijkheid of aansprakelijkheid bij het maken of delen van deepfakes. Sinds eind 2018 is er wel een kabinetsplan om nepnieuws te bestrijden. De overheid gaat de verspreiding van nepnieuws in Nederland onderzoeken en wil de weerbaarheid van burgers vergroten met een bewustwordingscampagne. De technologie die wordt gebruikt voor het maken van deepfake video's, kan ook helpen bij de bestrijding ervan. Door het herkennen van patronen kunnen computers signalen zien die verklappen dat een video nep is. Voorbeelden van dat soort signalen zijn ogen die niet knipperen, het schaduwpatroon van het gezicht en de vervaging van beeldkwaliteit bij armgebaren. In Nederland werkt Theo Gevers, computerwetenschapper aan de Universiteit van Amsterdam, aan software die gebruikers erop moet wijzen wanneer een video een deepfake is. Ook platformen als Facebook en Google werken aan oplossingen voor het herkennen van deepfakes.

Bron: www.mediawijsheid.nl/deep-fake/ (geraadpleegd op 23 januari 2020)