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

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:** Bedrijfsmodellen 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).