UNIVERSITEIT VAN TILBURG

Op het eerste gezicht

Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties.

Esther Keymolen, Merel Noorman, Bart van der Sloot, Colette Cuijpers, Bert-Jaap Koops, Bo Zhao

Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society
Postbus 90153
5000 LE Tilburg
www.uvt.nl/tilt/
Contactpersoon: dr. E.L.O. Keymolen
e.l.o.keymolen@uvt.nl
datum: 12 maart 2020

Afkortingen

AP	Autoriteit Persoonsgegevens
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
AWB	Algemene Wet Bestuursrecht
BW	Burgerlijk Wetboek
CCTV	Closed-circuit television
CDA	Christen-Democratisch Appèl
CEO	Chief Executive Officer
CIO	Chief Information Officer
CTO	Chief Technical Officer
D66	Democraten 66
DPO	Data Protection Officer
EDPB	European Data Protection Board
EER	Europees Economische Ruimte
EU	Europese Unie
Fedma	Federal Emergency Management Agency
GDPR	General Data Protection Regulation
HR	Hoge Raad
OJ	Official Journal
SNS	Social Network Sites
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VS	Verenigde Staten
Wav	Wet arbeid vreemdelingen
WWM	Wet wapens en munitie

DANKWOORD

De auteurs willen graag alle personen bedanken die bereid waren om deel te nemen aan de interviews en de expert workshop. Het inzicht en de kennis die dit opleverde was enorm waardevol voor dit rapport. Graag danken wij ook de leden van de begeleidingscommissie voor hun kritische maar te allen tijde constructieve commentaar gedurende dit onderzoek. Ten slotte willen wij ook nadrukkelijk Anne de Laat, Alissa Verhagen en Gargi Sharma bedanken die ons ondersteund hebben in het onderzoek en de vormgeving van dit rapport. Zo ook danken wij Georgios Bouchagiar en Katharina Creemer die als stagairs een bijdrage hebben geleverd aan het onderzoek voor dit rapport.

INHOUDSOPGAVE

Samenvatting

Gezichtsherkenningstechnologie wordt ingezet om op basis van digitale beelden (bijvoorbeeld een foto of video), gezichten of gezichtskenmerken te herkennen. De technologie wordt al enige tijd op beperkte schaal ingezet door overheden voor opsporing en beveiliging, maar is sinds kort ook beschikbaar voor bedrijven en burgers. Dit opent een scala aan mogelijkheden voor commerciële ondernemingen en particulieren om mensen te identificeren, te volgen en te profileren. Zo passen zoekmachines en sociale-mediaplatformen gezichtsherkenningstechnologie toe om portretten en beelden automatisch te beschrijven en van labels (*tags*) te voorzien; in de retailsector wordt het ingezet om winkelende klanten te monitoren en hen gepersonaliseerde aanbiedingen te doen; bij evenementen wordt de technologie gebruikt om mensen toegang te verschaffen of juist te weren; en diverse bedrijven bieden gezichtsanalyse -en gezichtsherkenningsmodules aan om zelf aan de slag te gaan met het ontwikkelen van bijvoorbeeld smartphone-applicaties. Mensen kunnen zulke gezichtsherkenningstoepassingen gebruiken om anderen op straat te identificeren en informatie over hen te vinden, zoals hun eerdere gedragingen, relaties tot andere mensen of voorkeuren.

Omdat het aannemelijk is dat gezichtsherkenningstoepassingen in de nabije toekomst op aanzienlijke schaal beschikbaar zullen zijn voor zowel burgers als bedrijven, is het noodzakelijk om in kaart te brengen of, en, zo ja, welke aanpassingen aan het huidige juridische raamwerk en aan andere reguleringsinstrumenten nodig zijn om de privacy van de burger te beschermen. Daarbij is het van belang om op te merken dat dit onderzoek zich uitsluitend richt op het gebruik van gezichtsherkenningstechnologie in *horizontale relaties:* relaties tussen bedrijven en burgers en tussen burgers onderling. De inzet van gezichtsherkenningstechnologie in verticale relaties, dat wil zeggen die tussen overheid en burger, is geen onderdeel van dit onderzoek.

Dit onderzoek is gebaseerd op een brede literatuurstudie naar geautomatiseerde gezichtsherkenningstechnologie en privacy-inbreuken, waarvoor naast academische literatuur ook nieuwsberichten, websites, blogs, persberichten en brochures zijn onderzocht. Hierbij hebben wij naar materiaal gekeken afkomstig uit zowel Nederland als het buitenland. De literatuurstudie is vervolgens toegespitst aan de hand van vier specifieke gezichtsherkenningstoepassingen (zogenaamde domeinstudies). Deze domeinstudies richten zich op: de evenementensector, smartphone-apps, de slimme deurbel en de retailsector. Voor deze domeinstudies is de literatuurstudie verder aangevuld met 11 stakeholder- en expertinterviews; oftewel bedrijven die in de genoemde sectoren opereren en wetenschappers die op dit terrein onderzoek doen. Er is tevens een workshop georganiseerd met 12 experts (bedrijfsleven, wetenschap, beleid, maatschappelijke organisaties) waarbij een aantal van de genoemde domeinstudies kritisch is besproken en de eerste bevindingen zijn voorgelegd. Om in kaart te brengen wat de huidige juridische middelen zijn om gezichtsherkenningstechnologie te reguleren, is een rechtsverkenning uitgevoerd die zich richt op de rechtsgebieden privacy- en gegevensbescherming, privaatrecht en strafrecht. Daaruit zijn tot slot een aantal reguleringsopties voortgekomen, evenals factoren die van invloed zijn op de keuze tussen de verschillende opties.

In dit onderzoek staan twee vragen centraal:

1) *Hoe wordt gezichtsherkenningstechnologie door Nederlandse burgers en bedrijven gebruikt en hoe kan het gebruik van gezichtsherkenningstechnologieën door burgers en bedrijven een inbreuk vormen op de privacy van de burger (nu en over vijf jaar)?*
2) *Hoe kunnen huidige en potentiële privacy-inbreuken worden voorkomen of beperkt?*

De beantwoording van deze vragen op basis van het onderzoek is als volgt:

Antwoord vraag 1: toepassingen en privacyrisico's

Gezichtsherkenningstoepassingen in horizontale relaties (bedrijf-burger en burger-burger) bevinden zich in Nederland nog in de experimentele fase. Bedrijven onderzoeken op beperkte schaal of er rendabele gezichtsherkenningstoepassingen kunnen worden geïntroduceerd. Deze stapsgewijze aanpak van bedrijven wordt niet louter ingegeven door economische motieven. Ook het groeiende bewustzijn dat de inzet van gezichtsherkenning privacyrisico's met zich meebrengt en onzorgvuldig handelen tot mogelijke afbreukrisico's leidt, maakt dat bedrijven niet al te voortvarend willen handelen. Uit de interviews met de vertegenwoordigers van bedrijven blijkt dat het voor hen niet altijd helder is hoe de diverse juridische vereisten, zoals onder meer neergelegd in de Algemene Verordening Gegevensbescherming (AVG), geïnterpreteerd moeten worden ten aanzien van gezichtsherkenning. Ook dit draagt bij aan de keuze voor een behoedzame koers.

Het aantal gezichtsherkenningstoepassingen in Nederland is relatief beperkt; de projecten die reeds lopen zijn vooral op initiatief van bedrijven. Zij zetten deze technologie tot nu toe vooral in voor relatief eenduidige, specifieke doeleinden. Vaak gaat het om een bepaalde vorm van toegangscontrole. Deze toepassingen zijn niet louter van Nederlandse makelij. Zo leveren ook Amerikaanse bedrijven gezichtsherkenningsdiensten aan de Nederlandse markt. De initiatieven die in de burger-burger-relatie van de grond zijn gekomen betreffen vooral toepassingen gericht op gemak en vermaak (bijvoorbeeld smartphone-apps) en toegangscontrole (bijvoorbeeld de slimme deurbel met gezichtsherkenning). Ten slotte is het ook mogelijk om als burger zelf aan de slag te gaan met gezichtsherkenningstechnologie. Burgers met enige programmeerkennis kunnen gebruik maken van onlinediensten om zelf gezichtsherkenningstoepassingen te ontwikkelen.

Waar Nederland nog volop in de experimenteerfase zit, kent men in het buitenland –met name buiten de EU– reeds meer diverse gezichtsherkenningstoepassingen, hoewel die zich ook daar nog vaak in de implementatiefase bevinden. Deze buitenlandse toepassingen geven wel een idee van wat er technisch mogelijk is en wat er in de nabije toekomst misschien ook in Nederland te verwachten valt. Mogelijke ontwikkelingsrichtingen van gezichtsherkenningstoepassingen binnen de horizontale relatie in de komende vijf jaar kunnen onder meer het gebruik voor de volgende doelen zijn:

Gemak en efficiëntie: Gezichtsherkenningstoepassingen worden op dit ogenblik vooral aan de man gebracht met de belofte bestaande processen soepeler te laten verlopen. Een snelle check-in bij evenementen via gezichtsherkenning, het betalen in winkels via gezichtsherkenning, op afstand de toegang tot je huis regelen via de slimme deurbel, etc. Gezichtsherkenning kan ook ingezet worden om bestaande activiteiten te verrijken met extra mogelijkheden, zoals dating-apps die de mogelijkheid bieden om op *look-alikes* van beroemde mensen te zoeken. De meeste gezichtsherkenningstoepassingen die in Nederland worden gebruikt zijn gericht op efficiëntie, gemak en vermaak. Als deze tendens zich voortzet en samengaat met snellere systemen die ook zelfstandig op draagbare, kleine apparaten werken, dan kan daarvan een mogelijk gevolg zijn dat in het sociale verkeer gezichtsherkenning een prominente plaats zal gaan innemen. Smartphone-apps die worden gebruikt voor sociale interacties hebben dan ook een gezichtsherkenningsonderdeel, bijvoorbeeld om mensen die elkaar leren kennen via online platforms in staat te stellen elkaar ook offline te kunnen identificeren. Andersom kan de grote hoeveelheid aan informatie die de afgelopen jaren online over mensen beschikbaar is geworden worden gekoppeld aan individuen offline wanneer zij via gezichtsherkenning herkend worden. Als gemak en efficiëntie leidend blijven in de toekomstige ontwikkelingen en toepassingen van gezichtsherkenning, dan kan het bovendien zo zijn dat alle handelingen die nu nodig zijn voor identificatie vervangen worden door gezichtsherkenning. Toegangspassen, bonuskaarten, allerlei wachtwoorden en toegangscodes worden dan overbodig.

Beveiliging en controle: Vaak kennen bovenstaande voorbeelden ook een controle- en/of veiligheidscomponent. Inchecken via gezichtsherkenning is niet alleen handig, het biedt in principe ook de mogelijkheid om op basis van zwarte lijsten ongewenste individuen op geautomatiseerde wijze de toegang tot bepaalde ruimtes te ontzeggen. Gezichtsherkenning wordt niet alleen ingezet om foto's te *taggen* maar ook om identiteitsfraude tegen te gaan. Emotiedetectie als een specifieke vorm van gezichtsherkenning kan ook een rol spelen in beveiliging en controle, bijvoorbeeld wanneer bepaalde emoties als angst en boosheid op geautomatiseerde wijze herkend worden en dit wordt gebruikt om snel op te treden en escalatie te voorkomen. Als het gebruik van gezichtsherkenning voor dergelijke doeleinden zich voortzet en de accuraatheid en snelheid van de technologie toenemen, dan is het denkbaar dat gezichtsherkenning gekoppeld zal worden aan het inperken van toegang tot bepaalde plaatsen en diensten. Het kan dan een krachtig instrument worden om individuen of groepen te weren en gedrag dat als onwenselijk wordt aangemerkt tegen te gaan.

Personalisatie en proactieve dienstverlening: Gezichtsherkenning kan ten slotte ook ingezet worden om dienstverlening te personaliseren en proactief aan te bieden. In de retailsector worden

nu al menu's en aanbiedingen aangepast op basis van gezichts- en emotieherkenning. Zeker de mogelijkheid om met emotiedetectie, een specifieke vorm van gezichtsherkenning, geautomatiseerd en *real-time* te kunnen monitoren hoe klanten zich voelen en daar dan proactief op in te kunnen spelen, is een toepassing die commerciële partijen als veelbelovend beschouwen. Nieuwe functionaliteiten die gepersonaliseerde dienstverlening of advertenties nog verder verfijnen, zoals het meten van de hartslag op basis van digitale videobeelden van gezichten, maken het automatisch analyseren van gezichten nog aantrekkelijker. Als deze tendens zich voortzet, dan is het mogelijk dat door middel van gezichtsherkenning data *real-time* worden gekoppeld aan individuen in de (semi)publieke ruimte met het doel hun handelen te beïnvloeden (ook wel *nudging* genoemd) of hen te profileren. Niemand krijgt dan nog dezelfde aanbiedingen te zien in winkels en er kan op geautomatiseerde wijze onderscheid gemaakt worden in de manier waarop mensen worden behandeld. Gezichtsherkenning wordt dan een belangrijke sleutel om data-gedreven beslissingen te nemen en de keuze-infrastructuur van burgers in het dagelijks leven te beïnvloeden.

Op basis van de gezichtsherkenningsontwikkelingen en de hierboven geschetste scenario's zijn de volgende privacyrisico's geïdentificeerd:

Ondoorzichtige informatieverzameling: Veel gezichtsherkenningstechnologie werkt momenteel op basis van modellen die getraind zijn met beelddata waarvoor de afgebeelde personen geen toestemming hebben gegeven. Het internet vormt hierbij een belangrijke bron, maar ook beeldmateriaal verkregen in de publieke ruimte wordt hiervoor gebruikt. Omdat dit verzamelen van data zich op mondiaal niveau afspeelt is het moeilijk hier controle op uit te oefenen. Burgers verliezen controle over wat er gebeurt met hun foto's en video's.

Autonomie onder druk: Vanuit commercieel oogpunt houdt goed functionerende gezichtsherkenning vaak in dat burgers geen extra handelingen hoeven uit te voeren om de technologie zijn werk te laten doen. Het ontbreken van een actieve handeling ontneemt hen echter ook een belangrijk keuze- en reflectiemoment. Wil ik dit wel echt? In de situatie dat burgers wel bewust zijn van de aanwezigheid van de gezichtsherkenningsapplicatie en er de mogelijkheid wordt geboden een dienst te verkrijgen of een ruimte te betreden zonder gezichtsherkenning, zal het vaak zo zijn dat het alternatief zonder gezichtsherkenning een uitgeklede optie wordt waar nog maar weinig in wordt geïnvesteerd. Zij die vasthouden aan deze laatste optie moeten dan met een verminderde dienstverlening of een basaal functionerend product genoegen nemen.

Bias en fouten in gezichtsherkenning: Hoewel de kwaliteit en betrouwbaarheid van gezichtsherkenningstechnologie in de afgelopen jaren enorm is toegenomen, blijft het een bekend en niet te onderschatten probleem dat onder andere door *biases* in de trainingsdata,

gezichtsherkenningstoepassingen uitkomsten genereren die discriminatoir van aard zijn en minder goed werken bij bepaalde groepen (zoals vrouwen, kinderen en personen met een getinte huidskleur). Voor deze groepen is de kans groter dat zij ofwel onjuist of niet herkend worden, met als gevolg dat hen bijvoorbeeld de toegang tot een evenement wordt ontzegd, of dat zij geen gebruik kunnen maken van bepaalde diensten, wat tot uitsluiting en stigmatisering kan leiden.

Einde van anonimiteit: Wanneer gezichtsherkenning in horizontale relaties wijdverbreid raakt, en door zowel bedrijven als door burgers eenvoudig kan worden ingezet, dan zal het steeds moeilijker worden voor mensen om zich anoniem in de publieke, semipublieke en zelfs private ruimte te begeven.

Afhankelijkheid van anderen: Wanneer gezichtsherkenning via bijvoorbeeld apps wordt gebruikt door burgers in het sociale verkeer, dan is men in grote mate afhankelijk van de prudentie en discretie van die gebruiker om geen inbreuk te plegen op de privacy van derden. Veel burgers vinden het echter nu al moeilijk om bijvoorbeeld in te schatten hoe groot het publiek is dat ze bereiken met het online delen van informatie. Dit probleem wordt door gezichtsherkenning geïntensiveerd.

Secundair gebruik van data: Hoewel de focus van dit onderzoek uitgaat naar de horizontale relatie, blijft een belangrijk privacyrisico dat overheden aankloppen bij bedrijven om gebruik te kunnen maken van de gezichtsherkenningsinformatie verzameld in horizontale relaties. Deze specifieke vorm van secundair gebruik is reeds bekend van internetbedrijven die –soms dwingende– verzoeken krijgen om informatie te delen met onder meer inlichtingendiensten. Het waarborgen van privacy in horizontale relaties is dus ook van belang voor het beschermen van privacy in verticale relaties.

Machtsongelijkheid en *chilling effect*: Gezichtsherkenningstoepassingen die zich richten op controle of personalisatie doen dit eigenlijk altijd in combinatie met andere, reeds bestaande databestanden. Het gezicht wordt dan een aanknopingspunt voor andere (online) beschikbare informatie over die persoon. Gezichtsherkenning draait dan niet louter meer om iemand herkennen, maar om het toegankelijk maken van een heel scala aan informatie over diegene. De informatierijke profielen die hierdoor ontstaan kunnen de privacy van burgers op verschillende manieren aantasten. Zo wordt het voor burgers steeds moeilijker om in te schatten wat anderen over hen weten. Dit kan leiden tot machtsverschuivingen in horizontale relaties die ervoor zorgen dat burgers hun gedrag uit voorzorg gaan aanpassen (*chilling effect*). Wanneer de door gezichtsherkenning ontsloten informatie bovendien ingezet wordt om iemand te stalken of bedreigen, kan ook de lichamelijke integriteit op het spel komen te staan.

Antwoord vraag 2: Best practices en reguleringsopties

Om in beeld te brengen hoe huidige en potentiële privacy-inbreuken kunnen worden voorkomen of beperkt, brachten wij de bestaande *best practices* van bedrijven die gezichtsherkenningstechnologie inzetten en/of ontwikkelen in kaart, voerden wij een rechtsverkenning uit en benoemden wij een reeks reguleringsopties.

In de literatuur en door de geïnterviewde bedrijven worden als *best practices* voor het beschermen van de privacy van burgers onder meer verwezen naar de volgende mogelijkheden. Hierbij dient te worden vermeld dat wij de effectiviteit van deze maatregelen niet hebben kunnen vaststellen.

- **Andere bedrijfsmodellen dan data in ruil voor (gratis) diensten: B**edrijfsmodellen waarbij het verhandelen van data niet de kern is, hebben de voorkeur.
- **Privacy-by-design en privacy-by-default:** In het ontwerp van het systeem wordt zoveel mogelijk ingezet op privacyvriendelijke keuzes.
- **Bedrijfswaarden:** Bedrijfswaarden zoals transparantie, toestemming, eerlijkheid (*fairness*), en verantwoording liggen ten grondslag aan, en begrenzen, de keuzes die bedrijven maken.
- **Voorlichting:** Bedrijven investeren in een goede voorlichting aan klanten en gebruikers.
- **Regulering:** Bedrijven ondersteunen waar mogelijk duidelijke regulering vanuit de overheid en zijn actief in het ontwikkelen van zelfregulering.
- **Toestemming:** Bedrijven kiezen voor dataverwerking op basis van toestemming, ook als dit niet wettelijk verplicht is.

Uit de rechtsverkenning blijkt dat de juridische handvatten om gezichtsherkenningstechnologie te reguleren vooral gelegen zijn in de Algemene Verordening Gegevensbescherming, het privaatrecht en dan met name de onrechtmatige daadsactie, en in beperkte mate het strafrecht. Doorgaans zal de Algemene Verordening Gegevensbescherming van toepassing zijn op gezichtsherkenningstechnologie. Dit brengt met zich mee dat het gebruik en de inzet van gezichtsherkenning in horizontale relaties maar in beperkte gevallen zal zijn toegestaan bij wet. Er zijn juridische vragen omtrent, onder meer, het bestaan van een legitieme verwerkingsgrondslag. Meer in het algemeen zijn er twijfels over de noodzakelijkheid, proportionaliteit en subsidiariteit van gezichtsherkenningstoepassingen. Het enkele feit dat een gebruiker instemt met een technologie of toepassing maakt het gebruik daarvan immers nog niet geoorloofd.

Daarbij moet bovendien in ogenschouw worden genomen dat bij gezichtsherkenning biometrische gegevens worden verwerkt die juridisch gezien zijn aangemerkt als bijzondere persoonsgegevens, waarvoor een strikter nee-tenzij-regime geldt. De wetgever geeft voor het gebruik van biometrische gegevens in horizontale verhoudingen (specifiek: werkgever-werknemer-relaties) het voorbeeld dat het voor een kerncentrale toegestaan kan zijn om gebruik te maken van gezichtsherkenningstechnologieën om zo slechts geregistreerde werknemers

toegang te verlenen tot de faciliteit. Daarmee zijn de meeste andere in het rapport besproken voorbeelden onvergelijkbaar in ernst, belang en noodzaak. De Autoriteit Persoonsgegevens kan een belangrijke rol spelen bij het toezicht op dergelijke technologieën.

Het strafrecht speelt momenteel slechts een geringe rol bij de regulering van gezichtsherkenningstechnologieën, grotendeels beperkt tot gevallen waarin heimelijk afbeeldingen van mensen worden gemaakt. De wetgever zou, naar analogie met de bestaande bescherming tegen het heimelijk maken van afbeeldingen, kunnen overwegen om ook heimelijke gezichtsherkenning strafbaar te stellen, zelfs als de camera waarmee gezichten worden herkend zelf wel duidelijk aanwezig is. Hierbij moet worden afgewogen of toepassingen en gebruik zo ernstig zijn dat vervolging en handhaving via het strafrecht gepast is. Tot slot ligt voor de hand om een en ander via het privaatrecht en onrechtmatige-daadsactie te laten verlopen voor het geval de burger of een bedrijf zelf actie wil ondernemen.

Aan de wetgever ligt een spectrum aan reguleringsopties open:

- **Totaalverbod:** Allereerst kan de Nederlandse wetgever ervoor kiezen om een (tijdelijk) totaalverbod neer te leggen voor het gebruik van gezichtsherkenningstechnologieën. Daarmee wordt duidelijkheid gegeven en wordt slechts een marginaal aantal mogelijke toepassingen die momenteel juridisch legitiem zouden zijn onmogelijk gemaakt. Anders gezegd: dit is nu nog een optie met relatief beperkte negatieve gevolgen. De functionaliteiten van apps zijn vooralsnog erg beperkt, de resultaten niet altijd betrouwbaar en de potentiële voordelen veelal marginaal. Als Nederland voor een strenge reguleringslijn zou kiezen, zou die lijn op een later moment, als de technologie en de toepassingen zich hebben ontwikkeld, nog eens kunnen worden geëvalueerd. Dit zou aansluiten bij de strenge lijn die zich in de EU lijkt te ontwikkelen.
- **Voorafgaande goedkeuring:** In deze optie mogen toepassingen slechts worden gebruikt en aangeboden als daarvoor voorafgaande goedkeuring is verkregen. Een vanzelfsprekende rol is hier weggelegd voor de Autoriteit Persoonsgegevens. Omdat het hier gaat om een technologie die gebruik maakt van bijzondere persoonsgegevens ligt het voor de hand om een Data Protection Impact Assessment uit te voeren. De Autoriteit Persoonsgegevens zou een richtsnoer kunnen uitgeven waaruit volgt dat partijen altijd een Data Protection Impact Assessment moeten voorleggen en dat zij pas na expliciete goedkeuring van de Autoriteit Persoonsgegevens van start mogen gaan.
- **Gediversifieerde aanpak:** Om de juridische onzekerheid weg te nemen omtrent de toelaatbaarheid van specifieke gezichtsherkenningstoepassingen, kan de wetgever, regering of de Autoriteit Persoonsgegevens besluiten expliciet aan te geven welke toepassingen zijn toegestaan en welke niet, en onder welke voorwaarden. Hierbij kan worden gedifferentieerd naar domeinen, toepassingen en de positieve of negatieve effecten op het leven van burgers.

- **Regelgevend kader specifiek voor gezichtsherkenning:** De wetgever of de Autoriteit Persoonsgegevens heeft de vrijheid om, al dan niet in samenwerking met andere toezichthouders en (internationale) partijen, een specifiek regelgevend kader te ontwikkelen voor gezichtsherkenningstechnologieën, waarin de algemene juridische principes en uitgangspunten concreet worden uitgewerkt voor wat betreft deze technologie en voor het soort toepassingen dat voorzien is en legitiem wordt geacht.
- **Controle achteraf:** Er kan ook voor worden gekozen om het huidige regelgevende kader in stand te laten en in te zetten op controle achteraf op het gebruik van technologieën en toepassingen. Deze controle kan plaatsvinden ofwel op initiatief van een burger of bedrijf die een klacht indient ofwel op initiatief van een handhavende organisatie, zoals de Autoriteit Persoonsgegevens.
- **Gedragscode en certificering:** De Algemene Verordening Gegevensbescherming maakt het mogelijk om voor specifieke sectoren of toepassingen een aparte gedragscode te ontwikkelen, met een specifieke handhavende en toezichthoudende organisatie die door die code wordt aangewezen of ingesteld. Of het bij gezichtsherkenning echt om een aparte sector gaat waarbij een vertegenwoordigende instantie een dergelijke code kan opstellen en voorleggen aan de Autoriteit Persoonsgegevens, is echter de vraag. Wellicht ligt het werken met certificering meer voor de hand, waarvoor de Algemene Verordening Gegevensbescherming ook ruimte biedt. Het is dan aan een eventueel geaccrediteerd certificeringsorgaan om een certificaat te geven aan een bedrijf dat wordt geacht gezichtsherkenningstechnologie in overeenstemming met de Algemene Verordening Gegevensbescherming in te zetten. De Autoriteit Persoonsgegevens kan toezicht houden dat dergelijke certificering juist geschiedt.
- **Bewustwording:** De overheid kan inzetten op publiekscampagnes om burgers en bedrijven duidelijk te maken welke gevaren en juridische (en mogelijkerwijs ook sociale en ethische) grenzen er zijn aan het toepassen van gezichtsherkenningstechnologieën. Met name in burger-burger-relaties zullen sociale normen een belangrijke rol spelen in de manier waarop gezichtsherkenning wordt toegepast. Bij gezichtsherkenning zou een sociale norm behulpzaam kunnen zijn om bijvoorbeeld smartphones bewust *niet* te richten op personen op een manier dat die zich bekeken, herkend en gecategoriseerd zouden voelen. Hoewel zo een norm niet kan worden opgelegd, kunnen beleidsinterventies gericht op bewustwording wel bijdragen aan het ontwikkelen van sociale normen die de privacyrisico's van gezichtsherkenning kunnen helpen te beperken. Ook bij bedrijven kan hier nog het nodige worden gewonnen. Een onderzoek van de Autoriteit Persoonsgegevens naar de toelaatbaarheid van gezichtsherkenningstechnologie in een specifiek geval kan ook een duidelijke normerende werking hebben en meer bewustwording creëren ten aanzien van de privacyrisico's en grenzen van gezichtsherkenningstechnologieën.
- **Gedoogbeleid:** Tot slot kan de Autoriteit Persoonsgegevens of regering in beleid aangeven dat het gebruik van gezichtsherkenning voor een bepaalde tijdsperiode zal worden gedoogd

en naleving van wettelijke kaders niet zal worden afgedwongen, om het zo de kans te geven tot volle wasdom te komen en pas daarna te evalueren welke voordelen en mogelijke nadelen er zijn aan de na een aantal jaar ontwikkelde gezichtsherkenningstechnologieën. Wel moet worden bedacht dat burgers hun rechten als vervat in het Europees Verdrag voor de Rechten van de Mens en de Algemene Verordening Gegevensbescherming kunnen afdwingen via rechterlijke procedures en dat daar uiteindelijk het Europees Hof voor de Rechten van de Mens respectievelijk het Europees Hof van Justitie een oordeel over zal vellen.

Om het maken van deze keuze te ondersteunen hebben wij een onderscheid gemaakt in typen relaties, doeleinden, en benaderingswijzen. Door scherp te kijken door wie en voor welke doeleinden gezichtsherkenning wordt toegepast en te expliciteren wat de algehele houding van de overheid is ten opzichte van gezichtsherkenning (van risicomijdend tot kans optimaliserend), kan een gedegen afweging worden gemaakt.

Er kunnen drie specifieke horizontale relaties worden onderscheiden:

- **Burger-burger:** In dit onderzoek hebben wij nagenoeg geen voorbeelden gezien van toepassingen die de toets van noodzakelijkheid, proportionaliteit, subsidiariteit en legitimiteit zullen doorstaan. Daarbij dient te worden opgemerkt dat de technologie wel kwaadwillende burgers kan faciliteren in hun handelen (denk aan stalking of identiteitsdiefstal) en dat op dit ogenblik burgers toegang hebben tot commerciële diensten die hen de mogelijkheid bieden om zelf met gezichtsherkenningstechnologie aan de slag te gaan. Tegenover reële privacyrisico's staan dus vooralsnog weinig evidente voordelen van gezichtsherkenning door burgers.
- **Bedrijf-burger:** Hoewel het in deze relatie vaak gaat om toepassingen met een duidelijk en serieus doel, blijkt uit het onderzoek dat voor de inzet van gezichtsherkenningsapplicaties vaak goede en minder invasieve technologische alternatieven bestaan. Een gebrekkige proportionaliteit of subsidiariteit kan een belangrijk juridisch struikelblok opleveren.
- **Werkgever-werknemer:** Door de band genomen zal een werknemer geen vrije toestemming kunnen geven. Grosso modo zal als verwerkingsgrond alleen het bestaan van een algemeen zwaarwegend belang kunnen worden ingeroepen (denk aan beveiliging van kerncentrales).

Hiernaast kan er een onderscheid worden gemaakt tussen verschillende doeleinden waarvoor de gezichtsherkenningstechnologie wordt ingezet. Daarbij is er evident overlap met de vorige opsomming; het is slechts een andere manier om de diverse toepassingen te categoriseren:

- **Zorgdoeleinden:** De medische context is een bijzondere context want het gaat dikwijls om kwetsbare personen en gevoelige gegevens. Tegelijk is het ook een context waarin gezichtsherkenningstechnologie mogelijk een meerwaarde biedt. Het herkennen van personen of het toegang verlenen tot het huis van een persoon met geheugenverlies, en een

app die slechtzienden helpt om mensen in hun directe omgeving waar te nemen, zijn voorbeelden van toepassingen die mensen kunnen ondersteunen in hun leven en autonomie.

- **Commerciële doeleinden:** Veel van de voorziene toepassingen van gezichtsherkenningstechnologie zijn te categoriseren binnen de bedrijf-burger-relatie, waarbij het gaat om het vergroten van het gebruikersgemak (snelle incheck en registratie bij evenementen), het inspelen op emoties van klanten om producten of diensten aan te passen (retail) of om efficiëntere bedrijfsvoering te bewerkstelligen.
- **Beveiligingsdoeleinden:** Gezichtsherkenning kan ook worden gebruikt voor beveiligingsdoeleinden, zoals het gebruik voor identificatie- en authenticatiedoeleinden bij kritische infrastructuur. In hoeverre bijvoorbeeld een slimme deurbel, ingezet anders dan voor zieken en hulpbehoevenden, nu echt moet worden gezien als een hulpmiddel in het kader van een beveiliging van een woning of eerder moet worden gezien als een leuk gadget, is op dit moment niet eenduidig vast te stellen.
- **Recreatieve doeleinden:** Veel van de toepassingen van gezichtsherkenningstechnologie binnen burger-burger-relaties zijn aan te merken als toepassingen voor vermaak.

Voorts is het belangrijk om te expliciteren wat de grondhouding van de wetgever is ten opzichte van ontwikkelingen op het gebied van gezichtsherkenningstechnologie. De volgende benaderingen kunnen worden onderscheiden:

- **Risicomijdend:** Het uitgangspunt is dat gezichtsherkenningstechnologieën momenteel nog weinig vermogen en dat het maar de vraag is of dit in de toekomst anders zal zijn. In ieder geval worden er de nodige nadelen en risico's gesignaleerd ten aanzien van de toepassing van dergelijke technologieën. Daarom wordt de inzet van deze technologieën zoveel mogelijk aan banden gelegd, eventueel tot het moment dat er aanleiding zou zijn om te geloven dat dergelijke technologieën meer voordelen zouden bieden dan momenteel het geval is. Dit sluit aan bij het voorzorgsbeginsel: omdat het nu nog niet goed is in te schatten hoe de technologieën zich zullen ontwikkelen en hoe de gegevens die nu worden verzameld mogelijk in de toekomst kunnen worden gebruikt of misbruikt, past terughoudendheid.
- **Risicobeperkend**: Er wordt van uitgegaan dat gezichtsherkenningstechnologieën gebruik maken van zeer gevoelige gegevens en niet alleen zeer invasief zijn, maar ook de nodige risico's met zich mee kunnen brengen. Toch wordt erkend dat in bijzondere contexten de toepassing van deze techniek een positief effect zou kunnen sorteren. Daarom wordt de regulering die momenteel voorhanden is nader ingevuld en verder bijgestuurd, om duidelijk te maken dat gezichtsherkenningstechnologie in principe niet kan worden gebruikt, tenzij voldaan wordt aan voorwaarden die zijn neergelegd in wetgeving of in andersoortige regulering.
- **Kansbevorderend:** Er wordt van uitgegaan dat gezichtsherkenningstechnologieën weliswaar een aantal risico's met zich meebrengen, maar ook de nodige kansen. Daarom wordt geopteerd voor een gediversifieerde aanpak waarbij binnen een aantal sectoren wordt ingezet

op het toestaan van (experimenten met) gezichtsherkenningstechnologieën. Op basis van de resultaten die daar worden behaald en een evaluatie van de diverse voor- en nadelen wordt vervolgens een keuze gemaakt ten aanzien van de andere gebieden waarin gezichtsherkenningstechnologieën eventueel een rol zouden kunnen spelen.

- **Kansoptimalisatie:** Er wordt van uitgegaan dat gezichtsherkenningstechnologieën zich op termijn zullen ontwikkelingen op een wijze die veel positieve effecten heeft voor de burger, het bedrijfsleven, de economie en het welzijn in Nederland. Deze positieve gevolgen kunnen in ieder geval, eventueel met hulp van ondersteunende maatregelen, de eventuele negatieve gevolgen overschaduwen. Daarom wordt het van belang geacht dat de diverse barrières en obstakels die er nu in de wetgeving zijn vervat zo veel mogelijk worden weggenomen.

Deze vier benaderingswijzen zullen in onderstaande tabellen worden uitgesplitst, waarbij zal worden aangegeven welke reguleringsoptie voor de hand ligt ten aanzien van welk type relatie en welk type doeleinde. Daarbij zullen de reguleringskeuzes worden aangegeven in kleuren: **risicomijdend**, **risicobeperkend**, **kansbevorderend** en **kansoptimalisatie**.[1] Daarbij moet uiteraard worden opgemerkt dat bewustwording bij iedere reguleringskeuze als een ondersteunende maatregel kan worden gezien.

	Burger-burger	Bedrijf-burger	Werkgever-werknemer
Totaal verbod			
Voorafgaande goedkeuring			
Gediversifieerde aanpak			
Specifiek wettelijk kader	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////
Controle achteraf			
Sectorale controle			
Bewustwording			
Gedoogbeleid			

Tabel 1: reguleringsopties per type relatie

[1] //////////////////////////// staat voor de combinatie risicobeperkend/kansbevorderend.

	Zorgdoeleinden	Commerciële doeleinden	Beveiligings-doeleinden	Recreatieve doeleinden
Totaal verbod				
Voorafgaande goedkeuring				
Gediversifieerde aanpak				
Specifiek Wettelijk kader	//////////////////// ////////////////////	//////////////////// ////////////////////	//////////////////// ////////////////////	//////////////////// ////////////////////
Controle achteraf				
Sectorale controle				
Bewustwording				
Gedoogbeleid				

Tabel 2: reguleringsopties per context

Gezichtsherkenningstechnologie in horizontale relaties is nog geen voldongen feit in Nederland; het is gezichtsherkenning “op het eerste gezicht”. Maar de toepassingen die wereldwijd worden ontwikkeld en de privacyrisico’s die daarmee gepaard gaan zijn zeker reëel. Dit maakt dat de Nederlandse samenleving nu de fundamentele vraag dient te stellen: “wat vinden wij wenselijk als het gaat om gezichtsherkenningstechnologie in onze democratische rechtsstaat?” Dit rapport poogt bij te dragen aan deze gedachtenvorming en bovendien handvatten te bieden aan de Nederlandse regering, de wetgevende macht en aan de relevante handhavende organisaties om op een transparante en systematische wijze te kiezen voor de meeste geschikte reguleringsoptie(s).

Summary

Facial recognition technology is used to recognize faces or facial features based on digital images (for example a photo or video). For some time, governments have deployed the technology on a limited scale for detection and security purposes but in recent years, it has also become available to businesses and citizens. This opens up a range of opportunities for commercial companies and individuals to identify, track and profile people. For example, search engines and social media platforms, use facial recognition technology to automatically describe and label (tag) portraits and images; in the retail sector the technology is used to monitor shopping customers and to provide personalized services and promotions; at events it is used to grant or deny access; and various companies offer facial analysis and facial recognition modules and APIs so others can develop, for example, smartphone applications. Such do-it-yourself facial recognition applications can be used to identify others on the street and find information about them, such as previous behavior, relationships with others or personal preferences.

As it is likely that facial recognition applications will be available on a substantial scale for both citizens and businesses in the near future, it is necessary to evaluate whether and, if so, what adjustments to the current legal framework and other regulatory instruments are needed. It is important to note here, that this research focuses exclusively on the use of facial recognition technology in the horizontal relationship: relationships between companies and citizens and citizens themselves. The use of face recognition technology in the vertical relationship, that is to say between governments and citizens, is not part of this research.

This research is based on a broad literature study into automated facial recognition technology and privacy violations for which, in addition to academic literature, news reports, websites, blogs, press releases and brochures have been investigated. For this, we have studied material from both the Netherlands and abroad. The literature study focused on four specific facial recognition applications (so-called domain studies). These domain studies focus on: the event sector, smartphone apps, the smart doorbell and the retail sector. For these domain studies, the literature study was further supplemented with 11 stakeholder and expert interviews. A workshop was also organized with 12 experts, during which a number of domain studies were critically discussed, and the first findings were presented. To map out the current legal means to regulate facial recognition technology, a legal review has been carried out that focuses on privacy and data protection, private law and criminal law. Finally, a number of regulatory options have emerged as well as factors that determine the choice between the various options.

Two questions are central to this study:

1) *How is facial recognition technology used by Dutch citizens and companies and how can the use of facial recognition technologies by citizens and companies infringe the privacy of citizens (now and in five years)?*

2) How can privacy violations, both current and potential, be prevented or limited?

The answer to these questions as it follows from the research is as follows:

Answer to question 1: applications and privacy risks

Facial recognition applications in the horizontal relationship (company-citizen and citizen-citizen) are still in the experimental phase in the Netherlands. Companies are researching, on a limited scale, whether cost-effective facial recognition applications can be introduced. This step-by-step approach taken by companies is not merely motivated by economic motives. The growing awareness that the use of facial recognition entails privacy risks and careless handling leads to potential risks of harm, which leads to companies not wanting to act prematurely. Interviews with the representatives of companies show that it is not always clear to them how the various legal requirements, such as those laid down in the General Data Protection Regulation (GDPR), should be interpreted with regard to facial recognition. This also contributes to the choice of a cautious course.

The number of facial recognition applications in the Netherlands is relatively limited; the projects that are already running are mainly at the initiative of companies. So far, they mainly use this technology for unambiguous and specific purposes. It often concerns a certain form of access control. These applications are not purely of Dutch origin. For instance, American companies also provide facial recognition services to the Dutch market. The initiatives that have taken off in the citizen-citizen relationship mainly concern applications aimed at convenience and entertainment (for example smartphone apps) and access control (for example smart doorbell with facial recognition). Finally, it is also possible for citizens to get started with facial recognition technology. Citizens with some programming knowledge can use online services to develop facial recognition applications themselves.

Whereas the Netherlands is still in the experimental phase, there are already more diverse facial recognition applications abroad - particularly outside the EU - which, however, are often still in the implementation phase there. These foreign applications give an idea of what is technologically possible and what might be expected in the Netherlands in the near future. Possible directions for development of facial recognition applications in the next 5 years may include use for:

- **Ease and efficiency:** At present, facial recognition applications are mainly marketed with the promise of making existing processes run more smoothly. A quick check-in at events via facial recognition, paying in stores via facial recognition, remote access to your house via the smart doorbell, etc. Facial recognition can also be used to enrich existing activities with extra possibilities, such as dating apps that offer the possibility to search for look-a-likes of famous people. Most facial recognition applications that are used in the Netherlands are focused on

efficiency, convenience and entertainment. If this tendency continues and goes together with faster systems that also work independently on portable, small devices, a possible consequence may be that facial recognition will take a prominent place in social settings. Smartphone apps used for social interactions may therefore get a facial recognition component, for example to enable people who get to know each other through online platforms to be able to identify each other offline. Conversely, the large amount of information that has become available online about people in recent years may be linked to individuals offline when they are recognized through facial recognition. Moreover, if ease and efficiency remain the guiding principle in future developments and application of facial recognition, then it may also be the case that all actions that are now required for identification are replaced by facial recognition. Access cards, bonus cards, all kinds of passwords and access codes then become superfluous.

- **Security and control:** Often the above examples also have a control and / or safety component. Checking in via face recognition is not only useful, it also offers the possibility of automatically denying unwanted individuals' access to certain areas on the basis of blacklists. Face recognition is not only used to tag photos but also to prevent identity fraud. Emotion detection as a specific form of facial recognition can also play a role in security and control, such as when certain emotions such as fear and anger are automatically recognized and used to act quickly and prevent escalation. If the use of facial recognition for such purposes continues and the accuracy and speed of the technology increases, then it is conceivable that facial recognition will be linked to restricting access to places and services. It can then become a powerful tool to ward off individuals or groups and to combat behavior that is deemed undesirable.
- **Personalization and proactive services:** Facial recognition can also be used to personalize services and offer them proactively. In the retail sector, menus and offers are already being adjusted based on face and emotion recognition. Certainly, the possibility of being able to monitor how customers feel with emotion detection, a specific form of facial recognition, automated and real-time, and then be able to respond proactively to this is an application that is considered promising by commercial parties. New functionalities that further refine personalized services or advertisements, such as measuring the heart rate on the basis of digital video images of faces, make the automatic analysis of faces even more attractive. If this tendency continues, it is possible that through facial recognition, data can be linked in real time to individuals in the (semi) public space with the aim of influencing their actions (also known as nudging) or profiling them. Nobody will get to see the same offers in stores anymore and in an automated way a distinction can be made in the way people are treated. Facial recognition then becomes an important key to make data-driven decisions and to influence citizens' choice infrastructure in daily life.

Based on facial recognition developments and the scenarios outlined above, the following privacy risks have been identified:

- **Non-transparent information collection**: a lot of facial recognition technology currently works on the basis of models that have been trained with data for which no permission has been given. The internet is an important source for this, but also images obtained in the public space are used for this. Because this data collection takes place on a global level, it is difficult to control this. Citizens lose control of what happens with their photos and videos.
- **Autonomy under pressure:** From a commercial point of view, well-functioning facial recognition often means that citizens do not have to perform extra actions to let the technology do its work. However, the absence of an active action also deprives them of an important choice and reflection moment. Do I really want this? In the situation that citizens are aware of the presence of the facial recognition application and are offered the possibility of obtaining a service or entering space without facial recognition, it might often be the case that the alternative without facial recognition becomes a very stripped-down option with very little being invested in it. Those who hold on to the latter option must then be satisfied with a less-sophisticated service or basic product.
- **Bias and errors in facial recognition:** Although the quality and reliability of facial recognition technology has increased enormously in recent years, it remains a known and not to be underestimated problem that, among other things, *biases* in the training data, facial recognition applications generate outcomes that are discriminatory in nature and work less well with certain groups (such as women, children and persons with a tinted skin color). For these groups there is a greater chance that they will either be recognized incorrectly or not recognized at all, with the result that they will, for example, be denied access to an event, or that they cannot use certain services, which can lead to exclusion and stigmatization.
- **The end of anonymity:** When facial recognition becomes widespread in the horizontal relationship and can be easily deployed by both companies and citizens, it will become increasingly difficult for people to move anonymously into the public, semi-public, and even private space.
- **Dependence on others**: When facial recognition through example apps is used by citizens in social interaction, they are largely dependent on the prudence and discretion of the user to not infringe on their privacy. However, many citizens already find it difficult to estimate, for example, how large the audience is that they reach with online information sharing. This problem is intensified by facial recognition.
- **Secondary use of data:** Although the focus of this study is on the horizontal relationship, an important privacy risk is that governments turn to companies to be able to use the facial recognition information collected in the horizontal relationship. This specific form of secondary use is already known from internet companies that receive - sometimes compelling - requests to share information with, among others, intelligence services. Guaranteeing privacy in

horizontal relationships is therefore also important for protecting privacy in vertical relationships.

- **Inequality of power and chilling effect:** Facial recognition applications that focus on control or personalization actually always do this in combination with other, already existing data files. The face becomes a starting point for other (online) available information about that person. Facial recognition is then no longer simply about recognizing someone, but about making a whole range of information about that person accessible. The information-rich profiles that this creates can affect the privacy of citizens in various ways. This makes it increasingly difficult for citizens to estimate what others know about them. This can lead to power shifts in the horizontal relationship that cause citizens to adjust their behavior as a precaution (chilling effect). Moreover, when the information gained through facial recognition is used to stalk or threaten someone, physical privacy may also be at stake.

Answer to question 2: Best practices and regulatory options

In order to understand how current and potential privacy violations can be prevented or limited, we charted the existing best practices of companies that use and / or develop facial recognition technologies, we conducted a legal analysis, and identified a range of regulatory options.

The following are referred to as Best Practices for protecting the privacy of citizens in the literature and by companies. It should be noted that we have not been able to verify their effectiveness:

- **Services and products instead of data as a pillar of the business model:** Business models where data trading is not the core are preferred.
- **Privacy-by-design:** The design of the system focuses as much as possible on privacy-friendly choices.
- **Company values:** Company values such as transparency, consent, fairness and accountability underpin and limit business choices.
- **Public information:** Companies invest in quality education for customers and citizens.
- **Regulation:** Companies are demanding clear regulation from the government and are developing self-regulation.
- **Permission**: Companies opt for asking consent, even if this is not required by law.

From the legal analysis follows that the current legal tools for regulating facial recognition technology are mainly found in the General Data Protection Regulation, in private law and in particular in the unlawful act and to a limited extent in criminal law. In general, the General Data Protection Regulation will apply to facial recognition technology. This implies that the use of facial recognition in horizontal relationships will only be permitted by law in limited cases. There are legal questions about, among other things, the existence of a legitimate processing basis, and more

generally there are doubts about the necessity, proportionality and subsidiarity of facial recognition applications. After all, the mere fact that a user agrees to a technology or application does not in fact permit its use.

In addition, it must be borne in mind that for the use of facial recognition, biometric data is processed that is legally designated as special personal data, for which a no-unless regime applies. For the use of biometric data in horizontal relationships (specifically: employer-employee relationship), the legislator gives the example that a nuclear power plant may be allowed to use facial recognition technologies to provide access to the facility for registered employees only. This means that most of the other examples discussed in the report are incomparable in their seriousness, importance and necessity. The Dutch Data Protection Authority can play an important role in the supervision of such technologies.

Criminal law currently plays only a limited role in the regulation of facial recognition technologies. However, by analogy with the existing protection against covertly making pictures, the legislator could consider making covert facial recognition punishable, even if the camera itself is recognizable. It must be considered whether applications and use are so serious that prosecution and enforcement through criminal law is appropriate. Finally, it is obvious that this should be done through private law and tort in case a citizen or a company wants to take action themselves.

A range of regulation options is open to the legislator, such as:

- **Total ban:** First of all, the Dutch legislator can choose to lay down a (temporary) total ban for the use of facial recognition technologies. This provides clarity and only a marginal number of possible applications that are currently legally legitimate are nipped in the bud. In other words: this is now still an option with relatively limited negative consequences. The functionalities of apps are still very limited, the results are not always reliable, and the potential benefits are mostly marginal. If the Netherlands opted for a strict regulatory line, that line could be evaluated at a later time, once the technology and applications have developed. This would tie in with the strict line that seems to be developing in the EU.
- **Prior approval:** With this option, applications may only be used and offered if prior approval has been obtained. The Netherlands Data Protection Authority has a natural role to play here. Because this is a technology that uses special personal data, it is obvious to perform a Data Protection Impact Assessment. The Data Protection Authority could issue a guideline from which follows that parties must always submit a Data Protection Impact Assessment and that they may only start after explicit approval of the Data Protection Authority.
- **Diversified approach:** In order to eliminate the legal uncertainty regarding the admissibility of specific facial recognition applications, the legislator, government or the Dutch Data Protection Authority may decide to state explicitly which applications are permitted and which are not. A

distinction can be made between domains, applications and the positive or negative effects on the lives of citizens.

- **Regulatory framework specific to facial recognition:** The legislator or the Dutch Data Protection Authority has the freedom to develop a specific regulatory framework for facial recognition technologies, whether or not in collaboration with other supervisors and (international) parties, in which the general legal principles are formulated in concrete terms with regard to this technology and for the type of applications that are foreseen and considered legitimate.
- **Ex post control:** It may also be decided to maintain the current regulatory framework and to focus on ex post control of technologies, applications and their use. This check can be carried out either at the initiative of a citizen or company submitting a complaint or at the initiative of an enforcement organization, such as the Dutch Data Protection Authority.
- **Code of conduct and certification:** The General Data Protection Regulation makes it possible to develop a separate code of conduct for specific sectors or applications, with a specific enforcement and supervisory organization established by that code. The question is whether facial recognition is really a separate sector where a representative body can draw up such a code and submit it to the Dutch Data Protection Authority. Perhaps working with certification is therefore the more obvious choice, for which the General Data Protection Regulation also offers scope. It is then up to a possibly accredited certification body to issue a certificate to a company that is expected to use facial recognition technology in accordance with the General Data Protection Regulation. The Dutch Data Protection Authority can supervise whether such certification is done correctly.
- **Awareness:** The government can focus on public campaigns to make it clear to citizens and businesses what dangers and legal (and possibly also social and ethical) limits there are to applying facial recognition technologies. Social norms will play an important role in the way facial recognition is applied, especially in citizen-citizen relationships. With facial recognition, a social norm could be helpful, for example, to deliberately not target smartphones at people in a way that they would feel viewed, recognized and categorized. Although such a standard cannot be imposed, policy-oriented awareness-raising interventions can contribute to the development of social norms that can help reduce the privacy risks of facial recognition. A great deal can also be gained with regard to companies. An investigation by the Dutch Data Protection Authority into the admissibility of facial recognition technology in a specific case can also have a clear normative effect and create more awareness of the potential dangers of facial recognition technologies.
- **Tolerance policies:** Finally, the Dutch Data Protection Authority or the government can indicate in policies that the use of facial recognition will be tolerated for a certain period of time and compliance with legal frameworks will not be enforced, in order to give it the chance to reach maturity and to evaluate only after a few years what advantages and potential

disadvantages there are to facial recognition technologies. However, it should be borne in mind that citizens can enforce their rights as enshrined in the European Convention on Human Rights and the General Data Protection Regulation through judicial proceedings, and that ultimately the European Court of Human Rights and the European Court of Justice will pass judgment.

To support the decision-making, we have made a distinction between types of relationships, objectives, and approaches. A thorough assessment can be made by looking sharply at who and for what purposes facial recognition is applied and making abundantly clear what the general attitude of the government is towards facial recognition (from risk avoiding to optimizing opportunities).

Three specific, horizontal relationships can be distinguished:

- **Citizen-citizen:** In this study we have seen virtually no examples of applications that will stand the test of necessity, proportionality, subsidiarity and legitimacy. It should be noted that the technology can facilitate malicious citizens in their actions (such as stalking or identity theft) and that at present citizens have access to commercial services that offer them the opportunity to work with facial recognition technology themselves.
- **Company-citizen:** Although this relationship often involves applications with a clear and serious purpose, the study shows that the most important legal stumbling block to using facial recognition applications here is that there are perfectly good and less invasive technological alternatives.
- **Employer-employee:** Overall, an employee will not be able to give free permission. Grosso modo, as the ground for processing, only the existence of a generally important interest can be invoked (think of the security protection of nuclear power plants).

A distinction can also be made between different purposes for which facial recognition technology is used. In addition, there is obvious overlap with the previous list; it's just another way to categorize the various applications:

- **Health care purposes:** The health care context is a special context because it often concerns vulnerable people and sensitive data. At the same time, it is also a context in which facial recognition technology may offer added value. Recognizing people or granting access to the home of a person with memory loss or an app that helps visually impaired people to perceive people in their immediate environment are examples of applications that can support people in their lives and autonomy.
- **Commercial purposes:** Many of the anticipated applications of facial recognition technology can be categorized within the business-citizen relationship, which involves increasing user-

friendliness (rapid check-in and registration at events), responding to customer emotions to adjust products or services (retail) or to achieve more efficient business operations.

- **Security purposes:** Facial recognition can also be used for security purposes, such as the use of facial recognition technologies for identification and authentication purposes for critical infrastructure. To what extent, for example, a smart doorbell, used other than for the sick and those in need of help, should really be seen as a tool in the context of a safe entry policy for a private home or rather seen as a nice gadget, cannot be clearly determined at the moment.
- **Recreational purposes:** Many of the applications of facial recognition technology within citizen-citizen relationships can be classified as applications for entertainment.

It is important to make explicit what the basic attitude of the legislator is towards developments in the field of face recognition technology, such as:

- **Avoiding risks:** In principle facial recognition technologies currently have little power and the question is whether this will be different in the future. In any case, there are necessary disadvantages and risks identified with regard to the application of such technologies. That is why the use of these technologies is being restricted as much as possible, possibly until there is reason to believe that such technologies would offer more benefits than is currently the case. This is in line with the precautionary principle: because it is not yet possible to estimate how the technologies will develop and how the data that is currently being collected may be used or misused in the future, restraint is appropriate.
- **Risk mitigation**: It is assumed that facial recognition technologies use highly sensitive data and are not only highly invasive but can also entail the necessary risks. Yet it is recognized that in special contexts, the application of this technique could have a positive effect. That is why the regulation that is currently available should be further specified and further adjusted to make it clear that facial recognition technology cannot in principle be used, unless where explicitly indicated and under the conditions laid down, either in legislation or in other types of regulation.
- **Promoting opportunities:** It is assumed that facial recognition technologies involve a number of risks, but also the necessary opportunities. That is why one can opt for a diversified approach in which efforts are made within a number of sectors to allow (experiments with) facial recognition technologies. Based on the results achieved there and an evaluation of the various advantages and disadvantages, a choice may then made with regard to the other areas in which facial recognition technologies could possibly play a role.
- **Optimization of opportunities:** It is assumed that facial recognition technologies will develop in the long term in a way that has many positive effects for citizens, business, the economy and well-being in the Netherlands. These positive effects can in any case, possibly with the help of support measures, overshadow any negative consequences. It is therefore considered

important that the various barriers and obstacles that are now contained in the legislation are removed as much as possible.

These four approaches will be broken down into the tables below, indicating which regulatory option is obvious with regard to which type of relationship and which type of purpose. In addition, the regulatory choices will be indicated in colors: **risk-avoiding**, **risk-limiting**, **chance-promoting** and **chance-optimization**.[2] It should, of course, be noted that awareness of every regulatory choice can be seen as supportive.

	Citizen-citizen	Company-citizen	Employer - employee
Total ban			
Prior approval			
Diversified approach			
Specific legislative framework	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////
Ex post control			
Sectoral control			
Awareness			
Tolerance policy			

Table 1: Regulatory options per type of relationship

	Health care purposes	Commercial purposes	Security purposes	Recreational purposes
Total ban				
Prior approval				
Diversified approach				
Specific legislative framework	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////
Ex post control				
Sectoral control				
Awareness				
Tolerance policy				

Table 2: Regulatory options per context

[2] //////////////////////////// refers to the combination of risk-limiting and chance-promoting.

Facial recognition technology in horizontal relationships is not yet an accomplished fact in the Netherlands, it is facial recognition “at first sight”. Nevertheless, the applications that are being developed worldwide and the associated privacy risks are real. This means that Dutch society must now ask the fundamental question: "what do we find desirable when it comes to facial recognition technology in our democratic constitutional state?" This report aims to contribute to this development of ideas and, moreover, to offer guidance to the Dutch government, the legislative power and possibly the relevant enforcement organizations to opt for the most suitable regulatory option(s) in a transparent and systematic manner.

1. Inleiding

Geautomatiseerde gezichtsherkenning heeft de laatste jaren een grote vlucht genomen als gevolg van doorbraken in kunstmatige intelligentie en goedkopere en krachtigere computertechnologie. Met gezichtsherkenningstechnologie[3] bedoelen wij verschillende soorten digitale technieken die gebruikt worden om op basis van digitale beelden, bijvoorbeeld een foto of video, geautomatiseerd gezichten of gezichtskenmerken te herkennen.[4] Overheden gebruiken de technologie al enige tijd op beperkte schaal voor opsporing en beveiliging, maar inmiddels is de technologie ook in verschillende commerciële producten aanwezig voor burgers en bedrijven. Zoekmachines en sociale-mediaplatformen maken er gebruik van om portretten en beelden automatisch te beschrijven en van labels (*tags*) te voorzien;[5] smartphones kunnen ontgrendeld worden door middel van gezichtsherkenning; er zijn apps verkrijgbaar die beloven mensen op straat te herkennen; [6] en diverse organisaties en bedrijven bieden gezichtsanalyse- en gezichts-herkenningsmodules aan waarmee gebruikers zelf aan de slag kunnen gaan om toepassingen te ontwikkelen.[7]

De beschikbaarheid van gezichtsherkenningstechnologie voor commerciële toepassingen opent een scala aan nieuwe mogelijkheden om mensen te identificeren, te volgen, met elkaar in verband te brengen, te profileren en te benaderen. Winkels kunnen het inzetten om hun klanten te monitoren tijdens het winkelen en hen gepersonaliseerde aanbiedingen te doen. Bij evenementen kan de technologie worden ingezet om mensen toegang te verschaffen of juist te weigeren. Wanneer gezichtsherkenning wordt gecombineerd met andere informatiebronnen (bijvoorbeeld sociale-mediafoto's), kunnen mensen de technologie gebruiken om anderen op straat te identificeren en hen in verband te brengen met hun eerdere gedrag of uitspraken, met andere mensen of met hun voorkeuren, zonder dat zij daarvoor toestemming hebben gegeven of zelfs in de gaten hebben dat dit gebeurt. Waar men voorheen nog redelijk anoniem over straat kon gaan of in de trein of het café kon zitten, loopt men met de toenemende aanwezigheid van gezichtsherkenningstechnologie een steeds grotere kans om op elk moment herkend te kunnen

[3] In deze verkenning gebruiken wij afwisselend de termen geautomatiseerde gezichtsherkenning, gezichtsherkenningstechnologie en gezichtsherkenning om hetzelfde aan te duiden.
[4] W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld 'Face recognition: A literature survey' (2013) 35(4) ACM Computing Surveys 399.
[5] Zie bijvoorbeeld Shannon Liao, 'Google wins dismissal of facial recognition lawsuit over biometric privacy act' (2018) The Verge <http://www.theverge.com/2018/12/29/18160432/google-facial-recognition-lawsuit-dismissal-illinois-privacy-act-snapchat-facebook> geraadpleegd 4 februari 2019; Zak Stone, Todd Zickler en Trevor Darrell, 'Toward Large-Scale Face Recognition Using Social Network Context' (2010) 98 Proceedings of the IEEE 1408; Kwontaeg Choia, Kar-Ann Tohb en Hyeran Byuna, 'Incremental Face Recognition for Large-Scale Social Network Services' (2012) 45 Pattern Recognition 2868; K Chaykowski, 'Facebook's New Facial Recognition Switch Can Find Photos Of You Across The Social Network' (2017) Forbes <www.forbes.com/sites/kathleenchaykowski/2017/12/19/facebooks-new-facial-recognition-switch-can-find-photos-of-you-across-the-social-network/#415f44303fd7> geraadpleegd 4 februari 2019.
[6] Michelle Starr, 'Facial Recognition app Matches Strangers to Online Profiles' (2014) Cnet <www.cnet.com/news/facial-recognition-app-matches-strangers-to-online-profiles/> geraadpleegd 31 januari 2019.
[7] In Nederland bijvoorbeeld: Deurplus <www.deurplus.com/zakelijk/toegangscontrole/gezichtsherkenning/> geraadpleegd 7 februari 2020; ibid.

worden. Automatisch gezichtsherkenning kan dus de nodige privacy-inbreuken opleveren: het kan de individuele vrijheid en het vermogen van burgers een ongestoord leven te leiden, aantasten. Deze inbreuken kunnen ertoe leiden dat het in publieke en semipublieke ruimten steeds moeilijker wordt voor mensen om onbevangen zichzelf te kunnen zijn.

De mogelijke privacyrisico's van gezichtsherkenningstechnologie in de relaties tussen burgers onderling is aan de orde gesteld en uitgewerkt in de Initiatiefnota *Onderlinge privacy* van Tweede Kamerlid Sven Koopmans, als onderdeel van de bredere problematiek rondom onderlinge privacy tussen burgers in het licht van nieuwe technologieën.[8] Naar aanleiding van deze initiatiefnota, heeft de minister van Justitie en Veiligheid toegezegd om een verkennend onderzoek uit te laten voeren naar de wijze waarop het gebruik van gezichtsherkenningstechnologie door burgers en bedrijven een inbreuk kan vormen op de privacy van de burger, en naar de mogelijkheid om die potentiële privacy-inbreuk te voorkomen of te beperken.[9] Deze verkennende studie heeft in dit kader plaatsgevonden en biedt inzicht in de gesignaleerde problematiek en identificeert mogelijkheden voor regulering.

1.1. Vraagstelling

In deze verkenning richten wij ons op de privacyrisico's die voor burgers kunnen ontstaan bij het gebruik van automatische gezichtsherkenning door burgers en bedrijven en de mogelijke reguleringsopties die de overheid heeft om deze risico's te beperken. De centrale onderzoeksvragen, zoals geformuleerd door de opdrachtgever (i.e. het WODC), zijn:

1) *Hoe wordt gezichtsherkenningstechnologie door Nederlandse burgers en bedrijven gebruikt en hoe kan het gebruik van gezichtsherkenningstechnologieën door burgers en bedrijven een inbreuk vormen op de privacy van de burger (nu en over vijf jaar)?*
2) *Hoe kunnen huidige en potentiële privacy-inbreuken worden voorkomen of beperkt?*

Om deze vragen te verduidelijken is het noodzakelijk eerst kort stil te staan bij wat wij begrijpen onder privacy. Wetenschappelijke verhandelingen over privacy nemen vaak de disclaimer op dat privacy een zeer complex en 'fuzzy' concept is, wat definiëring ondoenlijk, zelfs onmogelijk zou maken. Er is discussie over wat het recht op privacy inhoudt, waar de lijn te trekken tussen privacy en gegevensbescherming en of privacy een instrumentele dan wel een intrinsieke waarde heeft. Wie ernaar streeft om de essentie van privacy te vatten, loopt enerzijds het risico te eindigen met een zeer beperkte privacyopvatting die niet alle domeinen bestrijkt die wij intuïtief wel onder privacy

[8] *Kamerstukken* 2017/18, 34926, nr. 2. Initiatiefnota van het lid Koopmans: Onderlinge privacy. Gepubliceerd op 5 april 2018.
[9] *Kamerstukken* 2017/18, 34926, nr. 7. Verslag van een notaoverleg. Gepubliceerd op 18 juli 2018.

zouden scharen, of anderzijds een definitie van privacy te formuleren die zo breed is dat het allerlei zaken omvat die wij door de band genomen helemaal niet onder privacy verstaan.[10]

Misschien is het enige punt waarover de meeste privacy-experts het wel eens zijn dat de sociale dimensie van privacy iets is wat voortdurend aan verandering onderhevig is en dat technologie daarin een centrale rol speelt.[11] De vele definities die de afgelopen eeuw (en langer) opmars maken, kunnen bijvoorbeeld niet los gezien worden van de technologische innovaties die diezelfde privacy onder druk zetten. Zo is het bekende, door juristen Warren en Brandeis geformuleerde, 'recht om met rust gelaten te worden' beïnvloed door de toenmalige opkomst van fotograferende tabloid-journalisten en is Westins focus op 'controle over informatie' mede ingegeven door de opmars van computers in de jaren 60 van de vorige eeuw.[12] Het ligt niet binnen de scope van dit onderzoek een overzicht te bieden van deze privacydiscussies en opvattingen. Dat is ook niet nodig voor de beantwoording van de vragen.

De ogenschijnlijke ongrijpbaarheid van wat privacy is, vatten wij in deze verkenning niet op als een onoverkomelijk probleem, maar eerder als een zwaarwegende reden om privacy als een meervoudig en flexibel in plaats van een eenduidig of absoluut fenomeen te begrijpen. Privacy moet daarom begrepen worden als onderdeel van een specifieke context. Dit houdt in dat afhankelijk van onder meer de betrokken actoren, de ingezette technologie en de plaats en tijd, sommige privacyaspecten meer op de voorgrond zullen treden dan andere.

Voor een deel is deze contextuele afbakening al bepaald in de onderzoeksopdracht. Deze vraagt met name te kijken naar horizontale relaties waarbij gezichtsherkenningstechnologie wordt ingezet.[13] Het gaat dan om burgers die de technologie gebruiken om anderen automatisch te herkennen, bijvoorbeeld via een app op een telefoon, of om bedrijven die de technologie inzetten om burgers te herkennen om bijvoorbeeld toegang tot gebouwen te verlenen. Dat betekent dat wij ons niet richten op publieke en publiek-private toepassingen, zoals het gebruik van gezichtsherkenning door politie of door publiek-private samenwerkingsverbanden tussen bijvoorbeeld politie, gemeentes en voetbalstadions. Wij hebben ervoor gekozen het onderzoek verder contextueel in te bedden door vier specifieke toepassingsgebieden centraal te stellen (zogenaamde domeinstudies, zie hoofdstuk 2 voor verdere toelichting).

Een tweede toelichting die nodig is om de onderzoeksvragen te verduidelijken betreft ons begrip van regulering. Wij achten het van belang om bij een analyse van horizontale privacy en de mogelijkheden om risico's te beperken een brede opvatting van regulering te hanteren. Dat wil zeggen dat wij niet alleen naar juridische mogelijkheden kijken maar ook naar andere

[10] Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087.
[11] JB Rule (2015) 'Privacy: the longue durée' in B Roesler and D Mokrosinska (eds), *Social Dimensions of Privacy*: *Interdisciplinary Perspectives* (Cambridge University Press 2015) 11-31.
[12] Alan F Westin, 'Privacy And Freedom' (1968) 25 Washington & Lee Law Review 166.
[13] Vgl. *Kamerstukken* 2017/18, 34926, nr. 7. Verslag van een notaoverleg. Gepubliceerd op 18 juli 2018.

reguleringsvormen, zoals technische opties en mogelijkheden tot het beïnvloeden van sociale waarden en normen omtrent het gebruik van gezichtsherkenning.

Bedrijven zijn een relatief makkelijk object voor regulering door middel van juridische middelen, hoewel de effectiviteit van regulering sterk afhankelijk zal zijn van de beschikbare instrumenten en de capaciteit om rechtsnormen te handhaven. Het reguleren van burgers onderling is op het gebied van privacy moeilijker juridisch te regelen en te handhaven, onder andere vanwege de schaal en (on)zichtbaarheid van privacy-inbreuken. Zo vormt de relatieve onzichtbaarheid van het gebruik van gezichtsherkenningsapps op smartphones bijvoorbeeld een uitdaging. Er moet rekening mee worden gehouden dat burgers ook zelf met gezichtsherkenningstechnologieën aan de slag gaan of simpelweg bestaande technologieën inzetten op een manier die niet was voorzien door de bedrijven die deze in de markt hebben gezet.

De potentiële grootschaligheid van toepassingen door burgers en bedrijven maakt handhaafbaarheid van wetgeving een aanzienlijke uitdaging. Hoewel de focus van dit onderzoek ligt op de toereikendheid van juridische instrumenten om gezichtsherkenning te reguleren, hebben wij daarom ook gekeken naar alternatieve reguleringsinstrumenten die met name in de horizontale relaties tussen burgers toepasbaar zijn. Zo is er ook aandacht voor de mogelijkheid om via sociale normen en waarden gezichtsherkenning op een verantwoorde en acceptabele manier in het sociale verkeer in te bedden en voor privacy-by-design-methoden (reguleren via technologie).[14] Het doel van het onderzoek is aldus om de privacyrisico's in kaart te brengen en de verschillende mogelijkheden om deze risico's te beperken middels regulering in brede zin te verkennen.

Gegeven de interpretatie van horizontale privacy en regulering zoals hierboven beschreven, hebben wij de twee centrale onderzoeksvragen verder gespecificeerd tot de volgende deelvragen:

Voor vraag 1:

1.1) Hoe wordt gezichtsherkenningstechnologie momenteel door burgers en bedrijven gebruikt? En hoe verwachten experts dat het gebruik van deze technologie zich de komende vijf jaar zal ontwikkelen?

1.2) Hoe kan het gebruik van gezichtsherkenningstechnologie door burgers en bedrijven een inbreuk vormen op de privacy van de burger? Wat zijn de grootste privacyrisico's? En met welke privacyrisico's dient volgens experts de komende vijf jaar rekening te worden gehouden?

Voor vraag 2:

2.1) Kunnen de geïdentificeerde privacyrisico's worden voorkomen of beperkt door bestaande juridische middelen? Zo ja, door welke en hoe? Wat zijn daarbij (mogelijke) juridische lacunes?

[14] Voor verschillende vormen van regulering zie ook: L Lessig, *Code: Version 2.0*. (Basic Books 2006).

2.2) Welke reguleringsstrategieën (juridisch en anderszins) hanteren overheden, bedrijven en burgers in de praktijk om de privacyrisico's voor burgers van het gebruik van gezichtsherkenningstechnologie te beperken?

2.3) Welke van de geïnventariseerde reguleringsstrategieën zijn succesvol, en waarom?

2.4) Lenen –onderdelen van– deze succesvolle reguleringsstrategieën zich ertoe te worden omgebouwd tot algemeen verbindende voorschriften in wetgeving om de geïdentificeerde juridische lacunes af te dekken? Zo ja, hoe? Is hier binnen de huidige wetgeving ruimte voor? Zo nee, lenen deze inzichten zich anderszins voor regulering om de privacyrisico's van het gebruik van gezichtsherkenningstechnologie te beperken?

Wij zullen deze vragen beantwoorden aan de hand van een literatuurstudie, aangevuld met interviews en een expertworkshop, en een juridische analyse. Wij maken hierbij gebruik van vier domeinstudies waarbinnen wij privacyrisico's verder uitdiepen door te kijken naar specifieke toepassingsgebieden van gezichtsherkenning en door diverse betrokkenen te interviewen. Binnen deze domeinstudies hebben wij, in navolging van de onderzoeksopdracht van het WODC, zogeheten *best practices*, zowel binnen als buiten Nederland, bestudeerd om van reeds bestaande praktijken te leren hoe het gebruik van gezichtsherkenning kan worden gereguleerd en de privacy van burgers kan worden gewaarborgd.

Onder *best practices* verstaan wij in dit onderzoek bestaande praktijken (maatregelen, aanpakken, methodes, etc.) waarvan wordt verwacht dat ze bijdragen aan de bescherming van privacy. In het onderzoek zijn wij echter ook minder of niet succesvolle voorbeelden –*worst* practices– tegengekomen. Deze hebben wij ook opgenomen in dit rapport omdat die eveneens iets kunnen leren over de reguleringsmogelijkheden.

Om het onderzoek te structureren, hebben wij zowel bij de literatuurstudie als ook bij de interviews binnen de domeinstudies gebruik gemaakt van de door Solove[15] ontwikkelde taxonomie van privacyschendende activiteiten. In de analyse van de literatuurstudie en domeinstudies, maken wij verder ook gebruik van de privacytypologie ontwikkeld door Koops et al. (2016),[16] om te kunnen specifiëren wat voor soort privacy in het gedrang komt bij deze activiteiten. Wij hebben de inzichten uit de overkoepelende analyse bediscussieerd en verder aangescherpt tijdens de expertworkshop. Op basis van de resultaten van deze analyse is de juridische analyse uitgevoerd en zijn reguleringsopties geformuleerd. Deze reguleringsopties betreffen de mogelijkheden om (potentiële) privacy-inbreuken door het gebruik van gezichtsherkenningstechnologie te voorkomen of te beperken via wetgeving of andere regulering.

[15] Daniel J Solove, 'A Taxonomy of Privacy' (2005) 154 University of Pennsylvania Law Review 477.
[16] Bert-Jaap Koops e.a. 'A Typology of Privacy' (2016) 38 University of Pennsylvania Journal of International Law 483.

Voor meer details omtrent de methodologie onderliggend aan dit rapport, verwijzen wij de lezer naar hoofdstuk 2.

1.2. Opbouw rapport

In het volgende hoofdstuk lichten wij de toegepaste methodes in dit onderzoek verder toe. Vervolgens beginnen wij het onderzoek in hoofdstuk 3 met een nadere omschrijving van gezichtsherkenningstechnologie en brengen wij de huidige en de te verwachten ontwikkelingen verder in kaart. Op basis van deze beschrijvingen geven wij eerst in meer algemene zin een overzicht van de mogelijke privacyrisico's van het gebruik van gezichtsherkenningstechnologie. In hoofdstuk 4 worden deze risico's verder verkend aan de hand van de vier domeinstudies. Hoofdstuk 5 geeft een overkoepelende analyse op basis van hoofdstuk 3 en 4, en beantwoordt daarmee de eerste onderzoeksvraag over hoe Nederlandse burgers en bedrijven gezichtsherkenningstechnologie gebruiken en hoe dit gebruik een inbreuk kan vormen op de privacy van burgers. In hoofdstuk 6 staat vervolgens de rechtsverkenning centraal ter beantwoording van vraag 2.1. Tot slot bevat hoofdstuk 7 de *best practices* en reguleringsopties, waarmee de rest van onderzoeksvraag 2 wordt beantwoord. Hoofdstuk 8 geeft een overzicht van de conclusies.

2. Methodologie

Om de onderzoeksvragen te beantwoorden hebben wij gebruik gemaakt van een combinatie van onderzoeksmethoden, zijnde: literatuurstudie, interviews, een expertworkshop en een juridische analyse. De literatuurstudie naar privacyrisico's is in eerste instantie breed opgezet om een goed idee te verkrijgen van de verschillende risico's. Vervolgens is ervoor gekozen de literatuurstudie, aangevuld met interviews, toe te spitsen op specifieke toepassingen van gezichtsherkenning in zogenaamde domeinstudies (bijvoorbeeld het domein detailhandel of evenementenorganisatie). Zo hebben wij de mogelijke bijkomende privacyrisico's en een aantal best practices verder uitgelicht en ter validatie ook voorgelegd en besproken tijdens een expertworkshop. De analyse van de privacyrisico's hebben wij uitgevoerd met behulp van twee complementaire kaders, geformuleerd door respectievelijk Solove en Koops et al.[17] Wij lichten de invulling en het gebruik van de verschillende onderzoeksmethodes hieronder verder toe.

2.1. Literatuurstudie

Voor de beantwoording van onderzoeksvragen 1, 2.2, 2.3 en 2.4 (voor zover deze betrekking hebben op burgers en bedrijven) hebben wij de ontwikkelingen op het gebied van geautomatiseerde gezichtsherkenning eerst in kaart gebracht aan de hand van een literatuurstudie van academische publicaties, websites, nieuwsartikelen, en rapporten (zie hoofdstuk 3 en 4). Dit hebben wij voor gezichtsherkenning in het algemeen gedaan en voor elke domeinstudie apart. Bij het zoeken naar literatuur hebben wij gebruik gemaakt van internetzoekmachines, de zoekfunctie van de universiteitsdatabase en referentielijsten uit eerdere rapporten en academische literatuur.[18] Bij elke domeinstudie volgt eerst een beschrijving van het type gezichtsherkenning, de huidige en mogelijke toekomstige (technologische) functionaliteiten en (on)mogelijkheden, en de daadwerkelijke en potentiële toepassing van gezichtsherkenning binnen het domein en de betrokken partijen. Ten slotte is gekeken naar de bestaande en potentiële privacyrisico's van gezichtsherkenning.

2.2. Domeinstudies en *best practices*

Om het gebruik van gezichtsherkenning en de privacyrisico's verder in kaart te brengen hebben wij gebruik gemaakt van vier domeinstudies. De inzichten uit de literatuurstudie hebben wij hiervoor aangevuld met semi-gestructureerde interviews met (technische) medewerkers van

[17] Daniel J Solove, 'A Taxonomy of Privacy' (2005) 154 University of Pennsylvania Law Review 477; Bert-Jaap Koops e.a. 'A Typology of Privacy' (2016) 38 University of Pennsylvania Journal of International Law 483.
[18] Een van de rapporten die een startpunt boden was: Annelli Janssen, Linda Kool en Jelte Timmer, *Dicht op de huid: Gezichts- en Emotieherkenning in Nederland* (Rathenau Instituut 2015).

bedrijven die gezichtsherkenning ontwikkelen, verkopen en gebruiken en met inzichten uit de expertworkshop (zie 2.3 en 2.4 voor verdere toelichtingen over de interviews en expertworkshops).

Elke domeinstudie richt zich op een specifieke type toepassing van gezichtsherkenningstechnologie (zie ook volgende hoofdstuk voor verdere beschrijving van diverse toepassingen): organisatie van events (1), smartphone apps (2), slimme deurbel (3), en retail (4). Voor een overzicht van de domeinstudies zie tabel 3.1.

Toepassing	**Functies**	**BEDRIJF**
1. Organisatie van evenementen	Identificatie en emotiedetectie	Zenus RAI Amsterdam 20Face
2. Smartphone apps	Matching, identificatie, categorisering, emotiedetectie	Facebook, Inc. SeeingAI (Microsoft) Microsoft NL (Face API) Amazon (Rekognition) DIY gezichtsherkenning
3. Slimme deurbel	Identificatie	Google (Nest)
4. Retail	Verificatie en categorisering	Chinees retail bedrijf[19]

Tabel 2.1 Overzicht domeinen

In onze keuze voor domeinen en betrokken bedrijven hebben wij ons door een aantal parameters laten leiden. Ten eerste hebben we, gezien de focus van deze verkenning op horizontale relaties tussen burgers en bedrijven ervoor gekozen evenredig aandacht te besteden aan beide relaties. Toepassingen 1 en 4 zijn met name gericht op bedrijf-burger, toepassingen 2 en 3 zijn met name gericht op burger-burger. Binnen deze twee categorieën relaties hebben wij gekozen voor toepassingen waar al producten voor beschikbaar zijn. Organisatie van evenementen en retail behoren beide tot de grootste markten voor gezichtsherkenningsproducten binnen de burger-bedrijf relatie.[20] Het was lastiger om producten of diensten te vinden om de burger-burger relatie te bestuderen, omdat deze nog niet veel worden aangeboden en als ze worden aangeboden er niet veel informatie over beschikbaar is. Wij hebben daarom gekozen voor het domein slimme deurbel, waarvoor in ieder geval optioneel een abonnement voor gezichtsherkenning beschikbaar is, en het domein sociale media apps, waarbij gezichtsherkenning een onderdeel is van de geleverde dienst. In beide domeinen worden producten aangeboden in Nederland.

[19] Op verzoek van de geïnterviewde contactpersoon is ervoor gekozen de desbetreffende naam van het bedrijf waarover deze contactpersoon spreekt, niet op te nemen in het rapport.
[20] 'Facial Recognition Market by Component (Software Tools and Services), Technology, Use Case (Emotion Recognition, Attendance Tracking and Monitoring, Access Control, Law Enforcement), End-User, and Region - Global Forecast to 2022' (Marketsandmarkets 2017).

Ten tweede hebben wij ons als doel gesteld alle technische toepassingen van gezichtsherkenning – identificatie, verificatie, matching, categorisering en emotieclassificering – aan bod te laten komen. Het onderscheid tussen deze toepassingen lichten wij in het volgende hoofdstuk verder toe. Identificatie en emotiedetectie komt aan bod bij toepassing 1, matching, identificatie, categorisering, en emotiedetectie bij toepassing 2, identificatie bij toepassing 3, en bij toepassing 4 verificatie en categorisering.

Ten derde, hebben wij ervoor gekozen om in elk domein meerdere bedrijven te belichten om zo een rijk beeld te krijgen van de mogelijkheden. Hierbij hebben wij ons niet beperkt tot Nederland, maar juist ook internationaal (buiten EU) gekeken om zo toepassingen die nu nog niet in Nederland beschikbaar zijn, mee te kunnen nemen in dit onderzoek. De achterliggende gedachte is dat deze toepassingen ons inzicht bieden in wat er in de toekomst –eventueel ook– mogelijk is in Nederland. De beschrijving van deze bedrijven en hun producten en services zijn gebaseerd op publiek toegankelijke bronnen en secundaire literatuur, zoals nieuwsartikelen en academisch literatuur en interviews.

In de keuze van deze bedrijven hebben wij een evenwichtige spreiding betracht. De reden hiervoor is dat wij een divers palet aan privacyrisico's en reguleringsstrategieën willen schetsen en ervan uitgaan dat het onder loep nemen van verschillende type bedrijven hieraan bijdraagt. Gebaseerd op Koops' classificatie van bedrijven hebben wij daarom een onderscheid gemaakt tussen bedrijven die als kernactiviteit de ontwikkeling en het direct gebruik van gezichtsherkenningstoepassingen hebben (toepassingen 3 en 4) bedrijven die als kernactiviteit de ontwikkeling en verkoop van gezichtsherkenningstoepassing hebben (toepassingen 1 en 2) en bedrijven die gezichtsherkenning gebruiken ter ondersteuning van hun bedrijfsactiviteiten (toepassingen 1, 3 en 4).[21] De verschillende categorieën betreffen zowel grote en middelgrote bedrijven alsook startups.[22] Daarnaast maken wij onderscheid tussen lokale/nationale en internationale bedrijven.

De desbetreffende bedrijven hebben wij geselecteerd door middel van een inventarisatie van gezichtsherkenningsbedrijven in Nederland en het buitenland. Bij deze inventarisatie hebben wij gebruik gemaakt van de literatuurstudie en een sneeuwbalmethode, waarbij wij mensen uit ons netwerk en uit de begeleidingscommissie hebben gevraagd naar informatie over gezichtsherkenningsbedrijven in Nederland en daarbuiten. Bij de selectie hebben wij bedrijven gekozen die al enige ervaring hebben met deze technologie om zo een goed beeld te krijgen van de huidige *state-of-the-art* gezichtsherkenningspraktijk. Uit onze inventarisatie bleek dat er een beperkt aantal bedrijven in Nederland is die zelf gezichtsherkenningstechnologie ontwikkelt en

[21] Bert-Jaap Koops, 'Input voor Discussie Over Horizontale Privacy' (2017) <https://www.tweedekamer.nl/downloads/document?id=10df366f-fc21-46f0-a12f-4ecb1f78e9fc&title=Position%20paper%20UvT%20-%20TILT%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Horizontale%20privacy%20d.d.%2012%20oktober%202017.docx.> geraadpleegd 7 februari 2020.

[22] De keuze hiervoor is ook in lijn met de vragen vanuit de Tweede Kamer.

levert, en dat de marktleiders zich vooral in China en de Verenigde Staten bevinden.[23] Bovendien gebruiken Nederlandse burgers en bedrijven ook de producten en services van buitenlandse bedrijven, zoals bijvoorbeeld van Google en Facebook. Wij hebben daarom in onze keuze voor bedrijven gekeken naar Nederlandse, Chinese en Amerikaanse bedrijven. Bij de selectie van bedrijven speelde ook mee of wij genoeg informatie konden vinden over de producten, contact konden leggen met de bedrijven en of zij open stonden voor interviews.

Ten slotte geven deze domeinstudies inzicht in hoe regulering in de praktijk kan uitwerken, waar er mogelijk lacunes optreden en hoe deze geadresseerd zouden kunnen worden. Omdat het een verkenning betreft, zijn deze inzichten vooral indicatief en signalerend van aard en kunnen wij geen generaliserende uitspraken doen over de onderzochte prakijken en technologieën.

Best practices

Aan de hand van de producten en services die de geselecteerde bedrijven aanbieden, hebben wij de mogelijke risico's onderzocht in de contexten waarin deze producten en services worden gebruikt. Daarnaast hebben wij de manieren in kaart gebracht waarop deze partijen de risico's proberen te minimaliseren en hebben wij *best* (en *worst*) *practices* geïdentificeerd. Onderzoek naar *best practices* kijkt doorgaans naar bestaande praktijken om die te vergelijken en te kijken welke beter in staat zijn om een bepaald doel te bereiken.[24] In deze verkenning kijken wij naar een technologische trend waar producten en services nog volop in ontwikkeling zijn en praktijken nog in wording zijn. Het is daarom lastig om praktijken een-op-een te vergelijken. Wij hanteren daarom een enigszins aangepaste definitie van *best practice* en kijken naar praktijken, inclusief organisatie- en communicatiestrategieën en technologische aanpakken, die bedrijven inzetten om privacyrisico's te beperken. Daartoe hebben wij in de interviews bedrijven expliciet gevraagd wat zij zelf als *best practices* beschouwen. In deze verkennende studie kunnen wij echter niet uitputtend onderzoeken in hoeverre deze praktijken daadwerkelijk succesvol zijn. Wij zullen ons daarom beperken tot het benoemen van de gepercipieerde effectiviteit en signaleren daarmee de mogelijke kansen en risico's van deze praktijken.

2.3. Interviews

[23] Nederlandse bedrijven zijn onder andere: Gemalto (onderdeel van Thales), VicarVision en 20Face. Voor een marktanalyse zie bijvoorbeeld: Unlocking potential, 'Facial Recognition Technology Market Research' <www.unlocking-potential.co.uk/wp-content/uploads/2019/06/Facial-Recognition-Technology-Market-Research.pdf> geraadpleegd 15 januari 2020; 'Facial Recognition Market by Component (Software Tools and Services), Technology, Use Case (Emotion Recognition, Attendance Tracking and Monitoring, Access Control, Law Enforcement), End-User, and Region - Global Forecast to 2022' (Marketsandmarkets 2017). Voor een overzicht van gezichtsherkenningsbedrijven zie bijvoorbeeld: Biometric update, 'Facial Recognition Solutions' (2020) <www.biometricupdate.com/service-directory/facial-recognition> geraadpleegd 15 Januari 2020.

[24] Stuart Bretschneider, Frederick J. Marc-Aurele, and Jiannan Wu. '"Best practices" research: a methodological guide for the perplexed' 15.2 Journal of Public Administration Research and Theory (2004) 307-323.

Zoals gezegd hebben wij de literatuurstudies waar mogelijk aangevuld met semi-gestructureerde interviews met personen die betrokken zijn bij de onderzochte bedrijven in de domeinstudies. Een lijst met geïnterviewde personen is opgenomen in bijlage II. De interviews duurden allemaal ongeveer een uur en waren gericht op vragen rondom de mogelijke privacyrisico's maar ook op eventuele mitigerende maatregelen ten einde te komen tot best practices voor het gebruik van gezichtsherkenning. Wij hebben gebruik gemaakt van een interviewleidraad om de interviews te structureren en ervoor te zorgen dat door ons vooraf geselecteerde relevante onderwerpen aan bod zouden komen (zie interviewleidraad in bijlage I). Deze leidraad diende als geheugensteun en, omdat het semi-gestructureerde interviews betrof, kon de interviewer er ook van afwijken als het gesprek daar om vroeg. De interviews waren ondersteunend van aard en bedoeld om lacunes in de literatuurstudie verder in te vullen. Ons doel was om zowel technisch en juridische medewerkers te interviewen als leidinggevenden met een meer strategische blik op de activiteiten van het bedrijf. Op die manier konden wij meer inzicht krijgen in de technische producten en services van het bedrijf, hoe het bedrijf omgaat met regulering en hoe producten en services in de markt gezet worden.

Bij de selectie van personen waren wij afhankelijk van de welwillendheid van bedrijven om ons te woord te staan. Niet in alle gevallen was het mogelijk een interview te verkrijgen. Het is ons bijvoorbeeld niet gelukt medewerkers van SeeingAI (onderdeel van Microsoft) of Google voor de slimme deurbel te interviewen. Toch hebben wij deze bedrijven meegenomen in de verkenning omdat zij bestaande producten aanbieden die betrekking hebben op de burger-burger relatie en er relatief veel openbare informatie beschikbaar was over deze producten. Ook konden wij als alternatief interviews houden met relevante experts. Zo hebben wij binnen het domein van de slimme deurbel ervoor gekozen een interview met een expert op het gebied van privacy en veiligheid te houden. Binnen het domein van sociale media apps konden wij weliswaar niemand van SeeingAI interviewen, maar wel medewerkers van Facebook en Microsoft Nederland interviewen.

Wij hebben de interviews opgenomen en uitgeschreven. De gebruikte quotes in het rapport zijn voorgelegd aan de desbetreffende geïnterviewde. De uitgeschreven interviews hebben de onderzoekers gebruikt bij de beschrijving van de producten en activiteiten van de bedrijven en de motivaties die bedrijven zelf zeggen te hebben voor de keuzes die zij maken op het gebied van privacybescherming.

2.4. Expertworkshop

Om de inzichten uit de domeinstudies en de beschouwing van de reguleringsmogelijkheden verder aan te vullen, hebben wij een expert workshop georganiseerd. In deze workshop hebben wij met elf experts vanuit verschillende professionele achtergronden de door ons geïnventariseerde privacyrisico's aangescherpt, best practices bediscussieerd, de verschillende

reguleringsmogelijkheden verder in kaart gebracht en gereflecteerd op de haalbaarheid en wenselijkheid van deze mogelijkheden. Bij de selectie van experts hebben wij gezocht naar een spreiding van personen uit de wetenschap, maatschappelijke organisaties en het bedrijfsleven (zie bijlage II voor een overzicht van de experts). Wij hebben de experts geselecteerd met behulp van de eerdergenoemde sneeuwbalmethode: op basis van onze initiële literatuurstudie, eerder onderzoek, en het netwerk van de onderzoekers en de begeleidingscommissie hebben wij mensen benaderd en hen ook gevraagd om suggesties voor experts. De workshop vond plaats in de middag en duurde vier uur inclusief pauze. Vanwege de beperkte duur van de workshop en omdat wij dieper op de materie in wilden gaan hebben wij voor de expertworkshop gebruik gemaakt van drie van de genoemde domeinstudies om de discussie te structureren: toegangscontrole, sociale media apps, en de slimme deurbel. De discussie over de domeinstudies vond plaats rondom drie vragen: welke ontwikkelingen kunnen wij in de nabije toekomst verwachten, wat zijn de kansen en risico's en welke mogelijkheden voor regulering zijn er?

Er is een verslag gemaakt van de workshop, welke ter controle aan de deelnemers is voorgelegd. De onderzoekers van het team hebben het verslag bestudeerd voor de overkoepelende analyse om zo mogelijke lacunes in deze analyse te signaleren.

2.5. Analyse van privacyrisico's

Om op systematische wijze te onderzoeken hoe privacyinbreuken ontstaan hebben wij in de literatuurstudie naar (horizontale) privacyrisico's en in de domeinstudies gebruik gemaakt van de *privacytaxonomie* van Solove.[25] De taxonomie van Solove onderscheidt vier groepen van activiteiten die privacy kunnen schaden: (1) informatieverzameling, (2) informatieverwerking, (3) informatieverspreiding en (4) overschrijding. De taxonomie sluit goed aan bij de onderzoeksvragen omdat deze vertrekt vanuit de burger, technologie-neutraal is en dus toepasbaar op verschillende technologieën. Bovendien is de taxonomie voldoende flexibel zodat, indien het lopend onderzoek dit vraagt, verder toegespitst kan worden.

Bij de analyse van de literatuurstudie en de domeinstudies hebben wij vervolgens ook gebruik gemaakt van de *privacytypologie* ontwikkeld door Koops et al..[26] De auteurs geven een beschrijving van de verschillende *privacytypen* die helpen om een nadere invulling te geven aan het soort schade dat de door Solove onderscheiden activiteiten kunnen veroorzaken. In de typologie van Koops et al. zijn *privacytypen* gegroepeerd langs een spectrum van interactie met de omgeving, lopend van een strikt persoonlijke sfeer tot aan de publieke sfeer, en langs een spectrum van negatieve en positieve vrijheid.

[25] Daniel J Solove, 'A Taxonomy of Privacy' (2005) 154 University of Pennsylvania Law Review 477.
[26] Bert Jaap Koops e.a. 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

De taxonomie van Solove is het vertrekpunt voor de structurering van de literatuurstudie en domeinstudies omdat deze focust op de dataverwerkingsactiviteiten die privacy-breuken kunnen veroorzaken. Vervolgens verheldert de typologie van Koops waar nodig welke type privacy hierdoor onder druk komt te staan. De taxonomie van Solove en de typologie van Koops lichten wij in de volgende subparagrafen verder toe.

2.5.1. **De privacy taxonomie van Solove**

Solove's taxonomie onderscheidt 4 groepen van activiteiten die privacy kunnen schaden (met elk nog verder uitgewerkte subcategorieën die wij enkel zullen benoemen wanneer relevant, zie Tabel 2.2): informatieverzameling (1), informatieverwerking (2), informatieverspreiding (3), en overschrijding (invasion) (4).

Informatieverzameling	**informatieverwerking**	**informatieverspreiding**	**overschrijding**
surveillance	aggregatie	vertrouwensbreuk	intrusie
ondervraging	identificatie	onthulling	inmenging in besluitvorming
	onveiligheid	blootstelling	
	secundair gebruik	toenemende toegankelijkheid	
	uitsluiting	afpersing	
		toe-eigenen	
		verstoring	

Tabel 2.2 Overzicht taxonomie van activiteiten die privacy kunnen schaden. Gebaseerd op Solove, Daniel J. (2008), Understanding Privacy. *Harvard: Harvard University Press.*

Informatieverzameling

De eerste activiteit die mogelijk een privacyrisico oplevert betreft het verzamelen van informatie. Bij deze categorie houden wij dus nog geen rekening met het doel waarvoor de gezichtsherkenningsapplicatie gebruikt wordt, welke weer andere privacy-inbreuken kan veroorzaken. Solove benoemt twee vormen van informatieverzameling die privacyrisico's inhouden: surveillance en ondervraging. Surveillance verwijst naar het monitoren van personen (al dan niet heimelijk), terwijl ondervragen gaat over het onder druk zetten van mensen om informatie te delen.

Informatieverwerking

Onder informatieverwerking verstaat Solove het gebruik, opslaan, en manipulatie van verzamelde data. Het gaat hier dus met name over hoe de eerder verzamelde data op verschillende manieren wordt gebruikt. Solove onderscheidt vijf subcategorieën van verwerking. De eerste is *aggregatie*, waarmee verwezen wordt naar het samenbrengen van verschillende stukjes informatie over één persoon. Juist in dit combineren van verschillende informatiebronnen ligt het privacy risico omdat er een totaalplaatje kan ontstaan van een burger dat vele malen onthullender is dan wat de informatiebronnen los van elkaar laten zien.[27] Omdat burgers bepaalde verwachtingen hebben met betrekking tot wat derden over hen weten, kan aggregatie die privacyverwachtingen schenden aangezien de combinatie van bronnen nieuwe kennis kan opleveren die burgers niet voorzien hadden.

De tweede is *identificatie*, welke overeenkomsten heeft met aggregatie omdat het ook hier gaat om het bijeenbrengen van verschillende informatiebronnen waarvan één van die bronnen de identiteit van een persoon is. Identificatie verschilt van aggregatie doordat het een link legt met een persoon van vlees en bloed. Identificatie kan verschillende privacyproblemen veroorzaken. Zo kan identificatie een hindernis vormen voor burgers' vermogen zich te ontwikkelen en te veranderen omdat ze vastgepind worden op een bepaald profiel.[28] Identificatie kan het moeilijker maken voor burgers om anoniem of pseudo-anoniem in het sociale verkeer te begeven en het kan –net zoals bij informatieverzameling- leiden tot een machtsdisbalans waarbij degene die in staat is de ander te identificeren dit kan gebruiken om die ander vervolgens ook te controleren.

De derde subcategorie wordt aangeduid onder de noemer *onveiligheid* en behelst een variëteit aan issues: identiteitsdiefstal, beveiliging, misbruik, verspreiden van valse informatie, etc.[29] Het ondoordacht gebruik van informatie door bedrijven maar zeker ook door burgers zelfs, maakt burgers kwetsbaar voor toekomstige schade. Dit kan gaan om het oneigenlijk openbaar maken van informatie, maar ook om het verspreiden van verkeerde informatie wat onder andere kan leiden tot reputatieschade.

De vierde subcategorie betreft *secundair gebruik* van informatie. Met secundair gebruik verwijst Solove naar het inzetten van informatie voor een doel dat niet is gerelateerd aan het initiële doel waarvoor het was verzameld.[30] Vaak wordt hierbij ook verwezen naar *data creep* of *function creep*. Wanneer dit optreedt bestaat er het risico dat privacyverwachtingen van burgers worden geschonden. De mogelijkheid tot secundair gebruik kan leiden tot angst en onzekerheid bij burgers over hoe hun data in de toekomst gebruikt zal worden. Dit brengt dan een gevoel van machteloosheid en kwetsbaarheid met zich mee.[31]

De vijfde en laatste subcategorie is *uitsluiting*. Hiermee verwijst Solove naar de schade die berokkend kan worden wanneer een burger wordt uitgesloten van het gebruik van data die hem

[27] Daniel J Solove, *Understanding privacy* (Harvard University Press 2008) 118.
[28] Ibid. p.124.
[29] Ibid. p.127.
[30] Ibid. p.131.
[31] Ibid. p.132.

of haar betreft, door niet geïnformeerd te zijn over het gebruik van de data, en door niet in de positie te zijn om het gebruik van die data op enigerwijze bij te sturen.[32]

Informatieverspreiding

Een derde omvangrijke categorie van privacy-inbreuken valt onder de noemer van gegevensverspreiding.[33] Gegevensverspreiding betreft privacy-inbreuken die te maken hebben met het openbaar maken van persoonsgegevens of de dreiging daartoe. Verschillende typen van gegevensverspreiding kunnen worden onderscheiden en Solove benoemt er 7: vertrouwensbreuk, onthulling, blootstelling, toenemende toegankelijkheid, afpersing, toe-eigenen en verstoring.

Zowel bij het *onthullen* van persoonlijke informatie als bij een *vertrouwensbreuk* gaat het erom dat persoonlijke informatie wordt gedeeld die de persoon in kwestie schaadt. In de eerste instantie is er met name sprake van reputatieschade voor de persoon door de verspreiding van accurate informatie, in de tweede ligt de nadruk niet zozeer op de gegevensverspreiding zelf maar op de schade die wordt berokkend door het geschonden vertrouwen in de partij die de gegevens heeft verspreid.[34] Dit geschonden vertrouwen speelt met name een rol in specifieke, geprivilegieerde relaties zoals die bestaan tussen een patiënt en dokter of een cliënt en advocaat. In die relaties vertrouwen wij erop dat onze belangen worden behartigd en persoonsgegevens die daarbij worden gedeeld ook alleen voor datzelfde belang worden ingezet.

Bij *blootstelling* gaat het om het verspreiden van een specifiek type van primordiale informatie, zoals emotionele en fysieke informatie die betrekking heeft op bijvoorbeeld rouw, pijn, naaktheid, seks, of uitwerpselen.[35] Dit soort informatie heeft niet noodzakelijk een negatief effect op iemands reputatie maar kan wel schaamte teweegbrengen en de menselijke waardigheid aantasten.[36]

Bij een *toenemende toegankelijkheid* gaat het niet zozeer om het actief verspreiden van informatie, maar door middel van technologische innovatie de toegang tot informatie te vergroten. Dit kan ertoe leiden dat de eerdergenoemde privacyproblemen –reputatieschade, vertrouwensbreuk, blootstelling– in omvang toenemen.[37]

Afpersing houdt in dat er gedreigd wordt met het onthullen van persoonlijke, geheime informatie van een individu die, om dit te voorkomen, vaak geld moet betalen. Afpersing maakt dat een individu kan worden gedomineerd en gecontroleerd door een derde partij.[38]

Toe-eigening is het gebruik van iemand anders' identiteit of persoonlijkheid uit eigenbelang.[39] Niet alleen kan dit de waardigheid van mensen aantasten, het kan ook een

[32] Ibid. p.134.
[33] Ibid. p.136.
[34] Ibid. p.138.
[35] Ibid. p.147.
[36] Ibid. p.148.
[37] Ibid. p.150.
[38] Ibid. p.152-153.
[39] Ibid. p.155.

negatieve impact hebben op iemands vrijheid en persoonlijke ontwikkeling.[40] Wanneer iemands afbeelding gebruikt wordt zonder toestemming kan dit zijn of haar vrijheid om het eigen levensverhaal te vertellen beknotten.[41]

Verstoring verwijst naar het manipuleren van de wijze waarop een individu gezien en beoordeeld wordt door anderen.[42] Laster, roddels en eerroof zijn daar voorbeelden van. Net zoals bij het onthullen van informatie heeft verstoring een mogelijk negatieve impact op iemands reputatie en kan het leiden tot stigma's en schaamte. Verstoring verschilt echter van onthulling doordat het hier gaat om het verspreiden van valse informatie.[43]

Overschrijding

De laatste categorie van privacyrisico's valt onder de noemer van overschrijding en kent twee types: intrusie en inmenging in besluitvorming. De categorie overschrijding verschilt van de vorige omdat er niet altijd data mee gemoeid is.[44]

Intrusie slaat op activiteiten die de dagelijkste activiteiten van een persoon verstoren. Data-gerelateerde voorbeelden hiervan zijn: spam, junk mail en telemarketing.[45] Dit soort inbreuk schendt de persoonlijke sfeer die mensen nodig hebben om zich terug te kunnen trekken, weg van het sociale verkeer. Intrusie kan overigens ook plaatsvinden in de publieke sfeer, bijvoorbeeld wanneer mensen geen gepaste afstand houden of zich mengen in een gesprek tussen bekenden.

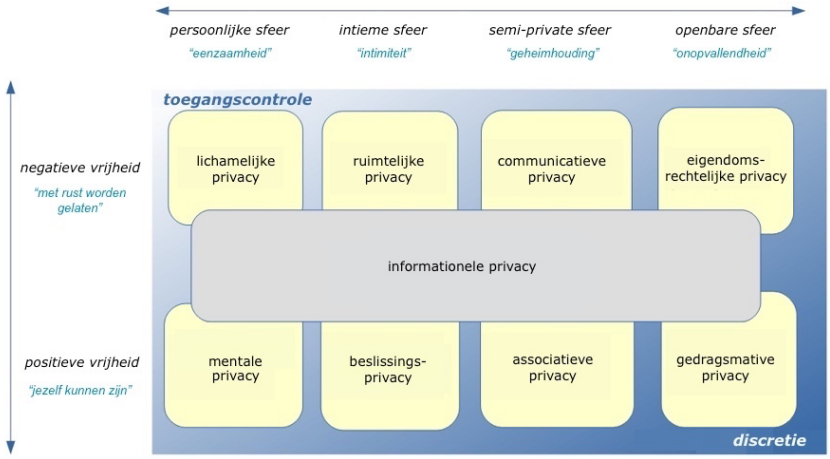
Inmenging in besluitvorming gaat om de onwenselijke bemoeienis van derden in de beslissingen die iemand neemt over belangrijke zaken in zijn of haar leven.[46] Waar dit in eerste instantie met name betrekking had op onwenselijke overheidsinmenging, kan het in toenemende mate ook slaan op bedrijven, aangezien die in de data-gedreven samenleving een steeds grotere invloed hebben op fundamentele aspecten van ons leven (gezondheid, werk, veiligheid).[47]

We gebruiken deze vier categorieën om de privacyrisico's beschreven in de literatuur en in de domeinstudies systematisch in kaart te brengen. Het kan echter best zo zijn dat in het feitelijk gebruik van gezichtsherkenning alle vier voorkomen en overlappen. Vanwege het verkennend karakter van dit onderzoek is het voornaamste doel om inzicht te geven in de verschillende soorten mogelijke risico's en niet om een allesomvattende inventarisatie te geven. Zoals gezegd, geeft Solove een raamwerk om de activiteiten die bij gezichtsherkenning tot privacy-inbreuken kunnen leiden geordend in beeld te brengen, maar daarmee zegt het nog niet iets over wat voor soort privacy wordt geraakt. Om dit verder te kunnen duiden gebruiken wij in de analyse waar nodig Koops et al.'s typologie.

[40] Ibid. p.156.
[41] Ibid. p.158.
[42] Ibid. p.160.
[43] Ibid.
[44] Ibid. p.162.
[45] Ibid. p.163.
[46] Ibid. p.167.
[47] Ibid. p.168.

2.5.2. **De privacy typologie van Koops et al.'s**

Koops et al. hebben op basis van een uitgebreide studie van academische literatuur op het gebied van privacy (met name op het gebied ven rechtswetenschap, filosofie en sociologie) een typologie van de verschillende privacytypen ontwikkeld (zie figuur 2.1).



Figuur 2.1 Typologie van privacytypen. Gebaseerd op Bert-Jaap Koops et al (2017). 'A Typology of Privacy', University of Pennsylvania Journal of International Law. 38,2, p.483-575.

In deze typologie zijn privacytypen gegroepeerd langs een horizontale as van interactie met de omgeving, lopend van een strikt persoonlijke sfeer tot aan de publieke sfeer, en langs een verticale as van negatieve (met rust worden gelaten) en positieve (jezelf kunnen zijn) vrijheid. Het is goed om op te merken dat de eerdergenoemde publieke en persoonlijke sfeer op de horizontale as niet louter naar een specifieke ruimte verwijzen –bijvoorbeeld 'in het openbaar vervoer' of 'binnenshuis'– maar eerder naar het karakter van een bepaalde sociale interactie (als daarvan sprake is). De *persoonlijke sfeer* wordt gekenmerkt door alleen zijn, gewenst (je terugtrekken) of ongewenst (eenzaamheid of isolatie). De *intieme sfeer* wordt gekenmerkt door sociale interactie, hoewel beperkt tot intieme partners, familieleden en goede vrienden, evenals activiteiten die plaatsvinden in besloten ruimtes, zoals het huis waar mensen hun leven delen met intieme partners en familie. De *semi-private sfeer* omvat sociale interactie met een breder scala aan actoren, waaronder kennissen, collega's en professionele relaties (bijvoorbeeld interactie met een arts of een verkoper), en activiteiten die plaatsvinden in meer quasi-openbare ruimte. De *openbare sfeer* wordt gekenmerkt door activiteiten die in het openbaar plaatsvinden - bijvoorbeeld op een openbaar plein, in het openbaar vervoer of op openbaar toegankelijke online platformen - waarbij het privacybelang wordt gekenmerkt door de wens onopvallend te zijn ondanks fysieke of virtuele zichtbaarheid in de openbare ruimte.

In het model van Koops et al. is er voor dit onderzoek ook nog een derde belangrijke as te onderscheiden, namelijk een diagonale as die loopt van zelfcontrole over de toegang tot de privésfeer (linksboven) waar een persoon bij machte is om haar privacy zelf te bewaken – bijvoorbeeld door een bivakmuts op te zetten om de (visuele) toegang van anderen tot het gezicht te beperken – tot rechtsonder waarbij de burger in sterke mate afhankelijk is van anderen om haar privacy te beschermen –bijvoorbeeld door erop te vertrouwen dat mensen in de tram haar niet zomaar zullen fotograferen–. Wat deze as inzichtelijk maakt is dat voor privacybescherming zowel juridische als sociale normen een belangrijke rol vervullen.[48]

Uiteindelijk worden in de typologie van Koops et al. acht ideaaltypische privacytypen onderscheiden, waarbij informationele privacy als een negende variant over de andere privacytypen heen komt te liggen. Deze variant valt dus niet volledig samen met de acht varianten, maar maakt eerder onderdeel uit van alle acht. De verschillende varianten zijn dan de volgende:

1. *Lichamelijke privacy*: deze vorm wordt gekenmerkt door de interesse van individuen in de privacy van hun lichaam, waar de nadruk ligt op negatieve vrijheid – bijvoorbeeld door af te dwingen dat anderen niet zomaar hun lichaam aan mogen raken.
2. *Ruimtelijke privacy* wordt gekenmerkt door het al dan niet toegang verlenen tot of controle geven over een private ruimte, de plaatsen waar mensen hun privéleven leiden. Voordehand liggende ruimtes zijn bijvoorbeeld de slaapkamer of de woonkamer, maar ook andere plaatsen zoals hotelkamers of werkplekken kunnen tot op een bepaalde hoogte als een private ruimte gezien worden.
3. *Communicatieve privacy* wordt gekenmerkt door het belang van een persoon bij het controleren van de toegang tot communicatie of het gebruik van informatie welke reeds aan derden is gecommuniceerd.
4. *Eigendomsrechtelijke privacy* wordt gekenmerkt door het belang van een persoon om eigendom te gebruiken als een middel om een activiteit, feiten, dingen of informatie af te schermen van anderen. Een persoon kan bijvoorbeeld een portemonnee gebruiken om items of informatie te verbergen die hij liever privé houdt terwijl hij zich in openbare ruimtes verplaatst.
5. *Mentale privacy* wordt gekenmerkt door iemands behoefte vrij te zijn van de inmenging van anderen bij het reflecteren en de ontwikkeling van meningen en overtuigingen.
6. *Beslissingsprivacy* wordt gekenmerkt door intieme beslissingen over seksuele of voortplantings-gerelateerde onderwerpen, maar ook inclusief andere besluitvorming over gevoelige onderwerpen in de context van intieme relaties.
7. *Associatieve privacy* wordt gekenmerkt door het belang van individuen om vrij te zijn met wie ze willen communiceren: vrienden, verenigingen, groepen en gemeenschappen. Dit past in de semi-privézone, omdat de relaties vaak plaatsvinden buiten strikt privé-plaatsen

[48] Bert Jaap Koops e.a. 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

of intieme omgevingen, in semi-openbare ruimtes zoals kantoren, vergaderruimtes of cafés.

8. *Gedragsmatige privacy* wordt gekenmerkt door de privacybelangen die een persoon heeft tijdens het uitvoeren van openlijk zichtbare activiteiten. In tegenstelling tot items die mensen in het openbaar bij zich dragen (die kunnen worden verborgen en daarom tot op zekere hoogte worden uitgesloten van het zicht van anderen), is iemands persoonlijk gedrag in openbare ruimtes moeilijker te verbergen. 'Zichzelf zijn' in het openbaar kan dan alleen worden bereikt als anderen privacy respecteren door burgerlijke onoplettendheid of men kan proberen controle uit te oefenen door te proberen zich onopvallend te gedragen in de openbare ruimte.
9. *Informationele privacy* wordt geconceptualiseerd als een overkoepelend aspect van elk onderliggend ideaaltype. Elk ideaaltype privacy bevat immers een element van informatie. Zo gaat lichamelijke privacy niet alleen over het beperken van fysieke toegang tot het lichaam, maar ook tot het beperken en beheersen van informatie over het lichaam (bijv. gezondheid of genetische informatie).[49]

We zullen in hoofdstukken 3 en 4 waarin wij de privacyrisico's in kaart brengen Solove's vier categorieën, zoals gezegd, als analytisch instrument gebruiken om het onderzoek naar privacy-inbreuken te structureren. De privacytypen van Koops et al. zullen waar nodig ingezet worden om de mogelijke veroorzaakte privacyschade verder te duiden.

2.6. Juridische Analyse

Om de tweede onderzoeksvraag te beantwoorden hebben wij een juridische analyse uitgevoerd, voortbouwend op de inzichten uit de literatuurstudie en domeinstudies. Deze verkenning richt zich op de rechtsgebieden privacy- en gegevensbescherming, privaatrecht en strafrecht. Onze keuze voor de drie genoemde gebieden is ingegeven door het feit dat deze een generieke privacybescherming bieden, ten opzichte van gebieden die specifieke vormen van rechtsbescherming bieden in bepaalde sectoren (bijvoorbeeld telecommunicatie) of machtsverhoudingen (bijvoorbeeld arbeidsrecht). Meer rechtsgebieden kunnen van toepassing zijn, maar in deze rechtsverkenning kunnen wij niet alle mogelijke rechtsgebieden behandelen.

De relevantie van het privacy- en gegevensbeschermingsrecht voor dit onderzoek is evident; de onderzoeksvraag heeft immers betrekking op privacy. In het privacyrecht speelt daarbij het gegevensbeschermingsrecht een dominante rol,[50] zodat dit de meeste aandacht krijgt in dit rapport. Daarnaast biedt het strafrecht een belangrijke vorm van rechtsbescherming, omdat dit

[49] ibid. p.569.
[50] Bert Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250, 256-259.

zich richt op de ernstigste vormen van privacyschendingen: inbreuken die zo ingrijpend zijn dat een strafrechtelijke sanctie op zijn plaats is. Het strafrecht biedt aldus een minimumniveau aan privacybescherming, dat verder wordt aangevuld door bescherming in andere rechtsgebieden. Het privaatrecht heeft daarbij een belangrijke vangnetfunctie door via het onrechtmatigedaadrecht ook bescherming te bieden tegen privacy-inbreuken die niet worden afgedekt door het privacy-, gegevensbeschermings- of strafrecht.

De belangrijkste onderzoeksmethode voor dit deel van het onderzoek is doctrinair juridisch onderzoek. Bij deze methode van juridisch onderzoek worden relevante wetgeving, jurisprudentie en literatuur geïdentificeerd, geanalyseerd en gesynthetiseerd.[51] Naast een analyse van de relevante wet- en regelgeving is jurisprudentieonderzoek uitgevoerd. Ter nadere duiding van concepten uit wet- en regelgeving maar ook om een beeld te krijgen of er reeds juridische vraagstukken rondom gezichtsherkenning zijn voorgelegd bij de Nederlandse rechter. Aan de hand van dit onderzoek is in kaart gebracht welke mogelijkheden en beperkingen er uit de verschillende rechtsgebieden volgen met betrekking tot de implementatie van gezichtsherkenningstechnologie. Tevens is er gekeken of er richtlijnen en randvoorwaarden te destilleren zijn voor een rechtmatige en risico-averse implementatie van gezichtsherkenning.

De hierboven beschreven combinatie van onderzoeksmethoden stelt ons instaat om: (1) een overzicht te verkrijgen van de huidige stand van zaken en toekomstige ontwikkelingen op het gebied van automatische gezichtsherkenning; (2) de toereikendheid en lacunes van bestaande reguleringsinstrumenten voor het voorkomen en beperken van privacyrisico's van de technologie te analyseren; (3) reguleringsopties te formuleren en handvatten te bieden voor het op systematische en transparante wijze maken van deze reguleringskeuze.

[51] Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2015) 3 Erasmus Law Review 130.

3. Gezichtsherkenning en privacy

Al sinds de jaren zeventig wordt er geëxperimenteerd met automatische gezichtsherkenning, maar pas in het laatste decennium hebben technologische ontwikkelingen een grote vlucht genomen.[52] Als gevolg van deze ontwikkelingen zijn er tegenwoordig steeds meer gezichtsherkennings-producten en systemen beschikbaar voor burgers en bedrijven. Maar met de toenemende aanwezigheid van deze technologieën in het dagelijks leven worden de risico's ook steeds duidelijker. In dit hoofdstuk maken wij een begin met het in kaart brengen van deze risico's.

Dit hoofdstuk en hoofdstuk 4 bevatten de bouwstenen voor het beantwoorden van de eerste onderzoeksvraag: *Hoe wordt gezichtsherkenningstechnologie door Nederlandse burgers en bedrijven gebruikt en hoe kan het gebruik van gezichtsherkenningstechnologieën door burgers en bedrijven een inbreuk vormen op de privacy van de burger (nu en over vijf jaar)*? Het huidige hoofdstuk geeft een meer algemene beschrijving van de huidige en te verwachte toepassingen en doelen van gezichtsherkenningstechnologie voor zover die betrekking hebben op de burger-burger en de burger-bedrijf relatie en de mogelijke privacyrisico's die deze met zich brengen (sub-vraag 1.1). Omdat privacyrisico's niet los gezien kunnen worden van de context waarin ze plaatsvinden, zullen wij vervolgens in hoofdstuk 4 dieper ingaan op een aantal specifieke toepassingen aan de hand van vier domeinstudies (zie hoofdstuk 2 voor verdere toelichting van de domeinstudies). In hoofdstuk 5 zal ten slotte de eerste onderzoeksvraag vervolgens worden beantwoord.

3.1. Gezichtsherkenning: technologische ontwikkelingen

In deze paragraaf zullen wij eerst verder beschrijven wat er nodig is om automatisch een gezicht te herkennen in digitaal beeld en hoe de verschillende technieken zich hebben ontwikkeld in de laatst decennia. Daarna bespreken wij enkele beperkingen van de techniek en verwachte ontwikkelingen zoals zij uit de literatuurstudie naar voren komen. Tot slot staan wij stil bij de verschillende soorten toepassingen van de technologie.

3.1.1. **Technieken voor gezichtsherkenning**

Om een gezicht automatisch te herkennen moet er een aantal stappen worden doorlopen: detectie, uitlijnen, afleiden van kenmerken en de uiteindelijke herkenning.[53] Detectie houdt in dat de locatie en de omvang van het gezicht moeten worden gevonden. Meer specifiek: detectietechnieken gaan op zoek naar de pixels die onderdeel zijn van een gezicht in een afbeelding en maken daar vervolgens een uitsnede van. Dit kan een lastige opgave zijn als de

[52] T Kanade, *Picture processing system by computer complex and recognition of human faces.* PhD thesis (Kyoto University, 1973)
[53] AK Jain en SZ Li, *Handbook of Face Recognition* (Springer 2011).

achtergrond niet duidelijk contrasteert met het gezicht. Vervolgens zal het systeem het gezicht uitlijnen en aanpassen om het vergelijkbaar te maken met andere gezichten of delen van gezichten. Dit kan bijvoorbeeld betekenen dat de uitsnede groter of kleiner gemaakt moet worden of de belichting aangepast. Hierna kunnen de kenmerken van het gezicht worden afgeleid op basis waarvan de uiteindelijke herkenning kan plaatsvinden. Een kenmerk kan bijvoorbeeld het gebied rondom de mondhoeken zijn of een door een algoritme afgeleid kenmerk. Herkenning kan dan door een uitsnede van een gezicht, of beter gezegd een afgeleide representatie daarvan, te vergelijken met één of meerdere gezichten.

Er zijn verschillende technieken die automatische herkenning van (kenmerken van) gezichten mogelijk maken op basis van twee dimensionale stilstaand of bewegend beeld (soms ook op driedimensionaal of thermisch beeld).[54] De meer traditionele technieken maken ofwel gebruik van kenmerkende delen van gezichten om beelden te vergelijken, of ze maken gebruik van geabstraheerde representaties van het gehele gezicht. Kenmerkende delen van of punten op gezichten worden bij deze technieken vooraf met de hand geselecteerd op een reeks afbeeldingen van gezichten, om zo een *model* te trainen wat dan gebruikt kan worden voor automatische herkenning. Een voorbeeld van zo een meer traditionele techniek is de *Active Appearance Model* (AAM) techniek.[55] Deze techniek maakt aan de hand van een reeks voorbeeldgezichten een model van de diverse texturen, vormen en afstanden tussen specifieke, vooraf met de hand geselecteerde punten in het gezicht. Elk gezicht kan op basis van dit model worden gekenmerkt door specifieke texturen en vormen, en worden vergeleken met andere gezichten. Een AAM werkt dan als een soort masker dat over een afbeelding van het gezicht wordt geplaatst om gezichten te matchen en zo een persoon te herkennen.

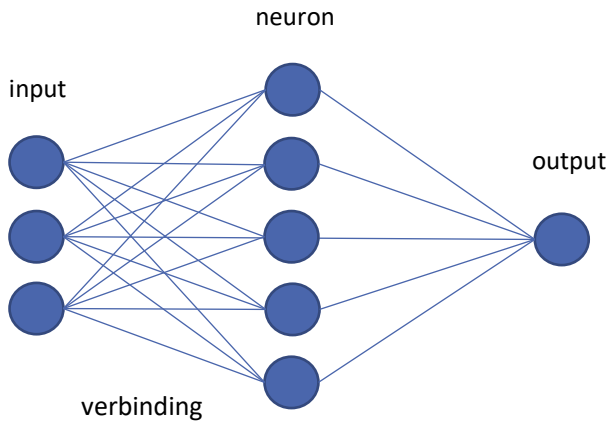
Sinds 2014 zijn er grote vooruitgangen geboekt op het gebied van gezichtsherkenning door de ontwikkeling van zogeheten *deep learning* algoritmen.[56] Dit zijn zogeheten artificiële neurale netwerken: algoritmen die op een sterk versimpelde manier netwerken van neuronen nabootsen. Door de individuele verbindingen tussen lagen van neuronen stap voor stap sterker of zwakker te maken aan de hand van een mathematische formule, kan het systeem patronen in een reeks voorbeelden leren herkennen (zie figuur 3.1 voor een schematisch weergave van een simpel artificieel neuraal netwerk). Het netwerk creëert dan zelf een model van de patronen in de aangeboden voorbeelden die als input worden gegeven. De input laag kan één of meer neuronen

[54] M Wang en W Deng, Deep Face Recognition: A Survey (2018) arXiv:1804.06655; L Fang e.a., 'Overview of Face Recognition Methods' In S Sun (ed), *Signal And Information Processing, Networking And Computers* (Springer 2018) 22-31; M Kristo en M Ivasic-Kos, 'An Overview of Thermal Face Recognition Methods' (2018) 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 174. Wij richten ons in dit verkennend onderzoek uitsluitend op 2D beelden verkregen met gewone camera's, omdat gezichtsherkenning op basis van 3D of thermisch beeld gespecialiseerde apparatuur nodig heeft en daardoor veel minder wordt toegepast in de burger-burger relatie of de burger-bedrijf relatie.

[55] AK Jain en SZ Li, *Handbook of Face Recognition* (Springer 2011).

[56] Sinds het verschijnen van Y Taigman e.a., 'Deepface: Closing the Gap to Human-Level Performance in Face Verification' (2014) Conference on Computer Vision and Pattern Recognition. Deep-learning werd al eerder met succes in andere domeinen gebruikt zie bijvoorbeeld I Goodfellow, Y Bengio en A Courville, *Deep Learning* (MIT Press 2017).

hebben. Dit model kan dan worden gebruikt om patronen te herkennen in nieuwe voorbeelden. De output is dan bijvoorbeeld een 1 of een 0 (wel of niet iets) of numerieke waarde(s) waarvan de hoogte bijvoorbeeld aangeeft of iets bij een bepaalde categorie hoort. De output laag kan dus ook één of meer neuronen bevatten. *Deep learning* algoritmen voor gezichtsherkenning zijn neurale netwerken die bestaan uit meerdere lagen en daardoor een fijnmaziger model kunnen maken.



Figuur 3.1: Schematisch weergave van simpel artificieel neuraal netwerk met drie input neuronen en een output neuron.

Op basis van een grote hoeveelheid voorbeelden van gezichten kunnen deze netwerken zelf patronen afleiden om gezichten te kunnen onderscheiden of te classificeren. Er zijn hiervoor geen met de hand geselecteerde punten nodig. Deze netwerken nemen als invoer een uitsnede van een gezicht – een rechthoekig deel van het beeld dat het gezicht bevat – en kunnen verschillende soorten uitvoer hebben, zoals een classificatie van een gezicht of een geabstraheerde representatie van een gezicht. De geabstraheerde representatie heet wel een *template* of kenmerkvector (*feature vector*). In het geval van classificatie geeft het algoritme een matchscore tussen een gegeven gezicht en eerder opgeslagen gezichten. Een algoritme dat een template als uitvoer geeft kan deze bijvoorbeeld vergelijken met andere, eerder opgeslagen, templates om zo een mate van gelijkenis tussen gezichten of kenmerken van gezichten te kunnen bepalen. Het is dus niet altijd nodig om de originele beelden van gezichten op te slaan om gezichten te herkennen; een template kan voldoende zijn.

Om de algoritmen te trainen maar ook om te testen zijn dus veel beelden van gezichten nodig. Er zijn verschillende databases beschikbaar voor het trainen van modellen. Zowel wetenschappelijke onderzoekers als diverse bedrijven hebben dergelijke databases ontwikkeld. Deze bevatten vaak meerdere foto's van een enkel persoon om zo de algoritmen te trainen op verschillen in poses en variaties en onder verschillende belichting. Hoe meer poses en variatie in belichting, hoe nauwkeuriger het algoritme de vergelijking kan maken. Grote partijen, zoals Google

en Facebook, hebben hun eigen zeer grote databases. Voor wetenschappelijke studies gebruiken onderzoekers vaak vrij beschikbare databases zoals 'Labeled faces in the Wild' en 'MegaFace'.[57]

Inmiddels zijn verschillende gezichtsherkenningssystemen zo goed dat ze beter in staat zijn dan mensen om gezichten te herkennen in de vrij beschikbare databases. Sommige algoritmen halen zelfs een score van 99,9% nauwkeurigheid op deze databases.[58] *Deep learning* algoritmen blijken ook beter dan oudere technieken om te kunnen gaan met variatie in gezichten door bijvoorbeeld belichting en schaduw, de draaiing van het hoofd of gedeeltelijke bedekking van het gezicht. Vanwege deze voordelen zijn ze tegenwoordig de standaard geworden voor automatische gezichtsherkenning.

3.1.2. **Beperkingen van gezichtsherkenning en verdere ontwikkelingen**

Hoewel er grote vooruitgangen geboekt zijn, heeft de technologie nog altijd diverse beperkingen. Zo werkt de gezichtsdetectie die nodig is voor de verdere analyse nog niet onder alle omstandigheden.[59] Zolang de persoon die moet worden herkend meewerkt en dus goed zichtbaar in beeld verschijnt, zijn zeer goede resultaten behaald. De meeste algoritmen hebben echter nog problemen met het analyseren van gezichten onder niet-gecontroleerde omstandigheden. De stand van het gezicht, de mate van occlusie van het gezicht, de belichting, de leeftijd van de persoon, en de kwaliteit van het digitale beeld kunnen de uitkomsten van het algoritme sterk negatief beïnvloeden.[60] Ook het onderscheiden van tweelingen of het herkennen van personen na een operatie is nog altijd lastig. Sommige problemen zijn ook structureel van aard. Als iemand zijn gezicht verandert, door middel van bijvoorbeeld make-up, dan zal dat ook voor automatische herkenningssystemen moeilijk blijven.

Daarnaast blijken gezichtsherkenningssystemen over het algemeen last te hebben van bias, bijvoorbeeld in termen van huidskleur of etniciteit.[61] Een aantal van de meest bekende

---

[57] GB Huang e.a. 'Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments' (2008) Technical report <www.researchgate.net/publication/29622837_Labeled_Faces_in_the_Wild_A_Database_forStudying_Face_Recognition_in_Unconstrained_Environments> geraadpleegd 7 februari 2020; I Kemelmacher-Shlizerman e.a., 'The Megaface Benchmark: 1 Million Faces for Recognition at Scale' (2016) Conference on Computer Vision and Pattern Recognition 4873.

[58] M Wang en W Deng, 'Deep Face Recognition: A Survey' (2018) Cornell University arXiv:1804.06655; Iacopo Masi, Yue Wu, Tal Hassner and Prem Natarajan 'Deep face recognition: A survey' (2018) 31st SIBGRAPI conference on graphics, patterns and images (SIBGRAPI) 471-478.

[59] A Kumar, A Kaur en M Kumar, 'Face Detection Techniques: A Review' (2018) 52 Artificial Intelligence Review 927.

[60] E Learned-Miller e.a., 'Labeled Faces in the Wild: A Survey' in Michal Kawulok, M Emre Celebi, Bogdan Smolka (eds), *Advances in Face Detection and Facial Image Analysis* (Springer 2016);
Mostafa Mehdipour Ghazi and Hazim Kemal Ekenel 'A Comprehensive Analysis of Deep Learning Based Representation for Face Recognition' (2016) arXiv:1606.02894 34; Aisha Azeem e.a., 'A Survey: Face Recognition Techniques under Partial Occlusion' (2014) 11 The International Arab Journal of Information Technology 1; Joy Buolamwini en Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.

[61] M Wang en W Deng, Deep Face Recognition: A Survey (2018) arXiv:1804.06655; Joy Buolamwini en Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 Proceedings of Machine Learning Research 77.

gezichtsherkenningssystemen is beter in staat om bijvoorbeeld mannen met een lichte huidskleur te herkennen dan vrouwen met een donkere huidskleur.[62] Dat heeft onder andere te maken met de datasets die gebruikt worden om de modellen te trainen. Deze bevatten vaak een over-representatie van bepaalde categorieën gezichten (bijvoorbeeld blanke mannen) ten koste van anderen. Momenteel zijn er diverse partijen bezig om oplossingen te vinden voor problematische bias in gezichtsherkenningssystemen, onder meer door het samenstellen van databases met meer diversiteit.[63]

Een ander uitdaging is dat het mogelijk is om *deep learning* systemen om de tuin te leiden. Zo lukte het een consumentenorganisatie om smartphones met een op gezichtsherkenning gebaseerd beveiligingssysteem alsnog toegang te laten verlenen aan onbevoegden door een foto te gebruiken van de eigenaar van de telefoon.[64] Extreme make-up kan het gebruik van gezichtsherkenning bemoeilijken, maar ook speciaal ontwikkelde patronen op t-shirts, petten of brillen kunnen een juiste identificatie verhinderen of zelfs een verkeerde identificatie forceren. Onderzoekers aan de Carnegie Mellon Universiteit in de VS hebben specifieke patronen ontwikkeld die op een bril kunnen worden geprint om een *deep learning* systeem op het verkeerde been te zetten.[65] Deze patronen duwen als het ware het model richting de verkeerde classificatie, waardoor een persoon als een ander individu wordt aangemerkt. Ook zijn er systemen beschikbaar die foto's op het internet 'onleesbaar' maken voor gezichtsherkenningssystemen.[66]

Zo heeft een Amerikaanse privacy-organisatie een app ontwikkeld die volgens de makers foto's van gezichten zo bewerkt dat gezichtsherkenningssystemen ze niet goed meer kunnen verwerken.[67] De app bewerkt de gezichten bijvoorbeeld door automatisch gezichtskenmerken te identificeren en te anonimiseren door subtiel ruis aan het digitale beeld toe te voegen.

Een andere limiterende factor van de huidige gezichtsherkenningssystemen is dat ze veel rekenkracht en data nodig hebben om modellen te maken en nieuwe gezichten te herkennen. Ze hebben dus krachtige computers nodig om goed te kunnen werken. Dat betekent dat ze nog niet goed op kleine mobiele apparaten werken als losstaande applicatie (dus zonder internetconnectie).

---

[62] Inioluwa Deborah Raji en Joy Buolamwini 'Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products' (2019) 1 AAAI/ACM Conference on AI Ethics and Society 429.
[63] Zie bijvoorbeeld: IBM offers free 1m Face Dataset to Combat Bias (2019) 2 Biometric Technology Today 1.
[64] Peter Kulche, 'Gezichtsherkenning op Smartphone Niet Altijd Veilig' (2019) Consumentenbond <www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken> geraadpleegd 7 februari 2020.
[65] Synced, 'Adversarial Patch on Hat Fools SOTA Facial Recognition' (2019) Medium <www.medium.com/syncedreview/adversarial-patch-on-hat-fools-sota-facial-recognition-82e8c4f83498> geraadpleegd 7 februari 2020; Mahmood Sharif e.a., 'Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition' (2016) Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 1528.
[66] 'New System Shields People from Face Recognition' (2019) 7 Biometric Technology Today 1; Entropic 'volteFace v1.3 - Photo Anonymization. Now supports iPad.' (2019) <https://www.scentropic.com/blog/2019/jun/vf-release-1-3/vf-release-1-3.shtml> geraadpleegd 7 februari 2020.
[67] Zie ook de FaceShield app <https://faceshield.ai> geraadpleegd 20 januari 2020. Volgens de maker voegt deze app op specifieke plekken ruis toe aan een gezicht in een foto waardoor gezichtsdetectiesystemen het gezicht niet meer kunnen vinden.

Ook de beperkte uitlegbaarheid van *deep learning* modellen is een uitdaging. Vanwege de complexiteit van *deep learning* netwerken is het niet altijd duidelijk waarom een gezichtsherkenningssysteem met bepaalde resultaten komt.[68] Deze netwerken leren patronen te herkennen in grote hoeveelheden voorbeelden. Deze patronen kunnen anders zijn dan de gezichtskenmerken die mensen gebruiken om gezichten te herkennen. Op basis van welke patronen een *deep learning* netwerk uiteindelijk een gezicht herkent is doorgaans lastig af te leiden uit de complexe verbindingen tussen de meerdere lagen neuronen in een netwerk.

Verdere ontwikkelingen

Uit onze literatuurstudie en de expertworkshop komt naar voren dat de ontwikkelingen op het gebied van gezichtsherkenningstechnologie in de nabije toekomst vooral gericht zullen zijn op het verhelpen van de genoemde beperkingen, zoals het verder vergroten van de nauwkeurigheid en snelheid van de gezichtsherkenning en het ontwikkelen van algoritmen die beter in staat zijn om onder diverse uiteenlopende omstandigheden mensen te herkennen. Ook wordt er gewerkt aan methodes om meer soorten informatie uit beelden van gezichten te halen. Zo zijn er technieken ontwikkeld om de hartslag van een persoon te meten aan de hand van videobeelden van het gezicht.[69] Daarnaast zijn bedrijven en wetenschappers bezig om systemen te ontwikkelen die minder rekenkracht nodig hebben zodat ze makkelijker op mobiele apparaten gebruikt kunnen worden. Ook wordt het belang van het inzicht kunnen hebben in wat *deep learning* algoritmen precies doen steeds duidelijker en zullen er op het gebied van de uitlegbaarheid van algoritmen ook meer ontwikkelingen plaatsvinden. Er zijn daarnaast ook initiatieven die zich richten op het ontwikkelen van algoritmen die privacy beter beschermen door, bijvoorbeeld, de netwerken op zo een manier te trainen dat data niet gedeeld hoeven te worden tussen verschillende partijen.[70]

3.1.3. **Soorten toepassingen**

Gezichtsherkenning wordt momenteel in verschillende toepassingen gebruikt. In navolging van het Rathenau Instituut maken wij onderscheid tussen vijf *soorten* toepassingen: identificatie, verificatie, matching, categorisering en emotieclassificering.[71] Bij *identificatie* gaat het om het identificeren van personen op basis van digitale opnamen uit een bestaande database van personen. Dit is een 1-op-N vergelijking. Zo kan een winkel bijvoorbeeld een vaste klant identificeren aan de hand van camerabeeld op basis van een eerder gemaakt en opgeslagen biometrisch profiel van de klant. *Verificatie* betreft het 1-op-1 vergelijken van templates om te

[68] D. Castelvecchi, 'Can we open the black box of AI?' (2016) Nature News 538.7623, 20.
[69] M. A. Hassan, A. S. Malik, D. Fofi, N.I Saad, B. Karasfi, Y. Salih Ali, and F. Meriaudeau. 'Heart rate estimation using facial video: A review.' (2017), *Biomedical Signal Processing and Control*, 38, 346-360.
[70] I Masi e.a. 'Deep Face Recognition: A Survey' (2018) 31st SIBGRAPI Conference on Graphics, Patterns and Images 471.; Zie bijvoorbeeld R Shokri and V Shmatikov, Privacy-preserving deep learning.' (2015), *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*.
[71] Annelli Janssen, Linda Kool en Jelte Timmer, *Dicht op de huid: Gezichts- en Emotieherkenning in Nederland* (Rathenau Instituut 2015).

bepalen of een persoon de juiste persoon is. Zo kan een afgeleide representatie van het gezicht van een klant in een sportschool worden opgeslagen op een pas om vervolgens vergeleken te worden zodra de klant zich meldt voor camera's bij de toegangspoortjes van de sportschool. Bij *matching* worden beelden in een database vergeleken met andere beelden om zo foto's van personen bij elkaar te zoeken, zoals dat bijvoorbeeld gebeurt bij het automatisch *taggen* van personen op sociale media (het identificeren van iemand is hierbij niet het doel). Bij *categorisering* worden gezichtskenmerken gebruikt om personen in een bepaalde categorie te scharen (bijvoorbeeld 'oud' of 'jong', 'man' of 'vrouw'). *Emotieclassificering* lijkt op categorisering in de zin dat mensen worden gecategoriseerd naar hun (kennelijke of vermeende) emotie, waarbij een gezichtsuitdrukking gemeten en geclassificeerd wordt in termen van waargenomen basisemoties, zoals blij, boos, of verdrietig. Het verschil met categorisering is dat emoties een momentopname betreffen, terwijl categorisering veelal meer om duurzame (en daarmee meer identiteitsbepalende) kenmerken van personen gaat.

In de volgende sectie zullen wij in gaan op diverse huidige en verwachte toepassingen. Vooralsnog lijken veel toepassingen momenteel (nog) niet op grote(re) schaal bruikbaar. Omdat ontwikkelingen echter relatief snel gaan (onder andere door de enorme hoeveelheid beeldmateriaal die bij of via online platformen beschikbaar is en kan worden gebruikt om met Big Data Analytics de algoritmen voor gezichtsherkenning te trainen en optimaliseren), valt te verwachten dat de nodige toepassingen wel binnen een paar jaar op grotere schaal beschikbaar zullen zijn.

Daarbij moet worden opgemerkt dat voor veel van de huidige commerciële toepassingen de accuraatheid en kwetsbaarheid van modellen van relatief minder belang zijn dan bij publieke toepassingen. De gevolgen van fout-positieven (verkeerd herkend) of fout-negatieven (verkeerd niet herkend) zijn door de band genomen in winkels of bij reclame minder ingrijpend dan bijvoorbeeld op douanecontrole op Schiphol. Een onjuiste herkenning in een winkel (bijvoorbeeld als gevolg van een problematisch bias in de trainingsdata) kan bijvoorbeeld leiden tot een aanbeveling die niet relevant is voor een klant, terwijl dat bij een douanecontrole als gevolg kan hebben dat ongewenste personen worden toegelaten of dat bepaalde groepen personen disproportioneel vaak extra worden gecontroleerd.

3.2. Gezichtsherkenning: privacyrisico's

Nu wij de verschillende technieken en soorten toepassingen hebben beschreven, kunnen wij nader ingaan op de mogelijke privacyrisico's die verbonden zijn met het gebruik van gezichtsherkenningstechnologie in de horizontale relatie. In de sociologische, politicologische en techniekfilosofische literatuur is er nog niet uitgebreid onderzoek gedaan naar privacy-inbreuken in de context van gezichtsherkenningstechnologie in de horizontale relatie. Als er specifiek aandacht is voor gezichtsherkenning en de daarmee gemoeide privacyrisico's is dit vooral in de

verticale relatie, tussen overheid en burger. Met name *surveillance studies* onderzoekt deze verticale relatie.[72] Wél is er reeds uitgebreid aandacht besteed aan privacy-inbreuken door het gebruik van data-gedreven technologie in algemene zin en de rol van biometrische gegevens in het bijzonder.

Dat er in de wetenschappelijke literatuur nog maar weinig terug te vinden is over het onderwerp van dit onderzoek valt waarschijnlijk te verklaren doordat de toepassingen nog relatief nieuw zijn vergeleken bij het gebruik van gezichtsherkenningstechnologie door overheden. Zeker in Nederland wordt automatische gezichtsherkenning in horizontale relaties nog maar op beperkte schaal gebruikt. Niettemin constateren wij dat in het afgelopen jaar in zowel de media als in de politiek er in toenemende mate aandacht is voor dit fenomeen.

In deze sectie combineren wij dan ook de meer algemene literatuur over privacy-inbreuken en het gebruik van data-gedreven toepassingen met de eerste voorbeelden die wij zien in de praktijk. Wij gaan daarbij niet alleen uit van Nederland, maar kijken juist ook naar het buitenland waar gezichtsherkenning al vaker wordt toegepast. Deze internationale oriëntering geeft ons een vooruitblik op ontwikkelingen die wij misschien ook in Nederland kunnen verwachten. Om de risico's die met deze (toekomstige) gezichtsherkenningstoepassingen gepaard gaan geordend in kaart te brengen structuren wij dit hoofdstuk aan de hand van de vier categorieën van acties die privacy kunnen schenden (Solove) zoals beschreven in het vorige hoofdstuk: informatieverzameling, informatieverwerking, gegevensverspreiding en overschrijding. Om verder te duiden welke typen privacy door deze acties onder druk komen te staan maken wij gebruik van de typologie van Koops et al, ook beschreven in het vorige hoofdstuk.

3.2.1. Gezichtsherkenning en informatieverzameling in de horizontale relatie: privacyrisico's

In het geval van gezichtsherkenning is de activiteit van informatieverzameling voornamelijk gericht op het verzamelen van gezichtsafbeeldingen. Dit verzamelen kan zowel heimelijk als openlijk gebeuren. Er kan, bijvoorbeeld, een camera verstopt zijn of de camera kan duidelijk in het zicht geplaatst worden, vergezeld van een bord met de mededeling dat er gefilmd wordt. Er kan expliciet om een afbeelding gevraagd worden of deze kan zonder medeweten van de persoon in kwestie worden vergaard. Een belangrijk onderdeel van dit expliciet vragen om een afbeelding te mogen verwerken is dat het voor de betrokkene voorzienbaar is wat er met de afbeelding verder gebeurt.

Voor een goed functionerende gezichtsherkenningsapplicatie is het noodzakelijk, zoals hierboven reeds uiteengezet, om voldoende trainingsdata ter beschikking te hebben. Zo maakte IBM in januari 2019 een geannoteerde dataset beschikbaar voor onderzoek. Deze dataset heet

[72] Voor een overzicht van het domein Surveillance studies zie: David Lyon, *Surveillance Studies: An Overview* (Polity Press 2007) 256.

Dif (*Diversity in Faces*) en bestaat uit 1 miljoen afbeeldingen van gezichten die middels een speciale coderingsmethode voor raciale, leeftijdsgebonden, gender en andere gezichtskarakteristieken zijn geannoteerd. Dit moet ertoe leiden dat biases in gezichtsherkenningstoepassingen worden teruggedrongen.[73] Deze foto's zijn onderdeel van een nog veel grotere database namelijk YFCC[74] die maar liefst 99,2 miljoen foto's bevat die eerder online onder een Creative Commons licence is gepubliceerd. Creative Commons is een online overeenkomst betreffende auteursrechten, die het toestaat om afbeeldingen te kopiëren en te gebruiken voor academische en commerciële onderzoeksdoeleinden.

Ophef ontstond toen de media rapporteerden dat deze foto's merendeels afkomstig zijn van Flickr –een online platform waarop personen foto's delen– en er door de gebruikers geen expliciete toestemming was verleend voor het gebruik ervan voor het trainen van gezichtsherkenningstechnologie.[75] In reactie op de ophef stelt de CEO van Creative Commons, Ryan Merkley, dat de Creative Commons licence bedoeld is om al te restrictieve copyright regels open te breken. De achterliggende motivatie hierbij is dat het vrij gebruik van publiek toegankelijke informatie ten goede komt aan innovatie en vooruitgang. Maar, zo zegt Merkley, copyright is niet het goede vehikel om individuele privacy te beschermen, het gebruik van online surveillance tools te reguleren, of onderzoeksethiek vorm te geven in het AI-domein.[76]

Zo is één van de problemen waar Flickr gebruikers op stuiten, die niet willen dat hun foto's gebruikt worden om algoritmen te trainen, dat het niet duidelijk is welke foto's in de dataset zitten. Dit maakt bezwaar maken gecompliceerd.[77] Met andere woorden, waar Creative Commons licences ruimte maken voor dit soort gegevensverzameling met het oog op innovatie, lijken ze in de huidige vorm niet een adequaat instrument om naast auteursrechtelijke bescherming ook privacybescherming vorm te geven.

Uit een ander onderzoek blijkt dat de overheid, onderzoekers en bedrijven uit de Verenigde Staten afbeeldingen van immigranten, misbruikte kinderen en overleden personen hebben ingezet om hun gezichtsherkenningssysteem te trainen en testen. Het Facial Recognition Verification Testing program is een programma van het The National Institute of Standards and Technology (NIST).[78] Uit het onderzoek bleek dat de datasets van het testprogramma van NIST onder meer afbeeldingen bevatten van kinderen die uitgebuit zijn voor kinderpornografie, visa-aanvragers en

[73] 'IBM offers free 1m Face Dataset to Combat Bias (2019) 2 Biometric Technology Today 1.
[74] Bart Thomee e.a., 'YFCC100M: The New Data in Multimedia Research' (2016) 59 Communications of the ACM 64.
[75] Olivia Solon, 'Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent' (2019) NBC News <www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921> geraadpleegd 15 mei 2019.
[76] Ryan Merkley, 'Use and Fair Use: Statement on Shared Images in Facial Recognition AI' (2019) Creative Commons <www.creativecommons.org/2019/03/13/statement-on-shared-images-in-facial-recognition-ai/> geraadpleegd 15 mei 2019.
[77] Shannon Liao, 'IBM Didn't Inform People When it Used Their Flickr Photos for Facial Recognition Training (2019) The Verge <www.theverge.com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training> geraadpleegd 15 mei 2019.
[78] Os Keyes, Nikki Stevens and Jacqueline Wernimont, 'The Government Is Using the Most Vulnerable People to Test Facial Recognition Software' (2019) Slate <www.slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html> geraadpleegd 20 mei 2019.

overleden gearresteerden. Een deel van de dataset kan daarnaast worden gedownload, opgeslagen en gebruikt door private ondernemingen of burgers om hun eigen gezichtsherkenningssystemen te testen. NIST laat weten dat de afbeeldingen zijn verzameld door andere overheidsinstanties en dat ze erop vertrouwt dat dit is gebeurd volgens de missies van deze instanties.[79]

Als het gaat om gegevensverzameling is er ook een tendens om foto's van mensen 'in het wild' te gebruiken. Geposeerde portretfoto's als trainingsdata matchen immers niet zo goed met hoe gezichtsherkenningstechnologie in de praktijk moet fungeren, namelijk door het herkennen van mensen die bijvoorbeeld niet recht in de lens kijken, verhullende kledij dragen, of zich voortbewegen. Vanuit technisch oogpunt valt er dus iets te zeggen voor het gebruik van foto's van mensen die niet weten dat hun afbeelding vastgelegd wordt. Dit was bijvoorbeeld het geval bij de UnConstrained College Students Dataset [80] waarbij studenten op verschillende dagen zijn gefotografeerd door beveiligingscamera's van de universiteit zonder dat zij hiervan op de hoogte waren. Volgens de maker van de set, Prof. Terrance Boult, is toestemming niet vereist zolang hun identiteit niet bekend is, aangezien de studenten zich bevonden op een openbare locatie.[81]

Een ander recent voorbeeld werd bekend gemaakt door de *Financial Times*. De krant meldde dat foto's van Jillian York, een Amerikaanse activiste, onderdeel zijn van een dataset, IARPA Janus Benchmark-C.[82] Het betrof meerdere foto's, genomen over een periode van bijna tien jaar, waaronder ook screenshots afkomstig van YouTube video's. Ook deze dataset wordt gebruikt om commerciële systemen te trainen en te testen.

Ook Google is in opspraak gekomen doordat het bedrijf via een bemiddelingskantoor teams in onder andere Atlanta erop uit had gestuurd met het doel om foto's te maken van mensen en zo trainingsdata te verzamelen voor *Pixel 4 Facial Recognition*. De teams leken zich daarbij expliciet te richten op daklozen en mensen met een donkere huid en dit schijnbaar zonder te zeggen dat zij voor Google werkten en zonder te laten weten dat ze feitelijk mensen hun gezichten aan het vastleggen waren.[83]

Verschillende privacytypen onder druk

Wanneer wij door de lens van Koops' typologie kijken naar de privacyrisico's die met gegevensverzameling gepaard gaan, dan raken deze risico's vooral aan *de informationele*

[79] Ibid.
[80] Een voorbeeld van zo een studie: Manuel Günther e.a., 'Unconstrained Face Detection and Open-Set Face Recognition Challenge' (2017) IEEE International Joint Conference on Biometrics (IJCB) 697.
[81] J. Adrian Stanley, 'UCCS Secretly Photographed Students to Advance Facial Recognition Technology' (2019) Colorado Springs Independent <www.csindy.com/coloradosprings/uccs-secretly-photographed-students-to-advance-facial-recognition-technology/Content?oid=19664437> geraadpleegd 20 juni 2019.
[82] Madhumita Murgia, 'Who's Using Your Face? The Ugly Truth About Facial Recognition' (2019) Financial Times <www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e> geraadpleegd 15 mei 2019. IARPA is een Amerikaanse overheidsinstantie die innovatief onderzoek naar onder meer gezichtsherkenning financiert.
[83] Sean Hollister, 'Google Contractors Reportedly Targeted Homeless People for Pixel 4 Facial Recognition' (2019) The Verge <www.theverge.com/platform/amp/2019/10/2/20896181/google-contractor-reportedly-targeted-homeless-people-for-pixel-4-facial-recognition?__twitter_impression=true> geraadpleegd 7 oktober 2019.

component van lichamelijke privacy in de publieke en semi-publieke sfeer. Door het heimelijk vergaren van foto's is het voor individuen moeilijk om hun negatieve vrijheid te handhaven (de vrijheid om toegang tot hun fysieke kenmerken te ontzeggen). Wanneer de gegevensverzameling openlijk gebeurt, leidt dit mogelijk ook tot '*chilling effects'* en dus een aantasting van de *gedragsmatige privacy*.[84] Mensen gaan zich anders gedragen omdat ze zich bekeken voelen. De mogelijkheid om 'zichzelf te zijn' in de publieke ruimte wordt beknot. Zelfs wanneer mensen openlijk gevraagd wordt om informatie te delen en ze de mogelijkheid hebben dit te weigeren kan er ongemak ontstaan omdat men zich verplicht voelt na te denken over hoe het besluit al dan niet mee te werken te onderbouwen en hoe dit besluit vervolgens overkomt op anderen.

3.2.2. Gezichtsherkenning en informatieverwerking in de horizontale relatie: privacyrisico's

Zoals beschreven in het vorige hoofdstuk, verstaat Solove onder informatieverwerking het gebruik, opslaan, en manipulatie van verzamelde data. Het gaat hier dus met name over hoe de eerder verzamelde data op verschillende manieren wordt gebruikt. Zoals beschreven in hoofdstuk 2, maakt Solove hierbij onderscheidt tussen vijf subcategorieën *aggregatie*, *identificatie*, *onveiligheid*, *secundair gebruik* en *uitsluiting*.

Wanneer wij kijken naar informatieverwerking bij het gebruik van gezichtsherkenningstechnologie in de praktijk, dan zien wij dat ook hier in de bedrijf-burger relatie een aantal privacy-inbreuken zich reeds voordoet, bijvoorbeeld ten behoeve van het kunnen uitoefenen van een dienst zoals die van Uber. Het beveiligingssysteem van Uber, 'Real-Time ID Check', veroorzaakt dat transgender chauffeurs tijdelijk of permanent geen gebruik meer kunnen maken van de app. Het beveiligingssysteem vereist namelijk dat de chauffeurs op willekeurige momenten een selfie maken om hun identiteit te bevestigen. Als de foto niet overeenkomt met andere foto's in het systeem, wordt de gebruiker tijdelijk geschorst waarna Uber de zaak onderzoekt. Het systeem houdt echter geen rekening met veranderingen in het uiterlijk van mensen die een geslachtstransformatie ondergaan, waardoor zij onterecht worden verbannen uit de app.

Deze privacy-inbreuken vallen in Solove's taxonomie onder de subcategorie *onveiligheid* en *uitsluiting*. Uber kan dit weer ongedaan maken, maar hiervoor moet de chauffeur soms uren rijden om zich te melden bij een helpdesk. Daarnaast kan Uber niet garanderen dat de persoon in de toekomst niet weer onterecht geschorst wordt. Uber heeft aangegeven dit probleem te zullen verhelpen door gebruikers de mogelijkheid te bieden hun gendersituatie aan te geven in de app.

[84] C S Milligan, 'Facial Recognition Technology, Video Surveillance, and Privacy (1999) 9 Southern California Interdisciplinary Law Journal 295.

Volgens een woordvoerder van Uber is deze mogelijkheid reeds gecreëerd.[85] Wij hebben niet kunnen achterhalen of deze al in gebruik is genomen.

Identificatie via gezichtsherkenning werd ook ingezet op een Zweedse school om bij te houden of studenten aanwezig waren. De Zweedse toezichthouder heeft echter geoordeeld dat in het specifieke geval dit niet in overeenstemming was met de GDPR en heeft een boete van €20.000 opgelegd. Toestemming als wettelijke grondslag voor het gebruik van gezichtsherkenning was niet geldig. Aangezien er duidelijk sprake was van een machtsdisbalans tussen de studenten en de schoolleiding was het voor studenten niet mogelijk hier vrijelijk toestemming voor te geven.[86]

Ook *secundair gebruik* vormt een privacyrisico voor gezichtsherkenning. Zo werd gezichtsherkenningstechnologie ingevoerd door Lockport, een schooldistrict in New York om de veiligheid op school te vergroten.[87] Schoolbestuurders geven echter aan het ook te kunnen inzetten om bijvoorbeeld leerlingen te volgen die handelen tegen de regels om zo vast te kunnen stellen met wie ze omgaan en waar ze waren voor en na een incident.[88] Dit wordt ook wel *function creep* genoemd: technologieën die ontwikkeld en geïmplementeerd zijn met een specifieke functie krijgen er sluipenderwijs steeds meer functies bij.

Function creep ligt ook op de loer in het domein van personeelswerving. Daar wordt gezichtsherkenning en dan met name emotieherkenning ingezet als één van de factoren die mee worden genomen in de beoordeling van de kandidaat. Zo is er het bedrijf HireVue,[89] een start-up die gebruik maakt van algoritmen om gezichtsuitdrukkingen te matchen met karaktereigenschappen.[90] HireVue verkoopt onder andere zijn gezichtsherkenningsdiensten aan Unilever.[91] Volgens Privacy International –een non-gouvernementele organisatie die zich inzet om overheden en bedrijven bij de les te houden als het gaat om de bescherming van privacy– is het echter onduidelijk wat er gebeurt met de data die door zulke bedrijven worden vergaard. Ook is het niet duidelijk of werkgevers de gemoedstoestand van hun medewerkers ook blijven monitoren na de sollicitatieprocedure.[92]

Ook *aggregatie* vormt een privacyrisico. Er is bijvoorbeeld sprake van aggregatie als gezichtsherkenningsresultaten worden gecombineerd met andere informatiebronnen zoals informatie van sociale media. De onderzoekers Aqcuisti et al. hebben in een reeks experimenten

---

[85] Jaden Urbi, 'Some Transgender Drivers are Being Kicked off Uber's App' (2018) CNBC <www.cnbc.com/2018/08/08/transgender-uber-driver-suspended-tech-oversight-facial-recognition.html> geraadpleegd 10 juni 2019.
[86] EDPB, Facial Recognition in School Renders Sweden's First GDPR Fine (2019) <www.edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en> geraadpleegd 7 oktober.
[87] Ava Kofman 'Face Recognition Is Now Being Used In Schools, But It Won't Stop Mass Shootings' <www.theintercept.Com/2018/05/30/Face-Recognition-Schools-School-Shootings/> geraadpleegd 15 juni 2019.
[88] Thomas J Prohaska, 'Lockport Schools Turn to State-Of-The-Art Technology to Beef up Security' (2018) The Buffalo News <www.buffalonews.com/2018/05/20/lockport-schools-turn-to-state-of-the-art-technology-to-beef-up-security/> geraadpleegd 15 juni 2019.
[89] <www.hirevue.com/products> geraadpleegd 22 juni 2019.
[90] Patricia Nilsson, 'How AI Helps Recruiters Track Jobseekers' Emotions' (2018) Financial Times <www.ft.com/content/e2e85644-05be-11e8-9650-9c0ad2d7c5b5> geraadpleegd 15 juni 2019
[91] 'Emotional Recognition Technology Enters Recruitment' (2018) <www.privacyinternational.org/examples-abuse/1971/emotional-recognition-technology-enters-recruitment> geraadpleegd 15 juni 2019.
[92] Ibid.

vastgesteld dat het mogelijk is om individuen te re-identificeren online en offline, en gevoelige informatie over mensen af te leiden door het combineren van gezichtsherkenningstechnologie en data van sociale media.[93] Zij ontwikkelen ook het argument dat ondanks de nog aanwezige technische belemmeringen het in de lijn der verwachting ligt dat dit soort van surveillance 'gedemocratiseerd' zal worden. Met name door de beschikbaarheid van gegevens afkomstig van online sociale netwerken zal deze vorm van surveillance niet voorbehouden blijven aan overheden en grote bedrijven, maar ook in 'peer-to-peer relaties' plaatsvinden, dus tussen burgers onderling.[94] Deze ontwikkeling vormt een bedreiging voor de nog steeds breed gedragen privacyverwachting dat men anoniem is in de menigte en in de publieke ruimte. Acquisti et al. geven aan dat waar eindgebruikers het sowieso al lastig vinden om effectief hun privacy te beschermen in het dagelijks leven, dit probleem door gezichtsherkenningstechnologie verder wordt geïntensiveerd. Niet alleen verwachten wij niet dat vreemden ons zo eenvoudig kunnen identificeren, maar daarboven komt nog de verrassing over wat er allemaal over ons afgeleid kan worden door online beschikbare informatie.

Verschillende privacytypen onder druk

De bovenbeschreven voorbeelden van informatieverwerkingsactiviteiten raken verschillende privacytypen. Uber's gezichtsherkenning vormt een risico voor de *beslissingsprivacy* van transgender bestuurders, die gedwongen worden deze gevoelige informatie te delen als ze voor Uber willen blijven werken. Toepassingen zoals het identificeren van leerlingen op de Zweedse school raakt aan communicatieve en *gedragsmatige privacy*. Dergelijke toepassingen hebben invloed op hoe vrij mensen zich voelen om zichzelf te zijn. Function creep maakt het moeilijk om controle te houden over iemands *communicatieve privacy*. Wat in een bepaalde context wordt gebruikt, kan zomaar in een andere context weer opduiken. Het raakt ook *gedragsmatige privacy*, omdat, wanneer men weet dat gezichtsherkenning wordt ingezet, men zich mogelijk anders gaat gedragen om een zo goed mogelijke indruk te maken op het algoritme (wat "goed" dan ook moge betekenen). Het raakt ook aan *ruimtelijke privacy*, wanneer men op school –een semi-publieke ruimte– plots overal gevolgd kan worden.

3.2.3. Gezichtsherkenning en gegevensverspreiding in de horizontale relatie: privacyrisico's

Wanneer wij kijken hoe *gegevensverspreiding* bij gezichtsherkenning privacyrisico's veroorzaakt, dan zien wij dat dit, tot op een bepaalde hoogte en met name in het buitenland, zich reeds in de praktijk voordoet. Solove noemt zeven verschillende soorten mogelijk schadelijke activiteiten die onder gegevensverspreiding vallen: *vertrouwensbreuk*, *onthulling*, *blootstelling*, *toenemend*e

[93] Acquisti, Alessandro and Gross, Ralph and Stutzman, Frederic D., Face Recognition and Privacy in the Age of Augmented Reality (2014). Journal of Privacy and Confidentiality, 6(2), 1, 2014.
[94] Ibid. p. 13.

toegankelijkheid, *afpersing*, *toe-eigenen* en *verstoring*. Gezichtsherkenning maakt bepaalde informatie toegankelijker waardoor het risico op het onthullen van persoonlijke informatie groter wordt. Voor de burger kan dit onder meer leiden tot reputatieschade, het risico zich beknot te voelen in zijn of haar persoonlijke vrijheid, maar ook ongewenste gevolgen als afpersing en identiteitsdiefstal. Van sommige soorten gegevensverspreiding zijn wij geen voorbeelden tegen gekomen, maar kunnen wij door beargumenteerde extrapolatie toch aannemelijk maken dat deze zich in de nabije toekomst voor zouden kunnen doen.

Een voorbeeld van hoe gegevensverspreiding bij gezichtsherkenning kan leiden tot privacyrisico's is het gebruik van de Russische applicatie FindFace. Vrouwen werkzaam in de porno-industrie werden via deze app op Vkontakt –een veelgebruikt Russisch sociale media platform– geïdentificeerd.[95] Vervolgens werden hun contactgegevens gedeeld, wat onder meer leidde tot stalking (zijzelf maar ook vrienden en familie waren doelwit), afpersing en reputatieschade. Overigens is het ook goed mogelijk dat er bij deze toepassing van gezichtsherkenning valse positieven voorkomen en dat sommige slachtoffers helemaal niet werkzaam zijn in de porno-industrie. Er is dan sprake van het verspreiden van valse informatie (*verstoring*).

Toepassingen zoals Findface, waarvoor men louter een smartphone nodig heeft om er gebruik van te kunnen maken, kunnen van invloed zijn op het sociaal verkeer. Hoewel het voorbeeld van het blootstellen van porno-actrices aan de buitenwereld zeer duidelijk de risico's voor het voetlicht brengt, zijn er tal van andere meer alledaagse privacy-inbreuken te bedenken via apps zoals Findface. Deze inbreuken halen het nieuws misschien niet, maar kunnen wel een negatieve impact hebben op iemands vrijheid. Gezichtsherkenning gebruiken om mensen heimelijk te zoeken op sociale media bijvoorbeeld, kan leiden tot tal van *onthullingen* die men liever voor zichzelf zou willen houden.

Net zoals bij andere data-gedreven bedrijven, kan het vertrouwen in gezichtsherkenningsbedrijven ook worden geschaad (*vertrouwensbreuk*) wanneer zij de databases waarmee ze werken niet voldoende beschermen en daarmee grote hoeveelheden persoonsgerelateerde data toegankelijk maken (datalek). Dit was het geval met het gezichtsherkenningsbedrijf SenseNets dat zijn database met meer dan 2.500.000 persoonlijke records (inclusief identiteitsnummers, adressen en locatiedata) onbeschermd en voor iedereen vrij toegankelijk opsloeg.[96]

---

[95] <www.tjournal.ru/flood/26824-polzovateli-dvacha-deanonimizirovali-rossiyskih-pornoaktris-s-pomoshchyu-findface> geraadpleegd op 2 augustus 2019; Kevin Rothrock, 'Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses' (2016) Ars Technica <https://arstechnica.com/tech-policy/2016/04/facial-recognition-service-becomes-a- weapon-against-russian-porn-actresses/> geraadpleegd op 12 augustus 2019.

[96] AlfredNG,'ChineseFacialRecognitionCompanyLeftDatabaseofPeople'sLocationsExposed'(2019) CNET <www.cnet.com/news/chinese-facial-recognition-company-left-database-of-peoples- location-exposed/> geraadpleegd 12 augustus 2019.

Ook kan gezichtsherkenning reeds aanwezige informatie toegankelijker maken. Zo zijn er gezichtsherkenningsbedrijven die hun diensten aan zomerkampen en ouders aanbieden.[97] Gezichtsherkenning wordt toegepast om de kinderen te identificeren op de foto's die gedurende de dag gemaakt zijn en de ouders krijgen hiervan een bericht. Naast dat het ouders het gevoel geeft dat zij in verbinding blijven met hun kinderen en het sommige zorgen wegneemt, kan het ook leiden tot extra zorgen, wanneer een kind bijvoorbeeld niet blij op een foto staat. Medewerkers van de zomerkampen geven aan dat dit leidt tot extra telefoontjes van verontruste ouders. De voorheen redelijk van hun ouders afgeschermde zomerkampen worden nu minder privé. Bovendien gaan kinderen zich ook anders gedragen. Ze gaan duidelijk glimlachend op de foto en zorgen ervoor dat ze op voldoende foto's staan. Zo stelt een zomerkampdeelnemer: "a picture a day, keeps your mum away".[98]

Gezichtsherkenning wordt vaak ingezet voor verificatie en identificatie met als reden dat het veiliger dan andere methodes zou zijn, zoals het gebruik van toegangspassen, omdat identiteitsdiefstal moeilijker is. Het stelen van iemands gezicht is immers ingewikkelder dan het namaken of ontvreemden van een ID kaart of toegangspas. Op dit terrein is echter ook misbruik mogelijk. Zo toonden onderzoekers van de Universiteit van North Carolina aan verschillende, veel gebruikte gezichtsherkenningssystemen –o.a. voor het beveiligen van toegang tot gegevens of mobiele telefoons– te kunnen misleiden op basis van foto's die ze op sociale media platformen zoals Facebook, LinkedIn, en Google konden vinden.[99] Door de gevonden foto's zodanig te bewerken –onder andere door het gebruik van 3D modeleringstechnieken– konden ze de systemen om de tuin leiden en zich toegang verschaffen. Hoewel het niet onmogelijk is om zo een aanval te voorkomen, bijvoorbeeld door te investeren in extra beveiligingschecks zoals infrarood scanners, hangt aan zulke innovaties een investering vast welke niet in alle situaties rendabel is.

Verschillende privacytypen onder druk

Deze voorbeelden van informatieverspreiding kunnen verschillende privacyaspecten onder druk zetten. Zo raakt Findface aan de *beslissingsprivacy*[100] van vrouwen omdat het hun vrijheid aantast zelf te beslissen over gevoelige onderwerpen in de intieme sfeer. Door het delen van deze informatie worden ze ongewild blootgesteld aan de buitenwereld. Ze kunnen niet langer zelf beslissen welke intieme aspecten van hun leven ze delen met anderen.

In het voorbeeld van het gebruik van gezichtsherkenning tijdens zomerkampen worden de *ruimtelijke privacy* en *gedragsmatige privacy* van kinderen geraakt. Het enigszins vrij zijn van

[97] Drew Harwell 'As Summer Camps Turn on Facial Recognition, Parents Demand: More smiles, Please' (2019) <www.washingtonpost.com/technology/2019/08/08/summer-camps-turn-facial-recognition-parents-demand-more-smiles-please/> geraadpleegd 7 oktober 2019.
[98] Idem.
[99] Lily Hay Newman, 'Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?)' (2016) Wired <www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/> geraadpleegd 11 september 2019.
[100] We gaan er hierbij vanuit dat deze vrouwen vrijwillig in deze sector werkzaam zijn. Als zij echter gedwongen worden is er in eerste instantie sprake van een grove schending van hun lichamelijke privacy.

ouderlijk toezicht wordt door de gezichtsherkenning tenietgedaan en kinderen passen hun gedrag aan om ouders niet onnodig ongerust te maken.

3.2.4. **Gezichtsherkenning en overschrijding in de horizontale relatie: privacyrisico's**

Solove maakt, zoals eerder uitgelegd in hoofdstuk 2, bij de vierde en laatste categorie van mogelijk schadelijke activiteiten, *overschrijding,* een onderscheid tussen *intrusie* en *inmenging in besluitvorming.* Beide liggen op de loer bij het gebruik van gezichtsherkenning voor het personaliseren van diensten en advertenties. In de retailsector wordt gezichtsherkenning gezien als een mogelijkheid om –net zoals op het internet– een gepersonaliseerde interactie mogelijk te maken. Op basis van reeds bekende informatie en eventueel in combinatie met *real-time* emotiedetectie kunnen aanbiedingen worden gepersonaliseerd en mensen worden *genudged*[101] in hun besluitvorming. Zo experimenteert de Californische keten CaliBurger met gezichtsherkenning in hun verkooppunten. Klanten met een *loyalty status* worden via gezichtsherkenning geïdentificeerd. Ze kunnen hierdoor sneller afrekenen en het aanbod dat ze te zien krijgen is aangepast aan hun profiel.[102] Ook slimme reclamezuilen zijn in opkomst. De slimme camera's die in deze reclamezuilen zijn verborgen, zijn in staat om onder andere leeftijd, geslacht, en gemoedstoestand vast te stellen en in een fractie van een seconde het reclamebord daarop aan te passen.[103] Zulke toepassingen zijn erop gericht om mensen in het dagelijks leven te beïnvloeden in hun keuzes.

Verschillende privacytypen onder druk

Waar deze voorbeelden op zichzelf nog redelijk onschuldig ogen, houdt het vooruitzicht op een semi-publieke ruimte waarin gepersonaliseerde advertenties en data-gedreven interacties in winkels alomtegenwoordig zijn wel degelijk een privacyrisico in. De spam en gepersonaliseerde advertenties die velen online als onprettig ervaren, kunnen door middel van gezichtsherkenning nu ook offline toegepast worden. Gezicht -en emotiedetectie kan bovendien ingezet worden om klanten te verleiden tot het doen van bepaalde aankopen. Wanneer gezichtsherkenning wordt ingezet om mensen te beïnvloeden in hun keuzes en zij zich daar niet meer goed aan kunnen

---

[101] Nudging is een term afkomstig uit de gedragswetenschappen en behavioural economics waarmee wordt aangeduid dat mensen hun keuzes gestuurd kunnen worden door de keuze-architectuur aan te passen en in te spelen op bepaalde gewoontes en biases. Een geprefereerde uitkomst kan met deze vorm van regulering dan voorgesorteerd worden. Voor meer info zie: R. H. Thaler and C.R. Sunstein, *Nudge: improving decision about health, wealth, and happiness.* (New Haven: Yale University Press, 2008)

[102] Rick Ferguson, 'Facial recognition Software Comes to Loyalty' (2018) Retailwire <www.retailwire.com/discussion/facial-recognition-software-comes-to-loyalty/?utm_source=Listrak&utm_medium=Email&utm_term=http%3a%2f%2fwww.retailwire.com%2fdiscussion%2ffacial-recognition-software-comes-to-loyalty%2f&utm_campaign=Today+on+RetailWire%3a+Alexa-enabled+glasses%3b+Kohl%27s+omni-progress%3b+Facial+recog+loyalty+-+1%2f9%2f18> geraadpleegd 9 oktober 2019.

[103] Eden Gillespie, 'Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop' (2019) The Guardian <www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop> geraadpleegd 9 oktober 2019.

onttrekken staat de *mentale privacy* onder druk. Wanneer mensen er zich van bewust worden dat ze gevolgd en geanalyseerd worden wanneer ze zich in winkels of in de publieke ruimte begeven, bestaat bovendien het risico dat ze hun gedrag hierop aan gaan passen.

3.3. Conclusie

Gezichtsherkenningstechnologie en -toepassingen zijn momenteel volop in ontwikkeling. Het is aannemelijk dat ze in de komende jaren op grotere schaal onderdeel zullen vormen van onze dagelijkse interacties met anderen en met bedrijven. Er zijn echter ook nog een aantal technische uitdagingen en beperkingen in het gebruik, zoals de bias in gezichtsherkenningsmodellen en het herkennen van mensen in ongecontroleerde omstandigheden.

Ook zien wij dat de gezichtsherkenningstoepassingen die nu worden uitgerold risico's op privacy-inbreuken met zich meebrengen als gevolg van informatievergaring, informatieverwerking, gegevensverspreiding en overschrijding. Bewust van de continu monitorende blik van gezichtsherkenningssystemen in publiek en semi-publieke ruimte, zoals pleinen of scholen, kunnen mensen bijvoorbeeld zich gedwongen voelen hun gedrag aan te passen of bepaalde plekken te vermijden. Een ander voorbeeld is dat de technologie mensen in staat stelt om gegevens over een persoon die maar voor een beperkt publiek waren bedoeld op grotere schaal te onthullen. Om meer grip te krijgen op wat deze risico's voor de privacy van burgers concreet inhouden, zullen wij in het volgende hoofdstuk in meer detail deze risico's onderzoeken aan de hand van een viertal domeinstudies.

4. Domeinstudies

Nu wij een globaal idee hebben van de verschillende privacyrisico's die het gebruik van gezichtsherkenning in horizontale relaties kan voortbrengen, zal dit hoofdstuk zich richten op vier domeinen waarbinnen gezichtsherkenningstechnologie wordt toegepast, binnen Nederland en daarbuiten: organisatie van evenementen (1), smartphone apps (2), slimme deurbel (3), en retail (4). Onderstaande verkenning is gebaseerd op een literatuurstudie, stakeholder-interviews en de resultaten uit de expertworkshop. In navolging op de literatuurstudie in het vorige hoofdstuk structureren wij de privacyrisico's aan de hand van Solove's onderscheidingen. Waar nodig worden deze privacyrisico's verder geduid aan de hand van Koops' privacy types. In hoofdstuk 5 wordt op basis van de bevindingen uit hoofdstuk 3 en 4, de eerste onderzoeksvraag beantwoord.

4.1. Organisatie van evenementen

In het domein van de evenementenorganisatie wordt gezichtsherkenning gezien als een krachtige technologie die verschillende aspecten van een evenement kan verbeteren. In een brochure uitgegeven door Zenus (één van de bedrijven die wij gesproken hebben in het kader van dit onderzoek) worden zeven specifieke toepassingen onderscheiden.[104] Ten eerste is er de snelle *check-in* (waar wij later nog uitgebreider op terug zullen komen). Om lange rijen tegen te gaan bij de *check-in*, kunnen bezoekers opteren voor gezichtsherkenning. Nadat ze thuis bij de aanmeldingsprocedure een foto hebben geüpload, kunnen ze bij aankomst op het evenement via gezichtsherkenning geïdentificeerd worden. Indien gewenst kan een toegangsbewijs bij aankomst onmiddellijk geprint worden zonder extra handelingen van bezoeker of host.[105]

Ten tweede is er de identiteitscheck of *ID check*. Omdat *ID check* veel tijd kost en niet altijd goed wordt uitgevoerd, wordt de mogelijkheid ontwikkeld om een *ID check* uit te voeren bij de registratie. Bezoekers dienen dan een selfie te nemen met hun paspoort of ID kaart. Gezichtsherkenningstechnologie wordt dan ingezet om de *ID check* uit te voeren. Een soortgelijke check kan ook op het evenement zelf worden uitgevoerd.[106]

Ten derde is er de mogelijkheid tot het invoeren van *watchlists*. Om de veiligheid te bevorderen is het mogelijk om een lijst op te stellen van mensen die geen toegang horen te verkrijgen. Het systeem kan dan alarm slaan wanneer dit toch gebeurt. Tevens kan zo een lijst

[104] Zenus, 'Facial Recognition and Events: A Comprehensive Guide (2018)' <www.eventmanagerblog.com/facial-recognition-guide-2018> geraadpleegd 24 juli 2019.
[105] Ibid, p.4.
[106] Ibid, p.5.

ook juist gebruikt worden om belangrijke mensen te detecteren en hen een VIP behandeling aan te bieden.[107]

Ten vierde is er de mogelijkheid tot *sessie tracking.* Met gezichtsherkenning wordt het mogelijk om bij te houden welke sessies goed en welke minder goed bezocht worden. Een bedrijf of organisatie kan ook nagaan wie er een sessie bijwoont, wat van belang kan zijn voor educatie-evenementen waarbij professionals punten kunnen verdienen of bij sessies waarbij de inhoud sensitief is en alleen bedoeld voor een specifiek deel van de bezoekers.[108]

Ten vijfde worden er *heatmaps* ontwikkeld. Gezichtsherkenning kan ingezet worden om te monitoren hoe bezoekers zich bewegen op het evenement. Dit kan gebruikt worden om bijvoorbeeld de prijs van stands te bepalen, *crowd control* en het optimaliseren van de inrichting van een evenement.[109]

Gemak en personalisatie zijn ook een belangrijk toepassingsgebied voor gezichtsherkenning in de evenementen industrie. Gezichtsherkenning kan ingezet worden om bezoekers op een persoonlijke wijze te begroeten, hen gepersonaliseerde aanbiedingen te doen of hen via schermen de weg te wijzen naar de juiste sessie.[110]

De laatste toepassing die als veelbelovend wordt gezien is '*lead retrieval*'. Gezichtsherkenning kan de interactie tussen bezoekers en standhouders op een evenement soepeler laten verlopen. Nu is het nog nodig om een badge manueel te scannen als een bezoeker een stand bezoekt. Met gezichtsherkenning wordt dit overbodig. De relevante gegevens worden direct doorgegeven aan de standhouder die zijn of haar bezoeker persoonlijk kan begroeten en die eventueel een VIP behandeling kan bezorgen.[111] Er kan bovendien ook bijgehouden worden wie de stand bezocht heeft. Dit kan tot waardevolle inzichten leiden voor de standhouder.

Om een meer gedetailleerd beeld te krijgen van de genoemde toepassingen belichten wij in het hiernavolgende twee bedrijven. Centraal staan Zenus en 20Face. Beide bedrijven ontwikkelen en leveren gezichtsherkenningstechnologie voor evenementorganisaties. Zenus is gevestigd in de Verenigde Staten, 20Face in Nederland. In aanvulling daarop hebben wij ook gesproken met congrescentrum RAI Amsterdam, afnemer van gezichtsherkenningstechnologie (geleverd door onder andere Zenus).

4.1.1. **De bedrijven**

Zenus en 20Face zijn beide ontwikkelaars en leveranciers van gezichtsherkenningstechnologie. Zenus is gevestigd in Houston, Texas (Verenigde Staten). Deze startup, opgericht in 2015, richt zich met zijn dienstverlening exclusief op de evenementenindustrie. Op dit ogenblik heeft het

[107] Ibid, p.7.
[108] Ibid. p.7.
[109] Ibid. p.8.
[110] Ibid. p.9.
[111] Ibid. p.10.

bedrijf twee productielijnen: *identificatie* en *analytics* door middel van gezichtsherkenning. Identificatie richt zich op een snelle check-in. Analytics biedt op dit ogenblik de mogelijkheid om bij te houden hoeveel bezoekers een stand aantrekt en dit te vergelijken met de prestaties van andere exposanten. Ook het bijhouden van bezoekersaantallen bij specifieke sessies of workshops behoort tot de mogelijkheden. Analytics biedt ook de mogelijkheid tot emotiedetectie. Met emotiedetectie kan in kaart worden gebracht hoe mensen zich voelen bij het bezoek aan verschillende stands. In de pijplijn zitten ook nog andere toepassingen zoals: demografische analyse op basis van gezichtscategorisatie. Door middel van gezichtsanalyse kunnen exposanten meer over hun doelgroep –zoals leeftijdsgroep en geslacht– te weten komen zonder dat bezoekers moet worden gevraagd formulieren in te vullen. Het gaat hier om het gebruik van zogenaamde geaggregeerde gegevens. Dit niveau van analyse, zo stelt Zenus op hun website, is nodig om zinvolle zakelijke inzichten te verkrijgen en tegelijkertijd de privacy van mensen te beschermen.[112] Maar ook het monitoren van wie er binnenkomt is een mogelijke toepassing. Gezichtsherkenning wordt dan ingezet om ongewenste gasten te identificeren en hen de toegang te ontzeggen.

20Face is een Nederlands bedrijf, opgericht in 2017, als spin-off van de Universiteit Twente. Het biedt op maat gemaakte gezichtsherkenningssystemen, vooral op het gebied van beveiliging en verbeterde klantervaringen. Het bedrijf ziet de horeca, kaartverkoop, zorg, beveiliging, surveillance en cybersecurity als belangrijke markten. Momenteel is 20Face ook bezig met de ontwikkeling van een optie die het mogelijk moet maken dat de bezoekers van evenementen de controle behouden over hun eigen data door de data decentraal op te slaan. Het bedrijf beschrijft dit systeem als een ecosysteem voor “self-enrollment, consent and personal data release management”.[113]

4.1.2. **Gezichtsherkenningstechnologie**

Zenus en 20Face maken beide gebruik van algoritmen om gezichten te herkennen. Een deel is gebaseerd op *deep learning* methoden, maar ze maken volgens de betrokkenen die wij gesproken hebben ook gebruik van andere typen algoritmen. Het is echter onduidelijk gebleven welke dit zijn.

Zenus’ systeem leidt een biometrisch template (Facial Geometry) af uit een foto en slaat uitsluitend deze template op. In het interview met de CEO en CTO van Zenus wordt benadrukt dat Zenus geen afbeeldingen bewaart. Het gecreëerde template is een unieke collectie van meetpunten van een gezicht op een afbeelding. Dit template kan gebruikt worden om hetzelfde gezicht op een andere afbeelding te herkennen. Het template wordt een week na afloop van het evenement ook verwijderd. Zenus heeft bovendien geen toegang tot persoonsgegevens zoals naam, achternaam, e-mailadres. Om hun diensten te kunnen leveren hebben ze enkel de foto en een registratienummer nodig.

---

[112] <www.zenus-biometrics.com/services/event-management> geraadpleegd 28 juli 2019.
[113] <https://smartregiontwente.nl/netwerk/20-face> geraadpleegd 14 februari 2020.

20Face maakt gebruik van een systeem van verschillenden algoritmen om gezichten te herkennen. Afhankelijk van de kwaliteit van het beeld kan een specifiek algoritme gekozen worden om zo het beste resultaat te verkrijgen. De gezichtsherkenningsalgoritmen van 20Face zijn vooral ontwikkeld voor identificatie en verificatie. Ze zijn bovendien gemaakt om in ongecontroleerde omgevingen te werken en ze kunnen goed omgaan met variatie in pose en lage resolutie beelden. Bovendien kan het 20Face systeem met behulp van de set van algoritmen mensen herkennen op basis van slechts een deel van het gezicht en werkt het ook onder extreme belichting. De gebruiker hoeft zich daarom niet al te veel aan te passen aan het systeem (bijvoorbeeld in de juiste pose en onder juist belichting staan) om het goed te kunnen gebruiken.

Net zoals bij Zenus werkt ook het systeem van 20Face op basis van een template ('Face square'). Het systeem leidt deze af uit een afbeelding van een gezicht en slaat deze versleuteld op in de *cloud*. De template en enkele persoonsgegevens, zoals naam en adres, vormen samen een 'biometrisch profiel', welke ook weer opgeslagen kan worden in de *cloud*. De template uit een biometrisch profiel kan vergeleken worden met gezichten van bezoekers die langs een zogenaamd *end-point* -een applicatie met een camera- lopen. Een end-point scant gezichten en maakt templates, die dan vervolgens vergeleken worden met de templates van biometrische profielen. Om templates te vergelijken moet een end-point toestemming hebben voor toegang tot een biometrisch profiel.

Beide bedrijven bieden de gezichtsherkenningsfunctionaliteit in verschillende producten en services aan. Zo heeft Zenus drie verschillende modules voor klanten: *API integratie, microsites* en *snippets.*[114] Bij *API integratie* wordt er alleen een connectie gelegd tussen het systeem van Zenus en van de klant. De rest van het systeem moet nieuw ontwikkeld worden. Deze module vergt dus meer inspanning om te bouwen en onderhouden. Er zal ook meer tijd en aandacht geïnvesteerd moeten worden in het compliance gedeelte. Het voordeel van deze module is dat het systeem helemaal in de huisstijl en wensen van de klant kan worden gegoten.

De *microsites module* is een complete integratie van Zenus' software in het systeem van de klant door middel van een door Zenus gebouwde gebruikersinterface. Het is hierbij mogelijk het logo en de kleurschakering overeen te laten stemmen met het merk van de klant. Compliance is, zo stelt Zenus, expliciet meegenomen in het ontwerp van het systeem. Deze module is het snelst te verwezenlijken.

De *snippets module* maakt het mogelijk om gebruik te maken van de geoptimaliseerde broncode ontwikkeld door Zenus. Volgens het bedrijf geeft dit de mogelijkheid om de geïntegreerde software module verder te personaliseren zowel op het terrein van performance als ook op het gebied van gebruikerservaring. Compliance is ingebouwd in het systeem.

Naast de gezichtsherkenningsdienstverlening heeft Zenus kortgeleden ook een eigen analytics camera uitgebracht. Deze camera kan gezichtsherkenningsanalyses uitvoeren op het

[114] <www.zenus-biometrics.com/services/services-integrations> geraadpleegd 28 juli 2019.

apparaat zelf of in de cloud.[115] Daarnaast biedt Zenus ook de optie om on-site servers te installeren. Volgens Zenus biedt dit voordelen omdat de servers geoptimaliseerd kunnen worden voor de zware rekenkracht die nodig is wanneer verschillende gezichtsherkenningsberekeningen tegelijk plaatsvinden. Bovendien is men niet afhankelijk van internetconnectiviteit die bij overbelasting voor interrupties kan zorgen.[116]

De technologie van Zenus is onder meer ingezet door het congrescentrum RAI in Amsterdam. Bij het evenement Horecava in januari 2019, heeft daar een test plaatsgevonden waarbij 1250 bezoekers zich voor het evenement hebben geregistreerd via gezichtsherkenning. Bezoekers uploaden thuis een foto die door het systeem onmiddellijk in code werd omgezet. Voor Horecava werd de foto tevens opgeslagen en afgedrukt op bezoekersbadges. Bij aankomst bij de ingang werden gezichten gescand door een camera, gedigitaliseerd, vergeleken met de code in het systeem en herkend. Nadat de bezoeker zijn of haar identiteit had bevestigd, werd een badge door het systeem afgedrukt.[117]

Via interactieve panelen ('trylikes') konden bezoekers aangeven wat ze van de toegang via gezichtsherkenning vonden. Van de respondenten zei 92% enthousiast te zijn. Een e-mailenquête na het evenement vroeg om meer specifieke input en 80% van de gebruikers verklaarde dat ze 'tevreden' tot 'zeer tevreden' waren met de nieuwe technologie. Mensen waren vooral enthousiast over het gebruiksgemak, vlotte toegang en persoonlijke ontvangst. Sommige mensen genoten er gewoon van omdat het iets nieuws was. Zoals een van de bezoekers aangaf: "Je ziet dit soort dingen in films, dus het is geweldig om te zien dat het echt werkt in het echte leven."[118]

20Face zet in op dienstverlening op maat en werkt op basis van licenties en '*shared revenu models*'. Zo heeft het bedrijf een gezichtsherkenningssysteem ontwikkeld voor de skyboxen in het voetbalstadion van Heracles in Almelo. In deze toepassing, konden skybox leden een aantal dagen voor een wedstrijd een foto sturen naar Heracles. Op de dag van de wedstrijd konden de leden die een foto hadden gestuurd toegang krijgen door middel van gezichtsherkenning.[119] Bij deze proefopstelling werd gebruik gemaakt van een centrale database. Het bedrijf heeft aangekondigd dat indien de testen goed verlopen ook VIP leden en uiteindelijk ook jaarleden op deze manier en op vrijwillige basis toegang zouden kunnen krijgen tot het stadion.

Voor de op maat gemaakte dienstverlening maakt het bedrijf gebruik van een modulair platform dat bestaat uit drie modules: *self-enrollment*, datamanagement en de herkenning en identificatie software. De *self-enrollment* functionaliteit van 20Face stelt gebruikers in staat om

[115] <www.zenus-biometrics.com/services/smart-camera> geraadpleegd 28 juli 2019.
[116] <www.zenus-biometrics.com/services/services-server> geraadpleegd 28 juli 2019.
[117] Pim Schoonderwoerd & Paul Hassink 'A More Friendly and Efficient Reception With Facial Recognition' (2019) RAI Amsterdam <www.rai.nl/en/rai-amsterdam/blogs/a-more-friendly-and-efficient-reception-with-facial-recognition/> geraadpleegd 18 oktober 2019.
[118] Ibid.
[119] <www.20face.com/heracles-almelo-skybox-members/> 19 oktober 2019.

zichzelf aan te melden voor het gebruik van het systeem en zelf een biometrisch profiel aan te maken. Deze *enrollment* procedure vraagt een actieve en expliciete medewerking van de gebruiker en het is daarom ook relatief makkelijk om toestemming voor de opslag van de data te vragen. Het bedrijft heeft een app ontwikkeld voor het *self-enrollment* proces. Met deze app kan de persoon ook de toegang tot dit profiel beheren.

De datamanagement module zorgt ervoor dat een profiel wordt opgeslagen in een persoonlijke 'datakluis' en dat deze met de juiste toestemming van de gebruiker opgevraagd kan worden door derden. Derden zijn dan bijvoorbeeld de evenementlocaties die gezichtsherkenning gebruiken voor een snelle check in. 20Face maakt hiervoor gebruik van een blockchain systeem. De datakluis is opgeslagen in een cloud, waarvan de servers in Nederland staan.

20Face streeft ernaar om het platform zo generiek mogelijk te maken zodat in de toekomst andere bedrijven hun eigen biometrie of andere soorten module kunnen toevoegen aan het platform.

4.1.3. **Privacyrisico's**

Informatieverzameling

Bij zowel Zenus als 20Face werkt gezichtsherkenning voor een snelle check-in altijd op *opt-in* basis. Bezoekers moeten expliciet toestemming verlenen en hebben altijd de mogelijkheid om zich aan te melden voor het desbetreffende evenement zonder gebruik te maken van gezichtsherkenning. Omdat beide bedrijven in de meeste gevallen ook de interface aanleveren voor het uploaden van de afbeelding en het verkrijgen van de toestemming, kunnen zij erop toe zien dat dit op een adequate wijze gebeurt. De enige manier waarop het biometrisch profiel kan worden aangemaakt in beide systemen is doordat de gebruiker zichzelf inschrijft en zelf een foto afgeeft. De deelname in beide gevallen is geheel vrijwillig.

Bij de toegangscontrole zijn de camera's in principe ook duidelijk zichtbaar en zal de gebruiker gevraagd worden actief mee te werken. Op evenementen is in veel gevallen de interactie met de camera ook merkbaar aanwezig voor het analytics gedeelte van het Zenus systeem. Een foto wordt gemaakt en data opgevraagd of een persoon wordt gevraagd in een camera te kijken.

De zichtbaarheid van de camera en de bewuste interactie met het systeem is echter (op termijn) niet noodzakelijk. 20Face heeft zelfs de ambitie om de toegang zo soepel mogelijk te maken. De gebruiker zou zich niet hoeven aan te passen aan het systeem, door stil te staan of in een camera te kijken. Hij of zij zou gewoon direct moeten kunnen doorlopen.[120] Het vergroten van gemak en efficiëntie zijn hierbij het streven. Afhankelijk van hoe het systeem geplaatst wordt zou dat kunnen betekenen dat van iedere bezoeker een gezichtstemplate wordt gecreëerd.

Tijdens de discussie over gezichtsherkenningstechnologie voor toegangscontrole bij evenementen in de expertworkshop, wezen de experts erop dat indien de technologie op grotere

[120] 20Face 'Facial Recognition Technology: Challenges and Opportunities' Whitepaper` (2019).

schaal wordt gebruikt, het risico groter is dat mensen zich genoodzaakt zien om gezichtsherkenning toe te staan om op die manier sneller binnen te komen en lange rijen te vermijden. Bovendien kan het leiden tot stigmatisering van personen die weigeren deel te nemen. De aanwezigheid van camera's kan het gedrag van mensen op den duur ook beïnvloeden. Mensen zouden evenementen kunnen gaan vermijden vanwege de aanwezigheid van camera's uitgerust met gezichtsherkenningsfunctionaliteit. En hoewel de evenement-organisatoren en leveranciers die wij spraken zich zeer bewust tonen van de noodzaak om altijd een keuze te bieden (wel of geen gezichtsherkenning) is er natuurlijk ook het commercieel belang om zo veel mogelijk mensen richting de optie gezichtsherkenning te bewegen.

Informatieverwerking

Beide bedrijven geven aan zich bewust te zijn van mogelijke privacyrisico's bij het verwerken van data. Ze hebben verschillende maatregelen genomen om de data veilig op te slaan en enig inzicht te houden in het gebruik van data. De dienstverlening van Zenus richt zich op identificatie en *analytics*. Identificatie is redelijk eenduidig. Op basis van een zelf geüploade foto wordt een bezoeker herkend en krijgt vervolgens het toegangsbewijs uitgereikt. Het risico dat persoonsgegevens worden gebruikt voor doeleinden waar de persoon geen toestemming voor heeft gegeven wordt beperkt doordat Zenus geen foto's bewaart en ook het template uiteindelijk wordt vernietigd. Het wordt verder niet gebruikt voor andere evenementen of doorverkocht. Voor de Horecava test werden er wel foto's op de badges geprint. Pim Schoonderwoerd van de RAI legt uit dat bij Horecava men een kaartje moet kopen wanneer men niet is uitgenodigd en met foto's op de badges de controle hierop omhooggaat:[121]

> *"Een van de wensen vanuit de organisatie was om efficiënter aan toegangscontrole te kunnen doen. Gezichtsherkenning kan daarbij helpen. Het is dan niet meer mogelijk om je badge door te geven of te verkopen aan iemand anders. Zonder foto kan dit wel en verlies je omzet en ontstaan vervuilde data."*

Het identificatieproces bij 20Face loopt iets anders dan bij Zenus. 20Face slaat zelf geen persoonlijke data op. In de huidige proefopstellingen beheert een klant –bijvoorbeeld een evenementlocatie– de data van bezoekers op (o.a. naam, gezichtstemplate, abonnementsdata). De herkenning kan ter plekke op een lokale server worden uitgevoerd, of in de cloud. In het nieuwe ecosysteem worden biometrische profielen opgeslagen in datakluizen op een server in Nederland of op een mobiele telefoon. De verwerking van data kan dus op meerdere plekken plaatsvinden, maar als een persoon eenmaal is ingeschreven dan is een verdere opslag van foto's van gezichten

[121] Citaten zijn geredigeerd met het oog op leesbaarheid.

niet meer nodig. Alleen het biometrisch profiel en een gezichtstemplate zijn nodig. Voor het gebruik van het 20Face systeem hoeft dan geen pas te worden gebruikt. Het idee hier is dat uitsluitend de bezoeker toestemming kan geven voor het gebruik van zijn of haar data en overzicht kan houden op wanneer het template gebruikt wordt en door welke camera of welk end-point.

Het is niet altijd direct duidelijk wie de verwerkingsverantwoordelijke of de verwerker is bij de geïntegreerde systemen die 20Face levert. In sommige samenwerkingsverbanden is via individuele contracten geregeld dat 20Face de verwerker is en hun businesspartners/klanten de verwerkingsverantwoordelijke.[122] Het verhaal wordt ingewikkelder op het moment dat de gebruiker zelf zijn of haar data beheert. 20Face gaat ervan uit dat de bezoeker dan de verwerkingsverantwoordelijke is.

Het risico van *aggregatie* en *secundair gebruik* bij beide bedrijven, als het gaat om identificatie, lijkt niet heel groot. Bij het analytics gedeelte van Zenus –dat nu nog in ontwikkeling is– kan het echter ingewikkelder worden omdat het vaak het bijeenbrengen van verscheidene datastromen betreft. In het interview met Zenus wordt benadrukt dat het analytics gedeelte altijd op geaggregeerd niveau plaatsvindt. Daarmee wordt bedoeld dat het niet zozeer gaat om het in kaart brengen van hoe één bepaalde bezoeker zich gedraagt, maar hoe een groep bezoekers zich gedraagt. Bijvoorbeeld '75% van de bezoekers aan stand A bleven minder dan 5 minuten'. Deze statistiek kan vervolgens worden afgezet tegenover de uitkomst bij een andere stand. Op basis van zulke statistieken kunnen dan bepaalde beslissingen worden genomen, bijvoorbeeld over de prijs van een bepaalde standplaats, of de investering voldoende oplevert. In combinatie met demografische analyses, kunnen deze resultaten verder worden verfijnd. Bijvoorbeeld: '75% van de bezoekers aan stand A bleven minder dan 5 minuten. 80% van deze bezoekers was vrouw, 20% was man'. Of '34% van deze bezoekers werkt in de publieke sector, 54% van deze bezoekers werkt in de private sector, 12% is werkzoekende'. Met andere woorden, de analyses die mogelijk worden gemaakt door de gezichtsherkenning, draaien volgens Zenus niet om het individu maar om de groep en daarmee worden privacyrisico's voor het individu geminimaliseerd.

Of zoals Zenus CEO Panos Moutafis het verwoordt: "…het maakt ons niet uit wie je bent, het gaat ons niet om het individu, het gaat ons om hoe die aggregeren, dus om de statistieken…"[123] Dit geldt volgens Moutafis ook voor emotie-analyse, die hij bestempelt als "op zichzelf één van de minst invasieve toepassingen". "Zolang je emotie-analyse uitvoert zonder ook andere *identifiers* te betrekken", zo stelt Moutafis, "dan valt de analyse niet te herleiden tot het individu. Een emotie is geen *identifier*."

Schoonderwoerd heeft geen test gedaan met emotie-herkenning maar ziet wel mogelijkheden voor de evenementenorganisatie: "Stel we hebben een sessie gehad van een bepaalde spreker, als het mogelijk zou zijn zouden we kunnen kijken naar wat de gemiddelde emotie was van de mensen in de zaal of wanneer zij de zaal uit komen." Maar, zo stelt hij:

[122] Interview met Anne Alicia Kier van 20Face.
[123] Alle citaten uit interviews die in het Engels hebben plaatsgevonden zijn vertaald naar het Nederlands door de auteurs.

“Sommige mensen zullen misschien anoniem over een beurs willen wandelen. Wij moeten wel in staat zijn om deze keuze te bieden.” Ook de CTO van Zenus Rakshak Talwar nuanceert het risico van emotieherkenning. “Misbruik is alleen mogelijk wanneer je de emotie-herkenning koppelt aan een andere database die bijvoorbeeld bijhoudt wie wanneer welke emotie vertoont, maar dat is niet iets wat Zenus doet”, vertelt hij. “Er wordt alleen op geaggregeerd niveau emotie-analyse uitgevoerd”.

Zoals uit het bovenstaande blijkt hebben Zenus en 20Face maatregelen getroffen om de risico’s *identificatie*, *aggregatie, secundair gebruik* en *onveiligheid* te beperken. Deze maatregelen zijn echter wel in hoge mate afhankelijk van de houding van het bedrijf. Bovendien liggen er ook nog andere privacyrisico’s op de loer, zoals het risico van uitsluiting. De systemen werken niet altijd en sommige mensen zullen minder snel herkend worden met als risico dat een bezoeker ten onrechte wordt buitengesloten. Zeker als de modellen niet goed om kunnen gaan met verschillende etniciteiten, afwijkingen of seksen kan dit een stigmatiserend effect hebben. Ook hier is het daarom van belang dat er altijd een terugval mogelijkheid is om bezoekers bij falende gezichtsherkenningstechnologie alsnog te registreren. De experts uit de expertworkshops wezen er ook op dat voor mensen die vaak niet worden herkend door de systemen dit een belemmering kan zijn en ook hier weer tot stigmatisering kan leiden.

Ook de emotieanalyse kan privacyrisico’s met zich meebrengen als het gaat om uitsluiting of gedragsbeïnvloeding. De classificatie op basis van emoties en de daaraan gekoppelde services kunnen het gedrag van mensen beïnvloeden als dat leidt tot toegang tot services. Bijvoorbeeld als aanbiedingen of interacties afgestemd worden op de automatisch waargenomen emoties, kunnen mensen hun gedrag daarop aanpassen of juist wegblijven.

Informatieverspreiding en overschrijding

Op het gebied van informatieverspreiding en overschrijding kwamen wij een aantal activiteiten tegen die mogelijk een risico vormen voor de privacy van burgers. Sommige subcategorieën van deze twee categorieën van Solove’s taxonomie waren minder duidelijk aanwezig in de verkenning, zoals afpersing en toe-eigenen, en zullen wij dan ook hier niet bespreken.

Bij beide bedrijven is *vertrouwen* in een goed gebruik van gezichtsherkenning een belangrijk thema. Volgens de CEO van 20Face, Tauseef Ali, kan gezichtsherkenning veel dingen makkelijker maken, zoals het openen van een auto, het betalen van een kopje koffie of toegang krijgen tot een kantoor, maar is er nog een groot wantrouwen bij het publiek. Hij merkt op: “Gezichtsherkenning is op de een of andere manier, vanuit een privacy of sociaal oogpunt niet echt acceptabel”. Om het privacy probleem op te lossen en het vertrouwen te vergroten richt 20Face zich volgens de CTO op wat ze bij het bedrijf zien als drie aspecten van vertrouwen: beveiliging, transparantie, en controle.

Het bedrijf stelt veel aandacht te hebben besteed aan een veilige opslag van gegevens door encryptie en decentrale systemen. Door gebruikers inzicht te geven in wat er met hun data

gebeurt –welke partij vraagt wanneer toegang tot een biometrisch profiel- wil het bedrijf de transparantie van het ecosysteem waarborgen. Zo moet het duidelijk zijn voor de gebruiker wanneer identificatie plaatsvindt door bijvoorbeeld een tijdlijnoverzicht in een mobiele app. De gebruiker kan dan nagaan op welke plekken en wanneer identificatie heeft plaatsgevonden. Bovendien moeten gebruikers volledige controle hebben over hun profiel. Ze moeten zichzelf aan -en af kunnen melden, gegevens in hun profiel kunnen veranderen en zelf de toegang tot de data kunnen beheren door expliciet toestemming te geven of in te trekken voor het gebruik van hun gegevens.

Het risico op *onthulling* en *blootstelling* lijkt op deze manier technisch beperkt. Het gebruik van gegevens zou in principe alleen kunnen gebeuren met expliciete toestemming van de gebruiker. De toekomstige blockchain van 20Face legt deze restrictie bovendien vast in de technologie. Echter, in de huidige proefopstellingen die nog geen gebruik maken van een persoonlijke datakluis, is de toegang tot data gebaseerd op contractuele afspraken tussen de samenwerkende partners.

Vertrouwen van evenementorganisatoren en bezoekers in hun product is ook cruciaal voor Zenus. Om dit vertrouwen te creëren worden privacy en transparantie als twee belangrijke pijlers van het bedrijf benoemd. Zenus verzamelt zo min mogelijk persoonlijke informatie en heeft ook expliciet opgenomen in haar privacy policy dat klanten geen informatie zoals naam van de bezoeker, contact informatie en dergelijke met hen mogen delen.[124] Informatie die men niet bezit, kan men ook niet delen of verliezen.

Moutafis geeft aan dat voor hen niet alleen hun eigen reputatie op het spel staat, maar ook die van de biometrische technologie zelf en van de evenementenindustrie als geheel. “Zeker in de tijd dat gezichtsherkenning nog in de kinderschoenen stond, was er een mismatch tussen wat mensen verwachtten en de feitelijke accuratesse van de technologie. Dit schaadde de markt.” Ook Pim Schoonderwoerd onderschrijft het belang van reputatie in deze nieuwe ontwikkelingen en de RAI ziet hier ook een rol voor zichzelf als expert in evenement-organisatie:

> *“Veel van onze gasten organiseren grote events. Zij hebben daarmee ook een redelijk hoge exposure. Alles wat schade kan berokkenen aan hun evenement is iets dat ze niet willen. De AVG is ook voor hen ook een onderwerp waaraan veel aandacht besteed wordt, zeker in relatie tot registratie. Als met de registratiegegevens iets misgaat kan dat grote impact hebben voor het evenement en de uitstraling. De impact kan dus groot zijn.”*

[124] <www.zenus-biometrics.com/privacy-security> geraadpleegd 30 juli 2019.

De dienstverlening zoals Zenus die voor ogen heeft is om gezichtsherkenning in te zetten ten dienste van de interpersoonlijke relatie en vooral niet om deze te domineren of over te nemen (*intrusie*). Met het huidige aanbod van snelle check-in en *basic analytics* lijkt dit ook niet aan de orde. Wel is het de vraag of dit nog steeds zo blijft wanneer emotiedetectie wordt ingezet. In het fictieve voorbeeld dat een bezoeker ervoor kiest om niet de werkelijke reden voor zijn of haar desinteresse in een bepaald product te delen met een standhouder, zou dit via gezichtsherkenning alsnog achterhaald kunnen worden. In die zin zorgt emotiedetectie ervoor dat informatie die eerst onbereikbaar was toch toegankelijk is voor derden. Zelfs wanneer de analyse op geaggregeerd niveau plaatsvindt, kan het argument gemaakt worden dat dit toch een vorm van *onthulling* is en deels ook impact kan hebben op de keuzes die mensen maken over wat ze al dan niet willen delen met anderen (*inmenging in besluitvorming)*.

4.1.4. **Best practices**

Bedrijfswaarden

Als start-up heeft Zenus ervoor gekozen om privacy en transparantie als uitgangspunten te nemen voor de opbouw van hun bedrijf. De drie kernwaarden op basis waarvan ze opereren: bescherm mensen hun privacy, wees radicaal eerlijk en doe dingen op een goede manier. Gevraagd naar de motivatie hiertoe geven Moutafis en Talwar aan geleerd te hebben van de eerdere introducties van technologieën waar regulering nog veel minder aan de orde was en privacy-inbreuken nu veel vaker voorkomen. Ze zijn ervan overtuigd dat privacy een cruciale waarde is voor hun domein en dat het beschermen van privacy noodzakelijk is om het vertrouwen van klanten en bezoekers te krijgen en behouden.

> *"Sinds we het bedrijf hebben opgericht, ongeveer drie jaar geleden, is er een steeds grotere nadruk komen te liggen op privacy in het technologische landschap. Dus ik denk dat dit belang in de toekomst nog verder zal toenemen. Ik denk dat het zal helpen ons te positioneren als pionier en dat het bijdraagt aan het vergroten van vertrouwen. Wij hebben het geluk gehad dat we vanaf het begin al het vertrouwen hadden van veel mensen. Wij hadden geen hele hoge opt-in aantallen verwacht toen we begonnen, maar dat kregen we wel. En dat had veel te maken, denk ik, met onze duidelijke boodschap en uitleg over hoe data gebruikt worden." (Rakshak Talwar, CTO Zenus)*[125]

[125] Uit het Engels vertaald door de auteurs.

Zenus ziet het ook als hun verantwoordelijkheid om kennis te delen over gezichtsherkenning en hoe het goed te gebruiken. Dit doen ze op verschillende manieren. Zo publiceren ze geregeld blogs[126] en case-studies[127], hebben ze een gids met info over gezichtsherkenning gepubliceerd[128], en nemen deel aan publieke bijeenkomsten. Zenus's stelt dat hun businessmodel dan ook uitdrukkelijk niet bestaat uit het op enige manier te gelde maken van verzamelde gegevens. Ze geven aan dat gegevens niet worden verkocht aan derden. Hun inkomsten bestaan uit het leveren van de gezichtsherkenningsservice en wordt medebepaald door de omvang van het evenement: hoe meer mensen zich aanmelden, hoe groter de omzet.

Het oorspronkelijk doel van 20Face was om alleen gezichtsherkenningssoftware te verkopen aan bedrijven. Deze zouden het dan kunnen integreren in bestaande of te ontwikkelen systemen. Maar net als bij Zenus, groeide het besef dat het waarborgen van privacy een voorwaarde is voor de acceptatie van de technologie:

> *"We wilden gespecialiseerd zijn in het direct en naadloos identificeren van mensen. Dus, je hoeft niet te stoppen en te kijken in de camera of op een scherm, je kan gewoon simpelweg binnenlopen op weg naar huis, in een gebouw, en dan ben je herkend. Dat levert veel gemak op. Maar deze naadloze en directe gezichtsherkenningstechnologie… het was heel mooi vanuit een technisch oogpunt, maar veel mensen waren erg bezorgd over privacy." (Tauseef Ali, CTO 20Face)*[129]

Twee jaar geleden heeft het bedrijf daarom besloten om zich vooral te richten op de ontwikkeling van volledige systemen - of ecosystemen zoals het bedrijf het zelf noemt - waarin het waarborgen van privacy een centrale doelstelling is.

Privacy-by-design

Privacybescherming is ook het uitgangspunt voor het ontwerp van het systeem van Zenus. Zo verklaart Zenus als standaard de meest strikte privacyvereisten te handhaven. Ter illustratie vertelt Moutafis dat in sommige staten in de Verenigde Staten toestemming niet opt-in hoeft te zijn maar bijvoorbeeld ook via reeds aangevinkte opties kan. Maar Zenus kiest er desalniettemin voor om toestemming altijd als een opt-in keuze te geven (zoals dit in de EU het geval is), dus ook als dat wettelijk niet is vereist. Deze strikte visie op privacystandaarden zorgde er volgens Moutafis mede

[126] Bel Booker, 'How Your Face Will Become Your Ticket to Event Success' (2018) Eventbrite </www.eventbrite.co.uk/blog/facial-recognition-tech-for-events-ds0c/> geraadpleegd 31 juli 2019.
[127] Zenus, 'Streamlining Registration At Large Events With Face Recognition [Case Study]' (2019) Event <www.eventmanagerblog.com/face-recognition-case-study> geraadpleegd t 31 juli 2019.
[128] Zenus, 'Facial Recognition and Events: A Comprehensive Guide (2018)' (2018) Event <www.eventmanagerblog.com/facial-recognition-guide-2018> geraadpleegd 24 juli 2019.
[129] Uit het Engels vertaald door de auteurs.

voor dat “toen de Algemene Verordening Gegevensbescherming in werking trad, dit voor ons prima was, alle zaken waren eigenlijk al bijna helemaal op orde”. Moutafis schat in dat 50% van hun klanten uit Europa komt. Wanneer gevraagd of privacy hun bedrijf een marktvoordeel biedt, antwoordt Moutafis: “ik denk van wel. En als het niet zo is, dan zou het dat eigenlijk moeten doen”.

20Face beschermt gegevens op verschillende manieren, waarbij ze inzetten op privacy-by-design methodes. Zo stellen zij dat het mogelijk is om gezichtsherkenning uit te voeren zonder foto’s van personen te bewaren. Per persoon wordt alleen een template opgeslagen, een reeks nummers die het profiel bevat van het gezicht van de person in kwestie. De foto wordt vervolgens verwijderd. De template wordt beveiligd (versleuteld) opgeslagen. De template kan niet worden terug herleid naar een persoon. Door middel van de decentrale opslag van biometrische profielen in persoonlijke datakluizen wil het bedrijf privacyrisico’s zoals aggregatie en ongeoorloofd secundair gebruik tegengaan.

Businessmodel

Zenus kiest voor een businessmodel dat niet afhankelijk is van het verkopen van data en distantieert zich van bedrijven die dat wel doen. Dit heeft ook gevolgen voor de samenwerkingen die ze aangaan. Zo hebben ze opgenomen in hun privacy policy dat bedrijven die met hen samen willen werken alleen gezichtsherkenning als optie mogen inzetten en altijd om de uitdrukkelijke toestemming van bezoekers moeten vragen.[130] Om ervoor te zorgen dat dit niet louter een papieren werkelijkheid is, werken ze ook op het vlak van het verkrijgen van de toestemming en de afbeelding samen met de evenement-organisator. Met bedrijven die zich hier niet aan willen committeren, wordt niet samengewerkt.

“Het verschil tussen ons en sommige andere bedrijven die gratis services bieden, is dat hun doel is om geld te verdienen met jouw data en dan ben jij het product. Dat is helemaal niet het geval bij ons. Wij verdienen geen geld met andermans data.” (Rakshak Talwar, CTO Zenus)[131]

Ook 20Face kiest voor een businessmodel dat geen gratis services aanbiedt in ruil voor data. Het uitgangspunt bij 20Face is dat de gebruiker controle houdt over het proces en haar data. Het bedrijf heeft voor een businessmodel gekozen waarbij de gebruiker betaalt voor het beheer van zijn of haar data:

[130] <zenus-biometrics.com/privacy-security> geraadpleegd 31 juli 2019.
[131] Uit het Engels vertaald door de auteurs.

"Mensen hebben soms een probleem met bedrijven vertrouwen met hun data. En wij ontwerpen systemen om hier antwoord op te geven. Wij zijn een systeem aan het ontwerpen waarbij jij betaalt voor je privacy. Dus, mensen moeten ervoor betalen. Voor elk biometrisch profiel geldt dan dat mensen hun eigen ruimte zullen moeten kopen, ongeveer 10 euro per jaar of 15 euro. Daarna is de belofte dat wij de data niet verkopen." (Tausseef Ali, CTO 20Face)[132]

Bedrijven die op hun beurt gebruik willen maken van gezichtsherkenning voor toegangscontrole betalen dan voor de integratie en het gebruik van het platform.

Gevraagd of het bedrijf de gezichtsherkenningstechnologie ook apart verkoopt aan bedrijven, dus los van het 'privacy-proof platform', antwoordt de CTO van 20Face dat ze ervoor gekozen hebben om dat niet te doen. Bovendien verkoopt het deze systemen direct aan de gebruiker en werkt het bedrijf alleen met geselecteerde partners die privacy ook centraal stellen. Het bedrijf zegt zo de zorgen over privacy en mogelijk misbruik van de software beter te kunnen adresseren.

"Waar wij ons als bedrijf op positioneren of plaatsen in de markt is dat wij de technologie, de techniek, niet apart verkopen. Wanneer andere mensen hun oplossing op onze techniek bouwen, weten wij niet wat voor oplossing zij bouwen en of die privacy proof zijn; of deze GDPR proof zijn of waarvoor zij de applicatie hebben. Het is Artificiële Intelligentie. De technologie kan mensen identificeren. Wij kunnen dat niet zomaar aan iedereen verkopen. Het biedt mensen mogelijkheden en als zij de technologie op de juiste manier gebruiken is dat goed, maar wij willen zeker weten dat de partijen die het gebruiken het op de juist manier gebruiken." (Tauseef Ali, CTO 20Face)[133]

Wetgeving en beleid

Wetgeving en beleid hebben een sturende werking op bedrijven en bij beide speelt privacywetgeving een grote rol. 20Face opereert voornamelijk in een Europese context en wordt daarbij sterk geleid door de AVG en ook voor Zenus is de AVG, naast de verschillende Amerikaanse federale wetten en staatswetten die betrekking hebben op privacy en gegevensbescherming, leidend. Gevraagd naar wat Zenus en 20Face nodig zouden hebben om

[132] Uit het Engels vertaald door de auteurs.
[133] Uit het Engels vertaald door de auteurs.

privacy te beschermen vanuit wetgeving en beleid, komen vier zaken nadrukkelijk aan bod: certificering, sectorspecifieke richtlijnen, proactieve handhaving en regulering via de technologie.

Certificering is vooral een aandachtspunt bij Zenus. Het bedrijf ziet certificering als een manier om aan de buitenwereld op een transparante wijze te tonen dat het bedrijf zich committeert aan bepaalde technische en juridische standaarden en daarop aanspreekbaar is. Aangezien veel evenement-organisatoren niet gewend zijn om met gezichtsherkenning te werken en/of niet de nodige juridische en technische kennis in huis hebben om een potentiële gezichtsherkenningspartner goed te beoordelen, zou certificering vanuit een betrouwbare, derde partij dit probleem deels kunnen verhelpen.

Sectorspecifieke richtlijnen zouden dan weer bij kunnen dragen aan het verlagen van de administratieve druk die nu –met name onder invloed van de AVG– als enorm toegenomen wordt ervaren door Zenus. Het ontwikkelen van specifieke checklists voor het domein van de evenement-organisatie zou hier een uitkomst bieden. Met name voor kleine bedrijven en start-ups is dit belangrijk, omdat zij niet altijd toegang hebben tot uitgebreid juridisch advies.

Volgens de DPO van 20Face is het een uitdaging om inzicht krijgen in wat is toegestaan volgens de AVG. Het bedrijft kan terecht voor advies bij verschillende organisaties, zoals de Autoriteit Persoonsgegevens en een juridisch bureau dat is aangesloten bij de Universiteit Twente om start-ups te adviseren over relevante wetgeving. Toch wijst de DPO erop dat zulk advies niet voor alle kleine bedrijven makkelijk voor handen is:

> *"Er zijn veel kleine bedrijven die worden geleid door mensen die geen achtergrond hebben in rechten en ook, tot op zeker hoogte, niet de optie hebben om juridische adviseurs in te schakelen of om iemand in te huren die meer weet hierover. Dus dan is het makkelijker voor hen en voor mij om het uitgelegd te krijgen in leken termen" (Anna Alicia Kier, DPO 20Face)*[134]

Zenus en 20Face zijn voorstanders van actieve handhaving. In een opkomend domein is het belangrijk dat spelers die het niet zo nauw nemen met de (privacy)regels daarvoor beboet worden. Dit bezorgt het domein en gezichtsherkenning namelijk een slechte naam en kan een negatieve impact hebben op innovatie en het vertrouwen van klanten. Handhaving levert wel een uitdaging, merkt de DPO van 20Face op, omdat het voor gebruikers en anderen niet gemakkelijk is te achterhalen of privacy- en gegevensbeschermingsregels worden nageleefd. Naar mate gezichtsherkenningssystemen op grotere schaal gebruikt gaan worden zal deze uitdaging alleen maar toenemen.

[134] Uit het Engels vertaald door de auteurs.

Tot slot, moet er ook aandacht zijn voor technische oplossingen. Volgens Ali kunnen wij niet alles aan handhaving van de wettelijk kaders overlaten en moet technologie ontwikkeld worden om privacy te waarborgen; privacyregulering moet in de architectuur van een systeem worden gebouwd. Het systeem moet het moeilijk, zo niet onmogelijk maken om tegen wetgeving in te gaan.

"Een betere keus is om het in het ontwerp, de architectuur van het systeem te stoppen. Dus de administratie of mensen die het system controleren, zelfs zij zouden niet dingen moeten kunnen doen die niet stroken met de GDPR of privacy. Omdat het systeem zo ontworpen en geautomatiseerd is dat het mensen niet toe staat met de regels te knoeien. Dus, dat is wat wij proberen, om regulering in de architectuur van het systeem te stoppen." (Tausseef Ali, CTO 20Face) [135]

4.2. Smartphone apps

De tweede toepassing die wij onder de loep nemen betreffen smartphone apps met gezichtsherkenning. Meer dan 90% van de Nederlanders bezit een mobiele telefoon of smartphone [136] en meer dan 80% gebruikt deze om zich op sociale media platformen te begeven.[137] Gezichtsherkenning als manier om de telefoon te ontgrendelen is reeds wijdverbreid. De rekenkracht en connectiviteit van deze smartphones maakt het echter ook mogelijk om gezichtsherkenning toe te voegen aan bestaande applicaties en nieuwe smartphone applicaties te ontwikkelen. Tech bedrijven zoals IBM, Microsoft en Amazon leveren hiervoor API's (Application Program Interfaces) en cloud services die app ontwikkelaars vervolgens kunnen integreren in hun software. Deze applicaties worden niet alleen gebruikt op sociale media platformen, maar worden ook steeds vaker ingezet door bedrijven en instanties op de werkvloer of om de interactie met klanten te ondersteunen.

Zo is er in het sociale verkeer de emotieherkenningstoepassing *Emoticonar*, een applicatie die toegevoegd kan worden aan de populaire berichtendienst Messenger. Deze app detecteert op een foto hoe iemand zich voelt en voegt daar automatisch de corresponderende emoticon aan

---

[135] Uit het Engels vertaald door de auteurs.
[136] 'Smartphonebezit gegroeid naar 93% van Nederlanders, veelvuldig gebruik storend' (2018) Consultancy.nl <www.consultancy.nl/nieuws/15292/smartphonebezit-gegroeid-naar-93-van-nederlanders-veelvuldig-gebruik-storend> geraadpleegd 2 augustus 2019;
https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/technology-media-telecommunications/2017%20GMCS%20Dutch%20Edition.pdf; geraadpleegd 17 februari 2020.
<https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?ts=1564740480460> geraadpleegd 2 augustus 2019.
[137] <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?ts=1564740480460> geraadpleegd 2 augustus 2019.

toe.[138] *Logme* is een zoekmachine gebaseerd op gezichten.[139] Leden van de Logme Community kunnen foto's uploaden en gebaseerd op gelijkenissen andere foto's bekijken. Er wordt aan de mogelijkheid gewerkt om vervolgens direct contact op te nemen met andere leden die bijvoorbeeld gelijkende foto's geüploade hebben.[140] De app *Face Secret* belooft te laten zien hoe men veroudert. Ook is er de mogelijkheid om etniciteit te analyseren en te voorspellen hoe iemands baby eruit komt te zien.[141]

Ook voor instanties en bedrijven worden gezichtsherkenningsapps ontwikkeld. *FacePhi* ontwikkelt een gezichtsherkenningsapplicatie voor de bankensector die ingezet kan worden voor identiteitscontrole bij bijvoorbeeld online bankieren om zo fraude tegen te gaan.[142] *Railer* is een gezichtsherkenningsapp die door bedrijven ingezet kan worden om de aan -en afwezigheid van hun personeel te registreren en monitoren.[143]

Op het terrein van health-apps voor niet-professioneel gebruik zien wij ook interessante gezichtstechnologie-ontwikkelingen. Zo zijn er verschillende apps beschikbaar die zijn bedoeld voor slechtzienden om omgevingen, objecten, teksten en mensen 'zichtbaar' te maken, zoals Seeing AI en Envisioning AI.[144] Ook Facebook ontwikkelt een toepassing voor slechtzienden bedoeld ter ondersteuning van de interactie met Facebook Messenger. Deze app kan bekenden herkennen (op basis van getagde foto's van Facebook vrienden) en gezichtsexpressie en -kenmerken aflezen. Een andere toepassing van gezichtsherkenning is het ondersteunen van mensen met geheugenverlies. De enige commercieel verkrijgbare app die wij hiervoor tegen kwamen is de relatieve nieuwe *Timeless.care*.[145] Wel lopen er diverse onderzoeksprojecten die toepassingen op dit gebied onderzoeken. Een voorbeeld van een dergelijk experimentele toepassing is *SocioGlass.* Dit is een applicatie voor GoogleGlass die in combinatie met een mobiele telefoon slechtzienden en mensen met geheugenverlies kan ondersteunen in sociale interacties onder andere door middel van gezichtsherkenning.[146] Een ander voorbeeld is de open-source Personalized Active Learner, een draagbaar systeem dat verschillende functionaliteiten biedt waaronder gezichtsgebaseerde geheugenondersteuning.[147] Deze toepassingen zijn momenteel nog in een experimentele fase.

---

[138] <www.apkpure.com/emoticonar-for-messenger/com.qualcomm.emotionar> geraadpleegd 2 augustus 2019.
[139] <https://play.google.com/store/apps/details?id=com.facequare.mob> geraadpleegd 2 augustus 2019.
[140] <https://play.google.com/store/apps/details?id=com.facequare.mob> geraadpleegd op 2 augustus 2019.
[141] <https://play.google.com/store/apps/details?id=faceapp.facereading.horoscope.zodica.signs.astrology&hl=en_US> geraadpleegd op 2 augustus 2019.
[142] <www.facephi.com/en/content/banks/> geraadpleegd 2 augustus 2019.
[143] <https://play.google.com/store/apps/details?id=com.facequare.mob> geraadpleegd 2 augustus 2019.
[144] Other apps and appliances <www.orcam.com/en/myeye2/> (camera that can be mounted on a pair of glasses with app).
[145] Voor het eerste aangeboden in 2019 en momenteel alleen beschikbaar in de V.S.
[146] Qianli Xu e.a., 'SocioGlass: Social Interaction Assistance with Face Recognition on Google Glass' (2016) 2 Scientific Phone Apps and Mobile Devices.
[147] Mina Khan e.a., 'PAL: A Wearable Platform for Real-time, Personalized and Context-Aware Health and Cognition Support' (2019) arXiv:1905.01352.

Hoewel het merendeel van de smartphone applicaties dus nog in de kinderschoenen staan en –afgaand op sommige gebruikersreviews[148]– nog zeker niet al hun beloftes waarmaken of uitblinken in gebruikersgemak, geeft deze eerste generatie gezichtsherkenningsapps wel een idee van wat wij in de toekomst kunnen verwachten. Voor de onderstaande verkenning van de ontwikkeling van gezichtsherkenning in smartphone-apps hebben wij gekeken naar Facebook's gebruik van gezichtsherkenningstechnologie, Microsoft 's Seeing AI, Microsoft's Face API, en Amazon's Rekognition. Wij hebben gesproken met Microsoft NL (leverancier van gezichtstherkenningstechnologie) en Facebook, Inc. (social media platform met gezichtsherkenningsfuncties). Ook hebben wij zelf onderzocht in welke mate het mogelijk is om als individu met beperkte technische en financiële capaciteiten gezichtsherkenningstechnologie toe te passen. Hierbij hebben wij gebruik gemaakt van Amazon's Rekognition.

4.2.1. **Gezichtsherkenningstechnologie**

Bij gezichtsherkenning in smartphone apps is het belangrijk om verschillende varianten te onderscheiden aangezien die elk gepaard gaan met specifieke privacyrisico's. Wij benoemen er vier: gezichtsherkenningstechnologie die bedrijven zowel ontwikkelen alsook zelf inzetten (1), smartphone apps met gezichtsherkenningstechnologie die door bedrijven op de markt zijn gebracht en die burgers naar eigen inzicht kunnen gebruiken (2), leveranciers van gezichtsherkenningsdiensten voor de zakelijke markt (3), en gezichtsherkenningsdiensten die burgers kunnen gebruiken om hun eigen app te ontwikkelen (4). De eerste variant is dus wanneer gezichtsherkenningstechnologie ontwikkeld en ingezet wordt door één en hetzelfde bedrijf. Tot die eerste categorie behoort Facebook. Met 2,4 miljard gebruikers wereldwijd die maandelijks inloggen op het sociale netwerk, is Facebook het grootste sociale media platform wereldwijd.[149] Sociale media apps behoren tot de meest populaire apps en Facebook staat hierbij ook op nummer één, gevolgd door Whatsapp en Facebook Messenger (welke ook tot het Facebook imperium behoren).[150]

Gezichtsherkenning wordt ingezet om Facebookgebruikers te herkennen in foto's en (live)video's die op het platform worden gedeeld. Aan gebruikers die de instelling voor gezichtsherkenning hebben ingeschakeld, laat Facebook weten dat ze in een bepaalde video of op een bepaalde foto voorkomen, ook als ze niet *getagd*[151] zijn. Deze foto's kunnen dan door de

[148] Gebruikersreviews: <play.google.com/store/apps/details?id=com.facequare.mob&hl=en>; <apps.apple.com/us/app/timeless-care/id1439644684> geraadpleegd op 17 februari 2020.
[149] Facebook, 'Facebook Q2 2019 Results' (2019) <https://s21.q4cdn.com/399680738/files/doc_financials/2019/Q2/Q2-2019-Earnings-Presentation-07.24.2019.pdf> geraadpleegd 14 oktober 2019.
[150] Mansoor Iqbal, 'App Download and Usage Statistics (2019)' (2019) <www.businessofapps.com/data/app-statistics/> geraadpleegd 18 oktober 2019.
[151] Gebruikers kunnen aangeven wie in een bepaalde video of foto voorkomt door de naam van die persoon toe te voegen. Dit wordt "taggen' genoemd. Door een naam van een persoon aan een foto of video toe te voegen kan deze bijvoorbeeld gezien worden door vrienden van de persoon die getagd is (dit is afhankelijk van de privacy-instellingen van de getagde persoon).

persoon in kwestie gecontroleerd worden. Gezichtsherkenning maakt het ook mogelijk suggesties te doen voor het *taggen* zelf. Wanneer gebruikers iemand *taggen* kan de persoon in kwestie vervolgens deze foto's en video's controleren alvorens ze op zijn of haar tijdlijn worden geplaatst, mits de instelling *Controle voor tijdlijn* is ingeschakeld.[152] Facebook koppelt het gebruik van gezichtsherkenning ook nadrukkelijk aan het voorkomen van ongewenste imitatie en identiteitsmisbruik. Wanneer iemand de foto van een ander gebruikt als profielfoto, laat Facebook dit weten aan de persoon in kwestie. Door gezichtsherkenning in te schakelen zou de betrouwbaarheid van het platform worden vergroot.[153] Ten slotte wordt gezichtsherkenning op Facebook ook ingezet voor gebruikers met een visuele beperking. Wanneer de gezichtsherkenningsfunctie is ingeschakeld wordt aan hen verteld welke personen op een foto staan.

De tweede variant betreft smartphone apps met gezichtsherkenning ontwikkeld door bedrijven die burgers naar eigen inzicht kunnen gebruiken. De app Seeing AI valt in deze categorie. Deze gratis app is ontwikkeld door Microsoft voor slechtzienden.[154] De app heeft verschillende functionaliteiten, zoals tekst naar spraak, audio begeleiding, barcodes scanning, beschrijving van de omgeving, kleurherkenning en ook het herkennen van bekende gezichten. Naast het identificeren van bekende gezichten kan de app ook de gezichtsexpressies en een aantal andere kenmerken afleiden, zoals sekse en leeftijd.

Om een persoon te herkennen moet de eigenaar van de mobiele telefoon de gezichtsherkenning functie ('person mode') selecteren. De default camera is de camera aan de voorkant van de telefoon, zodat de persoon die gefotografeerd wordt een 'selfie' kan maken. De camera aan de achterkant van de telefoon kan wel geselecteerd worden. Wanneer de camera op een of meerdere personen wordt gericht, detecteert de app de gezichten in het beeld een geeft een verbale beschrijving van waar in het beeld de gezichten zich bevinden en wat de afstand tot de camera is. Er kan dan een foto genomen worden. Als de persoon reeds bekend is – in de database staat – dan kan de app de persoon herkennen. Als de persoon nog niet bekend is, dan kan hij of zijn ingevoerd worden in de database door drie foto's en een naam toe te voegen. Ook als de persoon niet bekend is geeft de app een beschrijving van de persoon in de foto in termen van leeftijd, sekse en gezichtsuitdrukking. Het hele proces kan enkele seconden duren. Voor het gebruik van deze functionaliteit is een internetverbinding nodig.

Een derde variant betreft gezichtsherkenningstechnologie ontwikkeld voor de zakelijke markt ('business-to-business). Grote leveranciers zijn bedrijven zoals Amazon en Microsoft.[155] Zij bieden gezichtsherkenningsdiensten aan die andere bedrijven kunnen inzetten voor het ontwikkelen van hun diensten en producten, zoals smartphone apps. Zo levert Microsoft aan

[152] <www.facebook.com/help/122175507864081> geraadpleegd 14 oktober 2019.
[153] Ibid.
[154] Een vergelijkbare app is Envision AI.
[155] Hoewel Microsoft dus ook zelf gezichtsherkenning toepast in eigen producten zoals SeeingAI en ter ontgrendeling van bijvoorbeeld tablets en computers, zijn hun activiteiten op het gebied van gezichtsherkenning met name gericht op het leveren van diensten aan derden.

ontwikkelaars naast een 'app service omgeving' ter ondersteuning van het bouwen van apps ook een cloudgebaseerde Face-API (onderdeel van de Microsoft Azure Cognitive Services) die verschillende algoritmen biedt om gezichten van mensen te detecteren, herkennen en analyseren.[156] De gezichtsherkenning functionaliteit van de bovengenoemde Seeing AI is gebaseerd op de Azure Cognitive Services.

Amazon levert soortgelijke diensten via Amazon Rekognition en focust onder meer op gezichtsherkenning, gezichtsanalyse en emotie-analyse. Voorbeelden van toepassingen die Amazon geeft van hun diensten zijn: het herkennen van blijdschap, verdriet, en sinds kort ook van angst; een "Celebrity recognition" programma dat personen die beroemd of prominent in een domein zijn kan identificeren.[157]

Een laatste variant, die gelieerd is aan de vorige, maar apart aandacht verdient is gezichtsherkenningstechnologie die burgers kunnen gebruiken om hun eigen app te maken. Hoewel leveranciers zoals Microsoft en Amazon zich (nog) niet zeer expliciet richten op deze markt, is het voor burgers wel mogelijk van hun diensten gebruik te maken. Het is op dit ogenblik moeilijk vast te stellen welke vormen deze "Do It Yourself" (DIY) gezichtsherkenningsvariant aanneemt en kan aannemen in de nabije toekomst, aangezien deze ontwikkelingen niet noodzakelijk het grote publiek bereiken en documentatie ontbreekt. Dit maakt deze categorie wat speculatiever van aard dan de vorige drie. Het is desondanks belangrijk om deze variant mee te nemen in de analyse gezien de focus van dit onderzoek op horizontale privacy en de in de literatuur genoemde 'democratisering' van toepassingen zoals gezichtsherkenning (zie 4.2.2).

Om een inschatting te kunnen maken van de mogelijkheden voor burgers om zelf met gezichtsherkenning aan de slag te gaan, hebben wij onderzocht of het mogelijk is zonder te betalen en zonder programmeerkennis toch iets van een basale gezichtsherkenningstoepassing te ontwikkelen. Hiertoe hebben wij een account aangemaakt bij het Amerikaanse bedrijf Amazon. Dit gaf ons de mogelijkheid de gratis demoversie van hun gezichtsherkenningstechnologie-service *Rekognition* uit te proberen. Dit hield onder andere in dat wij functies zoals object detectie, gezichtsanalyse, gezichtsvergelijking en emotiedetectie in basale vorm toe konden passen.[158]

Amazon claimt dat gebruikers geen kennis van *machine learning* nodig hebben om hun diensten te kunnen gebruiken.[159] Op basis van zelf geüploade foto's van objecten en individuen, was het inderdaad mogelijk om onder andere vast te stellen wat er op de foto stond (zoals een boom) en wie (een man, leeftijd, wel of niet brildragend, vrolijk of kalm). Ook was het mogelijk om foto's met elkaar te vergelijken en bijvoorbeeld verschillende foto's van eenzelfde persoon met elkaar te matchen. De analyses zijn voorzien van *confidence thresholds*, die uitdrukken hoe waarschijnlijk het is dat een analyse klopt. In de kleine, niet-representatieve test die wij zelf hebben

[156] <www.docs.microsoft.com/nl-nl/azure/cognitive-services/face/index> geraadpleegd 17 oktober 2019.
[157] <www.aws.amazon.com/rekognition/> geraadpleegd 18 oktober 2019.
[158] AWS, 'Amazon Rekognition: Developer Guide' (2019) Amazon Web Services, 15-24 <https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf> geraadpleegd op 3 juli 2019.
[159] AWS, 'Amazon Rekognition: Developer Guide' (2019) Amazon Web Services 1 <https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf> geraadpleegd op 3 juli 2019.

uitgevoerd, verkregen wij verschillende thresholds terug, variërend van 70,3% tot 99,9%. Amazon raadt zelf aan om bij bepaalde toepassingen, zoals bijvoorbeeld verificatie van werknemers of bij veiligheid gerelateerde toepassingen, uitsluitend te werken met drempelwaarden van 99% en hoger. [160] Hoewel algemene programmeervaardigheden noodzakelijk zijn om bepaalde handelingen uit te voeren en zo een goed functionerende app met gezichtsherkenning te ontwikkelen,[161] is het dus mogelijk om, wanneer de app is ontworpen, gebruik te maken van gebruiksvriendelijke interfaces zonder dat hiertoe verder geprogrammeerd dient te worden.

4.2.2. **Privacyrisico's**

De verschillende soorten apps maken een hele reeks aan nieuwe activiteiten mogelijk in relaties tussen burgers. Zo stellen ze slechtzienden in staat mensen aan de hand van hun gezicht te herkennen en kunnen sociale mediagebruikers snel foto's zoeken van bekenden. Deze nieuwe mogelijkheden brengen ook privacyrisico's met zich mee. Hieronder belichten wij op basis van Solove's taxonomie de mogelijke privacy-inbreuken die de apps tot gevolg hebben. Hierbij richten wij ons op de vier hoofdcategorieën (informatieverzameling, informatieverwerking, informatieverspreiding en overschrijding). Waar nodig verwijzen wij ook naar subcategorieën.

Informatieverzameling

Gezichtsherkenningsapps voor burgers

De SeeingAI app kan positief bijdragen aan het gevoel van privacy (en veiligheid) van slechtzienden doordat het gebruikers in staat stelt om meer informatie te hebben over hoeveel en welke personen zich in hun direct omgeving bevinden, op welke afstand deze personen zich bevinden en zelfs in welke gemoedstoestand zij verkeren.[162] Daarmee kunnen gebruikers zich een beter beeld vormen van wat er zich afspeelt in hun directe omgeving. Momenteel vraagt dat nog enige medewerking van personen die automatisch dienen te worden herkend. Gebruikers moeten de camera duidelijk richten op een persoon, de persoon moet stil staan en het hele proces kan enkele seconden duren. Het is dus vooralsnog lastig om personen onopgemerkt of tegen hun wil te fotograferen.

De kans is groot dat hoe kleiner en onzichtbaarder de technologie wordt (bijvoorbeeld een camera in een bril), hoe meer het gebruikersgemak toeneemt en slechtziende personen de toepassing beter kunnen inzetten voor het waarnemen van hun omgeving en de mensen die zich in hun buurt bevinden.[163] Dit kan aan de ene kant de interactie met anderen en het gevoel van

[160] AWS, 'Amazon Rekognition: Developer Guide' (2019) Amazon Web Services, 143-144 <https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf> geraadpleegd op 3 juli 2019.
[161] AWS, 'Browse by Programming Language' (AWS Amazon) <www.aws.amazon.com/tools/#sdk> geraadpleegd op 3 juli 2019.
[162] T Ahmed e.a., 'Understanding Physical Safety, Security, and Privacy Concerns of People with Visual Impairments' (2017) 21 IEEE Internet Computing 56.
[163] Ibid.

privacy bij slechtzienden bevorderen, omdat gebruikers dan minder afhankelijk zijn van de medewerking van anderen en zich minder op de voorgrond hoeven te stellen in de interactie. Maar het kan ook de relatie tussen gebruikers en anderen problematiseren. Het idee dat iemand op elk moment herkend kan worden en dat gedragingen en gezichtsuitdrukkingen digitaal worden vastgelegd kan een *chilling effect* hebben op de personen die zich in de buurt van de gebruikers bevinden.[164] Zij kunnen zich meer bekeken en beoordeeld gaan voelen, waarop zij zich wellicht genoodzaakt zien om hun gedrag aan te passen en de gebruiker zelfs te gaan mijden.

Het gebruik van ondersteunende technologieën voor slechtzienden kan ook bijdragen aan een normalisering van *always-on* technologie in sociale interacties. Profita et al. laten zien dat derden het gebruik camera's op bril of hoofd eerder accepteren als de drager van de technologie gehandicapt is.[165] In een andere studie laten Ahmed et al. zien – op basis van interviews met omstanders bij het gebruik van visueel ondersteunende technologieën – dat mensen eerder bereid zijn om gegevens te delen als het gaat om ondersteunende technologie. Aan die bereidwilligheid zitten wel grenzen. Zo geven respondenten aan dat zij zich ongemakkelijk zouden voelen als de gebruiker meer zou waarnemen met behulp van de technologie dan een ziende persoon of als het niet duidelijk is dat hij of zij wordt waargenomen en geanalyseerd.[166]

Leveranciers gezichtsherkenning

Bedrijven zoals IBM, Microsoft en Amazon leveren niet alleen gezichtsherkenningsdiensten maar stellen ook datasets samen om de algoritmes te trainen. Deze datasets worden in sommige gevallen ook breder beschikbaar gesteld voor onderzoeksdoeleinden. Zo kwam IBM onder vuur te liggen na het beschikbaar stellen van hun "Diversity in Faces"[167] dataset die bedoeld is om met name bias en discriminatie tegen te gaan bij gezichtsherkenning.[168] Deze dataset bleek foto's te bevatten van Flickr gebruikers die hier niet van op de hoogte waren.

Ook is er de MS Celeb dataset van Microsoft die door verschillende bedrijven (Sensetime, Alibaba, en Panasonic) wordt gebruikt om hun algoritmes te trainen.[169] De dataset bevat ongeveer 10 miljoen foto's van 100 000 individuen die van het internet zijn geschraapt. Deze dataset is in juli 2019 door Microsoft echter offline gehaald. Eerder was bekend geworden dat deze dataset niet alleen foto's van beroemdheden bevatte, maar ook activisten en onderzoekers die hier niet van op

---

[164] L. Findlater e.a., *Fairness Issues in AI Systems that Augment Sensory Abilities* (ACM ASSETS Workshop on AI Fairness for People with Disabilities 2019).
[165] H. Profita e.a., 'The AT Effect: How Disability Affects the Perceived Social Acceptability of Head-Mounted Display Use' (2016) In proceedings of the 2016 CHI conference on human factors in computing systems 4884
[166] Ahmed, T., Kapadia, A., Potluri, V., & Swaminathan, 'Up to a Limit?: Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies' (2018) 2 Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 8.
[167] John R Smith, 'IBM Research Releases 'Diversity in Faces' Dataset to Advance Study of Fairness in Facial Recognition Systems' (2019) IBM <www.ibm.com/blogs/research/2019/01/diversity-in-faces/> geraadpleegd 3 november 2019.
[168] Biometric Technology Today (2019) 2 <www.sciencedirect.com/journal/biometric-technology-today> geraadpleegd 3 november 2019.
[169] Madhumita Murgia, 'Microsoft Quietly Deletes Largest Public Face Recognition Data Set' (2019) Financial Times <www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2> geraadpleegd 3 november 2019.

de hoogte waren noch wilden dat hun foto's deel uit maakten van deze dataset.[170] Adam Harvey, onderzoeker en kunstenaar, die onderzoekt doet naar databases en wiens werk aan de basis lag van de kritiek op de wijdverbreide toegang tot deze datasets geeft echter aan dat zelfs na het offline halen van de dataset door Microsoft, deze nog steeds beschikbaar is. Harvey stelt in de Financial Times:

> *"Je kunt een dataset niet laten verdwijnen. Zodra je het publiceert en mensen het downloaden, bestaat het op harde schijven over de hele wereld. Nu is het volledig losgekoppeld van alle licenties, regels of controles die Microsoft eerder had. Mensen plaatsen het op GitHub, hosten de bestanden op Dropbox en Baidu cloud, dus er is geen manier om te voorkomen dat ze het blijven posten en gebruiken voor hun eigen doeleinden."*[171]

DIY gezichtsherkenning

In principe is het ook mogelijk voor burgers om gebruik te maken van bovengenoemde datasets. Dit is zeker het geval wanneer deze datasets een eigen leven gaan leiden en niet meer uitsluitend bij de verstrekkende partij te verkrijgen zijn, maar ook via andere platformen en partijen zijn te downloaden.

Informatieverzameling in dit domein kan leiden tot verschillende type privacy-inbreuken. Eerst en vooral heeft het impact op communicatieve privacy, omdat het duidelijk wordt dat bij deze wijze van informatieverzameling er voor de betrokken individuen weinig tot geen controle is over de toegang tot hun foto's. Mensen die erachter komen dat hun foto's in deze datasets zitten, kunnen vervolgens geraakt worden in hun vermogen "zichzelf te zijn" in de openbare ruimte (gedragsmatige privacy), nu het duidelijk is dat foto's van hen genomen in de openbare ruimte in zo een dataset terecht kunnen komen.

Informatieverwerking

Gezichtsherkenningstechnologie ontwikkeld en ingezet door eenzelfde bedrijf

Om gezichtsherkenning toe te passen baseert Facebook zich op toestemming. De wijze waarop Facebook deze tracht te verkrijgen kent een grillige voorgeschiedenis en toont aan hoe moeilijk het is om toestemming voor gezichtsherkenning op een juridisch en ethisch zorgvuldige wijze te verkrijgen. Zo startte in 2015 een in Illinois (VS) verblijvende groep Facebook-gebruikers een

[170] <https://megapixels.cc/datasets/> geraadpleegd 3 november 2019.
[171] Madhumita Murgia, 'Microsoft Quietly Deletes Largest Public Face Recognition Data Set' (2019) Financial Times <www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2> geraadpleegd 3 november 2019.

rechtszaak tegen het platform (Patel vs. Facebook[172]) voor het niet naleven van de in deze staat geldende *Biometric Information Privacy Act* (BIPA).[173]

Volgens de klacht was Facebook's data policy, die in april 2018 werd aangepast, misleidend voor tientallen miljoenen gebruikers bij wie Facebook's gezichtsherkenningsinstelling genaamd "Tag Suggestions" aan stond. Deze instelling was standaard ingeschakeld, terwijl de data policy zou hebben gesuggereerd dat gebruikers ervoor moeten kiezen om gezichtsherkenning in te schakelen voor hun accounts (opt-in). Bovendien zou Facebook zich ook niet houden aan de bewaartermijn van de data. Ook de Federal Trade Commission (FTC) die op 24 juli 2019 een boete van 5 miljard dollar oplegde aan het bedrijf voor het schenden van consumenten hun privacy, betrok dit handelen van Facebook bij de onderbouwing van de totstandkoming van de boete.[174]

Enkele weken na de bekendmaking van de door de FTC opgelegde boete gaf het negende *US circuit court of appeals* in San Francisco groen licht voor het verderzetten van de rechtszaak tegen Facebook, waar het bedrijf bezwaar had tegenaan getekend.[175] Facebook had onder meer aangedragen dat het niet aannemelijk was gemaakt dat de klagers enige schade hadden geleden door de gezichtsherkenningstechnologie[176] en dat als die schade er al was dit op een individueel niveau diende te worden uitgezocht wat in een class-action zaak onmogelijk is. Beide argumenten werden verworpen door de rechtbank. In haar uitspraak geeft de rechtbank aan dat "hoewel tastbare schade weliswaar gemakkelijker te identificeren is, niet-tastbare schade nog steeds heel concreet kan zijn"[177].

---

[172] Case 18-15982 *Patel v Facebook* [2019] ID: 11390722 <https://assets.documentcloud.org/documents/6248797/Patel-Facebook-Opinion.pdf> geraadpleegd 15 oktober 2019..

[173] Fabienne Lang, 'Facebook Loses Facial Recognition Lawsuit and Could Owe Billions in Fines' (2019) Interesting Engineering <www.interestingengineering.com/facebook-loses-facial-recognition-lawsuit-and-could-owe-billions-in-fines> geraadpleegd 14 oktober 2019. BIPA vereist van bedrijven die biometrische gegevens verzamelen, gebruiken of delen, dat desbetreffende personen hiervoor geïnformeerd, opt-in toestemming moeten verlenen. Daarnaast moeten deze gegevens vernietigd worden wanneer ze het doel waarvoor ze verzameld worden bereikt is of drie jaar na het laatste contact met de desbetreffende persoon (welke optie het snelst is, telt). BIPA geeft individuen de mogelijkheid om zelf een bedrijf voor de rechter te dagen wanneer deze in hun ogen hun rechten schendt (*private right of action*).

[174] <www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> geraadpleegd 14 oktober 2019.

[175] Reuters, 'Facebook Facial Recognition Lawsuit Can Proceed, Says US Court' (2019) The Guardian <www.theguardian.com/technology/2019/aug/09/facebook-facial-recognition-lawsuit-can-proceed-us-court> geraadpleegd 14 oktober 2019.

[176] Sasha Ingber, 'Users Can Sue Facebook Over Facial Recognition Software, Court Rules' (2019) NPR <www.npr.org/2019/08/08/749474600/users-can-sue-facebook-over-facial-recognition-software-court-rules?utm_source=twitter.com&utm_campaign=npr&utm_medium=social&utm_term=nprnews&t=1571122361794> geraadpleegd 15 oktober 2019.

[177] Case 18-15982 *Patel v Facebook* [2019] ID: 11390722 11 <https://assets.documentcloud.org/documents/6248797/Patel-Facebook-Opinion.pdf> geraadpleegd 15 oktober 2019. Er wordt in de uitspraak uitgebreid ingegaan op de schade die gezichtsherkenning in het bijzonder kan veroorzaken voor individuen (Patel vs. Facebook, p.17): "Nadat een gezichtstemplate van een persoon is gemaakt, kan Facebook deze gebruiken om die persoon te identificeren in een van de andere honderden miljoenen foto's die elke dag naar Facebook worden geüpload; en om te bepalen wanneer de persoon op een specifieke locatie aanwezig was. Facebook kan ook de Facebook-vrienden of kennissen van de persoon identificeren die aanwezig zijn op de foto. Rekening houdend met de toekomstige ontwikkeling van dergelijke technologie zoals voorgesteld in Carpenter, lijkt het waarschijnlijk dat een persoon met een opgeslagen gezichtsfoto op basis van een bewakingsfoto genomen op straat of in een kantoorgebouw geïdentificeerd kan worden. Of een biometrisch gezichtstemplate kan worden gebruikt om het gezichtsherkenningsslot op de

Deze zaak wordt door Amerikaanse burgerrechtenbewegingen zoals de Electronic Frontier Foundation (EFF) als een “overwinning” en “keerpunt” beschreven voor de privacybescherming. Niet alleen omdat het doorgang biedt aan deze specifieke rechtszaak, maar zeker ook omdat het, steviger dan voorheen, uitlegt wat de privacyrisico’s van het gebruik van gezichtsherkenning zijn. De rechtbank onderschrijft dat wanneer privacyrechten onder BIPA worden geschonden dit voldoende grond biedt om te spreken van schade, en dat de mogelijkheid voor individuele burgers om een bedrijf hiervoor aan te klagen, cruciaal is voor een effectieve privacybescherming.[178]

Ook in Europa stuit het gebruik van gezichtsherkenning door Facebook op weerstand. In 2012 stopte Facebook met de tag suggestie in de EU na aanbevelingen van de toenmalige Ierse Data Protection Commissioner (DPC).[179] Bij het in werking treden van de AVG in 2018, introduceerde Facebook opnieuw de mogelijkheid tot gezichtsherkenning in de EU. Niet alleen de wijze waarop om toestemming werd gevraagd, met de nadruk op de noodzaak van gezichtsherkenning voor veiligheid, maar ook het gebrek aan een granulaire keuze –waarbij bijvoorbeeld een gebruiker de mogelijkheid heeft om gezichtsherkenning wel aan te zetten voor veiligheidsredenen, maar niet voor de tag optie– werd bekritiseerd.[180] Norberto Andrade (Global Policy Lead for Digital & AI Ethics at Facebook) legt uit dat Facebook gebruikers controle geeft over het gebruik van gezichtsherkenningstechnologie via een enkele controle, waardoor ze snel en eenvoudig alle functies en producten kunnen uitschakelen die gebruik maken van gezichtsherkenning op de Facebook-app.

“Deze instelling regelt het gebruik van gezichtsherkenning op de Facebook-app. Als je die activeert, weet je dat gezichtsherkenning in de hele FB-app wordt gebruikt of dat gezichtsherkenning helemaal is uitgeschakeld. Gebruikers hebben ons verteld dat ze de voorkeur gaven aan deze duidelijkheid." (Norberto Andrade. Privacy and Public Policy Manager bij Facebook).

Gezichtsherkenningsapps voor burgers

mobiele telefoon van die persoon te ontgrendelen. We concluderen dat de ontwikkeling van een gezichtssjabloon met behulp van gezichtsherkenningstechnologie zonder toestemming (zoals hier wordt beweerd) de privézaken en concrete belangen van een persoon binnendringt”.

[178] Adam Schwartz, ‘Victory! Lawsuit May Proceed Against Facebook’s Biometric Surveillance’ (2019) EFF www.eff.org/deeplinks/2019/08/victory-lawsuit-may-proceed-against-facebooks-biometric-surveillance-0> geraadpleegd 15 oktober 2019.

[179] Data Protection Commissioner, ‘Facebook Ireland Ltd: Report of Re-Audit 21 September 2012’ (2012) http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf; geraadpleegd 15 oktober 2019.

[180] Josh Constine ‘A Flaw-By-Flaw Guide to Facebook’s New GDPR Privacy Changes’ (2018) Techcrunch <www.techcrunch.com/2018/04/17/facebook-gdpr-changes/> geraadpleegd 15 oktober 2019.

Zoals gezegd kan de Seeing AI app het gevoel van privacy voor slechtzienden vergroten, maar ook op gespannen voet staan met de privacy van anderen. Vooralsnog worden de gegevens van de app niet lokaal verwerkt, maar op de servers van Microsoft. De app maakt gebruik van Microsofts algemene Privacy Statement, waarin onder andere is vermeld dat Microsoft gebruik maakt van de gegevens om services te verbeteren. Indien de gebruiker de app dagelijks gebruikt om mensen in zijn of haar omgeving te detecteren en te herkennen, heeft Microsoft in principe beschikking over een grote hoeveelheid informatie waarmee een rijk beeld kan worden geconstrueerd van het dagelijkse leven van de gebruiker, maar ook over de mensen met wie deze gebruiker omgaat. Alhoewel er bij ons momenteel weinig meer bekend is over hoe Seeing AI privacykwesties adresseert, is het na het MS Celeb incident en met de nadruk die Microsoft legt op de regulering van gezichtsherkenning waarschijnlijk dat het bedrijf de gegevens met enige voorzichtigheid behandelt (waarover hieronder meer).[181]

Leveranciers gezichtsherkenning

Een ander privacyrisico dat zich voordoet bij informatieverwerking is uitsluiting. Leveranciers van gezichtsherkenningstechnologie hebben een verantwoordelijkheid om bias zoveel mogelijk tegen te gaan in de producten die ze leveren. Bias kan in toepassingen immers leiden tot uitsluiting, discriminatie en misidentificatie. Of zoals Norberto Andrade (Facebook) stelt:

> *"[A]ls gezichtsherkenningsapplicaties niet met de juiste waarborgen gebouwd worden, namelijk met diverse datasets en middelen om de nauwkeurigheid van modellen te testen, kan het gebruik van deze technologie discriminerende effecten teweegbrengen."*

Omdat het onmogelijk is bias 100% uit te sluiten, is de noodzaak om transparant te zijn over de accuratesse en performance van de te leveren dienst des te groter. Microsoft geeft dan ook aan een groot voorstander te zijn van het 'auditable' maken van gezichtsherkenningstechnologie. Brad Smith (President van Microsoft) stelt:

> *"Potentiële klanten moeten goed geïnformeerd zijn en in staat om de technologie te testen op accuraatheid en risico's op oneerlijke bias, inclusief de bias die zich voordoet in de context van specifieke applicaties en*

[181] Op de App pagina staat overigens wel dat SeeingAI een doorgaand onderzoeksproject is. <https://apps.apple.com/us/app/seeing-ai-talking-camera-for-the-blind/id999062298>.

omgeving. Echter, tech bedrijven zijn niet allemaal even bereid om hun technologie beschikbaar te stellen voor dit doel."[182]

Ook Norberto Andrade onderschrijft dat auditing een belangrijk hulpmiddel kan zijn om bias te bestrijden, maar merkt op dat de vorm waarin dit moet gebeuren nog niet duidelijk is en goed moet worden besproken met de betrokken bedrijven.

"Het is bijna overbodig om een snapshot van een algoritmisch model te maken en te controleren, omdat het de volgende minuut alweer anders kan zijn. Het is dus een must om nauw samen te werken met bedrijven om vast te stellen wat de meest haalbare manier is om audits vorm te geven."

Afnemers van gezichtsherkenningstechnologie hebben daarnaast een eigen verantwoordelijkheid om hun eigen diensten en producten in overeenstemming met de relevante en van toepassing zijnde wet -en regelgeving op de markt te brengen. Hier houdt de verantwoordelijkheid van de leverancier in principe op. Echter zien wij wel dat sommige leveranciers zich actief inzetten om niet alleen het leveren van de technologie maar ook de ontwikkeling en toepassing ervan mede in goede banen te leiden. Zo heeft Microsoft zes principes ontwikkeld op basis waarvan ze oordelen of het aangaan van bepaalde samenwerkingsverbanden wenselijk is. Michael Vos (Government Affairs Consultant van Microsoft NL) licht toe:

"We gaan niet met een klant iets ontwikkelen dat duidelijk tegen onze principes ingaat. Er zijn voorbeelden waar Microsoft niet aan mee wil werken en waarbij we niet willen dat onze technologie daarvoor gebruikt wordt. […] Wat Microsoft voornamelijk ziet als belangrijkste rol is het voeren van een open dialoog met de kennis die we hebben. We gaan jullie niet vertellen hoe je de technologie moet gebruiken, want jullie hebben je eigen verantwoordelijkheden, maar denk aan deze en deze zaken. Onze zes A.I. principes hebben we in detail vastgelegd en delen we ook met potentiële klanten."

---

[182] Brad Smith, 'Facial Recognition: It's Time For Action' (2018) Microsoft <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/> geraadpleegd 11 november 2019.

Ook intern wordt de discussie gevoerd. Zo is er binnen Microsoft een commissie opgericht waar iedereen vragen aan kan stellen en een dialoog mee kan voeren. Martin Vliem (National Security Officer) stelt:

"We kijken wat er gebeurt met onze technologie en we kijken of we achter de manier staan waarop onze technologie wordt ingezet. De principes worden erlangs gehouden. Er wordt vaak een ethische discussie gevoerd. Het is immers vaak geen zwart-witte regelgeving. Zeker in een context waarin het niet duidelijk is wat wet- en regelgeving zegt of deze er niet is. Dan vallen we terug op de principes."

Tegelijk zijn er ook grenzen aan de verantwoordelijkheid en mogelijkheden van wat Microsoft vermag ten opzichte van klanten.

"Vanzelfsprekend is het uitgangspunt dat Microsoft en klanten vanuit hun eigen verantwoordelijkheden aan de wet voldoen. Dit wordt vervolgens ook in contracten opgenomen. Hierdoor staat er toch meer druk op. Echter, wanneer je een technologiedienst levert die veel controle en mogelijkheden legt bij de afnemers/klanten en tegelijk privacy en geheimhouding zoveel mogelijk waarborgt, dan is een gebruik voor verkeerde doeleinden niet altijd detecteerbaar of te voorkomen. Dan blijft goed communiceren belangrijk over wat wij acceptabel gebruik vinden en hoe wij vanuit verschillende principes kijken naar het gebruik van technologie."

DIY-gezichtsherkenningstechnologie

Wanneer burgers gebruik maken van gezichtsherkenningstechnologie om hun eigen toepassingen te fabriceren wordt het ingewikkelder voor leveranciers om ook een rol te spelen in de verdere toepassing en gebruik van de technologie. Een particuliere klant heeft geen 'code of conduct' of een duidelijke reputatie op basis waarvan er alarmbellen af zouden kunnen gaan. Daarbij komt dat leveranciers, op dit ogenblik, burgers ook niet in het vizier hebben als een belangrijke groep klanten. Wanneer gevraagd naar hoe leveranciers aankijken tegen deze groep klanten en hoe daarmee om te gaan geeft Martin Vliem (National Security Officer, Microsoft) aan:

"Alle suggesties die we doen voor de dialoog en de principes naar onze zakelijke partners, gelden ook als het gaat om consumenten. Als we direct aan consumenten leveren, moeten we de principes die we bespreken met zakelijke klanten, op onszelf van toepassing laten zijn. Dan zijn wij het bedrijf dat dit moet doen. Wij moeten zorgen dat wij het begrijpelijk maken, direct naar de eindgebruikers."

Daarnaast zet Microsoft in op voorlichting via hun blogs[183] en het recent vrijelijk te verkrijgen boek "Future Computed". [184] Bij het zelf uitproberen van Amazons' gezichtsherkenningsservice Rekognition, konden wij onder meer gebruik gemaakt van de Developer Guide die beschikbaar is gesteld door Amazon. In deze handleiding worden aanwijzingen gegeven hoe verantwoord om te gaan met de technologie. Zo worden er voorbeelden gegeven van toepassingen waarbij een zeer hoge *confidence threshold* van 99% of meer wordt aangeraden.[185] De vrijblijvendheid is hierbij echter groot. Ook als wij deze adviezen niet opvolgen, kunnen wij de gezichtsherkennings-technologie gebruiken.

Niet alle gezichtsherkenningsdiensten zijn vrijelijk te gebruiken door burgers. Zo heeft Google besloten "general purpose" gezichtsherkenning niet te leveren aan het grote publiek. Recentelijk is wel de "Celebrity Recognition API" aangekondigd. Deze API is echter niet voor algemene doeleinden en kan alleen gebruikt worden om bekende atleten en artiesten te herkennen. Toepassingen zijn bijvoorbeeld websites die hun aanbod willen organiseren of een app die een gepersonaliseerd aanbod geeft omtrent een bepaalde acteur.[186] Alleen professionele content (zoals TV-programma's) kan doorzocht worden (dus geen huis, tuin, -en keuken materiaal) en afnemers van deze dienst moeten van tevoren individueel goedgekeurd worden. Belangrijke voorwaarde voor zo een goedkeuring is dat het reeds gevestigde media -en entertainment bedrijven zijn. Ook zijn er extra algemene voorwaarden opgenomen die de uitdagingen van gezichtsherkenning adresseren.[187]

Bij informatieverwerking in het domein van gezichtsherkenningsapps zien wij met name dat communicatieve privacy, associatieve, en gedragsmatige privacy in het geding zijn.

[183] <https://blogs.microsoft.com/> geraadpleegd 11 november.
[184] Microsoft, The Future Computed: Artificial Intelligence and its Role in Society (Microsoft 2018) <https://blogs.microsoft.com/wp-content/uploads/2018/02/The-Future-Computed_2.8.18.pdf> geraadpleegd 11 november.
[185] Zie bijvoorbeeld: AWS, 'Amazon Rekognition: Developer Guide' (2019) Amazon Web Services 143-144.
[186] Abner Li, 'Google Cloud unveils facial 'Celebrity Recognition' API that follows AI Principles' *2019) 9to5Google <www.9to5google.com/2019/10/30/google-facial-celebrity-recognition/> geraadpleegd 13 november 2019.
[187] Parker Barnes en Andrew Schwartz, 'Celebrity Recognition Now Available To Approved Media & Entertainment Customers' (2019) GoogleCloud <https://cloud.google.com/blog/products/ai-machine-learning/celebrity-recognition-now-available-to-approved-media-entertainment-customers> geraadpleegd 13 november 2019.

Gezichtsherkenning als onderdeel van sociale media maakt dat gebruikers moeten afwegen hoe traceerbaar ze op een sociale media platform willen zijn (communicatieve privacy). Aangezien foto's offline worden gemaakt, kan het er ook toe leiden dat mensen steeds weigerachtiger worden om naar bijeenkomsten te gaan waar ze mogelijk gefotografeerd kunnen worden en via gezichtsherkenning vervolgens online herkend (gedragsmatige privacy).

Dit gaat ook niet louter om het zelf herkend worden, maar ook over met wie iemand op zo een foto komt te staan. Bepaalde relaties of interacties wil men misschien liever niet met anderen delen (associatieve privacy). Zelfs wanneer gezichtsherkenning voor een individu is uitgeschakeld, kan door gezichtsherkenning van een ander met wie deze persoon op de foto staat, informatie over deze persoon (waar men is, met wie, wat men aan het doen is) dus toch bij anderen terechtkomen, waar hij of zij dit liever voor zichzelf zou houden.

In het geval van Facebook, waar gezichtsherkenning platform-breed wordt ingezet, moeten gebruikers bovendien afwegen of ze ermee akkoord kunnen gaan dat gezichtsherkenning op alle gebieden wordt ingezet (dus niet alleen voor hun veiligheid, maar ook om herkend te worden in foto's van vrienden). Deze 'alles of niets' keuze maakt dat gebruikers minder vrij zijn in hun keuze en mogelijk concessies zullen doen (bv. eigenlijk vind ik het niet fijn dat mensen tagsuggesties krijgen voor mij maar ik wil ook geen verhoogd risico lopen op identiteitsfraude, dus zet ik de gezichtsherkenningsoptie maar aan). Ten slotte is er ook nog het risico op foutieve informatieverwerking. Zoals opgemerkt is bias in data een bekend probleem bij gezichtsherkenning. Het foutief herkennen van mensen kan leiden tot uitsluiting, discriminatie en sociaal ongemakkelijke omstandigheden.

Informatieverspreiding en overschrijding

Gezichtsherkenningstechnologie ontwikkeld en ingezet door eenzelfde bedrijf

Eén van de risico's met betrekking tot gezichtsherkenning is een hack waarbij het gezichtsherkenningstemplate dat Facebook heeft opgeslagen, wordt gestolen. Om dat tegen te gaan is het template dat Facebook gebruikt zodanig ontwikkeld dat het uitsluitend werkt op het Facebook platform. Norberto Andrade (Privacy and Public Policy Manager bij Facebook) verklaart: "het is op geen enkele manier mogelijk dat dit template in een andere database kan worden gebruikt voor bijvoorbeeld wetshandhaving of voor andere actoren. Het is niet interoperabel".

Gezichtsherkenningsapps voor burgers

Met het gebruik van ondersteunende technologie om de omgeving waar te nemen, wordt de interactie tussen de gebruiker en omstanders technologisch gemedieerd. Dat betekent dat de technologie mede vormt geeft aan hoe de interactie eruitziet. Dit kan de interactie verrijken, maar het kan ook een problematisch uitwerking hebben waarbij derden (in dit geval Microsoft) een te sturende werking hebben op de interactie. Dit kan bijvoorbeeld gebeuren als de gebruiker sterk leunt op de gebrekkige informatie die de app geeft. Als de app niet goed mensen herkend of

verkeerd emoties of leeftijd classificeert kan dat tot misverstanden of zelfs wantrouwen leiden.[188] Dit raakt aan mentale en communicatieve privacy: het kan de vrijheid die de gebruiker voelt om eigen beslissingen te maken of meningen te ontwikkelen en te delen, beperken.

Leveranciers gezichtsherkenning

De app FindFace werd in 2016 geïntroduceerd door de Russische ontwikkelaars Kabakov en Kukharenko (N-Tech Lab) als een technologie die onbekenden kan identificeren op basis van slechts één foto en dit met een nauwkeurigheid van 70 procent, mits de betreffende persoon een profiel op sociale media heeft.[189] De app werd gebruikt in combinatie met het zeer populaire Russische sociale mediaplatform Vkontakte, maar de technologie kan in principe "werken met elke foto database".[190]

Met het algoritme kunnen een miljard foto's in minder dan een seconde worden doorzocht. De app presenteert de gebruiker de meest waarschijnlijke overeenkomst met het geüploade gezicht en toont bovendien vergelijkbare gezichten. Kabakov ziet FindFace als een manier om een revolutie teweeg te brengen in de dating wereld: "Als je iemand ziet die je leuk vindt, kun je hem fotograferen, zijn identiteit vinden en hem dan een vriendschapsverzoek sturen. […] De app zoekt ook naar vergelijkbare mensen. Je kunt dus gewoon een foto uploaden van een filmster die je leuk vindt, of je ex, en dan 10 meisjes vinden die op haar lijken en ze berichten sturen."[191] In de praktijk bleek de app echter ook gebruikt te worden om porno-actrices te ontmaskeren en af te persen.

De app, zo bleek, was voor deze leveranciers vooral een manier om hun technologie voor het voetlicht te brengen. Zij zagen met name groeikansen op het terrein van wetshandhaving en detailhandel.[192] In 2018 werd de app dan ook stopgezet omdat het bedrijf overstapte naar het ontwikkelen van toepassingen voor bedrijven en overheden in plaats van voor het brede publiek. Nu levert het bedrijf zijn "FindFace Public Security", "FindFace Security" en "FindFace Enterprise Server SDK" aan retail, banken en financiën, openbare veiligheid, bedrijfsveiligheid, evenementen en casino's.

Dit maakt FindFace niet alleen een voorbeeld van hoe gezichtsherkenning op sociale media kan leiden tot grove privacy-inbreuken die mensen blootstelt en criminele handelingen zoals afpersing mogelijk maakt, maar ook hoe leveranciers van gezichtsherkenningsdiensten sociale media apps gebruiken als PR stunt en inzetten om hun technologie verder te ontwikkelen.

---

[188] T Ahmed e.a.,'Up to a Limit?: Privacy Concerns of Bystanders and Their Willingness to Share Additional Information with Visually Impaired Users of Assistive Technologies' (2018) 2 Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 89.

[189] Ben Guarino, 'Russia's New Findface App Identifies Strangers In A Crowd With 70 Percent Accuracy' (2016) Washington Post <www.washingtonpost.com/news/morning-mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70-percent-accuracy/?noredirect=on&utm_term=.72f7ba49d452> geraadpleegd 17 juli 2019.

[190] Ibid.

[191] Ibid.

[192] Ibid.

DIY gezichtsherkenning

Hoewel FindFace geen applicatie was die door burgers zelf is ontwikkeld, is het wel een app die zich dominant richt op de burger-burger relatie. In die zin geeft het een soort van doorkijkje naar wat te verwachten wanneer gezichtsherkenningstechnologie op een handzame wijze door burgers onderling kan worden gebruikt. Het illustreert hoe ontwrichtend gezichtsherkenning kan zijn voor deze horizontale relatie, zeker wanneer deze wordt ingezet in combinatie met sociale media. Gezichtsherkenning ontsluit veel meer informatie dan manuele zoekacties vermogen. Dat men op basis van foto's gemaakt in de publieke ruimte of gevonden op het internet, mensen op sociale media kan identificeren maakt dat burgers de controle verliezen over hun privacy. Was het sowieso altijd al ingewikkeld voor burgers om goed te kunnen inschatten wie precies hun berichten op sociale media kan zien, is dit in combinatie met gezichtsherkenning nog gecompliceerder geworden. Maar ook andersom is er het risico op het verlies van privacy. Wanneer mensen offline door middel van gezichtsherkenning eenvoudig gekoppeld kunnen worden aan hun acties online, wordt het onmogelijk zich nog langer onbespied te wanen in de openbare ruimte. Gezichtsherkenning wordt dan een sleutel om online en offline identiteiten *realtime* aan elkaar te verbinden.

4.2.3. **Best practices**

Best practices bij smartphone apps zijn niet eenvoudig te benoemen. Dit heeft deels te maken met de verschillende manieren waarop gezichtsherkenning in het domein wordt ingezet en de diversiteit aan spelers. Aan de ene kant van het spectrum staan grote tech bedrijven zoals Facebook, Amazon en Microsoft die niet alleen zelf gezichtsherkenning inzetten maar ook de bouwstenen leveren voor tal van andere bedrijven die hun eigen toepassingen ontwikkelen. Aan de andere kant staat de individuele burger die gebruik maakt van de apps ontwikkeld door deze bedrijven en misschien wel zelf aan de slag gaat met gezichtsherkenningstechnologie. Het is van al deze spelers afhankelijk of en hoe *best practices* zich vormen.

Bedrijfswaarden

Microsoft is één van de grote bedrijven die zich het meest uitspreekt over de risico's van gezichtsherkenning. Naast het ontwikkelen van eigen principes om sommige van die risico's te verlagen, zijn zij ook vragende partij voor meer overheidsregulering.[193] De zes principes die de

[193] Meer bedrijven zijn zich bewust van mogelijke problematisch consequenties van gezichtsherkenning. Om deze reden heeft het bedrijf Axon, producent van bewakingscamera's, bijvoorbeeld een ethics board voor AI. Deze board heeft geconcludeerd dat gezichtsherkenning op bodycams 'unethical' is. Zie bijvoorbeeld: C. Gartenberg, 'Axon (formerly Taser) says facial recognition on police body cams is unethical'. (2019) https://www.theverge.com/2019/6/27/18761084/axon-taser-facial-recognition-ban-ethics-board-recommendation geraadpleegd 20 februari 2020. Ook bedrijven zoals Google hebben opgeroepen tot duidelijke regulering van gezichtsherkenning technologie.

ontwikkeling en het gebruik van hun gezichtsherkenningstechnologie onderbouwen zijn de volgende:[194]

1. *Eerlijkheid*. Microsoft werkt eraan gezichtsherkenningstechnologie te ontwikkelen en in te zetten op een manier die ernaar streeft alle mensen eerlijk te behandelen.
2. *Transparantie*. Microsoft zal de mogelijkheden en beperkingen van gezichtsherkenningstechnologie documenteren en duidelijk communiceren.
3. *Verantwoording*. Microsoft zal zijn klanten aanmoedigen en helpen om gezichtsherkenningstechnologie in te zetten op een manier die een passend niveau van menselijke controle garandeert voor gebruik dat gevolgen kan hebben voor mensen.
4. *Non-discriminatie*. In Microsofts servicevoorwaarden wordt opgenomen dat het gebruik van gezichtsherkenningstechnologie voor onwettige discriminatie is verboden.
5. *Kennisgeving en toestemming*. Microsoft zal particuliere klanten aanmoedigen om kennisgeving en toestemming te geven voor de inzet van gezichtsherkenningstechnologie.
6. *Wettelijk toezicht*. Microsoft zal pleiten voor waarborgen voor de democratische vrijheden van mensen wanneer gezichtsherkenning wordt ingezet bij surveillance scenario's in het domein van de wetshandhaving. Microsoft zal geen gezichtsherkenningstechnologie implementeren in scenario's waarvan ze denken dat deze vrijheden onder druk komen te staan.

Door deze principes in de praktijk te brengen, koos Microsoft er bijvoorbeeld voor om af te zien van sommige samenwerkingsverbanden. Zo heeft Microsoft geweigerd om gezichtsherkennings-diensten te leveren aan Amerikaanse politiediensten die bij elke aanhouding de gezichtsherkenning wilden toepassen.[195] Wereldwijd kiest Microsoft ervoor 'notice and consent' (kennisgeving en toestemming) aan te moedigen, ook op plaatsen waar dit wettelijk (nog) niet vereist is.

Hoewel de aanpak van Microsoft kan gelden als een *best practice*, waarbij een bedrijf zijn maatschappelijke verantwoordelijkheid neemt voor de impact die een nieuwe technologie als gezichtsherkenning kan hebben, kent het ook beperkingen. Microsoft valt deels terug op deze principes omdat duidelijke wetgeving wereldwijd ontbreekt. Waar Microsoft op basis van de zes geformuleerde principes het leveren van gezichtsherkenning aan politiediensten afwijst, besluit het op basis van diezelfde principes ook om wel zijn diensten te leveren aan een gevangenis, wat als

[194] 6 principes voor gezichtsherkenningstechnologie van Microsoft https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf geraadpleegd op 17 februari 2020.
[195] James Vincent 'Microsoft Denied Police Facial Recognition Tech Over Human Rights Concerns' (2019) The Verge <www.theverge.com/2019/4/17/18411757/microsoft-facial-recognition-sales-refused-police-access> geraadpleegd 13 november 2019.

controversieel wordt beschouwd.[196] Waar Microsoft wereldwijd 'notice and consent' promoot, gaat het bedrijf echter niet zo ver te eisen dat deze toestemming expliciet is, zoals de AVG dit in de Europese Unie voorschrijft.[197] Zo stelt het bedrijf voor om consent vorm te geven via "het stemmen met de voeten". Wanneer een bedrijf duidelijk te kennen geeft (bijvoorbeeld via een bord bij de ingang) dat gezichtsherkenning wordt toegepast, dan zou –na zo een 'notice'– het betreden van de winkel kunnen gelden als toestemming (consent).[198]

Hoewel dit slechts een aanbeveling is van het bedrijf, illustreert het goed hoe keuzes omtrent gezichtsherkenning een bedrijfsaangelegenheid dreigen te worden wanneer een politieke en democratische besluitvoering ontbreekt. Dit laatste wordt overigens door Microsoft zelf ook onderschreven. Zij vragen expliciet om regelgeving voor gezichtsherkenning.

Privacy-by-design

De interface en het ontwerp van de technologie kunnen privacy-inbreuken beperken door expliciet de aandacht te trekken van omstanders, bijvoorbeeld door een opzichtig ontwerp of het onmogelijk te maken om ongezien informatie over omstanders te verzamelen en verwerken. Zo zagen wij bij SeeingAI dat de gebruiker momenteel de medewerking van een omstander moet vragen om herkenningen uit te voeren. Dit geeft omstanders meer ruimte om zich te onttrekken of expliciet toestemming te geven. Tegelijkertijd heeft dit in het geval van de SeeingAI app wel weer een privacy beperkend effect op de gebruiker van de app en blijft de bestaande informatieasymmetrie tussen slechtziende en ziende personen grotendeels in stand.

De gezichtsherkenningstemplate zodanig ontwikkelen dat het niet gebruikt kan worden buiten de eigen applicatie, zoals Facebook aangeeft te doen, is een ander voorbeeld van hoe een privacy-by-design aanpak kan bijdragen aan het voorkomen van bepaalde privacy-inbreuken.

Wet -en regelgeving

Wederom is het niet eenduidig of dit geldt als een *best practice*, maar noemenswaardig is wel dat bedrijven openstaan voor nieuwe regulering en daar zelf ook suggesties voor doen. Mogelijke oplossingsrichtingen die Microsoft aandraagt –vooral richting niet EU-landen aangezien sommige van deze zaken in de Europese Unie al geregeld zijn in met name de AVG– zijn onder meer: het bevorderen van betekenisvolle menselijke controle bij het nemen van impactvolle beslissingen met behulp van gezichtsherkenning, het eerdergenoemde "notice and consent" in de wet verankeren (met name buiten EU) en het verbieden van 'continue' surveillance van burgers door overheden.

[196] Joseph Menn, 'Microsoft Turned Down Facial-Recognition Sales On Human Rights Concerns' (2019) Reuters <www.reuters.com/article/us-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUSKCN1RS2FV> geraadpleegd13 november 2019.
[197] Microsoft, 'Six Principles for Developing And Deploying Facial Recognition Technology' <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf> geraadpleegd 13 november 2019.
[198] Brad Smith, Facial Recognition: It's Time For Action' (2018) Microsoft 7-12 <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/> geraadpleegd 11 november 2019.

Als het gaat om regelgeving, geeft Norberto Andrade (Privacy en Public Policy Manager bij Facebook) aan dat hij geen voorstander is van een volledig verbod op gezichtsherkenning, omdat het ook onmiddellijk alle positieve sociale gevolgen van de technologie teniet zou doen. Hij pleit voor een aanpak in drie fasen.

"Ik zou me eerst willen richten op het bieden van inzicht in hoe de technologie wordt ontwikkeld en ervoor zorgen dat deze is gebouwd op een manier die goed werkt voor alle gebruikers. Ten tweede, zorg ervoor dat gebruikers zich bewust zijn van en akkoord zijn gegaan met het gebruik van de technologie en ten derde dat de gevolgen en impact van de technologie op het leven van mensen, voor zover mogelijk, duidelijk in kaart zijn gebracht." (Norberto Andrade (Privacy and Public Policy Manager bij Facebook)

4.3. Slimme deurbel

Steeds vaker vervangen burgers hun traditionele deurbel door een zogenaamde slimme deurbel, ook wel videodeurbel genoemd. De redenen hiervoor zijn veiligheid en gemak. Veiligheid doordat via videobeelden zichtbaar is wie er aan de deur staat –ook zonder aan te bellen geeft de deurbel beeld door aan de gebruiker– en dit mogelijk de kans op huisinbraken terugdringt.[199] Gemak omdat er gecommuniceerd kan worden met degene die aan de deur staat en, in combinatie met een slim deurslot, zelfs op afstand toegang tot het huis gegeven kan worden. In dit kader is de slimme deurbel niet alleen interessant in de relatie burger-burger, maar zijn ook e-commerce bedrijven in deze technologie geïnteresseerd. Er zijn al meerdere proeven geweest om pakketbezorgers toegang tot een huis te verschaffen bij afwezigheid van de bewoners om zo toch het pakket te kunnen bezorgen.[200]

Er zijn verschillende aanbieders van slimme deurbellen op de markt - Ring[201], Blink, Skybell HD, August Doorbell, Nest Hello, om er een paar te noemen – en er zijn ook veel verschillende typen deurbellen op de markt. Vaak wordt de slimme deurbel verkocht in combinatie

---

[199] Een studie in de VS inderdaad een afname van buurtinbraken laat zien: Jefferson Graham 'Police Say Crime Drops With Video Doorbells' (2017) USA Today <https://eu.usatoday.com/story/tech/talkingtech/2017/03/29/crime-busting-video-doorbell-ring-expands-clones-undercut-price/99677840/>. Een studie uit Nederland uitgevoerd in Almere is minder positief: "Aangezien we op woningniveau geen preventief effect van de digitale deurbel ten aanzien van woninginbraken hebben kunnen vaststellen, is het niet aan te raden de digitale deurbel als voorwaarde voor het verkrijgen van het Politiekeurmerk Veilig Wonen toe te voegen." 'Rapportage Evaluatie pilot Digitale Deurbel Almere 2018' <https://veilig.almere.nl/fileadmin/files/almere/beeldbank/veiligheid/Evaluatierapport_digi_deurbel_20190325_def.pdf> geraadpleed 20 februari 2020.

[200] Ton Verheijen, ''Mensen houden van de slimme deurbel'' (2019) Twinkle <www.twinklemagazine.nl/2019/04/slimme-deurbellen/index.xml> geraadpleed 20 februari 2020.

[201] Overgenomen door Amazon. Bernadette van den Hooven, 'Amazon Investeert in Videodeurbellen' (2018) Twinkle <www.twinklemagazine.nl/2018/02/amazon-ring/index.xml> geraadpleed 20 februari 2020.

met een abonnement, waarvan er ook veel variaties bestaan.[202] Afhankelijk van het type deurbel en abonnement kan er bijvoorbeeld alleen op afstand in *real-time* via de mobiele telefoon gekeken worden wie er op een bepaald moment aan de deur staat, kunnen filmpjes hiervan worden opgeslagen en later worden teruggekeken, en/of kan op afstand gecommuniceerd worden met degene die er aan de deur staat.

Lang niet alle slimme deurbellen zijn uitgerust met gezichtsherkenning. De meeste deurbellen hebben wel de technologie om te kunnen detecteren dat er een persoon voor de deur staat, maar kunnen niet herkennen welke persoon er voor de deur staat. Op dit moment is Google Nest Hello een van de weinige deurbellen op de markt met gezichtsherkenning. Eind augustus 2019, heeft Amazon in Amerika wederom bevestigd dat Ring niet uitgerust zal worden met gezichtsherkenning, een mogelijke reden hiervoor is dat de technologie in verschillende Amerikaanse staten reeds verboden is.[203] Echter, een recente update van de privacy policy van Ring geeft aan dat waar het bij wet is toegestaan, Ring wel uitgerust kan worden met gezichtsherkenning. Deze functionaliteit zal enkel werken op basis van toestemming van de gebruiker van Ring, waarbij de gebruiker wel gewaarschuwd wordt dat er privacy implicaties kunnen zijn voor diegenen die door Ring in beeld worden gebracht.[204] Aangezien bij Google Nest reeds mogelijkheden zijn voor consumenten om gebruik te maken van gezichtsherkenning, wordt hieronder Google Nest gebruikt als onderwerp van deze domeinstudie.

4.3.1. **Google Nest Hello**

Google is een van de topproviders als het gaat om smart homes. Met de producten uit de "Nest" - lijn (voorheen Google Home tot de aankoop van Nest) wordt het hele huis met elkaar verbonden via slimme technologie, waarbij gedacht kan worden aan slimme thermostaten, spraak-gestuurde

[202] Zie voor de verschillende varianten abonnement die momenteel beschikbaar zijn: <https://nl-nl.ring.com/pages/protect-plans#subscription> geraadpleegd 20 februari 2020.
[203] Nicole Nguyen en Ryan Mac, 'Ring Says It Doesn't Use Facial Recognition, But It Has "A Head Of Face Recognition Research"' (2019) BuzzfeedNews <www.buzzfeednews.com/article/nicolenguyen/amazon-ring-facial-recognition-ukraine> geraadpleegd 20 februari 2020.
[204] <https://eu.ring.com/pages/privacy-notice>: "Where permitted by applicable law, you may choose to use additional functionality in your Ring product that, through video data from your device, can recognize facial characteristics of familiar visitors. For example, you may want to receive different notifications from your Ring Doorbell depending on whether a visitor is a stranger or a member of your household. If you choose to activate this feature, we obtain certain facial feature information about the visitors you ask your Ring product to recognize. We require your explicit consent before you can take advantage of this feature. Privacy, data protection and video surveillance laws in your jurisdiction may apply to your use of our products and services. You are the data controller with respect to personal information you obtain when using our products and services (such as video or audio recordings, live video or audio streams, images, comments, and data our products collect from their surrounding environment to perform their functions) and you are solely responsible for ensuring that you comply with applicable law when you use our products or services. For example, you may need to display a notice that alerts visitors to your home that you are using our products or services. Capturing, recording or sharing video or audio content that involves other people, or capturing others peoples' facial feature information, may affect their privacy and data protection rights."

assistenten en beveiligingscamera's. Google Nest's "Hello" is een slimme deurbel die volgens de advertentie slogan "makes other doorbells seem like dumbbells."[205]

De meest elementaire functie van Nest Hello is die van een deurbel die overal kan worden beantwoord zolang er een internetverbinding is. Wanneer iemand op de knop van de deurbel drukt, verschijnt er een waarschuwing op de mobiele telefoon van de gebruiker en/of op andere compatibele (smart home) apparaten. De gebruiker kan vervolgens desgewenst via de Nest-app met de persoon die voor de deur staat communiceren. Niet alleen heeft de gebruiker dan toegang tot de live feed van de camera, maar hij kan dus ook rechtstreeks communiceren met de bezoeker, deze negeren of een selectie van vooraf opgenomen berichten afspelen. De livestream is te allen tijde toegankelijk.[206]

Bovendien kan de gebruiker waarschuwingen instellen voor bepaalde gebeurtenissen. Standaardwaarschuwingen zijn een eenvoudige notificatie aan de gebruiker wanneer de camera een persoon ziet of hoort, bewegingswaarschuwingen voor elke bewegingsactiviteit die de camera registreert en geluidswaarschuwingen wanneer de microfoon (die afzonderlijk moet worden ingeschakeld) van de camera een geluid opneemt. Nest slaat momentopnamen van de meldingen op in een tijdlijn van evenementen.[207] Om toegang te krijgen tot 'videogeschiedenis'[208] - de cloud gebaseerde video-opname- en opslagservice van Nest - moet de gebruiker een abonnement op Nest Aware nemen. Videogeschiedenis slaat de videobeelden op in de cloud, waardoor de gebruiker toegang heeft tot een opname van de 24/7 live feed van gebeurtenissen voor de camera van de deurbel in plaats van alleen snapshots of korte clips van de afgelopen drie uur.[209] Afhankelijk van het abonnement kan de gebruiker toegang krijgen tot maximaal 30 dagen aan opnames.[210] Deze termijn is overigens hetzelfde bij de meeste Amazon Ring Protect Plans – de verschillende abonnementen van Ring – waarbij snapshots overigens langer bewaard worden, namelijk zeven dagen.[211]

4.3.2. **Gezichtsherkenningstechnologie**

In combinatie met Nest Aware is Nest Hello interessant voor dit onderzoek, omdat het abonnement de gebruiker 'intelligente activiteitswaarschuwingen' biedt, inclusief gezichts-

[205] Slogan en de informatie over de Nest Hello verkregen via: <https://store.google.com/gb/product/nest_hello_doorbell?hl=en-GB>.
[206] Samuel Gibbs, 'Nest Hello Review: Google's Smart Facial-Recognition Video Doorbell' (2018) The Guardian <www.theguardian.com/technology/2018/sep/20/nest-hello-review-google-smart-facial-recognition-video-doorbell> geraadpleegd 30 oktober 2019.
[207] <www.support.google.com/googlenest/answer/9210305?hl=en#camera-alerts-people> geraadpleegd 20 februari 2020.
[208] De terminologie in dit stuk vormen letterlijke vertalingen van de beschikbare informatie van Nest en Nest Aware welke beschikbaar is in het Engels.
[209] <www.support.google.com/googlenest/answer/9250907?hl=en>.
[210] <www.support.google.com/googlenest/answer/9227541?hl=en>.
[211] Zie de informatie over de verschilende Ring Protect Plans op <https://eu.ring.com/pages/protect-plans#subscription>.

herkenningsfuncties.[212] De functie die Google 'vertrouwdegezichtsdetectie'[213] noemt, gebruikt de gezichtsherkenningsalgoritmen van Nest om individuele gezichten te zoeken. In plaats van gebruik te maken van een openbare database, kan de gebruiker personen toevoegen in haar eigen database die de 'bekendegezichtenbibliotheek' wordt genoemd. Wanneer de camera een gezicht tegenkomt dat niet in de bekende gezichtenbibliotheek staat, vraagt de app of de gebruiker de persoon kent. De gebruiker kan vervolgens de gezichten *taggen* met namen of, in het geval van een fout, de app vertellen dat wat de waarschuwing veroorzaakt geen persoon is. Alle Nest-gebruikers in een huishouden kunnen bijdragen aan de bibliotheek.[214] Berichtgeving en ringtone kunnen vervolgens toegespitst worden op een bepaald persoon. Zoals eerder aangegeven is voor deze extra gezichtsherkenningsfuncties wel een abonnement nodig.

In reviews wordt de functie van gezichtsherkenning vooral in combinatie met andere smart producten genoemd als een meerwaarde.[215] De verbinding met andere producten van Google werkt goed, ook in de Nederlandse taal, en smart producten van concurrenten, hoewel niet direct compatible met Google Nest, kunnen wel gekoppeld worden via de clouddienst 'If This Then That'. Als voorbeeld wordt gegeven "Als je deurbel dat bellentrekkende buurjongetje herkent, hoor je door je slimme speakers - en zie je op je gekoppelde smart displays - ook wie er precies aan de deur is. Waarna je ervoor kunt kiezen niet thuis te geven".[216] Want vooralsnog blijft de identificatie met alleen de slimme deurbel beperkt. Standaard staat gezichtsherkenning uit, maar als men deze bij Google Nest aanzet dan wordt van iedereen die in beeld komt cameramateriaal verzameld om zo de gezichten te leren herkennen en als er voldoende beeldmateriaal van iemand is, kan men deze persoon een naam geven en wordt dus een database van bekende gezichten opgebouwd.

De melding via Google Nest gaat echter (nog) niet op naam, maar blijft beperkt tot 'bekend persoon' en 'onbekend persoon'.[217] In buitenlandse reviews over de Nest slimme deurbel wordt wel gesproken over de mogelijkheid van identificatie per persoon op naam.[218] Dat deze mogelijkheid wel bestaat lijkt ook te volgen uit de informatie die wordt gegeven op de Google support website.[219] Hieruit volgt dat de gebruiker hiervoor wel de extra stap moet zetten om de personen opgenomen in de bekendegezichtenbibliotheek te voorzien van een naam, of een

[212] <www.support.google.com/googlenest/answer/9210305?hl=en#camera-alerts-people> geraadpleegd 21 februari.
[213] Het gaat hier niet om een vertrouwde vorm van gezichtsdetectie, maar om de detectie van vertrouwde gezichten, vandaar één woord.
[214] <www.support.google.com/googlenest/answer/9268625?hl=en> geraadpleegd 20 februari 2020.
[215] Matthijs Meeuwsen 'De Strijd Tussen Ring En Nest: Wie Heeft De Beste Slimme Deurbel?' (2019) AD <www.ad.nl/tech/de-strijd-tussen-ring-en-nest-wie-heeft-de-beste-slimme-deurbel~ab19c61d/> geraadpleegd 15 december 2020.
[216] Ibid.
[217] Eric Verlooij, 'Amazon Ring Pro en Nest Hello' (2018) Consumentenbond <www.consumentenbond.nl/beveiligingscamera/amazon-ring-pro-en-nest-hello#no7> geraadpleegd 15 december 2020.
[218] Samuel Gibbs, 'Nest Hello Review: Google's Smart Facial-Recognition Video Doorbell' (2018) The Guardian <www.theguardian.com/technology/2018/sep/20/nest-hello-review-google-smart-facial-recognition-video-doorbell> geraadpleegd 15 december 2020;Terry Walsh, 'Nest Hello Video Doorbell Review' (2018) Digital Trends ,www.digitaltrends.com/home-security-reviews/nest-hello-review/> geraadpleegd 20 februari 2020.
[219] Zie: <https://support.google.com/googlenest/answer/9268625?hl=nl> geraadpleegd 20 februari 2020.

kernmerk, bijvoorbeeld postbode. Er wordt echter niet via de interface gevraagd naar toestemming van de betreffende persoon.

"Ik zie gezichtsherkenning heel concreet opkomen als mogelijke integratie in platformen die breder diensten aanbieden voor een veilige buurt voor bijvoorbeeld brandpreventie en inbraakpreventie. Hier speelt een nieuwe groep van jong gepensioneerden een interessante rol, ze hebben tijd, zijn kritisch en ze doen al allerlei dingen. En als ik het met hen verkennend heb over dit soort diensten, dan is direct de reactie: "Wacht even, we zijn nu dingen via Whatsapp aan het delen, daar voelen we ons vrij bij maar daar hebben we misschien al vragen bij, maar wat zien die nieuwe technologieën allemaal? Hier komt de term zien heel duidelijk naar voren, dat heeft toch een andere gevoelswaarde dan andere vormen van sensoring" Ben Kokkeler (Lector Digitalisering en Veiligheid)

Privacy statement

Een blik op de privacy statement van de Nest Aware en Nest Home geeft meer inzicht in hoe de technologie werkt en welke gegevens er worden opgeslagen en verwerkt. Google gebruikt dezelfde privacy voorwaarden voor al zijn Nest-producten. Het belooft transparant te zijn, toestemming te vragen voor het delen van gegevens met derden en gebruikt de best mogelijke tools voor gegevensbeveiliging. Eigenaars van Nest-accounts moeten 18 jaar of ouder zijn, geautoriseerde gebruikers ouder dan 13 jaar (afhankelijk van de toepasselijke jurisdictie) en enkel met toezicht en/of toestemming van de ouder of wettelijke voogd. Door een Nest-product te gebruiken, stemt de gebruiker in met internationale gegevensoverdrachten naar de Verenigde Staten en andere landen waarin Nest actief is (binnen het EU-VS Privacy Shield-kader).[220] De informatie die door een Nest-camera wordt verzameld, omvat setup-informatie van de gebruiker, omgevingsgegevens, video- en audiosignalen en gegevens, evenals alle gezichtsherkenningsgegevens die nodig zijn om de bekende gezichtsfunctie mogelijk te maken. De gebruiker kan het doel en de middelen aanpassen waarvoor hij video- en audiogegevens verzamelt.

Door de functie 'bekende gezichtswaarschuwingen' te gebruiken, stemt de gebruiker in met de verwerking van "gezichtsafbeeldingen en onderliggende gezichtsafdrukken om uw apparaat in staat te stellen bekende gezichten te herkennen en u te informeren over bekende en

[220] Privacy Shield is een overeenkomst tussen het Amerikaanse ministerie van Economische Zaken en de Europese Commissie over de uitwisseling van persoonsgegevens tussen bedrijven in de EU en de VS. Het Privacy Shield is sinds 1 augustus 2016 van kracht en vervangt het Safe Harbor-verdrag. Voor meer hierover zie: <www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu>

onbekende mensen." [221] De privacyverklaring benadrukt op verschillende plaatsen dat de gebruiker verantwoordelijk is voor het naleven van wetten die het gebruik van gezichtsherkenningstechnologieën reguleren, bijvoorbeeld door uitdrukkelijke toestemming te verkrijgen van de mensen die voor de deurbel verschijnen en bezoekers op de hoogte te brengen van de aanwezigheid van een deurbel met gezichtsherkenning.

Meerdere Nest-producten die in een huis zijn geïnstalleerd, communiceren onderling en met de Nest-app. Nest verwerkt ook persoonsgegevens voor eigen gerechtvaardigde belangen en die van derden en wanneer Google daartoe wettelijk verplicht is. Elke toestemming voor specifieke activiteiten kan op elk moment worden ingetrokken. Persoonlijke informatie wordt onder geen beding gedeeld voor commerciële of marketingdoeleinden die geen direct verband houden met de activering en levering van Nest-producten en -diensten zonder toestemming van de gebruiker. Persoonlijke informatie kan op elk moment door de gebruiker worden bekeken, gewijzigd of verwijderd. Met betrekking tot de gezichtsherkenningsfunctie stelt de privacyverklaring dat de gebruiker wordt aangemerkt als verwerkingsverantwoordelijke en Nest als verwerker. Op deze manier lijkt Google de verantwoordelijkheid voor de verwerking nadrukkelijk neer te leggen bij de burgers die zo een deurbel in huis halen.[222]

4.3.3. **Privacyrisico's**

Wanneer wij kijken naar Solove's taxonomie en de vier groepen van activiteiten die privacy kunnen schaden, valt op dat in alle vier deze categorieën risico's verbonden zijn aan de slimme deurbel. Wellicht niet met betrekking tot de mogelijkheden die nu geboden worden, maar zeker wel met het oog op mogelijke extra functionaliteiten die technisch gezien vrij eenvoudig te realiseren lijken te zijn.

Informatieverzameling

Voor de beoordeling van de implicaties voor de privacy van Nest Hello moet een onderscheid worden gemaakt tussen de functies van het product met en zonder het abonnement op Nest Aware. Zonder de gezichtsherkenningsfunctie zijn de privacykwesties van de videobewakingsfuncties van Nest Hello die van gewone videobewaking door burgers. Hierover heeft de European Data Protection Board in 2019 richtlijnen uitgevaardigd.[223]

Kijkend naar de categorieën van Solove, vindt de schadelijke activiteit plaats in de eerste fase van het verzamelen van informatie.[224] Afhankelijk van welke informatie wordt verzameld,

[221] Alle informatie in deze paragraaf afkomstig uit de privacy statement van Nest, beschikbaar via: <www.nest.com/ie/legal/privacy-statement-for-nest-products-and-services/>..
[222] Ibid.
[223] EDPB, Guidelines 3/2019 on processing of personal data through video devices. Beschikbaar via: <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en> geraadpleegd 20 februari 2020.
[224] Daniel J Solove, 'A Taxonomy of Privacy' (2005) 154 University of Pennsylvania Law Review 477.

varieert de schade van de surveillance. Als een camera puur op de ingang van een huis gericht is, filmt hij alleen mensen die aanbellen en die daarom door familieleden willen worden gezien. Zodra de camera meer in beeld brengt, en er mensen in beeld kunnen komen die geen interactie met de eigenaar van de camera willen hebben, kan er sprake zijn van een inbreuk op de privacy van deze personen. De camera brengt dan immers meer in beeld dan noodzakelijk is voor het doel om te kunnen zien wie er aan de voordeur staat. Zeker wanneer er sprake is van het in beeld brengen van de openbare weg of privéterrein van anderen kan dit ertoe leiden dat personen zich aangetast voelen in hun vrije bewegingsruimte.[225] Zij kunnen zich daarop gedwongen voelen om hun gedrag, bijvoorbeeld hun dagelijkse route, aan te passen.

Privacy-inbreuken kunnen ook samenhangen met de wijze waarop beelden bekeken worden. Gebeurt dit enkel in *real-time* of worden deze ook opgeslagen en hoe lang blijven ze vervolgens beschikbaar en voor wie? Beelden die bewaard worden, kunnen immers toegankelijk zijn voor anderen dan de eigenaar van de deurbel, kunnen met anderen gedeeld worden en kunnen in een andere context (her)gebruikt worden. Ook bij de gezichts- en objectdetectiefunctie van Hello gaat het voornamelijk om het verzamelen van de informatie. Oftewel, het systeem detecteert alleen of er een persoon voor de camera staat of niet, zonder individuen te identificeren. Indien mensen zicht bewust zijn van deze beperkte functionaliteit is de inbreuk mogelijk minder groot dan op het moment dat zij weten dat ze ook herkend kunnen worden.

Informatieverwerking

De bekendegezichtenfunctie van Nest Hello in combinatie met Nest Aware raakt de categorie die Solove informatieverwerking noemt, meer specifiek: identificatie.[226] Bezoekers kunnen worden geïdentificeerd door de gebruiker van Hello. Op basis van Koops 'typologie van privacy' vindt de interactie van de betrokkene met Nest Hello waarschijnlijk plaats in de semi-openbare zone. Terwijl de bezoeker zich voorbereidt op interactie met de leden van het huishouden, heeft hij nog steeds een zekere mate van anonimiteit en reserve.[227] De redenen voor het bezoek kunnen persoonlijk of professioneel van aard zijn en zonder slimme deurbel zou de bezoeker zich nog kunnen bedenken, een optie die voor bezorgers is uitgesloten. Er zijn scenario's denkbaar waarbij een bezoek aan een bepaald persoon de reputatie van de bezoeker kan aantasten. Dit kan bijvoorbeeld het geval zijn als iemand het huis van zijn maîtresse bezoekt of van een prostituee, zaken die men privé wilt houden maar hetgeen gecomprimeerd (kan) worden door de deurbel. De wetenschap dat het bezoek op beeld wordt vastgelegd, kan een reden zijn om af te zien van het bezoek, hetgeen een inperking van de vrijheid van de persoon betreft.

[225] De Autoriteit Persoonsgegevens geeft als richtlijn ook: "Is een camera wel (deels) gericht op een (deel) van de openbare weg? Of filmt iemand bijvoorbeeld de tuin van de buurman? Dan is de AVG wél van toepassing en houdt de Autoriteit Persoonsgegevens dus ook toezicht."
[226] Daniel J Solove, 'A Taxonomy of Privacy' (2005) 154 University of Pennsylvania Law Review 477.
[227] BJ Koops e.a. 'A Typology of Privacy' (2016) 38 University of Pennsylvania Journal of International Law 483, 551.

Informatieverspreiding en overschrijding

Er is een groot potentieel voor misbruik van de gegevens die worden verzameld door een slimme deurbel. Gebruikers kunnen videobeelden verspreiden van mensen die ze bestempelen als verdacht, hetgeen zelfs kan leiden tot *naming-and-shaming* op het internet. Vooral onthulling en afpersing liggen voor de hand, bijvoorbeeld het verspreiden van beelden van inbrekers via buurtapps of sociale media.

Dit soort potentieel misbruik is niet vergezocht, gezien de "Neighbors app" van concurrent Amazon Ring. Hoewel Amazon Ring nog geen gezichtsherkenning gebruikt[228], laat de manier waarop gebruikers op deze app communiceren, zien dat buren niet altijd dol op elkaar zijn en dat de inbreuk op privacy, zelfs zonder gezichtsherkenning, enorm kan zijn. Op de Neighbors app kunnen Ring-gebruikers elke feed van hun slimme deurbel delen. In de praktijk wordt het gebruikt als een soort buurtwacht. Zwartmakerij, het onthullen van intriges, het ten onrechte of terecht bestempelen van personen als criminelen, met als gevolg het recht in eigen hand nemen, zijn allemaal voorbeelden van onwenselijke situaties die voort kunnen komen uit het gebruik van de deurbel en de app. Ook zijn er reeds ernstige zorgen dat de app wordt ingezet om mensen van kleur te discrimineren en racisme actief te versterken door mensen van kleur als verdacht te melden.[229] Dus, zelfs zonder gezichtsherkenning, kan een slimme deurbel veel schade aanrichten. Dit geldt nadrukkelijk voor mensen die vanwege professionele redenen bij de deurbellen in beeld komen, zoals post- en pakketbezorgers. Dit sluit aan bij wat Solove *secundair gebruik* van informatie noemt: het inzetten van informatie voor een doel dat niet is gerelateerd aan het initiële doel waarvoor het was verzameld.[230] Steeds meer huishoudens besluiten tot het gebruik van een slimme deurbel en hoe meer beelden van deze apparaten gedeeld worden, des te groter zullen de privacyschendingen worden.[231]

"Met de toename van allerlei sensoringtechnieken in de openbare ruimte zien we een grote zorg bij groepen van mensen die mindervalide zijn, en die een niet normale manier van bewegen hebben op straat. Meneer of mevrouw loopt niet normaal, die heeft gedronken of heeft drugs gebruikt. Die sociale impact is enorm groot. Ook bij de slimme deurbel kun je gewoon wachten op de eerste escalaties, waarbij de situatie voor de deur compleet verkeerd geduid

---

[228] Amazon filed a patent for combining its Rekognition facial recognition technology with Ring: <http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=5&f=G&l=50&co1=AND&d=PG01&s1=amazon.AANM.&s2=siminoff.IN.&OS=AANM/amazon+AND+IN/siminoff&RS=AANM/amazon+AND+IN/siminoff>.

[229] Caroline Haskins, 'Amazon's Home Security Company Is Turning Everyone Into Cops, Motherboard' (2019) Vice <www.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops> geraadpleegd 20 februari 2020.

[230] Daniel J Solove, 'A Taxonomy of Privacy' (2005) 154 University of Pennsylvania Law Review 477.

[231] Molly Wood, 'Smart Home Cameras Bring Facial Recognition Ethics To Your Front Door' (2019) cnet <www.cnet.com/news/smart-home-cameras-bring-the-facial-recognition-ethical-dilemma-to-your-front-door/>

wordt met allerlei mogelijke gevolgen van dien, van eigen richting tot op Facebook plaatsen van beelden." Ben Kokkeler (Lector Digitalisering en Veiligheid)

Het verspreiden van Nest beelden en identificaties kan bovendien ook leiden tot wat Solove bestempeld als "*verstoring",* het manipuleren van de wijze waarop een individu gezien en beoordeeld wordt door anderen.[232] Wanneer het bijvoorbeeld niet echt gaat om een inbreker, maar de bewoner de onbekende persoon als zodanig bestempeld. De onbekende aan de deur kan daar met heel andere - legitieme - doelen gestaan hebben, maar kan door de bewoner ten onrechte verdacht worden gemaakt in buurtapps en/of sociale media. Dit kan leiden tot laster, roddels, reputatieschade, stigma's en schaamte. Verstoring verschilt van onthulling doordat het hier gaat om het verspreiden van valse informatie. Er lijkt hier wel degelijk een machtsdisbalans te ontstaan door een ongelijkwaardige informatiepositie. Zowel tussen de gebruiker van een deurbel en partijen die de diensten van de bel aanbieden, als tussen de gebruiker van de bel en de personen die van deze bel gebruik (moeten) maken.

Met Nest Hello heeft de betrokkene geen controle over zijn biometrische gezichtsgegevens. Er is geen manier om toestemming te vragen voordat de betrokkene is gefilmd door de camera van de deurbel en deze gegevens kunnen zelfs verwerkt worden op servers buiten de EU. Hoewel Nest Hello geen algemene database gebruikt, maar de gebruiker zijn eigen vertrouwde gezichtenbibliotheek laat maken, moeten de gezichten van een persoon in het gezichtsveld van de camera verwerkt worden om deze service te bieden. Hierdoor biedt deze functionaliteit van Googel Nest weinig privacywaarborgen. Een melding aan bezoekers dat er sprake is van een slimme deurbel met gezichtsherkenning maakt de inbreuk op privacy niet ongedaan.

Volgens recensenten komen valse meldingen vaker voor zonder het abonnement op Nest Aware.[233] "Schaduwen van voorbijgangers worden geïdentificeerd als personen waardoor een alarm in werking treedt terwijl deze personen zich eigenlijk niet in de bewegingszone bevinden"."[234] Hoewel Nest Hello werkt zonder het abonnement, alleen al het feit dat het beter werkt met, zal

---

[232] In dit verband kan gewezen worden op de documentatie van concrete voorbeelden waarbij gezichtsherkenning werd gebruikt om bepaalde volken in West China te traceren en het ten onrechte kwalificeren van personen als criminelen, zie: Khari Johnson, 'How Amazon's Facial Recognition Ambition Could Stunt Alexa's Development' (2019) Ventuebeat <www.venturebeat.com/2019/05/26/how-amazons-facial-recognition-ambition-could-stunt-alexas-development/> geraadpleegd 21 februari 2020.

[233] Vertaald uit het Engels door auteurs. Samuel Gibbs, 'Nest Hello Review: Google's Smart Facial-Recognition Video Doorbell' (2018) The Guardian <www.theguardian.com/technology/2018/sep/20/nest-hello-review-google-smart-facial-recognition-video-doorbell>; Terry Walsh, 'Nest Hello Video Doorbell Review' (2018) Digital Trends <www.digitaltrends.com/home-security-reviews/nest-hello-review/>

[234] Samuel Gibbs, 'Nest Hello Review: Google's Smart Facial-Recognition Video Doorbell' (2018) The Guardian <www.theguardian.com/technology/2018/sep/20/nest-hello-review-google-smart-facial-recognition-video-doorbell>

gebruikers ertoe verleiden om de gezichtsherkenningsfuncties te gebruiken, zelfs op plaatsen waar deze illegaal zijn.

"Je bent soms verbaast hoe snel die deurbellen zich verspreiden, ik ken de cijfers niet maar het gaat veel sneller dan ik verwacht had. Hier gaan service providers nieuwe mogelijkheden in zien dus daar verwacht ik zeer veel ontwikkelingen, zowel in positieve als in negatieve zin. De kansen kant zit echt in het bereiken en betrekken van burgers die via woord en cijfers niet bereikbaar zijn maar mogelijk wel participeren door beeld. In de risico-sfeer is privacy overduidelijk een groot punt van aandacht. Ik ben ook heel kritisch over de vraag of het ook echt de veiligheid gaat vergroten. We weten eigenlijk ook niet hoe we dat kunnen meten." Ben Kokkeler (Lector Digitalisering en Veiligheid)

4.3.4. **Best practices**

Google Nest herinnert gebruikers er herhaaldelijk aan dat ze verantwoordelijk zijn voor de naleving van de wet met betrekking tot de gezichtsherkenningstechnologie. Er worden echter geen aanbevelingen gedaan over hoe dit te doen in de jurisdicties waar het product wordt gebruikt. De enige uitzondering is een tip om een waarschuwing te geven door bezoekers op de hoogte te brengen van de aanwezigheid van een deurbel met gezichtsherkenning. De bedoeling hiervan is dat de gebruiker volledig verantwoordelijk wordt gemaakt voor eventuele privacyschendingen.

Een nog niet beproefde *best practice*, maar wel een interessant suggestie is te vinden op het forum van de Nest-community. Hier wordt het idee geopperd dat de privacykwesties kunnen worden opgelost door een andere optie voor privacy-by-design toe te voegen aan de functie van de deurbel zelf. Een gebruiker stelt voor om de camera alleen te activeren wanneer de deurbel wordt gebruikt, om constant filmen te voorkomen.[235] Op deze manier konden bezoekers op de hoogte worden gebracht van de camera (en de gezichtsherkenningsfunctie) en bijvoorbeeld met een extra functie zou men af kunnen melden door simpelweg de keuze te bieden om op de deur te kloppen in plaats van aan de bel te rinkelen, of het gezicht voor de camera te verbergen.

4.4. Retail

Gezichtsherkenning staat in toenemende mate in de belangstelling in de retailsector wereldwijd. De technologie kan bijvoorbeeld worden gebruikt om winkeldiefstal tegen te gaan; relevante

[235] <www.nest-community.com/s/question/0D51W00005iJBnfSAG/nest-hello-activate-camera-on-ringing-only-privacy-laws-in-some-countries> 20 februari 2020.

sms'jes te sturen naar binnenwandelende klanten om hen te verwelkomen, aanbevelingen, kortingen en andere aanbiedingen te doen of klanten een gepersonaliseerde service te bieden bij hun winkelbezoek. [236] Bovendien kan het worden ingezet om het betaalproces te vergemakkelijken, de wachttijd te verkorten, en om personeelskosten te verminderen (betalen zonder kassa's).

In Europese landen, zoals het Verenigd Koninkrijk, experimenteren winkeliers vooral met gezichtsherkenning om verlies door winkeldiefstal terug te dringen. Dit gebeurt momenteel met name op proefbasis.[237] Ook in Nederland werd bekend dat een Jumbo supermarkt in Alphen aan den Rijn een systeem met tachtig camera's heeft geïnstalleerd waarmee gezichten van bezoekers kunnen worden vastgelegd.[238] Mensen die aangehouden worden voor winkeldiefstal, kunnen later door het systeem worden geïdentificeerd en vervolgens de winkel uitgezet. Berichtgeving hierover leidde tot Kamervragen. Zo werd aan minister voor Rechtsbescherming dhr. Dekker gevraagd of hij van mening is dat "dit praktijkvoorbeeld van de Jumbowinkel evident in strijd is met de AVG?"[239]

In de literatuurstudie zijn wij geen voorbeelden tegengekomen van gezichtsherkennings-toepassingen voor het doen van betalingen in Europese winkels. Met uitzondering van Carrefour. Deze supermarktketen heeft gezichtsherkenning geïmplementeerd in een zogeheten *concept store* in Massy, Frankrijk.[240]

Ook in de VS wordt gezichtsherkenning in winkels ingezet, met name voor beveiliging en het tegengaan van diefstal. [241] Op welke schaal dit reeds gebeurt is niet duidelijk omdat veel van de grote retailers weigeren hun ontwikkelingen in de VS te onthullen, volgens een rapport uit 2018.[242] Het Amerikaanse retailbedrijf Walmart lijkt in ieder geval terughoudend te zijn geweest in het gebruik van de technologie, hoewel het twee patenten heeft aangevraagd om ontevreden klanten te kunnen identificeren en om gesprekken van medewerkers te kunnen beluisteren.[243] Daarentegen heeft Target, als een populaire retailer, systemen getest in een klein aantal Target

---

[236] Jesse Davis West, '3 Ways that Face Recognition Will Impact Future Retail Stores in 2019', (2019) FaceFirst <www.facefirst.com/blog/face-recognition-will-impact-future-retail-stores/> geraadpleegd 8 oktober 2019.
[237]Tom Chivers, 'Facial Recognition… Coming To A Supermarket Near You' (2019) The Observer <www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties> geraadpleegd 8 oktober 2019.
[238] Willem Heck (2019) "Uw gezicht dient steeds vaker als toegangskaartje". NRC, 29 november 2019. https://www.nrc.nl/nieuws/2019/11/29/dieven-en-onschuldigen-de-camera-ziet-iedereen-a3982154; bezocht 23 januari 2019.
[239] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D01497&did=2020D01497; bezocht 23 januari 2019.
[240] Ben Stevens, 'Carrefour Launches Cashierless Store Where Shoppers Pay Using Facial Recognition' (2019) Charged <www.chargedretail.co.uk/2019/06/19/carrefour-launches-cashierless-store-where-shoppers-pay-using-facial-recognition/> geraadpleegd 15 november 2019.
[241] Leticia Miranda 'Thousands Of Stores Will Soon Use Facial Recognition, And They Won't Need Your Consent' (2018) BuzzFeed News <www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at> geraadpleegd 8 oktober 2019.
[242] Esther Fung, 'Shopping Centers Exploring Facial Recognition in Brave New World of Retail' (2019) Wall Street Journal <www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802> geraadpleegd 8 oktober 2019.
[243] Leticia Miranda 'Thousands Of Stores Will Soon Use Facial Recognition, And They Won't Need Your Consent' (2018) BuzzFeed News <www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at> geraadpleegd 8 oktober 2019.

winkels om inzicht te krijgen in het vermogen van gezichtsherkenning, met als doel fraude en diefstal te helpen voorkomen.[244]

In China worden gezichtsherkenningstechnologieën reeds geregeld gebruikt in horizontale relaties, waaronder het openbaar vervoer en de detailhandel. Zo worden deze technologieën bijvoorbeeld al ingezet voor metrosystemen, het inchecken en de veiligheid op luchthavens, bankieren, mobiele betalingen, toezicht op de werkruimte, en zelfs in openbare toiletten.[245] In de retail wordt het met name ingezet voor winkelbeveiliging, het verlagen van de exploitatiekosten van winkels, het analyseren van het gedrag van klanten en het verbeteren van de klantervaring (door de wachttijd te verkorten).

4.4.1. **De Chinese retailsector**

De Chinese gezichtsherkenningstechnologie (met inbegrip van de bijbehorende kunstmatige intelligentie en praktische toepassingen) is wereldwijd leidend. In 2018, werd bijna de helft van de markt bediend door Chinese aanbieders.[246] Dit is, ten eerste, waarschijnlijk deels te wijten aan de zwakke juridisch-sociale omgeving op het gebied van privacy in China, waar de kans groter is dat mensen privacy inleveren voor gemak -de zogenaamde "*data for service*"- in China.[247] Ten tweede, dwingt de toenemende hevige concurrentie tussen de marktspelers hen om de arbeidskosten te drukken, de ervaring van de consument te verbeteren (verkorten van de wachttijd), en de veiligheid te bevorderen met behulp van meerdere technologieën. Gezichtsherkenning is dan een relatief geaccepteerde, kosteneffectieve oplossing. Een laatste mogelijke reden is de snelle uitrol van de 5G-infrastructuur van China (in de grote provinciale hoofdsteden) en technologie die het mogelijk maakt om *real-time* grote hoeveelheden online data te verwerken in de cloud, en de mogelijkheid om grote datasets met gezichtsgegevens te gebruiken voor het ontwikkelen van speciale algoritmen (met bijna geen wettelijke beperkingen).[248]

---

[244] Ibid.

[245] Zoals onlangs in nieuws berichten verscheen, zijn veel Chinese consumenten overgegaan van het betalen met een smartphone naar betalen met het gezicht. Zie: Takashi Kawakami en Yusuke Hinata, 'Pay with your face: 100m Chinese switch from smartphones' (2019) Nikkei Asian Review <www.asia.nikkei.com/Business/China-tech/Pay-with-your-face-100m-Chinese-switch-from-smartphones> geraadpleegd 14 november 2019; Tarvin Gill, 'China Is Installing Facial Recognition Toilet Paper Dispensers In Public Restrooms' (2019) Mashable <https://sea.mashable.com/culture/1621/china-is-installing-facial-recognition-toilet-paper-dispensers-in-public-restrooms>; Voor een kort overzicht zie: Zhoau Jiaquan, 'Drones, Facial Recognition And A Social Credit System: 10 Ways China Watches Its Citizens' (2018) South China Morning Post <www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china>.

[246] Yuang Yang & Madhumita Murgia (2019) Facial Recognition: how China cornered the surveillance market. Financial Times, 6 december 2019 https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385; bezocht 23 januari 2019.

[247] Chinese internetgebruikers gebruiken veelal gratis software (services), bijvoorbeeld, waarbij zij voor lief nemen dat zij daarvoor in ruil hun persoonlijke data onthullen. Dit geldt in het bijzonder voor jongeren generaties. See: Yu Zhang e.a.., 'Effects of Transparency of Service Design on User Attitude Toward 'Exchanging Information for Service' in Constantine Stephanidis ed HCI International 2019 – Posters (Springer 2019), 225–23

[248] Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (2019) The New York Times <www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> geraadpleegd 8 oktober 2019.

De toename van het gebruik van gezichtsherkenning wordt niet alleen gestimuleerd door praktische behoeften op het gebied van veiligheid, identificatie, openbaar bestuur, misdaadonderzoek, enz., maar wordt ook ondersteund door de industriële strategie van de centrale overheid. Met de aanzienlijke steun van de Chinese staat, moet het land tegen 2030 een wereldleider zijn op het gebied van kunstmatige intelligentie. In de afgelopen jaren hebben veel gezichtsherkenningsbedrijven en startende ondernemingen geprofiteerd van de industriële strategie en nationale subsidies.[249] Bovendien heeft het zowel op nationaal als op lokaal niveau veel risicokapitaal aangetrokken (met inbegrip van risicokapitaal van Alibaba en Tencent, twee grote Chinese actoren op het gebied van gezichtsherkenningstechnologie). Tegen deze achtergrond is gezichtsherkenning uitgegroeid tot een van de populairste hightech sectoren in China.

Om inzicht te krijgen in de inzet en het gebruik van gezichtsherkenningstechnologie in Chinese winkels, hebben wij contact gelegd met een Chinese advocaat die voor een van China's belangrijkste spelers op deze markt (een multinationale conglomeraatsholding) werkt, voor een interview (in het Chinees). Omwille van de vertrouwelijkheid en de inhoudelijke gevoeligheid hebben wij op verzoek van de geïnterviewde besloten om diens identiteit en de bedrijfsnaam niet bekend te maken. Wij spreken daarom van 'bedrijf Z' en 'de geïnterviewde', en hebben enkele identificerende verwijzingen weggelaten.

4.4.2. **Bedrijf Z in de retailsector**

Bedrijf Z heeft gezichtsherkenningstechnologie ontwikkeld door middel van haar investeringen in meerdere technologiebedrijven binnen en buiten China, waaronder enkele van de grotere gezichtsherkenningsbedrijven. Bedrijf Z heeft "gestaag geïnvesteerd in fysieke winkelfilialen" via een handvol supermarkten in grote Chinese steden, die het bedrijf volledig in eigendom heeft en volledig exploiteert. In deze winkels experimenteert bedrijf Z met nieuwe technologieën.

Het bedrijf levert samen met Chinese internetgiganten, zoals Jingdong, ook gezichtsherkenningstechnologie aan bedrijven in combinatie met de consumentengegevens die bedrijf Z en Jingdong via hun verschillende platformen hebben verzameld voor profileringsdoeleinden. Het bedrijf Z heeft een grote gebruikersdatabase van ongeveer 550 miljoen *real-name* gebruikers van het onlinebetaalservice platform van bedrijf Z (derde partij betaalplatform), waarmee zij rekeningen betalen, verkeersboetes afhandelen, vermogen beheren en kleine leningen verkrijgen. De bij bedrijf Z aangesloten financiële dienstengroep heeft ook een mobiel betaalsysteem ontwikkeld dat gebaseerd is op gezichtsherkenning.

De gezichtsherkenningstechnologie wordt ontwikkeld door de technische bedrijven waarin Z heeft geïnvesteerd. Ook heeft Z zijn eigen interne eenheden die werken aan

[249] Zie: James Lord, 'Retail Revolution: Can Facial Recognition Transform China's Retail Sector? (2019) CKGSB Knowledge <http://knowledge.ckgsb.edu.cn/2019/03/20/retail/sensetime-facial-recognition-china-retail/> 20 februari 2020.

gezichtsherkenningstechnologie, bijvoorbeeld om gebruikers in staat te stellen om afleverboxen bij ophaalpunten (pick-up points) te ontgrendelen in grote steden zoals Shanghai. Voor dit project wordt verwacht dat het foutieve acceptatiepercentage, of de kans dat het systeem ten onrechte een ongeautoriseerde gebruiker accepteert, onder de 0,001 procent ligt en verder kan worden verlaagd om de veiligheid op bankniveau te waarborgen. Bedrijf Z was ook betrokken bij de "smile to pay service" gelanceerd in Hangzhou, waar het werd getest bij een bekende restaurantketen. Deze service stelt een klant in staat om te betalen met een glimlach.

Er zijn twee groepen gebruikers van Bedrijf Z's gezichtsherkenningstechnologie. Het bedrijf is zelf een gebruiker, met inbegrip van gezichtsherkenning op de mobiele app van Z en de eigen winkels van Z. Daarnaast levert het bedrijf Z de technologie ook aan andere klanten, waaronder ook retailers.

In de winkels waar de gezichtsherkenningsapparaten van Z in gebruik zijn genomen, is het doel het bevorderen van de efficiëntie (gemak) en daarmee het verbeteren van de consumentenervaring. De achterliggende gedachte is het verlagen van de arbeidskosten (met stijgende salarissen in de grote Chinese steden), terwijl er relatief meer consumenten in de winkels zijn dan in de EU en de VS. Verder kan bedrijf Z meer persoonlijke gegevens verkrijgen om de database of het profiel te verrijken dat is gecreëerd bij de registratie van een klant voor een van zijn of haar betaalsystemen (mobiele app of tablet-app) en online E-commerce platformen (platform overschrijdende database binnen het bedrijf). De geïnterviewde gaf aan dat gezichtsherkenning haar (zakelijke) klanten kan helpen bij het efficiënt verwerven van nauwkeurige gegevens die hun bedrijfsvoering ten goede komen, zoals het nauwkeurig herkennen van waardevolle klanten, maar ook van oude klanten, om zo het marktaandeel te vergroten en de verkoop te verbeteren.

Het businessmodel van bedrijf Z lijkt gebaseerd op het koppelen van diverse gegevens. Volgens de geïnterviewde levert bedrijf Z gezichtsherkenningsdiensten aan winkels en slaat de verzamelde gegevens zelf op. Volgens andere bronnen, zoals nieuwsberichten, probeert bedrijf Z ook een verbinding te maken tussen de gezichtsgegevens en de consumentengegevens die via haar online winkelplatformen worden verzameld. Dit zou mogelijk zijn indien de verkoper/onderneming (met behulp van de gezichtsherkenning van bedrijf Z) zich ook op het e-commerce platform van Z bevindt, of wanneer de bezoekende consumenten gebruik maken van de diensten van Z, zoals de door Z ontwikkelde mobiele betaalapplicatie. De combinatie van deze gegevens zou bedrijven in staat stellen om diensten op maat aan te bieden, zodat op het moment dat een consument de winkel van de verkoper binnenkomt, de winkelbediende weet wat de klant wil.

4.4.3. **Gezichtsherkenningstechnologie**

Uit onze analyse is niet gebleken welk type algoritmen bedrijf Z gebruikt. Wel is er meer bekend over de werking van enkele producten, zoals bijvoorbeeld applicaties voor de authenticatie van betalingen, waaronder draagbare betaalapparatuur, kassa's en (code)scanners. Volgens nieuwsberichten is in het algemeen voor het betalingsproces geen smartphone nodig, ervan uitgaande dat de klant zich al heeft aangemeld voor de Z-betaalapp en gezichtsherkenning heeft ingeschakeld. Een 3D-camera bij het betaalpunt scant het gezicht van de klant om zijn of haar identiteit te verifiëren, met de mogelijkheid tot verificatie van zijn of haar telefoonnummer voor extra beveiliging.

De gezichtsherkenningstechnologie van Z wordt ingezet op voorwaarde dat een klant zich registreert op een van de onlineplatformdiensten van Z, inclusief de betaalapp of e-commerce websites, om authenticatie en nauwkeurigheid zo goed mogelijk te garanderen. Om een geldige account te hebben voor de service van Z, moet een klant zijn ID-kaart (met pasfoto) uploaden voor naamverificatie en een persoonlijke foto. Sinds 2016 worden alle gebruikers van Z gevraagd om het authenticatieproces volgens de Chinese wet te doorlopen door hun identiteits- of paspoortdocumenten (inclusief gezichtsfoto's) te verstrekken. Zo kan de grote gezichtsdatabase, in combinatie met andere persoonlijke informatie, het authenticatieproces in de winkels garanderen.

4.4.4. **Privacyrisico's**

De geïnterviewde verklaarde uitdrukkelijk dat beelden van gezichten in China standaard als uiterst gevoelige persoonsgegevens worden beschouwd. Het bedrijft Z stelt dat de gegevens die worden gebruikt voor analyse worden geanonimiseerd en dat persoonlijke gegevens van klanten niet worden gedeeld. Desalniettemin liggen er verschillende risico's op de loer bij het gebruik van gezichtsherkenningstechnologie zoals ontwikkeld door bedrijf Z. Wij hebben aan de hand van Solove's taxonomie deze privacyrisico's in kaart gebracht.

Informatieverzameling

De surveillance mogelijkheden voor de detailhandelaar nemen toe wanneer dergelijke gegevens systematisch kunnen worden opgeslagen en gebruikt om bezoekende klanten te controleren. Ook hier speelt het chilling effect weer een rol. Klanten kunnen zich mogelijk anders gaan gedragen wanneer zij zich continu geobserveerd voelen.

Bovendien kunnen de door bedrijf Z verzamelde gegevens van belang zijn voor de Chinese staat, bijvoorbeeld in kader van de ontwikkelingen op het gebied van het sociale kredietsysteem.[250]

[250] Zie: Alexandra Ma, 'China Has Started Ranking Citizens With A Creepy "Social Credit" System — Here's What You Can Do Wrong, And The Embarrassing, Demeaning Ways They Can Punish You' (2018) Business Insider <www.businessinsider.nl/china-social-credit-system-punishments-and-rewards-explained-2018-4?international=true&r=US> geraadpleegd 16 november 2019.

Naar aanleiding van de toekomstige Chinese wetgeving en het toekomstige Chinese beleid bestaat er dan ook een reëel risico dat de Chinese staat toegang zal krijgen tot de gegevens van bedrijf Z. Dit risico geldt overigens niet specifiek voor bedrijf Z. De meeste Chinese bedrijven zullen op verzoek van de staatsautoriteit toegang verlenen. Het toont de verwevenheid aan tussen horizontale en verticale privacy. Een gebrekkige borging van privacy in de horizontale relatie kan ook privacy in de verticale relatie in het geding brengen. Wanneer dergelijke gegevens zullen worden opgeslagen en door de overheid kunnen worden geraadpleegd, zal dit leiden tot verder toenemend, systematisch toezicht door de staat. Dit kan het gedrag van mensen in hoge mate beïnvloeden.

Informatieverwerking

De aggregatie van gegevens zal een probleem vormen en is mede afhankelijk van de grootte van bedrijven zoals bedrijf Z. De koppelingen van gegevens kan leiden tot de verdere identificatie van consumenten op andere momenten of andere plekken. Op die manier kunnen individuen nauwlettend in de gaten worden gehouden, bijvoorbeeld wanneer de persoon wordt geïdentificeerd als een 'slechte' consument. Ook hier kan een *chilling effect* optreden, maar het kan ook leiden tot uitsluiting, bijvoorbeeld wanneer mensen op basis van een profiel geen toegang hebben tot bepaalde diensten of locaties (zoals winkels).

Informatieverspreiding

Het is niet zeker dat de verzamelde gezichtsinformatie/gegevens niet zullen worden vrijgegeven aan derden die een nauwe band en een gedeeld belang met bedrijf Z hebben. De gezichtsgegevens van de consument kunnen aan het publiek worden blootgesteld wanneer bedrijf Z of winkels met wie het bedrijf zakendoet geen goede beveiligingsmaatregelen hebben getroffen of wanneer niet geautoriseerde personen gemakkelijk toegang hebben tot de database. Dit kan leiden tot een vertrouwensbreuk.

Overschrijding

Er kan sprake zijn van inmenging in de besluitvorming van de consument, aangezien de consument in deze winkels kan worden gemonitord, geprofileerd en mogelijk gemanipuleerd door middel van toekomstige nudgingstrategieën zoals verkoopacties of doelgerichte advertenties, die van invloed kunnen zijn op de besluitvorming van de klant bij toekomstige aankopen.

4.4.5. **Best practices**

De geïnterviewde wijst erop dat er in China geen specifieke wetgeving is die toeziet op gezichtsherkenning om zo gezichtsgegevens te beschermen. Er is dus geen duidelijk juridisch risico; in feite is het risico alleen een reputatierisico voor een bedrijf.

Desondanks heeft bedrijf Z, volgens de geïnterviewde, een aantal maatregelen getroffen om privacyrisico's te beperken. Zo verzamelt het bedrijf geen originele beelden, maar alleen templates van het gezicht van de consument en houdt het nauwkeurig bij wie toegang krijgt tot die templates. Bovendien hebben winkels en zakenpartners in principe geen directe toegang tot de verzamelde gegevens.

Het bedrijf heeft een juridisch team in dienst dat zorgt voor de naleving van de wetgeving voor de onderneming volgens een gedetailleerd plan en met een interne hervorming van het management. Het heeft ook interne mechanismen voor de controle en verwerking van gezichtsgegevens opgezet en een kader voor de naleving van de wetgeving vastgesteld. Op deze manier wil bedrijf Z ook ervoor zorgen dat gezichtsgegevens niet worden verstrekt aan derden, waaronder de zakelijke klanten van de onderneming. De geïnterviewde geeft voorts aan dat sectorspecifieke regels hard nodig zijn in China.

5. Privacy-inbreuken veroorzaakt door het gebruik van gezichtsherkenningstechnologie: een antwoord op de eerste onderzoeksvraag

In de voorgaande hoofdstukken hebben wij beschreven wat gezichtsherkenningstechnologie omvat, hoe bedrijven en burgers de technologie inzetten en hoe gezichtsherkenning een inbreuk kan vormen op de privacy van burgers. Dit hebben wij gedaan aan de hand van een algemene literatuurstudie in hoofdstuk 3, die in hoofdstuk 4 verder is toegespitst aan de hand van vier domeinstudies en aangevuld met interviews. Hierbij hebben wij internationaal gekeken om zo een beeld te krijgen van de meest recente ontwikkelingen (die zich niet noodzakelijk in Nederland afspelen) en zo ook een blik op de toekomst te werpen. Onze eerste bevindingen hebben wij vervolgens voorgelegd en bediscussieerd in een expertworkshop.

Op basis van dit onderzoek hebben wij de, naar ons oordeel, voornaamste gezichtsherkenningstoepassingen (nu en in de nabije toekomst) en de daarmee gepaard gaande privacyrisico's uitgewerkt in dit hoofdstuk. Hiermee zal hoofdstuk 5 de eerste centrale onderzoeksvraag van deze verkennende studie beantwoorden. Deze luidt: *Hoe wordt gezichtsherkenningstechnologie door Nederlandse burgers en bedrijven gebruikt en hoe kan het gebruik van gezichtsherkenningstechnologieën door burgers en bedrijven een inbreuk vormen op de privacy van de burger (nu en over vijf jaar)?*

Onderstaand presenteren wij eerst de huidige stand van zaken in Nederland en de te verwachten ontwikkelingen *(sub-vraag 1.1 Hoe wordt gezichtsherkenningstechnologie momenteel door burgers en bedrijven gebruikt? Hoe verwachten experts dat het gebruik van deze technologie zich de komende vijf jaar zal ontwikkelen?).* Vervolgens staan wij stil bij de grootste privacyrisico's nu en in de nabije toekomst *(sub-vraag 1.2 Hoe kan het gebruik van gezichtsherkennings-technologie door burgers en bedrijven een inbreuk vormen op de privacy van de burger? Wat zijn de grootste privacyrisico's? En met welke privacyrisico's dient volgens de experts de komende vijf jaar rekening te worden gehouden?).*

5.1. Huidige stand in Nederland: experimentele fase

Het huidige gebruik van gezichtsherkenningstechnologie in de horizontale relatie bevindt zich in Nederland in de experimentele fase. Er worden in diverse domeinen op kleine schaal proeven gedaan om te onderzoeken of een rendabele *use case* tot de mogelijkheden behoort. Dit zien wij bijvoorbeeld terug bij de proef uitgevoerd door de RAI en dit beeld wordt bevestigd in de gesprekken met ontwikkelaars en leveranciers van gezichtsherkenningstechnologie.

Deze stapsgewijze aanpak wordt niet louter ingegeven door economische motieven. Ook het toenemend bewustzijn bij bedrijven en afnemers van gezichtsherkenningstechnologie over de

privacyrisico's die ermee gemoeid zijn, maakt dat men niet al te voortvarend wil handelen. Alle gesprekspartners die opereren op de Nederlandse markt benoemen de AVG dan ook als het belangrijkste wettelijk kader waarmee ze rekening houden bij het ontwikkelen en opzetten van deze nieuwe gezichtsherkenningstoepassingen.

Het is echter niet altijd even helder voor betrokken partijen hoe de vereisten neergelegd in de AVG geïnterpreteerd moeten worden zodat gezichtsherkenning op een legitieme en aanvaardbare wijze kan worden toegepast. Deze onduidelijkheid draagt dan ook bij aan de waargenomen voorzichtigheid. Daarboven komt dat bedrijven zich ook terdege bewust zijn van mogelijke afbreukrisico's wanneer zou blijken dat zij onzorgvuldig handelen.

Gezichtsherkenning in Nederland beperkt zich niet tot Nederlandse bedrijven. Zo worden Amerikaanse bedrijven ingezet om gezichtsherkenning in de Nederlandse context mogelijk te maken. In Nederland gevestigde bedrijven leveren op hun beurt ook gezichtsherkenningsdiensten en producten aan de buitenlandse markt. Ook is er een grote diversiteit aan type bedrijven. Gevestigde technologiebedrijven zoals Amazon, Google, en Microsoft hebben allemaal een gezichtsherkenningstak, maar ook startups proberen een plek te veroveren in deze markt.

Het beperkt aantal gezichtsherkenningstoepassingen dat wij in Nederland hebben gevonden en bekeken, wordt gekenmerkt door een eenduidig en specifiek doel. Vaak gaat het om een bepaalde vorm van toegangscontrole waartoe identificatie of verificatie van individuen door gezichtsherkenning wordt ingezet. Dit zien wij bij de slimme deurbel en de snelle check-in die centraal staan in de domeinstudies, maar ook in het brede literatuuronderzoek en de expertworkshop komen zulke toepassingen voorbij, zoals toegangscontrole in Schiphol of in voetbalstadions.

De in dit rapport onderzochte horizontale relaties omvatten bedrijf-burger en burger-burger interacties. Het zijn, gezien de noodzakelijke kosten en expertise niet geheel verrassend, vooral bedrijven die het initiatief nemen om gezichtsherkenning in te zetten en dan vooral om die burger in zijn of haar hoedanigheid als klant te identificeren. Echter zien wij ook toepassingen die zich richten op de burger-burger relatie, in bijvoorbeeld de vorm van smartphone apps. Aangezien deze apps via aanbieders als Google Play en de App Store van Apple internationaal aangeboden kunnen worden, zijn deze ook dikwijls te gebruiken door Nederlandse burgers. Ook de slimme deurbel voorzien van een gezichtsherkenningsabonnement is een voorbeeld van een toepassing gericht op de burger-burger interactie. Ten slotte blijkt het ook mogelijk te zijn om als burger zelf aan de slag te gaan met gezichtsherkenning. Zo is het mogelijk om met behulp van een gratis proefaanmelding zonder al te veel voorkennis gebruik te maken van basale gezichtsherkennings-technologie. Burgers met enige programmeerkennis die bereid zijn om voor deze diensten te betalen, kunnen ook zelf gezichtsherkenningstoepassingen ontwikkelen.

5.2. Gezichtsherkenning: Wat te verwachten?

Waar Nederland nog volop in de experimenteerfase zit, treffen wij wereldwijd in de burger-burger en burger-bedrijf relaties reeds meer diverse gezichtsherkenningstoepassingen aan, die zich vaak ook al in de implementatiefase bevinden (zie de voorgaande hoofdstukken 3 en 4). De wijze waarop bijvoorbeeld in China de retailsector in toenemende mate gebruik maakt van gezichtsherkenning om klanten een meer efficiënte en persoonlijke dienstverlening te bieden, is er daar één van. Maar ook de steeds verder uitbreidende gezichtsherkenningsdiensten van internationale bedrijven zoals Microsoft en Amazon onderschrijven dat gezichtsherkenning in de lift zit. Deze buitenlandse toepassingen geven ons een idee van wat technisch reeds mogelijk is, wat relevante *use cases* kunnen zijn en wat wij in de nabije toekomst dus mogelijk ook in Nederland kunnen verwachten.

De informatieverzameling ten behoeve van het trainen van gezichtsherkenningsmodellen die voorafgaat aan deze *use cases* is echter reeds wijdverbreid. Het internet vormt hierbij een belangrijke bron. Maar zoals in eerdere hoofdstukken reeds naar voren kwam, ook beeldmateriaal "*in het wild*" –dus verkregen in de publieke en semi-publieke ruimte– wordt hiervoor gebruikt. Omdat dit verzamelen van data zich wereldwijd voordoet, is het zeer moeilijk hierop controle uit te oefenen.

Of en hoe vervolgens specifieke gezichtsherkenningstoepassingen in de Nederlandse context vorm krijgen, is iets wat de Nederlandse overheid wel nog deels in de hand heeft. In de gesprekken die wij hebben gevoerd ten behoeve van de domeinstudies, kwam geregeld naar voren dat bedrijven afwachtend zijn over wat juridisch nu eigenlijk is toegestaan. Bedrijven zijn ook vragende partij als het gaat om specifieke richtlijnen met betrekking tot gezichtsherkenning. Als wij de huidige stand van zaken vergelijken met die in het buitenland (met name buiten de Europese Unie), dan is er dus nog tijd en ruimte om op het toepassingsniveau keuzes te maken.

Wat volgt is dan ook nadrukkelijk niet een opsomming van zekere maar van *mogelijke* ontwikkelingsrichtingen van gezichtsherkenningstoepassingen. Om die reden wordt er gesproken over scenario's. Die scenario's zijn ideaaltypische onderscheidingen. In de praktijk is het zeker mogelijk dat ontwikkelingen gecombineerd plaatsvinden. Ook kunnen de scenario's enigszins extreem of zelfs onrealistisch overkomen. Toch dient dit een belangrijk doel. Immers, scenario's van ongelimiteerde technologische ontwikkeling kunnen verduidelijken waar er grenzen getrokken dienen te worden.

Op basis van de analyse in de vorige hoofdstukken en de expertworkshop onderscheiden wij drie richtingen waarin wij verwachten dat gezichtsherkenning verder ontwikkeld zal worden in de horizontale relatie: voor gemak en efficiëntie (1), beveiliging en controle (2), personalisatie en proactieve dienstverlening (3). Na de beschrijving van de scenario's, volgt een overzicht van de veronderstelde risico's die met deze ontwikkelingen gepaard gaan.

5.2.1. **Gemak en efficiëntie**

Gezichtsherkenningstoepassingen worden op dit ogenblik vooral aan de man gebracht met de belofte bestaande processen soepeler te laten verlopen. De snelle check-in bij evenementen via gezichtsherkenning, het betalen in winkels via gezichtsherkenning en op afstand de toegang tot een huis regelen via de slimme deurbel zijn daar voorbeelden van. Gezichtsherkenning kan ook ingezet worden om bestaande activiteiten te verrijken met extra mogelijkheden. Denk hierbij aan *dating* apps met de mogelijkheid te selecteren op basis van *look-a-likes* van beroemde mensen en de suggesties voor het *taggen* van foto's op sociale media door middel van gezichtsherkenning. Gezichtsherkenningstoepassingen die gericht zijn op gemak (soms in de vorm van vermaak) en efficiëntie zien wij nu het vaakst.

Als deze tendens zich voortzet en samengaat met snellere systemen die ook zelfstandig op draagbare kleine apparaten werken, dan moet men met de mogelijkheid rekening houden dat gezichtsherkenning een prominente plaats zal gaan innemen in het sociale verkeer. Vele smartphone apps die nu reeds de sociale interactie vormgeven, zouden ook een gezichtsherkenningsonderdeel kunnen krijgen. Zo zullen mensen die elkaar nu online leren kennen elkaar ook offline kunnen identificeren. Denk bijvoorbeeld aan het herkennen van huurders en verhuurders via Airbnb, chauffeurs en klanten via Uber, zakelijke contacten op congressen of aspirant geliefden via Tinder. Maar ook andersom biedt gezichtsherkenning mogelijkheden. De grote hoeveelheid aan informatie die de afgelopen jaren online over mensen beschikbaar is geworden, kan gekoppeld worden aan individuen offline wanneer zij via gezichtsherkenning herkend worden; zonder dat zij hier invloed op uit kunnen oefenen. Als gemak en efficiëntie leidend blijven, dan kunnen bovendien alle handelingen die nu nodig zijn om zich te identificeren vervangen worden door gezichtsherkenning. Toegangspassen, bonuskaarten, allerlei wachtwoorden en toegangscodes worden dan overbodig.

5.2.2. **Beveiliging en controle**

Vaak kennen bovenstaande voorbeelden ook een controle- en/of veiligheidscomponent. Inchecken via gezichtsherkenning is niet alleen handig, het biedt in principe ook de mogelijkheid om op basis van zwarte lijsten ongewenste individuen op geautomatiseerde wijze de toegang tot bepaalde ruimtes te ontzeggen. Gezichtsherkenning wordt niet alleen ingezet om foto's te *taggen* maar ook om identiteitsfraude tegen te gaan. Emotiedetectie als een specifieke vorm van gezichtsherkenning kan ook een rol spelen in beveiliging en controle. Wanneer bepaalde emoties zoals angst of boosheid op geautomatiseerde wijze herkend kunnen worden, kan dit aanleiding geven om snel op te treden en escalatie te voorkomen.

Als deze tendens zich voortzet en de accuraatheid en snelheid van de technologie toeneemt, dan moet men met de mogelijkheid rekening houden dat gezichtsherkenning gekoppeld zal worden aan het inperken van toegang tot plaatsen en diensten. Het wordt dan een krachtig

instrument om individuele of groepen burgers te weren en gedrag dat als onwenselijk wordt aangemerkt, tegen te gaan. Zich vrijelijk bewegen door de publieke en semi-publieke ruimte wordt hiermee aan banden gelegd.

5.2.3. **Personalisatie en proactieve dienstverlening**

Gezichtsherkenning kan ten slotte ook ingezet worden om dienstverlening te personaliseren en proactief aan te bieden. Dit zien wij met name terug in de retailsector waar nu al menu's en aanbiedingen aangepast worden op basis van gezichts- en emotieherkenning. Ook in de evenementenindustrie wordt de mogelijkheid om de interactie met bezoekers te personaliseren - op basis van identificatie en/of kenmerken zoals leeftijd en geslacht - een belangrijke meerwaarde van gezichtsherkenning genoemd. Zeker de mogelijkheid om met emotiedetectie geautomatiseerd en *real-time* te kunnen monitoren hoe klanten zich voelen en daar dan proactief op in te kunnen spelen is een toepassing die zowel in het domein van de retail als in de evenementenorganisatie als veelbelovend wordt beschouwd. Zo zou emotiedetectie de mogelijkheid bieden om advertenties en de inrichting van de een winkel of evenement te optimaliseren. Nieuwe functionaliteiten die gepersonaliseerde dienstverlening of advertenties verder verfijnen, zoals het meten van de hartslag op basis van digitale videobeelden van gezichten, maken automatisch analyseren van gezichten nog aantrekkelijker voor deze sectoren.

Als deze tendens zich voortzet, dan moet men met de mogelijkheid rekening houden dat door middel van gezichtsherkenning eerder vergaarde data *real-time* worden gekoppeld aan individuen in de (semi)publieke ruimte met het doel hun handelen te beïnvloeden (ook wel nudging genoemd).[251] Dit kan leiden tot profilering in het dagelijks leven zoals wij dat ook al kennen van op het internet. Niemand krijgt dan nog dezelfde aanbiedingen te zien in winkels en op geautomatiseerde wijze kan er onderscheid gemaakt worden in de manier waarop mensen worden behandeld. Dit beperkt zich niet tot de (semi)-publieke ruimte. Ook in de private sfeer kan gezichtsherkenning ingezet worden ter beïnvloeding van menselijk gedrag. eHealth applicaties die via emotie-detectie aanzetten tot het links laten liggen van alcoholische dranken of die mensen aansporen te gaan sporten behoren tot de mogelijkheden. Gezichtsherkenning wordt dan een belangrijke sleutel om data-gedreven beslissingen te nemen en de keuze-infrastructuur van burgers te beïnvloeden in het dagelijks leven.

5.3. De grootste privacyrisico's nu en in de nabije toekomst

De privacyrisico's die naar voren kwamen in de literatuurstudie en toegespitst werden in de domeinstudies hebben wij geordend aan de hand van de door Solove onderscheiden privacy schendende activiteiten: informatieverzameling, informatieverwerking, informatieverspreiding en

[251] RH Thaler en CR Sunstein, '*Nudge: Improving Health, Wealth, And Happiness'* (Yale University Press 2008).

overschrijding. Bij elk van deze activiteiten konden wij een scala aan voorbeelden van privacy-inbreuken vinden veroorzaakt door gezichtsherkenning (zie hiervoor sectie 3.2 en hoofdstuk 4). Wanneer wij deze risico's nu afzetten tegenover de hierboven genoemde ontwikkelingsrichtingen van gezichtsherkenning, dan zien wij onderstaande privacyrisico's als meest urgent.

5.3.1. Ondoorzichtige informatieverzameling

Gezichtsherkenningsmodellen moeten getraind worden. Hiertoe zijn beelden (video en foto's) nodig. Vaak worden deze van het internet gehaald of via smartphone apps verzameld zonder dat betreffende personen hiervan op de hoogte zijn of hiertoe toestemming hebben gegeven. Maar ook (video)beelden afkomstig van camera's in gebouwen of in de publieke ruimte worden gebruikt om data te verzamelen voor het trainen van algoritmes. Het is aannemelijk dat veel bedrijven een *legacy* probleem hebben: hun gezichtsherkenningstechnologie werkt op basis van modellen die getraind zijn op data waarvoor geen toestemming is gegeven. Het eerste risico op een privacy-inbreuk vindt plaats ruim voordat er sprake is van een duidelijke gezichtsherkenningstoepassing. Het gebeurt dus nu al dat burgers controle verliezen over wat er gebeurt met hun foto's en video's. Dit raakt aan hun communicatieve privacy.

5.3.2. Autonomie onder druk

Voor veel bedrijven betekent goed functionerende gezichtsherkenning dat het frictieloos werkt. Dit wil zeggen dat iemand geen extra handelingen hoeft uit te voeren om de technologie zijn werk te laten doen. Men hoeft geen vingerafdruk te geven, geen ID-kaart te tonen of kortingspas te scannen om geïdentificeerd te worden en gebruik te maken van een dienst of toegang te verkrijgen tot een plaats. Het ontbreken van een actieve handeling ontneemt burgers echter ook een belangrijk keuze – en reflectiemoment. Wil ik dit wel echt? De efficiëntie en het gemak dat gezichtsherkenning mogelijk maakt ondermijnt tegelijk de autonomie en beschikkingsmacht van burgers.

In de situatie dat burgers wel bewust zijn van de gezichtsherkenningsoptie en er de mogelijkheid wordt geboden een dienst te verkrijgen of ruimte te betreden zonder gezichtsherkenning toe te passen, speelt een ander autonomie-ondermijnend mechanisme een rol. Wanneer bedrijven investeren in gezichtsherkenning is het de bedoeling dat dit uiteindelijk rendabel is. Komt de opbrengst niet uit de gezichtsherkenningsapplicatie zelf, dan kan de data verkregen via gezichtsherkenning misschien op andere manieren te gelden gemaakt worden. Er is dus een *incentive* om zoveel mogelijk mensen te verleiden voor de gezichtsherkenningsoptie te kiezen.

Wanneer bovendien massaal gebruik wordt gemaakt van de gezichtsherkenningsvariant, kan dit uiteindelijk ertoe leiden dat het alternatief zonder gezichtsherkenning een zeer uitgeklede optie wordt waar nog maar weinig in wordt geïnvesteerd. Zij die vasthouden aan deze laatste optie

zullen dan met een uitgeklede dienstverlening of basaal functionerend product genoegen moeten nemen. Wat eerst nog een redelijk gelijkwaardige keuze was, verwordt tot een keuze waar, voor het privacyminnende individu, een prijskaartje aan vasthangt. Hierbij speelt sociale druk bovendien ook een rol. Wie gaat stug in de rij staan, als collega's inchecken via gezichtsherkenning? Dit kan leiden tot uitsluiting en stigmatisering.

5.3.3. **Bias en fouten in gezichtsherkenning**

Hoewel de kwaliteit en accuratesse van gezichtsherkenningstechnologie enorm is toegenomen de afgelopen jaren, blijft het een bekend en niet te onderschatten probleem dat onder andere door biases in de trainingsdata, gezichtsherkenningstoepassingen uitkomsten genereren die discriminatoir van aard zijn en minder goed werken bij bepaalde groepen (zoals vrouwen, kinderen, personen met een getinte huidskleur; zie paragraaf 3.1.2). Voor deze groepen is de kans groter dat zij ofwel onjuist of niet herkend worden, met als gevolg dat hen bijvoorbeeld de toegang tot een evenement wordt ontzegd of dat zij geen gebruik kunnen maken van bepaalde diensten. Ook hier ligt uitsluiting en stigmatisering op de loer. Bij categorisatie en emotieherkenning bestaat het risico dat personen uit bepaalde groepen systematisch verkeerd worden geclassificeerd. Dat kan er in minder ernstige gevallen toe leiden dat zij vaker niet passende adviezen of aanbiedingen krijgen, maar meer problematisch wordt het als deze groepen disproportioneel vaak worden benaderd door bijvoorbeeld de beveiliging omdat hun gezichtsexpressie consequent verkeerd wordt geïnterpreteerd. Zodanig raken bias en fouten in de resultaten van gezichtsherkennings-systemen aan meerdere typen privacy, waaronder gedragsmatige en beslissingsprivacy.

5.3.4. **Einde van anonimiteit**

Wanneer gezichtsherkenning in de horizontale relatie wijdverbreid geraakt, zal het de facto niet langer mogelijk zijn voor mensen om zich anoniem in de publieke en semi-publieke ruimte te begeven. Gedragsmatige privacy en de informationele component van ruimtelijke privacy komen hiermee onder druk te staan. Als de democratisering van gezichtsherkenningstechnologie zich doorzet, dan zullen niet alleen bedrijven maar ook burgers onderling gezichtsherkenningstoepassingen kunnen inzetten.

In Nederland heeft naar schatting 92% van de bevolking van 12 jaar en ouder een mobiele telefoon of smartphone.[252] Het feit dat de gezichtsherkenningstechnologie op smartphones kan draaien en via cloud services te verkrijgen is, maakt het bovendien moeilijk om eventuele verboden te handhaven. De mogelijkheid dat burgers zelf aan de slag gaan met gezichtsherkenning en de privacy-implicaties die dat met zich meebrengt, is op dit ogenblik onderbelicht.

[252] Smartphonegebruik in Nederland. <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?dl=2B6DD> geraadpleegd 15 november 2019.

5.3.5. **Afhankelijk van anderen**

Wanneer gezichtsherkenning via bijvoorbeeld apps wordt gebruikt door burgers in het sociale verkeer, dan is men in grote mate afhankelijk van de prudentie van die gebruiker om geen inbreuk te plegen op de privacy van derden. Het vertrouwen in de ander om die privacy te respecteren, berust in eerste instantie op gedeelde waarden en normen die zich vertalen in tal van privacypatronen.[253] Zo houden wij een bepaalde afstand ten opzichte van elkaar in de publieke ruimte en mengen wij ons niet zo snel in gesprekken waar wij geen deel vanuit maken. Deze privacypatronen komen echter onder druk te staan door gezichtsherkenning. Veel burgers vinden het sowieso al moeilijk om in te schatten hoe groot het publiek is dat ze bereiken met het online delen van informatie. Dit probleem wordt door gezichtsherkenning geïntensiveerd. Privacybescherming in de horizontale relatie van burgers is moeilijk top-down te handhaven en zal in grote mate afhangen van het verantwoordelijk gebruik van burgers zelf.

5.3.6. **Van horizontaal naar verticaal: Secundair gebruik van informatie**

Hoewel de focus van dit onderzoek op de horizontale relatie ligt, betreft een belangrijk privacyrisico dat overheden aankloppen bij bedrijven om gebruik te kunnen maken van de gezichtsherkenningsinformatie verzameld in de horizontale relatie. Deze specifieke vorm van secundair gebruik van informatie zagen wij al eerder bij internetbedrijven die –soms dwingende– verzoeken krijgen om informatie te delen met onder meer inlichtingendiensten.[254] Gezien de huidige interesse vanuit overheidsdiensten wereldwijd –bijvoorbeeld gezichtsherkenning om demonstranten in Hongkong te identificeren of gezichtsherkenning ingezet door Amerikaanse politie– en de groeiende maatschappelijke weerstand hiertegen, is het niet ondenkbaar dat indirect –dus via de bedrijven– alsnog gepoogd zal worden gebruik te maken van de opbrengsten van gezichtsherkenningstechnologie. Het waarborgen van privacy in horizontale relaties is dus ook van belang voor het beschermen van privacy in verticale relaties.

5.3.7. **Machtsongelijkheid en *chilling effect***

Gezichtsherkenningstoepassingen die zich richten op controle of personalisatie doen dit eigenlijk altijd in combinatie met andere, reeds bestaande databestanden. Gezichtsherkenning functioneert dan als de sleutel om informatie aan een bepaald persoon te koppelen. Gezichtsherkenning draait

[253]Tamar Sharon en Bert-Jaap Koops, 'Facial recognition and the Ethics of Indifference: Revitalising Civil Inattention As A Privacy-Protecting Mechanism in Public Spaces', (2018) paper workshopped at Amsterdam Privacy Conference 2018; E Keymolen, 'Horizontale Privacy: Een Kwestie van Vertrouwen? Position paper d.d. 9 oktober 2017, ten behoeve van hoorzitting/rondetafelgesprek horizontale privacy, Tweede Kamer' <www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2017A03202#> geraadpleegd.

[254]Zie bijvoorbeeld: Ronald J Deibert, *Black Code: The Battle for the Future of Cyberspace* (Signal/ McClelland & Stewart 2013).

dan niet louter meer om iemand herkennen, maar om het toegankelijk maken van een heel scala aan informatie over hem of haar. De informatierijke profielen die hierdoor ontstaan kunnen de privacy van burgers op verschillende manieren aantasten.

Zo wordt het voor burgers heel moeilijk om in te schatten wat anderen over hen weten. Zich anoniem wanen wordt praktisch onmogelijk. Dit kan leiden tot grote machtsverschillen welke zich niet uitsluitend in de bedrijf-burger interactie maar ook in de burger-burger interactie kunnen afspelen, zo illustreerde de Russische datingapp FindFace (zie Hoofdstuk 3 en 4). Onder meer burgers' associatieve privacy (met wie ze omgaan) en gedragsmatige privacy (*chilling effect*) komt onder druk te staan. Wanneer de door gezichtsherkenning getraceerde informatie bovendien ingezet wordt om iemand te stalken of bedreigen, kan ook de lichamelijke privacy op het spel komen te staan.

Het personaliseren en proactief aanbieden van bepaalde producten via gezichtsherkenning moet mensen tot aankopen verleiden. Hierin speelt emotieherkenning een sleutelrol. Als het mogelijk is om emoties van iemands gezicht af te lezen of iemand te herkennen, kan deze kennis gebruikt worden om de persoon en diens emoties vervolgens te bespelen.

Nu worden mensen altijd wel op een bepaalde manier beïnvloed door hun omgeving. Maar wanneer gezichtsherkenning met dit doel wordt ingezet gebeurt dit op een zeer gepersonaliseerde, niet-transparante en voor de individuele burger moeilijk te doorgronden wijze. Het vrij zijn van de inmenging van derden in het overdenken en vormen van besluiten (mentale privacy) komt hiermee onder druk te staan.

5.4. Conclusie

Centraal in dit hoofdstuk staat de vraag hoe gezichtsherkenningstechnologie nu en in de nabije toekomst ingezet wordt in de horizontale relatie en wat de (te verwachten) privacyrisico's zijn. Wij hebben vastgesteld dat Nederland zich nog in de experimentele fase bevindt als het gaat om de inzet van gezichtsherkenningstechnologie. Er is nog niet sprake van grootschalige toepassingen. In paragraaf 5.2 identificeren wij drie mogelijke ontwikkelingsrichtingen van gezichtsherkennings-toepassingen: voor gemak en efficiëntie (1), beveiliging en controle (2), personalisatie en proactieve dienstverlening (3). Ten slotte schetsen wij zeven privacyrisico's die ontstaan wanneer gezichtsherkenningstechnologie zich ongebreideld kan ontwikkelen (5.3).

6. Rechtsverkenning

Na de beantwoording van de eerste onderzoeksvraag in het vorige hoofdstuk, kunnen wij ons nu richten op de tweede onderzoeksvraag: Hoe kunnen huidige en potentiële privacy-inbreuken worden voorkomen of beperkt? Deze vraag zal in hoofdstuk 7 worden beantwoord. Daartoe verkennen wij in dit hoofdstuk eerst de rechtsgebieden en gestelde normen die mogelijk relevant zijn voor de regulering van gezichtsherkenningstechnologie in de horizontale relatie. Dit hoofdstuk richt zich daarmee op een inventarisatie voor de beantwoording van sub-vraag 2.1: *Kunnen de geïdentificeerde privacyrisico's worden voorkomen of beperkt door bestaande juridische middelen? Zo ja, door welke en hoe? Wat zijn de (mogelijke) juridische lacunes?* Sectie 6.1 richt zich op het recht op privacy en gegevensbescherming, sectie 6.2 op het privaatrechtelijke domein, en 6.3 betreft het strafrecht.

6.1. Recht op privacy en gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG)[255] is van toepassing op delen van het proces die zijn gemoeid met gezichtsherkenning. In deze sub-paragraaf bespreken wij in welke gevallen en op welke punten de AVG van toepassing zal zijn en staan daarna stil bij verschillende vereisten en principes die uit deze wet voortvloeien.

6.1.1 **Toepassingsbereik van de AVG**

De AVG is van toepassing op een gegevensverwerkingsproces als er persoonsgegevens worden verwerkt, de AVG, territoriaal gezien, van toepassing is en er geen uitzondering van toepassing is. Het begrip persoonsgegeven heeft een zeer brede reikwijdte binnen de Algemene Verordening Gegevensbescherming. Er vallen direct identificerende gegevens onder en indirect identificerende gegevens, openbare gegevens en privégegevens, alledaagse gegevens en gevoelige gegevens. Zelfs zogenoemde identificeerbare gegevens, dat wil zeggen gegevens die iemand op dit moment niet kunnen identificeren, maar in de toekomst mogelijk wel, vallen onder het begrip.[256] Daarbij kan worden gedacht aan het geval waarin twee databases op zichzelf geen identificerende gegevens bevatten maar als zij worden samengevoegd wel.[257]

[255] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
[256] Artikel 4 sub a AVG.
[257] Zie over de relatie tot gezichtsherkenning onder meer: Commission Nationale de l'Informatique et des Libertés, Facial recognition - for a debate living up to the challenges, <https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf>.

Bij gezichtsherkenning gaat het voor een flink deel om zogenoemde biometrische gegevens, die in artikel 4 sub 14 van de Algemene Verordening Gegevensbescherming zijn gedefinieerd als

> [P]ersoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

Dit zijn bijzondere (ook wel gevoelige) persoonsgegevens, waarvoor een extra zwaar beschermingsregime van toepassing is.[258] Voor het verwerken van biometrische gegevens geldt een 'nee-tenzij' regime, in tegenstelling tot de verwerking van gewone, niet-bijzondere persoonsgegevens, waarvoor een 'ja-mits' regime geldt. Artikel 9 lid 1 vermeldt:

> Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

In principe mag het verwerken van biometrische gegevens met als doel de identificatie van personen dus niet, tenzij er een uitzondering geldt.

Niet iedere verwerking van foto's en beelden moet worden gezien als een verwerking van biometrische of andere bijzondere persoonsgegevens, zo stelt overweging 51:

> De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.[259]

---

[258] Zie ook Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (01248/07/EN WP136 2007) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>; Article 29 Data Protection Working Party, 'Opinion 02/2012 on Facial Recognition in Online and Mobile Services' (00727/12/EN WP 192 2012) <https://www.pdpjournals.com/docs/87997.pdf>; Article 29 Data Protection Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies' (00720/12/EN WP 193 2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>.

[259] C. Jasserand, 'Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data' (2016) 2 The European Data Protection Law Review 297.

Toch heeft de Hoge Raad in een uitspraak uit 2010 bepaald dat foto's een verwerking van rasgegevens met zich kunnen meebrengen.[260] In deze strengere lijn zou iedere foto waaruit rederlijkwijs iemands ras of etniciteit zou zijn af te leiden zijn aan te merken als een verwerking van bijzondere persoonsgegevens.[261]

De Artikel 29 Werkgroep, het adviesorgaan op het gebied van gegevensbeschermingsrecht in de EU, stelt hieromtrent:

> Foto's en afbeeldingen, zoals die worden gepubliceerd op het internet of worden opgenomen door verkeerscamera's of andere surveillance apparatuur, zijn extra problematisch. Aangezien afbeeldingen onder meer informatie over een persoons etnische afkomst of gezondheidstoestand kunnen onthullen, kunnen zij worden beschouwd als gevoelige gegevens zoals gedefinieerd in artikel 8 lid 1 van de Richtlijn [de voorloper van de AVG], met als gevolg dat ze niet zonder de toestemming van die persoon mogen worden verwerkt.[262]

Ook heeft het College Beschermingsgegevens, de voorloper van de Autoriteit Persoonsgegevens, de handhavende organisatie ten aanzien van het gegevens-beschermingsrecht in Nederland, zich eerder in die zin uitgelaten ten aanzien van slimme camera's.

> Dergelijke camera's identificeren personen aan de hand van gegevensbestanden met unieke gezichtskenmerken. Aangezien het op deze wijze dus mogelijk is om een persoon te identificeren, zijn ook de gezichtskenmerken in de bestanden persoonsgegevens in de zin van de Wbp. Voorts geldt dat verwerkingen door middel van dit soort camera's veelal identificatie tot doel heeft. Dit betekent dat de Autoriteit Persoonsgegevens de camerabeelden dan aanmerkt als rasgegevens in de zin van artikel 16 en 18 Wbp. De verwerking van rasgegevens is verboden behoudens de uitzonderingen die de Wbp noemt in artikel 17 tot en met 23.[263]

---

[260] HR 23 maart 2010, ECLI:NL:HR:2010:BK6331. <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2010:BK6331>.

[261] G J Zwenne en L Mommers, 'Zijn Foto's en Beeldopnamen 'Rasgegevens' in de zin van art. 126nd Sv en art. 18 Wbp?' (2010) 5 Privacy en Informatie 11.

[262] Article 29 Data Protection Working Party, 'Advice paper on special categories of data ("sensitive data")' (2011) <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf>.

[263] College Bescherming Persoonsgegevens, 'Vragen Over Inzet Gezichtsherkenning' (2004) <https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2003-1529.pdf>. In de beleidsregels over cameratoezicht wordt weinig gezegd over de verwerking van biometrische gegevens of gezichtsherkenning: Autoriteit Persoonsgegevens, 'Cameratoezicht: Beleidsregels voor de Toepassing Van Bepalingen uit de Wet bescherming persoonsgegevens en de Wet Politiegegevens (2016) <https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf> en zie ook Autoriteit Persoonsgegevens, 'Biometrie' <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie>.

Een minder verstrekkende interpretatie lijkt te volgen uit een recent richtsnoer van het Europees Comité voor gegevensbescherming, de opvolger van de Artikel 29 Werkgroep.[264] Er is dus bij gezichtsherkenningstechnologie in ieder geval sprake van het verwerken van persoonsgegevens; sterker nog, het zullen vaak zogenoemde 'bijzondere persoonsgegevens' betreffen.

De AVG is van toepassing als deze gegevens worden 'verwerkt'. Het is evident dat er in het geval van gezichtsherkenning sprake is van geautomatiseerde verwerking van persoonsgegevens. Ook is duidelijk dat de AVG territoriaal van toepassing is bij het gebruik van gezichtsherkenningstechnologieën in horizontale verhouding, als het gaat om personen die zich in Nederland bevinden. Derhalve is de AVG in principe van toepassing op gezichtsherkenningstechnologieën in horizontale verhoudingen in Nederland.

Als gezichtsherkenning wordt gebruikt door een persoon of organisatie, dan kan er evenwel een uitzondering van toepassing zijn. Voor dit onderzoek is van belang de zogenoemde huishoudelijke exceptie.[265] Zoals overweging 18 aangeeft:

> Deze verordening is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon in het kader van een louter persoonlijke of huishoudelijke activiteit die als zodanig geen enkel verband houdt met een beroeps- of handelsactiviteit. Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten. Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.

Omdat zowel artikel 2 AVG als deze overweging *louter* spreekt van persoonlijke of huishoudelijke doeleinden moet deze uitzondering restrictief worden begrepen. Ook is deze uitzonderingsgrond in de jurisprudentie restrictief uitgelegd. Daarbij zijn met name twee zaken van het Europees Hof van Justitie van belang.

De ene restrictie volgt uit de zaak Bodil Lindqvist uit 2003, waar een persoon een soort persoonlijke hobbypagina bijhield op het internet en daarop ook informatie en wetenswaardigheden over kennissen en collega's deelde, zoals onder meer dat een van hen en been had gebroken. De vraag was of een dergelijke handeling onder de huishoudelijke exceptie viel, nu het doeleinde waarvoor de gegevens werden verwerkt primair persoonlijk was en de internetpagina vooral voor de persoon zelf en een kleine kring bekenden was bedoeld. Het Hof van Justitie ging daar echter niet in mee en stelde dat: "Die uitzondering moet derhalve aldus worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of

[264] EDPB. 'Guidelines 3/2019 on processing of personal data through video devices' (2019). <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf>.
[265] Artikel 2 lid 2 sub c AVG.

gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van persoonsgegevens die bestaat in hun openbaarmaking op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt."[266] Het openbaar maken van gegevens aan een onbepaalde groep mensen is derhalve in ieder geval geen verwerking voor puur persoonlijke of huishoudelijke doeleinden, al was het maar omdat de verdere verwerking niet kan worden begrensd voor wat betreft die doeleinden.

Ook als persoonlijke informatie wordt gedeeld met mensen buiten een kleine kring van vrienden en familieleden zal de verwerking niet snel onder de huishoudelijke exemptie vallen. Zo gaf de voormalig Artikel 29 Werkgroep, het adviesorgaan op het gebied van gegevensbescherming in de Europese Unie, bijvoorbeeld ten aanzien van Social Network Sites (SNS) aan dat die sites:

> standaard en gratis privacyvriendelijke settings dienen te hanteren die de toegang tot informatie limiteren tot de door gebruikers geselecteerde contacten. Wanneer toegang tot profielinformatie verder gaat dan deze contacten, zoals wanneer toegang tot het profiel wordt geboden aan alle deelnemers van een SNS of wanneer de data wordt geïndexeerd door zoekmachines, dan gaat de toegang verder dan de persoonlijke of huishoudelijke sfeer. Als een gebruiker zelf informatie deelt buiten de cirkel van geselecteerde vrienden, dan zal hij als verantwoordelijke worden aangemerkt. Effectief zal dan hetzelfde juridische regime van toepassing zijn als wanneer een persoon een ander technologisch platform gebruikt om persoonlijke informatie te publiceren op het web.[267]

Een tweede begrenzing volgt uit de zaak Rynes uit 2013. Daarin stond centraal een persoon die een camera had gericht op de toegang tot zijn erf, voor veiligheidsdoeleinden. Wederom was de vraag of deze toepassing onder de huishoudelijke exceptie viel, nu het doel van de werking van persoonsgegevens (in casu van mensen die toegang zochten tot het huis) primair van persoonlijke aard was en de gegevens niet waren bedoeld om openbaar te worden gemaakt. Toch oordeelde het Hof van Justitie ook in deze zaak anders.

> Voor zover het gebruik van een videobewakingssysteem, zoals dat in het hoofdgeding, de openbare ruimte bestrijkt – zelfs gedeeltelijk – en hierdoor buiten de privésfeer geraakt van degene die door middel van dit systeem gegevens verwerkt, kan het niet worden beschouwd als een activiteit die met uitsluitend "persoonlijke of huishoudelijke doeleinden" wordt verricht'.[268] Datzelfde geldt waarschijnlijk, mutatis mutandis, voor gevallen waarin

[266] Hof Göta hovrätt – Zweden 6 november 2003, ECLI:EU:C:2003:596 ro 47.
[267] Article 29 Data Protection Working Party, 'Opinion 5/2009 on online social networking' (01189/09/EN WP163 2009) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf>. Citaat vertaald door auteurs.
[268] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, ro 33.

niet de openbare ruimte, maar de privéruimtes van anderen worden gefilmd. Dat betekent dat in zoverre er opnames worden gemaakt ten behoeve van gezichtsherkenning in ruimtes buiten de privésfeer van de eigenaar en daar persoonsgegevens worden verzameld, er vermoedelijk geen beroep op de huishoudelijke exceptie kan worden gedaan, ongeacht het doeleinde (bijvoorbeeld recreatief en dus van persoonlijke aard) van de verwerking.[269]

Voor wat betreft het gebruik van gezichtsherkenning door burgers, bijvoorbeeld door een slimme deurbel of app kan de huishoudelijke exceptie van toepassing zijn, zolang de beelden van gezichten maar niet worden geregistreerd in de openbare ruimte, niet worden gebruik voor andere dan persoonlijke doeleinden en niet worden gedeeld met een groep groter dan een beperkte kring van familieleden of vrienden. Voor een apparaat zoals de slimme deurbel moet dan wel in overweging worden genomen waar de verwerking van de data plaatsvindt. In het geval van de in sectie 3.3 besproken Nest deurbel worden persoonsgegevens momenteel verwerkt op de servers van Nest. Het is in zo'n geval onduidelijk of de huishoudelijke exceptie op zou kunnen gaan.

6.1.2 **Noodzakelijk, proportioneel en subsidiair**

Als de AVG van toepassing is dan volgt daaruit dat de persoon of organisatie die gezichtsherkenningstechnologieën gebruikt, de verantwoordelijke genoemd, aan tal van plichten en rechten gebonden is. Fundamentele rechten als het recht op gegevensbescherming mogen alleen worden ingeperkt als er aan een aantal voorwaarden is voldaan. Daarbij zijn in de context van gezichtsherkenningstechnologieën onder meer de volgende principes van belang:

1. De inperking moet noodzakelijk zijn om een legitiem doel te bereiken. Wat noodzakelijk is hangt van de context af.
2. De inperking moet proportioneel zijn. Dat wil zeggen dat de inbreuk op het fundamentele recht in verhouding moet staan tot het doel. Dat is belangrijk in de context van het onderzoek, omdat het verwerken van biometrische gegevens heeft te gelden als een verwerking van bijzondere persoonsgegevens en dus alleen zal zijn toegestaan in uitzonderlijke gevallen.
3. De verwerking moet voldoen aan het subsidiairiteitsvereiste. Dat wil zeggen dat het gekozen middel het minst inbreukmakende middel is dat voor handen is. Ook dat ligt niet altijd voor de hand bij gezichtsherkenningstechnieken, zeker niet in horizontale

[269] De voormalige Artikel 29 Werkgroep heeft zich zelfs laten ontvallen dat de huishoudelijke exceptie wellicht verder zou moeten worden beperkt. 'The regulation should differ from the current Directive in that all processing of personal data performed – even for exclusively personal or household purposes – should to some extent come within the scope of the Regulation.' Proposals for Amendments regarding exemption for personal or household activities <www.ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.

verhoudingen, aangezien er vaak goede alternatieven beschikbaar zijn. Een eenduidige onderbouwing voor het gebruik van gezichtsherkenningstechniek ontbreekt in de huidige praktijk dikwijls.

4. De inperking moet effectief zijn. Dat wil zeggen, het moet duidelijk zijn dat het verwerken van persoonsgegevens ook echt effectief is in relatie tot het te bereiken doel.

De Uitvoeringswet AVG (UAVG), die de AVG binnen de Nederlandse context in- en aanvult op punten waarop de AVG dat toestaat, zoals met betrekking tot de regels aangaande de verwerking van bijzondere persoonsgegevens, geeft één algemene uitzonderingsgrond op het verbod om biometrische gegevens te verwerken en één specifieke.

De algemene bepaling geeft aan dat het verwerken van biometrische gegevens mag als:

- de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;
- de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;
- de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt; of
- de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.[270]

Binnen het kader van dit onderzoek is eigenlijk alleen de eerste uitzonderingsgrond, de uitdrukkelijke toestemming, van belang, aangezien de andere algemene uitzonderingsgronden vrijwel nooit van toepassing zijn in horizontale verhoudingen. De vraag is of toestemming als

[270] Artikel 22 UAVG. Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming).

legitieme uitzonderingsgrondslag snel van toepassing zal zijn in het geval van gezichtsherkenningstechnologieën. Zo stelt ook de regering in de Memorie van Toelichting:

> In de publieke en private sector zijn biometrische systemen sterk in opkomst voor bijvoorbeeld het reguleren van de toegang tot bepaalde plaatsen en gebouwen, maar ook toegang tot informatiesystemen. Veel voorkomend is de situatie waarin bijvoorbeeld klanten of werknemers zich identificeren met behulp van biometrie. De huidige rechtsgrondslag hiervoor is het gerechtvaardigd belang van de verwerkingsverantwoordelijke, opgenomen in artikel 8, onderdeel f, van de Wbp. Hoewel deze rechtsgrondslag ook is opgenomen in artikel 6, eerste lid, onderdeel f, van de verordening zal deze zonder nadere lidstatelijke regeling geen basis kunnen zijn voor verwerking van biometrische gegevens, omdat biometrische gegevens straks onder het verbod van artikel 9, eerste lid, van de verordening vallen. Net als bij andere bijzondere categorieën van persoonsgegevens is het onder omstandigheden ook bij biometrische gegevens mogelijk om de toestemming van de betrokkene als grondslag te hanteren voor het verwerken, maar hiervoor is wel vereist dat betrokkene de toestemming in vrijheid kan geven (op grond van artikel 9, tweede lid, onderdeel a, van de verordening jo. het voorgestelde artikel 22, tweede lid, onderdeel a). Of deze toestemming in vrijheid wordt gegeven, hangt af van de omstandigheden van het geval. In de relatie tussen klant en aanbieder zal in sommige gevallen wel kunnen worden uitgegaan van de vrije toestemming. Juist in de relatie tussen werknemer en werkgever zal de werknemer in de praktijk in redelijkheid echter nauwelijks toestemming kunnen weigeren, zeker wanneer de toegang tot bepaalde plaatsen noodzakelijk is voor de uitoefening van de werkzaamheden, in het bijzonder de toegang tot specifieke plaatsen, gebouwen, apparatuur en informatiesystemen.[271]

De European Data Protection Board stelt in haar richtlijn die momenteel ter publieke consultatie is vrijgegeven ten aanzien van gevallen waarin de verwerking wordt gebaseerd op de geïnformeerde toestemming van het datasubject dat er altijd een redelijk alternatief voorhanden moet zijn:

> [W]anneer toestemming is vereist door artikel 9 AVG, zal de verantwoordelijke de toegang tot zijn diensten niet afhankelijk maken van het accepteren van de verwerking van biometrische gegevens. In andere woorden en met name wanneer biometrische gegevens worden gebruikt voor authenticatiedoeleinden, dient de verantwoordelijke een alternatief aan te bieden dat niet afhankelijk is van het verwerken van biometrische gegevens – zonder beperkingen of additionele kosten voor het datasubject.[272]

[271] *Kamerstukken II* 2017–2018, 34 851, 3.
[272] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data through Video Devices' (2019) <www.edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf>

Omdat, zoals ook zal blijken uit de volgende paragraaf, legitieme toestemming voor de verwerking van biometrische gegevens niet snel als uitzonderingsgrond zal kunnen dienen voor gezichtsherkenningstechnologieën zou dit betekenen dat het gebruik van dergelijke technologieën zelden legitiem zou zijn onder de AVG. Dit vond de regering onwenselijk.

> Het afzien van een nationale uitzondering voor biometrische gegevens zou, gelet op het voorgaande, betekenen dat de bestaande ontwikkelingen in het gebruik van biometrie als identificatiemiddel sterk gehinderd zouden worden. Bestaande verwerkingen van biometrische gegevens, zoals bijvoorbeeld die in de relatie tussen werkgever en werknemer zouden hun rechtsgrondslag verliezen. Dit is niet wenselijk.[273]

Daarom heeft het nog een specifieke bepaling toegevoegd voor de legitieme verwerking van biometrische gegevens. “Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.”[274]

Evenwel is de regering in de Memorie van Toelichting tamelijk strikt ten aanzien van het vereiste van noodzakelijkheid, proportionaliteit en subsidiariteit.

> Er dient wel een afweging te worden gemaakt of identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De werkgever zal dan moeten afwegen of de gebouwen en informatiesystemen zodanig beveiligd moeten zijn dat dit met biometrie dient plaats te vinden. Dit zal het geval zijn als de toegang beperkt dient te zijn tot bepaalde personen die daartoe geautoriseerd zijn, zoals bij een kerncentrale. Het verwerken van biometrische gegevens dient ook proportioneel te zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Aan de andere kant kan biometrie soms juist een belangrijke vorm van beveiliging zijn voor bijvoorbeeld informatiesystemen, die zelf veel persoonsgegevens bevatten, waarbij onrechtmatige toegang, ook van werknemers, moet worden voorkomen. Om deze afweging mogelijk te maken in omstandigheden waarin toestemming niet in vrijheid kan worden gegeven, is in het wetsvoorstel een bepaling opgenomen die een uitzondering op het verbod voor verwerking van biometrische gegevens mogelijk maakt met het oog op de identificatie van de betrokkene, indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Uit

[273] *Kamerstukken II* 2017–2018, 34 851, 3.
[274] Artikel 29 UAVG.

> artikel 32 van de verordening vloeit onder meer reeds voort dat in dat geval passende technische en organisatorische maatregelen moeten worden getroffen ter beveiliging van deze gegevens.[275]

Dit betekent dat gezichtsherkenningstechnologieën alleen kunnen worden gebaseerd op de algemene grond van legitieme toestemming (zie volgende paragraaf) of op de specifieke grond van de inzet van gezichtsherkenningstechnologieën voor authenticatie- of beveiligingsdoeleinden. De regering legt daarbij de nadruk op het feit dat die technologie noodzakelijk, proportioneel en subsidiair moet zijn en verwijst daarbij naar het voorbeeld van een kerncentrale. Alhoewel het evident is dat niet slechts kerncentrales of vergelijkbare faciliteiten een beroep kunnen doen op de specifieke verwerkingsgrond is wel duidelijk dat de lat hoog ligt.

Daarnaast moet worden bedacht dat de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit, zoals onder meer is uitgewerkt in het dataminimalisatiebeginsel,[276] dat luidt dat persoonsgegevens toereikend dienen te zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, ook geldt als de legitieme verwerkingsgrond de expliciete toestemming van het datasubject is gegeven. De AVG geeft ter nadere duiding aan dat persoonsgegevens alleen mogen "worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt."[277] Wat redelijk is en wat niet, kan niet exact worden bepaald, maar duidelijk is dat hier restrictief naar moet worden gekeken.

Stel een sportcentrum biedt klanten de mogelijkheid om in plaats van met een pasje, toegang te verkrijgen tot de faciliteit door gebruikmaking van de gezichtsherkenningstechnologie en een klant gaat hiermee akkoord. Dan nog kan het zijn dat deze toepassing niet legitiem is omdat er een redelijk alternatief beschikbaar is, namelijk het werken met toegangspasjes waarvoor slechts een minimaal aantal gegevens hoeft te worden verwerkt. De toestemming doet niets af aan het vereiste van noodzakelijkheid, proportionaliteit en subsidiariteit.

Tot slot kan hier nog worden verwezen naar de zaak Manfield, waarin de introductie van een vingerscanautorisatiesysteem werd ingevoerd door een schoenenwinkel. De rechter oordeelde daarbij als volgt:

> Manfield heeft verder aangevoerd dat de noodzaak van het gebruik van een vingerscanautorisatiesysteem bestaat uit het beveiligen van gevoelige informatie die via haar kassasysteem toegankelijk is; informatie die zowel betrekking heeft op financiën, persoonsgegevens van klanten en persoonsgegevens van werknemers. Daarbij wijst Manfield er verder op dat zij ook vanuit haar verplichting om voormelde gegevens zo veilig mogelijk te verwerken belang heeft bij invoering van het vingerscanautorisatiesysteem.

[275] *Kamerstukken II* 2017–2018, 34 851, 3
[276] Artikel 5 AVG.
[277] Overweging 39 AVG.

Daardoor wordt ongeoorloofd inloggen door derden van buitenaf en/of het ongeoorloofd "afkijken" van een inlogcode voorkomen. [verzoeker 2] heeft de noodzaak om in verband hiermee een vingerscanautorisatiesysteem in te voeren gemotiveerd bestreden. Alternatieven zoals toegangspas, werknemerspas en/of cijfercodes, al dan niet in combinatie met elkaar, zijn naar haar oordeel onvoldoende onderzocht. Via een dergelijk systeem is zonodig een "dubbele" waarborg te realiseren die naar haar oordeel geen inbreuk maakt op de privacy. Naar het oordeel van de kantonrechter heeft Manfield dit argument van [verzoeker 2] niet of onvoldoende bestreden en heeft zij evenmin, bijvoorbeeld aan de hand van documenten, onderbouwd waarom, met afweging van voors en tegens van verschillende systemen, zij heeft gekozen voor het vingerscanautorisatiesysteem. Om te kunnen toetsen aan de voorwaarden van noodzakelijkheid en proportionaliteit die artikel 29 UAVG aan het toelaten van een uitzondering op de hoofdregel van het verbod van verwerking van biometrische gegevens stelt, had dat wel op haar weg gelegen.[278]

6.1.3 **Uitzonderingsgrond**

Artikel 9 lid 1 AVG geeft aan dat de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon, verboden is. Lid 2 geeft vervolgens tien uitzonderingsgronden. De UAVG geeft, naast de eerde besproken specifieke uitzondering voor het verwerken van biometrische gegevens voor authenticatie en beveiligingsdoeleinden, aan dat slechts vijf algemene gronden een legitieme basis kunnen vormen voor het verwerken van biometrische gegevens, waarvan, zoals eerder gesteld, slechts toestemming relevant is voor gezichtsherkenningstechnologieën in horizontale verhoudingen. Daarbij geven artikel 4 sub 11 en artikel 8 AVG vrij stringente eisen voor een legitieme toestemming:

1. *Vrij*: Ten eerste moet de toestemming 'vrij' zijn gegeven door een datasubject. Als een persoon zijn gegevens moet afgeven voor het verkrijgen van een bepaalde dienst, voor toegang tot een website of voor de levering van een product, dan kan dit betekenen dat de toestemming niet vrij is.
2. *Specifiek*: Daarnaast moet de toestemming 'specifiek' zijn. Dat betekent dat toestemming niet legitiem zal zijn in het geval een bedrijf een datasubject middels een algemeen contract of algemene voorwaarden toestemming vraagt voor het verwerken van 'alle relevante' gegevens of voor algemene doelen zoals 'commerciële doeleinden'. Specifieke toestemming betekent dat het duidelijk moet zijn welke gegevens er precies worden verzameld, waarvoor die precies worden gebruikt en waarom die gegevens nodig zijn voor dat doel.

[278] Rechtbank Amsterdam 12-08-2019, ECLI:NL:RBAMS:2019:6005.

3. *Geïnformeerd*: De toestemming moet 'geïnformeerd' zijn. Het datasubject moet geïnformeerd worden over welke gegevens er worden verwerkt, voor welke doeleinden en hoe ze worden gebruikt. De organisatie die gegevens verwerkt, moet ervoor zorgen dat het datasubject redelijkerwijs kan begrijpen wat er staat. Een twintig pagina's tellende verklaring in juridisch jargon is dus niet voldoende. Eerder moet worden gedacht aan een halve pagina aan informatie in simpele taal die een gemiddelde burger begrijpt en die niet veel tijd kost om te lezen.
4. *Ondubbelzinnig*: De toestemming moet 'ondubbelzinnig' zijn. Een handtekening is doorgaans een duidelijke vorm van toestemming; een 'I agree'-knop op een website die wordt aangeklikt kan dat ook zijn. Belangrijk is hoe dan ook dat de toestemming expliciet wordt gevraagd voor het verwerken van de persoonsgegevens en dat deze verwerking niet volgt uit de kleine lettertjes van een contract met een ander doel.
5. *Bewijsbaar*: De toestemming moet bewijsbaar zijn. Het is aan de verantwoordelijke voor de gegevensverwerking om aan te tonen dat het datasubject inderdaad zijn toestemming heeft gegeven en dat dit legitiem is gebeurd. Als er dus een juridisch conflict is, dan is er een omkering van de bewijslast. Niet het datasubject moet aantonen dat hij geen (legitieme) toestemming heeft gegeven, maar het is aan de dataverwerkende organisatie om aan te tonen dat dit wel is gebeurd.
6. *Minderjarigen*: Voor kinderen op het internet geldt dat hun toestemming niet rechtsgeldig is, maar dat er toestemming moet zijn van hun ouders of wettelijk vertegenwoordigers. De verantwoordelijke moet ervoor zorgen dat in het geval van een kind inderdaad toestemming is gegeven door een wettelijk vertegenwoordiger. Waar de leeftijdsgrens precies wordt gelegd moet per situatie en land worden bekeken; de AVG spreekt van maximaal 16 en minimaal 13 jaar. In Nederlands is middels de Uitvoeringswet AVG gekozen voor de grens van 16 jaar.
7. *Uitdrukkelijk:* Tot slot geeft artikel 9 lid 2 nog een extra vereiste voor toestemming ten aanzien van de verwerking van bijzondere persoonsgegevens, namelijk dat die uitdrukkelijk moet zijn gegeven.

Het is niet uitgesloten dat toestemming voor een gezichtsherkenningsapplicatie zal worden gegeven conform deze vereisten. Toch zal een aantal punten goed moeten worden nagelopen per specifiek geval en context.

Ten eerste is de vraag hoe vrij de toestemming is gegeven, bijvoorbeeld in werkgever-werknemerrelaties, zoals aangestipt in de vorige paragraaf. Ook in de relatie tussen klant en bedrijf, in het bijzonder als er een evident machtsverschil is of het bedrijf een monopoliepositie heeft, of in burger-burger relatie waar er een evident verschil is in positie (hulpbehoevende oudere-verzorgend kind, minderjarig kind-ouder, etc.) kan het lastig zijn om aan het vereiste van een vrij gegeven toestemming te voldoen. Ook is de vraag of de alternatieven die de klant worden geboden

redelijk zijn. Het is de vraag of een sportcentrum dat acht toegangspoortjes neerzet voor klanten met toegang op basis van gezichtsherkenningstechnologie en slechts 1 voor toegang op basis van een sportkaart, waardoor er voor dat poortje altijd een lange wachtrij staat, een redelijk alternatief biedt. Derhalve is het niet zeker dat de eventuele toestemming die de klant geeft voor de verwerking van zijn biometrische gegevens, bijvoorbeeld voor een snelle check in bij events, juridisch gezien vrij gegeven is.

Ten tweede is de vraag in hoeverre de gemiddelde burger echt begrijpt waar hij toestemming voor geeft als hij akkoord gaat met het verwerken van zijn biometrische gegevens voor gezichtsherkenningstechnologieën. Het betreft immers zeer complexe materie, waarvan op voorhand niet altijd evident is op welke wijze de technologie zal worden ingezet en op welke wijze biometrische gegevens daarvoor zullen worden ingezet. Zeker als de technologie wordt ingezet in burger-burger relaties vergt het van de burger die deze technologie gebruikt de nodige kennis en kennisoverdracht over de precieze werking en de daaraan verbonden risico's van deze techniek.

Ten derde zal de toestemming specifiek moeten zijn, met daarbij een duidelijke uitleg aan de burger waarom er gezichtstechnologie wordt gebruikt, welke gegevens daarvoor noodzakelijk zijn en hoe de technologie in elkaar steekt.[279]

6.1.4 **Automatische besluitvorming en datakwaliteit**

Veel van de gezichtsherkenningstechnieken worden gebruikt voor geautomatiseerde, dat wil zeggen computergestuurde, besluitvormingsprocessen. Artikel 22 van de AVG stelt, voor zover hier relevant, dat de betrokkene het recht heeft niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Dit verbod geldt niet als de betrokkene zijn uitdrukkelijke toestemming heeft gegeven of de besluitvorming een doel van zwaarwegend algemeen belang dient. Dat laatste zal zelden het geval zijn en het is, zoals in de vorige paragraaf uitgelegd, bepaald niet evident dat de burger zijn uitdrukkelijke toestemming geeft voor dergelijke technieken en eventuele daarop gebaseerde besluitvormingsprocessen. Dit recht (of eigenlijk plicht van de verantwoordelijke) is alleen van toepassing als het gaat om belangrijke besluiten, zoals een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Bij onbelangrijke handelingen - zoals het aanbieden van advertenties op basis van profielen - geldt deze plicht niet.[280] In horizontale verhoudingen wordt gezichtsherkenning nog maar zelden ingezet op een wijze die de burger in aanmerkelijke mate treft, waardoor deze verbodsbepaling vooralsnog van beperkt belang is.

[279] Zie over toestemming ook: Zaak C-673/17 Europees Hof van Justitie, ECLI:EU:C:2019:801.
[280] Artikel 40 van de UAVG geeft uitzonderingen op verbod geautomatiseerde individuele besluitvorming voor zover die noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.

Daarnaast geeft artikel 5 AVG aan dat de gegevens die worden verzameld, correct en up-to-date moeten zijn. Dit is een plicht voor de organisatie die de gezichtsherkenningstechnologie inzet. Daaraan correlerend heeft het individu het recht om gegevens die incorrect zijn aan te (laten) passen en gegevens die onvolledig zijn aan te (laten) vullen, zo volgt uit artikel 16 AVG.

De portee van beide bepalingen is dat als er gegevens over een persoon worden verwerkt en er besluiten over een persoon worden genomen op basis van deze gegevens, er in ieder geval dient te worden gezorgd dat die gegevens zelf kloppen en dat een algemeen profiel of statistische correlatie, op basis waarvan een algoritme of computerprogramma een besluit neemt over een individueel geval, ook inderdaad van toepassing is op dat specifieke geval. Dit uitgangspunt is belangrijk omdat veel van de gezichtsherkenningstechnologieën die momenteel op de markt komen nog een hoge foutmarge hebben. Dit kan überhaupt problematisch zijn, gezien het vereiste van datakwaliteit, en zal des te knellender zijn als dergelijke technologieën worden gebruikt voor toepassingen waar belangrijke gevolgen aan gekoppeld zijn voor het datasubject.

6.1.1. **Transparantie**

Dan is tot slot nog relevant het principe dat gegevensverwerking transparant moet geschieden.[281] Dit principe is verder uitgewerkt in een tweetal artikelen in de Algemene Verordening Gegevensbescherming.[282] Allereerst het geval waarin gegevens direct worden verkregen van of door middel van observatie van personen waarover persoonsgegevens worden verzameld en anderzijds het geval waarin die gegevens op een andere weg worden verkregen, bijvoorbeeld via derden. De European Data Protection Board, de opvolger van de eerder genoemde Article 29 Working Party, stelt in dit verband dat onder de eerste categorie onder meer moet worden meegenomen de situatie waarin: “een verwerkingsverantwoordelijke persoonsgegevens van een natuurlijk persoon verzamelt door middel van observatie (bijvoorbeeld door gebruik te maken van apparatuur of software programma’s die geautomatiseerd data verzamelen, zoals camera’s, netwerkapparatuur, Wi-Fi tracking, *Radio-Frequency Identification* (RFID) of andere type sensoren.” [283] Daarvan zal zeker sprake zijn in het verband van gezichtsherkenningstechnologieën.

Dat betekent dat de personen over wie gegevens worden verzameld op de hoogte moeten worden gesteld van het feit dat er gegevens over hen worden verzameld, niet later dan het moment van de verzameling zelf. De informatie die dient te worden verstrekt aan ieder datasubject behelst onder meer de identiteit en de contactgegevens van de verantwoordelijke, de verwerkingsdoeleinden en de legitieme verwerkingsgrond, de bewaartermijn voor de gegevens en

[281] Artikel 5 lid 1 sub a AVG.
[282] Artikel 13 en 14 AVG.
[283] Vertaald uit het Engels door auteurs. European Data Protection Board, ‘Guidelines on Transparency under Regulation 2016/679’ (17/EN WP260 rev.01 2017) <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025>.

de diverse rechten van de personen over wie gegevens worden verzameld. Belangrijk is dat hier ook onder valt uitleg over de onderliggende logica, alsmede het belang en de verwachte gevolgen van geautomatiseerde besluitvorming en profiling.

Kritisch hierbij is dat de informatie moet worden verstrekt voordat of op het moment dat de gegevens worden verzameld, opgeslagen, geanalyseerd of gebruikt. Dat betekent dat iedere vorm van heimelijk gebruik van gezichtsherkenningstechnologie, waarbij degene wiens gezicht wordt herkend of *gematched* daarvan niet expliciet op de hoogte is gesteld uiterlijk op het moment dat dit gebeurt, in principe verboden is. De enige uitzondering die in de AVG wordt geboden staat in artikel 85 AVG, die lidstaten de mogelijkheid geeft om op dit punt een uitzondering te bieden. De UAVG heeft deze mogelijkheid echter beperkt uitgelegd. Terwijl de AVG naast het verwerken van persoonsgegevens voor artistieke, journalistieke, academische en soortgelijke doeleinden ook refereert aan het algemene recht op informatieverzameling en -verspreiding in het kader van de vrijheid van meningsuiting, legt de UAVG slechts begrenzingen neer ten aanzien van, onder meer, de transparantieplicht in het kader van de eerdergenoemde specifieke doeleinden. Binnen het gegevensverwerkingsrecht geldt in horizontale relaties ten aanzien van gezichtsherkenningstechnologieën dus slechts een uitzondering op de transparantieplicht voor zover het gaat om gegevensverwerking voor uitsluitend journalistieke doeleinden en ten behoeve van uitsluitend academische, artistieke of literaire uitdrukkingsvormen. Uit deze studie is niet naar voren gekomen dat gezichtsherkenning inderdaad op grote schaal voor deze doeleinden wordt gebruikt. Voor het gebruik van gezichtsherkenning voor andere doeleinden, die wel in deze studie aan bod zijn gekomen, is geen uitzondering op de transparantieplicht binnen het gegevensbeschermingskader.

6.1.2. **Conclusie**

Op basis van onze verkenning van de AVG concluderen wij dat de AVG doorgaans van toepassing zal zijn op gezichtsherkenningstechnologie. Daaruit volgt dat de inzet van dergelijke technologie noodzakelijk, proportioneel en subsidiair moet zijn. Dit lijkt vooralsnog het grootste obstakel voor de legitimiteit van gezichtsherkenning, omdat voor veel toepassingen redelijke alternatieven zijn waar minder persoonsgegevens en minder gevoelige persoonsgegevens voor hoeven te worden verwerkt.

Daarnaast moet er sprake zijn van een legitieme verwerkingsgrondslag. Daarvan zal enerzijds sprake zijn als de technologie wordt ingezet voor authenticatie en beveiligingsdoeleinden van kritische infrastructuur. Voor de toepassing in horizontale relaties lijkt de enige relevante grond anderzijds slechts de specifieke, vrije, uitdrukkelijke, geïnformeerde en ondubbelzinnige toestemming van het datasubject. Alhoewel het niet is uitgesloten dat daar in bepaalde gevallen sprake van kan zijn, is ook duidelijk dat veel contexten, zoals de werkgever-werknemer relatie, zich daar slecht voor lenen. Beide verwerkingsgrondslagen hebben in ieder geval tot gevolg dat

gezichtsherkenning slechts mag worden ingezet in beperkte en gecontroleerde omgevingen en niet, bijvoorbeeld, in de openbare ruimte waar er geen controle is over wiens biometrische gegevens worden verwerkt. Dat volgt ook uit het vereiste van transparantie dat in de Algemene Verordening Gegevensbescherming is vervat.

Tot slot is ook van belang dat de data die over burgers worden verwerkt correct zijn en dat de eventuele gevolgen die aan de inzet van gezichtsherkenning zijn gekoppeld, gestoeld zijn op juiste aannames over die specifieke casus in dat specifieke geval. Alhoewel in de toekomst gezichtsherkenningstechnologieën wellicht accurater en betrouwbaarder worden, zijn er vooralsnog tekenen dat de betrouwbaarheid van gezichtsherkenning in veel gevallen nog te wensen overlaat.

Dan tot slot nog een viertal recente ontwikkelingen. Ten eerste, in een brief van 31 oktober 2019, aangaande voornemens met betrekking tot de UAVG en AVG, stelde de minister:

> Op grond van artikel 29 UAVG is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Deze uitzondering stoelt op de mogelijkheid die artikel 9, eerste lid, onder g, AVG, biedt om bij lidstatelijk recht een uitzondering te maken op voornoemd verbod. De uitzondering dient noodzakelijk te zijn om redenen van zwaarwegend algemeen belang en aan de overige, in dit verband verder niet relevante voorwaarden uit dit artikel te voldoen. Tijdens een ambtelijk gesprek over de wijze waarop Nederland de UAVG heeft vormgegeven, was de Europese Commissie kritisch over het feit dat in de tekst van artikel 29 UAVG zelf geen verwijzing is opgenomen naar het voornoemde zwaarwegende algemeen belang dat met de in artikel 29 UAVG vastgelegde uitzondering is gediend. De voorbeelden en uitleg, zoals opgenomen in de artikelsgewijze toelichting van artikel 29 UAVG, vond de Commissie niet afdoende. Om tegemoet te komen aan deze kritiek is het wenselijk in artikel 29 UAVG expliciet het belang te benoemen dat in de rechtspraktijk noodzakelijk kan maken om biometrische gegevens te verwerken voor authenticatie en beveiligingsdoeleinden. Het betreft hier het belang van een rechtmatige toegang tot bepaalde plaatsen, gebouwen, informatie- of werkprocessystemen, diensten of producten. Een dergelijke aanvulling van artikel 29 zou bijdragen aan de rechtszekerheid bij het verwerken van biometrische gegevens voor genoemde doeleinden en kan daarmee de gewenste duidelijkheid bieden over een punt van aandacht dat door VNO-NCW en MKB-Nederland naar voren is gebracht.[284]

[284] Dekker, S. “Kamerbrief over aanpassingen UAVG en evaluatie AVG”, 31 oktober 2019. <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/31/tk-voornemens-met-betrekking-tot-de-uavg-en-avg> geraadpleegd 21 februari 2020.

Ten tweede, in een brief van de minister van 25 november 2019 geeft de minister aan open te staan voor verder en meer gebruik van gezichtsherkenningstechnologieën door de politie in het kader van veiligheid gerelateerde vraagstukken. Dat is voor dit onderzoek niet direct van belang, maar onderstaande quote geeft wel aan dat er wordt nagedacht over de voorwaarden waaronder dergelijke technologieën een breder toepassingsbereik zouden kunnen vinden:

> Ik sta open voor een verdere ontwikkeling van deze technologie. Om de kennis en reeds aanwezige ervaring te bundelen is dan ook al enige tijd geleden aan de politie opdracht gegeven te komen tot de vorming van een Centrum voor Biometrie ten behoeve van het hele Ministerie van Justitie en Veiligheid. Bij de toekomstige inzet van gezichtsherkenningstechnologie zal veel afhangen van de wijze van inzet. Het gaat dan niet om het enkele feit dat er gezichtsherkenningstechnologie wordt ingezet, maar om hoe dat wordt gedaan en welke waarborgen worden ingebouwd om op een zorgvuldige wijze om te gaan met de inzet en de analyse. In mijn antwoord op de Kamervragen over gezichtsherkenning heb ik uw Kamer geïnformeerd over de onderzoeken van de politie naar een bredere inzet van gezichtsherkenningstechnologie bij de uitvoering van de politietaak. Het is op zich gebruikelijk dat de politie bij de start van experimenten voor zichzelf inzichtelijk maakt wat de wettelijke waarborgen zijn, welke juridische mogelijkheden en beperkingen er zijn en wat de praktische bruikbaarheid is. Specifiek voor de experimenten met gezichtsherkenningstechnologie, waar door het gebruiken van biometrische gegevens, in beginsel inbreuk wordt gemaakt op de grondrechten van de betrokken personen, vind ik het belangrijk dat er geen twijfel is over het wettelijke kader dat van toepassing is en dat alle noodzakelijke (technische en organisatorische) waarborgen zijn getroffen. Ik vind het ook belangrijk dat er – voordat een nieuwe toepassing van gezichtsherkenningstechnologie bij de politie operationeel wordt ingezet – goed is nagedacht over vragen van juridisch-ethische aard. De politie heeft voor het operationele gezichtsherkenningssysteem CATCH al voldoende waarborgen getroffen om de persoonlijke levenssfeer van de betrokkenen te beschermen. Ik heb de politie opdracht gegeven om ten aanzien van de toekomstige, andere inzet van gezichtsherkenningstechnologie samen met betrokken partijen inzichtelijk te maken wat het wettelijk kader is, welke waarborgen er zijn getroffen en wat de uitkomst is van de juridisch-ethische toets. Zolang daar geen opgave van is gedaan, mag een desbetreffende experiment niet operationeel worden ingezet.[285]

Ten derde, in antwoord op Kamervragen omtrent gezichtsherkenningstechnologieën als gebruikt door Jumbo stelde de minister op 20 januari 2020:

[285] *Kamerstukken II*, 2019-2020, 32 761, 152

> Ter uitvoering van de recente motie van de leden Verhoeven (D66) en Van Dam (CDA) over gezichtsherkenning zal ik de Tweede Kamer een brief doen toekomen waarin ik verder in ga op het juridisch kader rond het gebruik van gezichtsherkenningstechnologie en zal ik daarbij ook stilstaan bij andere weten regelgeving dan de AVG en UAVG die voor toepassing van gezichtsherkenning relevant is, zoals de Richtlijn gegevensbescherming bij opsporing en vervolging en de Wet politiegegevens. In deze brief wordt ook uitgebreid ingegaan op het gebruik van gezichtsherkenning door bedrijven.[286]

Ten vierde en tot slot, de EU heeft onder meer bij monde van Ursula von der Leyen gepleit voor meer en striktere regulering van artificiële intelligentie en daarbij aangegeven dat met name gezichtsherkenning aan banden wordt gelegd.[287]

6.2. Privaatrecht

Wanneer wij het hebben over burgerlijk recht, civiel recht of privaatrecht –welke begrippen als synoniemen worden gebruikt– gaat het over de relaties tussen burgers onderling, een relatie die grotendeels geregeld wordt in het Burgerlijk Wetboek (BW). De voorbeelden uit deze verkenning laten zien dat gezichtsherkenning reeds breed wordt toegepast in het private domein, zo gebruiken bedrijven het voor toegangscontrole; is de technologie aanwezig in zoekmachines en op sociale-mediaplatformen; zijn er verschillende apps op de markt die beloven mensen op straat te kunnen herkennen en zijn er diverse bedrijven die gezichtsanalyse- en gezichtsherkenningsmodules aanbieden om zelf aan de slag te gaan.

Het verbintenissenrecht regelt relaties tussen private personen en is voornamelijk neergelegd in boek 6 en 7 van het Burgerlijk Wetboek. Een verbintenis is een vermogensrechtelijke rechtsbetrekking tussen twee of meer personen op grond waarvan de ene partij (schuldenaar) verplicht is tot een bepaalde prestatie, waartoe de andere partij (schuldeiser) is gerechtigd. Verbintenissen kunnen voortvloeien uit een overeenkomst (contract) of uit de wet. De verbintenissen uit de wet zijn te onderscheiden in onrechtmatige daad, zaakwaarneming, onverschuldigde betaling en ongerechtvaardigde verrijking.

Als wij kijken naar de domeinstudies, zijn bij gezichtsherkenning vooral de bepalingen omtrent contract en onrechtmatige daad relevant. In een contract kunnen afspraken worden gemaakt over het gebruik van gezichtsherkenning. Een partij kan optreden tegen het schenden van deze afspraken. In de algemene voorwaarden van Google Nest is bijvoorbeeld het volgende te lezen over het gebruik van gezichtsherkenning: *"*Door de functie 'bekende

[286] *Aanhangsel Handelingen II*, 2019-2020, 1414. Verwezen wordt naar motie: Kamerstuk 35 300VI, nr. 64.
[287] Zie onder meer: <https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/190714-Letter-Candidate-RENEW-1.pdf>; TA Madiega "EU guidelines on ethics in artificial intelligence: Context and implementation", 2019. <https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf> geraadpleed 21 februari 2020.

gezichtswaarschuwingen' te gebruiken, stemt de gebruiker in met de verwerking van gezichtsafbeeldingen en onderliggende gezichtsafdrukken om het apparaat in staat te stellen bekende gezichten te herkennen en u te informeren over bekende en onbekende mensen."[288] Ook zonder nadere afspraken kan gezichtsherkenning echter eenzijdig door een partij worden ingezet. Zo zijn er algemene voorwaarden van toepassing in de relatie gebruiker en aanbieder van een slimme deurbel, welke algemene voorwaarden zijn opgesteld door de aanbieder van de deurbel en welke de gebruiker accepteert door het product te gebruiken. Echter, er zijn geen nadere afspraken tussen de gebruiker van de deurbel en de personen die door deze deurbel in beeld worden gebracht. In deze tweede situatie zal er, bij gebrek aan een contractuele verhouding, geen sprake kunnen zijn van niet nakoming van een verbintenis. Er kan wel sprake zijn van een onrechtmatige daad, als blijkt dat de inzet van gezichtsherkenning strijdig is met de wet of met wat in het maatschappelijk verkeer betamelijk wordt geacht.

In de volgende twee paragrafen wordt nader ingegaan op niet-nakoming van een verbintenis (paragraaf 6.2.1) en de onrechtmatige daad (paragraaf 6.2.2). Daarna wordt kort stilgestaan bij Richtlijn (EU) 2019/770 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten. Deze Richtlijn stelt conformiteitseisen aan overeenkomsten betreffende digitale inhoud en diensten, waaronder bepaalde vormen van gezichtsherkenning in private relaties kunnen vallen. Tot slot wordt gekeken of er in Nederland reeds rechterlijke uitspraken zijn waarin de (niet) contractuele aansprakelijkheid voor gezichtsherkenning centraal staat. Hieruit zouden nadere richtlijnen kunnen volgen betreffende de toelaatbaarheid van gezichtsherkenning in private relaties.

6.2.1. **Niet nakoming van een verbintenis**

Het Burgerlijk Wetboek bepaalt in artikel 6:74 lid 1:

> Iedere tekortkoming in de nakoming van een verbintenis verplicht de schuldenaar de schade die de schuldeiser daardoor lijdt te vergoeden, tenzij de tekortkoming de schuldenaar niet kan worden toegerekend." Zoals reeds aangegeven kan het gebruik van gezichtsherkenning nader bepaald zijn in een contract, maar dit betekent niet dat het contract de gezichtsherkenning legitimeert. De Algemene Verordening Gegevensverwerking (AVG) en de Uitvoeringswet AVG (UAVG) vereisen voor de verwerking van biometrische gegevens een legitieme verwerkingsgrond. De artikelen 22

[288] Vrije vertaling van de in het Engels opgestelde privacy statement van Nest, welke uitdrukkelijk onderdeel uitmaakt van de Algemene voorwaarden – "All additional guidelines, terms or rules and the Website Privacy Policy ("Website Privacy Policy") and the Privacy Statement ("Privacy Statement") are incorporated by reference into these Terms and you are agreeing to accept and abide by them by using the Services and Products" zie: <www.nest.com/legal/terms-of-service/>. Het privacy statement is beschikbaar via: <www.nest.com/ie/legal/privacy-statement-for-nest-products-and-services/>. Meer over gezichtsherkenning en de slimme deurbel in hoofdstuk 3.

> en 29 van de UAVG laten weinig ruimte voor de verwerking van biometrische gegevens in horizontale verhoudingen. Zoals uitgelegd kunnen gezichtsherkenningstechnologieën alleen worden gebaseerd op de algemene grond van legitieme toestemming (zie volgende paragraaf) of op de specifieke grond van de inzet van gezichtsherkenningstechnologieën voor authenticatie of beveiligingsdoeleinden. De regering legt daarbij de nadruk op het feit dat die technologie noodzakelijk, proportioneel en subsidiair moet zijn en hiervan lijkt geen sprake te zijn in horizontale relaties. De Autoriteit Persoonsgegevens heeft immers bepaald dat bij de inzet van biometrie: "Een strenge toets nodig is of het belang van het gebruik van biometrie in verhouding staat tot de inbreuk op de privacy. En of het gebruik van biometrische gegevens de beste manier is de toegang te beveiligen of dat er ook andere manieren zijn.[289]

In de eerdergenoemde praktijkvoorbeelden waarbij gezichtsherkenningstechnologie voornamelijk wordt ingezet voor het verlenen van toegang tot bepaalde plaatsen en het kunnen identificeren van (on)gewenste gasten en/of potentiële klanten, kan alleen toestemming een mogelijke verwerkingsgrond bieden.

Hoewel het gebruik van gezichtsherkenning dus niet per definitie uitgesloten is op grond van de UAVG, moet de rechtmatigheid beoordeeld worden aan de hand van een strenge toets en hier ligt dus zeker ruimte om op te treden tegen gezichtsherkenning wanneer men van mening is dat de toepassing hiervan deze toets niet kan doorstaan en dus onrechtmatig is. In het navolgende kijken wij niet naar de grenzen die het privacy en gegevensbeschermingsrecht stellen met betrekking tot de rechtmatigheid van gezichtsherkenning, zie hierover het voorgaande hoofdstuk, maar naar de rol die de onrechtmatige daad kan spelen indien men van mening is dat in een private relatie sprake is van onrechtmatige gezichtsherkenning.

6.2.2. **Onrechtmatige daad**

In artikel 6:162 van het Burgerlijk Wetboek is de onrechtmatige daad omschreven als:

> 1. Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.
>
> 2. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht

[289] Autoriteit Persoonsgegevens, 'Grip op Persoonsgegevens: Jaarverslag 2018', (2018) <www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2018.pdf>, verwijzing in link op pagina 47, verwijst naar: <www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie#mag-ik-biometrie-gebruiken-voor-toegangscontrole-6711>.

in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.

3. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

Uit het tweede lid van dit artikel blijkt dat er in drie gevallen sprake kan zijn van een onrechtmatige daad: bij de inbreuk op een recht, bij een doen of nalaten in strijd met een wettelijke plicht, of een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. Deze laatste categorie laat dus ruimte, zelfs als het niet helemaal duidelijk of zeker is dat de gezichtsherkenning in strijd met een wettelijke plicht heeft plaatsgevonden. Zelfs al zou gezichtsherkenning op basis van toestemming hebben plaatsgevonden en met inachtneming van de toepasselijke wettelijke kaders, kan er nog steeds schade ontstaan. Bijvoorbeeld door een verkeerde matching, een fout-negatief of een fout-positief. In een dergelijke situatie kan de betrokkene zich mogelijk niet beroepen op een doen of nalaten in strijd met een wettelijke plicht, maar wel op een handelen dat strijdig is met hetgeen in het maatschappelijk verkeer betaamt, namelijk een onterechte behandeling door een onterechte (niet)identificatie van een gezichtsherkenningssysteem dat als zodanig in overeenstemming met de wet was ingezet.

Bij gezichtsherkenning kan sprake zijn van inbreuken op verschillende rechten, zoals privacyrechten, gegevensbeschermingsrechten en portretrechten. Het doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt zal, gezien de strenge test zoals genoemd door de AP, al snel leiden tot een inbreuk op het privacy- en of gegevensbeschermingsrecht. Als er bijvoorbeeld niet voldoende beveiligingsmaatregelen of data-minimalisatie maatregelen genomen zijn.

Bij niet-naleving van de AVG kan de Autoriteit Persoonsgegevens optreden, ook zonder dat er sprake is van een klacht of aantoonbare schade. De onrechtmatige daad is een juridisch instrument dat door een belanghebbende gebruikt kan worden wanneer daadwerkelijk schade is geleden door gezichtsherkenning. Wil een beroep op de onrechtmatige daad slagen, moet er voldaan zijn aan verschillende vereisten. Naast de onrechtmatigheid moet er sprake zijn van toerekenbaarheid, schade, causaliteit en relativiteit. Op grond van artikel 6:162 lid 1 BW is de daad toerekenbaar aan degene die de onrechtmatige daad pleegt. Bij gezichtsherkenning betreft het degene die hier gebruik van maakt en op basis hiervan beslissingen neemt. Er moet sprake zijn van schuld aan de gedraging, of deze gedraging moet krachtens de wet of de in het verkeer geldende opvattingen voor rekening van de gebruiker van gezichtsherkenning komen. Dit wordt ook wel verwoord wanneer de gedraging ligt in de risicosfeer van de dader. Aan dit criterium lijkt, gezien de gevoeligheid van gezichtsherkenning en de strenge eisen die hieraan gesteld mogen worden, snel sprake te zijn.

In de tweede plaats moet er sprake zijn van schade, een begrip dat in de wet niet als zodanig gedefinieerd is. In artikel 6:95 BW is bepaald dat: “De schade die op grond van een wettelijke verplichting tot schadevergoeding moet worden vergoed, bestaat in vermogensschade en ander nadeel, dit laatste voor zover de wet op vergoeding hiervan recht geeft.” Op grond van art. 6:96 BW omvat vermogensschade zowel verlies als gederfde winst. Bij ander nadeel moet vooral gedacht worden aan zogenaamde immateriële schade. Artikel 6:106 BW bepaalt:

- Voor nadeel dat niet in vermogensschade bestaat, heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding:
- indien de aansprakelijke persoon het oogmerk had zodanig nadeel toe te brengen;
- indien de benadeelde lichamelijk letsel heeft opgelopen, in zijn eer of goede naam is geschaad of op andere wijze in zijn persoon is aangetast;
- indien het nadeel gelegen is in aantasting van de nagedachtenis van een overledene en toegebracht is aan de niet van tafel en bed gescheiden echtgenoot, de geregistreerde partner of een bloedverwant tot in de tweede graad van de overledene, mits de aantasting plaatsvond op een wijze die de overledene, ware hij nog in leven geweest, recht zou hebben gegeven op schadevergoeding wegens het schaden van zijn eer of goede naam.

Er zijn voorbeelden waarbij vooral het tweede lid relevant lijkt bij onrechtmatige gezichtsherkenning. Hoewel de inzet van gezichtsherkenning als zodanig onrechtmatig kan zijn, zal het niet altijd eenvoudig zijn om aan te tonen wat voor schade hierdoor geleden wordt. Wanneer een persoon bijvoorbeeld wel toegang verleend wordt tot een recreatieplas nadat gezichtsherkenning geen match heeft opgeleverd, kan deze persoon zich nog steeds aangetast voelen in zijn privacy, doordat het proces van gezichtsherkenning doorlopen moet worden. Maar wat is precies de schade die deze persoon dan lijdt? Bij immateriële schade is dat vaak lastig vast te stellen en op waarde te schatten, ofwel, welke vergoeding moet er tegenover de geleden schade staan? Bij vermogensschade is dit eenvoudiger. Als bijvoorbeeld de toegang tot een stadion ontzegd wordt voor een voetbalwedstrijd op grond van een onterechte gezichtsherkenning. Er is dan sprake van vermogensschade doordat de betrokkene reeds betaald heeft voor het kaartje voor de wedstrijd. In deze situatie is het ook eenvoudiger om voor deze specifieke persoon hard te maken dat hij zich in zijn persoon en reputatie voelt aangetast, het systeem merkt hem immers ten onrechte aan als een hooligan.

Desalniettemin, in de Nederlandse rechtspraak zien wij momenteel een ontwikkeling richting meer ruimte voor immateriële schadevergoeding. Zowel in een zaak tegen de gemeente Deventer als in een zaak tegen het UWV, is een schadevergoeding opgelegd van respectievelijk 500 euro en 250 euro wegens immateriële schade geleden door onrechtmatige verwerking van persoonsgegevens. In beide zaken is overigens geen beroep gedaan op de onrechtmatige daad,

maar is op grond van artikel 82 AVG om schadevergoeding verzocht wegens schending van de AVG.[290] De rechter oordeelt in deze zaken dat voor de toekenning van schadevergoeding aansluiting mag en moet worden gezocht bij het Nederlands rechtsbestel. Dit betekent dat eiser op grond van artikel 82 van de AVG in samenhang met artikel 6:106 van het BW recht heeft op een naar billijkheid vast te stellen schadevergoeding.

Naast toerekenbaarheid en schade moet er bij een onrechtmatige daad ook sprake zijn van causaliteit. Bij causaliteit gaat het om het verband tussen de onrechtmatige gedraging en de schade. Het is in principe de benadeelde die moet stellen en bewijzen dat er van een dergelijk verband sprake is. In het voorbeeld hierboven is dat eenvoudig, het stadion bepaalt dat gezichtsherkenning wordt ingezet om hooligans buiten te houden, het door het stadion ingezette middel faalt en leidt ertoe dat deze persoon de wedstrijd niet kan zien, dus er is hier sprake van causaal verband. Ook bij de andere voorbeelden is het over het algemeen duidelijk wie de gezichtsherkenning gebruikt en met welk doel. Als de inzet van de gezichtsherkenning leidt tot schade, kan de gebruiker door de benadeelde aansprakelijk gesteld worden. Eventueel kan er sprake zijn van regres op de aanbieder van de gezichtsherkenningstechnologie, als de gebruiker kan aantonen dat de schade niet zozeer komt door het feit dat hij de technologie heeft gebruikt, maar door het verkeerd functioneren van de technologie als zodanig.

Het relativiteitsvereiste is neergelegd in artikel 6:163 BW: “Geen verplichting tot schadevergoeding bestaat, wanneer de geschonden norm niet strekt tot bescherming tegen de schade zoals de benadeelde die heeft geleden.” Ofwel, de door de dader overtreden norm moet geschreven zijn ter bescherming van het geschonden belang.[291]

Recent is door het Parket van de Hoge Raad nog uitleg gegeven aan dit vereiste in het kader van het schietincident in Alphen aan den Rijn. In deze zaak hebben nabestaanden en anderen het politiekorps aansprakelijk gesteld wegens onrechtmatige daad omdat de korpschef ten onrechte een wapenverlof aan de schutter had verleend. De vraag in relatie tot het relativiteitsverseiste in deze zaak is of de Wet wapens en munitie en het daarin neergelegde stelsel en de normen voor het verlenen van een verlof mede strekken ter bescherming van individuele (vermogens)belangen van burgers.[292] In de hierboven geschetste voorbeelden lijkt het relativiteitsvereiste geen bepalende rol te spelen wanneer iemand een beroep wil doen op onrechtmatige daad, want privacyrechten, gegevensbeschermingsrechten en portretrechten zijn juist bedoeld ter bescherming van de belangen van de individuele persoon die mogelijk geschaad wordt door gezichtsherkenning en de daaraan verbonden consequenties.

---

[290] Iris de Groot, ‘UWV Moet Werknemer 250 Euro Schadevergoeding Betalen Na Datalek’ (2019) ICTRECHT <www.ictrecht.nl/2019/09/13/uwv-moet-werknemer-250-euro-schadevergoeding-betalen-na-datalek/> geraadpleegd 11-01-2020. Onder verwijzing naar de betreffende rechtszaken Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827 en Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 en naar een uitspraak van de Hoge Raad van 15 september 2019, ECLI:NL:HR:2019:376 waarin bepaald is dat “ook buiten gevallen van geestelijk letsel sprake kan zijn van aanspraak op vergoeding van immateriële schade.”

[291] Zie over relativiteit bijvoorbeeld: L van den Berge, ‘‘Rechtmatig Tegenover den een, Onrechtmatig Tegenover den Ander’: Relativiteit In Privaat- En Bestuursrecht’ (2017) 2 Rechtsgeleerdheid Magazijn Themis 43 – 55.

[292] Parket bij de Hoge Raad 24 juni 2019, ECLI:NL:PHR:2019:450.

In artikel 6:196c BW staat een aansprakelijkheidsuitsluiting voor aanbieders van diensten van de informatiemaatschappij. Op grond van dit artikel zijn deze aanbieders niet aansprakelijk voor het enkele doorgeven of (tijdelijk) opslaan van informatie afkomstig van derden, voor zover zij geen weet hebben van het onrechtmatige karakter hiervan. Deze bepaling is niet relevant voor aanbieders van apps[293] waarin of waarmee gezichtsherkenning wordt toegepast; het gaat hierbij om aansprakelijkheid voor onrechtmatige informatie, zoals kinderporno, laster, smaad, discriminatie en andere informatie die als zodanig een onrechtmatige daad oplevert. Een gezichtsscan is als zodanig geen onrechtmatige informatie die wordt doorgegeven door de aanbieder van de app. Het maken van de gezichtsscan kan wel onrechtmatig zijn, maar dat is geen onrechtmatige informatie maar een onrechtmatige handeling, en daarop ziet de aansprakelijkheidsuitsluiting van 6:196c BW niet.

Waar de bepaling wel op van toepassing kan zijn is de aanbieder van het platform waarin apps worden aangeboden, indien een gezichtsherkenningsapp als zodanig als onrechtmatige software wordt bestempeld.

6.2.3. **Richtlijn 2019/770 EU**

Indien gezichtsherkenning wordt aangeboden als een dienst aan consumenten kan Richtlijn (EU) 2019/770 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten van toepassing zijn.[294] Deze richtlijn, met als doel een goede werking van de interne markt en een hoog niveau van consumentenbescherming, legt gemeenschappelijke regels vast betreffende bepaalde voorschriften voor overeenkomsten tussen handelaren en consumenten voor de levering van digitale inhoud of digitale diensten.[295] Het gaat hierbij met name om regels betreffende conformiteit van digitale inhoud of een digitale dienst met de overeenkomst, de remedies in geval van een conformiteitsgebrek of leveringsverzuim en de wijze waarop die remedies kunnen worden uitgeoefend.

Voor de toepassing van deze richtlijn wordt verstaan onder digitale inhoud: “gegevens die in digitale vorm worden geproduceerd en geleverd” en onder digitale dienst:

> [E]en dienst die de consument in staat stelt gegevens in digitale vorm te creëren, te verwerken of op te slaan, of toegang tot die gegevens te krijgen of *een dienst die voorziet in de mogelijkheid van het delen van gegevens of andere interactie met gegevens in*

[293] Hetzelfde geldt hier voor de aanbieder van producten waarmee, veelal in combinatie met de afname van een bijbehorende dienst, gezichtsherkenning wordt toegepast zoals bijvoorbeeld de slimme deurbel.
[294] Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten (Voor de EER relevante tekst.) PE/26/2019/REV/1, *OJ L 136, 22.5.2019.*
ELI: http://data.europa.eu/eli/dir/2019/770/oj
[295] Artikel 1 van Richtlijn (EU) 2019/770.

digitale vorm die door de consument of door andere gebruikers van die dienst worden geüpload of gecreëerd.[296]

Vooral het gecursiveerde deel is relevant voor gezichtsherkenning in private relaties. De richtlijn is van toepassing op alle overeenkomsten waarbij de handelaar digitale inhoud of een digitale dienst aan de consument levert of zich ertoe verbindt die te leveren en de consument een prijs betaalt of zich ertoe verbindt een prijs te betalen. De richtlijn is ook van toepassing als de handelaar digitale inhoud of een digitale dienst aan de consument levert of zich ertoe verbindt die te leveren en de consument de handelaar persoonsgegevens verstrekt of zich ertoe verbindt die te verstrekken. Dit tenzij deze gegevens enkel worden verwerkt om de digitale inhoud of digitale dienst te leveren of om te voldoen aan de wettelijke vereisten waaraan de handelaar is onderworpen en hij gegevens niet voor andere doeleinden verwerkt.[297]

In relatie tot gezichtsherkenning is vooral de uitzondering uit artikel 3 (4) relevant: "De richtlijn is niet van toepassing op digitale inhoud of digitale diensten die verwerkt zijn in of onderling verbonden zijn met 'goederen met digitale elementen'". Onder dergelijke goederen wordt verstaan: "Alle roerende lichamelijke zaken waarin digitale inhoud of een digitale dienst zijn verwerkt of die daarmee onderling verbonden zijn, op zodanige wijze dat het ontbreken van die digitale inhoud of digitale dienst ertoe zou leiden dat de goederen hun functies niet kunnen vervullen". Bij twijfel of de levering van verwerkte of onderling verbonden digitale inhoud of een verwerkte of onderling verbonden digitale dienst deel uitmaakt van de koopovereenkomst, wordt de digitale inhoud of digitale dienst geacht onder de koopovereenkomst te vallen.[298] Gezien deze formulering zal bijvoorbeeld de slimme deurbel met gezichtsherkenning niet onder de reikwijdte van deze Richtlijn vallen, tenzij de gezichtsherkenning aangeboden wordt als een extra dienst. Het juridische criterium luidt namelijk "dat het ontbreken van die digitale inhoud of digitale dienst ertoe zou leiden dat de goederen hun functies niet kunnen vervullen". De slimme deurbel kan in de huidige opzet ook zonder gezichtsherkenning zijn functie vervullen en momenteel is gezichtsherkenning als zodanig een extra functionaliteit die kan worden toegevoegd. Pas wanneer deze functie een integraal onderdeel uit gaat maken van de deurbel, waardoor deze niet meer kan functioneren zonder deze functie, zou de deurbel vallen binnen de uitzondering van artikel 3 (4).

Wanneer de Richtlijn van toepassing is, houdt dit in dat de aanbieder van gezichtsherkenning gebonden is aan de conformiteitsvereisten zoals neergelegd in de artikelen 5 tot en met 8 van de Richtlijn. In overweging 48 is zeer uitgebreid en uitdrukkelijk gesteld dat onder het conformiteitsvereiste ook valt het voldoen aan de vereisten die voortvloeien uit de AVG.[299] De

[296] Artikel 2 van Richtlijn (EU) 2019/770.
[297] Artikel 3 van Richtlijn (EU) 2019/770.
[298] Artikel 3(4) van Richtlijn (EU) 2019/770
[299] Overweging 48 van Richtlijn (EU) 2019/770.

handelaar is aansprakelijk wanneer hij niet voldoet aan de conformiteitsvereisten en op hem rust de bewijslast om conformiteit aan te tonen.[300]

Richtlijn (EU) 2019/770 kan van toepassing zijn op alle gevallen waarin gezichtsherkenningstechnologie wordt aangeboden als een digitale dienst aan consumenten. De Richtlijn kan dus ook van toepassing zijn op grote techgiganten zoals Facebook en Amazon, die dergelijke technologieën rechtstreeks aanbieden aan consumenten, die met hun gegevens betalen om mensen te *taggen*, maar ook hun profielen automatisch laten scannen en matchen met de grote datasets die deze techgiganten bezitten.[301] Ook in deze gevallen vereist Richtlijn (EU) 2019/770 conformiteit met contracten en naleving van gegevensbeschermingswetgeving en het zou inbreukmakers blootstellen aan rechtsmiddelen wegens niet-naleving.[302] Op grond van artikel 14 heeft de consument in geval van een conformiteitsgebrek het recht de digitale inhoud of digitale dienst conform te laten maken, een evenredige prijsvermindering te krijgen, of de overeenkomst te ontbinden volgens de in dit artikel bepaalde voorwaarden. Op grond van artikel 3 (10) en overweging 73 is het beginsel van aansprakelijkheid van de handelaar voor schade een wezenlijk onderdeel van de overeenkomsten voor de levering van digitale inhoud of diensten, en doet de Richtlijn geen afbreuk aan de reeds in alle lidstaten bestaande rechten op schadevergoeding.

Richtlijn (EU) 2019/770 kan worden gezien als een instrument om handelaren onder druk te zetten om te voldoen aan contracten en gegevensbeschermingswetten en de rechten van de betrokkenen te respecteren.[303] In een tijdperk waarin mensen gewillig gevoelige persoonlijke gegevens delen en bergen van dergelijke gegevens opgeslagen worden in databanken welke gekoppeld kunnen worden en waarin, al dan niet met behulp van gezichtsherkenning, verbanden gelegd kunnen worden, is bescherming nodig op grond van sui generis regimes.[304] Daarnaast is er tevens behoefte aan uniforme regels die kwetsbare partijen in staat stellen zichzelf te beschermen door plichten op te leggen aan degenen die controle hebben over technologieën voor gezichtsherkenning en rechtsmiddelen te bieden wanneer deze verplichtingen niet worden nageleefd. Richtlijn (EU) 2019/770 levert hier een bijdrage aan.

---

[300] Artikel 11 en 12 van Richtlijn (EU) 2019/770.

[301] Mark Scott, Laurens Cerulus en Nicholas Vinocur, 'Europe Eyes Stricter Rules on Facial Recognition' (2019) Politico <www.politico.eu/article/europe-facial-recognition-facebook-privacy-data-protection/> geraadpleegd 3 juli 2019; April Glaser, 'Facebook's Face-ID Database Could Be the Biggest in the World. Yes, It Should Worry Us' (2019) Slate <www.slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.amp> geraadpleegd 3 juli 2019.

[302] Richtlijn (EU) 2019/770 overwegingen 11, 24, 48, arts 1, 14.

[303] Geraldine Proust, 'EU: The Circling of Legislative Wagons to Better Protect Consumers' (2019) FEDMA <www.fedma.org/2019/07/eu-the-circling-of-legislative-wagons-to-better-protect-consumers/> geraadpleegd 3 juli 2019.

[304] European Commission, 'Evaluation of Directive 96/9/EC on the Legal Protection of Databases' (2018) SWD(2018) 147 final para 5.3.3.1 <http://edz.bib.uni-mannheim.de/edz/pdf/swd/2018/swd-2018-0146-en.pdf> geraadpleegd 3 juli 2019. Met het sui generis recht wordt gedoeld op het databankenrecht: het verbodsrecht ter zake opvraging of het hergebruik van een databank dat de producent van een databank kan inroepen.

[304] Databank geraadpleegd op 21 juni 2019.

6.2.4. **Nederlandse rechtspraak over de toelaatbaarheid van gezichtsherkenning**

Met het oog op het identificeren van nadere richtlijnen omtrent de (on)toelaatbaarheid van gezichtsherkenning in private relaties is gekeken naar de Nederlandse rechtspraak. De zoekcombinatie “onrechtmatige daad” en “gezichtsherkenning” levert in de databank van www.rechtspraak.nl geen hits op.[305] Het zoeken naar “gezichtsherkenning” en “onrechtmatig” geeft 18 hits. [306] Hierbij gaat het voornamelijk om zaken waarbij een verdachte de betrouwbaarheid van zijn herkenning op camerabeelden of bij een fotoherkenning in twijfel trekt.[307] In een van de zaken wordt verzocht om camerabeelden op basis waarvan gezichtsherkenning plaats kan vinden uit te sluiten van bewijs.[308] In een andere zaak stond het argument centraal dat ook zonder gezichtsherkenningssoftware gezien had moeten worden dat een persoon niet degene was afgebeeld op een paspoort.[309] In nog een andere zaak wordt gesteld dat het niet rechtmatig is om voor het verkrijgen van een paspoort te vereisen dat hierin biometrische gegevens worden opgenomen.[310] In geen van deze zaken betreft de vraag naar onrechtmatigheid het gebruik van gezichtsherkenning als zodanig. Ook is er in de beschreven zaken geen sprake van contractuele verhoudingen. In het Burgerlijk Wetboek, zoals hierboven ook aangegeven, is het bestaan van een contract of nadere afspraken niet nodig om op te kunnen treden tegen gezichtsherkenning als men van mening is dat het gebruik hiervan niet rechtmatig is. In tegenstelling tot het strafrecht, waarbij het Openbaar Ministerie bepaalt welke strafbare feiten worden vervolgd, of het gegevensbeschermingsrecht waarbij de Autoriteit Persoonsgegevens bepaald of en zo ja welke maatregelen genomen worden tegen overtreding van de UAVG, ligt bij civiele zaken het initiatief bij een van de partijen.

Uit de analyse van het strafrecht zal blijken dat daar de strafbaarheid vooral samenhangt met de heimelijkheid, iets dat in de bovenstaande voorbeelden en rechtspraak geen rol lijkt te spelen. Zoals beschreven in het voorgaande, binnen het civiele recht gelden andere criteria dan in het strafrecht om te beoordelen of gezichtsherkenning al dan niet rechtmatig is en mogelijk leidt tot een verplichting van vergoeding van geleden schade. In een contractuele verhouding gaat het vooral om de vraag of er sprake is van conformiteit met hetgeen is overeengekomen, ofwel of er een tekortkoming in de nakoming van een verbintenis is. Bij de onrechtmatige daad moet voldaan zijn aan de vereisten van toerekenbaarheid, schade, relativiteit en causaliteit.

[305] Databank geraadpleegd op 21 juni 2019.
[306] Zoekopdracht uitgevoerd op 18-10-2019.
[307] Bijvoorbeeld de zaken: Rb Amsterdam 24 oktober 2018, ECLI:NL:RBAMS:2018:8828; Rb Amsterdam 22 mei 2019, ECLI:NL:RBAMS:2019:3729; Rb Amsterdam 31-08-2017, ECLI:NL:RBAMS:2017:6329; Rb Middelburg 26 mei 2011, ECLI:NL:RBMID:2011:BQ6043.
[308] Gerechtshof Amsterdam 18 november 2014, ECLI:NL:GHAMS:2014:4776.
[309] Rb Groningen, 18 februari 2010, ECLI:NL:RBGRO:2010:BL7232.
[310] Raad van State 25 mei 2016, ECLI:NL:RVS:2016:1416.

6.2.5. **Conclusie**

Zoals uit bovenstaande blijkt, biedt het privaatrecht een eigenstandige mogelijkheid voor partijen om op te treden tegen non-conforme en/of onrechtmatige toepassingen van gezichtsherkenning. Het biedt mogelijkheden om afspraken te maken over gezichtsherkenning en daarmee de kans op schendingen van de persoonlijke levenssfeer van de betrokkenen te beperken. Daarnaast biedt het mogelijkheden om schade vergoed te krijgen. Aansprakelijkheid voor het vergoeden van geleden schade kan voor aanbieders van gezichtsherkenning een extra prikkel zijn om gezichtsherkenning conform gemaakte afspraken, de wet en hetgeen in het maatschappelijk verkeer betaamt, toe te passen. Dit kan inbreuken op privacy helpen voorkomen. Deze prikkel is op Europees niveau nog eens extra verankerd in Richtlijn 2019/770 EU.

6.3. Strafrecht

Het strafrecht vormt een belangrijk onderdeel van de normstelling in Nederland. De strafbaarstelling van bepaalde handelingen vormt als het ware de ondergrens van wat maatschappelijk aanvaardbaar handelen wordt geacht. Overschrijding van deze grens leidt niet alleen tot sancties, maar deze sancties hebben ook een punitief karakter, dat gepaard gaat met een moreel oordeel over het handelen. Een belangrijk verschil met het civiele recht is immers dat strafrechtelijke sancties niet alleen aangeven dat iemand onjuist heeft gehandeld, maar ook dat dit *moreel* onjuist gedrag betreft.

De belangrijkste strafbepalingen zijn te vinden in het commune strafrecht: het Wetboek van Strafrecht (Sr). Er zijn ook strafbepalingen in het bijzondere strafrecht, zoals de Opiumwet of de Wet op de economische delicten, maar daarin zijn geen bepalingen te vinden die van toepassing zijn op gezichtsherkenning.[311] Het Wetboek van Strafrecht kent misdrijven (Tweede Boek) en overtredingen (Derde Boek). Bij misdrijven zou de onrechtmatigheid normaliter op voorhand voor iedereen duidelijk moeten zijn ('onrecht vóór de wet'), terwijl bij overtredingen de onrechtmatigheid vooral door de strafbaarstelling zelf wordt bewerkstelligd ('onrecht dóór de wet').[312] Ook is bij overtredingen, in tegenstelling tot misdrijven, meestal niet expliciet opzet (dolus) of schuld (culpa) vereist; wie de handeling als omschreven pleegt, is in beginsel zonder meer strafbaar, tenzij een wettelijke strafuitzonderingsgrond (art. 39-43 Sr, bijvoorbeeld overmacht of noodweer) van toepassing is. [313] De meeste misdrijven bevatten het element van

[311] Hypothetisch kunnen sommige bijzondere strafbepalingen wel van toepassing zijn. Zo valt een gezichtsherkenningstoepassing op een killer-drone (die zich automatisch zou richten op het doelwit op basis van gezichtsherkenning) onder de Wet wapens en munitie, omdat het in zo'n geval een hulpstuk van wezenlijke aard is voor het wapen (art. 3 lid 1 WWM). Zulke toepassingen laten wij buiten beschouwing omdat ze, zeker in horizontale relaties, te hypothetisch zijn.
[312] CPM Cleiren, JH Crijns, MJM Verpalen, *Tekst &Commentaar Strafrecht*, Derde Boek, Inleidende opmerkingen, aant. 1.
[313] Ibid., aant. 2. In theorie kan iemand daarnaast ook een beroep doen op de buitenwettelijke uitzonderingsgrond 'afwezigheid van alle schuld', maar die wordt in de praktijk zelden erkend.

'wederrechtelijkheid'. Dit is een algemene term die aanduidt dat de desbetreffende handeling alleen strafbaar is als deze plaatsvindt zonder toestemming of in strijd met een wettelijk voorschrift of met wat in het maatschappelijk verkeer betamelijk wordt geacht; daarmee wordt voorkomen dat alledaagse handelingen (zoals het aanzetten van de eigen computer) onder een strafbaarstelling (zoals hacken: het opzettelijk *en wederrechtelijk* binnendringen in een computer, art. 138ab Sr) vallen.

Voor de interpretatie van de reikwijdte van strafbepalingen moet men voor ogen houden dat Nederland het opportuniteitsbeginsel hanteert: het Openbaar Ministerie bepaalt welke strafbare feiten worden vervolgd, en kan ook besluiten om van vervolging af te zien, onder andere op gronden van algemeen belang (art. 167 en 242 Sv). Het opportuniteitsbeginsel maakt het mogelijk om strafbepalingen enigszins ruim te formuleren, waardoor ook de nodige (relatief) triviale handelingen binnen de reikwijdte van de strafbaarstelling kunnen vallen, die dan normaliter niet zullen worden vervolgd. Zo valt het zonder toestemming opzettelijk verfrommelen van het boodschappenlijstje van iemand anders onder zaakbeschadiging, art. 350 Sr, maar dit zal niet tot vervolging en strafrechtelijke sanctionering leiden. Dit betekent dat, om te onderzoeken of bepaalde maatschappelijke onwenselijke gedragingen voldoende door het strafrecht worden bestreden, niet alleen naar de letter van de bepaling moet worden gekeken, maar ook naar de waarschijnlijkheid van strafvervolging.

De Nederlandse strafwet is van toepassing op strafbare feiten die in Nederland (art. 2 Sr) of aan boord van een Nederlands (lucht)vaartuig (art. 3 Sr) worden gepleegd. In sommige andere gevallen is de wet ook extraterritoriaal van toepassing (art. 4 t/m 8d Sr), maar de hieronder te behandelen bepalingen, die relevant zijn voor gezichtsherkenning, vallen daar niet onder.[314]

Met deze algemene kenmerken van het strafrecht in gedachten, bespreken wij in de volgende sub-paragraaf de strafrechtelijke bepalingen die mogelijk van toepassing zijn op gezichtsherkenning.

6.3.1. **Toepassing op gezichtsherkenning**

Er bestaat geen specifiek op gezichtsherkenning toegesneden strafbepaling. Wij bespreken daarom hier bepalingen die elementen bevatten die van toepassing zouden kunnen zijn op gezichtsherkenning. Voor zover wij kunnen nagaan, is er nog geen jurisprudentie over de eventuele strafbaarheid van gezichtsherkenning;[315] onderstaande discussie van strafbepalingen is daarom gebaseerd op onze eigen analyse op basis doctrinair juridisch onderzoek. Omdat geautomatiseerde gezichtsherkenning gebaseerd is op computertechnologie, hebben wij gekeken

[314] Wel is de wet ook van toepassing op Nederlanders (of vreemdelingen met een vaste woon- of verblijfplaats in Nederland) die in het buitenland misdrijven plegen die aldaar ook strafbaar zijn gesteld (art. 7 Sr), maar voor de analyse van de toepasbaarheid van strafbepalingen op gezichtsherkenning is dat niet relevant.
[315] Zoeken in uitspraken op rechtspraak.nl op "gezichtsherkenning" levert wel tientallen treffers op, maar deze hebben betrekking op het herkennen van de verdachte (door verbalisanten of op camerabeelden) als bewijsmiddel.

naar de strafbepalingen die van toepassing zijn op computercriminaliteit;[316] wij bespreken daarvan de bepalingen die mogelijk toepasbaar zijn op de casussen van gezichtsherkenning zoals in dit rapport behandeld.

Heimelijke observatie

De meest voor de hand liggende bepalingen die van toepassing kunnen zijn op het gebruik van gezichtsherkenning, zijn de in 1971 ingevoerde (en nadien aangepaste) strafbaarstellingen van heimelijke visuele observatie in art. 139f en 441b Sr.[317]

Art. 139f Sr is een bepaling die het heimelijk en wederrechtelijk maken van afbeeldingen van een persoon in niet-publiek toegankelijke plaatsen als misdrijf strafbaar stelt:

> Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie[318] wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.

Voor het heimelijk en wederrechtelijk maken van afbeeldingen op niet-besloten plaatsen geldt de overtreding van art. 441b Sr:

> Met hechtenis van ten hoogste twee maanden of geldboete van de derde categorie[319] wordt gestraft hij die, gebruik makende van een daartoe aangebracht technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, van een persoon, aanwezig op een voor het publiek toegankelijke plaats, wederrechtelijk een afbeelding vervaardigt.

Hiermee wordt een duidelijk onderscheid gemaakt tussen het heimelijk observeren van personen in woningen en andere besloten plaatsen en het heimelijk observeren van personen op publiek toegankelijke plaatsen. Met niet voor het publiek toegankelijke plaatsen bedoelt de wetgever plaatsen waar niet een in beginsel onbeperkte groep toegang toe heeft; voorbeelden zijn hotelkamers, plaatsen die uitsluitend toegankelijk zijn voor leden van een vereniging of een bepaald gezelschap en kantoor- en bedrijfsruimten.[320] Een plaats is wel voor het publiek toegankelijk 'indien het feitelijk toegankelijk is voor een in beginsel onbeperkt aantal personen b.v. een restaurant, een museum.'[321] Binnen publiek toegankelijke plaatsen kunnen wel bepaalde deelruimten gelden als een besloten plaats; zo zal het heimelijk maken van afbeeldingen op een

[316] BJ Koops en JJ Oerlemans 'Materieel Strafrecht en ICT', in BJ Koops en JJ Oerlemans (eds), *Strafrecht en ICT* (3e druk, SDU 2019), 29-116.
[317] Wet van 7 april 1971, houdende *enige strafbepalingen tot bescherming van de persoonlijke levenssfeer*, Stb. 1971, 180.
[318] Een geldboete van de vierde categorie is een boete van maximaal 21.750 € (art. 23 lid 4 Sr). [voetnoot auteurs]
[319] Een geldboete van de derde categorie is een boete van maximaal 8.700 € (art. 23 lid 4 Sr). [voetnoot auteurs]
[320] *Kamerstukken II* 1967/68, 9649, 3, 4.
[321] Ibid.

toilet in een restaurant of museum wel onder art. 139f Sr vallen,[322] evenals het heimelijk fotograferen of filmen van personen in een (afsluitbaar) omkleedhokje van een zwembad[323] of in pashokjes in een kledingzaak.[324]

Oorspronkelijk (bij de invoering in 1971) was art. 139f Sr beperkt tot woningen en niet voor het publiek toegankelijke *lokalen*, en art. 441b Sr was beperkt tot 'voor het publiek toegankelijke besloten ruimte[n], waarin spijzen, dranken of andere waren aan particulieren worden geleverd'; het ging dus om bepaalde ruimten met beperkte zichtbaarheid en niet om de openbare ruimte. In 2003[325] werd de strafbaarstelling echter uitgebreid tot alle voor het publiek toegankelijke plaatsen, waaronder ook de openbare weg, omdat het recht op privacybescherming 'thans ruimer [wordt] uitgelegd dan ten tijde van de totstandkoming van de artikelen 441b en 139f Sr. Ook op voor het publiek toegankelijke plaatsen kan onder omstandigheden sprake zijn van een aantasting van de persoonlijke levenssfeer.'[326] Dat komt mede door 'de toename van het gebruik van camera's voor toezicht en beveiliging ook op andere plaatsen dan in winkels of horecagelegenheden, zoals bijvoorbeeld op stations, in uitgaansgebieden, in het openbaar vervoer, in banken en casino's.'[327]

Niettemin bestaat er nog steeds een duidelijk verschil in normstelling tussen heimelijke observatie in besloten en niet-besloten plaatsen. Dit heeft vooral te maken met het verschil in redelijke privacyverwachting: in woningen en andere besloten plaatsen voelt men zich veelal vrijer om onbevangen zichzelf te zijn, in de wetenschap niet zichtbaar te zijn voor het algemene publiek. Niettemin geeft de strafbaarstelling van art. 441b Sr aan dat men ook in niet-besloten plaatsen een zekere privacyverwachting mag koesteren: weliswaar moet men er (vanzelfsprekend) rekening mee houden dat men zichtbaar is, maar men hoeft er geen rekening mee te houden dat anderen hen zo maar mogen fotograferen of filmen. De heimelijkheid van de (technische) observatie speelt daarbij een cruciale rol: de strafbaarstelling geldt voor technische hulpmiddelen waarvan de aanwezigheid niet duidelijk kenbaar is gemaakt.

De strafbaarstelling is beperkt tot het maken van afbeeldingen met een technisch hulpmiddel, zoals (foto- of film)camera's; tekeningen met een potlood of stift vallen daar niet onder, 'omdat zij de uiterlijke schijn van authenticiteit ontberen.'[328] Geautomatiseerde gezichtsherkenning zal altijd plaatsvinden met een technisch hulpmiddel zoals bedoeld in art. 139f en 441b Sr. Daarbij is van belang dat de afbeeldingen niet per se hoeven te worden *vastgelegd*. Hoewel de strafbaarstelling primair bedoeld is om tegen te gaan dat zonder toestemming afbeeldingen van personen worden gemaakt die vervolgens een eigen leven kunnen gaan leiden als een exacte weergave van die persoon op een bepaalde plaats en tijd, valt ook het in *real time* doorgeven van

[322] Rb. Almelo 16 augustus 2011, ECLI:NL:RBALM:2011:BR5076 (in casu ging het om een toilet in een kapperszaak).
[323] HR 14 februari 2012, ECLI:NL:HR:2012:BU5254. Het Hof overwoog in deze casus: '[d]oor het kleedhokje af te sluiten, maakte aangeefster duidelijk zich in afzondering en buiten het gezichtsveld van derden te willen aan- en uitkleden.'
[324] *Kamerstukken II* 2000/01, 27 732, 3, 13.
[325] *Stb.* 2003, 198.
[326] *Kamerstukken II* 2000/01, 27 732, 3, 3.
[327] *Kamerstukken II* 2000/01, 27 732, 3, 5.
[328] *Kamerstukken II* 1967/68, 9649, 3, p. 4.

afbeeldingen zonder vastlegging eronder.[329] Dit betekent dat het gebruik van CCTV-camera's met *live streaming* van beelden, waarbij bijvoorbeeld gezichtsherkenning wordt gebruikt om bepaalde beelden te selecteren en te doen bekijken door bewakers, ook onder de strafbaarstelling valt, voor zover de aanwezigheid van de camera's niet duidelijk kenbaar is gemaakt.

Wat betekent bovenstaande nu voor de toepassing van gezichtsherkenning? Geautomatiseerde gezichtsherkenning zal altijd plaatsvinden met behulp van een camera die beeldopnamen maakt. Indien de aanwezigheid van die camera niet duidelijk kenbaar is gemaakt, zal de toepassing van gezichtsherkenning veelal strafbaar zijn (tenzij er redenen zijn waarom dit niet wederrechtelijk is, bijvoorbeeld als een journalist heimelijk beelden maakt om een publieke misstand aan de kaak te stellen).[330] De strafbaarheid zit hem daarbij echter niet in de toepassing van gezichtsherkenning, maar in het heimelijk gebruik van een camera. Dit zal een deel van de maatschappelijk onwenselijke vormen van gezichtsherkenning kunnen afdekken. Omdat art. 139f en 441b Sr echter niet specifiek toegesneden zijn op onrechtmatige gezichtsherkenning, zijn er diverse mogelijke belemmeringen bij de toepassing van deze bepalingen.

Ten eerste gaat het om het vervaardigen van afbeeldingen. Hoewel dit, zoals gezegd, niet per se het vastleggen van beelden op een geheugendrager hoeft te betreffen, maar ook het *live* doorgeven van beelden kan omvatten, lijken de bepalingen niet van toepassing op het gebruik van een camera waarmee iemand direct (dus zonder doorgifte van beelden naar een ander ontvangend apparaat) wordt geobserveerd en met gebruikmaking van gezichtsherkenning. Bij het gebruik van de camera in een smartphone om iemand in de trein te herkennen, fungeert de camera immers niet als technisch hulpmiddel om het beeld vast te leggen (als een versterking van het menselijk geheugen waardoor iemand – op een andere plaats of een ander tijdstip – toegang heeft tot een exact gereproduceerd beeld). Het fungeert eerder als een versterking van de waarnemingscapaciteit, waarin iemand een persoon kan herkennen niet (alleen) op basis van het eigen geheugen, maar (ook) op basis van extern vastgelegde 'herinneringen' over de geobserveerde persoon. In de wetsgeschiedenis zijn geen aanknopingspunten te vinden om het gebruik van een camera zonder registratie, en zonder doorgifte naar een persoon elders die *live* meekijkt, onder de reikwijdte van deze strafbepalingen te laten vallen.

Een tweede punt is dat de strafbaarstellingen spreken van een technisch hulpmiddel 'waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt'. Dit roept de nodige vragen op in relatie tot toepassingen van gezichtsherkenning. Als gezichtsherkenning plaatsvindt met een camera die wel zichtbaar aanwezig is, zijn de bepalingen niet van toepassing. Dit lijkt ons één van de grootste beperkingen van de huidige strafwetgeving met betrekking tot gezichtsherkenning: de nadruk ligt op heimelijk gebruik van camera's, niet op heimelijk gebruik van gezichtsherkenning

[329] Fokkens, Noyon/Langemeijer/Remmelink Strafrecht, commentaar op 139f Sr, aant. 2. Zie bijv. Rb. Gelderland 29 augustus 2016, ECLI:NL:RBGEL:2016:4801: het *live* uitkijken van webcambeelden moet worden aangemerkt als het vervaardigen van afbeeldingen in de zin van art. 139f Sr.
[330] Vgl. *Kamerstukken II* 2000/01, 27 732, 5, 13.

met duidelijk aanwezige camera's. Zo zal een caféhouder of winkeleigenaar die zichtbaar CCTV-camera's gebruikt en daarbij (zonder kennisgeving aan het publiek) gezichtsherkenning toepast, niet onder art. 441b vallen. Ook valt te betwijfelen of iemand die een gezichtsherkenningsapp gebruikt op haar smartphone onder de bepalingen valt, als de smartphone zichtbaar is gericht op iemand.

Zo heeft de minister toegelicht dat het maken van beelden voor infotainment-programma's niet onder de strafbaarstelling valt, omdat het niet heimelijk plaatsvindt; immers, "[i]n het geval van reality tv-programma's wordt openlijk met een camera op de schouder (…) gefilmd."[331] Nu is een tv-filmcamera iets prominenter en zichtbaarder dan een smartphone-camera, maar in het huidige tijdsgewricht zal men zich ervan bewust moeten zijn dat smartphones camera's bevatten, zodat bezwaarlijk kan worden gezegd dat een smartphone-camera niet duidelijk aanwezig is als men een smartphone ziet. (Dat ligt natuurlijk anders als de smartphone verstopt is, bijvoorbeeld in een shampoofles in een doucheruimte, om heimelijk beelden te maken.[332])

Dit hangt samen met een derde belemmering: in publiek toegankelijke plaatsen is de strafbaarstelling beperkt tot *"daartoe aangebracht* technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt" (art. 441 Sr, cursivering toegevoegd). De camera moet dus zijn aangebracht voor het doel van het fotograferen of filmen van mensen. Het gaat daarbij om "in beginsel een enigszins permanente installatie".[333] De strafbaarstelling is dus in beginsel beperkt tot vaste en enigszins duurzaam gemonteerde camera's, zoals CCTV-bewakingscamera's op publiek toegankelijke plaatsen.[334] Onder omstandigheden kunnen ook mobiele camera's eronder vallen, maar alleen

> [w]anneer een extra handeling is verricht met de handcamera waardoor diens aanwezigheid niet meer duidelijk kenbaar is – deze is bijvoorbeeld verstopt in een voorwerp of voertuig – dan is ook sprake van een «daartoe aangebracht technisch hulpmiddel». Ook in dat geval kan het vervaardigen van een afbeelding van een persoon een strafbaar feit opleveren. Is echter niets extra ondernomen met de handcamera en wordt deze gewoon door een persoon uit de hand bediend dan is artikel 441b Sr niet van toepassing.[335]

Hoewel smartphone-camera's in 2001 nog niet op het netvlies van de wetgever stonden, suggereert de wetsgeschiedenis duidelijk dat het maken van afbeeldingen met smartphone-camera's niet onder art. 441 Sr valt zolang de smartphone gewoon in de hand wordt gehouden. Alleen als de smartphone (of een ander soort camera) verstopt is, bijvoorbeeld in een tas of kleding, kan de strafbaarstelling van toepassing zijn.

---

[331] *Kamerstukken II* 2000/01, 27 732, 5, 12-13.
[332] Vgl. 'Naakte Meisjes Filmen met een Shampoofles', (2019) NRC www.nrc.nl/nieuws/2019/03/11/naakte-meisjes-filmen-met-een-shampoofles-a3952773 geraadpleegd
[333] *Kamerstukken II* 2000/01, 27 732, 5, 11.
[334] Machielse, Noyon/Langemeijer/Remmelink Strafrecht, commentaar op 441b Sr, aant. 2.
[335] *Kamerstukken II* 2000/01, 27 732, 5, 10.

Bovenstaande betekent dat de strafbaarstelling van heimelijke visuele observatie alleen toepasbaar is op gevallen van gezichtsherkenning als daarbij beelden worden vastgelegd (dan wel *live* worden doorgegeven naar een ontvangapparaat elders) en als de camera niet duidelijk aanwezig is. Veelvoorkomende situaties van gezichtsherkenning vallen hierbuiten: zowel de burger die met haar smartphone een andere burger observeert en gebruik maakt van automatische gezichtsherkenning, als de winkeleigenaar die met zichtbare camera's gezichtsherkenning toepast, zijn niet strafbaar, ook niet als het gebruik van gezichtsherkenning niet kenbaar is voor de geobserveerde.

Er valt echter een belangrijk argument te ontlenen aan de wetsgeschiedenis van art. 139f en 441b Sr dat ervoor pleit om heimelijke gezichtsherkenning strafbaar te stellen. Aanvankelijk, in 1971, was de strafbaarstelling van art. 139f Sr beperkt tot gevallen waarin de fotograaf of filmer gebruik maakt "van een door een list of een kunstgreep daartoe geschapen gelegenheid" om een afbeelding van iemand te maken "waardoor diens rechtmatig belang kan worden geschaad" (art. 139f Sr-oud). Daarbij dacht de wetgever vooral aan 'candid camera'-gevallen, oftewel "een speciaal daartoe gecreëerde situatie, welke in het bijzonder door de afgebeelde persoon als zodanig redelijkerwijs niet kan worden onderkend." [336] Daarbij moest bovendien de gefotografeerde in een rechtmatig belang zijn geschaad, omdat anders "te veel gevallen onder de strafbepaling vallen die niet strafwaardig zijn te achten. Het gebeurt vaak dat men door op onverwachte wijze een foto te maken een meer ongedwongen afbeelding hoopt te verkrijgen, zonder dat daardoor enig belang van de gefotografeerde wordt geschaad."[337] Alleen gevallen waarin iemand door de foto in een rechtmatig belang was geschaad, werden dus strafwaardig geacht.

Bij de wetswijziging in 2003 gaf de wetgever echter blijk van een gewijzigd inzicht. Art. 441b Sr kende geen bestanddeel dat de afgebeelde in een rechtmatig belang was geschaad, en het was onwenselijk dat art. 441b in dat opzicht meer rechtsbescherming zou bieden dan art. 139f Sr. Daarbij ging het volgens de wetgever niet meer om de *aard* van de afbeelding om te bepalen of het fotograferen strafwaardig was.

> Dit strookt niet meer met de huidige opvattingen omtrent de bescherming van de persoonlijke levenssfeer. Immers ongeacht de aard van de afbeelding moet het met een daartoe aangebracht technische hulpmiddel heimelijk vervaardigen van een afbeelding van een persoon op een voor het publiek toegankelijke plaats als strafwaardig worden aangemerkt. Datzelfde dient ook, of misschien wel in versterkte mate, te gelden voor woningen en andere niet voor het publiek toegankelijke plaatsen.[338]

[336] *Kamerstukken II* 1967/68, 96 49, 3, 5.
[337] *Kamerstukken II* 1969/70, 9649, 8, 5.
[338] *Kamerstukken II* 2000/01, 27 732, 5, 2.

Hieruit blijkt duidelijk dat de wetgever het gebruik maken van (vaste of verborgen) camera's om heimelijk afbeeldingen van iemand te maken, strafwaardig acht, ongeacht hoe de persoon is afgebeeld en ongeacht wat de mogelijke gevolgen voor de afgebeelde persoon kunnen zijn. De *heimelijkheid* van deze vorm van observatie staat daarbij voorop, niet *wat* er precies wordt geobserveerd of vastgelegd.

Deze redeneerlijn volgend, valt er iets voor te zeggen dat ook heimelijke gezichtsherkenning strafwaardig kan worden geacht. Ook daarbij gaat het immers om een belemmering van de vrijheid om onbevangen zichzelf te kunnen zijn, in beslotenheid, in gezelschap of op de openbare weg. Hoewel heimelijke gezichtsherkenning een iets andere dynamiek heeft dan heimelijk fotograferen of filmen (het gaat bij gezichtsherkenning vooral om de koppeling van een persoon aan informatie, en niet zo zeer om een reproduceerbaar beeld van de persoon), gaat het in beide gevallen om een bepaald beeld dat ontstaat van de persoon door een handeling die de burger niet verwacht en die daarom een significante belemmering kan vormen van haar vrijheid onbevangen zichzelf te zijn. Net zoals een burger geen camera hoeft te verwachten in een shampoofles of in een gaatje in de kast, hoeft de burger ook geen gezichtsherkenningsapp te verwachten op een camera.

Identiteitsfraude

Omdat geautomatiseerde gezichtsherkenning een vorm van biometrie betreft, is ook de strafbaarstelling van biometrie-gerelateerde identiteitsfraude van belang. Artikel 231a lid 1 Sr stelt strafbaar het *vervalsen* van biometrische kenmerken of biometrische persoonsgegevens in gevallen waarin biometrie wordt gebruikt voor identiteitsvaststelling:

> Hij die biometrische kenmerken of biometrische persoonsgegevens valselijk opmaakt of vervalst met het oogmerk om deze als echt en onvervalst te gebruiken of te doen gebruiken in gevallen waarin die kenmerken of persoonsgegevens worden gebruikt voor het vaststellen van iemands identiteit, teneinde zijn identiteit te verhelen of de identiteit van een ander te verhelen of misbruiken, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.[339]

Het tweede lid van dit artikel stelt ook het *gebruik* van vervalste biometrie in zulke gevallen strafbaar:

> Met dezelfde straf wordt gestraft hij die in gevallen waarin biometrische kenmerken of biometrische persoonsgegevens worden gebruikt voor het vaststellen van iemands identiteit, opzettelijk gebruik maakt van valse of vervalste biometrische kenmerken of biometrische persoonsgegevens als waren deze echt en onvervalst met het oogmerk om zijn identiteit te verhelen of de identiteit van een ander te misbruiken of opzettelijk gebruik maakt van biometrische kenmerken of biometrische persoonsgegevens van

[339] Een geldboete van de vijfde categorie is een boete van maximaal 87.000 € (art. 23 lid 4 Sr).

een ander met het oogmerk om de verdenking van een strafbaar feit op de ander of niet op hem te doen ontstaan.

Deze strafbaarstelling is relevant wanneer iemand misbruik maakt van gezichtsherkennings-technologie in gevallen waarin deze wordt gebruikt voor toegangscontrole, zoals de door Zenus en 20Face aangeboden technologie (zie paragraaf 4.1). Denkbaar is bijvoorbeeld dat iemand probeert een biometrisch beveiligd gebouw binnen te komen door in de databank met templates de template van het gezicht van een geautoriseerde bezoeker te vervangen door een template van zijn eigen gezicht. (Dat vergt wel bekendheid met het gebruikte algoritme, dat een bedrijfsgeheim kan zijn, zodat deze mogelijkheid niet makkelijk uit te voeren zal zijn.) Het vervangen van de templates valt onder lid 1 van artikel 231a Sr. Het gebruik ervan valt vervolgens onder lid 2; dat kan relevant zijn als iemand ongeautoriseerd de nodige templates van anderen in de databank heeft weten te krijgen, waarna deze anderen proberen het beveiligde gebouw binnen te komen.

Een ander type misbruik is lookalike-fraude. Indien iemands gezicht sterk lijkt op dat van iemand anders, kan hij proberen om gebruik te maken van de toegangsrechten die gekoppeld zijn aan het template van die ander. Biometrie is juist bedoeld om lookalike-fraude tegen te gaan, maar de technologie kan bijvoorbeeld tweelingen mogelijk niet altijd uit elkaar houden. Het hangt er ook van af hoe scherp de biometrische controle is ingesteld: als men weinig fout-positieven tolereert bij een toepassing (bijvoorbeeld om de doorstroming bij een evenement te bevorderen), is er vaak een hogere tolerantie van fout-negatieven en zullen er makkelijker mensen doorheen kunnen glippen die sterk lijken op een geautoriseerde gebruiker. Ook daarop is artikel 231a lid 2 Sr van toepassing. Weliswaar zijn bij lookalike-fraude de biometrische gegevens niet letterlijk vervalst, maar het ongeautoriseerd gebruik van de biometrie van iemand anders zal vallen onder het gebruik maken van valse biometrie, zoals ook het ongeautoriseerd gebruik van een echte huissleutel of wachtwoord in de rechtspraak als het gebruik van een valse sleutel wordt gekwalificeerd.[340]

Ook bij misbruik van Facebook kan er sprake zijn van identiteitsfraude volgens artikel 231a Sr. Facebook gebruikt immers gezichtsherkenning om de betrouwbaarheid van het platform te vergroten en koppelt het gebruik van gezichtsherkenning aan het voorkomen van ongewenste imitatie en identiteitsmisbruik (paragraaf 4.2.1). Wanneer iemand de foto van een ander gebruikt als profielfoto, is er sprake van valselijk gebruik van biometrie in een context waarin de biometrie dient voor het vaststellen van de identiteit van de Facebookgebruiker en is artikel 231 dus van toepassing. Dat lijkt zelfs het geval als het gebruik van de foto van iemand anders met diens toestemming gebeurt, omdat er daarmee nog steeds misleiding van Facebook (en van andere gebruikers) plaatsvindt, zodat dit ook onder het valselijk opmaken van biometrische kenmerken valt.

[340] HR 20 mei 1986, ECLI:NL:PHR:1986:AC9359 (huisvredebreuk); Hof Den Haag 8 juni 2004, ECLI:NL:GHSGR:2004:AP7974 (computervredebreuk).

Ook bij het gebruik van dating-apps die gezichtsherkenning inzetten, zou identiteitsfraude kunnen plaatsvinden, bijvoorbeeld als iemand probeert om met de gezichtsfoto van iemand anders een date voor elkaar te krijgen. De vraag is echter of bij dating-apps sprake is van het gebruik van gezichtsherkenning "voor het vaststellen van iemands identiteit". Momenteel lijkt gezichtsherkenning vooral te worden gebruikt om geautomatiseerd interessante matches te vinden van personen die lijken op een favoriete persoon, bijvoorbeeld een beroemdheid.[341] In de nabije toekomst zouden datingplatforms echter ook gezichtsherkenning kunnen gebruiken om een veiliger omgeving te creëren, mogelijk met dezelfde doeleinden als Facebook;[342] in dat geval zou het misbruiken van de foto van iemand anders ook hier de identiteitsfraude van artikel 231a lid 2 Sr kunnen opleveren.

Concluderend kunnen wij stellen dat in bepaalde gevallen het misbruiken van gezichtsherkenningstechnologie onder de strafbaarstelling van biometrie-gerelateerde identiteitsfraude valt. Dat is alleen het geval in situaties waarin deze technologie wordt toegepast voor het vaststellen van iemands identiteit. Van de in dit rapport behandelde toepassingen is dat bijvoorbeeld het geval bij toegangscontrole of bij online platforms als Facebook die gezichtsherkenning inzetten om de betrouwbaarheid van het platform te vergroten. De strafbaarstelling van identiteitsfraude kan in die gevallen helpen om misbruik van gezichtsherkenning tegen te gaan. In situaties waarin gezichtsherkenning niet als zodanig wordt toegepast voor het vaststellen van iemands identiteit, heeft eventueel misbruik van de technologie niet het karakter van identiteitsfraude en is het dus logisch dat de strafbaarstelling dan niet van toepassing is.

Andere strafbepalingen

Heimelijke observatie en identiteitsfraude zijn de strafbaarstellingen die het dichtst in de buurt komen bij onrechtmatige gezichtsherkenning, aangezien gezichtsherkenning met camera's plaatsvindt en een vorm van biometrie gebruikt. Afhankelijk van de context kunnen ook andere strafbepalingen relevant zijn. Deze zijn echter slechts zeer indirect van toepassing op gezichtsherkenning, zodat wij deze bepalingen hier slechts in vogelvlucht behandelen.

- *Heling van gegevens* (art. 139g Sr): indien bij het gebruik van gezichtsherkenning beelden worden vastgelegd op een manier die onder art. 139f Sr valt (dus heimelijk op een besloten plaats), is het bezit van deze beelden vervolgens ook strafbaar. Dit was van oudsher een zelfstandig onderdeel van art. 139f (onder 2º) Sr-oud, maar is bij de Wet computercriminaliteit III per 1 maart 2019 opgegaan in een algemenere strafbaarstelling van heling van gegevens in art. 139g Sr: bezit of verspreiding van niet-openbare gegevens waarvan men weet (of redelijkerwijs moet vermoeden) dat die uit misdrijf zijn verkregen. Heimelijk gemaakte

[341] Zie bijvoorbeeld Francesca Gillett, 'Dating App's Feature Lets You Go Out With People Who Look Like Your Celebrity Crush' (2017) The Evening Standard <www.standard.co.uk/news/uk/dating-app-uses-face-recognition-to-match-users-with-their-favourite-celebrity-lookalikes-a3583976.html> geraadpleegd 21 februari 2020.
[342] Zie bijvoorbeeld <www.kairos.com/dating> geraadpleegd 7 januari 2020.

gelaatsfoto's die verder worden verspreid ten behoeve van gezichtsherkenningstoepassingen scheppen dus ook strafbaarheid voor de ontvanger en verdere verspreider daarvan.

- *Seksuele afbeeldingen en wraakporno* (art. 139h Sr): in januari 2020 is een wet in werking getreden die de strafbaarstelling van heimelijke observatie aanvult, voor zover het gaat om afbeeldingen van seksuele aard.[343] Lid 1 stelt strafbaar het opzettelijk en wederrechtelijk maken van een afbeelding van seksuele aard, bijvoorbeeld *upskirt*-foto's (en de heling van zulke afbeeldingen); in lid 2 wordt de openbaarmaking van aldus gemaakte foto's strafbaar gesteld, maar ook in meer algemene zin het openbaar maken van een afbeelding van een persoon van seksuele aard 'terwijl hij weet dat die openbaarmaking nadelig voor die persoon kan zijn.' Dit laatste ziet vooral op wraakporno. Een afbeelding van seksuele aard is 'een afbeelding die een zodanig intiem seksueel karakter heeft dat deze door ieder redelijk denkend mens als privé zal worden beschouwd.'[344] Toepassingen van gezichtsherkenning zullen normaliter niet leiden tot afbeeldingen van seksuele aard (behalve wellicht op naaktstranden, in sauna's of in nudistengebieden, maar daar is het openlijk gebruik van camera's sowieso vaak gelimiteerd, zodat de strafbaarstelling van heimelijke observatie daar zal volstaan).
- *Onderscheppen van communicatie* (art. 139c Sr): deze bepaling betreft het opzettelijk en wederrechtelijk met een technisch hulpmiddel aftappen of opnemen van telecom- of computergegevens, oftewel aftappen van gegevens. Dit kan aan de orde zijn in gevallen waarin biometrische templates worden onderschept ten behoeve van een gezichtsherkenningstoepassing. Hetzelfde geldt voor *computervredebreuk* (art. 138ab Sr): als iemand een computer hackt en een bestand met biometrische templates kopieert, is dit strafbaar (met de strafverzwarende omstandigheid van het kopiëren van gegevens uit lid 2).
- *Smaad, laster, belediging* (art. 261/262/266 Sr): denkbaar is dat gezichtsherkenning wordt gebruikt om foto's die online staan van personen wier identiteit onbekend is, aan een bepaalde persoon toe te schrijven en dat vervolgens bekend te maken. Als de foto een compromitterend gehalte heeft (bijvoorbeeld een naaktfoto of een foto van dronken mensen op een Love Parade), kan de publicatie van iemands naam in combinatie met de foto in sommige gevallen een uitingsdelict als smaad of belediging opleveren, bijvoorbeeld als dit gepaard gaat met een snerende opmerking.
- *Belaging* (art. 285b Sr): belaging (*stalking*) betreft het wederrechtelijk stelselmatig opzettelijk inbreuk maken op iemands privacy met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen. Gezichtsherkenning maakt het mogelijk om iemand geautomatiseerd te herkennen en daarmee te volgen op camerabeelden. Dit volgen zal normaliter niet gebeuren met de bedoeling om de gevolgde persoon vrees aan te jagen of

[343] *Staatsblad* 2019, 311 (Wet herwaardering strafbaarstelling actuele delictsvormen), inwerkingtreding 1 januari 2020 (*Staatsblad* 2019, 421).
[344] *Kamerstukken II* 2018/19, 35 080, 3, 22.

haar gedrag te doen veranderen. Gezichtsherkenning kan wellicht wel een versterkend of faciliterend effect hebben in gevallen waarin iemand al wordt gestalkt.

- *Afdreiging* (art. 318 Sr): wanneer gezichtsherkenning wordt gebruikt om onbekende personen op online compromitterende foto's te identificeren, zou deze identificatie gebruikt kunnen worden om te persoon af te dreigen (dwingen geld te geven onder dreiging van smaad of bekendmaking van een geheim).

Concluderend kunnen wij vaststellen dat diverse strafbaarstellingen in bepaalde, tamelijk uitzonderlijke, situaties van toepassing zijn op diverse vormen van misbruik van gezichtsherkenningstechnologie. Die situaties behelzen vooral gevallen waarin reeds andere strafbare feiten zijn of worden gepleegd, zoals computervredebreuk, of gevallen waarin misbruik van gezichtsherkenning een nieuwe modus operandi is voor een bestaand strafbaar feit, zoals afdreiging. Omdat misbruik van gezichtsherkenningstechnologie niet het primaire element is in deze situaties, maar eerder een bijproduct is van andere typen strafbare feiten, fungeren deze strafbepalingen hooguit als aanvullingen op de rechtsbescherming tegen misbruik van gezichtsherkenning. Voor bescherming tegen bepaalde vormen van misbruik van gezichtsherkenning als zodanig zal de burger vooral aangewezen zijn op de strafbaarstellingen van heimelijke observatie en, in voorkomende gevallen, identiteitsfraude.

6.3.2. **Conclusie**

De belangrijkste strafbepalingen die relevant zijn voor gezichtsherkenning zijn de strafbaarstellingen van heimelijke observatie in artikelen 139f en 441b Sr en identiteitsfraude in artikel 231a. In de volgende gevallen is de strafbaarstelling van heimelijke visuele observatie echter niet van toepassing, terwijl het wel om mogelijk strafwaardige handelingen gaat. Het betreft situaties waarin er heimelijk gebruik wordt gemaakt van gezichtsherkenning en burgers zich daar niet bewust van hoeven te zijn:

- heimelijk gebruik van gezichtsherkenning met zichtbaar gebruikte camera's;
- heimelijk gebruik van gezichtsherkenning met een enigszins heimelijk gebruikte smartphone-camera (bijvoorbeeld van achter de rug van iemand): hierbij is geen (of niet per se) sprake van vastleggen van beelden (noch van doorgifte aan een apparaat waarbij iemand beelden live uitkijkt).

Naar analogie met de bestaande bescherming tegen het heimelijk maken van afbeeldingen (art. 139f en 441b Sr), valt er volgens ons iets te zeggen voor het strafbaar stellen van deze vormen van heimelijke gezichtsherkenning. Zowel bij heimelijk afbeeldingen maken als bij heimelijke gezichtsherkenning ontstaat immers een bepaald beeld van een persoon door een handeling die deze persoon niet verwacht en die daarom een significante belemmering kan vormen van haar vrijheid onbevangen zichzelf te zijn.

6.4. Resultaten van de rechtsverkenning

De in dit hoofdstuk beschreven rechtsverkenning dient ter beantwoording van sub-vraag 2.1: *Kunnen de geïdentificeerde privacyrisico's worden voorkomen of beperkt door bestaande juridische middelen? Zo ja, door welke en hoe? Wat zijn de (mogelijke) juridische lacunes?*

Deze verkenning richt zich op de rechtsgebieden privacy- en gegevensbescherming, privaatrecht en strafrecht. Meer rechtsgebieden kunnen van toepassing zijn, maar in deze rechtsverkenning kunnen wij niet alle mogelijke rechtsgebieden behandelen. Het hoofdstuk toont duidelijk aan dat het gebruik en de inzet van gezichtsherkenning in horizontale verhoudingen maar in beperkte gevallen zal zijn toegestaan bij wet. Er zijn juridische vragen omtrent, onder meer, het heimelijk observeren en identificeren van personen, het bestaan van een legitieme verwerkingsgrondslag en meer in het algemeen zijn er twijfels over de noodzakelijkheid, proportionaliteit en subsidiariteit van dergelijke technieken. Het enkele feit dat een gebruiker instemt met een technologie of toepassing maakt het gebruik daarvan nog niet geoorloofd.

Daarbij moet in ogenschouw worden genomen dat voor het gebruik van gezichtsherkenning biometrische gegevens worden verwerkt die juridisch gezien zijn aangemerkt als bijzondere persoonsgegevens, waarvoor een nee-tenzij regime geldt. De wetgever geeft voor het gebruik van biometrische gegevens in horizontale verhoudingen (specifiek: werkgever-werknemer relatie) het voorbeeld dat het voor een kerncentrale toegestaan kan zijn om gebruik te maken van gezichtsherkenningstechnologieën om zo slechts geregistreerde werknemers toegang te verlenen tot de faciliteit. Daarmee zijn de meeste andere in deze studie besproken voorbeelden onvergelijkbaar in ernst, belang en noodzaak.

Toch is de regulering thans niet spijkerhard. Zo bleek uit de vorige hoofdstukken dat de kennis van de wet niet bij alle partijen die gezichtsherkenningstechnologieën (willen) gebruiken optimaal is en met name worden de regels lang niet altijd afgedwongen door middel van handhaving door toezichthouders of door rechtszaken door burgers die nadelig (zouden) zijn getroffen door dergelijke toepassingen. Hierdoor ontstaat er ruimte voor partijen om te experimenteren met gezichtsherkenningstechnologie terwijl het de vraag is of de meeste van de thans gangbare toepassingen in overeenstemming zijn met de wet. Er bestaat dus met name een lacune tussen wet en praktijk. Deze lacune kan op verschillende wijzen worden opgevuld, zo zal meer uitgebreid worden besproken in het volgende hoofdstuk.

7. Reguleringsopties voor het voorkomen of beperken van privacy-inbreuken: een antwoord op de tweede onderzoeksvraag

Op basis van het onderzoek beschreven in hoofdstuk 5 en 6, richten wij ons nu op het beantwoorden van de tweede onderzoeksvraag onderliggend aan dit project: *Hoe kunnen huidige en potentiële privacy-inbreuken worden voorkomen of beperkt?* Verschillende reguleringsstrategieën zijn in de studie naar voren gekomen. In dit hoofdstuk hebben wij de naar ons oordeel meest relevante opties geselecteerd en tegen elkaar afgezet. Wij zijn hierbij uitgegaan van een brede opvatting van regulering, waarbij zowel is gekeken naar juridische instrumenten als naar mogelijkheden om via sociale normen of technisch ontwerp te reguleren.[345]

Ter beantwoording van sub-onderzoeksvraag 2.2 *(Welke reguleringsstrategieën (juridisch en anderszins) hanteren overheden, bedrijven en burgers in de praktijk om de privacyrisico's van het gebruik van gezichtsherkenningstechnologie voor burgers te beperken?)*, belichten wij allereerst een aantal bestaande maatregelen die door bedrijven zelf als privacy bevorderend worden beschreven en ervaren (zogenaamde *best practices*) (zie paragraaf 7.1). Deze reguleringsstrategieën hebben met name betrekking op sociale normen en het ontwerp van de technologie. In paragraaf 7.1 ligt de nadruk daarom op bedrijven. De, naar ons inziens, belangrijkste reguleringsstrategieën waarover de wetgever beschikt, bespreken we apart, onder de noemer van reguleringsopties in paragraaf 7.2. De mogelijke strategieën die burgers –kunnen– ontwikkelen, stippen wij kort aan in 5.3.5 en 7.2.1 (sub-paragraaf *bewustwording*).

Sub-onderzoeksvragen 2.3 (*Welke van de geïnventariseerde reguleringsstrategieën zijn succesvol, en waarom?*) en 2.4 *(Lenen –onderdelen van– deze succesvolle reguleringsstrategieën zich ertoe te worden omgebouwd tot algemeen verbindende voorschriften in wetgeving om de geïdentificeerde juridische lacunes af te dekken? Zo ja, hoe? Is hier binnen de huidige wetgeving ruimte voor? Zo nee, lenen deze inzichten zich anderszins voor de regulering van de privacyrisico's van het gebruik van gezichtsherkenningstechnologie?)* hebben wij op basis van het onderzoek niet kunnen beantwoorden omdat het niet mogelijk bleek de impact van de gebezigde strategieën (de *best practices*) in kaart te brengen. Wel hebben wij op basis van de gepercipieerde impact enkele suggesties gedaan waar deze strategieën (bij aangetoonde effectiviteit) de voorgestelde reguleringsopties mogelijk kunnen versterken. De inzichten die 7.1 en 7.2 voortbrengen, samen met de conclusies van de rechtsverkenning uit hoofdstuk 6, lenen zich, ons inziens, afdoende om vraag 2 te beantwoorden.

[345] Zie ook: L Lessig, *Code: Version 2.0*. (Basic Books 2006).

7.1. Best practices

Het was één van de (deel)vragen van dit onderzoek om in kaart te brengen welke reguleringsstrategieën overheden, bedrijven en burgers toepassen om de privacyrisico's van het gebruik van gezichtsherkenningstechnologie voor burgers te beperken. Wij hebben ons daarbij primair gericht op de reguleringsstrategieën die de geïnterviewde bedrijven nu reeds in praktijk brengen om sommige van de vastgestelde privacyrisico's tegen te gaan, zogeheten *best practices*. De naar ons oordeel meest relevante strategieën die wij tegenkwamen zijn:

Dienstverlening en producten in plaats van data als pijler van het bedrijfsmodel
De voor dit onderzoek bestudeerde bedrijven geven aan geleerd te hebben van de privacy-incidenten van de grote internetbedrijven de afgelopen tien jaar. Er wordt expliciet gekozen voor een bedrijfsmodel dat niet is gebaseerd op het verhandelen van data, maar het leveren van diensten en producten. Voor die dienst of dat product moet met geld en niet met data betaald worden. Hierbij zetten bedrijven in op het zo weinig mogelijk bezitten van databases en zoveel mogelijk controle over de data decentraal, bij de gebruiker zelf laten.

Privacy-by-design
De mogelijkheid om via het ontwerp van technologie privacyvriendelijk gedrag te bevorderen is een reguleringsstrategie die in de horizontale privacyrelatie veelbelovend lijkt.[346] Sommige voor dit onderzoek bestudeerde bedrijven zetten ook zelf in op het verankeren van privacy in het ontwerp en functioneren van hun systemen. Zo zijn er in het systeem vastgelegde momenten wanneer data worden verwijderd en foto's, na te zijn omgezet naar versleutelde templates, onmiddellijk worden verwijderd; ook wordt er in bepaalde systemen voor gekozen geen persoonlijke data aan deze templates te koppelen en worden diensten ontwikkeld die automatisch bijhouden wanneer en door wie toestemming voor verwerking wordt gevraagd en wanneer deze komt te vervallen.

Om secundair gebruik van gezichtsherkenning tegen te gaan, worden templates opgeslagen in een format dat niet gebruikt kan worden buiten het eigen ecosysteem. Daarnaast ontwikkelen verschillende bedrijven systemen waarbij de controle over de gezichtsdata niet bij een of meerdere bedrijven ligt, maar bij de persoon zelf, bijvoorbeeld door middel van persoonlijke datakluizen. Met behulp van apps kan de persoon dan zelf de toegang beheren en inzien wanneer welke camera's zijn of haar gezicht proberen te herkennen.

Ook kunnen ontwikkelaars via de interface bepaalde gedragsnormen stimuleren, bijvoorbeeld door de gebruiker expliciet toestemming te laten vragen voor het opnemen van een

[346] Vgl. t.a.v. de aan gezichtsherkenning verwante problematiek van augmented reality: Michael Katell e.a., 'Seeing the Whole Picture: Visualising Socio-Spatial Power through Augmented Reality', (2019) 11 Law, Innovation and Technology 279 (forthcoming).

persoon in een gezichtenbestand of door de gebruiker extra handelingen te laten verrichten waardoor het voor anderen duidelijk wordt dat deze persoon bezig is met gezichtsherkenning. Dit zien wij bijvoorbeeld bij de SeeingAI app, waar de gebruiker de camera expliciet moet richten op een te-herkennen persoon en het hele proces wel enkele seconden duurt.

Bedrijfswaarden

Bij zowel de kleine als gevestigde bedrijven is er veel aandacht voor bedrijfswaarden en hoe deze vorm moeten geven aan de samenwerkingen die aangegaan worden met andere bedrijven. Belangrijke waarden die worden genoemd zijn transparantie, toestemming, eerlijkheid (fairness), en verantwoording. Door deze bedrijfswaarden als leidraad te gebruiken in hun operaties, komt het voor dat sommige samenwerkingen worden afgewezen. In sommige gevallen leiden deze bedrijfswaarden ook tot strengere eisen dan juridisch noodzakelijk is. Deze focus op bedrijfswaarden heeft in meerdere gevallen er ook toe geleid dat bedrijven niet de gezichtsherkenningssoftware als API of apart product aanbieden, maar uitsluitend in geïntegreerde systemen die deze waarden moeten reflecteren.

Voorlichting

Omdat bedrijven zich bewust zijn van de privacyrisico's, investeren sommige ook actief in voorlichting. Deze communicatie is niet alleen gericht op potentiële, professionele klanten maar ook op de overheid en het bredere publiek. Hierbij wordt kennis gedeeld over de mogelijkheden die gezichtsherkenning biedt en hoe deze tot meerwaarde kan leiden, maar er wordt ook uitgebreid stilgestaan bij de risico's. Voorlichting richting professionele klanten betreft zowel wat de technologie wel, maar ook wat die niet vermag; daarnaast kan er worden stilgestaan bij de vraag wat ervoor nodig is om de technologie op een verantwoorde manier in zetten, bijvoorbeeld in termen van menselijke controle en organisatorische aanpassingen.

Regulering

Alle bedrijven die wij hebben gesproken roepen daarbij op tot verdere ontwikkelingen op het gebied van wet -en regelgeving. Met name het verder uitleggen en specifiëren van wettelijke bepalingen wordt hierbij genoemd. Ook het belang van strenge handhaving wordt onderstreept.

Toestemming

Sommige bedrijven vragen altijd om expliciete toestemming, ook al is dit –bijvoorbeeld in sommige Amerikaanse staten– niet vereist. Deze extra inspanning van bedrijven om meer controle te geven aan het datasubject kan aangemerkt worden als een *best practice*.

Zoals beschreven in het vorige hoofdstuk is toestemming echter vaak ook een wettelijke plicht. Het kader dat door de Algemene Verordening Gegevensbescherming wordt geboden vereist, behalve in gevallen waarin biometrische gegevens worden verwerkt voor identificatie- en

authenticatiedoeleinden voor zwaarwichtige redenen, dat er toestemming wordt gegeven door degene wiens gezicht wordt herkend. Het is dan ook de vraag of toestemming nog steeds als *best practice* kan worden aangemerkt als het een wettelijke plicht is. Is het bovendien realistisch om van burgers te verwachten dat zij controle houden over hun data als dergelijke technologieën wijdverbreid in burger-burger relaties worden gebruikt? Snappen zij de implicaties en gevolgen van deze technologie? Is het geen privatisering van sociaal-maatschappelijk vraagstukken om de toelaatbaarheid van een dergelijke ingrijpende technologie afhankelijk te maken van de toestemming van de individuele burger van geval tot geval?

Al deze reguleringsstrategieën zijn aangemerkt als *best practices* omdat de verwachting is dat ze uiteindelijk bijdragen aan de privacybescherming van burgers. De effectiviteit van deze strategieën hebben wij in dit onderzoek echter niet kunnen beoordelen. Wel zien wij dat deze reguleringsstrategieën dikwijls voortvloeien uit of een reactie zijn op het aanwezig juridisch kader. Waar de juridische verplichting ophoudt en de *best practice* begint is daarom niet eenduidig vast te stellen. Meer onderzoek naar de reikwijdte en effectiviteit van deze maatregelen en de wisselwerking met het juridisch kader is dan ook wenselijk.

7.2. Reguleringsopties Nederlandse wetgever

Als de Nederlandse wet- en regelgever sturend wil optreden, dan zijn er verschillende reguleringsopties denkbaar, zo is gebleken uit deze studie. De naar ons oordeel meest relevante reguleringsopties hebben wij hieronder kort opgenomen. Voor al deze reguleringsopties geldt dat Nederland ervoor kan kiezen om een eigenstandige koers te varen, primair in te zetten op internationale regulering, met name in EU verband, of een combinatie van beide.

7.2.1. **Reguleringsopties**

Totaal verbod:
Allereerst kan de Nederlandse wetgever ervoor kiezen om een (tijdelijk) totaalverbod neer te leggen voor het gebruik van gezichtsherkenningstechnologieën. Daarmee wordt duidelijkheid gegeven en wordt slechts een marginaal aantal mogelijke toepassingen die momenteel juridisch legitiem zou kunnen zijn in de kiem gesmoord. Anders gezegd: dit is nu nog een optie met relatief beperkte negatieve gevolgen. De functionaliteiten van apps zijn vooralsnog erg beperkt, de resultaten niet altijd betrouwbaar en de potentiële voordelen veelal marginaal. Als Nederland voor een strenge reguleringslijn zou kiezen, zou die lijn op een later moment, als de technologie en de toepassingen zich hebben ontwikkeld, nog eens kunnen worden geëvalueerd. Dit zou ook aansluiten bij de strengere lijn die zich in Brussel lijkt te ontwikkelen. Andere landen, zoals China en de Verenigde Staten, kunnen dan als het ware de proeftuinen zijn waar dergelijke technologieën

tot wasdom komen, of niet; als het moment daar is kan Nederland zich alsnog buigen over de vraag welke toepassingen eventueel wenselijk en toelaatbaar zijn en daar dan een specifieke en afgeschermde juridische ruimte voor creëren. Tot die tijd kan het totaalverbod in stand worden gelaten. Overigens is het – net als bij elk verbod – van groot belang naast de wet- en regelgeving een strategie te kiezen en aanpak te ontwikkeling om het verbod te handhaven.

Voorafgaande goedkeuring:
In deze optie mogen toepassingen slechts worden gebruikt en aangeboden als daarvoor voorafgaande goedkeuring is verkregen. Een vanzelfsprekende rol is hier weggelegd voor de Autoriteit Persoonsgegevens. Omdat het hier gaat om een technologie die gebruik maakt van bijzondere persoonsgegevens ligt het voor de hand om, voordat een dergelijke technologie wordt ingezet, een Data Protection Impact Assessment (DPIA) te laten uitvoeren door de partij die goedkeuring vraagt. De AP zou een richtsnoer kunnen uitgeven waaruit volgt dat partijen deze DPIA altijd moeten voorleggen aan de AP en pas van start mogen gaan als zij expliciete goedkeuring van de AP hebben gekregen. Voor een model DPIA voor de specifieke context van gezichtsherkenning zou kunnen worden onderzocht hoe de *best practices* en richtsnoeren die nu al binnen sommige bedrijven zijn ontwikkeld hieraan bij kunnen dragen.[347]

Gediversifieerde aanpak:
Aangezien de meeste toepassingen van gezichtsherkenningstechnologieën niet zijn toegestaan onder het huidige juridische regime, maar een aantal mogelijk wel, en hier verwarring over kan ontstaan, kan de wetgever, regering of de Autoriteit Persoonsgegevens besluiten expliciet aan te geven welke toepassingen zijn toegestaan en welke niet. Een belangrijk element hierin zou kunnen zijn het expliciet strafbaar stellen van het onrechtmatig heimelijk gebruik van gezichtsherkenningstechnologieën, zelfs als de camera zelf wel kenbaar is.

Regelgevend kader specifiek voor gezichtsherkenning:
De wetgever of de AP hebben de vrijheid om, al dan niet in samenwerking met andere toezichthouders en (internationale) partijen, een specifiek regelgevend kader te ontwikkelen voor gezichtsherkenningstechnologieën, waarin de algemene juridische principes en uitgangspunten concreet worden uitgewerkt voor wat betreft deze technologie en voor het soort toepassingen dat voorzien zijn en legitiem worden geacht.

Controle achteraf:

[347] De autoriteit persoonsgegevens heeft aangegeven dat een effectbeoordeling verplicht is voor grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren. <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf> geraadpleegd 21 februari 2020.

Er kan ook voor worden gekozen om het huidige regelgevende kader in stand te laten en in te zetten op ex post controle op technologieën, toepassingen en het gebruik daarvan. Deze controle kan plaatsvinden ofwel op initiatief van een burger of bedrijf die een klacht indient ofwel op initiatief van een handhavende organisatie, waarbij de Autoriteit Persoonsgegevens wederom de meest aangewezen instantie lijkt om deze controle uit te voeren.

Gedragscodes en certificering:
De Algemene Verordening Gegevensbescherming maakt het mogelijk om voor specifieke sectoren of toepassingen een aparte gedragscode te ontwikkelen, met een sectorspecifieke handhavende en toezichthoudende organisatie die door die code wordt opgericht. Of het bij gezichtsherkenning echt om een aparte sector gaat waarbij een vertegenwoordigende instantie een dergelijke code kan opstellen en voorleggen aan de AP is echter de vraag. Wellicht ligt het werken met certificering meer voor de hand, waarvoor de AVG ook ruimte biedt. Het is dan aan een eventueel geaccrediteerd certificeringsorgaan om een certificaat te geven aan een bedrijf dat wordt geacht gezichtsherkenningstechnologie in overeenstemming met de AVG in te zetten. De AP kan toezicht houden of dergelijke certificering juist geschiedt. Zowel de gedragscodes als certificering zijn voorzien in de AVG voor wat betreft compliance met het gegevensbeschermingsrecht, maar beide instrumenten kunnen ook breder worden ingezet.

Bewustwording:
De overheid kan inzetten op publiekscampagnes om burgers en bedrijven duidelijk te maken welke gevaren en juridische (en mogelijkerwijs ook sociale en ethische) grenzen er zijn aan het toepassen van gezichtsherkenningstechnologieën, met name als het gaat om de privacy van (andere) burgers. Sociale normen en waarden vormen in het licht van de beperkingen van wet, markt en technologie een belangrijk aanvullend reguleringsmechanisme.

In burger-burger-relaties zullen sociale normen een belangrijke rol (moeten) spelen in de manier waarop gezichtsherkenning wordt toegepast. Een voorbeeld van een relevante sociale norm is 'civil inattention': welbewust *niet* de aandacht richten op iemand in situaties waarin die persoon verwacht of aangeeft niet het object van aandacht te willen zijn (denk aan het naar de grond staren in een drukke lift). Bij gezichtsherkenning zou een sociale norm behulpzaam kunnen zijn om smartphones bewust *niet* te richten op personen op een manier dat die zich bekeken, herkend en gecategoriseerd zouden voelen. Beleidsinterventies gericht op bewustwording en nudging zouden kunnen bijdragen aan het ontwikkelen van sociale normen die de privacyrisico's van gezichtsherkenning kunnen helpen te beperken.[348]

Ook ten aanzien van bedrijven kan hier nog het nodige worden gewonnen. Zoals eerder aangegeven maakt bijvoorbeeld het enkele feit dat een gebruiker instemt met een technologie of

[348] Zie over deze problematiek en oplossingsrichting Tamar Sharon en Bert-Jaap Koops, 'Facial recognition and the Ethics of Indifference: Revitalising Civil Inattention As A Privacy-Protecting Mechanism in Public Spaces', (2018) paper workshopped at Amsterdam Privacy Conference 2018.

toepassing nog niet dat het gebruik daarvan geoorloofd is. Aangezien dit laatste punt mogelijk niet bij elk bedrijf bekend zal zijn kan een goede uitleg van de bestaande wet- en regelgeving op dit punt nog het nodige opleveren. Ook zou een onderzoek van de AP naar de toelaatbaarheid van gezichtsherkenningstechnologie in een specifiek geval ook een duidelijke normerende werking kunnen hebben voor andere bedrijven die dergelijke technologie inzetten of dat overwegen. De uitkomsten van een dergelijk onderzoek kunnen meer bewustwording creëren ten aanzien van de mogelijke gevaren van gezichtsherkenningstechnologieën bij zowel burgers als bedrijven die deze technologie wensen te gebruiken als bij de burgers die aan dergelijke technologieën (kunnen) worden onderworpen.

Gedoogbeleid:
Tot slot kan de AP of regering in beleid aangeven dat het gebruik van gezichtsherkenning voor een bepaalde tijdsperiode zal worden gedoogd en naleving van wettelijke kaders niet zal worden afgedwongen, om het zo de kans te geven tot volle wasdom te komen en pas daarna te evalueren welke voordelen en mogelijke nadelen er zijn aan de na een aantal jaar ontwikkelde gezichtsherkenningstechnologieën. Wel moet worden bedacht dat burgers hun rechten als vervat in het Europees Verdrag voor de Rechten van de Mens en de Algemene Verordening Gegevensbescherming kunnen afdwingen via rechterlijke procedures en dat daar uiteindelijk het Europees Hof voor de Rechten van de Mens respectievelijk het Europees Hof van Justitie een oordeel over zal vellen.

7.2.2. **Type relaties en contexten**

In de vorige sub-paragraaf is een aantal van de door ons meest relevant geachte, in deze studie naar voren gekomen, reguleringsopties besproken. Deze studie geeft geen antwoord op de vraag welke van deze opties het meest wenselijk of voor de hand liggend is. Wel volgt uit deze studie dat er duidelijke verschillen bestaan in termen van de (vermeende) voordelen en de privacyrisico's tussen het type relaties waarbinnen de gezichtsherkenningstechnologieën worden ingezet en de contexten waarbinnen dat geschiedt. In horizontale verhoudingen kan een onderscheid worden gemaakt tussen drie verschillende type relaties:

- *Burger-burger*: Bij het gebruik van apps en andere toepassingen die gebruik maken van gezichtsherkenning in burger-burger relaties hebben wij in deze studie geen voorbeelden gezien die de toets van noodzakelijkheid, proportionaliteit, subsidiariteit en legitimiteit zullen doorstaan. Het gaat in deze relaties vaak om betrekkelijk beperkte nadelen voor de burger op wie gezichtsherkenning wordt toegepast. Veelal zijn aan de zijde van de gebruiker echter ook slechts vrij marginale belangen gemoeid. De toepassingen hebben meer het karakter van leuke gadgets dan van noodzakelijke hulpmiddelen. Daarbij dient te

worden opgemerkt dat de technologie echter wel kwaadwillende burgers kan faciliteren in hun handelen (denk aan stalking of identiteitsdiefstal). Op dit ogenblik hebben burgers toegang tot commerciële diensten die hen de mogelijkheid bieden om zelf met gezichtsherkenningstechnologie aan de slag te gaan.

- *Bedrijf-burger*:[349] Bij het gebruik van dergelijke apps in bedrijf-burger relaties gelden ook de nodige bedenkingen. Alhoewel het daar gaat om toepassingen voor aanzienlijke doeleinden is daar het belangrijkste juridische struikelblok dat er goede en minder invasieve technologische alternatieven bestaan. Toegang tot een sportfaciliteit of concertgebouw kan zonder gebruikmaking van gezichtsherkenning, namelijk door een sportpas of een concertkaartje. Een indruk krijgen van hoeveel mensen er zich in een zaal begeven kan ook zonder gezichtsherkenning in te zetten.
- *Werkgever-werknemer*: Het gebruik van gezichtsherkenningstechnologieën in een werkgever-werknemerrelatie is al kort besproken. Daaruit blijkt dat, in elk geval als de werknemer geen vrije toestemming kan geven voor het gebruik van dergelijke technologieën, er een beroep zal moeten worden gedaan op een andere verwerkingsgrond dan toestemming. Dat zal grosso modo alleen het bestaan van een zwaarwegend algemeen belang kunnen zijn. Daarvan kan sprake zijn in uitzonderlijke gevallen, zoals bij het gebruik van gezichtsherkenning voor identificatie en authenticatie bij kerncentrales.

Ook kan er een onderscheid worden gemaakt tussen verschillende doeleinden waarvoor de gezichtsherkenningstechnologie wordt ingezet. Daarbij is er evident overlap met de vorige opsomming; het is slechts een andere manier om de diverse toepassingen te categoriseren. Hieronder zullen vier doeleinden kort worden besproken die in deze studie aan bod zijn gekomen:

- *Zorgdoeleinden*: Een bijzondere context is de medische context, waar het gaat om bijzonder kwetsbare personen en bijzonder gevoelige gegevens. Dit kan zowel in de professionele zorgcontext (bedrijf-klant) of in de particuliere context, zoals mantelzorg, (burger-burger). Toch is het ook een context waar gezichtsherkenningstechnologieën personen op termijn zouden kunnen helpen en ondersteunen in hun leven en autonomie. Het herkennen van personen of het toegang verlenen tot het huis van een persoon met geheugenverlies, een app die slechtzienden helpt om mensen in hun directe omgeving waar te nemen, een zorgrobot die aan de gezichtsuitdrukking kan zien in welke gemoedstoestand zijn eigenaar verkeert en daarop acteert en mogelijke andere toekomstige toepassingen zijn voorstelbaar als nuttig en wenselijk in de medische context.
- *Commerciële doeleinden*: Veel van de voorziene toepassingen van gezichtsherkenningstechnologie zijn te categoriseren binnen de bedrijf-burger relatie, waarbij het gaat om het vergroten van het gebruikersgemak (sneller inchecken), het

[349] De burger is hier vooral in de rol van klant.

inspelen op emoties van klanten om producten of diensten aan te passen of om efficiëntere bedrijfsvoering te bewerkstelligen.

- *Beveiligingsdoeleinden*: Gezichtsherkenning kan ook worden gebruikt voor beveiligingsdoeleinden, zoals het gebruik van gezichtsherkenningstechnologieën voor identificatie- en authenticatiedoeleinden ten aanzien van kritische infrastructuur. In hoeverre een slimme deurbel, ingezet anders dan voor zieken en hulpbehoevenden, nu echt moet worden gezien als een hulpmiddel in het kader van een veilig toetredingsbeleid van een privéwoning of eerder moet worden gezien als een leuke gadget is op dit moment niet eenduidig vast te stellen.
- *Recreatieve doeleinden*: Veel van de toepassingen van gezichtsherkenningstechnologie binnen burger-burgerrelaties zijn aan te merken als toepassingen voor recreatieve doeleinden.

7.2.3. **Benaderingswijzen**

Het is aan de Nederlandse regering, de wetgevende macht en eventueel de relevante handhavende organisaties om te kiezen voor de juiste regulering. Dat kunnen zij doen op basis van het onderscheid in relaties of op basis van de doeleinden, zoals besproken in de vorige sub-paragraaf. Welke invulling de reguleringskeuze vervolgens krijgt, wordt mede bepaald door de verkozen benaderingswijze. Vier ideaaltypische benaderingswijzen zijn te onderscheiden:

- *Risicomijdend*: Er wordt van uitgegaan dat gezichtsherkenningstechnologieën momenteel nog weinig vermogen en dat het maar de vraag is of dit in de toekomst anders zal zijn. In ieder geval worden er de nodige nadelen en risico's gesignaleerd ten aanzien van de toepassing van dergelijke technologieën. Daarom wordt de inzet van deze technologieën zoveel mogelijk aan banden gelegd, eventueel tot nadere orde – tot het moment dat er aanleiding zou zijn om te geloven dat dergelijke technologieën meer voordelen zouden bieden dan momenteel het geval is. Dit sluit aan bij het voorzorgsprincipe: omdat het nu nog niet goed is in te schatten hoe de technologieën zich zullen ontwikkelen en hoe de gegevens die nu worden verzameld mogelijk in de toekomst worden gebruikt of misbruikt, past terughoudendheid.
- *Risicobeperkend*: Er wordt van uitgegaan dat gezichtsherkenningstechnologieën gebruik maken van zeer gevoelige gegevens en niet alleen zeer invasief zijn, maar ook de nodige risico's met zich mee kunnen brengen. Toch wordt erkend dat in bijzondere contexten en in bepaalde relaties, de toepassing van deze techniek een positief effect zou kunnen sorteren. Daarom wordt de regulering die momenteel voorhanden is nader ingevuld en verder bijgestuurd om duidelijk te maken dat gezichtsherkenningstechnologie in principe

niet kan worden gebruikt, tenzij waar expliciet aangegeven en onder de voorwaarden die zijn neergelegd, ofwel in wetgeving ofwel in andersoortige regulering.

- *Kans bevorderend*: Er wordt van uitgegaan dat gezichtsherkenningstechnologieën weliswaar een aantal risico's met zich meebrengt, maar ook de nodige kansen. Daarom wordt geopteerd voor een gediversifieerde aanpak waarbij binnen een aantal sectoren wordt ingezet op het toestaan van (experimenten met) gezichtsherkenningstechnologieën. Op basis van de resultaten die daar worden behaald en een evaluatie van de diverse voor- en nadelen wordt vervolgens een keuze gemaakt ten aanzien van de andere gebieden waarin gezichtsherkenningstechnologieën eventueel een rol zouden kunnen spelen.
- *Kans optimalisatie*: Er wordt van uitgegaan dat gezichtsherkenningstechnologieën zich op termijn zullen ontwikkelingen op een wijze die veel positieve effecten heeft voor de burger, het bedrijfsleven, de economie en het welzijn in Nederland. Deze positieve gevolgen kunnen in ieder geval, eventueel met hulp van ondersteunende maatregelen, de eventuele negatieve gevolgen overschaduwen. Daarom wordt het van belang geacht dat de diverse barrières en obstakels die er nu in de wetgeving zijn vervat zo veel mogelijk worden weggenomen.

7.2.4. **Handvatten voor de regelgever**

In onderstaande tabellen (tabel 7.1 en tabel 7.2) zal worden aangegeven welke reguleringsoptie voor de hand ligt ten aanzien van welke relatie respectievelijk welke doeleinden. Daarbij zullen de benaderingswijzen worden aangegeven in kleuren: **risicomijdend**, **risicobeperkend**, **kansbevorderend** en **kansoptimalisatie**.[350]

Deze tabellen zijn louter bedoeld als een hulpmiddel om op een transparante en systematische wijze te kunnen afwegen welke reguleringsopties het meest geschikt worden geacht. Ter verduidelijking: stel de regelgever opteert voor een risicomijdende benaderingswijze, welke type reguleringsoptie ligt dan voor de hand per relatie en context; stel de regelgever opteert voor een risicobeperkende benaderingswijze, welke type reguleringsoptie ligt dan voor de hand per relatie en context; etc.

Daarbij moet worden benadrukt dat in deze studie niet elk mogelijk denkbare toepassing, relatie of context waarbinnen gezichtsherkenning kan worden ingezet aan bod is gekomen en dat deze opsomming bovendien een selectie betreft van de door ons meest relevante geachte bevindingen van dit onderzoek.

[350] ////////////////////////////// staat voor de combinatie risicobeperkend/kansbevorderend.

	Burger-burger	Bedrijf-burger	Werkgever-werknemer
Totaal verbod			
Voorafgaande goedkeuring			
Gediversifieerde aanpak			
Specifiek Wettelijk kader	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////
Controle achteraf			
Sectorale controle			
Bewustwording			
Gedoogbeleid			

Tabel 7.1 Reguleringsopties per type relatie

	Zorgdoeleinden	Commerciële doeleinden	Beveiligings-Doeleinden	Recreatieve doeleinden
Totaal verbod				
Voorafgaande goedkeuring				
Gediversifieerde aanpak				
Specifiek Wettelijk kader	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////
Controle achteraf				
Sectorale controle				
Bewustwording				
Gedoogbeleid				

Tabel 7.2 Reguleringsopties per context

7.3. Drie keuzes

Dan zijn er tot slot nog drie vervolgvragen. Ten eerste is de vraag via welk juridisch instrument voor regelgeving en naleving wordt gezorgd. Het ligt voor de hand om een en ander via het civielrecht en onrechtmatige-daadsactie te laten verlopen voor het geval de burger of een bedrijf zelf actie wil ondernemen en dat de overheid een belangrijke handhavende rol kan spelen via onder meer de Autoriteit Persoonsgegevens. Uit deze studie is gebleken dat het strafrecht alleen een rol speelt in horizontale verhoudingen als een handeling normen van maatschappelijk acceptabel gedrag dusdanig overschrijdt dat deze als *moreel* onjuist moet worden gekwalificeerd, zoals het geval is bij heimelijke observatie en identiteitsfraude. In sommige situaties zal ook gezichtsherkenning onder die strafbepalingen kunnen vallen, bijvoorbeeld als dit met een heimelijk aangebrachte camera gebeurt of een biometrische beveiliging op basis van gezichtsherkenning wordt misbruikt. In veel gevallen valt gezichtsherkenning echter niet onder een bepaalde strafbepaling, terwijl deze wel privacyrisico's kan opleveren. Omdat de maatschappelijke normen in relatie tot het gebruik van gezichtsherkenning nog weinig zijn uitgekristalliseerd, zal het lang niet altijd duidelijk zijn wanneer een bepaalde toepassing als *moreel* onjuist moet worden gekwalificeerd.

Eventuele verboden ten aanzien van gezichtsherkenningstechnologieën zouden via het strafrecht geregeld kunnen worden, zoals bijvoorbeeld het doortrekken van de strafbaarstelling van het onrechtmatig heimelijk maken van afbeeldingen van personen naar heimelijke gezichtsherkenning. Hierbij moet worden afgewogen of toepassingen en gebruik zo ernstig zijn dat vervolging en handhaving via het strafrecht gepast is. In lijn met de strafbaarstelling van onrechtmatige heimelijke observatie (die vooral samenhangt met het gebruik van heimelijke camera's), valt te overwegen om ook het *onrechtmatig heimelijk gebruik van gezichtsherkenning* strafbaar te stellen in situaties waarin burgers zich wel bewust kunnen zijn van de aanwezigheid van camera's maar zich niet per se bewust zijn van gezichtsherkenningstoepassingen van die camera's. Dit is het geval bij heimelijk gebruik van gezichtsherkenning met zichtbare camera's (zoals zichtbaar aanwezige CCTV-camera's of smartphone-camera's). Evenals heimelijke observatie, zoals strafbaar gesteld in artikelen 139f en 441b Sr, kan zulk heimelijk gebruik van gezichtsherkenning een significante belemmering vormen van iemands vrijheid onbevangen zichzelf te zijn.[351]

[351] De in deze studie besproken reguleringsoptie zijn primair materieel rechtelijk van aard. Procesrechtelijk is in een andere studie voor het WODC reeds uiteengezet welke aanpassingen zouden kunnen worden doorgevoerd in verband met de data-gedreven samenleving, zoals het leggen van een grotere nadruk op collectieve en algemene belangenacties. B. van der Sloot & S. van Schendel, De modernisering van het Nederlands procesrecht in het licht van big data: Procedurele waarborgen en een goede toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving, <https://www.wodc.nl/binaries/2900_volledige_tekst_tcm28-402015.pdf> geraadpleegd 21 februari 2020.

Ten tweede is de vraag waar drukpunten moeten worden geplaatst: op de ontwikkelaar van dergelijke technologieën, de aanbieder, de eventuele tussenpersoon of de gebruiker? Het antwoord op deze vraag zal afhangen van het reguleringsmodel dat wordt gekozen. Kiest men voor een streng beleid van gehele of gedeeltelijke verboden, dan lijkt het dat daar de aanbieder van dergelijke diensten de meest aangewezen normadressant is, gaat het om controle achteraf of voorafgaande toestemming, dan zal het doorgaans gaan om de gebruiker van de technologie, enzovoort.

Ten derde en tot slot is het van belang dat veel aanbieders van dergelijke diensten en producten uit de Verenigde Staten of Azië komen, waar andere regels gelden ten aanzien van het aanbieden en het gebruik. Dat kan problemen opleveren ten aanzien van de handhaving van de in Nederlands gestelde normen.

Evenwel is duidelijk dat de AVG een redelijke brede reikwijdte van het gegevensbeschermingsrecht voorstaat.[352] In de Verordening staat niet alleen dat alle verwerkingen van persoonsgegevens die plaatshebben op EU-grondgebied onder de Verordening vallen, maar ook dat als de persoonsgegevens worden verwerkt buiten de EU, maar dit in het kader gebeurt van de activiteiten van een vestiging in de EU, de AVG van toepassing is. Zelfs als organisaties helemaal geen vestiging hebben in de EU, dan nog is de AVG van toepassing als een organisatie ofwel producten ofwel diensten aanbiedt aan EU-burgers en daartoe persoonsgegevens verzamelt (denk aan een Amerikaanse webshop die ook een '.de' extensie van de webshop heeft om de Duitse markt te bereiken) of als zij het gedrag van EU-burgers monitort (denk aan een Amerikaans bedrijf dat een cookie op de computer van een EU-burger plaatst of op een andere wijze het internetgedrag van de persoon bijhoudt).

Deze zeer brede regel omtrent de territoriale reikwijdte van de AVG, gecombineerd met de regel dat persoonsgegevens slechts mogen worden doorgevoerd naar een land dat of organisatie die niet direct is gebonden aan de AVG als dat land of die organisatie zich committeert aan een beschermingsregime dat min of meer gelijk is aan de AVG,[353] heeft tot de term 'the Brussels effect' geleid.[354] Omdat vrijwel alle grote internationale bedrijven ook zaken doen in de EU of persoonsgegevens verwerken van EU-burgers, dienen zij zich in ieder geval voor dat gedeelte van hun bedrijfsprocessen te houden aan de gegevensbeschermingsregels van de EU. Deze regels zullen dan ook volgens velen de wereldwijde standaard zetten op dit punt.[355]

Alhoewel hier niet zozeer een juridische drempel ligt zal het toch niet altijd eenvoudig zijn Nederlandse regelgeving ten aanzien van het ontwikkelen van technologieën, het aanbieden van producten en diensten en het gemedieerd gebruik van deze producten en diensten goed af te dwingen ten aanzien van buiten de EU verblijvende partijen. Of dit consequenties heeft voor de

[352] Artikel 3 AVG.
[353] Artikel 44 e.v. AVG.
[354] Bradford, Anu (2012). "The Brussels Effect". Northwestern University Law Review. 107 (1). SSRN 2770634, Columbia Law and Economics Working Paper No. 533.
[355] Zie ook Zaak C-507/17, Europees Hof van Justitie 24 september 2019, ECLI:EU:C:2019:772.

inrichtingen van beleid en de keuze voor reguleringsopties is aan de Nederlandse regering, de wetgever en eventueel de relevante handhavende organisaties.

7.4. Conclusie

Centraal in dit hoofdstuk staat de vraag hoe privacy-inbreuken veroorzaakt door gezichtsherkenningstechnologie kunnen worden voorkomen of beperkt. Naast het in kaart brengen van *best practices* van bedrijven die deze technologie inzetten en/of produceren (waarvan het de verwachting is dat zij bijdragen aan de privacybescherming van burgers), hebben wij een aantal reguleringsopties geformuleerd dat zich bevindt op een spectrum van een totaalverbod tot gedoogbeleid. Afhankelijk van de door de wetgever verkozen benaderingswijze (van risicomijdend tot kans optimaliserend) en het type horizontale relatie en doel van de gezichtsherkenningstechnologie, kan een reguleringskeuze worden gemaakt. Als handvat voor het maken van een transparante en systematische keuze hebben wij tabellen toegevoegd.

8. Conclusies

Twee onderzoeksvragen liggen ten grondslag aan dit rapport, namelijk:

1) *Hoe wordt gezichtsherkenningstechnologie door Nederlandse burgers en bedrijven gebruikt en hoe kan het gebruik van gezichtsherkenningstechnologieën door burgers en bedrijven een inbreuk vormen op de privacy van de burger (nu en over vijf jaar)?*
2) *Hoe kunnen huidige en potentiële privacy-inbreuken worden voorkomen of beperkt?*

Om de onderzoeksvragen te beantwoorden hebben wij gebruik gemaakt van een combinatie van onderzoeksmethoden, zijnde: literatuurstudie, interviews, een expertworkshop en een juridische analyse. De literatuurstudie naar gezichtsherkenningstechnologie en de bijbehorende privacyrisico's is in eerste instantie breed opgezet om een goed idee te verkrijgen van de staat van de techniek en de verschillende risico's. Vervolgens is ervoor gekozen de literatuurstudie toe te spitsen op specifieke toepassingen van gezichtsherkenning in zogenaamde domeinstudies (bijvoorbeeld het domein detailhandel of evenementenorganisatie) en aan te vullen met interviews. De privacyrisico's en *best practices* die hierdoor werden bevonden, zijn verder uitgelicht en kritisch besproken tijdens een expertworkshop. Op basis van deze inzichten werd een juridische analyse uitgevoerd en de reguleringsopties voor het gebruik van gezichtsherkenningstechnologie door burgers en bedrijven in kaart gebracht.

Ter beantwoording van vraag 1 hebben wij vastgesteld dat Nederland zich op het gebied van gezichtsherkenning nog in de experimentele fase bevindt. Op beperkte schaal onderzoeken vooral bedrijven welke *use-cases* rendabel en acceptabel zijn in de Nederlandse context. Hierbij valt enige terughoudendheid op, mede ingegeven door juridische onzekerheid en vrees voor reputatieschade. Hoewel dit nog niet op grote schaal gebeurt, hebben wij vastgesteld dat het ook mogelijk is om als burger zelf aan de slag te gaan met het ontwikkelen en gebruiken van (eenvoudige) gezichtsherkenningstechnologie. Hiervoor zijn geen of zeer minimale programmeervaardigheden vereist.

In hoofdstuk 5 schetsen wij drie mogelijke ontwikkelingsrichtingen van gezichtsherkenningstoepassingen: voor gemak en efficiëntie (1), beveiliging en controle (2), personalisatie en proactieve dienstverlening (3). Het is onder meer afhankelijk van de door de Nederlandse wetgever gekozen reguleringsopties en de daarbij ingezette handhaving, of en hoe deze scenario's ook daadwerkelijk zullen plaatsvinden. De privacyrisico's die met deze ontwikkelingsrichtingen gepaard gaan zijn de volgende:

- *Ondoorzichtige informatieverzameling*. Bedrijven hebben waarschijnlijk een legacy probleem. Hun gezichtsherkenningsmodellen zijn getraind op data die veelal zonder medeweten van burgers zijn verkregen.

- *Autonomie staat onder druk*. De vrijheid van burgers om al dan niet te kiezen voor gezichtsherkenning wordt negatief beïnvloed doordat gezichtsherkenning frictieloos ingezet kan worden. Er is geen actieve handeling nodig van burgers waardoor een moment van reflectie dikwijls zal ontbreken. Om de gezichtsherkenningstoepassing bovendien rendabel te laten zijn, is er een incentive bij bedrijven om zoveel mogelijk burgers te overtuigen gezichtsherkenning te gebruiken. Dit kan in de toekomst leiden tot een uitgeklede terugvaloptie voor niet-gebruikers.
- *Bias en fouten in gezichtsherkenning*. Gezichtsherkenningstoepassingen kunnen uitkomsten genereren die discriminatoir van aard zijn en minder goed werken bij bepaalde groepen (zoals vrouwen, kinderen, personen met een getinte huidskleur). Dit kan leiden tot uitsluiting, discriminatie en stigmatisering, wat onder andere kan leiden tot inbreuken in gedragsmatige privacy en beslissingsprivacy.
- *Einde van anonimiteit*. Wanneer gezichtsherkenning in de horizontale relatie wijdverbreid geraakt, zal het de facto niet langer mogelijk zijn voor mensen om zich anoniem in de publieke, semi-publieke ruimte en zelfs private ruimte te begeven. Gedragsmatige privacy en ruimtelijke privacy komen hiermee onder druk te staan.
- *Afhankelijkheid van anderen*. Privacybescherming in de burger-burger relatie is moeilijk top-down te handhaven en zal in grote mate afhangen van het verantwoordelijk gebruik van burgers zelf.
- *Van horizontaal naar verticaal gebruik: secundair gebruik van informatie.* Gezien de datahonger van overheidsdiensten wereldwijd, is het niet onaannemelijk dat via omwegen –dus via de bedrijven– gepoogd zal worden gebruik te maken van de opbrengsten van gezichtsherkenningstechnologie. Het waarborgen van privacy in de horizontale relatie is dus ook van belang voor het beschermen van privacy in de verticale relatie.
- *Machtsongelijkheid en chilling effect*. De informatierijke profielen die hierdoor ontstaan kunnen leiden tot significante machtsverschillen in zowel de burger-burger alsook de bedrijf-burger relatie. Burgers kunnen niet meer inschatten wat anderen over hen weten en het risico op inmenging van derden in het nemen van besluiten neemt toe (mentale privacy). Dit kan ertoe leiden dat burgers hun gedrag aanpassen (gedragsmatige en associatieve privacy).

Ter beantwoording van vraag 2 hebben wij een rechtsverkenning uitgevoerd, gekeken naar bestaande *best practices* (wat doen bedrijven zelf om deze privacyrisico's tegen te gaan) en beschikbare reguleringsopties benoemd. Wij kiezen voor een brede opvatting van regulering in dit rapport, waarbij wij zowel juridische instrumenten als ook mogelijkheden om via sociale normen of technisch ontwerp te reguleren noemen. De meest voorkomende strategieën die wij bij bedrijven in dit onderzoek tegenkwamen zijn:

- *Dienstverlening en producten in plaats van data als pijler van het bedrijfsmodel.* Er wordt expliciet gekozen voor bedrijfsmodellen waarbij het verhandelen van data niet de kern is.
- *Privacy-by-design*. In het ontwerp van het systeem wordt zoveel mogelijk ingezet op privacyvriendelijke keuzes.
- *Bedrijfswaarden* zoals transparantie, toestemming, eerlijkheid (fairness), en verantwoording funderen en begrenzen bedrijfskeuzes.
- *Voorlichting*. Bedrijven investeren in informatiedeling.
- *Regulering*. Bedrijven zijn vragende partij voor duidelijke regulering.
- *Toestemming*. Bedrijven opteren voor toestemming, ook als dit niet nodig is (met de aantekening dat toestemming ook duidelijke tekortkomingen heeft, zie voorgaand hoofdstuk).

Als de wetgever sturend wil optreden om eerdergenoemde privacyrisico's te beperken en voorkomen, dan zijn er verschillende reguleringsopties denkbaar. Afhankelijk van de gekozen invalshoek (risicomijdend, risico beperkend, kans bevorderend, of kans optimalisatie), de context en het beoogde doel, is een aantal –te combineren– sturingsmogelijkheden denkbaar:

- *Totaal verbod*: Daarmee wordt duidelijkheid gegeven en wordt slechts een marginaal aantal mogelijke toepassingen die momenteel juridisch legitiem zou zijn in de kiem gesmoord.
- *Voorafgaande goedkeuring*: Toepassingen mogen slechts worden ingezet wanneer vooraf toestemming is verkregen (bijvoorbeeld bij de AP).
- *Gediversifieerde aanpak*: Er kan expliciet aangegeven worden welke toepassingen wel en welke toepassingen niet zijn toegestaan (bijvoorbeeld door de AP of wetgever).
- *Regelgevend kader specifiek voor gezichtsherkenning*: De wetgever of de AP ontwikkelen een specifiek regelgevend kader voor gezichtsherkenningstechnologieën.
- *Controle achteraf*: huidig regelgevend kader blijft intact en er wordt ex post controle uitgevoerd op technologieën, toepassingen en het gebruik daarvan.
- *Gedragscodes en certificering*: ontwikkeling van een sectorspecifieke gedragscode en/of certificering, eventueel gebruikmakend van de reeds bestaande best practices.
- *Bewustwording*: De overheid kan inzetten op publiekscampagnes om burger en bedrijven duidelijk te maken welke gevaren en juridische grenzen er zijn aan het toepassen van gezichtsherkenningstechnologieën (dit kan in combinatie met andere reguleringsopties).
- *Gedoogbeleid*: de AP of regering geven in beleid aan dat het gebruik van gezichtsherkenning voor een bepaalde tijdsperiode zal worden gedoogd en naleving van wettelijke kaders niet zal worden afgedwongen.

Ten slotte

Gezichtsherkenningstechnologie in de horizontale relatie is wereldwijd in opmars en dat brengt, zo toont deze studie, een reeks privacyrisico's met zich mee. Zo moet men er rekening mee houden dat het voor burgers steeds moeilijker zal worden om zich anoniem te wanen in de publieke, semi-publieke en zelfs private ruimte als gezichtsherkenningstechnologie wijdverbreid wordt ingezet. De mogelijkheid om te allen tijde herkend te worden kan te weeg brengen dat mensen zich niet meer vrij voelen om onbevangen zichzelf te zijn. Wanneer gezichtsherkenning bovendien wordt aangewend om burgers in verband te brengen met allerlei informatiebronnen, wordt het voor burgers steeds moeilijker om in te schatten wat anderen eigenlijk over hen weten. Dit kan leiden tot machtsverschuivingen in horizontale relaties en burgers ertoe bewegen uit voorzorg hun gedrag aan te passen (*chilling effect*).

In Nederland wordt gezichtsherkenning op dit ogenblik nog niet op grote schaal toegepast in interacties tussen burgers en bedrijven en burgers onderling. In de gesprekken die wij hebben gevoerd ten behoeve van de domeinstudies, kwam geregeld naar voren dat bedrijven afwachtend zijn over wat juridisch nu eigenlijk is toegestaan. En hoewel burgers wel de mogelijkheid hebben om zelf met online-gezichtsherkenningsdiensten aan de slag te gaan, hebben wij niet kunnen vaststellen dat dit in de praktijk reeds vaak gebeurt.

Uit dit onderzoek blijkt dat gezichtsherkenningstechnologie in horizontale relaties nog geen voldongen feit is in Nederland; het is gezichtsherkenning "op het eerste gezicht". Maar de toepassingen die wereldwijd worden ontwikkeld en de privacyrisico's die daarmee gepaard gaan zijn zeker reëel. Dit maakt dat de samenleving nu de fundamentele vraag dient te stellen: "wat vinden wij wenselijk als het gaat om gezichtsherkenningstechnologie in onze democratische rechtsstaat?" Dit rapport poogt bij te dragen aan deze gedachtenvorming en bovendien handvatten te bieden aan de Nederlandse regering, de wetgevende macht en aan de relevante handhavende organisaties om op een transparante en systematische wijze te kiezen voor de meeste geschikte reguleringsoptie(s).

Bijlage I: Interviewleidraad Gezichtsherkenning

INTRO:

Voorstellen, doel interview, aanpak, toestemming, tijdsduur

Algemene vragen

1. Hoe lang ben je in dienst van het bedrijf?
2. Wat is de kernactiviteiten van het bedrijf?
3. Wat is je rol binnen het bedrijf?
4. Op welke manier speelt gezichtsherkenning een rol in deze werkzaamheden?

Gezichtsherkenning:

1. Kan je kort uitleggen wat voor gezichtsherkenningsproduct jullie bedrijf ontwikkelt/gebruikt?
2. Wie is jullie doelgroep?
3. Wat zijn de aspecten van het product die je benadrukt in een presentatie (verkoop/marketing)?
4. Kan je iets meer vertellen over de technologie die jullie inzetten?
5. Werken jullie samen met andere actoren (bedrijven/organisaties/ leveranciers/freelancers)?
6. Kan je kort uitleggen wat voor businessmodel achter het product zit?
7. Hoe denk je dat dit product er over 5 jaar uitziet?
8. Welke grote ontwikkelingen voorzie je in de komende 5 jaar op het gebied van gezichtsherkenning in het algemeen.

Privacy en gegevensbescherming wetgeving

1. Op welke manier speelt privacy een rol in je werkzaamheden? En in die van je bedrijf?
2. Met welke wet -en regelgeving dien je rekening te houden voor je product?
3. Helpt deze wet -en regelgeving bij de ontwikkeling en/of gebruik van je product?
4. Verhindert of bemoeilijkt deze wet -en regelgeving de dingen die je zou willen ondernemen?
5. Als je het voor het zeggen had, wat voor regelgeving zou je dan invoeren/aanpassen/afvoeren?

Uitdagingen privacy

1. In welke situatie(s) zou je je zelf ongemakkelijk voelen als je weet dat anderen je kunnen herkennen met gezichtsherkenningstechnologie?
2. Is privacy een kernwaarde voor jullie bedrijf? Zo ja, hoe uit zich dat? Zo niet, waarom niet?
3. Denk je dat gezichtsherkenning op zich privacyrisico's met zich meebrengt voor mensen in de maatschappij en zo ja, welke zouden dat zijn?
4. Verwacht je dat in de toekomst er nog meer privacyrisico's zullen ontstaan bij het gebruik van gezichtsherkenning?
5. Zijn er specifieke privacy-uitdagingen verbonden aan jullie product? Zo ja, wat zijn de belangrijkste? Zo niet, waarom zijn die er niet?
6. Hoe communiceren jullie over die privacyrisico's? Intern en extern?
7. Hebben jullie voldoende expertise in huis op het gebied van privacy of zoeken jullie die extern op? Intern: hoe belegd? Extern: bij wie? (consultant, toezichthouder, brancheverenigingen, internet,…)
8. Zou je meer ondersteuning willen op het gebied van privacy? Zo ja, uit welke hoek zou die idealiter moeten komen?
9. Zijn er bepaalde toepassingen van gezichtsherkenning of domeinen waarbinnen je vindt dat gezichtsherkenning verboden moet zijn/blijven/worden?

Best Practices privacy

1. Passen jullie privacy-by-design toe in de ontwikkeling van jullie product? Zo ja, hoe? Zo niet, waarom niet?
2. Zijn jullie daar als bedrijf uniek in/voorlopers?
3. Investeren jullie ook in voorlichting voor klanten/gebruikers?
4. Geven jullie privacyrichtlijnen mee voor het gebruik van jullie product? Zo ja, welke, zo niet, waarom niet?
5. Hoe wil je als bedrijf bekend staan op het gebied van gezichtsherkenning en privacy?
6. Kan je deze zin aanvullen? "Op het gebied van privacy zijn wij pas tevreden als…."
7. Wat vind jij in jouw domein het beste voorbeeld van een privacyvriendelijke gezichtsherkenningstoepassing?
8. Geeft een privacyvriendelijk product je als bedrijf een voordeel op de markt? Of een nadeel? Waarom?

Overige

1. Wat hebben we nog niet besproken wat zeker nog moet genoemd worden?
2. Waar zou je met het bedrijf over 5 jaar willen staan?

Bijlage II: Geïnterviewde personen en experts

Personen die geïnterviewd zijn voor de domeinstudies

Geïnterviewde	Affiliatie
Panos Moutafis	CEO, Zenus Biometrics
Rakshak Talwar	CTO, Zenus Biometrics
Pim Schoonderwoerd	Product manager IT Services, RAI Amsterdam
Logan Havern	Co-founder, Blip Biometrics
Michael Vos	Government Affairs Consultant, Microsoft
Martin Vliem	National Security Officer, Microsoft
Norberto Andrade	Privacy and Public Policy Manager, Facebook
Tauseef Ali	CTO 20Face
Anna Alicia Kier	DPO 20Face
Persoon X	Bedrijfsjurist bij een evenementenlocatie
Persoon Y	Bedrijfsjurist bij een retail bedrijf

N.B. wij hebben twee personen geïnterviewd die anoniem wilden blijven.

Deelnemers expertworkshop:

Expert	Affiliatie	Expertise
Marc van Lieshout	TNO/PI.lab	Wetenschap/technisch/privacy
Lotte Houwing	Bits of Freedom	Maatschappelijke org./privacy
Vincent Böhre	Privacy First	Maatschappelijke org./privacy
Inge Bremmer	NLDigital	Bedrijfsleven
Hans Bos	Microsoft NL	Bedrijfsleven
Jurriën Hamer	Rathenau Instituut	Beleid/regulering
Christiaan Roorda	Raad van State	Overheid
Koen van Nol	Schiphol	Bedrijfsleven
Stefan Kulk	Universiteit Utrecht	Wetenschap/rechten
Gerard Ritsema van Eck	Universiteit Groningen	Wetenschap/rechten

Victor Klos	Autoriteit Persoonsgegevens	Overheid
Olya Kudina	TU Delft	Wetenschap/filosofie

Bijlage III: Begeleidingscommissie

- de heer prof. dr. mr. G.J. Zwenne (voorzitter)
- de heer drs. S. Flight (lid)
- mevrouw dr. A.L. van Leeuwen (lid)
- mevrouw mr. S.L. Hartholt (lid)
- de heer dr. ir. L.J. Spreeuwers (lid)