Gezichtsherkenning: de technologie waar zelfs big tech van afbleef

Dominique Deckmyn

Google en zelfs Facebook wilden zich er niet aan wagen. Daarom kon een obscuur bedrijfje met een bedenkelijke voorgeschiedenis, Clearview AI, de markt van de gezichtsherkenning naar zich toetrekken – en daarmee het einde inluiden van privacy zoals we die ooit kenden.

Anoniem zijn bestaat niet meer. Op straat, tijdens een feestje, een sportwedstrijd of een betoging: overal waar u uw gezicht laat zien, kunt u ogenblikkelijk worden geïdentificeerd. En kunnen meteen ook alle andere beelden van u die op het internet te vinden zijn, worden opgespoord – zelfs als u ergens op de achtergrond stond op een foto die iemand anders op Instagram postte. De technologie bestaat al jaren.

In het boek Je gezicht is nu van ons beschrijft The New York Times-journaliste Kashmir Hill de merkwaardige opmars van Clearview AI, het bedrijfje dat gezichtsherkenningstechnologie in handen stopte van politiediensten en privébedrijven.

Het was Hill die in januari 2020 Clearview AI outte in haar krant. Politie en privébedrijven in de Verenigde Staten en daarbuiten waren de software toen al enthousiast aan het gebruiken, maar de buitenwereld had daar geen idee van. Het artikel veroorzaakte een internationale storm van verontwaardiging en een roep om wetgeving die mensen zou beschermen.

Andere journalisten wierpen zich op het onderwerp. Buzzfeed publiceerde begin 2020 een lijst van organisaties die de app van Clearview AI hadden uitgeprobeerd – onder meer de Belgische politie, die dat fel ontkende, maar uiteindelijk toch moest bekennen. In België bestaat geen wettelijke basis voor het gebruik van gezichtsherkenning door de politie, dat was dus illegaal.

Bouwstenen voor het rapen

Achter Clearview AI bleek een toen 31-jarige Vietnamees-Australische programmeur te zitten: Hoan Ton-That. Maar hoe slaagde een bedrijfje zonder kantoren, omzeggens zonder personeel en met minimale financiële steun erin om in het geheim zo'n grensverleggende technologie te ontwikkelen?

Het antwoord is simpel: de bouwstenen lagen voor het oprapen. Ton-That las wetenschappelijke artikels op het open access-archief arxiv.org en downloadde gratis programmacode van de website Github, onder meer de OpenFace-software ontwikkeld door onderzoekers aan de Carnegie Mellon Universiteit.

Van AI had hij geen kaas gegeten, voordien had hij vooral Facebook-quizjes en iPhone-games geschreven, maar in enkele maanden tijd puzzelde Ton-That een goed werkend systeem voor gezichtsherkenning in elkaar. Zo goed als in zijn eentje, al kreeg hij wel wat hulp van een (naar verluidt briljante) Chinese wiskundige, Terence Liu.

Waarom hadden anderen hem dat niet voorgedaan? De reuzen van Silicon Valley experimenteerden met gezichtsherkenning, maar durfden niet door te duwen. Google lanceerde in 2008 in zijn toenmalige online fotoalbum Picasa de mogelijkheid om de gezichten van je vrienden automatisch te herkennen op je foto's. Facebook introduceerde een gelijkaardige functie in 2010: als je een foto uploadde, stelde Facebook voor om je vrienden erop te taggen.

Google en Facebook vergeleken de gezichten op een foto met een beperkt lijstje personen. Maar zelfs dat vonden mensen al behoorlijk griezelig. Al snel besliste Facebook om de technologie in Europa van de markt te halen.

Google had ooit ook een versie van die technologie klaar die een veel bredere groep mensen kon herkennen – in maart 2011 kreeg een journalist daar een demonstratie van te zien. Maar toen er een artikel over verscheen, noemde Google het een 'verzinsel van de reporter'. Toenmalig Google-baas Eric Schmidt gaf later toe hoe de vork aan de steel zat. 'We hebben die technologie ontwikkeld en toen beslist ze achter te houden.' Hij voegde eraan toe dat het, bij zijn weten, de enige technologie was die zijn bedrijf ontwikkelde maar daarna besliste om die niet uit te brengen.

Technologie die toeliet om elke persoon te identificeren op basis van zijn gezicht werd beschouwd als té verregaand. Daarover bestond een soort zwijgende consensus in de VS, schrijft Hill. Maar die consensus werd nooit omgezet in een wet, toch niet op federaal niveau.

Een handvol staten voerde wel eigen wetten in. De meest verregaande is die in Illinois, waar het illegaal is om biometrische informatie zoals vingerafdrukken en irisscans van iemand te vergaren of bewaren zonder toestemming. Een systeem van gezichtsherkenning wordt beschouwd als biometrische informatie.

Witte nationalisten

Het algoritme voor gezichtsherkenning van Clearview AI is niet zo bijzonder. Maar wat het bedrijf vanaf 2019 zo aantrekkelijk maakte voor politiediensten, was het aantal gezichten in zijn database. Ton-That was begonnen met twee miljoen foto's die hij van Tinder en Venmo stroopte, maar al snel zette hij schimmige hulpjes in om van overal op het internet foto's te vergaren. Daarbij moest de beveiliging van websites als Facebook worden omzeild, maar erg moeilijk bleek dat – tot de verbazing van Ton-That zelf – niet te zijn. Al snel had hij drie miljard foto's. De FBI had ook een systeem van gezichtsherkenning – met een database van 36 miljoen foto's, bijna honderd keer minder.

Clearview AI had een onfrisse voorgeschiedenis die Ton-That probeerde weg te moffelen. Het bedrijf en de app heetten aanvankelijk Smartcheckr. Dat was een app waarmee je, op basis van een naam, snel iemands achtergrond kon uitpluizen om diens politieke overtuiging te achterhalen. Gezichtsherkenning kwam er pas later bij.

Ton-That had Smartcheckr bedacht samen met zijn toenmalige kameraad Chuck Johnson, een van X (Twitter) gebannen uiterst rechtse provocateur. Hun geldschieter was Peter Thiel, medeoprichter van Paypal en een belangrijk financier van de presidentscampagne van Donald Trump.

De naamsverandering naar Clearview AI, in 2018, was nodig omdat de naam 'Smartcheckr' op Google te

veel zoekresultaten opleverde die te maken hadden met Johnson, de Amerikaanse alt-right en witte nationalisten. Ton-That zegt dat hij sindsdien veranderd is van politieke overtuiging.

Bril die gezichten opzoekt

De verontwaardiging die de berichtgeving over Clearview AI in 2020 veroorzaakte, is intussen gaan liggen. Zeker in de VS. Het boek van Hill suggereert dat de technologie er stilaan genormaliseerd geraakt. Iemand ‘clearviewen’ is bij de Amerikaanse politie een haast even gewone uitdrukking als ‘googelen’. Wat betreft de vergaring van foto’s, is Clearview allesbehalve gas terug aan het nemen: het bedrijf zit intussen aan dertig miljard beelden.

Hoewel er verschillende processen lopen die kunnen uitlopen op gigantische boetes, onder meer in Illinois, heeft Clearview AI zijn imago opgepoetst. Heel wat tegenstanders van gezichtsherkenning weifelden toen die werd ingezet om uiterst rechtse bestormers van het Capitool te identificeren. De burgerrechtenbeweging ACLU, die Clearview had aangeklaagd, bereikte in mei 2022 een schikking met het bedrijf.

Hill heeft, merkwaardig genoeg, het vertrouwen van Hoan Ton-That weten te winnen. Op het einde van het boek demonstreert hij haar een prototype: een bril die de gezichten kan opzoeken van iedereen die je ziet. Zo’n apparaat is al lang de nachtmerrie van heel wat privacy-activisten. Ton-That heeft er een gemaakt, alweer gebruikmakend van technologie die al vrij te vinden is: een slimme bril met ingebouwde camera en beeldscherm van het merk Vuzix.

Vermiste kinderen

In Europa gaat het de andere kant op. Afgelopen zomer keurde het Europees Parlement de AI Act goed, een verordening die strenge regels en grenzen oplegt aan het gebruik van artificiële intelligentie.

Het Parlement amendeerde de tekst om gezichtsherkenning in de openbare ruimte nagenoeg volledig te bannen, omdat de technologie een ‘onacceptabel risico’ meebrengt. In realtime mensen herkennen op videobeelden mag niet. Dat kan alleen achteraf op opgenomen beelden bij zware misdaden en na een gerechtelijk bevel. Die tekst maakt het gebruik van Clearview AI in Europa onwettig, zegt criminologe Rosamunde Van Brakel (VUB), die zich specialiseert in surveillance en AI.

Maar de tekst van de AI Act is nog niet definitief. De komende maanden bestaat de kans dat sommige lidstaten toch proberen het gebruik van gezichtsherkenning door de politie opnieuw toe te laten. Volgens het kabinet van de Belgische minister van Justitie Vincent Van Quickenborne (Open VLD) pleit België voor een principieel verbod met ‘uitzonderingen voor veiligheidsdoeleinden die strikt omschreven zijn, proportioneel (alleen voor ernstige feiten zoals terrorisme of kinderontvoering) en met rechterlijke controle a priori en a posteriori’. Wat dus minder streng is dan de huidige tekst.

Zelfs als de technologie verboden wordt in Europa, valt de geest nog moeilijk in te fles te krijgen. Haast iedereen kan het kunstje van Clearview AI overdoen – al zijn bedrijven als Meta (Facebook) nu alerter dan vroeger voor organisaties die proberen miljoenen foto’s van hun websites te vergaren. De van oorsprong Poolse website Pimeyes doet bijvoorbeeld al jaren ongeveer hetzelfde als Clearview, maar is toegankelijk

voor iedereen die betaalt.

Lees ook