Dicht op de huid

Gezichts- en emotieherkenning in Nederland

Annelli Janssen, Linda Kool en Jelte Timmer

Rathenau Instituut

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over wetenschap en technologie. Daartoe doet het instituut onderzoek naar de organisatie en ontwikkeling van het wetenschapssysteem, publiceert het over maatschappelijke effecten van nieuwe technologieën, en organiseert het debatten over vraagstukken en dilemma's op het gebied van wetenschap en technologie.

Dicht op de huid

Gezichts- en emotieherkenning in Nederland

Rathenau Instituut
Anna van Saksenlaan 51

Postadres:
Postbus 95366
2509 CJ Den Haag

Telefoon: 070-342 15 42
E-mail: info@rathenau.nl
Website: www.rathenau.nl

Uitgever: Rathenau Instituut
Redactie: Boland Tekst
Ingekorte interviewverslagen: ChristinevoorTaal
Opmaak: Boven de Bank, Zeist
Beeld: Bram Belloni /Jacob & Jacobus, Hollandse Hoogte/Corbis Images

ISBN/EAN: 978-90-77364-67-3

Deze publicatie kan als volgt worden aangehaald/ Preferred citation:
Janssen A., Kool, L. & Timmer, J., *Dicht op de huid - Gezichts- en emotie-herkenning in Nederland*. Den Haag, Rathenau Instituut 2015

Dicht op de huid

Gezichts- en emotieherkenning in Nederland

Annelli Janssen, Linda Kool & Jelte Timmer

Bestuur Rathenau Instituut

mw. G.A. Verbeet (voorzitter)
prof. dr. E.H.L. Aarts
prof. dr. ir. W.E. Bijker
prof. dr. R. Cools
dr. H.J.M. Dröge
drs. E.J.F.B. van Huis
prof. dr. ir. H.W. Lintsen
prof. mr. J.E.J. Prins
prof. dr. M.C. van der Wende
dr. ir. M.M.C.G. Peters (secretaris)

Voorwoord

De technologie die het mogelijk maakt om gezichten automatisch te herkennen is in de afgelopen jaren sterk verbeterd. Met behulp van deze techniek kun je personen op afstand identificeren. In de praktijk wordt dit al op allerlei manieren toegepast, bijvoorbeeld bij de toegangspoortjes van het stadion van ADO Den Haag. Nog verfijnder is de techniek voor emotieherkenning, die het mogelijk maakt om gezichtsuitdrukkingen automatisch af te lezen en te interpreteren.

De opkomst en snelle verbreiding van gezichts- en emotieherkenning is een typische uiting van het thema 'Intieme technologie', dat het Rathenau Instituut in de afgelopen jaren heeft uitgediept. Het gaat om technologieën die privacy-gevoelige informatie aan anderen bloot kunnen leggen, en niet altijd met onze voorafgaande kennis of toestemming. Het Rathenau Instituut stelt bij dit soort ontwikkelingen altijd de vraag naar de maatschappelijke betekenis ervan. Voor welke doelen zouden we gezichts- en emotieherkenning in de toekomst willen inzetten? En voor welke doelen juist niet?

In dit rapport schetst het Rathenau Instituut op basis van literatuurstudie en interviews met experts een beeld van de huidige toepassingen van gezichts- en emotieherkenning in Nederland. We gaan eerst in op de technische stand van zaken. Daarna laten we zien welke kansen deze techniek biedt op gebied van publieke veiligheid en van persoonlijke dienstverlening. Ook gaan we in op de mogelijke implicaties voor privacy, gelijke behandeling van bevolkingsgroepen en sociale omgangsvormen. Vervolgens doen we verslag van een rondetafelbij-eenkomst met experts en belanghebbenden. De aanwezigen onderschreven onze conclusie dat de technologische ontwikkelingen bijzonder snel gaan en dat het om een urgent onderwerp gaat. Databases worden groter en worden ook steeds vaker met andere databases verbonden, waardoor informatie uit voor-heen gescheiden domeinen steeds vaker gekoppeld kan worden. De technolo-gie wordt snel beter, en kan daardoor in steeds meer situaties ingezet worden.

Als burger en consument sta je niet altijd stil bij de maatschappelijke implicaties van deze technologische ontwikkelingen. Ook voor beleidsmakers en politici zijn die niet makkelijk te overzien. Met deze verkennende studie willen wij de discussie aanjagen over de toepassing van gezichts- en emotieherkenningstech-nologie. De studie vormt voor het Rathenau Instituut voldoende aanleiding voor nader onderzoek en dient als aandachtspunt voor beleidsmakers en politici. In het komende werkprogramma 2015-2016 zal het Rathenau Instituut deze impact verder in kaart brengen en onderzoeken hoe een maatschappelijk verantwoorde ontwikkeling van deze technologie mogelijk gemaakt kan worden.

Dr. Ir. Melanie Peters
Directeur Rathenau Instituut

1 Inhoudsopgave

1 Inleiding

De ontwikkeling van automatische gezichts- en emotieherkenning is in volle gang. Een foto van een voorbijganger kunnen we koppelen aan zijn Facebook-profiel (Acquisti & Gross 2009) en computers worden steeds beter in het onderscheiden van echte en gespeelde emoties (Andrade 2014). In supermarkten bepaalt soms niet de caissière, maar een gezichtsherkenningssysteem of je oud genoeg bent om alcohol te kopen (AIT-bv 2014).

Het inzetten van deze geavanceerde technieken biedt voordelen, bijvoorbeeld op het gebied van veiligheid, omdat het makkelijker wordt om een verdachte te identificeren. Maar de inzet van de technologie roept ook vragen op. Welke informatie valt er eigenlijk van ons gezicht af te lezen? Welke partijen gebruiken die informatie, op welke manier? Zijn wij nog wel 'de eigenaar' van ons eigen gezicht en van onze eigen emoties? De technieken stuiten bij sommigen op verzet, bijvoorbeeld van kunstenaars die gezichtsherkenning op creatieve wijze omzeilen (Polo 2010).[1]

Deze verkennende studie van het Rathenau Instituut signaleert een belangrijke ontwikkeling op het gebied van gezichts- en emotieherkenning: de techniek is indringend en raakt wijdverbreid. Databases groeien, toepassingsmogelijkheden nemen toe, en de techniek wordt steeds beter. Daardoor zitten deze technologieën ons steeds dichter op de huid. In de Verenigde Staten lijkt dit besef toe te nemen: bedrijven ontwikkelen gedragscodes,[2] er vinden politieke hoorzittingen plaats over de impact van de technologie op privacy en andere burgerrechten[3] en senatoren stellen bedrijven kritische vragen over de impact van deze technologie (Persbericht Al Franken 2014).

In Nederland is een dergelijk debat (nog) niet op gang gekomen, hoewel beleidsmakers, juristen, technici en ethici wel geïnteresseerd lijken in de ontwikkelingen op het gebied van gezichts- en emotieherkenningstechnologie. Het doel van dit discussiestuk is de informatie over gezichts- en emotieherkenning op zo'n manier te structureren, dat deze een goede basis vormt voor een publieke discussie in Nederland. De centrale vragen zijn:

1. Wat is de huidige stand van de techniek? Hoe heeft de technologie zich ontwikkeld en wat zijn technische uitdagingen voor de toekomst?

---

1 Zie ook https://decorrespondent.nl/2176/Kunstenaar-Zach-Blas-laat-zien-dat-surveillance-meer-op-het-spel-zet-dan-alleen-onze-privacy/165728747008-d3e4fbce voor een beschrijving van de gezichtsmaskers van Zach Blas.

2 Een recent voorbeeld is het stakeholdersoverleg dat geïnitieerd werd door de National Telecommunication and Information Administration van de U.S. Department of Commerce.

3 Zo vond er in juli 2012 een hoorzitting plaats van de Senate Judiciary Committee, getiteld: 'What Facial Recognition Technology Means for Privacy and Civil Liberties'. (Hill 2012).

2. Op welke schaal en op welke manier worden deze technieken ingezet in Nederland?
3. Wat zijn de maatschappelijke aspecten die hiermee gepaard gaan?

Methode en theoretisch perspectief
Dit verkennend onderzoek is tot stand gekomen door literatuuronderzoek en interviews met experts en belanghebbenden (zie bijlage 1). De verslagen van deze interviews zijn in korte intermezzo's in dit boekje verwerkt. Het Rathenau Instituut heeft vervolgens een rondetafeldiscussie georganiseerd om de bevindingen te valideren. Dit rapport dient als input voor de publieke discussie in Nederland over gezichts- en emotieherkenning: wat is de impact van deze technologie en wat is nodig voor een maatschappelijk verantwoorde ontwikkeling van deze technologie?

In dit rapport zien we de ontwikkeling van technologieën voor gezichts- en emotieherkenning niet als een op zichzelf staande ontwikkeling. We benaderen haar vanuit haar sociaal maatschappelijke context, waarbij we bekijken hoe de ontwikkeling van technologie en maatschappij elkaar wederzijds beïnvloeden en vormen. De ontwikkeling van een nieuwe technologie wordt beïnvloed door bestaande opvattingen, regelgeving, instituties en infrastructuur, maar de technologie beïnvloedt op haar beurt diezelfde opvattingen, regels, instituties en infrastructuur.

De maatschappelijke impact van gezichts- en emotieherkenning is dan ook niet los te zien van de maatschappelijke context waarin de technologie wordt toegepast. Dat is onder andere te zien bij het gebruik van gezichtsherkenningstechnologie bij de toegangspoortjes van ADO Den Haag. De prestatie van het systeem hangt af van de manier waarop de technologie in een bepaalde situatie is ingebed. Er zit een *menselijke hand* achter de technologie: bij het instellen van de software, bij het interpreteren van de data, en bij de keuze van een vervolgactie. Wat gebeurt er als de poortjes in het ADO-stadion niet opengaan, omdat een supporter niet herkend wordt? De manier waarop data opgeslagen worden, heeft invloed op de privacy van de betrokkenen. Het maakt uit of de data lokaal of in een grote database worden opgeslagen, en hoe ze worden beveiligd. Zelfs de manier waarop de software 'getraind' wordt, heeft maatschappelijke gevolgen: als er in de trainingsdatabase alleen Aziatische personen voorkomen, zullen individuen van een andere etniciteit minder goed herkend worden. Omgekeerd kan de groeiende aandacht voor privacy in het publieke debat van invloed zijn op de manier waarop ontwikkelaars hun software ontwerpen – bijvoorbeeld door meer waarborgen voor privacy in de techniek in te bouwen.

Leeswijzer
Bij zowel gezichts- als emotieherkenning wordt het gezicht gebruikt als informatiebron. Dat kan op verschillende manieren. In dit hoofdstuk bespreken we vijf varianten: verificatie, identificatie, *matching*, categorisatie en emotieherkenning.

We lichten vervolgens het technische proces toe en de technische uitdagingen waar de huidige software en hardware voor staan. Hoofdstuk 2 gaat over toepassingen van gezichts- en emotieherkenningstechnologie in binnen- en buitenland (per variant). In hoofdstuk 3 geven we een indicatie van de mogelijke maatschappelijke betekenis van gezichts- en emotieherkenning voor privacy, gelijke behandeling en sociale omgang. In hoofdstuk 4 doen we verslag van een rondetafeldiscussie waarin experts met ons meedachten, zowel over de mogelijkheden die gezichts- en emotieherkenning te bieden heeft, als over de maatschappelijke vraagstukken die ermee gepaard gaan. Tot slot blikken we vooruit. Welke inzichten heeft deze verkennende studie ons geboden en hoe gaat het Rathenau Instituut verder met dit onderzoek?

1.1 Gezicht als informatiebron

Onder automatische gezichtsherkenning verstaan we: 'Het automatisch verwerken van digitale afbeeldingen die gezichten van individuen bevatten, met als doel de identificatie, verificatie of categorisatie van deze individuen.'[4]
Automatische emotieherkenning is het meten van iemands emoties door het analyseren van de uitdrukkingen in zijn gezicht.

We bespreken vijf soorten toepassingen waarbij het gezicht als informatiebron is gebruikt: verifiëren, identificeren, matching, categoriseren en emotieherkenning. Deze vijf vormen zijn niet alleen in technisch opzicht te onderscheiden, maar hebben ook te maken met verschillende maatschappelijke issues, zoals we later zullen zien. De eerste drie soorten zijn gericht op het koppelen van een gezicht aan een identiteit. Gezichtsherkenning waarbij een gezicht aan een identiteit wordt gekoppeld is een vorm van biometrie: het verzamelen van iemands unieke lichaamskenmerken met het doel die persoon te identificeren. Andere vormen van biometrie zijn bijvoorbeeld irisscans, spraakherkenning en het afnemen van vingerafdrukken.

1. Verificatie (1:1)

Gezichtsherkenning voor verificatie betekent dat de technologie ingezet wordt om te controleren of een persoon is wie hij claimt te zijn. Wanneer iemand zijn gezicht presenteert aan een gezichtsscanner, wordt zijn gezicht vergeleken met een eerder opgeslagen sjabloon (*template*) of afbeelding van zijn eigen gezicht. Die informatie kan lokaal worden opgeslagen (bijvoorbeeld op een pasje of smartphone), of in een algemene database. Om de identiteit te verifiëren, hoeft het systeem maar één afbeelding of sjabloon te vergelijken met het gezicht dat op dat moment aan hem getoond wordt ('*live' beeld*). Daarom wordt verificatie ook wel 1:1-gezichtsherkenning genoemd.

4 Vertaald uit (Article 29 data protection working party 2012, p. 2).

2. Identificatie (1:N)

Bij gezichtsherkenning met als doel identificatie wordt een live beeld van een persoon vergeleken met afbeeldingen of sjablonen in een database. Omdat het live gezicht met de hele database wordt vergeleken , is dit een 1:N-vergelijking. Er bestaan twee bijzondere varianten van identificatie, die met behulp van een kleinere database individuen in- of uitsluiten: respectievelijk de voorkeursbehandeling en de zwartelijsttoepassing. Bij de eerste variant krijgen de personen die in de database staan een speciale behandeling; bijvoorbeeld omdat ze vaste klant zijn bij een bedrijf. Bij de tweede wordt er met behulp van gezichtsherkenning vastgesteld of de persoon op een zwarte lijst staat. Afhankelijk van de specifieke toepassing kan een persoon de toegang ontzegd worden, of geeft het systeem een alarmsignaal af.

3. Matching (N:N)

In het geval van matching worden er afbeeldingen in een database met elkaar vergeleken, in plaats van een live beeld met een database. Het doel van matching is om afbeeldingen van dezelfde persoon bij elkaar te zoeken, bijvoorbeeld als hulpmiddel op social media. Omdat in principe alle gezichten in de database met elkaar vergeleken worden, is matching een N:N- vergelijking. Hierin verschilt matching van identificatie, waarbij er gezocht wordt naar de identiteit van een persoon op één of enkele beelden.

4. Categorisatie

Categorisatie is erop gericht om informatie uit gezichten te halen die niet direct verbonden is aan één persoon. Hierbij kunnen we denken aan groepskenmerken als leeftijd, ras en sekse. Gezichtsherkenning met als doel categorisatie kan worden toegepast met behulp van foto's of van live beelden.

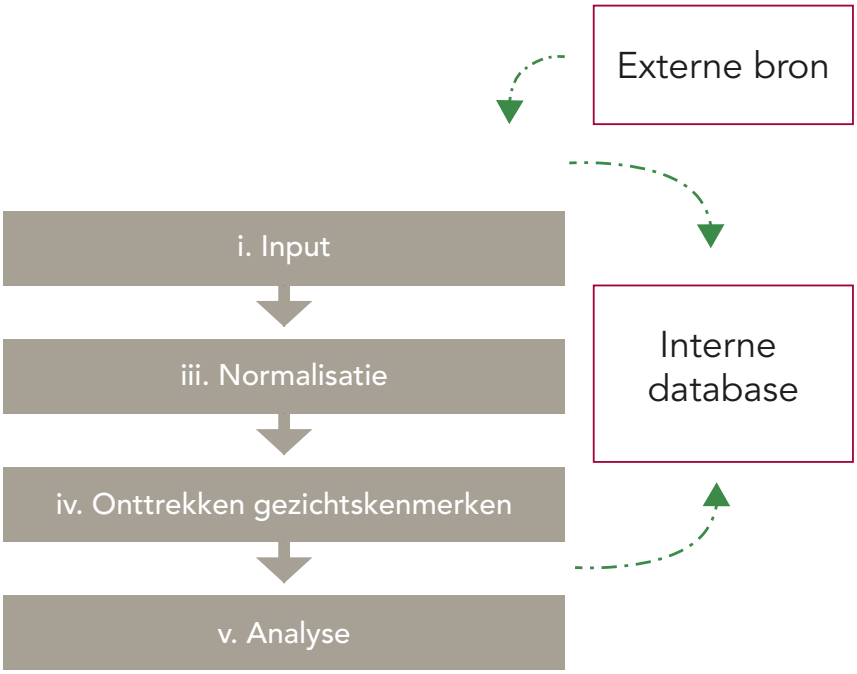
5. Emotieherkenning

Bij emotieherkenning worden de gezichtsuitdrukkingen of andere kenmerken[5] van die persoon vertaald naar diens emoties of algemene gemoedstoestand. De input voor het systeem is een live beeld, waarbij iemand zich voor een camera opstelt, of een eerder opgenomen video. Emotieherkenning verschilt van categorisatie, omdat het soort informatie dat uit het gezicht gehaald wordt bij emotieherkenning veel veranderlijker is. Emoties kunnen per microseconde verschillen, terwijl kenmerken als leeftijd, ras, en sekse relatief langzaam of helemaal niet veranderen. Ook wordt emotieherkenning (nog) niet ingezet om iemand te identificeren of te categoriseren.

5 Andere kenmerken zijn bijvoorbeeld het knipperen van de ogen of de 'micro-blushes' in het gezicht: verkleuringen die we met het oog niet kunnen waarnemen, maar die onze hartslag laten zien (Philips [z.j.]).

1.2 Technisch proces en technische uitdagingen

Het technisch proces van de verschillende toepassingen waarbij informatie uit het gezicht gehaald wordt, kan worden samengevat in het volgende schema.[6] Onder het schema is meer uitleg te vinden over de stappen.



i. Input: referentiebeeld en live beeld

Allereerst worden er beelden gemaakt die de input vormen voor de software. Deze beelden kunnen speciaal voor de toepassing gemaakt worden, of uit een externe bron gehaald worden.

Er kan een onderscheid gemaakt worden tussen referentiebeelden en live beelden. Referentiebeelden worden meestal opgeslagen in een (interne) database. Denk bij referentiebeelden bijvoorbeeld aan een foto in een paspoort (die is opgeslagen op de chip die in het paspoort zit), een foto in een database van verdachten bij de politie, of een foto die geplaatst wordt op sociale media.

Een live beeld is een foto of video die direct door de software geanalyseerd wordt. In het geval van verificatie en identificatie wordt dit live beeld vergeleken met een of meerdere referentiebeelden in de database. Bij matching worden verschillende referentiebeelden met elkaar vergeleken. Bij classificatie en emotieherkenning wordt er een live (video)beeld geanalyseerd.

---

6 Geïnspireerd door (Article 29 data protection working party 2012; Introna & Nissenbaum 2010;Noldus [z.j.])

ii. Gezichtsdetectie

Als tweede onderzoekt een algoritme of er een gezicht op de afbeelding staat en zo ja, waar.

iii. Normalisatie

Omdat gezichten er op verschillende beelden heel anders uit kunnen zien, moet het beeld genormaliseerd worden. Het normaliseren van een afbeelding van een gezicht gebeurt bijvoorbeeld door middel van het converteren van de afbeelding naar standaardafmetingen, het draaien van de afbeelding, of het aanpassen van de kleuren.

iv. Onttrekken gezichtskenmerken

Het onttrekken van gezichtskenmerken uit de afbeelding is de fase waarin informatie uit het gezicht gedestilleerd wordt. Dit kan gebeuren op basis van een holistische analyse (waarbij er een raster van een groot aantal punten 'over het gezicht wordt gelegd'), door een analyse van de bekende gezichtskenmerken (ogen/neus/kaaklijn), of door een combinatie van die twee. Bij verificatie, identificatie en matching gaat dit om biometrische informatie: kenmerken van het gezicht die uniek zijn voor dat individu. Die gegevens worden vervolgens opgeslagen in een sjabloon. Dit sjabloon kan ook worden opgeslagen in de interne database. Bij classificatie en emotieherkenning worden gegevens over het gezicht onttrokken die juist niet uniek zijn voor dat individu, maar iets zeggen over leeftijd, ras, sekse en emoties.

v. Analyse

Bij de laatste stap wordt het gemodelleerde gezicht vergeleken, gecategoriseerd of geclassificeerd. Bij verificatie, identificatie en matching worden meerdere sjablonen met elkaar vergeleken. Bij categorisatie wordt naar bepaalde eigenschappen van het gezicht gekeken om de sekse, het ras of de leeftijd van het gescande individu te bepalen. Bij emotieherkenning worden de gezichtsuitdrukkingen geclassificeerd: drukt iemand blijdschap, verdriet, boosheid, verrassing, angst of walging uit, of kijkt hij neutraal?[7]

Stand van de techniek en technische uitdagingen

Hoe goed gezichts- en emotieherkenning werkt, hangt in belangrijke mate van de soort toepassing en de kwaliteit van het beeldmateriaal af. Toch valt er in zijn algemeenheid wel iets over te zeggen. De belangrijkste uitdaging voor moderne gezichtsherkenningssoftware is de 'pose': gezichtsherkenning werkt veruit het beste als de persoon recht in de camera kijkt.[8] Als het gezicht meer dan zeven graden draait ten opzichte van een frontaal beeld, gaat de prestatie van

7 FaceReader (ontwikkeld door Noldus) geeft daarbij ook de intensiteit van die uitdrukking aan (Noldus [z.j.]).

8 Interview Ruud van Munster, interview Max Snijder.

het systeem significant achteruit.[9] Een andere uitdaging is de belichting van de foto – als twee beelden onder verschillende belichting genomen zijn, is het moeilijk om de gezichten te matchen.[10] Ook de kwaliteit van de belichting speelt een rol: de software werkt het best bij een gelijkmatige belichting. De prestatie van het systeem kan ook omlaag gaan als mensen donkere brillen dragen, of schmink of make-up op hebben.[11] Verder speelt leeftijd een rol: hoe ouder iemand is, hoe makkelijker het voor de software is om die persoon te herkennen.[12] Hoewel de kwaliteit van de beelden belangrijk is, kan moderne software steeds beter omgaan met beelden met een lagere resolutie en minder goede belichting.[13]

Emotieherkenning werkt vooralsnog alleen in relatief goed gecontroleerde omstandigheden. De persoon moet in de camera kijken terwijl zijn gezicht gescand wordt. In het begin had de software veel problemen met licht, draaiende gezichten, botox, baarden en brillen. Inmiddels kan de software daar beter mee overweg, hoewel een goede belichting nog steeds belangrijk is.[14] Deze verbeteringen hebben ertoe geleid dat emotieherkenning nu ook via internet toegepast wordt – mensen kunnen achter hun eigen computer blijven zitten terwijl hun beeld gescand wordt.[15] Ook werken softwareontwikkelaars aan de robuustheid van de technologie, zodat deze in de toekomst ook in minder gecontroleerde omstandigheden kan werken.[16]

2D versus 3D

3D-gezichtsherkenningssoftware kan een oplossing zijn voor het pose-probleem bij gezichtsherkenning. Het Nederlands Forensisch Instituut (NFI) zet bijvoorbeeld 3D-software in om te verifiëren of een bepaalde verdachte op een foto of videobeeld staat (zie interview met Arnout Ruifrok, pagina 17). Als het beeld dat zij van de gezochte persoon hebben niet frontaal genoeg is, maken zij met behulp van een infraroodcamera een 3D-model van de verdachte. Dit model kunnen zij in dezelfde pose draaien als de persoon op het beschikbare beeld. Ook de belichting kan zo worden aangepast dat die op beide beelden gelijk is. Vervolgens vindt er een (handmatige) vergelijking plaats door een rechercheur – maar er wordt al gewerkt aan een automatiseringstechniek.Aan de Universiteit Twente wordt gewerkt aan 3D-3D-gezichtsherkenning, waarbij twee 3D-beelden

9 Interview Arnout Ruifrok.
10 Interview Max Snijder.
11 Interview Ruud van Munster; interview Arnout Ruifrok.
12 NIST Face Recognition Vendor Test (FRVT) 2014.
13 In de NIST Face Recognition Vendor Test (FRVT) 2014 diende een webcam-foto als live beeld. In een database van 1,6 miljoen referentiebeeldenwerd met de beste software in 88,7 procent van de gevallen de juiste identiteit gevonden (op positie 1).
14 Interview Ricardo van der Valk.
15 Interview Ricardo van der Valk.
16 Interview Hans Theuws.


NAME
Arnout Ruifrok
JOB
Teamleider forensische biometrie
Nederlands Forensisch Instituut
LOCATION
Den Haag
100%

Intermezzo

Interview met
Arnout Ruifrok
Teamleider forensische biometrie
bij het Nederlands Forensisch Instituut

‘Wij krijgen het lastige materiaal’

Het Nederlands Forensisch Instituut (NFI) houdt zich onder meer bezig met forensische biometrie – een verzamelnaam voor technieken waarmee mensen op basis van biometrische kenmerken zoals het gezicht, de spraak, het handschrift of vingerafdrukken kunnen worden geïdentificeerd. Arnout Ruifrok, teamleider forensische biometrie bij het NFI, heeft in Nederland een werkgroep gezichtsvergelijking gestart. ‘We hebben twee doelen: van elkaar leren en zaken standaardiseren.’

De groep, met daarin onder meer experts van de politie, de Koninklijke Marechaussee, Defensie, de IND en justitiële inrichtingen, heeft inmiddels een gezamenlijke leidraad voor gezichtsvergelijking geschreven. Bovendien is Ruifrok via deze werkgroep betrokken geraakt bij een project van het ministerie van Veiligheid en Justitie inzake de harmonisering van diensten op het gebied van identiteitsvaststelling.

Ook op internationaal vlak probeert Ruifrok harmonisatie te bevorderen. Zo vertegenwoordigt hij het NFI bij de Facial Identification Scientific Working Group, een groep die hij omschrijft als erg toepassingsgericht. ‘Hoe moet de rijbewijsdienst omgaan met hun materiaal, bijvoorbeeld? En ook: wat kan je nu wel en wat kun je niet, en voor welke toepassingen?’

Het brengt hem op een essentieel punt als het gaat om de keuze voor bepaalde biometrische oplossingen. Ruifrok: ‘Mijn eerste tegenvraag is vaak: welk probleem wil je oplossen? Dat bepaalt wat de beste modaliteit is, hoe je het in moet richten, enzovoort.’

Wat dat betreft heeft het NFI bovengemiddeld veel obstakels te overwinnen. ‘Wij krijgen het lastige materiaal. Forensisch materiaal is ongecontroleerd verkregen; mensen willen meestal niet herkend worden.’ De beelden komen meestal van de politie, soms van de rechtbank of via een advocaat. Een wereld van verschil met de foto’s die worden verzameld om mensen bijvoorbeeld toegang tot een kantoorgebouw te geven. Ruifrok zit naar eigen zeggen op ‘een extreme van wat biometrie heet’. Geautomatiseerde biometrie is met forensisch materiaal dan ook vaak onmogelijk. ‘De huidige algoritmes kunnen nog niet met ongecontroleerd materiaal omgaan.’

Dit legt veel druk op de kwaliteit van het vergelijkingsmateriaal. Gezichtsherkenning – als identificatiemiddel in theorie net zo betrouwbaar als een pincode - werkt alleen goed op frontale beelden. Als van een verdachte alleen beeld beschikbaar is waarop hij opzij kijkt, kunnen de NFI-onderzoekers met hem op de plaats delict nieuwe opnames maken. Lukt dat niet, dan kan een 3D opname helpen. ‘Zo’n 3D opname werkt aardig als de verdachte niet

meewerkt en bijvoorbeeld beweegt of gekke bekken trekt.' Het kan ook helpen belichtingsproblemen op te lossen. Theoretisch is het zelfs mogelijk om in 3D modellen de gezichtsuitdrukkingen te veranderen. Vervolgens probeert men het 3D beeld qua positie zo goed mogelijk te matchen met de daderbeelden, waarna NFI-onderzoekers deze op het oog vergelijken.

Doel van de exercitie is doorgaans om te kijken: past een verdachte in het plaatje? En zo ja, komt daarna de volgende vraag: hoeveel anderen passen daar ook in? Door de slechte kwaliteit van de beelden zijn er dat vaak heel veel. Ruifrok: 'De standaard percentages gaan niet op voor onze beelden. Bij de ene foto is de kans 1 op 100 dat een andere persoon er ook in past, bij de andere foto 1 op 1000. Dit heeft gevolgen voor de bewijskracht.' Het schatten van deze kans doet het NFI nu met common sense, met subjectieve beoordelingen. 'Als we bepaald materiaal krijgen, zouden we echter graag in staat zijn om van te voren te zeggen met wat voor sterkte we aan de hand daarvan een uitspraak kunnen doen.'

Essentieel blijft wat de mens vervolgens met de uitslag doet, benadrukt Ruifrok: 'Ook als de mens de laatste factor is – dat blijft hij denk ik, zeker voor forensisch werk - dan heb je nog niet alle problemen opgelost, want die mens kan ook gewoon een keer fout zitten.'

met elkaar worden vergeleken.[17] Het Fraunhofer-Institut in München werkt aan de ontwikkeling van 2D-3D-matching software: hierbij wordt een tweedimensionaal beeld vergeleken met 3D-beelden in een database.[18]

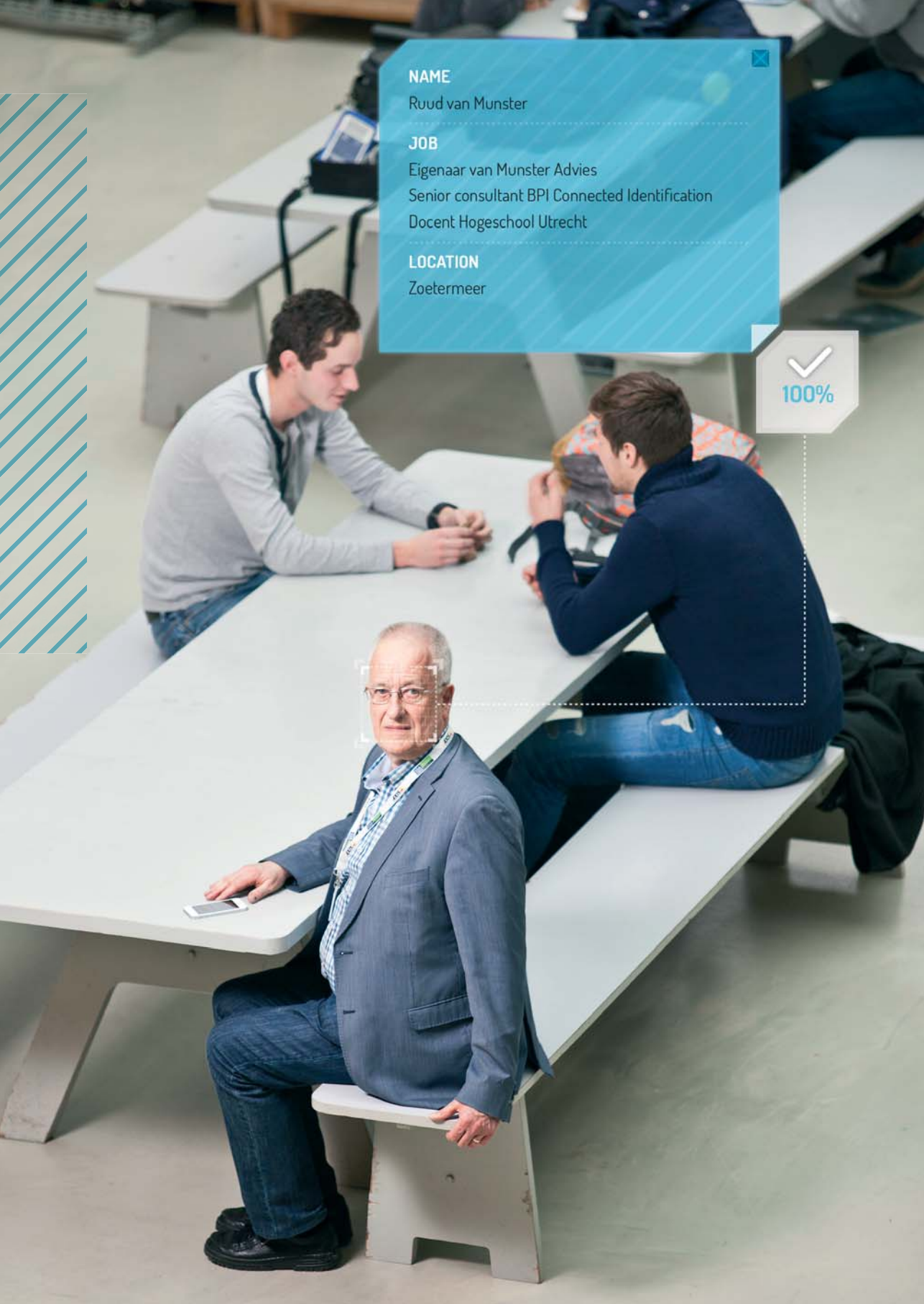
Fout-positieven, fout-negatieven en drempelwaarden

Gezichtsherkenning geeft nooit honderd procent zekerheid. De accuraatheid van gezichtsherkenning hangt in belangrijke mate af van beleidsmatige keuzes over de manier waarop de technologie wordt ingezet. Een van die keuzes is de instelling van de drempelwaarde. De drempelwaarde bepaalt bij welke mate van overeenkomst de software aangeeft dat twee afbeeldingen van dezelfde persoon zijn of kunnen zijn. De keuze voor deze waarde heeft invloed op het percentage fout-negatieve (het systeem denkt dat de afbeeldingen niet van dezelfde persoon zijn, terwijl dit wel zo is) en fout-positieve uitkomsten (het systeem denkt dat de afbeeldingen van dezelfde persoon zijn, terwijl dit niet zo is) . Het is belangrijk dat de drempelwaarden tijdens de analysefase van de technologische ontwikkeling goed worden ingesteld (zie deel 1.2).

Dit kunnen we goed zien in het voorbeeld van ADO Den Haag, waarbij supporters al dan niet toegelaten worden tot risicovakken door gebruik te maken van gezichtsherkenning (zie interview Ruud van Munster op pagina X). Bij het implementeren van deze technologie moet de drempelwaarde worden ingesteld. Als er voor een hoge drempelwaarde wordt gekozen, is het beleid streng: alleen als het systeem er vrij zeker van is dat de kaart bij deze supporter hoort, mag de supporter naar binnen. Dit betekent dat er weinig fout-positieve uitkomsten zijn: het zal niet vaak voorkomen dat het systeem denkt dat er een match is tussen supporter en kaart, terwijl dit niet zo is. Een hoge drempelwaarde heeft wel tot gevolg dat er veel fout-negatieve uitkomsten zijn: het zal relatief vaak voorkomen dat een supporter de toegang ontzegd wordt, terwijl hij wel de rechtmatige eigenaar van de kaart is. Het instellen van een lage drempelwaarde heeft het omgekeerde effect. Hierbij zullen er weinig fout-negatieve, maar veel fout-positieve uitkomsten zijn.

In deze concrete situatie zien we dat het instellen van de drempelwaarde om een afweging vraagt tussen veiligheid en gemak. Bij een strenge drempelwaarde zullen er weinig ongewenste supporters binnenkomen, maar zal de doorstroom erg langzaam zijn, omdat veel mensen onterecht worden geweigerd. Bij een soepeler beleid loopt men makkelijker door, maar bestaat de kans dat er raddraaiers naar binnen glippen.

17 Interview Arnout Ruifrok.
18 Interview Arnout Ruifrok.


NAME
Ruud van Munster
JOB
Eigenaar van Munster Advies
Senior consultant BPI Connected Identification
Docent Hogeschool Utrecht
LOCATION
Zoetermeer
100%

Intermezzo

Interview met
Ruud van Munster
Eigenaar van Munster Advies

‘We zijn op weg naar het verzamelen van een integraal mensbeeld’

Op termijn kunnen we niet meer over straat zonder herkend te worden, denkt Ruud van Munster, eigenaar van van Munster Advies en senior consultant op het gebied van biometrie.

‘We zijn op weg naar het verzamelen van een integraal mensbeeld… Een smartphone kan jouw bewegingen registreren en ook waar je bent. Dat wordt nu niet allemaal opgeslagen, maar via zo’n integraalplaatje - de combinatie van verschillende technieken; je oor, de textuur van je huid, je adempatroon en je hartslag - zou je mensen nu al goed kunnen identificeren.’

Naarmate de kosten van de technieken die worden ingezet om mensen te herkennen en die gegevens op te slaan, te verwerken of te delen omlaag gaan, wordt meer mogelijk, voorspelt Van Munster. Hij trekt een parallel met de smartphone – die kan inmiddels van alles wat vijf jaar geleden niet voor mogelijk werd gehouden en is bovendien betaalbaar geworden.

Bij camera’s constateert Van Munster een vergelijkbare beweging. De techniek verfijnt terwijl de prijs daalt, waardoor technisch geavanceerde camera’s bereikbaar worden voor een steeds grotere groep. Een infrarood camera die vijf jaar geleden nog €20.000 per stuk kostte, kan nu door een hobbyist voor €300 worden gekocht. Dat gaat heel snel.’

Bovendien zal het volgens hem steeds makkelijker worden om de benodigde software te verkrijgen waarmee de verzamelde gegevens kunnen worden geduid.

ADO Den Haag is al een eind op weg, aldus de consultant. Iedereen die een van de risicovakken in het stadium van de voetbalclub wil betreden, wordt gecontroleerd. ‘Iedereen die daar naar binnen wil, krijgt een pas. Met behulp van gezichtsopnamen is voor iedereen een template gemaakt. Van alle bezoekers van die vakken wordt het gezicht gescand. Het pasnummer is gekoppeld aan een blacklist.’

Als het zogeheten *proximity* pasje in de buurt van het toegangssysteem komt, wordt er in de database alvast gezocht naar het nummer van het pasje. Dit maakt een snelle matching mogelijk zodra de pasdrager in de camera kijkt. Het systeem is nog voor verbetering vatbaar, vervolgt Van Munster; doordat het in eerste instantie erg streng was, zorgde het voor veel oponthoud. ‘Geleidelijk

aan zijn ze toch wat gaan versoepelen… Ze zijn nu aan het kijken hoe ze hiermee verder moeten.'

Ook al is de toegangsscan bij ADO lang getoond als een schoolvoorbeeld van een succesvolle biometrische toepassing, toch blijft ook hier de blik van de mens onmisbaar. Van Munster: 'Ze hebben het toch niet aangedurfd om mensen er heel hard op te weigeren. Het besef dat die technologie wel helpt, maar er toch nog niet helemaal 100% is, is er wel.'

Dat moet ook wel. Want bij ADO hebben de voetbalsupporters een goede reden om mee te werken omdat ze het stadion in willen. Maar wie kwaad in de zin heeft, kan – bijvoorbeeld in het openbaar vervoer – bewust niet in de richting van beveiligingscamera's kijken. Ook het feit dat camera's tegen het licht inkijken maakt herkenning soms lastig. Verder kan iemand ook met schmink herkenning voorkomen.

Toch denkt Van Munster dat live gezichtsherkenning ooit niet meer uit ons leven weg te denken zal zijn. 'Je ziet dat overheden hun best doen om gezichtsbedekking te verbieden. Het gezicht wordt gezien als een essentieel gegeven dat je uitwisselt in het sociaal verkeer. Het wordt als minder privé gezien dan bijvoorbeeld een vingerafdruk of iris.'

Van Munster verwacht dat op termijn de politie bijvoorbeeld Google Glass zal gebruiken om mensen op straat te identificeren. Ook daarbuiten zitten er volgens hem grote veranderingen aan te komen. 'De beeldkwaliteit van Google Glass is nog niet heel geweldig, maar dat verandert natuurlijk binnen een aantal jaren.... Er komt een moment dat mensen in de trein in staat zijn jou te fotograferen met hun telefoon of bril en dan toch je telefoonnummer kunnen achterhalen.'

2 Toepassingen

De technologie voor gezichts- en emotieherkenning kent steeds meer toepassingen, en ook het aantal domeinen waarop de technologie wordt ingezet neemt toe. In dit hoofdstuk bespreken we verschillende toepassingen van gezichts- en emotieherkenning, per soort: verificatie, identificatie, matching, categorisatie en emotieherkenning. Daarbij kijken we vooral naar toepassingen in Nederland, maar noemen we ook belangrijke ontwikkelingen in bijvoorbeeld de Verenigde Staten.

2.1 Verificatie

Verificatie is doorgaans de makkelijkste methode van gezichtsherkenning, omdat de omstandigheden waaronder het live beeld genomen wordt goed te controleren zijn. De persoon heeft er baat bij als hij herkend wordt door het systeem; daarmee krijgt hij toegang tot een bepaald gebied of wordt vastgesteld dat hij de rechtmatige eigenaar van een document of computer is. De persoon zal daarom goed meewerken, en bereid zijn om recht in de camera te kijken. Ook is het bijvoorbeeld mogelijk om de belichting goed af te stellen, zodat het live beeld van goede kwaliteit is. Een ander belangrijk aspect is dat het live beeld maar met één foto in de database vergeleken hoeft te worden. De prestatie van verificatie hangt daarmee niet van de omvang van de totale database af.

Zoals eerder genoemd, koppelen verificatietoepassingen een persoon aan een drager. In sommige gevallen wordt het gezicht daarbij als wachtwoord (of pincode) gebruikt. Het Finse bedrijf Uniqul ontwikkelt software waarmee je kunt betalen door je gezicht te laten zien, in plaats van je pinpas te gebruiken.[19] Eerst moeten gebruikers zich registreren door hun gezicht aan hun betaalgegevens te koppelen. Daarna kunnen zij in de aangesloten winkels betalingen autoriseren door in een camera te kijken. Het principe van het gezicht als wachtwoord wordt ook gebruikt door de FastAccess Anywhere-app, ontwikkeld door SensibleVision.[20] Met deze app kun je inloggen op mobiele apparaten met behulp van je gezicht. Een vergelijkbare app is FaceCrypt,[21] waarbij een digitale 'kluis' wordt beveiligd met gezichtsherkenningssoftware.

Een andere belangrijke toepassing van verificatie is het Europese paspoort. In de chip die zich sinds 2006 in het Nederlandse paspoort bevindt, worden ook gegevens over het gezicht opgeslagen. Alleen de foto zelf, niet het sjabloon met biometrische gegevens[22] wordt opgeslagen. Op dit moment wordt de foto

19 Voor meer informatie, zie: http://uniqul.com/.
20 Voor meer informatie, zie: http://www.sensiblevision.com/.
21 Voor meer informatie, zie: http://facecrypt.com/.
22 Zie stap vier in paragraaf 1.2.

op het paspoort meestal nog op het oog vergeleken met de persoon die het paspoort presenteert. Op steeds meer vliegvelden echter, kunnen de sjablonen in het paspoort automatisch vergeleken worden. Op Schiphol zijn in 2011 36 *e-gates* geïnstalleerd, waarbij deze poorten de foto in het paspoort vergelijken met een opname van de persoon die het paspoort presenteert (De Rooij 2011). Op Aruba experimenteert de KLM zelfs met een 'Happy Flow' -concept, waarbij het gezicht fungeert als paspoort en instapkaart tegelijkertijd(Luchtvaartnieuws 2014). De reiziger passeert vanaf het inchecken tot het boarden verschillende poortjes waarbij hij alleen zijn gezicht hoeft te laten zien. Ook het besproken voorbeeld van ADO Den Haag is een verificatietoepassing.

2.2 Identificatie

De prestatie van identificatietoepassingen van gezichtsherkenningstechnologie hangt in belangrijke mate af van de vraag of de persoon met de identificatie meewerkt. Als iemand niet herkend wil worden, kan hij het de software erg lastig maken, door het hoofd te draaien of door bijvoorbeeld allerlei grimassen te maken. De kans dat iemand niet meewerkt, is het grootst als hij het risico loopt om uitgesloten te worden – met andere woorden, wanneer de persoon op een zwarte lijst staat. Andersom werken mensen vaak wel goed mee als ze voordeel hebben bij herkenning door het systeem. Hieronder bespreken we eerst algemene toepassingen van identificatie, en daarna de voorkeursbehandelingen en zwartelijsttoepassingen. Bij deze laatste twee soorten toepassingen van identificatie is de database vaak een stuk kleiner vergeleken met die voor algemene toepassingen.

Algemene identificatie

Algemene identificatie kent toepassingen in het commerciële domein en op het gebied van veiligheid. Een voorbeeld van een commerciële toepassing is de app NameTag, ontwikkeld door FacialNetwork.com. Met behulp van deze app kan iemand met een *Google Glass* een foto van een voorbijganger nemen en deze met behulp van gezichtsherkenningssoftware matchen met online-profielen die te vinden zijn op bijvoorbeeld social media. Ook wordt de opname vergeleken met verschillende databases van criminelen, zoals de *National Sex Offender Registry* (Vincent 2014). Er bestaat een opt-outsysteem voor deze technologie, waarbij mensen zich kunnen registreren op de website van NameTag als ze níet herkend willen worden door de app.

Op dit moment is NameTag beschikbaar voor Google Glass-Betatesters. Doordat Google heeft aangegeven geen gezichtsherkenningsapps te ondersteunen tot er een betere versie van Google's privacystatement bestaat, is NameTag niet beschikbaar als officiële app. Ook ondervindt NameTag weerstand vanuit de Amerikaanse Senaat. In februari 2014 uitte senator Al Franken diepe zorgen aan het adres van Kevin Alan Tussy – de bedenker van NameTag – over privacy en andere persoonlijke veiligheidsaspecten, en verzocht hem de lancering van de app uit te stellen (Press release Franken 2014). Kevin Alan

Tussy reageerde op de brief door te benadrukken hoe belangrijk privacy voor NameTag is. Volgens Tussy is die gewaarborgd doordat iedereen die zijn app gebruikt om anderen te identificeren, eerst zichzelf moet identificeren. Daarnaast wijst hij op het opt-outsysteem (McGee 2014). Ondanks deze verdediging heeft NameTag de lancering van de app, die gepland was voor het eerste kwartaal van 2014, tot nader order uitgesteld. In september 2014 lanceerde NameTag de tweede demoversie van de app voor Betatesters. Enkele dagen later ontving NameTag een sommatiebrief van Facebook, waarin Facebook stelt dat NameTag de gebruikersvoorwaarden van Facebook schendt. Ook heeft Facebook aan NameTag de toegang tot de eigen login-pagina ontzegd, omdat gebruikers die zich wilden registreren voor de opt-outregeling van NameTag naar die pagina verwezen werden (Haney 2014).

Een voorbeeld van een toepassing voor algemene identificatie op gebied van publieke veiligheid is het systeem dat de Politie Amsterdam gebruikt bij de opsporing van verdachten. Zij hebben een database met foto's van personen die in verzekering zijn gesteld in Amsterdam (zie interview René Lewis, pagina 31). Als het opsporingsteam een verdachte in beeld heeft, kan het team gebruikmaken van een gezichtsherkenningssysteem om de verdachte te helpen identificeren. Dit systeem laat de vijftig meest waarschijnlijke matches zien, waarna een rechercheur nagaat of een van deze foto's inderdaad overeenkomt met de verdachte. In twee tot vijf procent van de gevallen is er een foto van de gezochte persoon bij de top vijftig die het systeem heeft gegenereerd – een *hit*.[23] Dit percentage is vergelijkbaar met het aantal hits bij methodes zoals vergelijking van DNA-profielen of vingerafdrukken.

De database bevat op dit moment ongeveer 105.000 foto's, waarbij er ook meerdere foto's van één persoon kunnen voorkomen.[24] Met het fotonummer van de foto's in deze database kan gezocht worden in een andere database met signalementen, personalia en fotonummers van de verdachten. Op het moment dat een delict verjaart, een verdachte overlijdt, of een gerechtelijke uitspraak bepaalt dat een persoon niet langer verdacht is, wordt de foto uit deze tweede database verwijderd.[25]

Een vergelijkbare toepassing in het veiligheidsdomein wordt ontwikkeld door de FBI: *Next Generation Identification* (*NGI*). Met dit project wil de FBI bestaande databases, waarin alleen foto's en vingerafdrukken van verdachten worden opgeslagen, uitbreiden. De nieuwe database, de *Interstate Photo System* (*IPS*), maakt het mogelijk dat meerdere systeemgebruikers meerdere foto's kunnen uploaden van verdachten en andere burgers (FBI [z.j. (a)]). Ook kunnen er

23 Interview René Lewis.
24 Interview René Lewis.
25 Interview René Lewis.


NAME
René Lewis
JOB
Kwaliteitscoördinator forensische opsporing
Politie Amsterdam-Amstelland
LOCATION
Amsterdam
100%

Intermezzo

Interview met
René Lewis
Kwaliteitscoördinator forensische opsporing
bij de politie Amsterdam-Amstelland

‘Je kan en mag dit niet aan een machine overlaten’

Gezichtsherkenning is een handig hulpmiddel in de zoektocht naar verdachten, stelt René Lewis, kwaliteitscoördinator forensische opsporing bij de politie Amsterdam-Amstelland.

Iemand die verdacht wordt van een strafbaar feit waar minstens vier jaar voor staat en die daarvoor in Amsterdam-Amstelland in verzekering wordt gesteld, wordt op de foto gezet. In de loop der jaren heeft het korps zo een referentiebestand van ongeveer 105.000 verdachtenfoto’s opgebouwd. Wanneer er in een onderzoek een verdachte (letterlijk) in beeld komt, gaat het observatieteam van het korps op zoek naar foto’s – vaak van sociale media, bewakingscamera’s of in beslag genomen computers of camera’s. Die foto’s worden vergeleken met de verdachtenfoto’s in de database. Lewis: ‘Bij ons staat het systeem meestal zo ingesteld dat je vijftig gezichten te zien krijgt wanneer je een foto invoert.’ Nu al vindt zijn team met deze aanpak bij 2% tot 5% van het aangeboden beeldmateriaal een mogelijke bijbehorende persoon in de verzameling van vijftig foto’s.

Tot nu wordt gezichtsherkenning alleen toegepast op de Amsterdamse database. Lewis en zijn collega’s pleiten daarom al jaren voor een landelijke toepassing, maar tot nog toe was dat lastig. Alle verdachtenfoto’s waren eigendom van een bepaald korps. Lewis: ‘Je moest allerlei ingewikkelde convenanten sluiten als je die wilde gebruiken.’ Het samengaan van verschillende politiekorpsen in één nationale politiedienst is daarom goed nieuws, volgens Lewis. Nu we nationale politie zijn, is dat probleem opgeheven.’

Toch is er nog een reeks hobbels te nemen. Zo telt Nederland op dit moment 26 databases zoals die van Amsterdam. Het samenvoegen van deze foto’s is technisch weliswaar niet ingewikkeld, maar het blijft een behoorlijke klus. Het gaat om honderdduizenden foto’s die moeten worden ge-upload, waarvan een deel dubbel is. Personen kunnen immers zowel in Amsterdam als elders in verzekering zijn gesteld.

Er zijn nog meer databases met foto’s die van nut zouden kunnen zijn voor de identificatie van verdachten, vervolgt Lewis. Zo is er Project Progis, opgezet in 2006 onder het toenmalige ministerie van Justitie om te voorkomen dat mensen tegen betaling andermans straf uitzitten. De ruim 300.000 foto’s in deze zogeheten strafrechtketen database SKDB zijn volgens Lewis echter slecht toegankelijk en van onvoldoende kwaliteit. Binnenkort start een pilot om de SKDB met behulp van geautomatiseerde gezichtsvergelijking doorzoekbaar te maken. Daarnaast is er ook een landelijke database van ongeveer 350.000 foto’s die wordt gebruikt voor fotoconfrontaties. Deze foto’s, eveneens van mensen

die in verzekering zijn gesteld, hebben een relatief lage resolutie - een obstakel voor gezichtsherkenning.

Dan is er nog het kostenplaatje; de licentiekosten voor de gezichtsherkennings-software zijn afhankelijk van de omvang van de referentiedatabase. Lewis voegt toe: 'Een ander probleem is dat met de huidige reorganisatie, de besluitvorming wat stroef verloopt.' Toch is het zaak een landelijke database op te zetten, benadrukt hij. 'Ook omdat we nu regelmatig aanvragen vanuit de rest van het land krijgen. Op het moment dat iemand een link met Amsterdam vermoedt, komt er een aanvraag bij ons binnen.'

Zo'n tien jaar na de start van de gezichtsherkenningspilot in Amsterdam ligt het aantal hits op 2% tot 5%. Dat is vergelijkbaar met het aantal hits op basis van DNA of vingerafdrukken. Lewis: 'Het is net zo efficiënt of inefficiënt als de andere methodes, en daardoor wél een welkome aanvulling.'
Ongeacht de omvang van de database en de geavanceerde techniek blijft een menselijke blik onmisbaar, benadrukt de kwaliteitscoördinator forensische opsporing. 'Je kan en mag dit niet aan een machine overlaten.'

De software ziet soms dingen over het hoofd, bijvoorbeeld doordat niet naar de oren wordt gekeken. Omgekeerd is Lewis' team goed in het herkennen van West-Europeanen. 'In zijn algemeenheid is het zo dat je mensen van andere origine minder goed uit elkaar kunt houden dan mensen van dezelfde etniciteit als jezelf. Bij ons team geldt daardoor dat we beter zijn in het herkennen van West-Europeanen dan in het herkennen van bijvoorbeeld mensen uit het gebied van de Middellandse Zee, Afrikanen of Oost-Aziaten.'

meerdere biometrische gegevens van iemand worden opgeslagen, zoals een irisscan, *palm print* (afdruk van de handpalm) , opnamen van het stemgeluid, en foto's die gebruikt kunnen worden voor gezichtsherkenning (EFF [z.j.]). De FBI meldt inderdaad dat de mogelijkheden voor automatische gezichtsherkenning worden onderzocht (FBI [z.j. (a)]). NGI kan de data delen met meer dan 1800 wetshandhavingsinstanties en andere geautoriseerde partners in het strafrecht (FBI [z.j. (a)]). In een rechtszaak, aangespannen door de Electronic Privacy Information Center, heeft een rechter in november 2014 bepaald dat de FBI meer informatie moet vrijgeven over het NGI vanwege de omvang en reikwijdte van het project (EPIC 2014).

De documenten die door klokkenluider Edward Snowden zijn blootgelegd, laten zien dat ook de Amerikaanse veiligheidsdienst NSA steeds meer gebruikmaakt van gezichtsherkenningssoftware (Risen & Poitras 2014). Uit de gelekte documenten blijkt dat de NSA miljoenen gezichten per dag verzamelt bij het onderscheppen van data, waarvan er 55.000 geschikt zijn voor gezichtsherkenning (Risen & Poitras 2014). Veiligheidsdiensten leggen niet alleen zelf databases aan, maar maken ook gebruik van databases die door mensen zelf zijn aangelegd. De Politie Amsterdam, bijvoorbeeld, verkrijgt soms beelden uit in beslag genomen telefoons of computers, of zoekt foto's op social media. Sommige technologie rondom gezichtsherkenning, onder meer van Google, wordt door de politie gebruikt om verdachten te identificeren.[26]

De mogelijkheid om personen op straat te herkennen is een belangrijke drijfveer voor het ontwikkelen van gezichtsherkenning in het veiligheidsdomein – we zouden het bijna de zoektocht naar de heilige graal kunnen noemen. Met deze toepassing zouden bijvoorbeeld beveiligingscamera's op straat mensen kunnen volgen en identificeren. Een dergelijk systeem is op Schiphol getest.[27] Het doel van deze proef was om vluchtelingen te kunnen identificeren die soms dagen op Schiphol blijven om te verhullen met welke vlucht zij het land zijn binnengekomen (en dus waar zij vandaan komen). Voor deze toepassing was de techniek echter nog niet rijp, omdat de beelden niet altijd een frontaal gezicht bevatten.[28]

Voorkeursbehandeling

Gezichtsherkenning kan worden toegepast om simpelweg de identiteit van een persoon te achterhalen, maar het kan ook tot doel hebben om bepaalde personen een speciale behandeling te geven, bijvoorbeeld een voorkeursbehandeling. De database is in zo'n geval gevuld met de gezichten van personen die een speciale behandeling dienen te krijgen. De vorm van identificatie

26 Interview René Lewis.
27 Interview Ruud van Munster.
28 Interview Ruud van Munster; Robin Hermann.

waarbij mensen een voorkeursbehandeling krijgen is vaak commercieel van aard: door middel van gezichtsherkenning krijgen klanten speciale aanbiedingen of hebben zij bepaalde privileges. De app Facedeals van het Amerikaanse bedrijf Redpepper kan klanten identificeren als ze een winkel binnenkomen en hen speciale aanbiedingen sturen op basis van hun *likes* op Facebook.[29] Om deze aanbiedingen te ontvangen, moeten mensen zich eerst inschrijven op Facebook en daar een aantal foto's van henzelf verifiëren.

FaceFirst heeft vergelijkbare ambities; het bedrijf is van plan hun identificatie-software – ontwikkeld om dieven die op een zwarte lijst staan, te kunnen herkennen – uit te breiden, zodat winkeliers bepaalde groepen mensen die in aanmerking komen voor een voorkeursbehandeling makkelijker kunnen herkennen (Singer 2014). Een derde voorbeeld is Virgin Atlantic, dat gezichtsherkenning heeft geïntegreerd in Google Glass. Medewerkers kunnen *frequent flyers* op die manier herkennen, en hen vervolgens een vipbehandeling geven (Virgin Atlantic 2014).

Zwartelijsttoepassingen

Het tegenovergestelde van een voorkeursbehandeling is een toepassing die werkt met een zwarte lijst. Identificatie op basis van een zwarte lijst is meestal een veiligheidstoepassing. Bij deze categorie wordt gezichtsherkenning ingezet om de mensen op een zwarte lijst van een bepaalde plaats te weren of om speciale actie te kunnen ondernemen.

De inzet van gezichtsherkenning in trams door de RET is een voorbeeld van een zwartelijsttoepassing. Op een aantal tramlijnen van de Rotterdamse openbaar-vervoermaatschappij geldt een ov-verbod voor mensen op de zwarte lijst. In 2011 is de RET een proef gestart waarbij gezichtsherkenning ervoor moet zorgen dat het trampersoneel gewaarschuwd wordt als iemand met een ov-verbod toch in de tram stapt. Met dat doel zijn er camera's neergezet die alle passagiers registreren. Als de gezichtsherkenningssoftware iemand herkent van de zwarte lijst, gaat er een lampje branden bij de bestuurder van de tram. Die kan op zijn beurt aan de conducteur doorgeven dat er mogelijk een persoon met een ov-verbod is ingestapt. Hij kan ook aangeven bij welke deur die persoon is binnengekomen. De conducteur krijgt op zijn beurt de zwarte lijst te zien en probeert dan degene met het ov-verbod te identificeren door passa-giers naar hun identiteitsbewijs te vragen.

In 2013 is de proef geëvalueerd, en op basis van positieve reacties van de trambestuurders en positieve technische testen is het project naar meer lijnen uitgebreid.[30] Moeilijke omstandigheden zoals tegenlicht, weersomstandigheden en niet-meewerkende personen probeert de software op te vangen, wat

29 Voor meer informatie, zie: http://redpepperland.com/lab/details/check-in-with-your-face.
30 Interview Frouke Albers.

resulteert in een accuratesse van zeventig tot tachtig procent. Dat betekent dat een persoon met een ov-verbod ongeveer drie op de vier keer herkend wordt.[31] De software is ingesteld met een drempelwaarde om fout-positieve uitkomsten 'te allen tijde te voorkomen'.[32] Een ov-verbod kan worden opgelegd voor maximaal acht weken. Nadat het ov-verbod afloopt, wordt het sjabloon geheel uit de database verwijderd.[33]

Een vergelijkbare proef is gehouden bij Rotterdamse juweliers. Dit project – Fotoswitch – zette gezichtsherkenning in om juweliers te waarschuwen als er een 'zwarte lijster' voor hun deur stond.[34] De juwelier kon dan besluiten de deur niet te openen of hulp in te schakelen. Als de software een gezicht kon herkennen, en onder ideale omstandigheden opereerde, werden mensen op de zwarte lijst in 98 procent van de gevallen herkend. Het was ook mogelijk om de gezichtsherkenningssoftware te koppelen aan Liveview; als er een hit was, kon er iemand live meekijken. De zwarte lijst was ondergebracht bij de politie. Om organisatorische redenen (de politie had besloten geen externe projecten meer te financieren) is de proef uiteindelijk stopgezet.

Een derde voorbeeld van zwartelijsttoepassingen is een app ontwikkeld door de Chinese bedrijven Baby Back Home en JWT (Ramachandran 2013). Met deze app kun je een foto nemen van een kind waarvan je vermoed dat het ontvoerd is, waarna gezichtsherkenningssoftware de foto vergelijkt met de database van vermiste kinderen op de website Baby Back Home.[35]

2.3 Matching

Naast verificatie en identificatie is matching een manier om een gezicht aan een identiteit te koppelen.[36] Vaak wordt matching toegepast in social media, maar er zijn ook manieren om het in te zetten voor veiligheidstoepassingen.

Een belangrijk voorbeeld van matching is Facebook, dat gezichtsherkenning inzet om automatisch '*tags*' te suggereren. Allereerst worden de gezichten op foto's die getagd zijn met een bepaalde naam gescand en omgezet in een sjabloon dat opgeslagen wordt. Daarna wordt er elke keer een naam gesuggereerd als er een foto van die persoon op Facebook verschijnt. De gebruiker wordt niet expliciet op de hoogte gesteld van deze functie, maar kan wel voor een opt-out kiezen. Dit betekent dat de naam niet gesuggereerd wordt, maar

31 Interview Eugène de Geus.
32 Interview Eugène de Geus.
33 Interview Eugène de Geus. Dit kan wel één dag te laat gebeuren, wat vervelend kan zijn voor degene die een ov-verbod had.
34 Interview Henri Apeldoorn.
35 Voor meer informatie, zie: http://www.baobeihuijia.com/.
36 Strikt genomen worden er bij matching alleen foto's aan elkaar gekoppeld, maar die koppeling vindt plaats op basis van een identiteit.

heeft niet tot gevolg dat het sjabloon verwijderd wordt. Een gezicht moet namelijk eerst herkend worden, voordat de software weet dat er aan dit gezicht geen naam verbonden mag worden.

Omdat Facebook hiermee biometrische gegevens verzamelt zonder expliciete toestemming van de gebruiker, conflicteert deze toepassing met Europese wetgeving over persoonsgegevens (Information age 2011). Na klachten van de Data Protection Agency in Ierland is deze functie in september 2012 uitgeschakeld (Keijzer 2014). In september 2014 echter, werd het duidelijk dat Facebook weer gaat beginnen met de toepassing, onder de restrictie dat alleen voor Amerikanen een naam wordt gesuggereerd – Europeanen worden mogelijk wel gescand, maar van hen verschijnt geen tag-suggestie (Keijzer 2014).

De Picasa-software van Google zet gezichtsherkenning ook in om verschillende afbeeldingen van dezelfde persoon met elkaar te matchen. Dit doet de software met foto's die lokaal op een computer of tablet zijn opgeslagen, of met foto's die geüpload worden.

2.4 Categoriseren

Als gezichtsherkenning wordt ingezet om mensen te categoriseren, worden de beelden van deze personen niet direct aan een identiteit gekoppeld. Personen kunnen bijvoorbeeld op basis van leeftijd, sekse of ras worden gecategoriseerd. Dit wordt ook wel *soft biometrics* genoemd (Jain, Dass & Nandakumar 2004). De app SceneTap is een voorbeeld van een categorisatietoepassing van gezichtsherkenning. Deze app geeft aan hoe druk het is in een café of bar, hoe het met de man-vrouwverhouding staat en wat de gemiddelde leeftijd van de bezoekers is. Om dit te kunnen zien, zijn er camera's met gezichtsherkenningssoftware geïnstalleerd in deze cafés. De app is gelanceerd in Chicago, maar wordt inmiddels al in dertien Amerikaanse steden aangeboden.[37]

Een ander voorbeeld zijn digitale billboards die gepersonaliseerde advertenties laten zien op basis van iemands leeftijd en sekse. In 2010 is een aantal vervoersbedrijven in Tokio begonnen met een proef met deze billboards (AFP 2010), en in 2013 kondigde een Brits bedrijf aan dat het deze toepassing bij 450 tankstations ging installeren (Bosteels 2013).

In Nederland wordt gezichtsherkenning ook ingezet om leeftijd de categoriseren. Het bedrijf AIT biedt bijvoorbeeld software aan om te herkennen of iemand achttien jaar of ouder is, en daarmee alcohol of tabak mag kopen in een supermarkt. Een klant van 18 jaar of ouder kan zich eenmalig registreren, waarna zijn gezichtskenmerken opgeslagen worden. Elke keer als de klant alcohol of tabak wil kopen, kan een gezichtsherkenningssysteem bij de kassa herkennen of

37 Voor meer informatie, zie: https://scenetap.com/.

deze klant zich eerder heeft geregistreerd. Als de klant niet herkend wordt, dan moet de kassamedewerker alsnog beslissen of er naar een identiteitsbewijs gevraagd moet worden.

2.5 Emotieherkenning

De toepassingen van emotieherkenning bevinden zich vooral op drie gebieden: psychologisch onderzoek, marktonderzoek, en mens-machine-interactie.[38] Tot nu toe zijn de toepassingen beperkt tot een gecontroleerde setting; een persoon kijkt in een camera en de software leest vervolgens de gezichtsuitdrukkingen. Softwareontwikkelaars proberen hun programma's echter steeds robuuster te maken, zodat deze ook in ongecontroleerde settings gebruikt kunnen worden. Emotieherkenning kan nu ook op afstand gebruikt worden via internet. Door een online-versie kunnen personen achter hun eigen computer zitten terwijl de software hun gezichtsuitdrukkingen analyseertm (zie interview Ricardo van der Valk op pagina 41).

In psychologisch onderzoek wordt emotieherkenning bijvoorbeeld ingezet om de interactie tussen docenten en studenten te onderzoeken, of om de effectiviteit van lesmateriaal te testen (Parks & Mead 2014). Een andere toepassing binnen de psychologische wetenschap is wanneer emotieherkenning wordt gebruikt om te onderzoeken hoe autisten reageren op emotionele prikkels: kunnen zij deze emoties spiegelen?

Wanneer emotieherkenning wordt ingezet voor marktonderzoek, wordt er gekeken naar de manier waarop mensen reageren op merken, brochures, reclamecampagnes of producten die geïntroduceerd worden. Door de emoties van mensen te meten tijdens het zien van een reclamefilmpje, bijvoorbeeld, kunnen ontwikkelaars erachter komen of dit filmpje vooral negatieve of positieve emoties oproept.

Bij de mens-machine-interacties wordt emotieherkenning op drie manieren gebruikt: om de reacties op machine-interfaces te testen, om emoties van zorgbehoevenden te meten, en om machines er meer als mensen uit te laten zien. Een voorbeeld van de eerste manier is dat er gekeken wordt of mensen gefrustreerd, boos of gestrest reageren op een machine-interface. Dat kan een teken zijn dat de opzet van de interface veranderd moet worden.

Softwareontwikkelaars denken ook na over de vraag hoe emotieherkenning een rol kan spelen in Ambient Assisted Living (AAL).[39] AAL is erop gericht om

38 Interview Hans Theuws.

39 Noldus zit daarvoor in een aantal gesubsidieerde projecten met universiteiten en andere partners. Interview Hans Theuws.

mensen die zorg nodig hebben zolang mogelijk zelfstandig te laten wonen, en ontwikkelt instrumenten waarmee dat mogelijk gemaakt wordt.

Emotieherkenning kan een van die instrumenten zijn, omdat je daarmee kunt zien of iemand bijvoorbeeld droevig of blij is. Tot slot wordt emotieherkenning tegenwoordig ook gebruikt om emoties beter weer te geven in animatiefilms. Pixar heeft deze software bijvoorbeeld gebruikt in films zoals *Toy Story*.[40]

40 Interview Ricardo van der Valk.


100%
NAME
Ricardo van der Valk
JOB
Expertisemanager merk & communicatie
Blauw Research
LOCATION
Rotterdam
Weena

Intermezzo

Interview met
Ricardo van der Valk
Expertisemanager merk & communicatie
bij Blauw Research

‘Kijken of er een ”say-feel-gap” is: een verschil tussen zeggen en voelen’

Als reclamepsycholoog bij Panteia[1] doet Ricardo van der Valk onderzoek naar motieven en impliciete drijfveren van mensen, onder meer met behulp van de zogeheten Implicit Attitude Test (IAT) of Impliciete associatietest. Ook maakt hij gebruik van FaceReader, een impliciete meetmethode waarmee het bewuste, rationele antwoordenpatroon kan worden ontweken.

Emotieherkenning wordt al regelmatig ingezet in de reclamewereld, vertelt Van der Valk. Als hij reclamecampagnes test, laat hij storyboards met geluid zien. ‘Daar zetten we proefpersonen voor en daar staat dan de FaceReader op. Daarna stellen we vragen om te kijken of er een ”say-feel-gap” is: een verschil tussen wat mensen zeggen en wat ze voelen.’ Dat komt vooral voor wanneer sociale wenselijkheid een rol speelt, constateert de reclamepsycholoog.

Ook onderzoek naar reacties op merken, producten die geïntroduceerd worden en brochures kan een extra dimensie krijgen als de (niet uitgesproken) emoties boven water komen. Zo kan emotieherkenning in de gezondheidszorg van nut zijn om de effectiviteit van anti-rookcampagnes te meten, aldus Van der Valk.

Dat er een kloof bestaat tussen wat mensen zeggen en de emoties die af te lezen zijn op hun gezicht, is bekend. Maar over de mate waarin die deels onbewuste emoties sturend zijn voor beslissingen lopen de meningen uiteen. Van der Valk: ‘Je bevindt je dan op glad ijs.’ Hij verwijst naar Victor Lamme, hoogleraar en hersenonderzoeker in de programmagroep ‘Brain and cognition’ van de UvA. Lamme stelt dat 80% tot 90% van het gedrag van consumenten bepaald wordt door intuïtie en/of onbewuste drijfveren. Van der Valk relativeert: ‘Dat is een inschatting. Er is geen overkoepelende studie geweest die dat heeft aangetoond.’ Marjolein Moorman, directeur van de Stichting Wetenschappelijk Onderzoek Commerciële Communicatie en voormalig hoogleraar communicatiewetenschap aan de UvA, had het zelfs over 90% tot 95%.
Van der Valk voelt zich gesterkt door de stelling van Fred van Raaij, emeritus hoogleraar economische psychologie aan de Universiteit Tilburg, dat er een paradigma-shift bestaat: de manier van informatie verwerken in het kader van onbewuste keuzeprocessen richt zich steeds meer op impliciete factoren. ‘Dat steunt ons in onze methodes en visie.’

---

1 Inmiddels werkt Ricardo van der Valk als expertisemanager merk & communicatie bij Blauw Research.

Ook al is het niet keihard te maken in hoeverre mensen zich laten leiden door gevoelens waarvan ze zich niet bewust zijn of hun ware emoties verbergen, toch constateert de reclamepsycholoog dat zijn vertrouwen in wat mensen zeggen daalt. Er hoeft geen opzet in het spel te zijn: 'Je hebt bijvoorbeeld ook te maken met post-rationalisatie. Mensen proberen achteraf hun vertoonde gedrag voor zichzelf te verklaren, terwijl ze vaak geen idee hebben waardoor dit werd 'geactiveerd''.

Onderzoek met behulp van emotieherkenning heeft volgens hem daarom zeker toekomst. Mits aan de juiste voorwaarden wordt voldaan. Zo moet FaceReader nooit als stand-alone techniek worden aangeboden; één meetinstrument biedt onvoldoende zekerheid om je koers te bepalen. Alleen in combinatie met IAT (dat op merk-associaties is gericht), met kwalitatief onderzoek en/of in de nabije toekomst met tests inzake de doorbloeding van de huid als mate van arousal kan het een goede indicator zijn.

Van der Valk ziet ook (mogelijke) toepassingen buiten het commerciële vlak, zoals een gezichtscodeersysteem op de Google Glass waar in Duitsland mee is geëxperimenteerd. 'Autistische jongeren kunnen dan de emoties van hun gesprekspartner beter bepalen.' Dan zijn er nog de verzorgingsrobots die dankzij emotieherkenningstechnieken passende gezichtsuitdrukkingen en/of emoties kunnen tonen: aangenamer gezelschap voor depressieve mensen. Het gebruik van impliciete meetmethoden om emoties te meten zal toenemen en verbreden, verwacht Van der Valk, maar niet zonder slag of stoot. Men vindt het nog te eng, stelt hij. Dat niet alleen: 'Het heeft ook te maken met sociale wenselijkheid: als we alles van elkaar weten is de sociale lijm verdwenen.'

3 Maatschappelijke betekenis

Het vorige hoofdstuk ging over de diversiteit aan toepassingsmogelijkheden van technologieën voor gezichts- en emotieherkenning. De techniek biedt kansen, zowel in het veiligheidsdomein als in het commerciële domein (betere dienstverlening, meer gemak voor consumenten). Tegelijkertijd roepen de toepassingen vragen op over de maatschappelijke betekenis van deze technologieën. In de Verenigde Staten worden kritische vragen gesteld over onder andere privacyaspecten. Hoe kunnen we de maatschappelijke betekenis van de snelle ontwikkelingen in gezichts- en emotieherkenning duiden? Het Rathenau Instituut signaleert een ontwikkeling waarin gezichts- en emotieherkenning steeds indringender aanwezig is (*pervasive)*. In andere woorden: deze technologieën dringen in steeds meer contexten door. Dat komt door drie subontwikkelingen:

1. Grotere en beter verbonden databases.
2. Een diversificatie van toepassingen van de technologie.
3. Een verschuiving van toepassingen van gecontroleerde naar ongecontroleerde omgevingen.

Grotere databases

Databases worden steeds groter en raken steeds beter met elkaar verbonden, waardoor informatie uit steeds meer contexten aan elkaar gekoppeld wordt. Een voorbeeld is het Next Generation Identification-systeem van de FBI, dat ontworpen is om informatie uit verschillende databases te kunnen samenvoegen. Ook in Nederland zien we dergelijke ontwikkelingen: de politie van Amsterdam kan gezichtsherkenningstechnologie nu alleen toepassen op foto's van verdachte Amsterdammers, maar is van plan om dit uit te breiden naar de databases van andere steden.[41] Een praktische reden voor deze ontwikkeling is dat de opslag van data steeds goedkoper wordt en de distributie van gegevens makkelijker.[42]

De ontwikkeling van grotere en beter gekoppelde databases zien we echter niet alleen van bovenaf: de groei van databases komt ook voor een belangrijk deel door de opkomst van social media, waarin gebruikers zelf veel foto's en informatie op internet zetten. Dit betekent ten eerste dat er meer data zijn om te gebruiken, maar ook dat de algoritmes zeer snel verbeteren. De enorme hoeveelheid data maakt het mogelijk om software, die ontworpen is volgens principes van neurale netwerken, beter te trainen in het zelf leren herkennen van gezichten.[43]

41 Interview René Lewis.
42 Rondetafeldiscussie, Max Snijder.
43 Rondetafeldiscussie, Ruud van Munster en Eugène de Geus.

Ook de smartphone speelt een centrale rol. Omdat gebruikers hun smartphone altijd bij zich hebben, staat er vaak veel persoonlijke en identificerende informatie op, zoals foto's van de gebruikers zelf, hun vrienden en familie. De apps en databases die hieraan verbonden zijn staan voornamelijk 'in de cloud', waardoor het onderscheid tussen lokale en globale opslag makkelijk verdwijnt. Ook gezichtsherkenningssoftware gebruikt vaak materiaal dat in de cloud is opgeslagen.[44]

Diversificatie van toepassingen

Er zijn steeds meer toepassingsgebieden voor gezichts- en emotieherkenningstechnologieën. Aanvankelijk vond toepassing vooral plaats in het veiligheidsdomein (vaak toegepast in een (semi-)publieke context door de overheid). Nu zetten ook commerciële partijen gezichts- en emotieherkenning in, voor steeds meer doeleinden. Hierdoor komen wij de technologieën in meer facetten van ons leven tegen. Google en Facebook hebben in de afgelopen jaren bedrijven gekocht die gezichtsherkenningssoftware ontwikkelen (Van Est 2012) en zetten deze techniek nu volop in.

Doordat veel techniek vrij beschikbaar is ('opensourcesoftware'), komen toepassingen steeds meer in handen van particulieren.[45] Dit kan ertoe leiden dat prijzen van gezichtsherkenningssystemen gaan dalen, waardoor het toepassingsbereik verder kan toenemen.[46] Ook hier speelt de smartphone een rol: die is bepalend voor de snelle verbreiding van de technologie, omdat de techniek altijd voorhanden is en foto's maken en verwerken makkelijker wordt (zie ook interview Max Snijder, pagina 49).

Verschuiving naar ongecontroleerde omgevingen

De software en de camera's worden beter, waardoor de technologieën zich van een gecontroleerde naar een ongecontroleerde context kunnen bewegen. Moderne gezichtsherkenningssoftware kan beter omgaan met beelden van slechte kwaliteit. Daarnaast worden computers steeds krachtiger, waardoor continue (*realtime*) uitvoering van zware rekenklussen binnen bereik komt.[47] Tegelijkertijd neemt ook de kwaliteit van de beelden toe, omdat camera's beter en goedkoper worden[48] en doordat de software het beeld realtime kan verbeteren: bijvoorbeeld door ter plekke het contrast van het beeld aan te passen.[49]

Waar gezichtsherkenning eerst alleen werkte als iemand onder gecontroleerde omstandigheden recht in de camera keek, kunnen de beelden van de bewakingscamera's op straat de grootschalige toepassing van gezichtsherkenning op

44 Rondetafeldiscussie, Ruud van Munster.
45 Rondetafeldiscussie, Ruud van Munster.
46 Rondetafeldiscussie, Ruud van Munster.
47 Rondetafeldiscussie, Ruud van Munster.
48 Interview Ruud van Munster.
49 Rondetafeldiscussie, Ruud van Munster.

termijn binnen bereik brengen, al zal het nog enige tijd duren voordat de camera's op straat vervangen zullen zijn.[50] Emotieherkenning wordt ook robuuster, waardoor deze techniek in de toekomst waarschijnlijk bij zorgrobots kan worden ingezet.[51]

Wat betekent het dat de toepassing van technologieën voor gezichts- en emotieherkenning indringend en allesomvattend wordt? Wij gaan ervan uit dat de grootste maatschappelijke veranderingen plaats zullen vinden op gebied van privacy, gelijke behandeling en sociale omgangsvormen. We bespreken deze maatschappelijke veranderingen per toepassing. We groeperen de toepassingen in dit hoofdstuk in:

- biometrische toepassingen (verificatie, identificatie, matching);
- categorisatie;
- emotieherkenning.

We doen dit omdat de aard van deze toepassingen elk hun eigen maatschappelijke vragen oproepen.

3.1 Verificatie, identificatie en matching

Privacy
Als technologieën voor gezichts- en emotieherkenning worden ingezet voor verificatie, identificatie of matching worden er biometrische gegevens uit het gezicht gelezen. Experts en belanghebbenden zijn het niet eens over de vraag hoe privégevoelig deze gegevens zijn. Volgens de International Biometrics & Identification Association (IBIA), een Amerikaanse brancheverenigingdie het gebruik van biometrie stimuleert, heeft gezichtsherkenning weinig negatieve invloed op de privacy van consumenten. IBIA geeft als argument dat het gezicht hoe dan ook zichtbaar is – ook zonder toepassing van gezichtsherkenningstechnologie kunnen we ons nooit volledig anoniem in de publieke ruimte begeven; er bestaat altijd een kans dat we herkend worden (IBIA 2014). IBIA houdt in deze argumentatie geen rekening met het technologisch proces (zie hoofdstuk 1). Meer specifiek: IBIA houdt geen rekening met de manier waarop de beelden *verkregen* worden en de wijze waarop biometrische informatie *opgeslagen* en *gebruikt* wordt.

De ontwikkelingen waarbij toepassingen verbreden en de technologie zich uitbreidt van gecontroleerde naar ongecontroleerde omgevingen, zorgen ervoor dat beelden in meer situaties verkregen worden, en dat dat ook ongemerkt kan gaan. Doordat Facebook en Google grote databases met foto's

50 Rondetafeldiscussie, Ruud van Munster.
51 Interview Hans Theuws.


100%
NAME
Max Snijder
JOB
CEO en eigenaar European Biometrics Group
LOCATION
Naarden

Intermezzo

Interview met
Max Snijder
CEO en eigenaar van de
European Biometrics Group

‘Biometrie bevindt zich in een juridisch niemandsland’

Biometrie heeft een unieke kracht, stelt Max Snijder, directeur-eigenaar van de European Biometrics Group. Het is het enige middel waarmee een fysiek persoon naar een digitale omgeving kan worden omgezet. ‘Daarmee versmelten de wetten van de fysieke wereld met die van de digitale wereld.’

Voordeel van gezichtsherkenning is dat de techniek het gebruikers makkelijk maakt om te zien of iets een hit is, veel makkelijker dan bijvoorbeeld vingerafdrukken. Het is de hoogste tijd voor een brede discussie over gezichtsherkenning, vindt Snijder.

Niet voor niets is hij secretaris en medeoprichter van de European Association for Biometrics, een organisatie met 165 leden die bijeenkomsten organiseert, burgers informeert over de ontwikkelingen op het gebied van biometrie en het debat probeert aan te zwengelen.

De randvoorwaarden voor de techniek zijn inmiddels in onze paspoorten verwerkt en de toepassing ervan begint een trend te worden. Zowel overheden als het bedrijfsleven zetten in op gezichtsherkenning, vooral op het gebied van surveillance. Snijder komt met het ene na het andere voorbeeld. In Duitsland worden foto’s genomen van snelheidsovertreders. In de VS zijn mobiele eenheden en agenten op straat uitgerust met gezichtsherkenningsapparatuur en is een groots Biometric Centre of Excellence gebouwd waar alle biometrische gegevens binnenkomen. Schiphol heeft proeven gedaan met het verzamelen van gezichten uit surveillancebeelden. Een bekende commerciële toepassing is verificatie op basis van het gezicht, bijvoorbeeld voor toegangsbeheer.
Zelf was Snijder in het verleden betrokken bij een proef met Albert Heijn in samenwerking met de politie om winkeldiefstal tegen te gaan. De gezichten van mensen die binnenkwamen werden gescand en vergeleken met foto’s van mensen met een winkelverbod.

Tot zo ver wat is of bijna is. Dan is er nog alles wat komen gaat. Zo heeft Snijder onlangs onderzoek gedaan naar de inzet van biometrie in de gezondheidszorg. ‘Dat gaat niet alleen over iemand identificeren aan de balie’, benadrukt hij.
Er wordt veel nagedacht over biometrische oplossingen bij HomeCare, ofwel zorg op afstand. Snijder: ‘Hoe kun je echt goed verifiëren dat je de juiste persoon voor je hebt?’ Hij heeft grote verwachtingen voor het gebruik van biometrie in de gezondheidszorg. Toegang tot patiëntengegevens kan bijvoorbeeld met behulp van biometrie beter worden gecontroleerd.

De groei van de inzet van biometrie staat in schril contrast met de aandacht voor privacy rond het onderwerp. Biometrische gegevens zijn – vaak gevoelige - persoonsgegevens, maar desondanks is er weinig over vastgelegd. Snijder spreekt over een juridisch gat. 'Biometrie bevindt zich in een juridisch niemandsland. Het hangt er ook vanaf wat voor data eraan gekoppeld worden en waar ze toegang tot geven. Gaat het bijvoorbeeld om gegevens gelieerd aan een bankrekening of om een LinkedIn-foto? En hoe gevoelig is een foto op Facebook? Dat maakt het lastig om regelgeving te maken.' Het nieuws dat de Amerikaanse NSA miljoenen gezichten per dag verzamelt noemt hij illustratief: 'Het is een vogelvrij gebied.'

Als we zo doorgaan, "dreigt het recht op anonimiteit helemaal te verdwijnen," vreest Snijder. Terwijl niet voor niets in Nederland in de wet staat dat iemand niet zonder goede reden naar diens identiteit mag worden gevraagd. Het is een manier om de macht van de overheid te beperken. 'Als gezichten klakkeloos worden opgeslagen, is dat in het gedrang.'

Hoe langer het onderwerp een niemandsland blijft, hoe meer partijen allerlei toepassingen met gezichtsherkenning zullen ontwikkelen. Snijder verwoordt de twijfel: het is toch belangrijk dat de overheid beschikt over veel 'gezichten'!? Bovendien lijkt het de meeste mensen weinig te kunnen schelen.
Om te vervolgen: 'Maar wanneer gaat het fout? En wat gebeurt er als het fout gaat?'

Voor de grote middenstroom zal het geen problemen geven als overheden en andere partijen over (steeds meer) van hun biometrische gegevens beschikken, denkt Snijder. Desondanks is reflectie volgens hem urgent: 'Aan de randen kunnen rare dingen gebeuren.'

hebben, kan de politie deze foto's ook inzetten om verdachten te identificeren. Omdat de techniek op afstand kan werken, kunnen foto's die op straat of in een winkel genomen zijn ook door de software gebruikt worden. Dit kan vervolgens de trend versterken dat ons lichaam altijd beschikbaar moet zijn voor identificatie: '*the availability of the body*' (Van der Ploeg 2011). Dit kan een probleem zijn voor mensen die (gedeeltelijk) gezichtsbedekkende kleding dragen en bijvoorbeeld voor baby's, die door hun snel veranderende gezicht en hun beweeglijkheid moeilijk te identificeren zijn.

Biometrische gegevens kunnen op verschillende manieren worden opgeslagen, met verschillende privacyrisico's en vragen over beveiliging tot gevolg (Grijpink 2001). Het gezicht kan opgeslagen worden als afbeelding, of als sjabloon. In een sjabloon staan alleen de gegevens over de vorm van het gezicht. Een biometrisch sjabloon is niet direct herleidbaar tot de originele foto,[52] en kan de privacy van personen daarom beter beschermen. Daar staat tegenover dat handmatig herstel niet mogelijk is wanneer er iets misgaat bij het opslaan of verwerken van het sjabloon.[53] In sommige gevallen is een database streng beveiligd, zoals in het geval van de zwarte lijst van de RET, in andere gevallen gaat het om een openbare database – denk aan de afbeeldingen van gezichten die via Google te vinden zijn. Verder verdwijnt het verschil tussen lokale en centrale opslag van gegevens steeds vaker doordat databases gekoppeld worden. Van foto's die lokaal opgeslagen zijn, kan een centrale database met sjablonen bestaan. De foto's in Picasa lijken lokaal opgeslagen – op onze eigen computer, of in ieder geval in ons eigen beheer – maar de sjablonen van onze gezichten (die Picasa gebruikt om foto's te sorteren) worden centraal opgeslagen en beheerd.

De beveiliging van grotere en beter gekoppelde databases is een enorme uitdaging: de sjablonen die op het paspoort zelf goed beveiligd zijn (lokaal), zijn bijvoorbeeld niet automatisch goed beveiligd in de gemeentelijke database.[54]

Ook ontstaat bij centrale opslag en bij het koppelen van databases het risico van *function creep*, waarbij de beschikbare gegevens gebruikt kunnen worden voor een ander doel dan waarvoor ze oorspronkelijk verzameld zijn.[55] Een

---

52 Hoewel dit in sommige gevallen toch mogelijk lijkt te zijn (interview Max Snijder, interview Ruud van Munster).

53 Interview Max Snijder.

54 Een gemeentelijke database beschouwen we hier als centrale opslag. Hoewel het geen landelijke database betreft, heeft het individu zelf geen controle over deze gegevens, zoals het geval is bij data op een persoonlijke computer of op een paspoort.

55 'In het Nederlands bestaat er nog geen bevredigende vertaling van het fenomeen "function creep". De uit de bestuurskunde bekende term "doelverschuiving" komt in de buurt, maar is niet "creepy" genoeg. Het gaat hierbij om wetten, beleidsinstrumenten, maatregelen en programma's die een geheel andere uitwerking (soms ook op een totaal ander terrein) hebben dan oorspronkelijk bedoeld. In sommige gevallen zou je kunnen spreken van neveneffecten, die echter niet per se onvoorzien hoeven te zijn.' (Uit samenvatting van: WODC (2011), Function creep en privacy, Den Haag: Boom Juridische Uitgevers.)

voorbeeld is de invoering van het biometrisch paspoort in Nederland. Het oorspronkelijke doel was verificatiemogelijkheden te verbeteren en fraude met paspoorten te bestrijden. Maar er kwam een nieuw doel bij: door de afgenomen vingerafdrukken centraal op te slaan, zouden ze ook gebruikt kunnen worden voor opsporing en terrorismebestrijding. De kwaliteit van de biometrische gegevens was echter onvoldoende voor opsporingsdoeleinden (Snijder, Kool & Munnichs 2013).

Doordat de smartphone en andere persoonlijke digitale apparaten steeds meer biometrische gegevens bevatten, is een goede beveiliging van deze apparaten cruciaal. Maar dat is zeer moeilijk.[56] In de nasleep van de onthullingen door Edward Snowden is gebleken dat privacygevoelige gegevens opgevraagd of verzameld kunnen worden door veiligheidsdiensten. Daarnaast wordt technologie voor gezichtsherkenning online als dienst aangeboden door commerciële partijen. Hun verdienmodel is gebaseerd op het exploiteren van persoonlijke gegevens. Deze constateringen roepen de vraag op of adequate bescherming van persoonlijke (biometrische) gegevens technisch en praktisch haalbaar is.[57] Bij verificatie, identificatie en matching worden biometrische gegevens gekoppeld aan een identiteit. Doordat databases groeien en gekoppeld worden, raken steeds meer facetten van deze identiteit met elkaar verweven. Omdat niet alleen de overheid, maar ook commerciële instellingen gezichtsherkenning inzetten, groeit het aantal situaties waarin we geïdentificeerd kunnen worden. Voor veiligheidsdiensten is dit een zeer relevante ontwikkeling. Doordat er meer data beschikbaar en gekoppeld zijn, kunnen zij personen identificeren zonder dat er forensische sporen bestaan. Door deze nieuwe capaciteit kunnen veiligheidsdiensten een nieuwe strategie gaan volgen, waarbij identificatie zeer belangrijk is. Dit zien we bijvoorbeeld in de Verenigde Staten, die *Global Identity Dominancy* nastreven: de veiligheidsdiensten van de overheid willen op elk moment mensen kunnen identificeren (Woodward 2005).

Een ander gevaar is dat de data onder een bepaald regime verzameld worden en vervolgens via een onduidelijke route naar een ander regime verstuurd worden. Zo verzamelt de NSA onder de vlag van terrorismebestrijding een significante hoeveelheid data, waar nu ook andere overheidsdepartementen gebruik van maken.[58] Dit doet ons denken aan het doemscenario dat er een regime aan de macht komt dat de informatie op een dramatische manier misbruikt. In Nederland is dit scenario nu niet aan de orde, maar in de geschiedenis zijn er wel voorbeelden van te vinden.[59]

---

56 Rondetafeldiscussie, Max Snijder.
57 Rondetafeldiscussie, Max Snijder.
58 Rondetafeldiscussie, Max Snijder.
59 Rondetafeldiscussie, Eugène de Geus.

Gelijke behandeling

Naast privacyrisico's heeft de inzet van gezichts- en emotieherkenningstechnologie ook gevolgen voor de verhouding tussen de overheid of bedrijven enerzijds en burgers anderzijds. Het inzetten van gezichtsherkenning kan de overheid meer macht geven ten opzichte van haar burgers. De overheid komt immers steeds meer te weten over haar burgers. De overheid kan burgers op grond daarvan bijvoorbeeld de toegang tot een gebied ontzeggen. Ook automatisch gegenereerde, maar inaccurate voorspellingen of verkeerde conclusies kunnen het individu machteloos maken. Fout-positieve uitkomsten keren de bewijslast om. Het wordt steeds moeilijker om te bewijzen dat je niet bent wie het systeem zegt dat je bent.[60]

Het probleem van fout-positieve uitkomsten wordt nog groter als blijkt dat bepaalde bevolkingsgroepen in de samenleving hierdoor extra benadeeld worden, wat tot ongelijke behandeling van deze groepen zou leiden. Bepaalde bevolkingsgroepen kunnen bijvoorbeeld systematisch worden uitgesloten van diensten, of moeilijk toegang krijgen tot diensten. Dit kan op verschillende manieren gebeuren. Ten eerste bestaat gezichtsherkenningssoftware vaak uit een neuraal netwerk dat wordt getraind op basis van een database met foto's. Het soort foto's in deze database (etniciteit, leeftijd), heeft invloed op de werking van de software. Ook kunnen de algoritmes zelf soms beter omgaan met bepaalde groepen. Gezichtsherkenning werkt beter naarmate een persoon ouder wordt; kinderen zijn het moeilijkst te herkennen (NIST 2013). Er is weinig bekend over de prestaties van gezichtsherkenning met betrekking tot personen van een verschillende etniciteit.[61] Voor zover bekend zijn de prestaties van gezichtsherkenning niet afhankelijk van de sekse, mits de database niet oneven-redig veel foto's van een van beide seksen bevat.

Als de software duidelijk verschillende prestaties levert voor verschillende bevolkingsgroepen, draagt dit bij aan een ongelijke behandeling van burgers. Juist bij de verificatie- en identificatietoepassingen kunnen verschillen in prestaties verstrekkende gevolgen hebben voor de betrokkenen. Als de gezichtsherkenningssoftware bij ADO Den Haag minder goed werkt bij donkere mensen, kan dit betekenen dat hun de toegang in verhouding vaker geweigerd wordt. Als foto's van immigranten in een database van de overheid belanden – zoals bij het Next Generation Identification-project van de FBI het geval is – lopen asielzoekers een hoger risico om aangemerkt te worden als verdachte. Zo kan gezichtsherkenning discriminatie op grond van etnische kenmerken onge-merkt verergeren.

---

60 In het kader van kentekenfraude en in het rapport De burger gaat digitaal wees De Nationale Ombudsman al eens op dit gevaar (respectievelijk De Nationale Ombudsman 2015; 2013).

61 Wel was er een rel over Microsoft Kinect, dat blanken een stuk makkelijker herkende dan donkere mensen. (Ionescu 2010).

Daarnaast is er in de technologie een aantal aannames ingebouwd die niet vanzelfsprekend juist zijn voor alle individuen in de samenleving. De inzet van gezichtsherkenning als identificatiemiddel gaat ervan uit dat gezichten *verschillend* genoeg zijn, maar ook dat zij genoeg *overeenkomen* (Van der Ploeg 2011). De software gaat ervan uit dat iemand twee ogen heeft, een neus, een mond, et cetera. Sommige personen hebben door omstandigheden echter een gezicht dat niet genoeg overeenkomt met een standaardgezicht. Daarnaast neemt de software aan dat de kenmerken van het gezicht door de tijd heen relatief stabiel blijven (Van der Ploeg 2011). Er zullen altijd mensen zijn die niet aan deze aanname voldoen, door een operatie of andere omstandigheden. Dit kan verstrekkende gevolgen hebben voor de betrokkenen.

Aan de andere kant zou de inzet van gezichtsherkenningstechnologie onbewuste vooroordelen en foutieve menselijke interpretaties juist kunnen tegengaan. Als een blanke officier bijvoorbeeld denkt dat foto's van twee Aziaten een en dezelfde persoon laten zien, kan de software aangeven dat het wel degelijk om twee verschillende individuen gaat.[62] Hierbij moet echter wel bedacht worden dat de menselijke factor nog steeds betrokken is bij de meeste toepassingen. Zo kunnen onbewuste vooroordelen toch weer een rol gaan spelen in de uitkomst van het identificatieproces.

Sociale omgang
Hebben de ontwikkelingen op het gebied van verificatie-, identificatie- en matchingstoepassingen ook invloed op sociale omgangsvormen? Door de drie genoemde ontwikkelingen zijn er steeds meer contexten waarin onze identiteit aan ons gezicht gekoppeld wordt. Mocht de heilige graal van gezichtsherkenning – het herkennen van individuen op straat – ooit werkelijkheid worden, dan kunnen we in theorie op elk moment geïdentificeerd worden. Wat betekent het verlies van anonimiteit? De gevolgen voor de sociale omgang zijn nog moeilijk in te schatten, maar ze kunnen potentieel groot zijn.

3.2 Categorisatie

Privacy
Bij categorisatietoepassingen wordt er geen uniek biometrisch sjabloon van ons gezicht gemaakt, maar worden er andere gegevens van ons gezicht afgelezen, zoals ras, leeftijd en sekse. Deze data zijn duidelijk verbonden aan wat wij onze identiteit noemen. Aan de andere kant hoeven deze data niet direct gekoppeld te zijn aan een herleidbaar persoon. De informatie dat er een vrouw van 26 aanwezig is in één van de cafés die gemonitord wordt door de app SceneTap, hoeft niet te leiden tot identificerende informatie over de vrouw in kwestie.[63]

62 Interview René Lewis.
63 Hierbij geldt wel: hoe meer categorale kenmerken er van een persoon bekend zijn, hoe waarschijnlijker het wordt dat die informatie herleidbaar is tot een individu.

Opnieuw hebben de drie gesignaleerde ontwikkelingen (grotere en beter verbonden databases, diversificatie van toepassingen en een verschuiving van toepassingen van gecontroleerde naar ongecontroleerde omgevingen) invloed op privacyaspecten. Als databases beter verbonden worden, kunnen de categorieën juist wel gekoppeld worden aan één individu. De verbreding van toepassingen kan betekenen dat niet alleen de overheid de leeftijd en sekse van een persoon kent, maar dat ook commerciële partijen deze informatie kunnen gebruiken. De derde ontwikkeling heeft als gevolg dat wij soms niet eens weten dat onze leeftijd, sekse of etniciteit van ons gezicht wordt gelezen.

Gelijke behandeling

Treffen categorisatietoepassingen bepaalde groepen onevenredig? Dit lijkt vooral het geval te zijn wanneer de software gegevens uit ons gezicht afleidt die niet overeenkomen met de identiteit die wij van onszelf presenteren. Zo stelt gezichtsherkenningssoftware wel onze sekse vast, maar niet onze *gender*, wat problemen kan opleveren voor transgenders of interseksuelen. Ook de etniciteit die de technologie van het gezicht afleest, hoeft niet dezelfde te zijn als de etniciteit waarmee iemand zich identificeert.

Vaak weten we niet op welke basis de software mensen in bepaalde categorieën indeelt. De techniek is op dat punt een black box: we hebben geen vat op het beslismodel dat de software hanteert. Dit kan bezwaarlijk zijn, omdat de precieze constructie en interpretatie van die categorieën onwetenschappelijk, onethisch of betwistbaar kan zijn (Van der Ploeg 2011). Naast het genoemde verschil tussen sekse en gender, zijn ook etnische categorieën niet zo scherp gedefinieerd als ons dagelijks taalgebruik doet vermoeden. Verder gaat het bij categorisatietoepassingen van gezichtsherkenning meestal om gevoelige categorieën: de geschiedenis laat genoeg voorbeelden zien van discriminatie op basis van etniciteit.[64] Al met al lopen juist minderheden dus een groter risico op benadeling door een dergelijk systeem.

Sociale omgang

Heeft het opdelen van mensen in verschillende categorieën gevolgen voor sociale omgangsvormen? Een voorbeeld dat we in deze context zouden kunnen noemen is de app SceneTap. De app geeft voor een aantal cafés statistieken over 'het soort' bezoekers aan. Vrouwen die op zoek zijn naar een jonge man zullen misschien eerder naar een café gaan waar het percentage jonge mannen op dat moment hoog is, volgens de app. Tot nu toe zijn er echter geen categorisatietoepassingen bekend waardoor ons sociale leven op grote schaal zal veranderen.

64 Rondetafeldiscussie, Irma van der Ploeg.

3.3 Emotieherkenning

Privacy

Een belangrijke vraag met betrekking tot privacy in het domein van emotieherkenning is welke informatie af te leiden valt uit de herkende emoties en voor wat voor soort toepassingen deze informatie wordt gebruikt. Op dit moment is onduidelijk wat emoties feitelijk zeggen over gedragingen en beslissingen van mensen. Sommigen vinden dat korte flitsen van emoties veel zeggen over iemands gedachten en neigingen, bijvoorbeeld om iets te kopen.65 Aan de andere kant is het nu nog erg moeilijk om de vertaalslag te maken van emoties naar gedachten en motieven.[66] Ook ziet de software geen andere dingen dan een getrainde waarnemer, en kunnen acteurs emoties naspelen (en de software op die manier omzeilen). De meeste vormen van emotieherkenning analyseren gezichtsuitdrukkingen (zie ook interview Hans Theuws, pagina 59), en kunnen dus niet in ons hoofd kijken. De variant die emoties herkent op basis van de verkleuring van het gezicht – micro-blushes genoemd – gaat echter een stap verder. De mens heeft namelijk nog minder controle over zijn hartslag en ademhaling, dan over zijn gezichtsuitdrukkingen.

Binnen de psychologie lijkt er in ieder geval een beweging op komst die toewerkt naar impliciete meetmethodes, bijvoorbeeld om het probleem van sociaal wenselijke antwoorden in enquêtes te omzeilen. Volgens sommige psychologen wordt maar liefst negentig procent van ons gedrag door intuïtie en onbewuste drijfveren bepaald.[67]

Zal emotieherkenningssoftware uiteindelijk in staat zijn om innerlijke emoties, motieven en gedachten goed te interpreteren? Blijft het menselijk giswerk, of raakt de technologie in staat om onze gevoelens en gedachten 'uit te lezen'?

De urgentie van deze vraag is onlosmakelijk verbonden met het gegeven dat emotieherkenningssoftware steeds breder toepasbaar zal worden gemaakt. In gecontroleerde situaties zijn wij ons ervan bewust dat we gescand worden en vinden we het wellicht minder erg als onze emoties en gedachten gelezen worden. Verder heeft emotieherkenning een andere impact wanneer het in een academische context wordt ingezet, dan wanneer er gebruik van wordt gemaakt voor commerciële doeleinden, bijvoorbeeld als advertenties worden afgestemd op onze emoties.

65 Voor meer informatie, zie: http://www.emotient.com/about.
66 Interview Ricardo van der Valk.
67 Interview Ricardo van der Valk.


100%
NAME
Hans Theuws
JOB
Productmanager Noldus
LOCATION
Wageningen

Intermezzo

Interview met
Hans Theuws
Productmanager Noldus

‘Emotieherkenning wordt steeds robuuster’

Hans Theuws volgt de signalen uit de markt op de voet: als productmanager bij Noldus is hij diegene die bepaalt waar de ontwikkelafdeling zich op richt en die het marktonderzoek coördineert. ‘Je kijkt naar de lange termijn. Je bent de spil tussen sales, R&D en communicatie’, licht hij toe. Noldus ontwikkelt software voor gedragsonderzoek. Daarnaast verkoopt het bestaande producten, waaronder FaceReader, een softwareprogramma dat emoties kan herkennen.

De software analyseert de zes basisemoties: blijheid, verrassing, verdriet, kwaadheid, angst en walging en kan ook een neutrale uitdrukking op een gezicht constateren. Nadat een gezicht is herkend, worden er ruim 500 punten in een model verwerkt dat tegen de zogeheten expressieclassifier wordt aangelegd. Deze classifier is getraind met foto’s waarop mensen van uiteenlopende leeftijd en etnische achtergrond emoties vertonen. Zo is er een Aziatisch model, een model voor kinderen en een voor ouderen. De uitkomst is levensecht; net als het menselijk oog heeft de software soms moeite de expressie van oude mensen met veel rimpels te herkennen.

Door het model van het gezicht te vergelijken met het materiaal in de expressieclassifier, kunnen de getoonde emoties worden benoemd. Ook wordt naar een aantal individuele spieren in het gezicht – de action units – gekeken. FaceReader wordt ontwikkeld door het Amsterdamse VicarVision, maar Noldus denkt mee en Theuws kent de wensen van klanten over mogelijke verbeterpunten.

Het merendeel van de afnemers zit in de academische hoek. Zo kan emotieherkenning handig zijn bij psychologisch onderzoek naar de interactie tussen studenten en leraren. Ook bij psychologisch onderzoek rond autisme – hoe reageren mensen op emoties, welke emoties vertonen ze als ze bepaalde prikkels te zien krijgen,… – kan de software uitkomst bieden.

Ook bij zogeheten usability onderzoek, naar de interactie tussen mens en machine, is emotieherkenning van nut. ‘Als mensen heel moeilijk gaan kijken wanneer ze naar operating displays of een andere user interface kijken, zie je dat je de aangeboden informatie moet aanpassen.’

Daarnaast ziet Theuws de interesse uit de commerciële hoek toenemen. Emotieherkenning wordt al ingezet bij media-, markt- en consumentenonderzoek. ‘Hoe reageren mensen op commercials, op verpakkingen, op voedsel dat ze zien, ruiken of proeven?’

Groot voordeel van de software is de snelheid; doordat filmpjes frame by frame tot in detail worden bekeken, zijn ook heel kort durende expressies zichtbaar. Doordat de software in feite de expressie analyseert en niet de emotie, kan ze bij de neus worden genomen. Een namaaklach, waarbij de spieren rond de ogen niet mee doen, valt dankzij de action units door de mand, maar een goede acteur zou dat kunnen omzeilen. Als leugendetector kan de techniek niet dienen; ze kan weliswaar detecteren of iemand zich ongemakkelijk voelt, maar een menselijke interpretatieslag blijft hier volgens Theuws onmisbaar.

FaceReader moet nu nog in gecontroleerde omstandigheden gebruikt worden; te veel schaduw in het gezicht of een gedraaid gezicht kan roet in het eten gooien. Theuws: 'Maar het wordt steeds robuuster, zodat je het ook in andere omstandigheden kan gebruiken.' In woningen, en op termijn mogelijk in winkels of op straat.

Met een aantal partners wordt onderzoek gedaan naar de mogelijkheden op het gebied van Ambient Assisted Living. Dat is erop gericht om zorgbehoevenden zo lang mogelijk zelfstandig te laten wonen. Emotieherkenning zou daarbij kunnen helpen omdat je daarmee kunt zien of iemand bijvoorbeeld blij of droevig is.

Ook wordt er gewerkt aan de interpretatie van een combinatie van verschillende emoties. Zo bevat de nieuwe versie van FaceReader een circumplex model, een soort samenvatting van metingen. Theuws: 'Als iemand bijvoorbeeld naar een filmpje kijkt en blij is, en er veel activiteit zichtbaar is in het gezicht, dan heb je meer kans dat diegene zich iets herinnert. En dat wil je eigenlijk bij een reclame-filmpje.'

Gelijke behandeling

De inzet van emotieherkenning staat nog in de kinderschoenen. Het is niet mogelijk om te zeggen hoe diverse organisaties en particulieren deze technieken zullen inzetten en of dat op grote schaal zal gebeuren. Belangrijk aandachtspunt bij de ontwikkeling van deze techniek is om niet alleen af te gaan op emotieherkenning en voorzichtig te zijn in de conclusies die op basis van de emotiedetectie getrokken worden.

In tegenstelling tot gezichtsherkenning, werkt emotieherkenning juist minder goed bij oudere mensen, vooral als ze veel rimpels hebben.[68] Om bij emotieherkenning de verschillen in prestaties met betrekking tot etniciteit op te kunnen vangen, bestaan er verschillende modellen voor specifieke etnische kenmerken. Zo is er bijvoorbeeld een Aziatisch model, waarbij de software is getraind met behulp van een database met foto's van Aziaten.[69] Voor zover bekend zijn de prestaties van gezichts- en emotieherkenning niet afhankelijk van de sekse, mits de database niet onevenredig veel foto's van een groep bevat. Met het huidige scala aan toepassingen en met de toepassingen die in de nabije toekomst te voorzien zijn, lijkt het gevaar van een ongelijke behandeling van bepaalde groepen niet het meest urgent.

Sociale omgang

Als laatste kunnen we ons de vraag stellen of emotieherkenning invloed zal hebben op sociale omgangsvormen. Emotieherkenning kan sociale contacten versoepelen. Zo wordt er gewerkt aan de inzet van software voor emotieherkenning om mensen met autisme te helpen de emoties van anderen beter te interpreteren. Zorgrobots kunnen met behulp van emotieherkenning mogelijk adequater reageren op de emotionele staat van degenen voor wie ze zorgen. Tegelijkertijd ontstaat de vraag *in welke mate* de technologie in staat zal raken om emoties en gevoelens automatisch van ons af te lezen. Op dit moment kunnen wij denken, voelen en vinden wat we willen zonder dat iemand daar ooit achter hoeft te komen. We kunnen een leugentje om bestwil vertellen – om iemand niet te kwetsen of om sociale contacten soepeler te laten verlopen. Strooit emotieherkenning zand in deze sociale machine? Wellicht verliezen we ook onze spontane reactie op andermans emoties (Van Est 2014).

68 Voor oude mensen is er ook een apart model ontwikkeld, maar als het gezicht erg veel rimpels bevat, is het voor het algoritme nog steeds moeilijk om emoties te herkennen (interview Hans Theuws).

69 Interview Hans Theuws.

4 Rondetafelbijeenkomst

Dit rapport geeft een overzicht van de recente ontwikkelingen op het gebied van gezichts- en emotieherkenning en schetst de mogelijke maatschappelijke betekenis daarvan.

In Nederland zijn ontwikkelaars, gebruikers, juristen en ethici allemaal op hun eigen manier bezig met de opkomst van deze technologieën. Beleidsmakers volgen de ontwikkelingen, maar zijn vooralsnog niet actief bezig met het maken van beleid. Tegelijkertijd is een van de belangrijkste bevindingen van deze verkennende studie dat de inzet van gezichts- en emotieherkenning allesomvattend wordt: databases worden groter en raken beter verbonden, waardoor informatie uit steeds meer voorheen gescheiden contexten aan elkaar gekoppeld wordt. Er ontstaan steeds meer toepassingen en de software en camera's worden steeds beter.

Om de bevindingen – en de maatschappelijke betekenis daarvan – te toetsen organiseerde het Rathenau Instituut een rondetafeldiscussie met belanghebbenden uit verschillende domeinen – zie bijlage 1 voor de deelnemerslijst, en bijlage 2 voor de vragen die centraal stonden tijdens de discussie. In dit hoofdstuk brengen we verslag uit van de belangrijkste bevindingen van deze bijeenkomst (zie bijlage 3 voor een uitgebreider verslag). We beginnen met een reflectie op de inhoudelijke insteek van dit rapport: horen gezichts- en emotieherkenning thuis in één rapport of hebben we het over twee fundamenteel verschillende technologieën? Daarmee verbonden is de vraag: hebben we door het bespreken van gezichts- en emotieherkenning een belangrijke ontwikkeling afgebakend? Als laatste gaat het Rathenau Instituut in op mogelijke oplossingen voor maatschappelijke gevolgen die onwenselijk zijn.

4.1 Het gezicht als gemene deler

In deze studie heeft het Rathenau Instituut twee technologieën en hun maatschappelijke betekenis onderzocht. De reden om zowel gezichts- als emotieherkenning te bestuderen is dat beide technologieën informatie uit ons gezicht halen, waarbij dit vaak gaat om gevoelige informatie waarover we zelf controle willen houden.

Tijdens de rondetafeldiscussie kwam de vraag naar boven of gezichts- en emotieherkenning wel vergelijkbaar zijn. Eén deelnemer gaf een duidelijk negatief antwoord op deze vraag; hij vond gezichts- en emotieherkenning fundamenteel onvergelijkbaar.[70] Het belangrijkste verschil tussen deze twee technologieën is dat gezichtsherkenning meestal resulteert in het identificeren van een persoon. Zelfs categorisatie- en matchingtoepassingen zijn duidelijk

70 Rondetafeldiscussie, Max Snijder.

verbonden met een identiteit: bij categorisatie wordt gezocht op basis van een kenmerk dat onderdeel uitmaakt van de identiteit, en matching vindt plaats op basis van een identiteit, ook al wordt die niet altijd gekoppeld aan (andere) persoonsgegevens. Daarentegen is emotieherkenning niet gericht op het koppelen van het gezicht aan een identiteit.

Aan de andere kant lijkt het niet onmogelijk om iemand te identificeren door middel van emotieherkenning. Het is goed voor te stellen dat iedereen een uniek patroon van gezichtsuitdrukkingen laat zien.[71] Ook hartslag en ademhaling vormen een patroon dat in principe uniek is; emotieherkenning door het meten van micro-blushes is gebaseerd op het meten van hartslag en ademhaling. Wat de maatschappelijke betekenis betreft, zouden we kunnen stellen dat emotieherkenning het jongere broertje of zusje van gezichtsherkenning is.[72] De toepassingsmogelijkheden en maatschappelijke betekenis van emotieherkenning zijn minder vergaand, maar hebben wel met elkaar te maken, en de techniek staat niet stil.

De tweede vraag met betrekking tot de inhoudelijke insteek van dit onderzoek is of we een belangrijke ontwikkeling afgebakend hebben, of dat er nog andere, niet onderzochte factoren een rol spelen. De deelnemers aan de rondetafeldiscussie waren het erover eens dat er op het gebied van gezichts- en emotieherkenning maatschappelijke veranderingen plaatsvinden die vragen om actie. Een belangrijke ontwikkeling hierbij is dat toepassingen die gebruik maken van biometrie – identificatie op basis van unieke lichaamskenmerken – tegenwoordig vaak meerdere lichaamskenmerken tegelijkertijd in kaart brengen.[73] Dit betekent dat toepassingen niet alleen maar naar het gezicht kijken, maar bijvoorbeeld ook naar de iris, het oor, het looppatroon, de textuur van de huid, het bloedvatenpatroon, de ademhaling en de hartslag. Door deze verschillende kenmerken (modaliteiten) te combineren, lukt het vaker om iemand te identificeren. Ze vangen als het ware elkaars zwakke plekken op: als het hoofd niet in de goede stand staat voor een frontale herkenning, dan kan een analyse van het oor, de iris of een van de andere kenmerken uitkomst bieden. Biometrie wordt op deze manier *multimodaal*.

4.2 Oplossingen

Hoe kunnen we ervoor zorgen dat de maatschappelijke veranderingen ten gevolge van de inzet van gezichts- en emotieherkenning in goede banen worden geleid? In deze paragraaf besteden we aandacht aan drie mogelijke oplossingen: softwareontwikkeling, wet- en regelgeving, onderwijs en publieke opinie.

71 Rondetafeldiscussie, Ruud van Munster.
72 Rondetafeldiscussie, Els Kindt.
73 Rondetafeldiscussie, Ruud van Munster.

Privacy by design & value sensitive design

Het is mogelijk om inbreuken op de privacy te voorkomen (of in elk geval de kans erop te verminderen) door alvast beschermingsmaatregelen in te bouwen wanneer de software ontwikkeld wordt. *Privacy by design* houdt in dat er in het ontwikkelingsproces al rekening wordt gehouden met privacybescherming (CBP [z.j.]). *Value sensitive design* betekent dat maatschappelijke waarden centraal staan in het gehele ontwikkelingsproces (Friedman 1996). Tijdens de rondetafeldiscussie stelde een van de deelnemers een dergelijke oplossing voor. Bij de politie komt het namelijk in de praktijk wel eens voor dat de privacywetgeving overschreden wordt, omdat bijvoorbeeld de juiste bewaartermijnen van bewijsmateriaal niet in acht worden genomen.[74] Voor dit probleem lijkt het mogelijk om een technische oplossing te verzinnen.[75] Je zou de bewaartijd kunnen automatiseren door een privacy-'schil' om het verzamelde bewijsmateriaal heen te bouwen. Op deze manier is het technisch niet mogelijk om de privacywetgeving te schenden en gebruiken we de techniek in het voordeel van privacybescherming.

Tegen dit voorstel werden twee argumenten ingebracht. Ten eerste het argument dat de privacywetgeving erg ingewikkeld is: er zijn verschillende bewaartermijnen en de wet kent veel uitzonderingen.[76] Dit maakt een technologische oplossing inderdaad lastiger, maar niet direct onmogelijk. Ten tweede het argument dat het nog maar de vraag is of bedrijven dit soort oplossingen wíllen ontwikkelen. Bedrijven die software voor gezichts- en emotieherkenning ontwikkelen, functioneren immers in een markt en moeten hun concurrentiepositie in de gaten houden.

Er werden twee voorwaarden genoemd voor de ontwikkeling en inzet van *privacy enhancing technologies* (*PET's*) door bedrijven zonder hun concurrentiepositie te verzwakken. Namelijk als het waarborgen van de privacy juist een concurrentievoordeel betekent, of als de overheid een gelijk speelveld gecreëerd heeft. Als privacy een concurrentievoordeel wordt, betekent dit dat de vraag naar PET's groot genoeg is om op dit punt de concurrentie met andere bedrijven aan te gaan. Op dit moment is dat vaak niet het geval.[77] Dit betekent echter niet dat dit dus ook nooit het geval zal zijn in de toekomst. We zullen er later op terugkomen, wanneer we ingaan op de vraag hoe PET's gestimuleerd kan worden.

Met een gelijk speelveld creëren bedoelen we dat de overheid of dat bedrijven maatregelen nemen waardoor bedrijven die PET's ontwikkelen niet benadeeld

74 Rondetafeldiscussie, René Lewis.
75 Rondetafeldiscussie, Eugène de Geus.
76 Rondetafeldiscussie, René Lewis.
77 Rondetafeldiscussie, Eugène de Geus.

worden. Dit kan bijvoorbeeld door subsidie te verstrekken voor maatschappelijk verantwoorde technologieën, of door regels op te stellen die eisen stellen aan de privacy-vriendelijkheid van software. Dit brengt ons op de volgende categorie oplossingen: wet- en regelgeving.

4.3 Wet- en regelgeving

Een tweede aandachtspunt bij de ontwikkeling van technologie voor gezichts- en emotieherkenning is regulering. Het gebruik van de gegevens die verzameld worden voor gezichts- en emotieherkenning is zowel op nationaal als op Europees niveau gereguleerd door de dataprotectiewetgeving.[78] Binnen die wetgeving hebben nationale wetgevers wel nagedacht over biometrie, maar bestaat er weinig expliciete regelgeving voor biometrie.[79] Enkele nieuwe lidstaten vormen hierop een uitzondering; zij vermelden biometrische data als persoonsgegevens. Daarnaast ligt er in Frankrijk een voorstel bij het parlement om het gebruik van biometrie heel strikt te regelen.

Een mogelijke optie voor betere regulering van biometrie, en specifiek gezichts- en emotieherkenning, is om de functionaliteit van de techniek beter in te kaderen. Het is belangrijk dat er een overzicht bestaat van wat de techniek kan en wat de maatschappelijke risico's zijn die daarmee samenhangen, bijvoorbeeld het risico op het verlies van anonimiteit.[80]

Publieke opinie & onderwijs

Om wijzigingen in de regelgeving of veranderingen in de markt voor gezichts- en emotieherkenning door te voeren, brachten deelnemers van de rondetafelbijeenkomst in dat onderwerpen als privacy hoger op de politieke en maatschappelijke agenda moeten komen. Meer mensen moeten bewust gemaakt worden van de mogelijk onwenselijke gevolgen van nieuwe technologieën. Dit is onder meer mogelijk door dit onderwerp op school te gaan behandelen .[81] Op de middelbare school zouden scholieren al moeten leren dat de inzet van techniek niet neutraal is en negatieve maatschappelijke gevolgen kan hebben. Daarnaast zouden de specifieke risico's in het hoger onderwijs per vakgebied onderzocht en gedoceerd moeten worden. In de studie rechten is aandacht voor het onderwerp dataprotectie noodzakelijk, en in de technische studies moeten er vakken komen over de maatschappelijke inbedding van techniek. Zo wordt de dialoog tussen alfa- en bètawetenschappers bevorderd. Als laatste blijft het belangrijk dat het publieke debat op een goede manier gevoerd wordt, door alle belanghebbenden bij elkaar te brengen en met hen in overleg te blijven.

---

78 In Europa is er nieuwe privacywetgeving op komst, die naar verwachting in 2016-2017 in werking zal treden. Wat deze nieuwe wetgeving inhoudt voor gezichts- en emotieherkenning is nog onduidelijk en valt buiten de reikwijdte van dit onderzoek.

79 Rondetafeldiscussie, Els Kindt.

80 Rondetafeldiscussie, Els Kindt.

81 Rondetafeldiscussie, verschillende deelnemers.

5 Tot slot: kijkend naar de toekomst

In het Nederlands kennen we de uitdrukking 'gezichtsverlies lijden'. Technologieën voor gezichts- en emotieherkenning geven een nieuwe dimensie aan het concept gezichtsverlies. In dit verkennende rapport hebben we laten zien dat deze technologieën sterk in opkomst zijn en dat ze op steeds meer manieren worden toegepast. Een *state of the art*-overzicht van enkele interessante toepassingen van gezichts- en emotieherkenning geeft een goed beeld van de reikwijdte van deze technologieën, en een idee van de mogelijke impact ervan. Interessant genoeg bleken deze reikwijdte en potentiële impact ook voor de bij de rondetafeldiscussie betrokken experts een echte *eye opener* te zijn. Zij onderschreven de urgentie van een discussie over de maatschappelijke impact van deze technologische ontwikkeling.

De verbreiding en veelzijdigheid van gezichts- en emotieherkenningstechnologie roept de vraag op hoe deze ontwikkeling het beste bestudeerd kan worden. Welke ontwikkelingen horen hierbij, en welke niet? In deze verkenning hebben we het gezicht als informatiebron centraal gezet. Maar tijdens de rondetafeldiscussie met experts uit verschillende domeinen kwam naar voren dat gezichtsherkenningstechnologie niet los gezien kan worden van andere biometrische identificatiemethoden. Het is namelijk ook mogelijk om mensen te identificeren op basis van niet meer dan hun iris of oorschelp, of op basis van individuele fysieke kenmerken zoals looppatroon, stemgeluid en houding. Zelfs de manier waarop iemand typt kan een biometrisch identificatiemiddel zijn. Veel toepassingen van identificatietechnologie zullen dit soort gegevens in de toekomst waarschijnlijk combineren in een *multimodale* aanpak. Tegelijkertijd zagen we dat het gezicht nog veel meer informatie prijsgeeft dan alleen iemands identiteit. Van het gezicht is immers ook informatie af te lezen die mensen in categorieën indeelt: geslacht, ras, leeftijd. Bovendien is van het gezicht af te lezen hoe iemand zich voelt. of hij liegt of de waarheid spreekt, en zelfs of het waarschijnlijk is of hij in de komende jaren bij zijn partner zal blijven of niet. Deze twee dimensies – biometrische informatiebronnen en het type informatie dat daaruit kan worden gedistilleerd – zullen centraal staan in het verder uitdiepen van dit onderwerp (zie tabel).

		Informatietypen							
informatiebronnen		Identificatie	Ras	Leeftijd	Geslacht	Emoties	Leugen-detectie	Liefdes-leven	…
	Gezicht								
	Stem								
	Oorschelp								
	Iris								
	Looppatroon								
	Houding								
	…								

Bij het verder in kaart brengen van de ontwikkeling zal ook regelgeving een centraal thema zijn. Hoe wordt de technologie op (inter)nationaal niveau gereguleerd? In hoeverre voldoet de huidige regelgeving? Waar dient regelgeving eventueel te worden aangepast om een maatschappelijk verantwoorde ontwikkeling van de technologie mogelijk te maken? Ook wordt gekeken in hoeverre andere oplossingen soelaas kunnen bieden, zoals privacy by design.

Een zinvolle discussie over ontwerprichtlijnen of regulering komt echter niet vanzelf tot stand. De deelnemers aan de rondetafeldiscussie onderschreven de noodzaak om zowel softwareontwerpers als burgers en beleidsmakers op weg te helpen, zodat zij *geïnformeerd* over deze technologieën na kunnen denken. Dit is in lijn met eerdere publicaties van het Rathenau Instituut, zoals het essay *Intieme technologie – de slag om ons lichaam en gedrag* (Van Est et al. 2014), waarin wordt gepleit voor de bevordering van 'technologisch burgerschap'. De opkomst van technologieën voor gezichts- en emotieherkenning biedt een interessante case om te onderzoeken hoe dit technologisch burgerschap vorm kan krijgen.

Literatuur

Acquisti, A. & R. Gross (2009). 'Predicting Social Security numbers from public data'. In: *Proceedings of the National Academy of Sciences of the United States of America* 106, no. 27 (pp. 10975-10980).

AFP (2010). 'Tokyo trials digital billboards that scan passers-by'. http://phys.org/news198392688.html, 15 juli 2010.

AIT-bv (2014). 'Simpele manier om leeftijd te peilen'. http://www.ait-bv.com/nieuwsbericht/5/Simpele+manier+om+leeftijd+te+peilen, 14 juli 2014.

Andrade, N. (2014). 'Computers are getting better than humans at facial recognition'. http://www.theatlantic.com/technology/archive/2014/06/bad-news-computers-are-getting-better-than-we-are-at-facial-recognition/372377/, 9 juni 2014.

Article 29 data protection working party (2012). 'Opinion 02/2012 on facial recognition in online and mobile services'. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, 22 maart 2012.

Bosteels, K. (2013). 'Tesco installeert camera's met gezichtsherkenning voor adverteerders'. http://www.retaildetail.be/nl/belgie/algemeen/item/16917-tesco-installeert-cameras-met-gezichtsherkenning-voor-adverteerders, 5 november 2013.

CBP. 'Privacy by design'. https://cbpweb.nl/nl/zelf-doen/privacycheck/privacy-design, [z.j.].

De Nationale Ombudsman (2015). 'Overheid moet gedupeerden kentekenfraude helpen'. https://www.nationaleombudsman.nl/nieuws/2015/overheid-moet-gedupeerden-kentekenfraude-helpen, 16 januari 2015.

De Nationale Ombudsman (2013). *De burger gaat digitaal*. Bureau Nationale Ombudsman.

EFF. 'FBI's Next Generation Identification Biometrics Database'. https://www.eff.org/foia/fbis-next-generation-identification-biometrics-database, [z.j.].

Est, R. van (2014). 'De Mens als strijdtoneel'. In: *Christen Democratische Verkenningen*, nr. 3 (pp. 79-89).

Est, R. van (2012). 'Denk goed na voor je een [sic] 'even' een foto op internet plaatst'. http://www.trouw.nl/tr/nl/4328/Opinie/article/detail/3275963/2012/06/23/Denk-goed-na-voor-je-een-even-een-foto-op-internet-plaatst.dhtml, 23 juni 2012.

EPIC (2014). 'EPIC Prevails in Case Against FBI About Next Generation Identification'. https://epic.org/2014/11/epic-prevails-in-case-against-.html, 6 november 2014.

FBI. 'Next Generation Identification'. http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi, [z.j. (a)].

FBI. 'Integrated Automated Fingerprint Identification System'. http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis, [z.j. (b)].

Friedman, B. (1996). 'Value-sensitive design'. In: *Interactions* 3, no. 6, pp. 16-23.

Grijpink, J. (2001). 'Biometrics and Privacy'. In: *Computer law and security report* 17, no. 3, pp. 154-160.

Haney, J. (2014). 'FacialNetwork Releases New Demo Of Facial Recognition App NameTag On Google Glass, Receives Cease And Desist From Facebook'. http://www.prnewswire.com/news-releases/facialnetwork-releases-new-demo-of-facial-recognition-app-nametag-on-google-glass-receives-cease-and-desist-from-facebook-274649581.html, 10 september 2014.

Hill, K. (2012). 'Sen. Al Franken Grills Facebook and the FBI Over Their Use Of Facial Recognition Technology'. http://www.forbes.com/sites/kashmirhill/2012/07/18/sen-al-franken-grills-facebook-and-the-fbi-over-their-use-of-facial-recognition-technology/, 18 juli 2012.

IBIA (2014). 'IBIA Privacy Best Practice Recommendations For Commercial Biometric Use'. http://www.ibia.org/data/IBIA-Privacy-Best-Practice-Recommendations.pdf, augustus 2014.

Information age (2011). 'Facebook facial recognition breaks EU law – regulator'. http://www.information-age.com/technology/security/1669438/facebook-facial-recognition-breaks-eu-law---regulator, 11 november 2011.

Introna, L., & H. Nissenbaum (2010). *Facial Recognition Technology A Survey of Policy and Implementation Issues*. Lancaster: Lancaster University Management School.

Ionescu, D. (2010). 'Is Microsoft's Kinect Racist?' http://www.pcworld.com/article/209708/Is_Microsoft_Kinect_Racist.html, 4 november 2010.

Jacobi, A. et al. (2012). *Security of eGovernment Systems. Case Study Report.* http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Security%20of%20eGovernment%20-%20Case%20Study.pdf

Jain, A.K., S.C. Dass & K. Nandakumar (2004). 'Soft biometric traits for personal recognition systems'. In: *Proceedings of International Conference on Biometric Authentication*, pp. 731-738.

Keijzer, R. (2014). 'Facebook gaat toch weer gezichten scannen'. http://www.automatiseringgids.nl/nieuws/2014/36/facebook-gaat-toch-weer-gezichten-scannen, 2 september 2014.

Luchtvaartnieuws (2014). 'Eind dit jaar al in "Happy Flow" door controles Aruba Airport'. http://www.luchtvaartnieuws.nl/nieuws/categorie/3/airports/eind-dit-jaar-al-in-happy-flow-door-controles-aruba-airport, 19 mei 2014.

McGee, M. (2014). 'NameTag Replies to Franken: We'll Discuss Delaying Our App'. http://glassalmanac.com/nametag-replies-franken-well-discuss-delaying-app/2472/, 7 februari 2014.

NIST (2013). 'Face Recognition Vendor Test 2013'. http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf, 2013.

Noldus. *FaceReader methodology.* White paper. [z.j.].

Parks, R. & E. Mead (2014). 'A Socio-Technical Approach to Biometric Technology Deployment in Schools'. In: *Twentieth Americas Conference on Information Systems, Savannah*.

Ploeg, I. van der (2011). 'Normative assumptions in biometrics. On bodily differences and automated classifications'. In: *Innovating Government*,pp. 29-40. TMC Asser Press.

Polo, S. (2010). 'Memo From Five Years From Now: Anti-Facial Recognition Makeup'. http://www.themarysue.com/anti-facial-recognition/, 24 april 2010.

Philips. 'Philips vital signs camera'. http://www.vitalsignscamera.com/index.html [z.j.].

Persbericht Al Franken (2014). 'Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People'. http://www.franken.senate.gov/?p=press_release&id=2699, 5 februari 2014.

Ramachandran, V. (2013). 'Facial-Recognition App Can Help Identify Missing Children'. http://mashable.com/2013/05/31/chinese-missing-kids-app/, 1 juni 2013.

Risen, J. & L. Poitras (2014). 'N.S.A. Collecting Millions of Faces From Web Images'. http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=1, 31 mei 2014.

Rooij, J. de (2011). 'E-gates Schiphol verlagen veiligheid'. http://www.computable.nl/artikel/nieuws/security/4123595/1276896/egates-schiphol-verlagen-veiligheid.html, 31 augustus 2011.

Singer, N. (2014). 'When No One Is Just a Face in the Crowd'. http://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html?_r=0, 1 februari 2014.

Snijder, M., L. Kool & G. Munnichs (2013). 'Case study: E-passport'. In: Conference report STOA project 'security of e-Government systems'. http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Sec%20of%20eGovernment%20-%20Conference%20Report.pdf.

Vincent, J. (2014).'NameTag: Facial recognition app scans faces for dating profiles, criminal background'. http://www.independent.co.uk/life-style/gadgets-and-tech/facial-recognition-app-scans-strangers-faces-for-dating-profiles-criminal-background-9049568.html, 9 januari 2014.

Virgin Atlantic (2014). 'Virgin Atlantic Introduces Google Glass Trial'. https://blog.virgin-atlantic.com/t5/Our-Style/Virgin-Atlantic-Introduces-Google-Glass-Trial/ba-p/21547#.VGsohzTF-E4, februari 2014.

Woodward, J. (2005). 'Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism'. In: *Military Review*.http://www.rand.org/pubs/reprints/RP1194.html.

Bijlage 1 Geraadpleegde experts

- Bart Custers (23-09-2014). Afdelingshoofd *Afdeling Criminaliteit, Rechtshandhaving en Sancties, WODC, Ministerie van Veiligheid en Justitie* (telefonisch).
- Max Snijder (02-10-2014). CEO en eigenaar *European Biometrics Group.*
- Ricardo van der Valk (05-10-2014). Reclamepsycholoog *Panteia.*
- Ruud van Munster (06-10-2014). Eigenaar *Van Munster Advies*; senior consultant *BPI Connected Identification.*
- Frouke Albers (14-10-2014). Woordvoerder *RET* (telefonisch).
- Robin Hermann (16-10-2014). Hoofd Ontwikkeling *VDG Security BV* (per e-mail).
- René Lewis (27-10-2014). Kwaliteitscoördinator forensische opsporing *Politie Amsterdam-Amstelland.*
- Arnout Ruifrok (30-10-2014). Teamleider forensische biometrie *Nederlands Forensisch Instituut.*
- Eugène de Geus (30-10-2014). Algemeen directeur *SmarterVision* (telefonisch).
- Henri Apeldoorn (30-10-2014). Operationeel expert GCP *Wijkpolitie Rotterdam Centrum* (telefonisch).
- Hans Theuws (04-11-2014). Product Manager *Noldus.*

Bijlage 2: Vragenlijst rondetafeldiscussie

1. Hoe kijkt de beveiligingswereld naar de ontwikkeling dat databases groter en beter gekoppeld worden?

2. Hoe dicht bij onze gedachten en gevoelens kan emotieherkenning komen?

3. Welke specifieke technische ontwikkelingen zullen invloed hebben op de maatschappelijke issues in deel 3?

4. Wat doen de ontwikkelingen van gezichts- en emotieherkenning met onze identiteit?

5. In hoeverre is de huidige en/of toekomstige wetgeving toegerust om de genoemde maatschappelijke gevolgen in goede banen te leiden?

6. In hoeverre ligt er een taak voor ontwikkelaars om de maatschappelijke onrust weg te nemen?

7. In hoeverre wordt het debat over deze vraagstukken in de biometrie al gevoerd en waar liggen de mogelijkheden voor verder debat?

Bijlage 3 Verslag rondetafelbijeenkomst

Op uitnodiging van het Rathenau Instituut kwamen zeven experts bijeen voor een rondetafeldiscussie over de opkomst van technologieën voor gezichts- en emotieherkenning in de bibliotheek van het observatorium in Utrecht. De aanwezige experts vertegenwoordigden het ontwikkelings- en implementatie-perspectief, het ethische en het juridische perspectief:

- René Lewis: kwaliteitscoördinator forensische opsporing bij Politie Amsterdam-Amstelland.
- Els Kindt: universitair docent en onderzoeker bij The Interdisciplinary Centre for Law & ICT aan de KU Leuven.
- Max Snijder: CEO en eigenaar van de European Biometrics Group.
- Eugène de Geus: algemeen directeur van SmarterVision.
- Ricardo van der Valk: expertisemanager merk & communicatie bij Blauw Research.
- Irma van der Ploeg: senior onderzoeker Science and Technology Studies bij UNU-MERIT.
- Ruud van Munster: senior consultant bij Van Munster Advies, senior consultant bij BPI Connected Identification en docent aan Hogeschool Utrecht.

Het doel van de bijeenkomst was enerzijds om de voorlopige resultaten van het literatuuronderzoek en van de eerder afgenomen interviews te valideren,[82] en anderzijds om met elkaar in gesprek te gaan over mogelijke oplossingen voor negatieve maatschappelijke gevolgen van de opkomst van deze technologieën. De bijeenkomst was gestructureerd aan de hand van zeven vragen die vooraf onder de deelnemers waren uitgezet. De expert die vraag 1 toegestuurd had gekregen, gaf een eerste reactie. Daarna volgde de discussie met de overige deelnemers. Op dezelfde manier kwamen ook de andere vragen aan bod.Tot slot discussieerden de deelnemers over maatregelen die nu urgent zijn: wie moet er op welke manier ingrijpen?

Het verslag hieronder volgt de structuur van de bijeenkomst. De belangrijkste resultaten van de discussie zijn verwerkt in het rapport. Dit verslag is bedoeld als achtergrondinformatie.

82 Met hen en anderen; zie bijlage 1 voor alle geraadpleegde experts.

Vraag 1: Hoe kijkt de beveiligingswereld naar de ontwikkeling dat databases groter en beter gekoppeld worden?

René Lewis - kwaliteitscoördinator bij de politie Amsterdam -, beantwoordt de vraag vanuit zijn werkveld, de forensische opsporing. In dat werkveld bestaat er veel behoefte aan correcte, grote en goed gekoppelde databases, zodat een individu op basis van beperkte informatie toch geïdentificeerd kan worden. De kwaliteit van de aangeboden beelden is vooralsnog bedroevend. Door slechte belichting en verkeerde camerastandpunten raken afbeeldingen van gezichten vertekend.

Aan de andere kant ziet hij ook nadelen aan deze ontwikkeling: 'Hoe groter de databases, hoe groter het risico dat er dingen in zitten die je niet mag hebben.' Hij doelt hiermee op een categorie 'restinformatie': informatie die opgeslagen wordt terwijl men op zoek is naar iets anders. Bij deze restinformatie kan het ook om personen gaan. Op die manier komen mensen die niet direct verdacht worden toch in databases terecht. Over deze ontwikkeling maakt René Lewis zich zorgen: 'Bbij de politie zijn hier op papier misschien wel protocollen voor, maar deze worden in de praktijk nog niet altijd opgevolgd.'

Juridisch expert Els Kindt valt hem bij en benadrukt de complexiteit: in een onderzoek naar de hoeveelheid databases die er wettelijk worden bijgehouden, bleek dat minder dan de helft daadwerkelijk legaal was. Max Snijder – CEO en eigenaar van de European Biometrics Group – vindt het ook een urgente kwestie, omdat meer data en meer technische capaciteit ook kunnen uitnodigen tot een andere strategie. Hij noemt de Verenigde Staten als voorbeeld, waar Global Identity Dominance wordt nagestreefd. Men wil iedereen op ieder moment kunnen identificeren.

Eugène de Geus van SmarterVision geeft aan dat er technologische oplossingen zijn, die ervoor zorgen dat er in de praktijk geen informatie wordt gevonden die niet gebruikt mag worden. Hierbij kun je denken aan het automatiseren van de bewaartijd. Deze 'schil' over de data kan privacy waarborgen. René Lewis wijst echter op de ingewikkelde wetgeving die zoveel uitzonderingen bevat, dat dit in de praktijk lastig te programmeren is.

Vraag 2: Hoe dicht bij onze gedachten en gevoelens kan emotieherkenning komen?

Ricardo van der Valk – implementatiedeskundige van emotieherkenning – vindt dat de techniek van emotieherkenning al heel ver is. De validatie van de techniek is achter de rug en de universele emoties zijn zichtbaar: 'Pokerfaces bestaan niet meer.'

Irma van der Ploeg – senior onderzoeker Science and Technology Studies – betwijfelt of de technologie voor emotieherkenning in alle gevallen onze ware emoties kan vaststellen. We zouden hiermee voorbijgaan aan de culturele en individuele verschillen tussen mensen: 'Betekent een glimlach dat je blij bent of dat je gêne voelt?'

Ricardo van der Valk geeft toe dat culturele verschillen en etnische classificaties een uitdaging vormen voor de software, maar brengt wel naar voren dat er verschillende modellen bestaan voor bepaalde groepen mensen. Zo bestaan er speciale modellen voor oudere mensen en voor Aziaten. De software geeft ons echter niet altijd voldoende informatie: 'Ik zet emotieherkenning nooit alleen in – zonder andere informatie.'

Max Snijder stelt de discussie in een breder kader door te benadrukken dat er bij biometrie vaak een groot verschil is tussen de echte prestaties en de claims over deze prestaties.

Naar aanleiding van de vraag over emotieherkenning ontstaat er een discussie over de mate waarin gezichts- en emotieherkenning te vergelijken zijn. Max Snijder opent de discussie met de stelling dat deze twee technieken 'als appels en peren zijn'. Els Kindt erkent dat er grote verschillen bestaan tussen gezichts- en emotieherkenning; zo gaat het bij gezichtsherkenning vaak om identificatie, terwijl het inzetten van emotieherkenning niet altijd impliceert dat iemand geïdentificeerd wordt. Aan de andere kant lijken de technieken wel op elkaar. Emotieherkenning kan ook identificatie mogelijk maken. Ook heb je te maken met vergelijkbare gevolgen; bij beide technologieën verliezen we de controle over wat er met onze biometrische gegevens gebeurt. In deze context benadrukt zij dat we de risico's van emotieherkenning tijdig in kaart moeten brengen, omdat de techniek niet stil blijft staan: 'Eemotieherkenning is als het jongere broertje of zusje van gezichtsherkenning.'

Vraag 3: Welke specifieke technische ontwikkelingen zullen invloed hebben op de maatschappelijke issues in deel 3?

Ruud van Munster – biometrisch expert – maakt eerst een onderscheid tussen continue verbeteringen en schoksgewijze ontwikkelingen. Met de eerste categorie doelt hij op een gestage verbetering van de algoritmes in gezichtsherkenningssoftware. De tweede categorie behelst ontwikkelingen waardoor de prestatie van gezichtsherkenning ineens met sprongen vooruit gaat. Een goed voorbeeld hiervan is de inzet van neurale netwerken, zoals gebeurt bij de DeepFace-software van Facebook: 'Dit soort technieken vormen een mogelijke opmaat naar gezichtsherkenning onder moeilijke omstandigheden zonder medewerking van de geobserveerde personen.' Een andere ontwikkeling die Ruud van Munster belangrijk acht is de multimodale biometrie, waarbij men ook kijkt naar het haar, de oren, de textuur van de huid en de bloedvaten onder de

huid. Ruud van Munster benadrukt dat deze technieken elkaars zwakke plekken kunnen opvangen: 'Daarmee is het denkbaar dat we de stap zetten van gezichtsherkenning naar hoofdherkenning.'

Ruud van Munster wijst ook op een aantal veranderingen buiten het ontwikkelingsdomein, zoals de verbreiding van de techniek: 'Het is verbazingwekkend hoeveel hightech er opensource beschikbaar is.' Verder zal gezichtsherkenning door de opkomst van de smartphone in toenemende mate in de cloud plaatsvinden.

Naar aanleiding van de ontwikkeling van neurale netwerken ontstaat er een discussie tussen Ruud van Munster en Eugène de Geus over het idee dat de technologie verandert in een black box. Ruud van Munster is van mening dat wij mede door de ontwikkeling van neurale netwerken steeds minder weet hebben van de basis waarop de technologie tot bepaalde beslissingen komt. Eugène de Geus brengt daar tegenin dat neurale netwerken als techniek best wel simpel en duidelijk zijn. We kunnen het weliswaar wiskundig niet volgen, maar we begrijpen de aanpak wel: 'Het is geen zwarte magie.' Ruud van Munster blijft bij zijn standpunt dat een neuraal netwerk een beslissingsstrategie volgt die wij niet meer kunnen navolgen.

Vraag 4: Wat doen ontwikkelingen van gezichts- en emotieherkenning met onze identiteit?

Irma van der Ploeg geeft aan dat er een groot verschil bestaat tussen de definitie van identiteit in de context van datasystemen en het begrip van identiteit in de context van sociale wetenschappen. Waar onze identiteit in de eerste context bepaald wordt door datasets die leiden tot identificatie, is volgens de sociale wetenschappen ieder antwoord op de vraag 'wie ben je?' deel van onze identiteit. Irma van der Ploeg waarschuwt voor de trend waarin identiteit gemechaniseerd wordt: 'Onze identiteit is ongrijpbaar – we moeten die niet versmallen tot een identificatietechniek.' De versmalde definitie van identiteit zien we in steeds meer beleidsstukken terug, door de opkomst van informatiesystemen.

In het geval van de categorisatietoepassingen wijst Irma van der Ploeg op de controverse rond de definitie van etniciteit. Er bestaat binnen de sociale wetenschappen geen overeenstemming over wat etniciteit is, en hoe men etniciteit moet classificeren. Omdat de techniek een black box is, weten wij niet hoe die ons beoordeelt en classificeert. We krijgen daarmee een identiteit opgeplakt, zonder dat er overeenstemming is over wat deze identiteit behelst.

Vraag 5. In hoeverre is de huidige en/of toekomstige wetgeving toegerust om de genoemde maatschappelijke gevolgen in goede banen te leiden?

Els Kindt legt uit dat bij gezichts- en emotieherkenning de algemene dataprotectiewetgeving van toepassing is. Binnen die wetgeving hebben nationale wetgevers wel nagedacht over biometrie, maar de meeste EU-lidstaten kennen weinig expliciete regelgeving met betrekking tot biometrie. Enkele nieuwe lidstaten vormen hierop een uitzondering; zij vermelden biometrische data als persoonsgegevens. Daarnaast ligt er in Frankrijk een voorstel bij het parlement om biometrie heel strikt te regelen.

Zij ziet het als een uitdaging om deze wetgeving aan te passen om de risico's in te dammen. Een belangrijke stap in dit proces is om de functionaliteiten van de technologie te bekijken en van een kader te voorzien: 'Wat kan de techniek, wat zijn de daaraan verbonden functionaliteiten, en welke risico's hangen daarmee samen?' Een voorbeeld van een risico is het verlies van anonimiteit; de wetgever moet bekijken of het wenselijk is dat iedereen geïdentificeerd kan worden. Verder geeft zij aan dat we een onderscheid moeten maken in de discussie; regulering kan verschillend zijn voor gebruik van biometrie door de overheid, door marktpartijen of door individuele burgers.

Max Snijder vult aan dat de reguleringstaak bemoeilijkt wordt door het feit dat de nieuwe dataprotectiewet niet de definitie van biometrie volgt zoals die is vastgesteld door de International Organization for Standardization (ISO). Ook biedt de nieuwe wetgeving weinig oplossingen voor de regulering van biometrie. Alleen als het verzamelen van data een groot risico vormt, wordt er een *impact assessment* geëist. Max Snijder is echter van mening dat biometrie altijd gepaard gaat met grote risico's en dat snelle actie daarom vereist is.

Vraag 6: In hoeverre ligt er een taak voor ontwikkelaars om de maatschappelijke onrust weg te nemen?

Eugène de Geus vindt dat er zeker een taak ligt voor ontwikkelaars, maar dat deze niet anders is dan voor ieder ander. Ontwikkelaars hebben een plek aan tafel nodig in dit debat, omdat het realisme in sommige discussies ontbreekt. Toch vindt hij dat ontwikkelaars alleen hun verantwoordelijkheden kunnen nemen als er een gelijk speelveld is: de concurrenten zouden zich aan dezelfde afspraken moeten houden.

Op de vraag of privacy by design een concurrentievoordeel kan zijn, antwoord Eugène de Geus bevestigend. Hij voegt toe dat dit wel betekent dat het bedrijf maar een deel van de markt kan bedienen, omdat zijn klanten soms expliciet om meer mogelijkheden vragen die vervolgens de privacy kunnen schenden.

Max Snijder vult aan dat de publieke opinie belangrijker wordt bij private toepassingen. De publieke opinie is nu nog niet zo sterk ontwikkeld dat die op de markt gehoord wordt. Daarom ziet hij meer in regulering.

Ruud van Munster formuleert het nog sterker. Hij vindt dat men de ontwikkeling van software niet kan stoppen: 'We hebben juist meer regulering en handhaving nodig aan de kant van het *gebruik*.'

Vraag 7: In hoeverre wordt het debat over deze vraagstukken in de biometrie al gevoerd en waar liggen de mogelijkheden voor verder debat?

Max Snijder vindt dat de markt nog totaal niet bezig is met een debat over maatschappelijk verantwoord ondernemen. Zo'n debat kan alleen van de grond komen als het publiek daar om vraagt. De wetgever zal dan ook eerder in actie komen.

Frans Brom – hoofd Technology Assessment aan het Rathenau Instituut – vat de discussie over de laatste twee vragen samen: we kunnen alleen maatschappelijk verantwoord ondernemen, als er ook maatschappelijk verantwoord consumeren bestaat.

Wie is nu verantwoordelijk voor wat?

Allereerst benadrukken de deelnemers de urgentie van deze discussie. Max Snijder verwoordt die als volgt: 'Het debat moet gevoerd worden op de goede plek, zoals bij het Rathenau Instituut. Je voelt je klant, maar je bent het product. Het gat tussen de blije technologie en wat er feitelijk gebeurt is veel te groot. Aan de achterkant gebeuren er dingen waar wij geen weet van hebben. Zijn deze verdienmodellen wel duurzaam? Waar is de opt-outregeling?'

Behalve op het belang van wetgeving en verantwoord ondernemen, wijzen de deelnemers op het belang van structurele aandacht voor dit onderwerp in het onderwijs. Middelbare scholieren en studenten zouden onder andere moeten leren dat techniek niet neutraal is of louter 'een leuk extraatje'. In het hoger onderwijs zouden de specifieke risico's per professie in kaart gebracht moeten worden. Zo zou er in de studie rechten aandacht besteed moeten worden aan dataprotectie. De deelnemers zijn het erover eens dat de dialoog tussen de alfa- en bètawetenschappers bevorderd moet worden.

Wie was Rathenau?

Het Rathenau Instituut is genoemd naar professor dr. G.W. Rathenau (1911-1989). Rathenau was achtereenvolgens hoogleraar experimentele natuurkunde in Amsterdam, directeur van het natuurkundig laboratorium van Philips in Eindhoven en lid van de Wetenschappelijke Raad voor het Regeringsbeleid. Hij kreeg landelijke bekendheid als voorzitter van de commissie die in 1978 de maatschappelijke gevolgen van de opkomst van micro-elektronica moest onderzoeken. Een van de aanbevelingen in het rapport was de wens te komen tot een systematische bestudering van de maatschappelijke betekenis van technologie. De activiteiten van Rathenau hebben ertoe bijgedragen dat in 1986 de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA) werd opgericht. NOTA is op 2 juni 1994 omgedoopt in Rathenau Instituut.

Verbeterde camera's, slimmere software en grotere databases maken gezichts- en emotieherkenningstechnologie steeds preciezer. Steeds meer instanties, bedrijven en particulieren maken gebruik van de nieuwe mogelijkheden die deze verbeteringen bieden. Opsporingsdiensten kunnen bijvoorbeeld beter criminelen op straat herkennen. Aanbieders van sociale media kunnen automatisch hun gebruikers identificeren.

Maar wat betekent de inzet van deze technologie voor de maatschappij? Wat valt er uit de intieme gegevens uit ons gezicht af te lezen? Kunnen we nog anoniem over straat? Welke diensten worden op basis van deze technologie aangeboden en wat zijn de gevolgen voor verschillende groepen burgers als leeftijd, sekse en etniciteit automatisch uitgelezen worden?

In *Dicht op de huid* verkent het Rathenau Instituut de ontwikkeling van gezichts- en emotieherkenning en de mogelijke maatschappelijke betekenis ervan. Door verbeteringen in de techniek nemen de reikwijdte en de mogelijke impact voor de maatschappij snel toe. Hoe zorgen we ervoor dat deze technologie ons niet te dicht op de huid komt?

ISBN 978-90-77364-67-3