KU LEUVEN CiTiP imec
CENTRE FOR IT & IP LAW

Kenniscentrum Data & Maatschappij

Gelaatsherkenning in publieke ruimtes

Wim De Mulder[1]

Technische Universiteit Eindhoven, Faculteit Wiskunde en Informatica

Hoe zou u reageren op het nieuws dat uw gezicht werd gescand met geautomatiseerde technologie tijdens een gezellig zondags evenement, waarbij men de bedoeling had om gezochte criminelen te identificeren? Het overkwam de 100 000 bezoekers van de Super Bowl in Florida in 2001. Velen van hen waren in elk geval misnoegd toen ze dit achteraf vernamen, met als gevolg dat deze Super Bowl al snel de bijnaam "Snooper Bowl" kreeg ("snooper" betekent zoveel als "bemoeial"). Een recentere toepassing schept evenmin een rooskleurig beeld van geautomatiseerde gezichtsherkenning: de Metropolitan Police in Londen gebruikte tussen 2016 en 2018 gelijkaardige technologie om het gelaat van voorbijgangers te detecteren en hen vervolgens computergestuurd op te sporen in een databank. Er werden 46 overeenkomsten gevonden, maar slechts acht bleken correct te zijn. Naast de gebrekkige nauwkeurigheid, wezen critici op het feit dat het gebruik van de technologie wellicht moeilijk te verzoenen is met de wetgeving in Engeland en met de mensenrechten. In Zuid-Wales dacht een rechter er in elk geval helemaal anders over: hij oordeelde dat het volstrekt legaal is dat de politie zulke technologie aanwendt, en dat er geen sprake is van schendingen van privacy of mensenrechten.

Het mag dan ook niet verbazen dat geautomatiseerde gelaatsherkenning momenteel een 'hot topic' is, met vurige voorstanders en al even overtuigde tegenstanders. Omdat iedereen zich wel iets kan voorstellen bij computergestuurde gelaatsherkenning, behoort het tot de thema's waar elkeen wel een mening over heeft, zij het dat de ene opinie al meer gefundeerd is dan de andere.

1. Hoe werkt automatische gelaatsherkenning?

Technologie voor gelaatsherkenning kan mensen herkennen uit bewegende (live of opgenomen) beelden of uit foto's. Dit gebeurt door aan de hand van bepaalde kenmerken van het gezicht, zoals de afstand tussen de ogen en de breedte van de neus, na te gaan of dit gelaat aanwezig is in een databank met afbeeldingen van gezichten. Die afbeeldingen in de databank worden intern gerepresenteerd als een verzameling numerieke gegevens, zodat een computeralgoritme snel

[1] De auteur schreef dit werk in eigen naam met de bedoeling om bij te dragen aan het debat rond gelaatsherkenning in publieke ruimtes. Het Kenniscentrum Data & Maatschappij probeert dit debat met dergelijke papers eveneens vorm te geven.

kan nagaan of er een overeenkomst is tussen het bewuste gezicht en een van de gezichten in de databank. Het algoritme moet namelijk niet veel meer doen dan die numerieke gegevens met elkaar vergelijken. Het gebruik van artificiële intelligentie (AI) is cruciaal voor deze toepassing, want het is deze techniek die, op basis van een grote verzameling van gezichtsafbeeldingen, de numerieke gegevens (zoals dus de afstand tussen de ogen) kan extraheren die aan een gezicht zijn uniciteit geven. De databank met gezichtsafbeeldingen bevat meestal niet enkel de afbeeldingen zelf, maar ook bijhorende gegevens zoals naam en woonplaats, waardoor bij een overeenkomst met een afbeelding uit de databank de geviseerde persoon meteen ook volledig geïdentificeerd is.

2. Waarvoor kan de technologie gebruikt worden?

Het nut van automatische gezichtsherkenning is schier eindeloos. In de eerste plaats zal men natuurlijk denken aan het gebruik van deze technologie om criminelen op te sporen. Het opsporen kan echter ook betrekking hebben op vermiste personen. In New Delhi had de politie maar liefst 3000 vermiste kinderen teruggevonden binnen de vier dagen nadat een nieuw systeem voor automatische gezichtsherkenning was gelanceerd. AI kan ook het comfort van ons allen verhogen. Bedenk maar even dat je geen instapkaart voor je vlucht of geen treinticket meer nodig hebt, omdat software voor gezichtsherkenning automatisch detecteert of jij effectief een van de personen bent die de betreffende vlucht of treinrit heeft geboekt en betaald. Een ander nobel doel is het verhogen van de levensvreugde van bepaalde groepen mensen. We weten allemaal dat het een goed gevoel geeft wanneer iemand naar ons glimlacht. Blinde personen hebben natuurlijk deze ervaring niet. Men kan hen echter software ter beschikking stellen die in staat is om een glimlach te detecteren op het gezicht van een persoon in de buurt, waarna een bieptoon wordt gegenereerd om dit prettige nieuws te melden. Is dit science fiction? Absoluut niet, de software wordt momenteel gebruikt in het Verenigd Koninkrijk, Ierland en Duitsland.

3. De risico's van automatische gelaatsherkenning

Een van de vaak aangehaalde risico's van het gebruik van automatische gezichtsherkenning is dat de databank foutieve persoonlijke informatie kan bevatten, of dat het computeralgoritme dat een camerabeeld linkt aan een databank een foutieve overeenkomst kan vaststellen, met als mogelijk gevolg dat een onschuldig individu wordt geclassificeerd als zijnde gevaarlijk. Dit kan intimidatie door de politie tot gevolg hebben. Het voordeel van technieken die AI implementeren is echter dat het mogelijk is om hun accuraatheid te bepalen. Er kan namelijk berekend worden in hoeveel procent van de gevallen er een correcte overeenkomst wordt gedetecteerd tussen een foto of camerabeeld van een persoon enerzijds en een afbeelding in een databank anderzijds. Het risico op foutieve identificatie kan daardoor tot een aanvaardbaar niveau herleid worden door enkel deze systemen toe te laten die deze tolerantiedrempel halen. Fouten helemaal uitsluiten is echter onmogelijk, maar het publiek heeft de neiging kleine ongemakken of een beperkt aantal fouten te tolereren. Zo wordt gemakkelijk aanvaard dat men een fouillering moet ondergaan op de luchthaven, ook al heeft men geen verboden producten bij zich.

Een ander risico schuilt in de onveranderlijkheid van een gezichtsscan. Als een databank met afbeeldingen van gezichten wordt gehackt, kan dit een blijvend risico op misbruik van deze gegevens tot gevolg hebben. Wordt daarentegen een databank met wachtwoorden gehackt, dan kunnen de getroffen gebruikers eenvoudigweg een nieuw wachtwoord instellen.

4. Ethische kwesties

Een van de ethische kwesties omtrent het gebruik van geautomatiseerde software om gezichten te herkennen, heeft te maken met het unieke van het gezicht. Mensen zouden deze unieke kenmerken associëren met een eigen identiteit. Deze identiteit wordt echter gereduceerd tot een onpersoonlijke verzameling numerieke gegevens wanneer het gezicht als een informatiestructuur wordt opgeslagen in een computersysteem. Dit kan als een ontmenselijking opgevat worden.

Er worden ook bedenkingen geuit omtrent het privacy-aspect van automatische gezichtsherkenning. De technologie zou een hoog "Big Brother" gehalte hebben, omdat automatische gezichtsherkenning zou neerkomen op het onderwerpen van het publiek aan een digitale versie van de welgekende "lineup". De "lineup" is onder andere in Amerika populair en bestaat er in dat een ooggetuige een crimineel tracht aan te wijzen uit een aantal personen of uit foto's van deze personen. Met de invoering van AI technologie zou "Big Brother" niet op de deur kloppen, maar zichzelf reeds binnen gelaten hebben en zich daarbij gedragen alsof hij thuis is.

Stellen dat automatische gezichtsherkenning neerkomt op "Big Brother"-praktijken is misschien nogal sterk uitgedrukt. Een genuanceerder standpunt is dat van de filosoof Nissenbaum. Zij argumenteert dat zelfs in publieke ruimtes mensen bepaalde redelijke privacy-verwachtingen hebben. Dit zou blijken uit empirisch onderzoek dat aantoont dat mensen misnoegd zijn wanneer hen ter ore komt dat er persoonlijke informatie over hen werd verzameld, ook al bevonden ze zich daarbij in een publieke ruimte. Wanneer het gaat om de privacy van een publieke figuur, moet er volgens rechter Zupančič van het Europees Hof voor de Rechten van de Mens een afweging gemaakt worden tussen het recht van het publiek om op de hoogte te zijn van wat die persoon doet in zijn of haar leven, en het recht van die publieke figuur om zichzelf af te schermen van al te indringerig gedrag. Men zou deze afweging kunnen combineren met de opinie van Nissenbaum om de volgende stelling te verdedigen: het inzetten van software voor gelaatsherkenning in publieke ruimtes kan maar toegelaten worden indien het een belang dient dat het recht op privacy van een individu overstijgt.

Anderzijds zijn er voorstanders van automatische gezichtsherkenning die argumenteren dat privacy helemaal niet van tel is. Voor professor Chemerinsky bijvoorbeeld kan gelaatsherkenning in publieke ruimtes nooit een inbreuk op de privacy zijn, omdat in publieke ruimtes mensen sowieso niet redelijkerwijze kunnen verwachten over privacy te beschikken. Zeker met de opkomst van de smartphone en de social media is het schering en inslag dat mensen op een foto terechtkomen, vaak zelfs zonder dat dit de bedoeling was van de fototrekkende persoon. In de

VS heeft het Hooggerechtshof ('Supreme Court') een gelijkaardige, zij het een iets meer voorzichtige, opvatting. De rechters merken op dat een individu niet kan verwachten dat zijn of haar gezichtskenmerken een mysterie voor de wereld blijven, aangezien deze constant worden blootgesteld aan het publiek. Interessant is dat het onderscheid wordt gemaakt met de inhoud van een specifieke conversatie tussen personen: dit valt te allen tijde wél onder de redelijke privacy-verwachtingen.

Voorstanders werpen ook op dat automatische gelaatsherkenning niet méér zou zijn dan het automatiseren van een procedure die nooit opgevat werd als een inbreuk op de privacy. Want wat maakt het uit of een gezicht dat via een camera is opgenomen, door een politie-agent dan wel door automatische software wordt gelinkt aan gezichtsafbeeldingen in een databank? Meer zelfs, een computergestuurd systeem kan veel sneller deze koppeling tussen een camerabeeld en een databank maken dan om het even welk menselijk team. In China heeft men onlangs een crimineel gedetecteerd tijdens een popconcert met 60 000 bezoekers, louter dankzij het gebruik van automatische gezichtsherkenning-technieken. Hoeveel mankracht zou er niet nodig zijn om 60 000 camerabeelden manueel te vergelijken met duizenden gezichtsafbeeldingen in een databank?

5. Europese aanbevelingen voor het gebruik van AI

Op Europees niveau is er heel wat aan het bewegen in deze complexe problematiek.

De Europese Commissie heeft een "High-Level Expert Group on AI" in het leven geroepen, die ethische richtlijnen voor een betrouwbaar gebruik van AI heeft ontwikkeld. De zeven basisvereisten die daarbij werden geïntroduceerd moeten ervoor zorgen dat artificiële intelligentiesystemen rechtmatig zijn, ethisch verantwoord zijn, en een robuust karakter hebben vanuit een technisch en sociaal perspectief. Speciale aandacht gaat uit naar het gebruik van AI voor het identificeren en volgen van individuen, waartoe software voor automatische gezichtsherkenning behoort. De experts waarschuwen dat automatische identificatie een onvoorziene impact kan hebben op vele psychologische en socioculturele niveaus. Er moet daarom duidelijk omschreven worden op welke wijze en onder welke voorwaarden AI mag gebruikt worden voor automatische identificatie, en het is belangrijk om daarbij een onderscheid te maken tussen verschillende soorten situaties. Het identificeren en het volgen van individuen bijvoorbeeld zijn twee verschillende doelen, die elk een andere benadering vergen, net zoals dit het geval is voor gerichte observatie versus massa-observatie, aldus de expertgroep. Ook moet er rekening mee worden gehouden dat voor kwetsbare personen een hoger beschermingsniveau tegen eventuele nadelige gevolgen gerechtvaardigd kan zijn. Er kan daarbij gedacht worden aan mensen met een andere huidskleur, gehandicapte personen, ouderen en kinderen.

De Raad van Europa heeft op zijn beurt tien aanbevelingen gedaan die er voor moeten zorgen dat het inzetten van AI in overeenstemming is met de mensenrechten. Opnieuw wordt daarbij onder andere gewezen op de bijzondere aandacht die nodig is voor kwetsbare groepen. Om de mensenrechten van deze groepen te waarborgen, is het van belang hen te consulteren en hen

actief te laten participeren in alle fasen van de ontwikkeling van een AI product dat een impact op hun (mensen)rechten kan hebben.

Het Bureau van de Europese Unie voor de grondrechten heeft recent een uitgebreide analyse gemaakt van de implicaties van technologie voor gezichtsherkenning op de grondrechten. Ook zij komen onder andere tot de vaststelling dat het recht op non-discriminatie, en de rechten van ouderen en kinderen negatief beïnvloed kunnen worden door het gebruik van deze nieuwe technologie in publieke ruimtes.

6. Juridische hangijzers

De GDPR regels bevatten reeds enige aanwijzingen over de omstandigheden die het gebruik van automatische gezichtsherkenningstechnieken rechtvaardigen. Zo bepaalt de GDPR wetgeving onder andere dat het gebruik van biometrische data om een persoon te identificeren in het algemeen verboden is, hoewel er in maar liefst tien uitzonderingen is voorzien (bijvoorbeeld wanneer de betrokken persoon zijn expliciete toestemming geeft). Vele regels zijn echter erg algemeen, en bovendien spreekt de GDPR regelgeving zich niet uit omtrent het gebruik van biometrische data in de context van nationale veiligheid.

Een concreter juridisch kader om het gebruik van AI software voor automatische gelaatsherkenning te regelen, is dan ook onontbeerlijk. Dit bleek al naar aanleiding van het experiment van de federale politie, die software gebruikte om personen te identificeren op de luchthaven van Zaventem. Het Controleorgaan op de Politionele Informatie floot de federale politie al gauw terug: “momenteel ontbreekt een wettelijk kader dat voorziet in de mogelijkheid om camera’s met gezichtsherkenning in te zetten”.

Bij het ontwikkelen van een juridisch kader, zullen heel wat vragen in ogenschouw moeten genomen worden. Men zal onder andere grondig moeten nadenken over de doeleinden waarvoor automatische gelaatsherkenning in publieke ruimtes precies gebruikt mag worden. Zal het enkel gebruikt worden om criminelen op te sporen? En wat verstaat men dan precies wel onder “crimineel”? Wat met de vele andere nuttige doeleinden, zoals het opsporen van vermiste personen?

Men zal er ook voor moeten waken om software grondig te evalueren in termen van nauwkeurigheid alvorens het in de praktijk te gebruiken. In de VS heeft men dit alvast goed begrepen: in Californië is onlangs een verbod ingevoerd op biometrische observatietechnologie in camera’s die op het lichaam worden gedragen, alsook op het registreren van beeldmateriaal met behulp van camera’s op het lichaam om die dan vervolgens te verwerken met technologie voor gezichtsherkenning. Opvallend genoeg zijn deze regels ingevoerd hoewel zulke technologie nog niet eens werd gebruikt in camera’s die op het lichaam bevestigd worden. De reden is hoofdzakelijk dat Axon, die deze camera’s produceert voor de politie in Californië, ruiterlijk toegeeft dat het nog niet zulke technologie zal installeren wegens “nog niet nauwkeurig genoeg”. Foutieve identificaties blijken zich vooral voor te doen bij vrouwen en mensen met een andere

huidskleur. Dit laatste aspect verklaart meteen de hoger vermelde bezorgdheid vanuit de Europese Unie naar de impact van AI op kwetsbare groepen.

Omgekeerd bestaat echter evenzeer het gevaar dat bepaalde voordelen van AI over het hoofd gezien worden. Bij het ontwikkelen van een juridisch kader zal men even goed oog moeten hebben voor de bijkomende nuttige informatie die AI systemen kunnen genereren, naast het loutere identificeren van bepaalde individuen. Een voorbeeld kan dit verduidelijken. Stel dat een vandaal geregistreerd wordt door een camera met automatische gezichtsherkenning, en vervolgens gelinkt wordt aan persoon X in een databank. Indien het camerabeeld enigszins wazig was, zal de overeenkomst wellicht niet met zekerheid vastgesteld worden. Computeralgoritmes kunnen echter de kans berekenen dat de persoon op het camerabeeld inderdaad persoon X is, bijvoorbeeld “de kans dat de persoon op het camerabeeld meneer X is, is 98%”. In ons strafrecht geldt het beginsel van vrije bewijswaardering, wat betekent dat de rechter zelf oordeelt hoe overtuigend een bepaald bewijselement is. Maar als software heel nauwkeurig kan aangeven in welke mate een bewijsgegeven overtuigend is, moet dit dan niet de plaats innemen van de veel subjectievere beoordeling door de rechter?