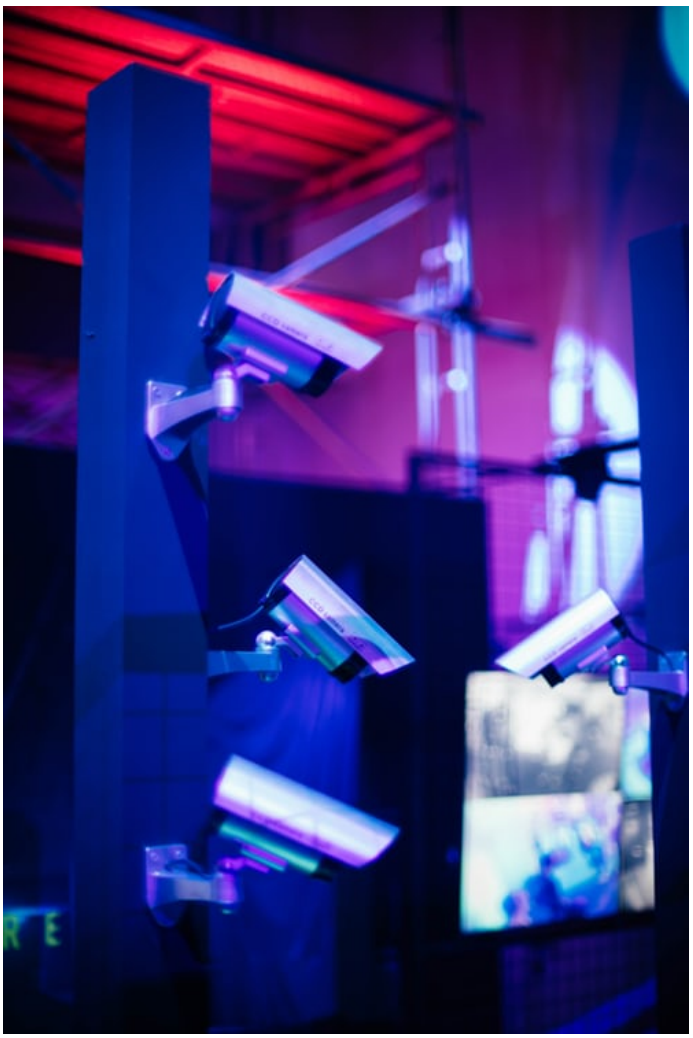
Datum: 30 oktober 2019



# Het ware gezicht van gezichts-herkennings-technologie

Paula Hooyman

## Inhoud

# 1. INLEIDING

Dit onderzoek richt zich op de problemen rondom het gebruik van gezichtsherkenningstechnologie door de politie in de publieke ruimte. Het doel van dit onderzoek is om meer bewustzijn te creëren over de mogelijk verstrekkende gevolgen van deze massasurveillance technologie.

In hoofdstuk twee wordt uitgelegd wat gezichtsherkenningstechnologie is en hoe het precies werkt. In het derde hoofdstuk worden de mogelijke toepassingen van gezichtsherkenningstechnologie opgesomd. In het vierde hoofdstuk worden de technologische tekortkomingen van de technologie uitgelegd. In het vijfde hoofdstuk wordt het gebruik van gezichtsherkenningstechnologie door de politie via het programma 'CATCH' besproken.[1] In het zesde hoofdstuk wordt gekeken welke grondrechten de politie zou schenden met het gebruiken van gezichtsherkenningstechnologie in de publieke ruimte.

De conclusie is dat de technologie gevaarlijk is: het maakt het mogelijk om groepen en individuen continu te bespioneren en te manipuleren, op een voorheen onmogelijke schaal en snelheid. De politie maakt op dit moment nog geen gebruik van de technologie in de publieke ruimte, maar het is niet onwaarschijnlijk dat ze dit in de toekomst wel gaan doen.[2] Er moet zo snel mogelijk worden ingegrepen, voordat het gebruik van deze technologie is genormaliseerd en mensen niet meer nadenken over de grootschalige gevolgen ervan.

# 2. WAT IS GEZICHTSHERKENNINGS-TECHNOLOGIE EN HOE WERKT HET?

## 2.1 Het ontstaan van gezichtsherkennings-technologie

De ontwikkeling van gezichtstechnologie is de laatste jaren enorm hard gegaan, maar de eerste stappen zijn lang geleden gezet. Al in 1964 bracht RAND Corporation de RAND Tablet uit, het eerste semiautomatische gezichtsherkenningssysteem. De RAND Corporation (wat staat voor Research ANd Development) was een Amerikaanse denktank, oorspronkelijk gespecialiseerd in nationale veiligheid. De Amerikaanse luchtmacht was de grootste opdrachtgever. In de eerste plaats werd gezichtsherkenningstechnologie dus ontwikkeld voor opsporingsdiensten – wie is onze vijand en hoe ziet die er uit? Tegenwoordig wordt het ook toegepast in commercieel gebruik: het vervangt onze pincodes, wachtwoorden en andere beveiligingsmethoden. Dat klinkt handig, want elk gezicht is uniek en het onderscheidt ons van anderen. Gezichtsherkenning kan zelfs eeneiige tweelingen van elkaar onderscheiden. Zo kan niemand anders bij je beveiligde spullen, of jouw telefoon ontgrendelen. Maar is deze techniek wel zo betrouwbaar? En nog belangrijker: moeten we de inzet van deze technologie wel willen?

De RAND Tablet werkte als volgt: op een foto konden handmatig de locaties van verschillende gezichtskenmerken geregistreerd worden. Deze gegevens konden in het geheugen worden opgeslagen. Wanneer het systeem een nieuwe foto van een gezicht te zien kreeg, kon het uit het geheugen het gezicht wat daar het meest op leek boven water krijgen. Een belangrijke eerste stap voor gezichtsherkenning, maar gehinderd door de toenmalige technologische stand van zaken: computerberekeningen gingen toen nog vrij traag en technologie had slechts beperkte mogelijkheden.

## 2.2 Hoe werkt gezichtsherkennings-technologie nu?

Tegenwoordig zijn er verschillende, zeer complexe technologieën in omloop, maar de basis van de meest gebruikte gezichtsherkenningstechnologie komt nog steeds overeen met het idee achter de RAND Tablet: de technologie detecteert het gezicht in een afbeelding of video, bepaalt de fysieke kenmerken daarvan, vergelijkt dit met de fysieke kenmerken van gezichten die staan opgeslagen in een databank, analyseert dit en maakt een beslissing.

Iets gedetailleerder houdt dit in dat door het gebruik van een ‘deep learning’ techniek een gezicht kan worden herkend. Deep learning is een subcategorie van ‘machine learning’. Machine learning maakt het mogelijk dat een systeem zichzelf dingen kan aanleren en zich kan aanpassen aan nieuwe situaties. Een zelflerend systeem dus. Machine learning technieken maken gebruik van neurale netwerken. Neurale netwerken worden zo genoemd omdat deze systemen op een vergelijkbare manier werken als het menselijk zenuwstelsel. Zoals een kind leert om patronen te herkennen, doet een neuraal netwerk dat ook. Hierdoor kan het systeem zichzelf trainen. Deep learning maakt gebruik van neurale netwerken met meer ‘lagen’ dan gewone machine learning. Het systeem voert voor een beslissing meerdere analyses uit, als het ware over elkaar heen. In elke volgende analyse wordt de informatie uit eerdere analyses toegepast. Door zo steeds ‘dieper’ in de materie te gaan, kunnen deep learning technieken complexere, verborgen verbanden en kenmerken ontdekken dan gewone machine learning technieken.

Deep learning werkt bijvoorbeeld als volgt: met de eerste analyse worden in de afbeelding de contouren van het gezicht bepaald. Met de tweede analyse worden binnen die contouren de kenmerken van het gezicht gelokaliseerd, zoals de ogen, wenkbrauwen, neus en mond. Met de derde analyse worden de afstanden tussen deze kenmerken berekend, en worden deze afstanden gebruikt om een unieke dataset voor dat gezicht te bouwen. Zo wordt een afbeelding of video geconverteerd naar ‘platte tekst’. De technologie heeft een databank, een geheugen vol met datasets van gezichten. Met de laatste analyse wordt de nieuwe dataset vergeleken met de andere datasets in het geheugen. Als je bijvoorbeeld de gezichtsherkenning op je telefoon hebt ingeschakeld, dan staat in de databank van jouw telefoon de dataset van jouw gezicht. De laatste stap is de beslissing: komen de datasets overeen, is dit hetzelfde gezicht? Zo ja, dan ontgrendelt je telefoon.

# 3. WAT ZIJN DE MOGELIJKE TOEPASSINGEN VAN GEZICHTSHERKENNINGS-TECHNOLOGIE?

Volgens makers van de technologie kan er veel met gezichtsherkenningstechnologie. Deze toepassingen kunnen onderverdeeld worden in de volgende categorieën: identificatie en verificatie, categorisatie en emotieherkenning. Belangrijk: in dit (niet complete) overzicht is nog geen rekening gehouden met wat er wel en niet wettelijk is toegestaan in Nederland. De technologie loopt vooruit op de juridische vraagstukken.

## 3.1 Identificatie en verificatie

Bij identificatie (wie is deze persoon?) en verificatie (is deze persoon wie zij zegt dat zij is?) wordt er naar kenmerken gekeken die uniek zijn voor een persoon, zoals de afstand tussen de ogen, het puntje van de neus en de aanhechting van de oren. Dit is de categorie die ook wordt gebruikt door opsporingsdiensten om verdachten op te sporen. Hierover meer in hoofdstuk 5.

Verdere toepassingen in die categorie zijn automatische paspoortcontrole op het vliegveld en andere toegangsfuncties, zoals gecontroleerde toegang tot een voetbalstadion.[3] Passagiers in het openbaar vervoer met een ov-verbod kunnen sneller herkend worden.[4] Je gezicht kan als wachtwoord gebruikt worden, zoals het geval is bij telefoonontgrendeling via je gezicht of bij kluizen met gezichtsherkenning. Om te betalen heb je straks geen pinpas meer nodig, alleen nog maar je gezicht.[5] Ook zijn er apps ontwikkeld waarmee je een gezicht kon opzoeken op social media en op datingsites, en in Amerika kon je zelfs controleren of degene tegenover je in de trein in de National Sex Offender Registry stond.[6]

## 3.2 Categorisatie

Bij categorisatie worden beelden van personen niet direct aan een identiteit gekoppeld. Er wordt gekeken naar kenmerken die gebruikt kunnen worden om personen in te delen in een bepaalde groep. Dit zijn kenmerken die juist niet uniek zijn voor een persoon, zoals leeftijd, huidskleur en geslacht. Zo kan er geprobeerd worden een demografisch overzicht te maken van een groep. Wat is de gemiddelde leeftijd van het publiek bij een concert, of de verhouding man/vrouw? Ook kunnen gepersonaliseerde reclames op 'slimme' reclamezuilen worden laten zien, gebaseerd op leeftijd en/of het geslacht van degene die langs loopt.[7]

Zorgwekkende ontwikkelingen zijn de toepassingen gebaseerd op fysionomie en frenologie: de leer dat aan het uiterlijk van een mens zijn karaktereigenschappen en voorkeuren af te lezen zijn. Uiteraard is inmiddels bekend dat dit een pseudowetenschap is – niet wetenschappelijk te onderbouwen. Maar niet iedereen wil dit geloven. Zo stelt een problematisch onderzoek dat er een algoritme is ontwikkeld wat uit kenmerken in het gezicht seksuele geaardheid zou kunnen afleiden.[8] Naast het feit dat het onderzoek gebaseerd is op een pseudowetenschap is het belangrijk om je af te vragen: waarom wordt dit ontwikkeld? Voor wie zou deze algoritmische 'gaydar' in het voordeel werken? Niet voor degenen waarvan tegen hun wil in hun seksuele geaardheid bekend wordt gemaakt, en zeker niet als zij leven in een land waar homoseksualiteit met de dood bestraft wordt.

Het bedrijf Faception past deze pseudowetenschap ook toe: het leest zogenaamd karaktereigenschappen af van een gezicht, en verdeelt mensen op basis daarvan onder in acht rubrieken, waaronder 'witteboordencrimineel', 'terrorist' en 'pedofiel'.[9] Deze praktijken doen denken aan de duistere geschiedenis van 'rassenwetenschap', dat werd toegepast door witte racisten in het 19e-eeuwse Amerika om slavernij te rechtvaardigen. Toen werd beweerd dat bepaalde gebieden van de schedel groter waren bij mensen van kleur, die daardoor onderdanig zouden zijn en dus een 'eigenaar' nodig hadden.[10]

Leveranciers stellen dat iemands etniciteit herkend kan worden via gezichtsherkenningstechnologie. Dit kan leiden tot grove mensenrechtenschendingen: zo is bijvoorbeeld na een beveiligingslek ontdekt dat de Chinese overheid gezichtsherkenningstechnologie gebruikt om Oeigoeren continu te monitoren. Oeigoeren zijn een Chinese moslimpopulatie in de provincie Xinjiang, een etnische minderheid. Deze groep wordt stelselmatig onderdrukt en gediscrimineerd door de Chinese overheid, omdat zij deze groep zien als terroristen, mede omdat ze onafhankelijkheid willen. Het is nog maar de vraag of de technologie altijd het verschil kan zien tussen Oeigoeren en Han-Chinezen. Meer dan een miljoen personen, door de technologie aangewezen als Oeigoeren, zitten vast in zogenoemde 'anti-extremismecentra', wat in de praktijk straf- of concentratiekampen zijn.[11] Gezichtsherkenningstechnologie draagt bij aan deze etnische zuivering.

## 3.3 Emotieherkenning

Gezichtsherkenningscamera's kunnen volgens de leveranciers ook emoties registreren. Emoties die tot

nu toe herkend kunnen worden zijn verdriet, blijheid, verrassing, angst, boosheid, kalmte, verbazing en walging.[12] Wanneer emotieherkenning zonder fouten verloopt (wat nog lang niet altijd het geval is), zou dit kunnen worden toegepast in psychologisch onderzoek of in de zorgsector, bijvoorbeeld bij zorg op afstand. Het kan ook worden toegepast in marktonderzoek, om te kijken hoe mensen reageren op bepaalde producten of diensten of reclame daarvoor. Dit betekent ook dat er gekeken kan worden hoe mensen reageren op bepaalde politieke uitingen, om zo de politieke verhoudingen te peilen. Deze informatie kan weer gebruikt worden voor gepersonaliseerde politieke reclame, waar gerichte advertenties kunnen worden toegespitst op specifieke individuen (wie is gevoelig voor dit onderwerp?). Dit brengt mogelijkheden voor organisaties die kiezers willen manipuleren met informatie die niet per se waar hoeft te zijn. Een partij kan bijvoorbeeld racistische kiezers informatie tonen over hoge misdaadcijfers onder immigranten. De verkiezingscampagnes vinden dan steeds vaker plaats op de schermen van individuele kiezers, in plaats van in de openbaarheid. Onwaarheden zijn dan moeilijk te controleren, en het is niet duidelijk wat de prioriteiten van een politieke partij zijn.

## 3.4 Wat zegt deze hoeveelheid aan toepassingen?

Er is een enorme hoeveelheid aan mogelijke toepassingen van gezichtsherkenningstechnologie, van onschuldig tot zeer problematisch. Dit geeft de impact van deze technologische ontwikkeling aan – en dus ook de reikwijdte van het probleem. De technologie zal zich in de toekomst alleen maar verder ontwikkelen: er zullen meer algoritmes ontwikkeld worden die dit kunnen, de kwaliteit zal steeds beter worden en de kosten van de technologie zullen omlaag gaan. Als de techniek steeds meer zal worden toegepast zal dit leiden tot een onwenselijke normalisering van dit massasurveillance middel.

Dit overzicht met mogelijke toepassingen kan nog vrij abstract klinken. Om duidelijk te maken hoe ingrijpend deze technologie is, hebben we zelf de proef op de som genomen. De uitkomst daarvan lees je in dit artikel. Voor dit korte onderzoek hebben we gebruik gemaakt van de gezichtsherkenningstechnologie van Amazon, ‘Rekognition’. Op de Dam in Amsterdam hangt een ‘slimme’ camera, die 24 uur per dag, zeven dagen per week de Dam filmt in 4K-kwaliteit, en deze beelden bijna gelijktijdig streamt naar YouTube. Dit onder het mom van ‘digitaal toerisme’. We zorgden ervoor dat we met ons gezicht in beeld waren en hebben onderzocht of de technologie ons herkent, wat de technologie kan zien en hoeveel informatie de technologie nodig had om iemand te kennen (spoiler alert: heel weinig).

# 4. WAT ZIJN DE TECHNOLOGISCHE TEKORTKOMINGEN VAN GEZICHTSHERKENNINGS-TECHNOLOGIE?

Er is veel mis met gezichtsherkenningstechnologie. De problemen kunnen opgedeeld worden in technologische tekortkomingen en grondrechtelijke en maatschappelijke problemen. De technologische tekortkomingen zijn waarschijnlijk grotendeels tijdelijk, want de technologie kan zich steeds verder doorontwikkelen en optimaliseren. De maatschappelijke problemen zullen daarentegen altijd blijven bestaan. In dit hoofdstuk worden de technologische tekortkomingen besproken. De grondrechtelijke en maatschappelijke problemen komen aan bod in hoofdstuk 6.

## 4.1 Kwaliteit van de beelden

Databanken met gezichten bestaan meestal uit beelden die in een ideale, gecontroleerde omgeving zijn gemaakt. Het beeld is dan scherp, van voren of meerdere kanten genomen en goed belicht. In veel toepassingen zijn ook de beelden van gezichten die 'herkend' moeten worden van een goede kwaliteit. Maar beelden die voor surveillance worden gebruikt, zoals beelden van bewakingscamera's, zijn ongecontroleerd, bevatten veel beweging, zijn vaak van matige kwaliteit en vanuit moeilijke hoeken genomen. Deze beelden kunnen enigszins verbeterd worden door de belichting te corrigeren en beelden aan te vullen of te draaien. Deze beelden zijn dan nog steeds niet van eenzelfde kwaliteit als beelden uit een gecontroleerde omgeving. Gezichtsherkenningstechnologie werkt dus het slechtst voor surveillance-doeleinden. Dit is één van de redenen waarom het gebruik van gezichtsherkenningstechnologie door opsporingsdiensten problematisch is.

## 4.2 Discriminatie en racisme

De algoritmen leren op basis van data uit een structureel ongelijke maatschappij, en nemen die ongelijkheid mee. Doordat de algoritmes door mensen gemaakt worden, zitten de vooroordelen en waarden van de programmeurs of hun opdrachtgevers in het algoritme. Vaak zit dit ook in de oefendata waarmee een zelflerend algoritme traint: witte mannen zijn daarin oververtegenwoordigd. Hierdoor functioneren de technologieën discriminerend en racistisch. Vrouwen, mensen van kleur, kinderen en andere minderheden zijn hier de dupe van. Een onderzoek van MIT en Stanford University naar verschillende commerciële gezichtsherkenningstechnologieën toont aan dat het foutpercentage bij vrouwen van kleur varieert van 20,8% tot 46,8%, terwijl deze bij witte mannen niet groter is dan 0,8%.[13] Een enorm verschil. Ook worden negatieve emoties (zoals boosheid) vaker toegekend aan mensen van kleur.[14] Uber-accounts van transgender bestuurders zijn geblokkeerd omdat de technologie, gebruikt als beveiligingsmechanisme, de gezichten van deze bestuurders in transitie niet herkende.[15] Daarnaast werkt de technologie in zijn algemeenheid nog niet goed. De technologie die de Metropolitan Police Service (een politie-eenheid in Engeland) gebruikt heeft in een proef tot juli 2019, heeft een foutpercentage van maar liefst 81%, blijkt uit een onderzoek van de University of Essex.[16] Deze technologische gebreken kunnen ervoor zorgen dat de verdachte verkeerd wordt geïdentificeerd en dat er een opsporingsonderzoek gestart wordt naar onschuldige mensen.

## 4.3 Gebrek aan transparantie

Daarnaast heeft gezichtsherkenningstechnologie ook een transparantieprobleem. Omdat de zelflerende algoritmes steeds 'dieper' in de materie gaan, en in elke volgende analyse de informatie uit eerdere analyses toegepast wordt, is de uitkomst een zeer ingewikkelde formule. Dit maakt het moeilijk voor mensen om te achterhalen wat er precies gebeurt in het proces, waardoor het lastig is om de uitkomst van een algoritme te voorspellen. Wanneer er iets niet goed is gegaan in het proces, bijvoorbeeld als er een verkeerde beslissing is gemaakt, valt het moeilijk te controleren in welke laag dit zich heeft voorgedaan en is het bijna onmogelijk om dit achteraf uit te leggen.

# 5. HET GEBRUIK VAN GEZICHTSHERKENNINGS-TECHNOLOGIE DOOR DE POLITIE

## 5.1 Hoe gebruikt de politie gezichtsherkennings-technologie en wat is het juridisch kader?

De politie maakt sinds 2016 gebruik van gezichtsherkenningstechnologie in het programma 'CATCH'. Het wordt ook wel gelaatsvergelijking genoemd, omdat CATCH geen oordeel geeft wie iemand 'is', alleen maar 'op wie iemand lijkt'. Om uit te zoeken hoe CATCH precies werkt, hebben we gesproken met John Riemen, hoofd van het Centrum voor Biometrie van de Nationale Politie. Dit centrum gaat over het gebruik van biometrische gegevens binnen de politie.

De politie gebruikt CATCH om de identiteit van een verdachte of veroordeelde te veriferiëren aan de hand van de strafrechtsketendatabank.[17] Dit is een databank met alle gezichten van verdachten en veroordeelden. Ook de vingerafdrukken van verdachten worden gebruikt om personen te identificeren. Vingerafdrukken zijn volgens Riemen veel betrouwbaarder dan gezichtsherkenning, zeker als je een goede afdruk hebt van alle tien de vingers: dan is de betrouwbaarheid nagenoeg 100%. Vingerafdrukken zijn dan ook leidend in het identificatieproces. De indringende technologie van gezichtsherkenning is dus niet noodzakelijk om iemand te identificeren wanneer iemand is opgepakt, maar fungeert 'slechts' als plan B. Een onnodige en indringende maatregel dus.

Als juridische grondslag voor het gebruik van gezichtsherkenningstechnologie wordt artikel 55c van het Wetboek van Strafvordering (Sv) gebruikt. Deze bepaling regelt welke foto's in de strafrechtsketendatabank komen. Deze bepaling regelt ook dat die foto's kunnen worden gebruikt voor het voorkomen, opsporen, vervolgen en berechten van strafbare feiten. De foto's in de databank zijn foto's van verdachten of veroordeelden van een relatief ernstig misdrijf: strafbare feiten waar een gevangenisstraf van vier jaar of meer op staat (ook wel voorlopige hechtenis-feiten genoemd), én foto's van verdachten van wie de identiteit onduidelijk is. Deze groep mensen wordt NN'ers genoemd (een afkorting van 'nomen nescio', een Latijnse uitdrukking voor 'ik weet de naam niet'). In de praktijk zijn dit vaak activisten die niet mee willen werken aan hun eigen identificatieproces. Bij NN'ers is er geen eis gesteld aan het soort strafbare feit. Zo kunnen er bijvoorbeeld foto's worden gemaakt van demonstranten die, na drie keer vorderen door de politie, niet zijn weggegaan bij de demonstratie en dus worden opgepakt. Een veel lichter vergrijp dan een voorlopige hechtenis-feit. Voor het maken van foto's van NN'ers is er een bevel van de officier van justitie of de hulpofficier nodig.

Elke keer dat iemand wordt aangehouden, wordt er een foto gemaakt. Er staan momenteel ongeveer 2,2 miljoen foto's, van 1,3 miljoen unieke personen in de strafrechtsketendatabank. De gezichten van verdachten, veroordeelden en NN'ers staan allemaal in dezelfde databank. Niet-geïdentificeerde NN'ers staan met een nummer van aanhouding in de databank. Wanneer een NN'er is geïdentificeerd, blijft deze persoon in de strafrechtsketendatabank staan, ongeacht het begane strafbare feit. Volgens de politie is dit een afweging van de wetgever geweest om identiteitsfraude te voorkomen. Deze lezing van de wet is op zijn minst opmerkelijk, want als iemands identiteit bekend is en diegene wordt niet verdacht van een voorlopige hechtenis-feit, waarom staat diegene dan nog in de strafrechtsketendatabank?

De gezichtsherkenningstechnologie die in CATCH wordt gebruikt, wordt aangeleverd door IDEMIA, een Frans bedrijf gespecialiseerd in beveiligings- en identiteitsoplossingen. IDEMIA kan niet bij het programma CATCH, het levert slechts de techniek. Alleen het Centrum voor Biometrie kan gebruik maken van CATCH. Het proces van CATCH gaat als volgt. Een politieagent stuurt een aanvraag met een opsporingsfoto naar het Centrum voor Biometrie. Dit kan een foto zijn die gemaakt is om een persoon die is opgepakt te identificeren, maar ook een opsporingsfoto, zoals beelden afkomstig van (beveiligings)camera's die in de publieke ruimte hangen. CATCH werkt dus niet *real time.* Politieagenten mogen een aanvraag alleen doen voor 'een goede vervulling van hun taak'.[18] De aanvraag wordt geregistreerd. Zo kan het centrum zien wie de aanvraag gedaan heeft en op welke datum.[19] Het centrum kan niet zien van welk strafbaar feit de persoon wordt verdacht of om welke zaak het gaat. Een opsporingsfoto is een foto waar een strafbare handeling in beeld is of een persoon die een rol speelt in een politiezaak. Het centrum beoordeeld of de foto van goede kwaliteit is, en dus bruikbaar voor de technologie. De kwaliteit van een opsporingsfoto kan 'verbeterd' worden, maar het centrum mag de beelden niet manipuleren. Als er wordt gecontroleerd of een verdachte of veroordeelde al in de strafrechtsketendatabank staat, wordt het gezicht uit het opsporingsbeeld vergeleken met alle gezichten die

daar in staan. Er kan dan worden opgegeven wat de minimale mate van gelijkenis moet zijn en hoeveel resultaten er getoond moeten worden. Vervolgens wordt er door een team beoordeeld welk gezicht uit de resultaten het meeste overeenkomt. Vervolgens gaat die foto samen met de originele opsporingsfoto naar twee experts. Deze beoordelen onafhankelijk van elkaar in hoeverre die met elkaar overeenkomen. Als zij beiden van oordeel zijn dat die gezichten waarschijnlijk van dezelfde persoon zijn, wordt de identiteit van die persoon uit de strafrechtsketendatabank en de mate van overeenkomst daarmee gerapporteerd aan de politieagent die de aanvraag heeft gedaan. Als de politieagent zelf al denkt te weten wie de persoon in het opsporingsbeeld is, kan de politieagent ook vragen aan het centrum om het opsporingsbeeld met één gezicht uit de strafrechtsketendatabank te vergelijken. De uitkomst van het onderzoek is een opsporingsindicatie. Op basis daarvan wordt een onderzoek naar een persoon gestart.

Het centrum beoordeelt de rechtmatigheid van de verkrijging van het opsporingsbeeld niet. Zij handelen op basis van het vertrouwensbeginsel: zij gaan ervan uit dat de politieagent de wet heeft nageleefd bij het verkrijgen van de beelden en de aanvraag is gedaan 'voor een goede vervulling van hun taak'.[20] De Gegevensautoriteit van de politie houdt steekproeven om te controleren of de aanvragen rechtmatig worden gedaan. Het centrum is gescheiden van de politieteams die de onderzoeken uitvoeren. De politieagenten kunnen niet zelf aan de slag met CATCH. Ook binnen het centrum zijn de processen gescheiden: er is een team dat de gezichtsherkenningstechnologie toepast, en een team dat die resultaten analyseert. Er is geen apart toezicht op de beslissingen die het centrum maakt in het kader van CATCH. Het onderzoeksrapport van het Centrum voor Biometrie wordt toegevoegd aan het proces-verbaal van de verdachte. Er zijn geen cijfers beschikbaar hoe vaak CATCH een verkeerde identiteit als 'meest waarschijnlijk' heeft aangedragen.

## 5.2 Toekomstige ontwikkelingen en 'function creep': gebruik in de publieke ruimte

Gezichtsherkenning wordt op dit moment dus alleen gebruikt om verdachten te identificeren, maar nog niet om *real time* (mogelijke) verdachten te lokaliseren in de publieke ruimte. Waarom richt dit onderzoek zich dan toch op het gebruik van gezichtsherkenningstechnologie *in de publieke ruimte*?

Omdat de kans bestaat dat de politie dit (op korte termijn) wil gaan doen. Dat zit zo: vaak wordt technologie op een gegeven moment ingezet voor andere doeleinden dan oorspronkelijk bedoeld was. Dit heet 'function creep'. Het onstaan van function creep bij informatie en technologie is eerder een gewoonte dan een uitzondering.[21] Bij technologie die ingezet wordt voor surveillance is het bijna onvermijdelijk: opsporingsdiensten hebben er belang bij om steeds efficiënter te werk te gaan om strafbare feiten te voorkomen. Het probleem van function creep is dat het er vaak voor zorgt dat in de toekomst precies datgene gebeurt wat op dit moment wettelijk wordt uitgesloten.[22] Terwijl de wetgever zoiets niet zonder reden heeft uitgesloten bij het opmaken van die wettelijke bepaling. Of er wel of niet een nieuwe wettelijke bepaling wordt opgesteld voor de nieuwe toepassing is daarbij irrelevant: nog steeds wordt er afgestapt van de eerdere 'begrenzing' en (in het kader van de opsporing) de mate van bescherming van de burger tegen inmenging door de overheid. En wanneer er geen nieuwe wettelijke bepaling wordt opgesteld, ontbreken de democratische controle, transparantie en andere waarborgen om misbruik en eventueel onevenredige inbreuken op (grond)rechten te voorkomen.

Riemen sluit niet uit dat de politie ooit met gezichtsherkenning in de publieke ruimte gaat werken. 'Als een terrorist na een aanslag ontkomt, wil je hem zo snel mogelijk vinden.'[23] Er worden ook al proeven gedaan met *real time* gezichtsherkenning. In het voetbalstadion van Heracles Almelo konden vip-klanten toegang krijgen via gezichtsherkenning.[24] En in een andere proef, genaamd Tec4se, is gezichtsherkenning ingevoerd in bodycams.[25] Het is dus technisch al mogelijk om *real time* gezichtsherkenning in de publieke ruimte toe te passen.

Het wetsartikel waarop het huidige gebruik wordt gebaseerd, artikel 55c Sv, is niet gemaakt om deze technologie te reguleren. De regels komen uit een tijd waarin gezichtsherkenningstechnologie nog niet gebruikt werd. Het gevolg hiervan is dat er rondom gezichtsherkenning geen gerichte wettelijke grondslagen zijn opgesteld, en dat over toepassingen hiervan in de strafvordering ook nog weinig maatschappelijk of politiek debat is gevoerd.[26] Dit probleem zal blijven bestaan wanneer verdere toepassingen van deze technologie op dit wetsartikel worden gebaseerd.

Function creep bij gezichtsherkenningstechnologie kan als volgt werken: op dit moment wordt de technologie alleen gebruikt voor identificatie. Door de

wens van opsporingsdiensten om steeds efficiënter te werken, kan de technologie in de toekomst ook *real time* gebruikt worden in de publieke ruimte, zoals in proeven al gebeurd is. En zo kunnen er steeds nieuwe vormen van gebruik worden bedacht voor de technologie. Identificatie kan verder uitgebreid worden naar het lokaliseren van terroristen in een menigte, wat verder uitgebreid kan worden naar het lokaliseren van 'potentiële terroristen', wat uitgebreid kan worden naar het lokaliseren van personen die zich regelmatig op een bepaalde locatie begeven, wat verder kan worden uitgebreid naar het volgen van bepaalde groepen of individuen. Deze kunnen worden gevolgd op verschillende gronden, zoals uiterlijke kenmerken, bepaalde gedragingen, geloofs- of politieke overtuiginen. Deze vorm van observatie kan in het geheim plaatsvinden, of in het openbaar. Deze ontwikkelingen klinken heftig, maar de technologie maakt het mogelijk om groepen en individuen indringend te observeren en te volgen. Dit is een zeer ongewenste en ongezonde situatie en moet voorkomen worden.

Er is dus een grote kans op het ontstaan van function creep, en de mogelijke gevolgen van die function creep zijn ernstig. Daarom bekijken we het breed en gaat dit onderzoek over het gebruik door de politie van gezichtsherkenningstechnologie *in de publieke ruimte*. Het volgende hoofdstuk bespreekt de juridische problematiek van die mogelijke toepassing.

# 6. WELKE GRONDRECHTEN ZIJN IN HET GEDING BIJ GEZICHTSHERKENNING IN DE PUBLIEKE RUIMTE?

Er zijn meerdere grondrechten in het geding bij het toepassen van gezichtsherkenningstechnologie in de publieke ruimte. Hieronder is uitgewerkt welke grondrechten van toepassing zijn en hoe deze beperkt worden. Vervolgens wordt gekeken of die beperking toegestaan is of niet, en wat het gevolg van die beperking is. Er wordt bij de beoordeling uitgegaan van artikel 55c van het Wetboek van Strafvordering (Sv) als de juridische grondslag, aangezien er geen andere wetsartikelen zijn waar het gebruik van gezichtsherkenning door de politie op gebaseerd kan worden. Het doel van gezichtsherkenning in de publieke ruimte kan zijn het opsporen of volgen van verdachten. Dit valt onder de zinsnede 'het voorkomen [en] opsporen […] van strafbare feiten'. De inbreuken worden uitgelegd aan de hand van het Europees Verdrag voor de Rechten van de Mens (EVRM).

Dit onderzoek richt zich op het gebruik van deze technologie door de politie. De focus van de grondrechtelijke en maatschappelijke problematiek ligt dus op 'verticale' verhoudingen; schendingen door de overheid (en niet op 'horizontale' verhoudingen, tussen burgers onderling).

## 6.1 Welke grondrechten zijn van toepassing bij het gebruik van gezichtsherkennings-technologie in de publieke ruimte?

De grondrechten die in het gedrang komen zijn het recht op privacy, het recht op bescherming van persoonsgegevens, het recht op vrijheid van meningsuiting, het recht op vrijheid van vergadering en vereniging, de godsdienstvrijheid en het discriminatieverbod. Hieronder volgt een uitleg waarom.

Het recht op privacy is ook wel bekend als het recht op eerbiediging van privéleven of de eerbiediging van de persoonlijke levenssfeer.[27] Privacy betekent dat je het recht hebt om 'jezelf' te zijn, en te doen en laten wat je wil, zonder dat anderen zich daarmee bemoeien. Het doel van dit artikel is in de eerste plaats om ervoor te zorgen dat je privéleven tegen willekeurige inmenging door de overheid beschermd wordt.[28] Dit privéleven heb je thuis, maar bestaat ook in de publieke ruimte.[29] Gezichtsherkenning in de publieke ruimte maakt het mogelijk voor de overheid om te monitoren wie je bent, waar je bent, wat je doet en met wie je bent. De overheid kan zo een gedetailleerd beeld vormen van zeer persoonlijke onderdelen van het leven van mensen. Deze maatregel is een beperking op je privacy, wat alleen mag als aan de wettelijke vereisten voor zo'n beperking is voldaan.[30] Het is een aantasting van het recht op anonimiteit. Dit is geen bestaand grondrecht in het EVRM, maar wel ontzettend belangrijk.[31]

Verwant aan het recht op privacy is het recht op bescherming van persoonsgegevens.[32] Persoonsgegevens die verwerkt worden door politie of justitie worden beschermd door de Wet politiegegevens (Wpg).[33] Gegevens over je gezicht zijn biometrische gegevens, en dus 'bijzondere' persoonsgegevens. Er moet bij de verwerking daarvan voldaan zijn aan de vereisten uit de Wpg.[34]

Ook de vrijheid van meningsuiting komt in het gedrang door gezichtsherkenning.[35] Dit recht houdt in dat iedereen de vrijheid heeft om meningen, gevoelens en gedachten te hebben, te verspreiden en te ontvangen. Dit kan in woord, in schrift, via samenkomsten of via protestacties. Het recht op vrijheid van meningsuiting is dus sterk verwant aan de demonstratievrijheid en de vrijheid van vergadering en vereniging.[36] Deze rechten maken het namelijk mogelijk dat iedereen op een vreedzame manier moet kunnen vergaderen, protesteren, bijeen komen en gelijkgestemden op moet kunnen zoeken, zonder bemoeienis van de overheid. Massasurveillance met behulp van gezichtsherkenning in de publieke ruimte is een vorm van overheidsbemoeienis, en hierdoor kunnen mensen zich minder vrij voelen om hun eigen gang te gaan, bijvoorbeeld op evenementen of bij bijeenkomsten die plaatsvinden. Wanneer mensen het gevoel hebben dat zij in de gaten worden gehouden, kan het zijn dat zij hun mening aanpassen, bepaalde meningen misschien niet meer durven te uiten of misschien wegblijven van bepaalde bijeenkomsten of demonstraties. Dit wordt een 'chilling effect' genoemd. Hierdoor worden zij belemmerd om op die plekken hun meningen en ideeën te delen en te communiceren met anderen. Mensen moeten zich zonder terughoudendheid kunnen aansluiten bij een demonstratie. Dat grondrecht hebben we niet voor de gezelligheid: het gaat er juist om dat ook controversiële meningen gedeeld en verspreid kunnen worden, zodat het publieke debat zich verder kan ontwikkelen.[37]

Nauw samenhangend met de vrijheid van meningsuiting, demonstratievrijheid en het recht op vergadering en vereniging, is de godsdienstvrijheid.[38] Door het toepassen van gezichtsherkenning in de publieke ruimte kan de geloofsovertuiging van mensen

worden geregistreerd. Je geloof moet je onbezorgd kunnen belijden. Net als dat het kan dat mensen zich niet meer vrij voelen om hun mening te uiten als ze in de gaten worden gehouden, kan massasurveillance door gezichtsherkenningstechnologie er ook toe leiden dat mensen zich niet vrij voelen om hun eigen godsdienst te bepalen, tot uitdrukking te brengen in bijeenkomsten of bepaalde gebedshuizen binnen te treden. Zeker als het gaat om religieuze minderheden. Het recht om je godsdienst te belijden of tot uitdrukking te brengen mag beperkt worden via maatregelen, maar niet ongelimiteerd.[39]

Ook van belang is het discriminatieverbod.[40] Dit verbod garandeert dat mensen hun rechten en vrijheden moeten kunnen uitoefenen, zonder discriminatie op welke grond dan ook. Dit recht moet dus samen met andere grondrechten bezien worden. Het doel van dit recht is niet dat iedereen altijd gelijk behandeld wordt. Soms moet er juist tussen verschillende personen of groepen onderscheid gemaakt worden om geen afbreuk te doen aan de individuele verschillen of wensen. Zoals in hoofdstuk 4 besproken is, functioneren de huidige gezichtsherkenningstechnologieën racistisch en discriminerend. Minderheidsgroepen zijn hier de dupe van.

## 6.2 Is er sprake van toegestane beperkingen op deze grondrechten?

Grondrechten beschermen de burger tegen te vergaande bemoeienis door de overheid. Wanneer de overheid maatregelen neemt, moet zij de grondrechten respecteren. Hiervoor moeten de maatregelen voldoen aan bepaalde vereisten. Maatregelen die het recht op privacy, de vrijheid van meningsuiting, godsdienstvrijheid en de vrijheid van vergadering en vereniging beperken, moeten allemaal voldoen aan de volgende vereisten: een maatregel moet 1) 'voorzien zijn bij wet', 2) 'noodzakelijk zijn in een democratische samenleving' en 3) een 'legitiem doel' dienen.[41]

Het eerste vereiste, 'voorzien bij wet', betekent dat in de wet moet staan dat de maatregel toegepast mag worden. Dit vereiste is hetzelfde voor elk van die vier grondrechten.[42] Dit zal in paragraaf 6.2.1 één keer worden uitgewerkt, geldend voor elk van de vier grondrechten. Het tweede vereiste, 'noodzakelijk in een democratische samenleving', is afhankelijk van het specifieke grondrecht. Dit wordt per recht apart beoordeeld in paragraaf 6.2.2. Het derde vereiste, het dienen van een 'legitiem doel', betekent dat er een goede reden moet zijn voor het inzetten van de maatregel. Deze doelen zijn op te maken uit de wetsartikelen. Dit zijn onder andere het beschermen van de nationale veiligheid, het beschermen van de openbare veiligheid en het voorkomen van wanordelijkheden en strafbare feiten.[43] Gezichtsherkenning in de publieke ruimte kan gebruikt worden om verdachten te lokaliseren en te volgen. Dit valt onder één of meerdere van deze doelen. Het derde vereiste zal daarom waarschijnlijk geen probleem vormen en wordt hier verder niet behandeld.

Tot slot wordt uitgewerkt of de persoonsgegevens voldoende beschermd zullen worden en of de inbreuk op het verbod op discriminatie toegestaan zal zijn.

### 6.2.1 Zijn de beperkingen voorzien bij wet?

'Voorzien bij wet' betekent dat de maatregel (hier dus het toepassen van gezichtsherkenningstechnologie in de publieke ruimte) een basis moet hebben in de nationale wet (dit kunnen geschreven en ongeschreven rechtsregels zijn[44]). Die wet moet voldoende toegankelijk zijn (bijvoorbeeld doordat het een openbaar document is, te vinden op het internet[45]). Verder moet de wet bescherming bieden tegen misbruik.[46] Dit betekent dat de omstandigheden waarin en de voorwaarden voor het inzetten van de maatregel uitgelegd moeten worden.[47] Dit kan door het volgende te specificeren: op welke categorie personen de maatregel van toepassing is, bij welke strafbare feiten de maatregel mag worden toegepast (dit hoeft niet uitputtend uiteengezet te worden, maar wel voldoende gedetailleerd[48]), wat de duur van de maatregel is, de procedure van het onderzoek, hoe de integriteit van het verkregen materiaal wordt gewaarborgd en wanneer het materiaal vernietigd moet worden.[49] Het bestaan van duidelijk, gedetailleerde regels is belangrijk, zeker wanneer de beschikbare technologie steeds complexer wordt.[50] Dit geldt voor maatregelen voor het observeren in het geheim, maar ook wanneer het observeren openlijk gebeurt.[51] Zonder voldoende duidelijke uitwerking bestaat het gevaar dat dit soort wetten de democratie ondermijnen of zelfs vernietigen.[52]

Wanneer de maatregel gebaseerd wordt op artikel 55c lid 4 Sv, heeft de maatregel een basis in de nationale wet. Deze wet is voldoende toegankelijk: de invoering van deze wet is gepubliceerd in het Staatsblad en is online te bekijken. Ook is duidelijk op welke categorie personen de maatregel kan worden toegepast: personen die worden verdacht van of veroordeeld zijn voor een misdrijf waarop een gevangenisstraf van vier jaren of meer staat (ook wel een voorlopige hechtenis-feit genoemd) én iedere andere verdachte over wiens identiteit twijfel bestaat.[53] Om aangemerkt te worden als verdachte moet er sprake zijn van een 'redelijk vermoeden van schuld' aan een strafbaar

feit.[54] In het Wetboek van Strafvordering zijn de eisen aan hoe sterk het vermoeden van schuld moet zijn strenger naar mate de toegepaste middelen ingrijpender zijn.[55] Deze balans ontbreekt bij gezichtsherkenningstechnologie: een redelijk vermoeden van schuld wordt in het algemeen vrij snel aangenomen[56], terwijl de technologie zeer ingrijpend is. Daarnaast moet er voldoende gedetailleerd zijn uitgewerkt bij welke strafbare feiten de maatregel mag worden toegepast. Dit is niet het geval bij 'iedere andere verdachte' van wie de identiteit niet bekend is: daar is elk strafbaar feit voldoende.

Regels over de uitvoering van het nemen van de foto's en het verwerken van de resultaten daarvan staan in het Besluit identiteitsvaststelling verdachten en veroordeelden (Bivv).[57] In dat besluit staan echter weinig regels voor de te volgen procedures. Er ontbreekt een regeling over toezicht vooraf door een rechter. Rechterlijk toezicht is wenselijk, aangezien automatische gezichtsherkenning een grote impact heeft op de gehele samenleving. Het verandert het karakter van de observatie, nu het op grotere schaal en binnen aanzienlijk kortere tijd kan worden toegepast. Het herkennen van personen met geautomatiseerde gezichtsherkenning zal eerder regel dan uitzondering worden.[58] Rechterlijk toezicht is de beste waarborg voor onafhankelijkheid en onpartijdigheid.[59] Op dit moment is de enige vorm van toezicht vooraf dat er een bevel nodig is van de officier van justitie als de maatregel moet worden toegepast op NN'ers. Dit geldt dus niet voor toepassing op verdachten van een voorlopige hechtenis-feit: daar is überhaupt geen bevel voor nodig. Ook moet er tijdens en na het toepassen van de maatregel onafhankelijk toezicht zijn op het algemene functioneren van de instantie die de maatregel uitvoert.[60] Uit de wet is verder niets op te maken over regels over de integriteit van het verkregen materiaal. De regels over vernietiging van het materiaal staan in het Bivv. Daar staat onder andere dat foto's van personen die niet meer als verdachte worden aangemerkt, vernietigd moeten worden.[61] Dit gedeelte is dus wel 'voorzien bij wet', maar uit de antwoorden op Kamervragen over CATCH blijkt echter dat de politie zich niet houdt aan de bewaartermijnen omdat er 'in de praktijk onduidelijkheid over bestaat', en volgens de minister moeten we maar accepteren dat er niet wordt voldaan aan de letter van de wet.[62] Dit betekent ook dat foto's van personen die niet meer verdacht worden van een strafbaar feit niet altijd verwijderd worden. Er blijven dus onschuldige mensen in de strafrechtsketendatabank staan. Uit de wet blijkt verder niet hoe het publiek geïnformeerd dient te worden over het gebruik van de technologie, en of het gebruik en de resultaten door de politie periodiek dienen te worden gepubliceerd in openbare rapporten. Dit zijn belangrijke regels om misbruik te voorkomen. Verder blijkt uit de eerder genoemde antwoorden op Kamervragen dat er ééns per vier jaar een 'privacy audit' wordt gedaan naar de naleving van de Wet politiegegevens[63], maar dat daarbij niet wordt gekeken naar specifieke systemen.[64] Er wordt dus niet specifiek naar de risico's van gezichtsherkenningstechnologie gekeken. Er gaat volgens de minister wel een gegevensbeschermingseffectbeoordeling voor CATCH worden uitgevoerd.[65]

Er ontbreekt een hoop uitleg en detail in het wetsartikel. Al met al blijkt dat deze wet onvoldoende is om bescherming te bieden tegen misbruik wanneer het de basis vormt voor gezichtsherkenning in de publieke ruimte. Er moet geconcludeerd worden bij dat type gebruik er niet voldaan wordt aan het vereiste 'voorzien bij wet'.

### 6.2.2 Noodzakelijk in een democratische samenleving?

De juridische betekenis van 'noodzakelijk in een democratische samenleving' is dat er een dringende maatschappelijke behoefte moet zijn voor de beperking van het grondrecht.[66] Het is belangrijk om hier te benadrukken dat 'noodzakelijk' niet hetzelfde betekent als 'efficiëntie' of 'gemak', iets wat in de praktijk nog wel eens vergeten wordt. Als iets dringend is, zegt dat iets over de urgentie van de maatregel: is de maatregel op het gegeven tijdstip (al) dringend?[67] Van urgentie zal slechts sprake zijn in uitzonderlijke gevallen, bijvoorbeeld als gezichtsherkenningstechnologie in de publieke ruimte wordt ingezet als een aanslagpleger weet te ontkomen. Het is urgent om die aanslagpleger snel te vinden om een mogelijke tweede aanslag te voorkomen. Maar meestal zal de vereiste urgentie ontbreken. Er zal dan geen 'dringende maatschappelijke behoefte' zijn. Er is daarnaast geen 'dringende maatschappelijke behoefte' om informatie van activisten, die nooit veroordeeld zijn voor een strafbaar feit, te bewaren in een databank met informatie van verdachten en veroordeelden van een voorlopige hechtenis-feit. Dit mag alleen wanneer dit 'absoluut noodzakelijk' is voor een specifiek onderzoek.[68] Het doel van de politie om identiteitsfraude te voorkomen zal hier niet aan voldoen als het opslaan slechts een voorzorgsmaatregel is, en er geen sterk vermoeden is dat die persoon daadwerkelijk identiteitsfraude heeft gepleegd of zal gaan plegen.[69]

Naast de urgentie wordt er gekeken of de maatregel voldoet aan de vereisten van proportionaliteit (het belang van de maatregel moet in verhouding staan tot de mate van inbreuk op het grondrecht) en

subsidiariteit (er zijn geen andere, minder ingrijpende maatregelen mogelijk). Een beperking kan gerechtvaardigd zijn als dit de rechten en vrijheden van anderen, de openbare orde of de openbare veiligheid beschermt.[70] De beperking moet wel proportioneel zijn in verhouding met het beoogde doel: er moet een rechtvaardig evenwicht bestaan tussen alle betrokken belangen. De bevoegdheid moet niet te breed geformuleerd zijn. De proportionaliteit hangt onder andere af van de aard, omvang en duur van de maatregel, op welk moment de maatregel mag worden ingezet, hoe het toezicht op de maatregel geregeld is en wat de rechtsmiddelen zijn.[71] De proportionaliteit wordt vanaf paragraaf 6.2.2.1 uitgewerkt per grondrecht. De proportionaliteit van een maatregel verschilt per specifieke situatie: de mate van inbreuk op een grondrecht en het belang van het inzetten van de maatregel zijn afhankelijk van de omstandigheden. Gezien onze beperkte reikwijdte en capaciteit zijn niet alle verschillende gevallen volledig uitgewerkt, maar is geprobeerd een algemeen overzicht te geven.

Ook het voldoen aan het vereiste van subsidiariteit is erg afhankelijk van de omstandigheden. Het verschilt per zaak wat voor minder indringende maatregelen de politie kan inzetten in plaats van gezichtsherkenning, afhankelijk van hoeveel kennis de politie heeft van de verdachte op dat moment. Een maatregel die de politie bijvoorbeeld kan inzetten is menselijke observatie. Dit gebeurt in het geheim en is doorgaans gelimiteerd tot de publieke ruimte, aangezien het volgen van iemand in de privéruimte, zoals een woning, niet zo onopvallend te doen is. Observatie kan zowel niet-stelselmatig als stelselmatig worden ingezet.[72] Vanwege de beperkte mogelijkheden met niet-stelselmatige observatie zal dit meestal een beperkte privacy inbreuk opleveren. Stelselmatige observatie is een grotere inbreuk op de privacy, want daarmee kan een redelijk gedetailleerd beeld van bepaalde onderdelen van iemands leven worden verkregen.[73] Er kan bijvoorbeeld informatie worden verkregen over iemands sociale contacten, religie of lidmaatschap bij een vereniging. Hoe groot de inbreuk is, is afhankelijk van de mate van stelselmatigheid van de observatie, wat onder andere wordt beïnvloedt door het gebruik van een technisch hulpmiddel, de plaats, de continuïteit, de frequentie en de duur van de maatregel.[74]

Een andere maatregel is GPS tracking. Dit kan bijvoorbeeld door stiekem een zender onder iemands auto te bevestigen. Een zender mag niet zonder toestemming op een lichaam worden geplaatst.[75] Het volgen via GPS tracking kan gelijk, meer, of minder indringend zijn dan menselijke observatie, afhankelijk van de duur, intensiteit en plek van observatie. De verkregen informatie met GPS tracking is minder privacygevoelig: het registreert alleen iemands locatie en bewegingen. Er wordt niet geregistreerd wat iemand doet of zegt.[76] GPS tracking kan een grotere privacy inbreuk opleveren wanneer iemands locatie met een hoge frequentie wordt geregistreerd. Dit levert veel meer en meer gedetailleerde informatie op. Waar iemand over een langere periode van tijd heen gaat kan meer onthullen over een persoon dan een enkele reis die afzonderlijk bekeken wordt. Dan kan bijvoorbeeld duidelijk worden of iemand vaak naar de kerk of het ziekenhuis gaat, misschien wel een affaire heeft of regelmatig naar politieke bijeenkomsten gaat. Hoe groot de privacy inbreuk is, is dus afhankelijk van hoe GPS tracking precies wordt ingezet.

Iemands locatie kan ook worden gevolgd via haar of zijn mobiele telefoon. Deze informatie kan onder andere worden opgevraagd bij de telecomprovider, er kan een ‘stille sms’ worden verzonden door de politie (deze sms ziet de ontvanger niet, en genereert ‘verkeer’: zo is te zien waar diegene is wanneer hij dat smsje krijgt), er kan gebruik gemaakt worden van een IMSI-catcher om iemands locatie te bepalen en het MAC-adres kan worden uitgelezen.[77] Het volgen van iemands locatie via de telefoon kan een zeer gedetailleerde locatie geven, en het vereist geen fysieke indringing: er hoeft niks stiekem te worden geplaatst, de maatregel kan van buitenaf worden ingezet. Afhankelijk van hoe de maatregel wordt ingezet kan deze locatiedata een kleinere of grotere privacy inbreuk opleveren dan het verkrijgen van informatie over wat iemand doet of zegt.

De politie kan ook elke andere informatie vorderen van degene die waarschijnlijk toegang heeft tot die informatie, zoals bijvoorbeeld pinbetalingen van de verdachte.[78] Deze informatie kan iets zeggen over de locatie van een persoon, omdat is op te maken waar de pinbetalingen zijn gedaan. Uit deze informatie kunnen ook gevoelige gegevens blijken, over bijvoorbeeld religie, gezondheid, seksualiteit, een lidmaatschap bij een bepaalde vereniging, enzovoort, afhankelijk van wat er gekocht is. Dit kan dus een grotere inbreuk op de privacy vormen.

Een andere maatregel is het publiceren van een visueel signalement (een beschrijving van hoe de persoon eruitziet) of een foto, in de hoop dat iemand de persoon herkent. Dit vormt een grotere inbreuk op iemands privacy, aangezien iemands uiterlijk bekend wordt gemaakt aan het publiek, samen met het feit dat diegene verdacht wordt van een strafbaar feit.

Als er wordt gezocht naar een auto waarvan de

nummerplaat bekend is, kan automatische nummerplaatherkenning worden ingezet, maar deze maatregel mag niet worden ingezet in strafrechtelijke onderzoeken. Politie-eenheden hebben dit voorheen wel gedaan, maar daarvoor ontbreekt een wettelijke grondslag.[79]

Het verschil tussen de voorgaande maatregelen en het toepassen van gezichtsherkenning in de publieke ruimte is dat de voorgaande maatregelen alleen de verdachte of een kleine kring betrokkenen rondom de verdachte treffen. Er wordt dus veel minder informatie geregistreerd. Dit zijn geen massasurveillance technieken. Met gezichtsherkenning worden de gezichten van alle personen die toevallig in de buurt zijn geregistreerd en kunnen ook hun locaties over een langere periode van tijd worden gevolgd, en uit deze data kan vervolgens verdere informatie blijken. Dit kan ongemerkt gebeuren: opnames van je gezicht kunnen gemaakt worden zonder dat je dit in de gaten hebt. Door de scherpere focus zullen de voorgaande maatregelen waarschijnlijk geen 'chilling effect' opleveren en worden burgers aanzienlijk minder beperkt in hun rechten en vrijheden.

**6.2.2.1 Het recht op privacy**
Zoals eerder uitgelegd vormt gezichtsherkenningstechnologie een vergaande inbreuk op de privacy van mensen. De maatregel is zeer indringend, en uit paragraaf 6.2.1 blijkt dat er onvoldoende (procedurele) mogelijkheden zijn om de inbreuk op het recht op privacy zo klein mogelijk te houden. Het belang van het inzetten van de maatregel zal doorgaans niet zwaar genoeg zijn om de ernstige inbreuk op de privacy van burgers te legitimeren, en een evenwicht tussen dat belang en die inbreuk ontbreekt. Er zal niet voldaan zijn aan de proportionaliteitseis. Alleen in uitzonderlijke gevallen kan het zo zijn dat het belang van het inzetten van de maatregel zwaarder weegt dan de vergaande inbreuk op de privacy van burgers. Dit is bijvoorbeeld het geval als er een aanslag is gepleegd, en de aanslagpleger weet te ontkomen. Het belang van het inzetten van de maatregel (het zo snel mogelijk lokaliseren van de aanslagpleger om een tweede aanslag te voorkomen) kan dan zwaarder wegen dan de vergaande inbreuk op de rechten en vrijheden van mensen.

Naast het feit dat er doorgaans niet voldaan zal zijn aan het vereiste van 'noodzakelijk in een democratische samenleving', zal er ook niet voldaan aan het vereiste 'voorzien bij wet'. De beperking op het recht op privacy is dus niet toegestaan, en er is dan sprake van een schending van dat grondrecht.

De gevolgen van deze schending zijn groot. Door gezichtsherkenningstechnologie in de publieke ruimte kun je niet meer anoniem over straat gaan. Het signaal dat smartphones continu uitzenden maakt al dat je te volgen bent, maar je smartphone kan je thuis laten. Je gezicht niet. En ja, er staan al camera's in de publieke ruimte en daar wordt je ook door gefilmd, maar die registreren geen gezichten en identificeren je niet. Ook het tegenargument dat iemand 'toch niks te verbergen heeft' is een verkeerde aanname.[80] Privacy gaat niet alleen over het verbergen van 'slechte' dingen. Privacy gaat om je vrijheid. Een mens moet vrije keuzes kunnen maken in hoe het zijn of haar leven inricht, en vrij zijn om zijn of haar eigen identiteit vorm te geven, zonder dat iemand zich daarmee bemoeit. Wanneer je weet dat je op straat in de gaten gehouden wordt, ga je je anders gedragen. Je probeert je zo 'normaal' mogelijk te gedragen, zo veel mogelijk buiten beeld te blijven of je gaat niet meer naar bepaalde plekken waar gezichtsherkenningscamera's hangen. Met de komst van emotieherkenning kan het zelfs zo zijn dat je je niet vrij meer voelt om je gezichtsuitdrukkingen te laten zien. Je autonome denken en handelen worden hierdoor aangetast. Het kan niet zo zijn dat we onze manier van leven aan moeten passen, en daardoor onze vrijheid beperken, om onszelf te beschermen tegen deze ongerechtvaardigde massasurveillance.

**6.2.2.2 Het recht op vrijheid van meningsuiting en het recht op vrijheid van vergadering en vereniging**
De toepassing van gezichtsherkenning in de publieke ruimte zal leiden tot een 'chilling effect', een ernstige inbreuk op het recht op vrijheid van meningsuiting. Er zijn weinig (procedurele) mogelijkheden om de inbreuk op de vrijheid van meningsuiting minimaal te houden (het ontbreken van voldoende duidelijke regels en procedurele waarborgen om misbruik te voorkomen zijn hierboven uitgewerkt). Het belang van het inzetten van de maatregel zal doorgaans niet zwaar genoeg zijn om deze ernstige inbreuk te legitimeren. Hier is dus ook geen evenwicht tussen het belang van de inzet en de inbreuk, en zal er niet voldaan worden aan de proportionaliteitseis. Alleen in uitzonderlijke gevallen zal het belang van de maatregel zwaarder wegen dan het recht op vrijheid van meningsuiting.

Ook hier zal de beperking doorgaans niet 'noodzakelijk in een democratische samenleving' zijn. Slechts in uitzonderlijke gevallen zal dit anders zijn. Er zal niet voldaan zijn aan het vereiste 'voorzien bij wet'. De beperking op het recht van vrijheid van meningsuiting is dus niet toegestaan en er is dan sprake van een schending van dat grondrecht.

Er is expliciet opgenomen dat de politie 'rechtmatige beperkingen' op de vrijheid van vergadering en vereniging mag opleggen, maar deze bevoegdheid

moet streng worden uitgelegd.[81] De inmenging moet beperkt blijven tot de 'uitoefening' van het recht, en mag niet de essentie van het recht op vergadering en vereniging aantasten.[82] Wanneer een beperking 'rechtmatig' is, moet hetzelfde worden uitgelegd als wanneer een beperking 'voorzien bij wet' is: er moet een effectieve waarborg bestaan tegen misbruik.[83] Een beperking bestaat niet alleen uit een direct verbod tot vereniging of vergadering, maar kan bestaan uit verschillende maatregelen die voor, tijdens of na een bijeenkomst of demonstratie kunnen worden toegepast.[84] Een maatregel die leidt tot een 'chilling effect' kan mensen ontmoedigen om deel te nemen aan een bijeenkomst. Hierdoor kunnen mensen niet meer ongehinderd het recht op vergadering en vereniging uitoefenen. Dit leidt tot een schending van het recht.[85]

Zoals eerder uitgelegd kan het zijn dat mensen niet meer naar bepaalde bijeenkomsten durven te gaan als ze weten dat ze in de gaten worden gehouden door de politie. Zij kunnen dus niet meer ongehinderd het recht op vergadering en vereniging uitoefenen: de maatregel zal de essentie van het grondrecht aantasten. Er zal dus sprake zijn van een beperking van het grondrecht door de politie. Vervolgens moet er gekeken worden of die beperking rechtmatig is. Zoals hierboven is uitgelegd, bevat de wet onvoldoende regels om misbruik van die maatregel te voorkomen. De voorwaarden voor het inzetten van de maatregel worden niet voldoende uitgewerkt. De beperking zal niet voldoen aan de vereiste voorzienbaarheid bij wet, en zal dus ook niet voldoen aan de hier vereiste 'rechtmatigheid'. De beperking is niet rechtmatig en er is dan sprake van een schending van het grondrecht.

Het verbieden van gezichtsherkenning op bepaalde plekken of zones of het niet mogen toepassen van gezichtsherkenning bij demonstraties en andere bijeenkomsten, kunnen de proportionaliteit van de maatregel beïnvloeden. Het effect hiervan zal echter beperkt zijn: het 'chilling effect' zal blijven bestaan. Het gevoel dat je op een bepaald moment bekeken kan worden blijft, ondanks dat dat op sommige plekken misschien niet gebeurt, met als gevolg dat je je alsnog anders gaat gedragen. De essentie op het recht op vrijheid van meningsuiting en vergadering en vereniging zal nog steeds aangetast worden.

De gevolgen van de schending van de vrijheid van meningsuiting en de vrijheid van vergadering en vereniging zijn ernstig. De ontwikkeling van het publieke debat wordt belemmerd. Wanneer mensen worden beperkt in hun deelname aan het publieke debat, worden zij ook beperkt in het vormen van een geïnformeerde mening. Dit is een aantasting van de zelfontwikkeling en zelfontplooiing van de mens. Het vrij kunnen uiten van ideeën en meningen is belangrijk voor actieve, betrokken burgers in de maatschappij en zorgt voor een goed functionerende democratie. Onbezorgd gedachten en ideeën kunnen uitwisselen met anderen is essentieel voor ontwikkeling en vooruitgang van de samenleving. Vrijheid van meningsuiting, gecombineerd met de demonstratievrijheid en de vrijheid van vergadering en vereniging, vormen de motor van verandering in de maatschappij. Het gevaar ontstaat ook dat het publieke debat geleid wordt door de geaccepteerde meerderheid, en voorbij gaat aan behoeften van minderheden. Dit leidt tot een verdeling in de samenleving, waar tolerantie en respect voor verschillen verminderen. Daarnaast zorgt een effectief publiek debat ervoor dat de overheid gecontroleerd wordt en verantwoordelijk kan worden gehouden, wat het risico op machtsmisbruik verkleint. Met de komst van gezichtsherkenningstechnologie in de publieke ruimte is het steeds moeilijker om anoniem je mening te kunnen uiten, bijvoorbeeld bij demonstraties. En soms wil je (controversiële) ideeën of meningen anoniem kunnen uiten. Bijvoorbeeld omdat je bang bent dat het gevolgen heeft voor je werk als je werkgever jouw meningen over een bepaald onderwerp weet, of je wil niet dat je familie op de hoogte is van sommige dingen. Of als je bang bent dat jouw ideeën of meningen je veiligheid in gevaar brengen. Gezichtsherkenningstechnologie in de publieke ruimte leidt tot een aantasting van een vrije, geïnformeerde, diverse en democratische samenleving.

#### 6.2.2.3 Het recht op godsdienstvrijheid

Door het toepassen van gezichtsherkenning in de publieke ruimte kan de belijding van een geloofsovertuiging van mensen worden geregistreerd. Dit kan er toe leiden dat mensen zich niet vrij voelen om hun eigen godsdienst tot uitdrukking te brengen in bijeenkomsten, of om bepaalde gebedshuizen binnen te treden. Dit is een inbreuk op hun godsdienstvrijheid. Er zijn weinig (procedurele) mogelijkheden om deze inbreuk minimaal te houden (het ontbreken van een duidelijke wettelijke grondslag en procedurele waarborgen om misbruik te voorkomen zijn hierboven uitgewerkt). Het belang van het inzetten van de maatregel zal doorgaans niet zwaar genoeg zijn om deze inbreuk te legitimeren. Hier is dus geen evenwicht tussen het belang van de inzet en de inbreuk, en er zal niet voldaan zijn aan de proportionaliteitseis. Slechts in uitzonderlijke gevallen kan het belang van de maatregel zwaarder wegen dan het recht op godsdienstvrijheid.

De beperking zal doorgaans dus niet 'noodzakelijk in een democratische samenleving' zijn. Daarnaast zal er

ook niet voldaan zijn aan het vereiste 'voorzien bij wet'. De beperking op de godsdienstvrijheid is dan niet toegestaan en dus is er sprake van een schending van dat grondrecht.

Ook hier zijn regels denkbaar die de proportionaliteit van de maatregel beïnvloeden. Het verbieden van gezichtsherkenning in de buurt van gebedshuizen bijvoorbeeld, of het niet mogen toepassen van gezichtsherkenning bij religieuze bijeenkomsten. Maar ook het effect van deze regels zal beperkt zijn: hier blijft het 'chilling effect' ook bestaan, omdat het gevoel dat je op een bepaald moment bekeken kan worden blijft. Daarnaast biedt het geen bescherming tegen mensen die op andere manieren hun geloof uitdragen, bijvoorbeeld via kleding of accessoires.

De schending van dit grondrecht kan er toe leiden dat mensen zich niet vrij voelen om hun eigen godsdienst te bepalen en tot uitdrukking te brengen in bijeenkomsten. Dit belemmert de innerlijke geestelijke vrijheid en de religieuze identiteitsvorming van mensen. Deze identiteitsvorming is belangrijk omdat het mensen kan helpen met het uitzoeken wie zij zijn, waar zij voor staan en wat zij willen in het leven. Het recht vormt een fundament van een diverse en tolerante samenleving. Wanneer mensen zich niet vrij voelen om hun geloof in het openbaar tot uitdrukking te brengen, draagt gezichtsherkenningstechnologie bij aan religieuze onderdrukking.

#### 6.2.2.4 Worden de persoonsgegevens voldoende beschermd?

Afbeeldingen van het gezicht zijn biometrische gegevens, en dus bijzondere persoonsgegevens.[86] De verwerking van bijzondere persoonsgegevens, in de Wet politiegegevens (Wpg) ook wel 'bijzondere politiegegevens' genoemd, mag alleen wanneer dit onvermijdelijk is voor het doel van de verwerking, in aanvulling op de verwerking van andere politiegegevens over de persoon en als de gegevens goed genoeg zijn beveiligd.[87] De gegevens moeten toereikend zijn (dit is de ondergrens, het moet niet te weinig informatie zijn), ter zake dienend (geschikt voor het doel) en niet excessief zijn (dit is de bovengrens, niet meer informatie dan nodig).[88] Er moet een onderscheid worden gemaakt tussen verschillende categorieën van betrokkenen, zoals verdachten, veroordeelden, slachtoffers en derden.[89] Uit het woord 'zoals' is op te maken dat de opsomming in het wetsartikel niet uitputtend is en zou ook de categorie van personen die niet meer verdacht worden (en dus onschuldig zijn) daar onder kunnen vallen.

Er zal met de inzet van gezichtsherkenning in de publieke ruimte op verschillende manieren inbreuk gemaakt worden op de Wpg. Wanneer een individu wordt gevolgd door de politie, hoeft dit niet op basis van zijn gezicht te gebeuren. Iemand kan bijvoorbeeld ook worden gevolgd via signalen uit haar of zijn telefoon. Het is dus nog maar de vraag of de verwerking onvermijdelijk is. Wanneer gezichtsherkenning in de publieke ruimte wordt toegepast om iemand te lokaliseren, worden de gezichten geregistreerd van iedereen die in beeld komt, ook van onschuldige burgers. Dit is te veel informatie voor het doel en voldoet niet aan het vereiste van excessiviteit. Als bij gezichtsherkenning in de publieke ruimte van dezelfde strafrechtsketendatabank gebruik wordt gemaakt als de databank die bij CATCH wordt gebruikt, worden de gegevens van alle personen in dezelfde strafrechtsketendatabank gestopt. Gegevens van zowel verdachten, veroordeelden én onschuldigen.Er wordt dus geen onderscheid gemaakt tussen de verschillende categorieën personen. De persoonsgegevens zullen onvoldoende beschermd worden bij het gebruik van gezichtsherkenning in de publieke ruimte.

#### 6.2.2.5 Is de beperking op het verbod op discriminatie toegestaan?

Het discriminatieverbod moet samen met andere verdragsrechten worden ingeroepen. Dat kan in dit geval samen met het recht op privacy, de godsdienstvrijheid, de vrijheid van meningsuiting en de vrijheid van vergadering en vereniging. In het Europees Verdrag voor de Rechten van de Mens staat niet letterlijk dat een beperking op het discriminatieverbod is toegestaan. Dit betekent niet dat elke vorm van ongelijke behandeling niet mag. Van strijd met het discriminatieverbod in combinatie met een ander grondrecht is sprake als er 1) een verschillende behandeling plaatsvindt, 2) deze verschillende behandeling geen gerechtvaardigd doel heeft (dit betekent dat er geen objectieve en redelijke rechtvaardiging is voor het doel en de gevolgen van de maatregel) en 3) er geen sprake is van proportionaliteit tussen de maatregel en het beoogde doel.[90] Om de proportionaliteit te beoordelen moet er gekeken worden of er een juist evenwicht is tussen alle betrokken belangen.[91] Als iemand anders behandeld wordt vanwege zijn of haar 'ras', levert dit sneller een mensonterende situatie op, dan een verschillende behandeling op een andere grond.[92]

Zoals in het vorige hoofdstuk besproken, functioneert gezichtsherkenningstechnologie op een discriminerende en racistische manier voor minderheidsgroepen. Hierdoor kunnen valse positieven ontstaan: iemand wordt door het systeem 'herkend', terwijl het niet die persoon is. Er zal dan

eerder een opsporingsonderzoek gestart worden naar deze personen. Daarnaast bestaat de kans dat bepaalde minderheidsgroepen eerder in het systeem terecht komen dankzij etnisch profileren. Dit vindt plaats wanneer de politie zonder goede of geldige reden iemand stopt, controleert, fouilleert of aanhoudt, (mede) vanwege zijn huidkleur of herkomst. Etnische minderheden zijn relatief oververtegenwoordigd in politiecontroles.[93] Minderheidsgroepen kunnen dus anders behandeld worden als deze technologie wordt toegepast. Hier is geen objectieve rechtvaardigheid voor: dit gebeurt 'slechts' door technologische gebreken en/of etnisch profileren. Dit is een mensonterende behandeling, en er zal niet voldaan zijn aan de vereiste proportionaliteit. Zelfs in uitzonderlijke gevallen zal het lastig zijn om aan de vereiste proportionaliteit te voldoen.

Door het ontbreken van een gerechtvaardigd doel is er sprake van een ongeoorloofde inbreuk op het discriminatieverbod en is er sprake van een schending van dit grondrecht. Toch is het niet wenselijk als de discriminerende en racistische werkwijze van de technologie 'gerepareerd' wordt. Voor het repareren van de technologische problemen moet de technologie namelijk verder 'trainen' met meer data van minderheidsgroepen. Dit kan alleen maar worden verkregen door middel van massale dataverzameling, terwijl minderheidsgroepen sowieso al redenen hebben om zich extreem oncomfortabel voelen over dataverzameling. Zo is er een onderzoeker die, zonder te vragen, beelden van transgender personen die hun transitie bijhielden op internet gebruikt heeft om zijn algoritme verder te trainen.[94] Zoé Samudzi, een promovenda aan de Universiteit van San Francisco, schrijft: "In een land waar opsporingsdiensten een donkere huidskleur nu al associëren met criminaliteit, waarom zouden we dan willen dat onze gezichten beter te registreren zijn via technologie die ontworpen is om ons te monitoren? Het is geen maatschappelijke vooruitgang om mensen van kleur zichtbaarder te maken voor deze technologie, die alleen maar verder tegen ons gebruikt gaat worden."[95] Daarnaast zal er nooit genoeg data verzameld kunnen worden om vooroordelen en het risico op valse positieven of valse negatieven te voorkomen.[96] Discriminatie en racisme zijn sociaal-maatschappelijke problemen. Dit willen oplossen met technologie zal altijd ontoereikend zijn, want de kans blijft bestaan dat degenen die de technologie toepassen, dit niet op een objectieve manier doen. Bijvoorbeeld wanneer de politie zich schuldig maakt aan etnisch profileren. Het toepassen van gezichtsherkenningstechnologie kan dit in de hand werken, ongeacht de mate van nauwkeurigheid of neutraliteit van de technologie.

#### 6.2.2.6 Uitzonderlijke gevallen, function creep en een verbod op gezichtsherkenning

Uit de vorige paragrafen blijkt dat er meestal alleen zal worden voldaan aan het vereiste van 'noodzakelijk in een democratie' in uitzonderlijke gevallen, zoals het voorbeeld van de ontsnapte aanslagpleger. Vergaande surveillancemiddelen worden dan ook vaak geïntroduceerd als 'rots in de branding' voor zulke gevallen: dat met de nieuwe technologie aanslagplegers snel opgespoord kunnen worden en zo meer aanslagen voorkomen kunnen worden. Iedereen veilig, iedereen blij. Maar dit zijn *uitzonderlijke gevallen*: zo vaak komen die helemaal niet voor. Weegt de kleine kans op zo'n situatie zwaarder dan de bescherming van de rechten en vrijheden van burgers? Met de argumentatie dat nieuwe technologieën noodzakelijk zijn voor onze veiligheid wordt ingespeeld op onze angstgevoelens, maar angst is een slechte raadgever.[97] Dankzij de ontstane angstcultuur denken we dat we vaker aan steeds groter gevaar worden blootgesteld, van epidemieën tot terrorisme. In werkelijkheid zijn zijn we veelal veiliger dan ooit.[98]

Wanneer het toch mogelijk is om de technologie in dit soort uitzonderingsgevallen toe te passen, bestaat het gevaar dat het gebruik langzaamaan steeds verder wordt uitgebreid naar andere situaties. De technologie wordt ingezet voor andere doeleinden dan oorspronkelijk bedoeld was: er ontstaat function creep. Gezichtsherkenning is een gevaarlijke technologie. Er zit een groot verschil tussen welke mogelijkheden de politie (legitiem) zal gebruiken en wat de technologie kan. Om misbruik en function creep te voorkomen, moet het gebruik van deze technologie in zijn geheel verboden worden. Het inperken van de bevoegdheden van de politie rondom gezichtsherkenningstechnologie is niet genoeg. Evan Selinger (hoogleraar filosofie) en Woodrow Hartzog (hoogleraar recht en informatica) zeggen hierover: 'Gezichtsherkenning moet verboden worden, voordat we er zo afhankelijk van worden dat we de onvermijdelijke aantasting van onze grondrechten accepteren als noodzakelijk voor "vooruitgang".'[99] Dat mensen vaak angstig zijn voor nieuwe technologie, maar dat dat een overdreven reactie is, gaat in het geval van gezichtsherkenning niet op. Het is een veel verdergaande bedreiging dan andere technologische ontwikkelingen. Alle informatie die ermee verzameld kan worden – waar je winkelt, waar je protesteert, waar je werkt, je identiteit (voor zover die af te lezen is uit beelden), je emoties, en ga zo maar door – kunnen gebruikt worden om je te controleren en te manipuleren. Het verhogen van privacybescherming tegen nieuwe technologieën door de Hoge Raad of het Europees Hof voor de Rechten van de Mens duurt jaren. Die tijd hebben we niet. Gezien de snelheid van

technologische ontwikkelingen, is tegen die tijd het gebruik van gezichtsherkenningstechnologie volledig genormaliseerd.

# 7. CONCLUSIE

Het gebruik door de politie van gezichtsherkenningstechnologie in de publieke ruimte is een massasurveillance middel. Het fungeert als een vangnet, waarmee te veel informatie over te veel mensen wordt geregistreerd. De politie maakt op dit moment nog geen gebruik van de technologie in de publieke ruimte, maar het is niet onwaarschijnlijk dat ze dit in de toekomst wel gaat doen.

Met de komst van deze technologie is ons gezicht niet langer van onszelf. De technologie functioneert discriminerend en racistisch, waardoor toch al kwetsbare minderheidsgroepen onevenredig benadeeld worden. Het gebruik ervan kan etnisch profileren in de hand werken en het levert een schending op van de rechten en vrijheden van burgers. Het recht op privacy, het recht op bescherming van persoonsgegevens, de vrijheid van meningsuiting, de demonstratievrijheid en de vrijheid van vergadering en vereniging, de godsdienstvrijheid en het discriminatieverbod worden allemaal geschonden. Gezichtsherkenning in de publieke ruimte vormt een kritieke bedreiging voor onze vrije, geïnformeerde, democratische en diverse samenleving. Het beïnvloedt ons autonome denken en handelen, en weerhoudt ons ervan om onbezorgd onze eigen gang te gaan. De zelfontwikkeling en zelfontplooiing van de mens worden ernstig aangetast. Gezichtsherkenning in de publieke ruimte zal bijna onmogelijk te ontwijken zijn, waardoor groepen en individuen continu kunnen worden geobserveerd, gevolgd en gemanipuleerd. En op een voorheen onmogelijke schaal en snelheid. Dit maakt ons niet veilig, maar onderdrukt ons.

Vergaande surveillancemiddelen worden vaak geïntroduceerd als ‘rots in de branding’ voor uitzonderlijke gevallen, bijvoorbeeld dat het dé maatregel zou zijn om een terrorist zo snel mogelijk op te sporen. Deze gevallen zijn niet voor niets *uitzonderlijk*: zo vaak komen ze helemaal niet voor, en de kleine kans op zo’n situatie zou niet zwaarder moeten wegen dan de bescherming van de rechten en vrijheden van burgers. De overheid moet stoppen met het inspelen op onze angstgevoelens. We moeten voorkomen dat we de onvermijdelijke aantasting van onze grondrechten accepteren als noodzakelijk voor ‘vooruitgang’. Het gebruik van gezichtsherkenningstechnologie moet zo snel mogelijk verboden worden, voordat het gebruik volledig genormaliseerd is in onze samenleving. Want wanneer het gebruik normaliseert, raken we gewend aan de hoeveelheid aan mogelijkheden die gezichtsherkenning biedt, en denken we niet meer na over de grootschalige gevolgen.

Het zo snel mogelijk verbieden van gezichtsherkenningstechnologie kan voorkomen dat Nederland steeds verder afglijdt naar een totale surveillancestaat, waarin niemand kan ontkomen aan het alziend oog van de overheid of van anderen.

**Paula Hooyman** volgt de master Informatierecht aan de Universiteit van Amsterdam. In september en oktober 2019 liep zij stage bij Bits of Freedom.

*Met veel dank aan Vera de Jong voor haar hulp bij het uitwerken van de technische werking van gezichtsherkenningstechnologie.*

*Veel dank aan Mohamed el Maslouhi voor zijn hulp bij het praten tegen de gezichtsherkennings-API voor onze test op de Dam in Amsterdam.*

*En ook veel dank aan John Riemen en Ben van Hoek van de Nationale Politie voor hun toelichting op het systeem CATCH.*

# Noten

1. In verband met de omvang van het onderzoek is er alleen gekeken naar het gebruik van de politie van de strafrechtsketendatabank. Er is niet gekeken naar het gebruik van de vreemdelingendatabank, waarvoor een andere juridische grondslag geldt.
2. Zie verder hoofdstuk 5.
3. In de stadions van ADO Den Haag, FC Den Bosch, FC Groningen en Heracles Almelo wordt/is gezichtsherkenning gebruikt als toegangsautorisatie.
4. RET Rotterdam heeft bijvoorbeeld een proef gedaan met gezichtsherkenning in 2010. Er zijn nieuwe trams gekomen waar geen camera's met gezichtsherkenning in hangen, maar de proef is nooit officieel beëindigd.
5. Zie bijvoorbeeld het Finse bedrijf Uniqul en het Chinese bedrijf Alipay. Je kan ook via Face ID betalen in de iOs App Store.
6. Dit kon met apps als NameTag en SearchFace.
7. Zo heeft de Britse supermarktketen Tesco camera's met gezichtsherkenning geïnstalleerd om gepersonaliseerde advertenties te kunnen laten zien.
8. Dit onderzoek is echter wel beperkt: er is alleen gekeken naar homo- en heteroseksuelen, en mensen van kleur zijn niet meegenomen in het onderzoek. Zie S. Levin, `New AI can guess whether you're gay or straight from a photograph', The Guardian 8 september 2017.
9. Zie hun website https://www.faception.com/our-technology.
10. J. Poskett, `Django Unchained and the racist science of phrenology', The Guardian 5 februari 2013.
11. `VN: miljoen Oeigoeren vast in Chinese strafkampen', NOS 10 augustus 2018.
12. Zie de API documentatie van Amazon's Rekognition, https://docs.aws.amazon.com/rekognition/latest/dg/API_Emotion.html
13. L. Hardesty, `Study finds gender and skin-type bias in commercial artificial-intelligence systems', MIT News 11 februari 2018.
14. L. Rhue, Racial Influence on Automated Perceptions of Emotions, (Wake Forest University) 9 november 2018.
15. J. Urbi, `Some transgender drivers are being kicked off Uber's app', CNBC 8 augustus 2018.
16. R. Manthorpe en A.J. Martin, `81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says', Sky News 4 juli 2019, zie het rapport hier: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.
17. Zie artikel 27b, vierde lid, Sv juncto artikel 2, onderdeel g, van het Besluit identiteitsvaststelling verdachten en veroordeelden.
18. Zie het Bivv artikel 4 lid 2.
19. Zie het Bivv artikel 4 lid 3.
20. Zie het Bivv art 4 lid 2.
21. Justitiële verkenningen 2011/08, p. 27.
22. Justitiële verkenningen 2011/08, p. 10.
23. R. Kist, `Politiesoftware scant gezichten van verdachten', NRC 19 februari 2018.
24. R. Kist, `Gezichtsherkenning wordt mainstream', NRC 19 februari 2018.
25. W. van Gaal, `Gezichtsherkenning op de Nederlandse straten: moeten we dat willen?' VICE News 18 juli 2019.
26. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p.190-191.
27. Dit recht staat onder andere in artikel 8 van het Europees Verdrag voor de Rechten van de Mens, artikel 7 van het Handvest van de Grondrechten van de Europese Unie, artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten en in artikel 10 van de Grondwet.
28. EHRM 16 december 1992, ECLI:NL:XX:1992:AD1800 (Niemietz), r.o. 31.
29. EHRM 25 september 2001, ECLI:CE:ECHR:2001:0925JUD004478798 (P.G. en J.H. t. Het Verenigd Koninkrijk), r.o. 56-57. Deze paragrafen maken ook duidelijk dat het privacyrecht zich niet alleen uitstrekt tot informatie verkregen via geheime surveillance, maar ook bij `any systematic or permanent record […] even where the information has not been gathered by any intrusive or covert method'.
30. De vereisten voor een beperking van de privacy zijn te vinden in artikel 8 lid 2 EVRM.
31. Zie ook het artikel `Anonimiteit moet een optie blijven', https://www.bitsoffreedom.nl/2019/01/04/anonimiteit-moet-een-optie-blijven/.
32. Dit recht wordt onder andere beschermd door artikel 8 van het Europees Verdrag voor de Rechten van de Mens (dit blijkt uit EHRM 4 december 2008, ECLI:NL:XX:2008:BH1813 (S. en Marper/Verenigd Koninkrijk), r.o. 103, 112, 125 en 126), artikel 8 van het Handvest van de Grondrechten van de Europese Unie en de Algemene Verordening Gegevensbescherming.
33. In de Wpg is de Europese Richtlijn 2016/680 geïmplementeerd. Deze richtlijn regelt de verwerking van politiegegevens door de Nationale Politie, de bijzondere opsporingsdiensten, de Koninklijke Marechaussee en de Rijksrecherche.
34. Zie artikel 5 Wpg.

35. Deze rechten zijn onder andere te vinden in artikel 10 van het Europees Verdrag voor de Rechten van de Mens, artikel 11 van het Handvest van de Grondrechten van de Europese Unie, artikel 19 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten en artikel 7 van de Grondwet.
36. De demonstratievrijheid en de vrijheid van vergadering en vereniging staan onder andere in artikel 11 van het Europees Verdrag voor de Rechten van de Mens, artikel 12 van het Handvest van de Grondrechten van de Europese Unie, artikelen 21 en 22 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten en artikelen 8 en 9 van de Grondwet.
37. EHRM 7 december 1976, ECLI:NL:XX:1976:AC0069 (Handyside), r.o. 49: `[…] it is applicable not only to ``information'' or ``ideas'' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.'
38. Dit grondrecht is onder andere te vinden in artikel 9 van het Europees Verdrag voor de Rechten van de Mens, artikel 10 van het Handvest van de Grondrechten van de Europese Unie, artikel 18 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten en artikel 6 van de Grondwet.
39. Zie artikel 9 lid 2 EVRM.
40. Dit recht is te vinden in artikel 14 van het Europees Verdrag voor de Rechten van de Mens, artikel 21 van het Handvest van de Grondrechten van de Europese Unie, artikel 26 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten en artikel 1 van de Grondwet.
41. Zie artikel 8 lid 2 EVRM, artikel 9 lid 2 EVRM, artikel 10 lid 2 EVRM en artikel 11 lid 2 EVRM.
42. EHRM 26 April 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (The Sunday Times t. Het Verenigd Koninkrijk, No. 1) r.o. 48 en EHRM 25 maart 1983, ECLI:CE:ECHR:1983:0325JUD000594772, (Silver e.a. t. Het Verenigd Koninkrijk), r.o. 85.
43. Zie artikel 8 lid 2 EVRM, artikel 9 lid 2 EVRM, artikel 10 lid 2 EVRM en artikel 11 lid 2 EVRM.
44. EHRM 26 April 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (The Sunday Times t. Het Verenigd Koninkrijk, No. 1) r.o. 47.
45. EHRM 18 mei 2010, ECLI:CE:ECHR:2010:0518JUD002683905 (Kennedy), r.o. 157.
46. EHRM 6 september 1978, ECLI:CE:ECHR:1978:0906JUD000502971 (Klass), r.o. 50.
47. EHRM 2 augustus 1984, ECLI:CE:ECHR:1984:0802JUD000869179 (Malone), r.o. 67.
48. EHRM 18 mei 2010, ECLI:CE:ECHR:2010:0518JUD002683905 (Kennedy), r.o.159 en EHRM 20 juni 2002, ECLI:CE:ECHR:2002:0620JUD005096399 (Al-Nashif), r.o. 121.
49. EHRM 24 april 1990, ECLI:CE:ECHR:1990:0424JUD001180185 (Kruslin en Huvig t. Frankrijk), r.o. 35 en EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (Roman Zakharov), r.o. 231.
50. EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (Roman Zakharov), r.o. 229 en EHRM 12 januari 2016, ECLI:CE:ECHR:2016:0112JUD003713814 (Szabó en Vissy t. Hongarije), r.o. 68.
51. EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (Catt t. Het Verenigd Koninkrijk), r.o. 114.
52. EHRM 6 september 1978, ECLI:CE:ECHR:1978:0906JUD000502971 (Klass), r.o. 49 en EHRM 12 januari 2016, ECLI:CE:ECHR:2016:0112JUD003713814 (Szabó en Vissy t. Hongarije), r.o. 68.
53. Zie artikel 55c lid 2 en 3 Sv.
54. Zie artikel 27 Sv.
55. Th.O.M. Dieben en J. Boksem in: T&C Strafvordering, artikel 27 Sv [Verdachte], aant. 3a.
56. Th.O.M. Dieben en J. Boksem in: T&C Strafvordering, artikel 27 Sv [Verdachte], aant. 5.
57. Zie artikel 55c lid 5 Sv.
58. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 189-190.
59. EHRM 6 september 1978, ECLI:CE:ECHR:1978:0906JUD000502971 (Klass), r.o. 55 en 56.
60. EHRM 28 June 2007, ECLI:CE:ECHR:2007:0628JUD006254000 (Ekimdzhiev t. Bulgarije), r.o. 85.
61. Zie artikel 5 lid 1 jo. artikel 2 onder g Wpg.
62. Aanhangsel Handelingen II 2018/19, nr. 3606, p. 2.
63. Op basis van artikel 33 Wpg.
64. Aanhangsel Handelingen II 2018/19, nr. 3606, p. 3.
65. Zie de beantwoording Kamervragen over het bericht `Gezichtendatabase vanpolitie bevat foto's van 1,3 miljoen mensen' van 30 oktober 2019, kenmerk 2729155.
66. EHRM 22 mei 1990, ECLI:CE:ECHR:1990:0522JUD001103484 (Weber), r.o. 46.
67. A. Nieuwenhuis, `Pressing social need: op zoek naar het dringende karakter van de maatschappelijke behoefte', NTM/NJCM-bull. 2014, nr. 1, p. 22.
68. Zie overeenkomstig EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (Catt t. Het Verenigd Koninkrijk), r.o. 116-124.
69. EHRM 24 januari 2019, ECLI:CE:ECHR:2019:0124JUD004351415 (Catt t. Het Verenigd Koninkrijk), r.o. 124 en Toelichting bij Aanbeveling 87/15 van het Comité van Ministers van de Raad van Europa (17 september 1987), Regulating the use of personal data in the police sector, par 48 (https://rm.coe.int/168062dfd4#_ftn1).
70. EHRM 13 februari 2003, ECLI:CE:ECHR:2003:0213JUD004134098 (Refah Partisi (De Welvaartspartij) e.a. t. Turkije), r.o. 92.
71. EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (Roman Zakharov), r.o. 229.
72. Niet-stelselmatige observatie kan gebaseerd worden op de algemene politietaak in artikel 3 Politiewet, stelselmatige observatie staat in artikel 126g Wetboek van Strafvordering.
73. Kamerstukken II 1996/97, 25 403, nr. 3, p. 26-27.
74. Voor een meer gedetailleerd overzicht, zie B.J. Koops, Criminal investigation and privacy in Dutch law (TILT Law & Technology Working Paper Series), 2016.
75. Zie artikel 126g lid 3 Sv.
76. EHRM 2 september 2010, ECLI:CE:ECHR:2010:0902JUD003562305 (Uzun t. Duitsland), r.o. 52.

77. Zie artikel 126n Wetboek van Strafvordering voor het opvragen van gegevens bij de telecomprovider, artikel 3 Poltiewet of 126g Wetboek van Strafvordering voor de stille sms en de IMSI-catcher (afhankelijk van de mate van intensiteit). Zie voor het gebruik van een IMSI-catcher ook HR 1 juli 2014, ECLI:NL:HR:2014:1562.
78. Deze maatregel wordt gebaseerd op artikel 126nd Wetboek van Strafvordering.
79. Nummerplaatherkenning kan worden gebaseerd op artikel 3 Politiewet. Zie ook Onderzoek naar de verwerking van no-hits bij de inzet van Automatic Number Plate Recognition (rapportage van definitieve bevindingen van het CBP), 11 januari 2010.
80. Zie ook het artikel `Zes kant-en-klare antwoorden op ``Ik heb toch niets te verbergen?''', https://www.bitsoffreedom.nl/bof_tools/niets-te-verbergen/.
81. Zie de laatste zin van artikel 11 lid 2 EVRM, en EHRM 20 november 2018, ECLI:CE:ECHR:2018:1120 JUD004487309 (Ognevenko t. Rusland), r.o. 59.
82. EHRM 12 november 2008, ECLI:CE:ECHR:2008:1112JUD003450397 (Demir en Baykara t. Turkije), r.o. 97.
83. EHRM, 20 mei 1999, ECLI:CE:ECHR:1999:0520JUD002539094 (Rekvényi t. Hongarije), r.o. 59.
84. EHRM 25 april 2019, ECLI:CE:ECHR:2019:0425JUD003646908 (Ter-Petrosyan t. Armenië), r.o. 59 en EHRM 26 april 1991, ECLI:CE:ECHR:1991:0426JUD001180085 (Ezelin t. Frankrijk), r.o. 39.
85. EHRM 3 mei 2007, ECLI:CE:ECHR:2007:0503JUD000154306 (Baczkowksi e.a. t. Polen), r.o. 67-68.
86. Zie artikel 1 sub s Wpg.
87. Zie artikel 5 Wpg.
88. Zie artikel 3 sub 2 Wpg.
89. Zie artikel 6b Wpg.
90. EHRM 23 juli 1968, Series A, vol. 6, p. 34 (Belgische taal).
91. EHRM 23 maart 2017, ECLI:CE:ECHR:2017:1214JUD005975213 (Wolter en Sarfert t. Duitsland), r.o. 62.
92. EHRM, 10 mei 2001, ECLI:CE:ECHR:2001:0510JUD002578194 (Cyprus t. Turkije), r.o. 306.
93. W. Landman en L. Kleijer-Kool, Een onderzoek naar proactief politieoptreden (Politie & Wetenschap, Apeldoorn; Twynstra Gudde, Amersfoort), 2016.
94. J. Vincent, `Transgender YouTubers had their videos grabbed to train facial recognition software', The Verge 22 augustus 2017.
95. Z. Samudzi, `Bots Are Terrible at Recognizing Black Faces. Let's Keep it That Way.', The Daily Beast 11 februari 2019.
96. W. Wiewiórowski, `Facial recognition: A solution in search of a problem?', European Data Protection Supervisor 28 oktober 2019.
97. Zie ook het artikel van Hans de Zwart, `Draconisch terreurbeleid maakt ons tot bange, geïsoleerde mensen', NRC 14 juli 2017.
98. Zie ook het boek van de Noorse filosoof Lars Svendsen, `A Philosophy of Fear' (P.D. Smith, `Review: A Philosophy of Fear', The Guardian 25 oktober 2008).
99. E. Selinger en W. Hartzog, `What happens when employers can read your facial expressions?', The New York Times 17 oktober 2019.

**Bits of Freedom komt op voor jouw vrijheid en privacy op internet.**
Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internetverkeer wordt afgeknepen en geblokkeerd.

Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.

Bits of Freedom
www.bitsoffreedom.nl
@bitsoffreedom
Prinseneiland 97HS
1013 LN Amsterdam

Contactpersoon:
Hans de Zwart
+31 6 2185 6845
hans@bitsoffreedom.nl

5BFC B00B 309E 8FEC 7F25
B4A7 4819 A622 ACFC E9C4
(bitsoffreedom.nl/openpgp)

# BITS OF FREEDOM

Voor jouw internetvrijheid