Beter beschermd tegen biometrie

Joost Gerritsen, Jurriën Hamer, Linda Kool & Petra Verhoef[*]

Samenvatting

Op steeds meer plekken in de samenleving worden kenmerken van het lichaam en het gedrag, zoals gezichten, stemmen en emoties, digitaal verzameld en verwerkt. Het gaat om intieme gegevens die gevoelige informatie kunnen blootleggen, bijvoorbeeld over iemands gezondheid, of waarmee iemand op afstand te identificeren is. In deze bijdrage richten we ons op biometrische toepassingen in de publieke sector en publieke ruimte. We laten zien dat met het groeiende aantal toepassingen het risico ontstaat dat fundamentele burgerrechten onvoldoende worden gewaarborgd. We betogen dat deze risico's dermate groot zijn dat extra wettelijke bescherming nodig is. We pleiten voor een wettelijk verbod op het gebruik van biometrische gegevens voor het identificeren van personen in de publieke ruimte en een vergunningsplicht voor gevallen waarin gebruik van de technologie voor verificatie op zijn plaats kan zijn.

1 Inleiding

Biometrische toepassingen worden in de publieke sector al vele jaren gebruikt, met name in de opsporing. Via vingerafdrukken en DNA kan de politie bijvoorbeeld trachten een dader te identificeren. De laatste jaren zien we dat de politie gebruik gaat maken van nieuwe biometrische technieken, zoals gezichts-[1] en stemherkenning.[2] In dit artikel richten we onze blik echter op toepassingen buiten het traditionele opsporingsdomein, vaak gericht op toegangscontrole. Zo loopt op Schiphol een proef met gezichtsherkenning om snel je identiteit te verifieren, zodat je soepel langs de controles kunt.[3] In zwembaden wordt naar je vingerafdruk gevraagd om te kunnen controleren of je op de lijst met raddraaiers staat.[4] Ook winkels experimenteren met het gebruik van gezichtsherkenning en andere biometrische toepassingen. Op deze manier worden op steeds meer plekken onze vingerafdrukken, gezichten en stemmen vastgelegd.

De keerzijde van biometrische toepassingen vinden we als overheden het gebruiken om burgers te volgen en hun gedrag te controleren. In het Chinese Xinjiang vindt massasurveillance plaats, onder meer door middel van camera's met gezichtsherkenning, DNA-scans, vingerafdrukken en irisscans (*Kamerstukken II* 2019/20, 35207, nr. 32). Maar ook in ons land wordt gezichtsherkenning toegepast en worden vingerafdrukken gescand. Biedt de huidige wetgeving burgers vol-

* Mr. Joost Gerritsen is advocaat bij Legal Beetle advocatuur. Dr. mr. Jurriën Hamer is onderzoeker bij het Rathenau Instituut. Linda Kool MSc MA is themacoördinator bij het Rathenau Instituut. Dr. ir. Petra Verhoef is themacoördinator bij het Rathenau Instituut.

doende bescherming? Of kunnen dergelijke 'Chinese toestanden' ook in Nederland voorkomen? Hoe waarborgen we fundamentele rechten van burgers?
Voor een beantwoording van deze vragen brengt dit artikel het gebruik van biometrische technologie in zowel de publieke ruimte als de publieke sector in kaart en analyseren we de wettelijke bescherming binnen deze domeinen. We zullen betogen dat deze bescherming op dit moment onvoldoende is. Met name het gebruik van biometrische gegevens voor identificatie brengt risico's naar voren. De informatiebronnen – gelaat, vingerafdruk of stem – bevatten zeer gevoelige gegevens die tegen je gebruikt kunnen worden, zonder dat je het weet. Juist in de publieke ruimte of publieke sector is het moeilijk voor burgers om zich aan biometrische surveillance te onttrekken. Wie naar buiten gaat, belandt immers al snel in de publieke ruimte of heeft de overheid nodig om essentiële zaken te regelen.
We starten dit artikel met het definiëren en afbakenen van de centrale begrippen publieke ruimte, publieke sector en biometrie, en maken onderscheid tussen verschillende typen biometrische toepassingen. Dan bespreken we diverse biometrische toepassingen in de publieke ruimte en sector. Vervolgens beschrijven we de huidige wettelijke bescherming en analyseren we waar risico's met het oog op het waarborgen van fundamentele rechten ontstaan. We doen dit op basis van studies van het Rathenau Instituut naar verschillende vormen van biometrie, waaronder gezichtsherkenning (Rathenau Instituut, 2015), spraaktechnologie (Rathenau Instituut, 2020a) en de reactie op de Verzamelwet gegevensbescherming (Rathenau Instituut, 2020b). In de conclusie betogen we dat de risico's voor het individu en de samenleving dermate groot zijn, dat een wettelijk verbod op het gebruik van biometrische gegevens voor het identificeren van personen in de publieke ruimte op zijn plaats is. Voor overige gevallen waarin gebruik van de technologie op zijn voor verificatie plaats is, dient een vergunningsplicht te worden ingevoerd. Tot slot dienen we ons te bezinnen op gevoelige gegevens die gepaard kunnen gaan met biometrische toepassingen, zoals gegevens over onze emoties en ons sentiment, die vooralsnog weinig wettelijke bescherming genieten.

Begripsafbakening

- *Publieke ruimte en publieke sector*

Onder 'publieke ruimte' verstaan we vrijwel hetzelfde als 'openbare plaatsen' zoals die onder de Wet openbare manifestaties vallen. Dit zijn plaatsen die openstaan voor het publiek, waar iedereen vrij is om te komen, te vertoeven en te gaan zonder meldings- of toestemmingsplichten of heffing van toegangsprijzen. Denk aan de straat, de weg, maar ook aan plaatsen die als het 'verlengde' van de weg kunnen worden gezien, zoals openbare parken en vrij toegankelijke gedeelten van overdekte passages van winkelcentra, stationshallen of Schiphol waaronder begrepen de grenzen met aanpalende niet-openbare plaatsen. Zowel de overheid als een bedrijf of particulier kan een 'openbare plaats' in eigendom hebben.
Als het gaat om de inzet van biometrische technologie door de 'publieke sector' richten we ons nadrukkelijk niet op politiewerk of anderszins strafvorderlijk onderzoek, ongeacht of er sprake is van een openbare plaats, maar aan andere

gevallen waarin de overheid een rol speelt. Denk aan biometrisch gegevensgebruik voor het verkrijgen van toegang tot IT-systemen van de overheid, of tot overheidsgebouwen als gemeentehuizen en locaties die de overheid bezit of beheert zoals gemeentelijke zwembaden. Soms ligt de inzet van de biometrische technologie in het verlengde van een publieke taak, zoals gemeentelijke handhaving, maar dat hoeft niet.

- *Biometrische technologie*[5]

Biometrie gaat over het verzamelen en verwerken van iemands unieke lichaams- of gedragskenmerken, vaak met het doel om die persoon te identificeren of de identiteit te controleren. Dat kan gebeuren op basis van lichamelijke kenmerken zoals vingerafdrukken of een irisscan. De bronnen van biometrische data omvatten zowel fysieke als fysiologische en gedragselementen.
Er zijn twee hoofdcategorieën van technieken: verificatie en identificatie. Bij *verificatie* wordt de technologie ingezet met als doel te controleren of een persoon is wie hij of zij claimt te zijn. Wanneer iemand zijn vingerafdruk toont aan een scanner, vergelijkt het systeem deze afdruk met een eerder opgeslagen sjabloon (*template*). De informatie kan lokaal worden opgeslagen (bijvoorbeeld op een pasje of een smartphone) of in een algemene database. Om de identiteit te verifiëren hoeft het systeem maar één sjabloon te vergelijken met de 'live' vingerafdruk. Daarom wordt verificatie ook wel 1 op 1-vergelijking genoemd.
Bij *identificatie* vergelijkt het systeem een 'live' vingerafdruk of beeld met vingerafdrukken of beelden in een database. Omdat het 'live' biometrische kenmerk met de hele database wordt vergeleken, wordt identificatie ook wel een 1 op N-vergelijking (*one to many*) genoemd. Je kunt met identificatie bepaalde groepen een 'voorkeursbehandeling' geven, zoals de proef op Schiphol. Of je kunt groepen uitsluiten, zoals in zwembaden of voetbalstadions om notoire raddraaiers de toegang te ontzeggen.
Er zijn ook andere toepassingen denkbaar, waaronder emotieherkenning. Bij emotieherkenning worden de gezichtsuitdrukkingen of andere kenmerken 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.

2 Hoe wordt biometrie ingezet?

Biometrische systemen zijn niet nieuw. Sterker nog, vingerafdrukken worden al meer dan honderd jaar gebruikt voor verificatie en identificatie, en gezichtsherkenning al zeker tientallen jaren. Dit waren vroeger arbeidsintensieve processen, maar dankzij de rekenkracht van computers is dat veranderd. De laatste jaren is de software die benodigd is voor biometrische analyse drastisch verbeterd, onder meer met behulp van *deep learning*-technologie, en zijn de kosten gedaald. Verder worden er de afgelopen jaren ook steeds meer verschillende kenmerken gebruikt, waaronder het gezicht en stemgeluid, maar ook oorschelpen, ademhaling en hartslag. Ook unieke gedragskenmerken kunnen worden gebruikt, zoals houding,

looppatroon of de manier waarop we typen. Een andere trend is dat deze toepassingen mensen van steeds grotere afstanden kunnen herkennen. Er zijn commerciële toepassingen die mensen op meer dan 15 meter afstand kunnen herkennen, en er is militaire technologie die mensen herkent op meer dan 1 kilometer afstand. Ook bestaat er infraroodtechniek die op 150 meter afstand iemand kan identificeren op basis van diens hartslag.[6]

Deze trends maakten het in de afgelopen twee decennia mogelijk om op allerlei plekken biometrische systemen in te zetten. Wordt in Nederland begin jaren 2000 nog gefilosofeerd over de mogelijkheden,[7] zes jaar later verschijnen de eerste krantenartikelen over de inzet van vingerafdrukscans in zwembaden en gezichtsherkenning in winkels.[8] Anno 2020 lopen er op diverse plekken proeven met gezichtsherkenning, zoals in winkels, op Schiphol, in voetbalstadions en natuurgebieden.[9] Regelmatig stuit dit op weerstand en worden proeven stopgezet.

Ook gemeenten gebruiken biometrische toepassingen. Zo voerde in 2018 de gemeente Zwolle als eerste documentscanners en gezichtsherkenning in bij de aanmeldzuil van de publieksbalie.[10] Dit werd al gebruikt bij het migratieloket. Nu wordt bij de bezoeker standaard verificatie toegepast nog voordat een ambtenaar van Burgerzaken de betreffende persoon spreekt. Tijdwinst en efficiëntie zijn hierbij de belangrijkste overwegingen, omdat de baliemedewerkers voorheen met het blote oog de identiteitsbewijzen moesten controleren op echtheid. Een andere gemeente zet gezichtsherkenning in als iemand een rijbewijs of paspoort aanvraagt.[11]

Over de grens zijn er eveneens interessante voorbeelden te vinden. Zo past de belastingdienst van Nieuw-Zeeland spraakverificatie toe om burgers en bedrijven informatie te laten opvragen of gegevens te wijzigen.[12] In het Verenigd Koninkrijk ging dit mis. De Britse belastingautoriteit, Her Majesty's Revenue & Customs, bleek vanaf 2017 miljoenen stemopnames te hebben gemaakt van bellers naar de belastinglijn. De opnames werden gebruikt voor *voice prints* waarmee de beller in de toekomst kon worden herkend. Bellers werd in het telefoongesprek geautomatiseerd gevraagd of zij wilden deelnemen aan dit Voice ID-programma, maar er bestond geen gemakkelijke manier om hiervoor *niet* te kiezen. Uiteindelijk oordeelde de Britse privacytoezichthouder ICO dat de stemopnames illegaal zijn verzameld en dat de database vernietigd moest worden.[13] Het zou wellicht wel hebben gemogen als er correct om toestemming was gevraagd. In Servië, een officiële kandidaat-lidstaat van de Europese Unie, worden camera's met gezichtsherkenning ingezet in Belgrado.[14] Dit past volgens de initiatiefnemers bij de 'digitale transformatie' en het is de bedoeling dat dit systeem de stad veiliger maakt. Ze gebruiken hiervoor surveillancecamera's van Chinese makelij. De vrees is dat het systeem tegen politieke tegenstanders wordt ingezet, nu deze gemakkelijk te herkennen zijn.

Marktonderzoekers verwachten dat ook het coronavirus voor een toename in het gebruik van biometrische toepassingen zal zorgen, omdat het kan helpen bij het vermijden van contact.[15] In Polen gebeurt dit al, weliswaar op een onverwachte manier. Daar moeten mensen met coronaklachten verplicht selfies maken met een app die de overheid ter beschikking stelt. Met behulp van locatiegegevens en

gezichtsherkenning ziet de overheid vervolgens of iemand in quarantaine zit. Gebeurt dit niet, dan kunnen hiervoor boetes worden opgelegd tot maximaal 6550 euro.[16]
De voorbeelden laten zien dat biometrische toepassingen voor verificatie- en identificatiedoelen vaker worden toegepast in de publieke sector en publieke ruimte. Daarbij wordt vaak gebruikgemaakt van vingerafdrukken, maar ook andere biometrische kenmerken zoals stem en gezicht worden inmiddels ingezet. Vaak genoemde redenen om biometrische toepassingen in te voeren zijn efficiëntere en betere procedures en het bevorderen van de veiligheid. Maar de toepassingen roepen ook zorgen en weerstand op met het oog op privacybescherming, anonimiteit en in vrijheid kunnen leven. Daarbij blijken diverse toepassingen niet in overeenstemming met de wettelijke kaders, en zijn diverse toepassingen door de toezichthoudende instanties als illegaal beoordeeld en stopgezet.

3 Hoe zijn biometrische gegevens wettelijk beschermd?

De Algemene Verordening Gegevensbescherming (AVG) reguleert de omgang met persoonsgegevens. Persoonsgegevens kunnen biometrische gegevens zijn, maar zijn dit niet per definitie. Persoonsgegevens betreffen informatie over geïdentificeerde of identificeerbare natuurlijke personen, zoals burgers. De AVG is overigens niet altijd van toepassing. Bijvoorbeeld als de gegevens worden gebruikt voor politiewerk of anderszins strafvorderlijk onderzoek.
Persoonsgegevens is een breed begrip. Het zijn gegevens die herleidbaar kunnen zijn naar een individu, of waarmee deze geïdentificeerd kan worden. Dat kan bijvoorbeeld een locatiegegeven zijn, of een ID-nummer, maar ook één of meer elementen die kenmerkend zijn voor de identiteit van een persoon. Dat is het geval bij biometrie. De AVG omschrijft 'biometrische gegevens' betrekkelijk nauw: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon. Op basis hiervan is eenduidige identificatie of verificatie van die persoon mogelijk. Verderop in dit artikel zullen we zien dat privacygevoelige gegevens die worden verzameld bij biometrische toepassingen, zoals gegevens over herkende emoties, niet zomaar 'bijzondere persoonsgegevens' zijn zoals de AVG dat bedoelt.
De AVG maakt onderscheid tussen gewone en bijzondere persoonsgegevens, omdat het ene persoonsgegeven gevoeliger is dan het andere. Bijzondere persoonsgegevens zijn extra gevoelig en zijn daarom onder de AVG extra beschermd. Een verkeerde behandeling ervan kan voor personen grote maatschappelijke of economische nadelen hebben, zoals discriminatie of reputatieschade. Biometrische gegevens vallen onder de categorie bijzondere persoonsgegevens, maar denk bijvoorbeeld ook aan gegevens over de gezondheid, het strafrechtelijk verleden of etnische afkomst. Bijzondere persoonsgegevens hebben met elkaar gemeen dat het in principe verboden is deze te gebruiken, tenzij uit de AVG volgt dat dit wel mag.

Naast de AVG en de Uitvoeringswet AVG is er ook de vreemdelingenwetgeving waarin voorschriften staan over biometrische gegevens gerelateerd aan gezichtsopnames en vingerafdrukken van vreemdelingen zoals vluchtelingen. Zulke gegevens komen overigens ook aan bod in andere wet- en regelgeving, bijvoorbeeld in de Paspoortwet, die onder meer voorschriften bevat over vingerafdrukken in identiteitsdocumenten. Deze wetgeving is net als de AVG het gevolg van wettelijke voorschriften vanuit de Europese Unie.

Verificatie en beveiligingsdoeleinden

Volgens de AVG mogen landen als Nederland hun eigen regels vaststellen over de omgang met biometrische gegevens.[17] Die lijken in Nederland beperkt. Nederland heeft hiervoor één artikel opgesteld in de Uitvoeringswet AVG. Dit artikel dient om het gebruik van biometrische gegevens mogelijk te maken als dit noodzakelijk is voor verificatie of beveiligingsdoeleinden.[18] Noodzakelijk betekent onder meer dat degene die de biometrische techniek wil inzetten, moet nagaan of er is voldaan aan het proportionaliteits- en het subsidiariteitsbeginsel. Proportionaliteit houdt in dat het doel in verhouding moet staan tot de (privacy)inbreuk die wordt gemaakt, en subsidiariteit betekent dat het doel niet op een andere minder nadelige, bijvoorbeeld meer privacyvriendelijke, manier kan worden bereikt. De invoerende partij zal die noodzakelijkheid moeten onderbouwen en dient de belangen af te wegen van de personen die aan de techniek onderworpen zullen worden, zoals burgers. De privacytoezichthouder, de Autoriteit Persoonsgegevens, toetst in voorkomende gevallen achteraf of de AVG en de Uitvoeringswet AVG correct zijn nageleefd.

De belangenafweging kan wisselend uitpakken. Zo is het goed voor te stellen dat biometrische toegangscontrole noodzakelijk wordt geacht in het geval van een kerncentrale, waar met het oog op de veiligheid de toegang beperkt moet zijn tot bepaalde geautoriseerde personen. Onbevoegde personen kunnen daar veel kwaad aanrichten. Maar voor de toegang tot een recreatiegebied is dit al snel disproportioneel. Volgens de Autoriteit Persoonsgegevens is in zo'n geval de noodzaak van beveiliging niet zo groot dat het geoorloofd is dat personen alleen door gebruik van biometrie toegang kunnen krijgen.

Partijen blijken dikwijls moeite te hebben met het maken van de juiste afwegingen. Zo zijn in Nederland diverse werkgevers door de rechter en de Autoriteit Persoonsgegevens teruggefloten bij de inzet van verplichte vingerafdrukscans. En hoewel biometrische identificatie door gezichtsherkenning en vingerafdrukscans bij zwembaden waarschijnlijk niet mag,[19] wordt dit nog steeds ingezet. In Zweden en Polen werden boetes opgelegd aan scholen die ontoelaatbaar gezichtsherkenning respectievelijk vingerscans toepasten voor controle op de aanwezigheid van de leerlingen en toegang tot de schoolkantine.[20] En een Franse rechtbank achtte gezichtsherkenning op twee scholen eveneens ontoelaatbaar, ook al betrof het hier een 'experiment'.[21]

Overige gebruiksdoelen

Bij andere gebruiksdoeleinden dan authenticatie of beveiliging, of als de inzet van de biometrische technologie ten behoeve van deze doelen disproportioneel is,

volgt uit de AVG en Uitvoeringswet AVG dat er toestemming moet worden gevraagd aan degenen op wie de biometrische gegevens betrekking hebben. Die toestemming moet wel 'in vrijheid' worden gegeven. Een manier om toestemming 'in vrijheid' te laten plaatsvinden, aldus de Autoriteit Persoonsgegevens, is om náást de biometrische toepassing (waarvoor toestemming wordt gevraagd) een privacyvriendelijk alternatief aan te bieden, zoals toegang met een pas waarvoor minder of geen gegevens verwerkt hoeven te worden.[22]
Het hangt af van de situatie of 'vrije toestemming' vragen mogelijk is. In een klant-aanbiedercontext is het geven van een vrije toestemming misschien denkbaar, maar in de relatie tussen burger-overheid is dat een stuk lastiger te realiseren. In die laatstgenoemde gevallen bestaat er immers een ongelijke verhouding tussen de partijen. De burger zal in de praktijk niet zo snel toestemming kunnen weigeren. Bijvoorbeeld als de weigering tot gevolg heeft dat de persoon de publieke ruimte niet mag betreden of een overheidsvoorziening niet mag gebruiken.

Tekortkomingen en bezwaren
Biometrische techniek belooft een snelle identificatie- of verificatie van personen, zonder dat de betreffende personen hiervoor iets bij zich hoeven te hebben, zoals een toegangspas. Hun lichamelijke kenmerken – zoals gelaat, stem en vingerafdruk – dragen zij immers altijd bij zich. Tegelijkertijd gaat het om gevoelige gegevens die – ook volgens de wetgever – nadere bescherming behoeven. Niet alle biometrische toepassingen kennen dezelfde bezwaren. In deze paragraaf kijken we naar verschillende biometrische toepassingen, en welke risico's met het oog op de bescherming van privacy en andere mensenrechten deze oproepen. We bespreken biometrische toepassingen voor verificatiedoeleinden en vervolgens voor identificatie.
Verificatie door middel van biometrie kan een belangrijke vorm van beveiliging zijn voor bijvoorbeeld IT-systemen met privacygevoelige gegevens, waarbij onrechtmatige toegang moet worden voorkomen. Verificatie met behulp van biometrie hoeft niet op gespannen voet met iemands privacyrechten te staan als het zo wordt ingezet dat alleen de minimaal benodigde informatie wordt gebruikt. Bijvoorbeeld om te controleren bij elektronische grenscontroles (e-gate). In het geval van e-gates op Schiphol wordt de identiteit niet prijsgegeven, maar blijft de verwerking beperkt tot verificatie: is het gezicht van de persoon voor de camera hetzelfde als dat in het paspoort? Ook bij leeftijdscontrole voor het kopen van alcohol, bijvoorbeeld op basis van vingerafdrukken, hoeft de slijter alleen te verifieren of iemand ouder dan 18 jaar is. De naam van de betreffende persoon is niet relevant.
Biometrische toepassingen die identificatie tot doel hebben, roepen meer bezwaren op, niet alleen met het oog op privacybescherming, maar ook met het oog op ongelijke behandeling van burgers, fouten in systemen en uitsluiting van burgers. Het Rathenau Instituut signaleert en waarschuwt voor dergelijke negatieve effecten in rapporten als *Dicht op de huid* (2015), *Opwaarderen* (2017) en *Hoor wie het zegt* (2020a). Zo kan het inzetten van gezichtsherkenning de overheid meer macht geven ten opzichte van haar burgers. De overheid komt meer te weten over

haar burgers en kan hen op grond daarvan bijvoorbeeld de toegang tot een gebied ontzeggen. Inaccurate systemen (en met name de zogenaamde foutpositieven, waarbij het systeem denkt dat je iemand bent terwijl dat niet zo is) kunnen het heel lastig maken voor een individu om dit te corrigeren. Het probleem van foutpositieven wordt nog groter als blijkt dat bepaalde bevolkingsgroepen in de samenleving hierdoor extra benadeeld worden, bijvoorbeeld door hen systematisch uit te sluiten van diensten. Het overal op straat kunnen identificeren kan ook leiden tot het verlies van anonimiteit op straat.
Sommige tekortkomingen en bezwaren hangen samen met het feit dat biometrische technologie imperfecte techniek betreft, ondanks de technologische vooruitgang die er is geboekt. Andere bezwaren blijven overeind staan, ook als de techniek geperfectioneerd is en bijna feilloos opereert. We lichten dat hierna verder toe.

Imperfecte techniek
Hoe goed biometrische systemen in staat zijn om mensen te herkennen, hangt onder andere af van de instellingen van het systeem en de data waarmee de systemen getraind zijn. Het Amerikaanse National Institute of Standards and Technology (NIST) concludeerde vorig jaar dat de accuraatheid van gezichtsherkenningsalgoritmes sterk verschilt per systeem. Hoewel er systemen waren die in staat waren mensen uit verschillende etnische groepen correct te identificeren, bleek dat bij het slechtste systeem zwarte vrouwen tot honderd keer meer kans hadden dan blanke mannen om verkeerd geïdentificeerd te worden (NIST, 2019). Deze systemen bleken getraind met een dataset met voornamelijk blanke mannen, waardoor er bij andere groepen meer fouten optraden. Vergelijkbare fouten zien we optreden bij stemherkenning,[23] bij gezichtsherkenning op smartphones[24] en recent bij het veranderen van de achtergrond tijdens videovergaderen, waarbij dit bij zwarte mensen niet goed gaat.[25]
Omdat diverse systemen onder meer donkere gezichten minder goed herkennen, is de kans dat mensen met een donkere huiskleur zich moeten verantwoorden omdat zij het elektronische poortje – of een equivalent daarvan – niet doorkomen, groter dan dat bij blanke mensen het geval is. In het ergste geval worden ze onterecht verward met criminelen.
Biometrische technologie is ook niet altijd voor iedereen toegankelijk. Wie geen handen heeft, kan geen vingerafdrukscan laten verrichten. Ook werkt gezichtsherkenning niet altijd goed als een gezicht bijvoorbeeld om medische redenen er anders uitziet. Dit is al het geval bij een verkoudheid. Ook kunnen vingerafdrukken deels slijten, waardoor de sensoren je niet herkennen. Voor 2 procent van de bevolking zijn vingerafdrukscans zelfs ongeschikt, omdat vanwege ouderdom of een bepaalde chemotherapie deze mensen geen vingerafdruk hebben die 'gelezen' kan worden. Stemherkenning kan gehinderd worden als de persoon in kwestie bijvoorbeeld erg emotioneel is en de stem niet overeenkomt met de opgeslagen *voice print*. Biometrie is dus niet voor alle mensen altijd inzetbaar en ook niet in alle situaties.
Kwaadwillenden kunnen ook toegang krijgen tot biometrische gegevens of zelfs onderdelen van het lichaam zelf. Bijvoorbeeld met nagemaakte vingerafdrukken

of nephanden.[26] Biometrische gegevens zijn al eens onderdeel geweest van datalekken.[27] En, anders dan een wachtwoord, kun je je gezicht of vingerafdruk niet wijzigen. Het is zelfs al eens voorgekomen dat iemands vinger werd afgesneden, zodat met de vinger een auto geopend en vervolgens gestolen kon worden.
Biometrische systemen zijn dus niet onfeilbaar. Sterker nog, verificatie en identificatie zijn gebaseerd op statistische vergelijkingen: hoe groot is de kans dat er sprake is van een match (1 op 1, of 1 op N)? Bij elk systeem worden hiervoor 'drempelwaardes' ingesteld: keuzes over de waarde die bepaalt bij welke mate van overeenkomst de software aangeeft dat twee afbeeldingen of vingerafdrukken, of een ander kenmerk, van dezelfde persoon zijn of kunnen zijn. De drempelwaarde bepaalt zo de kans op foutpositieven en foutnegatieven (Rathenau Instituut, 2015). Hoe hoger de drempelwaarde wordt ingesteld, hoe minder foutpositieven er zijn. Maar het betekent ook dat er meer foutnegatieven zijn: het systeem herkent de gerechtigd persoon ten onrechte niet en verleent bijvoorbeeld geen toegang tot een gebouw of stadion.
Als de persoon zich bij een vals negatief resultaat direct opnieuw kan identificeren, hoeft dit geen probleem te zijn, maar het kan ook voor ongemak zorgen. In de Verenigde Staten werd van iemand zijn rijbewijs ingenomen omdat een gezichtsherkenningssysteem hem aanzag voor een ander. Na meer dan een week bureaucratisch getouwtrek waarin hij kon bewijzen wie hij daadwerkelijk was, kreeg hij zijn rijbewijs terug. Een ander voorbeeld betreft de Australische immigratiedienst, die met behulp van een geautomatiseerd systeem nagaat of iemand goed genoeg Engels spreekt. Een Ierse immigrante faalde voor deze test – waarschijnlijk vanwege haar accent – waardoor ze geen visum kreeg.[28]
Dit zijn 'kleine' voorbeelden van een groter probleem: biometrische systemen kunnen leiden tot instrumentalisering van het individu. Het individu wordt dan gereduceerd tot kwantificeerbare kenmerken in een systeem en standaardprocedures. Voor wie ten onrechte door het systeem wordt aangeduid als 'verdacht' of 'onbevoegd' is het lastig, soms zelfs onmogelijk, om deze fout recht te zetten.

Perfecte techniek nog steeds risicovol

Een deel van de hierboven geschetste problemen kunnen verholpen worden door een beter ontwikkelproces, bijvoorbeeld het trainen van systemen met diverse datasets. Maar zelfs al zouden we de hiervoor geschetste imperfecties als kinderziekten beschouwen die op een dag worden verholpen, dan nog zijn er gevolgen van de inzet van biometrische technologie die nadelig kunnen zijn voor het individu en de samenleving.
Bij perfecte biometrische herkenningssystemen ontstaat namelijk een reële vrees dat we niet meer anoniem kunnen zijn. Als biometrie in publieke ruimten en publieke sectoren wordt toegepast, is het vrijwel onmogelijk om je daaraan te onttrekken. Mensen hebben namelijk lang niet altijd controle over de situaties waarin zij worden onderworpen aan biometrische toepassingen. Zo kunnen de toepassingen mensen van steeds grotere afstanden herkennen. Hoe kunnen mensen zich hiertegen verweren als zij niet eens weten dat er biometrische techniek op hen wordt toegepast? Ook kunnen elementen zoals foto's, die in een bepaalde context zijn verzameld – bijvoorbeeld op social media –, zonder mede-

weten van de betreffende persoon worden hergebruikt voor biometrische toepassingen. Het recente voorbeeld van ClearView AI illustreert dit. Dit in Amerika gevestigde bedrijf verzamelde meer dan drie miljard foto's van websites als Facebook en YouTube met daarop gezichten van personen. ClearView AI-appgebruikers kunnen eigen afbeeldingen, bijvoorbeeld foto's die zij van anderen maakten, uploaden en via gezichtsherkenning laten matchen met de verzamelde foto's van de websites. Zo kunnen gebruikers mensen identificeren voor eigen motieven, zoals manipulatie, stalking of opsporing. Dit heet doelverschuiving (*function creep*). Bovendien is het niet helder wat de aanbieders van de techniek met de verzamelde gegevens doen. We moeten daarom oog blijven houden voor alle belangen: de partij (of partijen) die de biometrische techniek inzet(ten), de personen die met de techniek te maken krijgen, zoals burgers, en de aanbieders van de techniek.[29]

Zeker het toepassen van gezichtsherkenning (voor identificatiedoeleinden) in openbare ruimten kan zo leiden tot een verregaande surveillancemaatschappij. De laatste tijd ontstaat er dan ook veel politieke en maatschappelijke discussie over deze toepassing. Niet voor niets zei onlangs Eurocommissaris Reynders (Justitie) op de AI Summit 2020 dat gezichtsherkenning voor massasurveillance nooit aan de maatstaf 'redenen van zwaarwegend algemeen belang' voldoet.[30] Met andere woorden, dergelijke inzet van die technologie is altijd disproportioneel.

Ook kunnen biometrische systemen privacy onder druk zetten, onder andere doordat ze kunnen leiden tot een *chilling effect*. Als systemen perfect in staat zijn mensen in de publieke ruimte te herkennen, kan dat de bewegingsvrijheid van burgers en de vrijheid om te demonstreren inperken.[31] Dit gebeurt al in Rusland en Hongkong, waar gezichtsherkenning werd gebruikt om demonstranten te identificeren. Techniek die ooit bedoeld was om zware criminaliteit en terrorisme tegen te gaan.[32] Omdat Rusland net als Nederland aangesloten is bij de Raad van Europa, hebben activisten een klacht over de vergaande gezichtsherkenning neergelegd bij het Europees Hof voor de Rechten van de Mens.[33]

En waar imperfecte technologie tot ongelijke behandeling kan leiden omdat systemen groepen mensen systematisch fout identificeren, kan ook perfecte herkenning leiden tot ongelijke behandeling. De Poolse school die een boete opgelegd kreeg vanwege de vingerafdrukscans, voerde als beleid dat leerlingen die niet meededen aan biometrische identificatie achterin de rij moesten aansluiten in de schoolkantine.[34] In Nederland hebben adepten van gezichtsherkenning soms ook een streepje voor. Zo kunnen zij sneller boarden bij Schiphol en sneller een voetbalstadion betreden.[35] Of hier sprake is van ongeoorloofde benadeling van individuen, in de zin van ongerechtvaardigde discriminatie, verdient nadere aandacht. Al deze elementen leiden ertoe dat biometrische toepassingen, ook als ze perfect werken, al snel disproportioneel zijn. Zo zetten gemeenten biometrie in om lookalike-fraude tegen te gaan, bijvoorbeeld in verband met identiteitsdocumenten, maar dergelijke fraude komt slechts een tiental keren per jaar voor.[36] Zijn die enkele gevallen de maatschappelijke risico's waard? In de strijd tegen racisme kondigde het kabinet zelfs plannen aan om camera's met gezichtsherkenning en microfoons in te zetten op de stadiontribunes. Zo zouden supporters die zich racistisch uitlaten, kunnen worden geïdentificeerd. Volgens staatssecretaris

Bruins zouden zulke slimme camera's langs honderden, mogelijk duizenden, amateurvelden geplaatst moeten worden. De vraag rijst: heiligt het doel de middelen?

Nieuwe biometrische toepassingen

Naast de bovengeschetste biometrische toepassingen voor verificatie en identificatie, en de kwesties die daarbij spelen, zien we een volgende generatie biometrische toepassingen opkomen. Lichamelijke kenmerken – het gelaat, de stem of de vingerafdruk – worden hierbij gebruikt voor doelen als het stellen van medische diagnoses, emotieherkenning of het maken van 'sentimentanalyses'. Het bedrijf Vocalis Health probeert bijvoorbeeld op basis van stemanalyse (analyse van zogenaamde vocale biomarkers) informatie vast te stellen over gezondheid of mentale gesteldheid.[37] Tijdens de corona-uitbraak is het bedrijf een proef gestart om te zien of op basis van stemanalyse Covid-19 kan worden vastgesteld. Onregelmatigheden in de vingerafdrukken kunnen duiden op leukemie of borstkanker. Soms zijn openbare bronnen voldoende. Zo kunnen YouTubebeelden worden gebruikt voor het opsporen van aanwijzingen van autisme.[38] Ook de mentale gezondheid kan worden blootgelegd.

Gegevens over gezondheid vallen onder de bijzondere categorieën van persoonsgegevens (Rathenau Instituut, nog te verschijnen). De term 'gezondheidsgegevens' moet onder de AVG breed worden opgevat. Het gaat om alle persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, bijvoorbeeld ziekte of handicap. Het is overigens niet altijd duidelijk wanneer een type gegeven wel of niet in een bepaalde categorie bijzondere persoonsgegevens valt, en hoe de toezichthouder dit begrip in de praktijk afbakent.[39] Emotieherkenningstechnologie probeert inzicht geven in de gemoedstoestand van mensen. Dit gebeurt op basis van gezichtsuitdrukkingen (Rathenau Instituut, 2014). Recente metastudies laten zien dat de technieken wel gezichtsuitdrukking meten, maar dat die niet op een betrouwbare manier zijn te koppelen aan een emotie of persoonlijkheid (Barrett e.a., 2019; Hoegen e.a., 2019). Ook van analyses op basis van het gezicht en expressie om na te gaan of je liegt[40] is de mate van betrouwbaarheid discutabel.[41] Ook andere lichamelijke of gedragskenmerken worden gebruikt om emoties te achterhalen, zoals stem, loopgedrag[42] en micro-blushes (verkleuringen die we met het oog niet kunnen waarnemen, maar die onze hartslag laten zien).[43]

Deze nieuwe toepassingen bevatten intieme gegevens en zijn zeer privacygevoelig. De wettelijke bescherming met betrekking tot bijzondere persoonsgegevens, waaronder biometrische persoonsgegevens, is echter niet zomaar op dit soort gevallen van toepassing. Het is onder de AVG namelijk niet zo dat iedere afbeelding, bijvoorbeeld een pasfoto of een still uit camerabeelden, moet worden beschouwd als gezondheidsinformatie of biometrisch gegeven (lees: bijzondere persoonsgegevens). Ze zijn dat pas als zij worden verwerkt (1) met technische middelen die (2) de unieke identificatie of authenticatie van een persoon mogelijk maken. Onder de AVG kunnen dus afbeeldingen met gezichten van personen en stemopnamen naargelang het gebruik 'verkleuren' naar biometrische gegevens of andere bijzondere persoonsgegevens.

Zolang deze gegevens niet onder de AVG-definitie van 'biometrische gegevens' vallen of anderszins 'bijzonder' zijn, bijvoorbeeld als gezondheidsinformatie, genieten ze geen extra wettelijke bescherming. Ze kunnen dus redelijk vrijelijk gebruikt worden, weliswaar binnen de algemene kaders van de AVG als dit persoonsgegevens zijn.

Conclusie: een voorstel voor een verbod en vergunningsplicht

Biometrische technologie zoals gezichtsherkenning maakt het mogelijk om mensen op grote schaal te identificeren of te verifiëren, te volgen en daarnaar te handelen. Bijvoorbeeld door hen de toegang te ontzeggen of aan te spreken op overlastgevend gedrag. Hoewel we geen samenleving hebben zoals China, waar de overheid met behulp van surveillance en biometrie burgers in het gareel houdt, zagen we dat ook in Nederland biometrische toepassingen gericht op identificatie in de openbare ruimte op gespannen voet kunnen staan met privacybescherming, gelijke behandeling, anonimiteit op straat en een menswaardige behandeling. In deze concluderende paragraaf bepleiten we eerst aanvullende wettelijke bescherming voor identificatie en vervolgens voor verificatie. Tot slot staan we stil bij de 'nieuwe generatie' biometrische toepassingen, waarbij lichamelijke en gedragskenmerken voor andere doelen worden ingezet.

Identificatie: verbod identificatie in de publieke ruimte

Op dit moment lijken de regels voor het verwerken van biometrische gegevens beperkt, terwijl er significante ethische en maatschappelijke bezwaren zijn. De Uitvoeringswet AVG geeft aan dat het gebruik van biometrische gegevens is toegestaan als het gebruik noodzakelijk is voor verificatie- of beveiligingsdoeleinden. Dit lijkt de weg open te zetten naar gezichtsherkenning (identificatie) van personen in de openbare ruimte voor beveiligings- en surveillancedoeleinden, terwijl juist dit een van de toepassingen is die kunnen leiden tot massasurveillance en verlies van anonimiteit op straat. Zoals de Eurocommissaris al aangaf, lijkt deze toepassing altijd disproportioneel te zijn.

Het lijkt daarom logisch om biometrische toepassingen voor identificatie in de publieke ruimte, al dan niet tijdelijk, te verbieden (Rathenau Instituut, 2020c). Zowel de Raad van Europa als de EU-toezichthouder European Data Protection Supervisory Board delen deze visie, in elk geval totdat er een publiek debat is gevoerd en hierover op Europees niveau regels zijn vastgesteld. Volgens de Europese Commissie moet biometrische identificatie als hoog risico worden gezien, en als 'intrusive surveillancetechnology'.[44] De Commissie houdt zo de deur open om gezichtsherkenning te verbieden.[45] De AVG maakt het mogelijk voor Europese lidstaten om een dergelijk verbod in te stellen.

Een verbod zou goed in de huidige tijdsgeest passen. Uit recent onderzoek blijkt dat slechts 6 procent van de Nederlandse ondervraagden bereid is aan private partijen gelaatsgegevens te verstrekken voor identificatiedoeleinden. Slechts 24 procent wilde dat doen als het identificatie door de overheid betrof. Op stedelijk niveau zijn in de Verenigde Staten reeds biometrische toepassingen verboden.

San Francisco en Boston hebben met betrekking tot gezichtsherkenning een verbod uitgevaardigd. Portland (Oregon)[46] heeft een verbod ingesteld voor zowel publieke als private toepassingen van gezichtsherkenning in de publieke ruimte, waaronder winkels. In Europa is België eveneens kritisch.

Verificatietoepassingen: vergunningsplicht

Biometrische toepassingen die verificatie mogelijk maken, kunnen noodzakelijk en gerechtvaardigd zijn. Denk bijvoorbeeld aan de toegangsbeveiliging van de eerdergenoemde kerncentrale, maar ook van belangrijke overheidsgebouwen of overheidsdatabases waarin vertrouwelijke informatie is opgeslagen. Tegelijkertijd lieten we in deze bijdrage zien dat ook verificatie nadelige gevolgen kan hebben, zoals inbreuk op privacy, uitsluiting en instrumentalisering. Onder de AVG is het nu aan de toezichthouder om de noodzakelijkheid en gerechtvaardigdheid van deze toepassingen op te sporen. Gezien het groeiende aantal toepassingen is dat een zeer veeleisende taak. Daarom stellen we voor om voor die situaties een vergunningsplicht in te voeren (Rathenau Instituut, 2020c).

De vergunningsplicht betekent dat de partijen die biometrische gegevens zouden willen verzamelen en verwerken voor verificatiedoeleinden, vooraf een vergunning moeten aanvragen bij de Autoriteit Persoonsgegevens. Deze plicht geldt al voor bepaalde verwerkingen van strafrechtelijke gegevens. Op deze manier houdt de Autoriteit Persoonsgegevens een vinger aan de pols. Bijvoorbeeld door het verbinden van voorwaarden aan de vergunning met het oog op de bescherming van de persoonlijke levenssfeer van burgers. De mogelijkheid om biometrische gegevens op basis van toestemming te verwerken komt daarmee te vervallen. Ook voor een deel van de nieuwe generatietoepassingen, zoals stemanalyse, kan een dergelijke vergunningsplicht worden ingevoerd.

We doen dit voorstel in het licht van de reikwijdte van dit artikel, te weten: biometrische toepassingen in de publieke ruimte en het gebruik van biometrische gegevens door de publieke sector. Het is echter goed denkbaar dat de vergunningsplicht uitgebreid dient te worden naar gebieden en actoren die buiten de reikwijdte vallen, zoals biometrische toepassingen in niet-publieke ruimten. De door ons gesignaleerde risico's kunnen ook daar van toepassing zijn. Nader onderzoek zal dit kunnen uitwijzen.

Tot slot zouden we ons moeten bezinnen over privacygevoelige gegevens die met biometrische toepassingen gepaard kunnen gaan, zoals informatie over hoe je je voelt, en die niet onder de extra bescherming van de AVG vallen als bijzondere persoonsgegevens. Is het terecht dat zulke gegevens betrekkelijk vrij gebruikt kunnen worden? Een onderzoek hiernaar en een opvolgend politiek debat zal hierover uitsluitsel kunnen geven.

Noten

1 www.rtlnieuws.nl/nieuws/nederland/artikel/4997021/gezichtsherkenning-openbare-ruimte-bits-freedom-digitaal-online.

2 www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Speaker-Identification-Integrated-Project-SIIP.
3 www.schiphol.nl/nl/pagina/proef-met-reizen-met-gezichtsherkenning-cathay-pacific/.
4 www.security.nl/posting/613779/Tilburg+onderzoekt+gezichtsherkenning+voor+zwembad.
5 Deze beschrijving is gebaseerd op de studie *Dicht op de huid* (Rathenau Instituut, 2015).
6 www.rtlnieuws.nl/editienl/artikel/4790236/biometrie-hartslag-gezichtsherkenning-stemherkenning-iris-handtekening.
7 D*e Volkskrant* 2 januari 2003, 'Beveiligingsfirma's floreren sinds 11 september 2001'.
8 *Leeuwarder Courant* 17 juli 2006, 'Eerst je gezicht laten zien en dan pas zwemmen'; *Reformatorische dagblad* 2 juni 2006, 'Amsterdam eens met gezichtsherkenning'.
9 https://tweakers.net/nieuws/138825/politiek-stelt-vragen-over-privacy-van-gezichtsherkenning-bij-henschotermeer.html; www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland; www.nrc.nl/nieuws/2019/11/29/dieven-en-onschuldigen-de-camera-ziet-iedereen-a3982154
10 *De Stentor* 6 juli 2018, 'Echt of nep? In Zwolle hebben ze het sneller door'.
11 www.limburger.nl/cnt/dmf20201006_00178886.
12 www.biometricupdate.com/201506/new-zealand-tax-departments-voice-identification-feature-enrolls-1-4m-users.
13 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/ico-says-that-voice-data-collected-unlawfully-by-hmrc-should-be-deleted/.
14 https://nos.nl/artikel/2294479-zorgen-om-chinese-camera-s-met-gezichtsherkenning-in-belgrado.html.
15 www.securitymagazine.com/articles/92665-biometrics-will-enable-many-covid-19-changes.
16 *NRC Handelsblad* 11 augustus 2020, 'Bellen, elektronische polsbandjes of verplicht hotelverblijf. Zo houden overheden toezicht op de quarantaine'.
17 Dit geldt overigens ook voor genetische gegevens en gezondheidsgegevens (artikel 9 lid 4 AVG: 'De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren').
18 Specifiek: het verklaart het verbod op het gebruik van biometrische gegevens als bijzondere persoonsgegevens buiten toepassing als het gebruik ervan noodzakelijk is voor authenticatie of beveiligingsdoeleinden.
19 https://univers.wpengine.com/nieuws/2019/06/19/gezichtsherkenning-en-vingerscan-stappegoor-mogen-allebei-niet/.
20 Zweden: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en; Polen: https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en.
21 https://iapp.org/news/a/french-court-rules-against-schools-school-facial-recognition-plans/.
22 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie#mag-mijn-sportschool-mij-verplichten-een-vingerafdruk-af-te-staan-5876.

23 https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases. *Metro* 8 december 2016, 'Paspoortsysteem beoordeelt ogen Aziaat als dicht'.
24 https://nypost.com/2017/12/21/chinese-users-claim-iphone-x-face-recognition-cant-tell-them-apart/.
25 https://techcrunch.com/2020/09/21/twitter-and-zoom-algorithmic-bias-issues/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLm5sLw&guce_referrer_sig=AQAAAGa8-NXfY5tZoSkuavpXQTd0Dtdg4e-9J8_IVmhyWKtkuOELvLmmnT3efU3AJoDCyHStmOu1rhNVENE8epPloyZlhsgkz-IeZfcbEe-9wfJQ3qNTttc1jrKlY6Xxj_7ggtB0tZs-QhcXLLLoJdxsZn2ZPb1sojAsbO3QyDshB3Zy.
26 www.agconnect.nl/artikel/aderverificatie-te-omzeilen-met-nephand.
27 www.bbc.com/news/technology-49343774.
28 www.abc.net.au/news/2017-08-09/voice-recognition-computer-native-english-speaker-visa-limbo/8789076.
29 https://ainowinstitute.org/regulatingbiometrics-ranganathan.pdf. 'Instead of treating biometric information simply as data to be guarded, law and regulation should reckon with the entire range of powerful market interests that the networked subject kicks into motion, as well as regulation's own malleability in the face of these forces.'
30 https://twitter.com/ellajakubowska1/status/1311570202648289280.
31 www.privacynieuws.nl/lichamelijke-integriteit/biometrie/21898-vn-tegen-gezichtsherkenning-om-betogers-te-identificeren.html.
32 www.trouw.nl/nieuws/die-tatoeage-op-de-linkerarm-die-licht-slepende-tred-200-000-camera-s-in-moskou-herkennen-burgers-overal~bf887b19/.
33 https://interfax.com/newsroom/top-stories/69211/.
34 https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en.
35 www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028/.
36 www.privacynieuws.nl/nieuwsoverzicht/lichamelijke-integriteit/biometrie/21215-privacy-first-kritisch-op-gebruik-gezichtsscans-bij-balie-gemeente.html.
37 www.theverge.com/2019/3/14/18264458/voice-technology-speech-analysis-mental-health-risk-privacy en https://ict.usc.edu/prototypes/simsensei/.
38 www.theatlantic.com/technology/archive/2019/09/breakthrough-autism-research-uses-social-media-videos/597646/.
39 Zo bleek uit onze analyse in *Werken op waarde geschat* (Rathenau Instituut, 2020c). In 2011-2012 onderzocht het CBP (nu Autoriteit Persoonsgegevens) Bureau Jeugdzorg Noord-Brabant. Dit bureau verplichtte zijn werknemers deelname aan een assessment, waarvoor gegevens werden verzameld over onder andere eigenwaarde, steunbehoefte, stressbestendigheid, conformeren, extraversie, sociale empathie, sociabiliteit, dominantie. De toezichthouder vond dit geen bijzondere persoonsgegevens, slechts gevoelige gegevens. In 2017-2018 oordeelde de toezichthouder over BrainCompass, een assessmentbureau dat rapporteert over de persoonlijkheidseigenschappen van werknemers. De toezichthouder concludeerde dat BrainCompass bij de gegevensverwerking informatie verschaft over de psychische gesteldheid, vaardigheden en beperkingen van de deelnemer en zijn emotionele capaciteit. Het ging het wel om gezondheidsgegevens, aldus de toezichthouder, onder meer omdat uit de (gecombineerde)

informatie bijvoorbeeld kan worden afgeleid in hoeverre de deelnemer stressbestendig of mentaal weerbaar is. Stressbestendigheid was in de zaak Bureau Jeugdzorg Noord-Brabant ook een factor, maar kennelijk in dat geval niet doorslaggevend om de gegevens aldaar als gezondheidsgegevens te kwalificeren.

40 www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html.

41 *NRC Handelsblad* 3 januari 2019, 'Hoe ziet de computer of je liegt?'.

42 www.fastcompany.com/90375885/a-new-ai-can-tell-how-you-feel-just-by-watching-you-walk-down-the-street.

43 www.vitalsignscamera.com/index.htm.

44 www.rijksoverheid.nl/documenten/kamerstukken/2020/04/20/aanbieding-kabinetsappreciatie-witboek-kunstmatige-intelligentie.

45 www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology/.

46 www.wired.com/story/portlands-face-recognition-ban-twist-smart-cities/.

Literatuur

Barrett, L.F., Adolphs, R., Marsella, S., Martinez, A.M., & Pollak, S.D. (2019). Emotional expressions reconsidered: challenges to inferring emotion from human facial movements. *Psychological Science in the Public Interest*, 20 (1): 1-68. https://journals.sagepub.com/doi/abs/10.1177/1529100619832930.

Hoegen, R., Gratch, J., Parkinson, B., & Shore, D. (2019). Signals of Emotion Regulation in a Social Dilemma: Detection from Face and Context. *8thInternational Conference on Affective Computing and Intelligent Interaction (ASCII)*. doi:10.1109/ACII.2019.8925478.

NIST (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. *NISTIR 8280*. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Rathenau Instituut (2014). *Intieme technologie: De slag om ons lichaam en gedrag*. Den Haag: Rathenau Instituut.

Rathenau Instituut (2015). *Dicht op de huid. Gezichts- en emotieherkenning in Nederland*. Den Haag: Rathenau Instituut.

Rathenau Instituut (2017). *Opwaarderen: borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut.

Rathenau Instituut (2020a). *Hoor wie het zegt. Handvatten voor het verantwoorde gebruik van spraaktechnologie*. Den Haag: Rathenau Instituut.

Rathenau Instituut (2020b). *Reactie verzamelwet gegevensbescherming. Wetgever moet persoonlijke gegevens van burgers beter beschermen*. Den Haag: Rathenau Instituut.

Rathenau Instituut (2020c). *Werken op waarde geschat. Grenzen aan digitale monitoring op de werkvloer door middel van data, algoritmen en AI*. Den Haag: Rathenau Instituut.