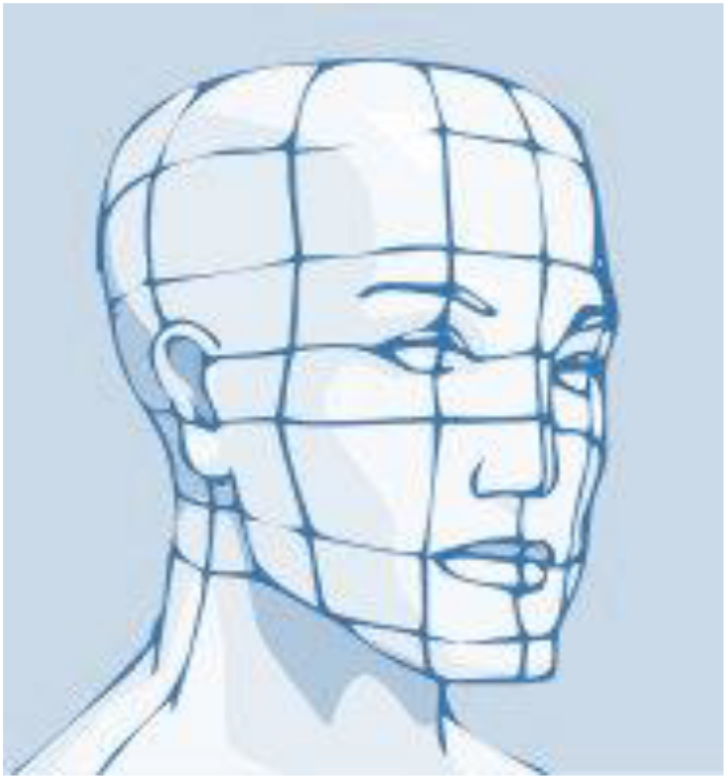


GEAUTOMATISEERDE GELAATSHERKENNING EN ZIJN FACETTEN

Master Thesis: Een onderzoek naar geautomatiseerde gelaatsherkenning als preventie- en opsporingsmiddel van veelvoorkomende criminaliteit in winkelcentra in Nederland

Auteur	Angela de Ridder
Studentnummer	2559846
Opleiding	Master Opsporingscriminologie
Onderwijsinstelling	Vrije Universiteit Amsterdam

Datum	25 januari 2019
Begeleider VU	10 2 e
Begeleiders stage	10 2 e

VU VRIJE UNIVERSITEIT AMSTERDAM

POLITIE

GEAUTOMATISEERDE GELAATSHERKENNING EN ZIJN FACETTEN

Een onderzoek naar geautomatiseerde gelaatsherkenning als preventiemiddel van veelvoorkomende criminaliteit in winkelcentra in Nederland

Naam student: Angela de Ridder
Studentnummer: 2559846
Email: 10.2.g @student.vu.nl

Opleiding: Master Opsporingscriminologie (voltijd)
Faculteit: Faculteit der Rechtsgeleerdheid
Onderwijsinstelling: Vrij Universiteit, Amsterdam
Stag instelling: Politie Driebergen, Programma Sensing
Studiejaar: 2017/2018

Plaats en datum:
Begeleider: 10.2.e
Begeleider op locatie: 10.2.e

Aantal woorden: 25.804

VOORWOORD

Voor u ligt de scriptie ‘Geautomatiseerde gelaatsherkenning en zijn facetten’. Het onderzoek voor deze scriptie is uitgevoerd binnen het Programma Sensing van de Nationale Politie. Deze scriptie is geschreven in het kader van mijn afstuderen aan de Master Opsporingscriminologie aan de Vrije Universiteit te Amsterdam. Het onderzoek is geschreven in opdracht van het Programma Sensing waarbinnen ik in de maanden april tot en met december 2018 stage heb gelopen.

Samen met mijn stagebegeleiders, 10.2.e , is het onderwerp voor deze scriptie bedacht. Vanuit het Programma Sensing is het de wens om nieuwe sensoren in te zetten op bestaande vraagstukken. Hier vandaan is ervoor gekozen om onderzoek te doen naar de mogelijkheden van het inzetten van geautomatiseerde gelaatsherkenning als preventiemiddel en opsporingsmiddel voor veel voorkomende criminaliteit in winkelcentra in Nederland. Tijdens het schrijven van dit onderzoek stonden mijn begeleiders op stage en vanuit mijn opleiding voor mij klaar om mijn vragen te beantwoorden en te helpen bij de vragen die ik had omtrent het schrijven van een kwalitatief onderzoek.

Bij deze wil ik graag mijn begeleiders binnen het Programma Sensing bedanken voor hun hulp bij het uitvoeren van dit onderzoek. Daarnaast wil ik mijn begeleider vanuit mijn opleiding bedanken voor het beantwoorden van mijn vragen omtrent het schrijven van een kwalitatief onderzoek. Tevens wil ik de respondenten bedanken die mee hebben gewerkt aan dit onderzoek en tijd hebben genomen om mijn vragen te beantwoorden.

Ik wens u veel leesplezier toe.

Angela de Ridder

Noordwijk, 28 december 2018

SAMENVATTING

Geautomatiseerde gelaatsherkenning is een techniek dat steeds vaker terug te zien is in het dagelijks leven. Zo is het tegenwoordig mogelijk om je telefoon te ontgrendelen door middel van het herkennen van je gezicht, wordt het gebruikt op vliegvelden en wordt het toegepast door organisaties zoals de politie en het Nederlands Forensisch instituut. Vanuit het Programma Sensing wordt er onderzoek gedaan naar de mogelijkheden van nieuwe sensoren en technologieën wanneer het gaat om het aanpakken van veiligheidsproblemen.

Het doel van dit onderzoek is om te achterhalen welke mogelijkheden en beperkingen er op technisch, juridisch en ethisch gebied zijn wanneer het gaat om het inzetten van geautomatiseerde gelaatsherkenning als preventiemiddel en opsporingsmiddel voor veel voorkomende criminaliteit in winkelcentra in Nederland. Hiervoor is de volgende onderzoeksvraag opgesteld: *'Wat zijn de mogelijkheden en beperkingen van het inzetten van geautomatiseerde gelaatsherkenning op basis van sensoren als preventie- en opsporingsmiddel voor veelvoorkomende criminaliteit in winkelcentra in Nederland door zowel private als publieke partijen?'* Geautomatiseerde gelaatsherkenning is hierbij een technologie dat toegepast wordt op bestaande sensoren, zoals bewakingscamera's. Door middel van deze technologie is het mogelijk om gezichten van voorbijgangers te herkennen als gezichten die opgeslagen staan in een database.

Om een antwoord te kunnen geven op de onderzoeksvraag is er onder andere gebruik gemaakt van een literatuurstudie. Aan de hand hiervan is inzicht verkregen in de technische mogelijkheden en beperkingen. Daarnaast is gebruik gemaakt van de wetgeving in Nederland en de ondersteuning van privacyjuristen. Op deze manier zijn de mogelijkheden en beperkingen, op juridisch gebied, inzichtelijk gemaakt. Ten slotte de ethische aspecten van het inzetten van geautomatiseerde gelaatsherkenning onderzocht op basis van inerviews, afgenomen bij de medewerkers van het Programma Sensing en een verkenning van de literatuur. Dit resulteerde in een aantal ethische factoren waarbij rekening gehouden moet worden wanneer geautomatiseerde gelaatsherkenning toepast wordt door de politie of door private partijen.

Uit de resultaten is gebleken dat er zowel mogelijkheden als beperkingen zijn wanneer het gaat om het inzetten van geautomatiseerde gelaatsherkenning. Vooral op juridisch vlak hangen de mogelijkheden af van de omstandigheden van het geval. Zo is het inzetten van gelaatsherkenning een mogelijkheid maar dit hangt af van een aantal factoren zoals ernst van het delict, grootte van het probleem, aanhoudendheid van het probleem, inbreuk op de persoonlijke levenssfeer enzovoort. Bij de techniek is er nog winst te behalen bij het inzetten van geautomatiseerde gelaatsherkenning op grotere groepen mensen. Voor alsnog is geautomatiseerde gelaatsherkenning vooral mogelijk op stilstaande beelden. Het inzetten van geautomatiseerde gelaatsherkenning op grote hoeveelheden mensen en live beelden is technisch gezien nog lastig. Vanuit ethisch oogpunt zijn er een aantal punten waarmee rekening gehouden dient te worden wil gelaatsherkenning door politie of private partijen worden ingezet. Een belangrijk punt dat uit de interviews

naar voren komt is de inbreuk op privacy. Daarnaast is er veel onduidelijkheid omtrent het omgaan met de informatie die geautomatiseerde gelaatsherkenning verschaft. Er zijn veel onduidelijkheden, voor zowel de gebruiker van het geautomatiseerde gelaatsherkenningssysteem als de burger die hiermee te maken krijgt, met betrekking tot wie de gegevens mag gebruiken, inzien en hoe de controle hierop dient te gebeuren.

Op basis van de onderzoeksresultaten kan worden aanbevolen dat vervolgonderzoek naar technisch, wetgeving en ethiek nodig is wil geautomatiseerde gelaatsherkenning toegepast kunnen worden ten behoeve van de preventie en opsporing van veel voorkomende criminaliteit. Daarnaast kan de politieorganisatie zich afvragen of ze geautomatiseerde gelaatsherkenning ook daadwerkelijk willen toepassen wanneer dit mogelijk blijkt te zijn. Hierbij spelen vragen omtrent de acceptatie van burgers en de wenselijkheid en noodzakelijkheid van het inzetten van het systeem een rol.

INHOUD

FIGUREN & TABELLEN

AFKORTINGEN

AVG	Algemene Verordening Gegevensbescherming
BVH	Basisvoorziening handhaving
CATCH	Centrale Automatische TeChnologie voor Herkenning van personen
DB&B	Dienst Bewaken en Beveiligen
EVRM	Europees verdrag tot bescherming van de rechten van de mens
HKS	Herkenningsdienstsystemen
NFI	Nederland Forensisch Instituut
NIST	National Institute of Standards and Technology
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
VVC	Veel voorkomende criminaliteit
WPG	Wet Politiegegevens
SV	Wetboek van Strafvordering

1. INLEIDING

Veel mensen zijn bekend met de beelden van CSI. Verdachten worden opgepakt omdat hun gezicht te zien is op een camera en deze meteen gelinkt is aan het politiesysteem. De politie krijgt een hit en agenten worden zo snel mogelijk op de persoon in kwestie afgestuurd. Maar is deze manier van handelen ook daadwerkelijk mogelijk? Het lijkt allemaal eenvoudig maar niets is minder waar.

Het koppelen van gezichten aan camerabeelden is nog niet zo vanzelfsprekend, toch is dit een onderwerp dat binnen het Programma Sensing en in de media terugkeert. Zo maakt de politie als organisatie sinds 2016 gebruik van een geautomatiseerde gelaatsherkenningssysteem dat gebruik maakt van de database Centrale Automatische TeChnologie voor Herkenning van personen [CATCH]. In deze database zitten de gegevens van Vreemdelingen en Verdachten en Veroordeelden opgeslagen (Politie, z.j., *Systeem voor geautomatiseerde gelaatsherkenning operationeel*; Politie, 2017[1]).

Maar wat houdt geautomatiseerde gelaatsherkenning precies in? Welke aspecten komen hierbij kijken? De politie mag niet zomaar een nieuwe sensortechnologie grootschalig toepassen, zij moet hierbij rekening houden met onder andere juridische en ethische dilemma's die hierbij komen kijken (Tweede Kamer, 2015[2]). Dit zijn aspecten waar het Programma Sensing, binnen de National Politie, zich mee bezig houdt. Het Programma Sensing richt zicht de komende jaren op het toepassen van sensortechnologie, zoals geautomatiseerde gelaatsherkenning, door de Nationale Politie. Omdat er de afgelopen jaren een toenemend besef is ontstaan dat sensortechnologie ondersteunend kan zijn in het politiewerk is het Programma Sensing opgericht. Naast ethische en juridische dilemma's houdt het Programma Sensing zich onder andere bezig met de effectiviteit van de sensoren, de ontwikkeling van sensortoepassingen en mogelijke samenwerkingsverbanden wanneer het gaat om het delen van sensorinformatie tussen publieke en private partijen.

Binnen het Programma Sensing is een van de nieuwere ontwikkelingen die onderzocht dient te worden; geautomatiseerde gelaatsherkenning. Dit is de opdracht voor dit onderzoek. De vraag hierbij is of geautomatiseerde gelaatsherkenning toegepast kan worden op een van de veiligheidsvraagstukken waar de politie mee kampt en in hoeverre geautomatiseerde gelaatsherkenning hierbij een verantwoorde keuze is en of de politie wel de aangewezen instantie is die een bepaalde technologie dient toe te passen (Programma Sensing[3]). Dit onderzoek wordt gedaan binnen de werkomgeving van de medewerkers van het Programma Sensing; namelijk Villa B. Villa B is een omgeving waar sensoren, indien deze nog niet grootschalig toegepast mogen worden, kunnen worden getest. De medewerkers van het Programma Sensing zijn allen in dienst van de politie.

---

[1] Bron afkomstig van het Landelijk Forensisch Service Centrum (niet publiek toegankelijk).
[2] T.K. waarnemen met technische hulpmiddelen; T.K. bijlage beleidsvisie 2015
[3] Bron afkomstig van het Programma Sensing (niet publiek toegankelijk).

1.1. Veiligheidsvraagstuk en maatschappelijke relevantie

Het veiligheidsvraagstuk, dat vanuit het Programma Sensing als opdracht is gegeven om onderzocht te worden, hangt samen met de maatschappelijke relevantie van dit onderzoek. Op de site van het CBS wordt duidelijk dat criminaliteit in winkelcentra nog steeds plaatsvindt. Zo is onder andere mobiel banditisme, waarbij bendes delicten plegen zoals zakkenrollerij en winkeldiefstal, een probleem in Nederland (Politie, z.j., *Mobiel banditisme*). Uit cijfers van het CBS blijkt dat het aantal meldingen voor delicten zoals zakkenrollerij, fietsendiefstal en vandalisme is afgenomen, echter blijkt ook dat er nog regelmatig melding van deze delicten wordt gemaakt (Akkermans, 2016; Eggen & Goudriaan, 2010). Veelvoorkomende criminaliteit [VVC] zoals bovengenoemde, kunnen de onveiligheidsgevoelens van burgers bevorderen (Muller, Van der Leun, Moerings & Van Calster, 2010). Het is dan ook belangrijk om deze vormen van criminaliteit zo veel mogelijk terug te dringen, hierdoor kan het veiligheidsgevoel van burgers en het vertrouwen van hen in de politie worden vergroot. Dit is van belang omdat het kan bijdragen aan een betere en effectievere samenwerking tussen politie en burger. Samenwerking van politie en burger leidt tot het vergroten van het vertrouwen van samenleving en het vergroten van het veiligheidsgevoel (Nationale Politie, 2012). Een mogelijk middel om deze vormen van criminaliteit terug te kunnen dringen, zou volgens Programma Sensing, geautomatiseerde gelaatsherkenning zijn. Dit is dan ook de reden dat geautomatiseerde gelaatsherkenning, en de mogelijkheid om dit middel in te zetten bij veelvoorkomende criminaliteit in winkelcentra, onderzocht wordt in dit onderzoek.

1.2. Wetenschappelijke relevantie

Voordat de politie sensoren, zoals een camera met geautomatiseerde gelaatsherkenning, inzet als hulpmiddel in haar dagelijkse bezigheden, zoals de opsporing van strafbare feiten en het vinden van de dader, is het van belang dat hierbij eerst alle mogelijkheden en beperkingen van de sensor worden onderzocht en in kaart worden gebracht (Tweede Kamer, 2015). Dit omdat het belangrijk is dat technische mogelijkheden en beperkingen worden onderzocht wil de sensor naar behoren kunnen werken. Daarnaast is het van belang dat de sensor volgens de wetgeving in Nederland wordt toegepast zodat het verkregen bewijsmateriaal rechtmatig is en er geen rechten van burgers worden overschreden. Ook is het van belang dat de sensor geen negatieve maatschappelijke reactie oproept waardoor het juist de onveiligheidgevoelens van burgers kan vergroten. Bij het in kaart brengen van de mogelijkheden en beperkingen van het gebruik van de sensor kan dan ook gedacht worden aan de huidige wetgeving en inzetkaders[4] voor de sensor, technische aspecten en ethische kwesties. Voor burgers en voor de politie is het belangrijk om te weten wanneer een sensor wel kan worden toegepast en wanneer dit juridisch, bijvoorbeeld door

[4] Met inzetkaders wordt bedoeld dat er een duidelijk kader gevormd dient te worden zodat zowel de politie als de burger weet wanneer en onder welke omstandigheden geautomatiseerde gelaatsherkenning toegepast mag worden en wanneer dit niet het geval is.

privacywetgeving, niet mogelijk is. Het is belangrijk dat de sensoren ook daadwerkelijk meten wat deze beogen te meten en de vooropgestelde doelen nastreven. Daarnaast moet er rekening gehouden worden met aspecten zoals de rechten van de burgers, de effecten op burgers, effecten op de politie zelf etc. Wanneer dit instrument meteen wordt ingezet zonder dat hier voorafgaand onderzoek naar wordt gedaan komen al deze vragen pas achteraf in de keten aan bod terwijl het voor de effectiviteit van het gebruik van de sensor van belang is dat deze aspecten eerst belicht worden. Wanneer achteraf blijkt dat de sensor geen bruikbare informatie oplevert, niet werkt, eenvoudig te verstoren is enzovoort, is dit zowel een verspilling van geld en van tijd geweest. Het gaat daarnaast niet alleen om het kunnen en mogen inzetten van een sensor, het is ook belangrijk dat we dit willen. Voor de politie is het, bij de uitvoering van haar politietaak, van belang dat de burgers meewerken en vertrouwen in haar heeft (Nationale Politie, 2012).

Omdat geautomatiseerde gelaatsherkenning steeds vaker voorkomt, denk hierbij aan de grenscontrole bij Schiphol, is het denkbaar dat geautomatiseerde gelaatsherkenning ook voor andere doeleinden gebruikt kan worden. Geautomatiseerde gelaatsherkenning wordt al veel gebruikt met stilstaande beelden. Er is echter nog weinig onderzoek gedaan naar de mogelijkheden van geautomatiseerde gelaatsherkenning bij live beelden. De wetenschappelijke relevantie hier ligt dan ook in het gegeven dat er nog geen duidelijke kaders zijn met betrekking tot het inzetten van geautomatiseerde gelaatsherkenning op straat en op massa's bewegende mensen. Dit kan mogelijkheden bieden voor de politie bij het ondersteunen van de opsporing en preventie van misdrijven en het kan ook bijdragen aan de veiligheid van de samenleving.

Kortom, het is belangrijk dat voordat een sensor wordt ingezet in de praktijk, er eerst wordt gekeken naar de mogelijkheden en beperkingen van het gebruik van deze sensor. Het gebruik van de sensor berust dan ook allereerst op wetenschappelijke kennis over de mogelijkheden die de sensor te bieden heeft en over de effecten van de sensor op haar omgeving.

1.3. Doel- en vraagstelling

Dit onderzoek geeft inzicht in de mogelijkheden en beperkingen wanneer het gaat om het inzetten van gelaatsherkenningssoftware bij het tegengaan en opsporen van veelvoorkomende criminaliteit in winkelcentra in Nederland. Omdat er bij het inzetten van sensoren onder andere rekening gehouden dient te worden met de wet (Tweede Kamer, 2015) is het van belang om een beschrijving te geven van scenario's waarin geautomatiseerde gelaatsherkenning toegepast kan worden. Op deze manier kan inzichtelijk worden gemaakt onder welke omstandigheden geautomatiseerde gelaatsherkenning, volgens de regels van de wet, wel mag worden toegepast en onder welke niet. Het doel van dit onderzoek is om een verkenning uit te voeren met betrekking tot de mogelijkheden, wanneer het gaat om het gebruiken van deze sensortechnologie in het politiewerk. Door onderzoek te doen naar de ethische dilemma's, juridische factoren en technische mogelijkheden kunnen nieuwe inzichten worden verkregen die bruikbaar zijn bij het

voorkomen en opsporen van veelvoorkomende criminaliteit in winkelcentra. Dit kan wellicht zorgen dat de aanpak van deze criminaliteit verbetert en de criminaliteit afneemt.

Het idee dat geautomatiseerde gelaatsherkenning kan bijdragen aan het vergroten en verbeteren van de preventie en opsporing van veelvoorkomende criminaliteit in winkelcentra berust op een aantal criminologische theorieën. De theorieën die het uitgangspunt zijn bij deze masterthesis en welke verder worden toegelicht in het volgende hoofdstuk, zijn de routine activiteitentheorie, afschrikkingstheorie en rationele keuzetheorie. Deze kunnen dan ook als handvat worden gezien wanneer het gaat om de keuze van het inzetten van geautomatiseerde gelaatsherkenning als preventie- en opsporingsmiddel voor veelvoorkomende criminaliteit.

Binnen het thema geautomatiseerde gelaatsherkenning wordt er in dit onderzoek ingezoomd op de verschillende facetten die het inzetten van een sensor, voor nieuwe doeleinden, met zich meebrengt. Juridische, ethische en technische aspecten spelen een rol. Sensoren onderzoeken vanuit ethische invalshoeken en vanuit juridisch oogpunt kan bijdragen aan het debat bij het wel of niet willen inzetten van een nieuwe sensortechniek in het politiewerk (Tweede Kamer, 2015).

Ook de ontwikkelingen die in het buitenland plaatsvinden omtrent geautomatiseerde gelaatsherkenning zijn belangrijk. Deze zouden namelijk aanknopingspunten kunnen bieden wanneer het gaat om de verschillende mogelijkheden en verbeteringen omtrent geautomatiseerde gelaatsherkenningssystemen.

Dit onderzoek beschrijft dan ook welke mogelijkheden er zijn met betrekking tot het inzetten van geautomatiseerde gelaatsherkenningssystemen en aan welk inzetkader er gedacht dient te worden. Daarnaast spelen de beperkingen een belangrijke rol voor vervolgonderzoek. De onderzoeksvraag die in deze thesis centraal staat is dan ook als volgt:

'Wat zijn de mogelijkheden en beperkingen van het inzetten van geautomatiseerde gelaatsherkenning op basis van sensoren als preventie- en opsporingsmiddel voor veelvoorkomende criminaliteit in winkelcentra in Nederland door zowel private als publieke partijen?'

Om de onderzoeksvraag te beantwoorden zijn er een aantal deelvragen geformuleerd. De antwoorden op deze deelvragen vormen het antwoord op de onderzoeksvraag. De deelvragen zijn als volgt:

- Welke mogelijkheden en beperkingen zijn er met betrekking tot de wetgeving in Nederland voor het inzetten van geautomatiseerde gelaatsherkenning bij de preventie en opsporing van veel voorkomende criminaliteit in winkelcentra?
- Met welke ethische vraagstukken dient rekening gehouden te worden met het inzetten van geautomatiseerde gelaatsherkenning als preventie- en opsporingsmiddel?
- Hoe denken de medewerkers van het Programma Sensing in Villa B over het toepassen van geautomatiseerde gelaatsherkenning in verschillende gevallen?

- Welke mogelijkheden en beperkingen zijn er op technisch gebied wanneer het gaat om geautomatiseerde gelaatsherkenning?
- Op wat voor manieren wordt geautomatiseerde gelaatsherkenning toegepast in zowel het binnen- als buitenland?

1.4. Type onderzoek

Dit onderzoek betreft een beschrijvend en exploratief onderzoek. De onderzoeksvraag en de deelvragen die in deze thesis centraal staan worden beantwoord aan de hand van een systematisch literatuuronderzoek, een test met een geautomatiseerd gelaatsherkenningssysteem in Villa B en interviews met professionals.

1.5. Leeswijzer

Om de onderzoeksvraag te kunnen bewoorden zal er allereerst in het volgende hoofdstuk een theoretisch kader worden gevormd. Hierin zullen de belangrijkste theoretische concepten worden gedefinieerd en zullen de onder 1.3 genoemde theorieën worden beschreven. Daarnaast zal er worden ingegaan op de begrippen sensoren, geautomatiseerde gelaatsherkenning, biometrie en veelvoorkomende criminaliteit. Het derde hoofdstuk beschrijft de onderzoeksmethoden die in dit onderzoek worden gebruikt. Dit hoofdstuk bevat tevens de verschillende scenario's die behandeld worden met betrekking tot geautomatiseerde gelaatsherkenning. Aan de hand van deze scenario's kunnen de mogelijkheden en beperkingen worden besproken wanneer het gaat om de mogelijkheden op juridisch gebied bij het inzetten van geautomatiseerde gelaatsherkenning. Vervolgens volgen de resultaten, in hoofdstuk 4 tot en met 7, die zijn verkregen door het systematische literatuuronderzoek, de interviews met professionals (medewerkers Villa B) en de resultaten die verkregen zijn uit het geautomatiseerde gelaatsherkenningssysteem dat geplaatst is in Villa B. Er wordt in deze hoofdstukken antwoord gegeven op de deelvragen die in dit onderzoek worden behandeld. Het achtste hoofdstuk omvat de conclusie en geeft een antwoord op de onderzoeksvraag en de deelvragen. Tevens bevat dit hoofdstuk de aanbevelingen voor vervolgonderzoek en de discussie.

2. THEORETISCH KADER

In het eerste deel van het theoretisch kader worden de verschillende criminologische theorieën besproken die een uitgangspunt kunnen bieden bij het kiezen van een nieuwe techniek, zoals geautomatiseerde gelaatsherkenning, voor de opsporing en preventie van delicten. Hierbij wordt het inzetten van geautomatiseerde gelaatsherkenning allereerst besproken vanuit de routine activiteitentheorie van Cohen en Felson. Vervolgens worden de afschrikkingstheorie en rationele keuzetheorie besproken.

In het tweede deel van het theoretisch kader wordt er ingegaan op verschillende begrippen die van belang zijn in dit onderzoek. Allereerst zal het begrip 'veelvoorkomende criminaliteit in winkelcentra' worden toegelicht. Op deze manier zal duidelijk worden om welke vormen van criminaliteit het in deze thesis gaat. Vervolgens zal het begrip 'sensoren' omschreven worden om een duidelijk beeld te verschaffen van wat sensoren eigenlijk zijn en wat de politie hieronder verstaat. Hierna wordt er gekeken naar de begrippen geautomatiseerde gelaatsherkenning en biometrie. Er zal ingezoomd worden op wat geautomatiseerde gelaatsherkenning precies inhoudt en welke rol biometrie hierbinnen speelt. Tevens wordt er in deze paragraaf besproken welke vormen van geautomatiseerde gelaatsherkenning er worden gebruikt door de politie in Nederland. Ten slotte volgen de verschillende toepassingsvormen van geautomatiseerde gelaatsherkenning in zowel het binnen- als buitenland. Aan de hand hiervan kan er een antwoord worden geformuleerd op de laatste deelvraag van dit onderzoek.

2.1. Routine activiteitentheorie

Het idee dat geautomatiseerde gelaatsherkenning kan bijdragen aan effectieve opsporing en wellicht aan het voorkomen van (nieuwe) delicten berust onder andere op de routine activiteitentheorie van Cohen en Felson. De routine activiteitentheorie stelt dat criminaliteit ontstaat wanneer er sprake is van het samenkomen van een drietal factoren in tijd en plaats: een geschikt doelwit, een gemotiveerde dader en een gebrek aan adequaat toezicht (Cohen & Felson, 1979). Wanneer er sprake is van alle drie deze factoren is de kans op criminaliteit het grootst. Een doelwit betreft hierbij niet alleen een persoon maar kan ook een object of plaats zijn.

Cohen en Felson (1979) benoemen dat wanneer de controle toeneemt, de kans op criminaliteit afneemt. Dit komt doordat er dan niet langer sprake is van een gebrek aan bewaking, een van de drie bovengenoemde factoren. Ook bewaking behoeft niet alleen door personen te gebeuren. Ook objecten die criminaliteit ontmoedigen, zoals een bewakingscamera, kunnen beschouwd worden als een vorm van toezicht. Daarnaast blijkt dat wanneer er zich meer potentiële daders en onbeschermde doelwitten op dezelfde tijd en plaats begeven de criminaliteit toeneemt (Sajtos, 2009). Dit geldt dan ook bijvoorbeeld in een winkelcentrum. In winkelcentra zijn namelijk veel onbeschermde doelwitten, denk hierbij aan winkels en het publiek dat de winkels bezoekt. Daarnaast zijn er vaak potentiële daders en bieden winkelcentra gelegenheid tot criminaliteit (Muller et. al., 2010).

Het voorbeeld dat wordt gebruikt om de theorie van Cohen en Felson nader uit te leggen is dat van woninginbraak. Dit voorbeeld kan ook toegepast worden op een winkelcentrum of haar winkels. Bij woningen zou de afwezigheid van zijn bewoners de kans op woninginbraak doen vergroten. Hiermee wordt gedoeld op de afwezigheid van controle (Sajtos, 2009; Vaane, 2014). Wanneer dit toegepast wordt op een winkelcentrum of een winkel zou de afwezigheid van bewaking of controle kunnen leiden tot een grotere kans op delicten, zoals winkeldiefstal.

Vanuit de routine activiteiten theorie kan beargumenteerd worden dat het inzetten van sensoren zoals geautomatiseerde gelaatsherkenning, en dus het vergroten van controle, een preventieve werking kan hebben als het gaat om het voorkomen van criminaliteit zoals zakkenrollerij en winkeldiefstal. Hierbij wordt namelijk een van de drie factoren, die volgens Cohen en Felson, een verklaring bieden voor het ontstaan van criminaliteit, weggenomen.

2.2. Afschrikkingstheorieën en Rationele keuze

Ook de afschrikkingstheorieën, waarvan de oorspronkelijke gedachtegang afkomstig is van Bentham en Beccaria (18e eeuw) kunnen een uitleg geven bij de keuze voor het inzetten van geautomatiseerde gelaatsherkenning als opsporings- en preventiemiddel (Pauwels, 2015). Vanuit de afschrikkingstheorieën wordt er verondersteld dat menselijk gedrag beïnvloed kan worden door straffen of door de kans op bestraffing. Dit wijst erop dat wanneer controle toeneemt de pakkans ook vergroot wordt, dit zou volgens de theorie een vermindering in delicten teweeg kunnen brengen (Burns & Hart, 1996). Bentham en Beccaria maken een onderscheid tussen een objectieve en een subjectieve pakkans. De objectieve pakkans is de daadwerkelijk kans van betrapping terwijl de subjectieve pakkans de inschatting van de crimineel in kwestie is. Een preventief effect kan hier optreden wanneer de subjectieve pakkans en de zekerheid van bestraffing groter zijn en wanneer de straf sneller volgt op een overtreding. Wanneer de crimineel de subjectieve pakkans hoger achter dan de baten van het delict zal de crimineel sneller afzien van het begaan van het feit. Op deze manier werkt de subjectieve kans op bestraffing als afschrikkingsmiddel (Bentham & Beccaria in Goldenbeld, Morsink, Dragutinovic & Scheper, 2006, p. 7). Dit zijn allemaal factoren die met een geautomatiseerde gelaatsherkenningssysteem een rol spelen. Zo is er hierdoor meer controle waardoor de subjectieve pakkans, en in het geval van herkenning ook de objectieve pakkans, en de kans op bestraffing worden vergroot. Dit kan een preventieve werking met zich teweegbrengen.

De afschrikkingstheorieën zeggen niets over de besluitvorming van betrokkenen. Daarom hangen deze vaak samen met de rationele keuzetheorie van Cornish en Clarke (1989) (Beyens, 2007). Deze theorie verklaart dat misdrijven worden gepleegd naar aanleiding van de keuzen en gedragingen van daders. Er wordt een kosten- en batenanalyse gedaan waarbij een misdrijf wordt gepleegd wanneer de verwachte baten hoger zijn dan de kosten. Een dader streeft naar maximale baten bij minimale kosten. De verhouding tussen de kosten en baten bij elke handeling bepaald de uiteindelijke handeling van de dader. Bepaalde interventies kunnen de verwachte kosten van doelwitten verhogen, bijvoorbeeld wanneer de dader de

pakkans hoger acht. Wanneer de dreiging van een bepaalde interventie hoger is dan de baten dan zal criminaliteit verminderen. Daders zullen dan sneller geneigd zijn hun criminele activiteiten elders voort te zetten, op een plaats waar de kosten minder hoog zijn (Muller et. al., 2010). Ook deze theorie zou de keuze voor het inzetten van geautomatiseerde gelaatsherkenningssystemen als preventiemiddel kunnen ondersteunen. Geautomatiseerde gelaatsherkenning zou er namelijk voor kunnen zorgen dat zowel de subjectieve als de objectieve pakkans groter zijn, dit zou de keuze van de dader bij het wel of niet plegen van het delict, kunnen beïnvloeden.

2.3. Belangrijke begrippen

In deze paragraaf zullen er een aantal begrippen worden verduidelijkt welke van belang zijn voor het beantwoorden van de onderzoeksvraag. Allereerst wordt het begrip veelvoorkomende criminaliteit nader toegelicht. Vervolgens wordt er gekeken naar wat er onder het begrip sensoren wordt verstaan. Ten slotte worden de begrippen geautomatiseerde gelaatherkenning en biometrie besproken.

2.3.1. Veelvoorkomende criminaliteit

Veelvoorkomende criminaliteit, ook wel ‘kleine criminaliteit’, is een verzamelnaam voor strafbaar gedrag dat op grote schaal voorkomt. Vanwege deze massaliteit is het hinderlijk en bevordert het de onveiligheidsgevoelens van burgers. Bij veelvoorkomende criminaliteit gaat het vooral om geweld in de publieke ruimte, vernielingen en diefstal. Enkele voorbeelden zijn autodiefstal, zakkenrollerij, vernielingen, vandalisme, inbraak, fietsdiefstal, mishandeling en bedreiging. Veel voorkomende criminaliteit speelt zich vaak af in de publieke ruimte en draagt bij aan de onveiligheidsgevoelens van burgers (Van den Brandhof, 2007). Voorbeelden van veelvoorkomende criminaliteit in de publieke ruimte, zoals winkelcentra zijn, vernieling (van zowel de winkels zelf als de omgeving), winkeldiefstal, zakkenrollerij of diefstal van tas/portemonnee, fietsendiefstal en inbraak (Colder & Nuijten-Edelbroek, 1988).

2.3.2. Sensoren

Sensoren kunnen ook wel gezien worden als het verlengde van de menselijke zintuigen. Het zijn technische hulpmiddelen die bijvoorbeeld in staat zijn om geluiden, beelden, geuren, temperatuur en bewegingen te herkennen. Dit kan zowel gedaan worden door een sensor, zoals een camera, of een software die werkt in combinatie met de sensor, zoals geautomatiseerde gelaatsherkenning. Sensoren verzamelen informatie die niet direct binnen handbereik van de agent ligt. Hierbij kan gedacht worden aan camerabeelden welke de route van een verdachte in kaart brengen of Automatic Number Plate Recognition waarbij een kenteken gelinkt wordt aan een bepaald voertuig of persoon. De politie gebruikt sensoren ter ondersteuning van de

politietaak. Het menselijk waarnemen wordt door middel van sensoren ondersteund en versterkt wat de politie helpt bij de preventie en opsporing (Custers & Vergouw, 2015; Engberts & Copini, 2016; Programma Sensing, 2017[5]; Technologiescan, 2017[6]). Sensing gaat dan ook om het waarnemen en verzamelen van informatie, dat betrekking heeft op een object of persoon, met betrekking tot een sensor. Het gaat dan ook om het doen van een waarneming met behulp van sensoren (Engberts & Copini, 2016; Programma Sensing, 2017). Voorbeelden van sensoren zijn camera's, weegplaten, laserguns bij verkeerscontroles, warmtesensoren bij helikopster etc. (Custers & Vergouw, 2015; Engberts & Copini, 2016; Technologiescan, 2017).

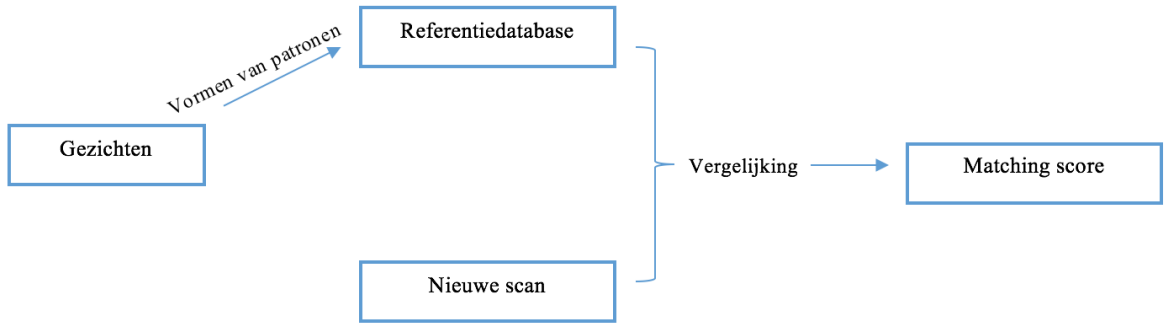
2.3.3. Geautomatiseerde gelaatsherkenning en biometrie

Om te begrijpen hoe geautomatiseerde gelaatsherkenning, ook wel gezichtsherkenning of gezichtsvergelijking genoemd, precies werkt is het van belang om kennis te nemen van het begrip biometrie. Biometrie is een verzameling van technieken die gebruikt kunnen worden om personen te authentiseren of te identificeren. Aan de hand hiervan kan er worden vastgesteld of de gebruiker is wie hij/zij beweert te zijn of wat de identiteit van de gebruiker is (Brouwers, 2004; Grijpink, 2008; Posthoorn, 2015; Veldhuis, 2014). Een biometrisch systeem bepaalt hoe aannemelijk het is dat twee lichaamskenmerken van dezelfde persoon afkomstig zijn. Om een lichaams- of gedragskenmerk te kunnen rekenen tot een biometrisch kenmerk zijn er een aantal eisen opgesteld. Allereerst is het van belang dat het kenmerk algemeen is, iedereen moet dit kenmerk hebben, hierbij kan gedacht worden aan een kleine teen of een neus. Een tweede eis is de uniciteitseis. Dit betekent dat het kenmerk gebruikt moet kunnen worden om individuen te kunnen onderscheiden. Vervolgens de eis van permanentie, het kenmerk moet over de tijd niet, of zo min mogelijk, veranderen. Een vierde eis is de eis van meetbaarheid waarbij het van belang is dat het kenmerk te meten is. Vervolgens prestatie, hoe nauwkeurig en hoe snel kunnen deze biometrische kenmerken worden vergeleken? De laatste twee eisen zijn de eisen van acceptatie en onvervalsbaarheid. Niet iedereen accepteert bijvoorbeeld dat zijn of haar vingerafdruk wordt gebruikt, dit associeert men namelijk vaak met criminaliteit. Biometrische kenmerken voldoen vaak niet aan alle eisen, echter bepalen deze eisen wel hoe je deze kenmerken kan gebruiken en wat de beste technologie is die hierbij kan worden ingezet (Veldhuis, 2014). Er zijn een aantal voorbeelden te noemen die gebruikt worden als biometrische gegevens en welke kunnen helpen bij het authentiseren en identificeren van personen. Hierbij kan onder andere gedacht worden aan DNA, vingerafdrukken, irisscans, aderpatronen, lichaamsgeur en het gezicht (Grijpink, 2008; Posthoorn, 2015; Veldhuis, 2014).

Veel biometrische technieken werken hetzelfde. Echter wordt er in dit onderzoek gericht gekeken naar geautomatiseerde gelaatsherkenning en zal aan de hand van dit voorbeeld uitgelegd worden hoe een biometrische techniek precies werkt. Allereerst is het van belang dat er biometrische data wordt verkregen

[5] Bron afkomsting van het Programma Sensing (niet publiek toegankelijk).
[6] Bron afkomsting van het Ministerie van Veiligheid en Justitie (niet publiek toegankelijk).

en dat hieruit een patroon wordt gehaald welke wordt opgeslagen. Een patroon is een codereeks waarbij een code voor een specifiek kenmerk van een gezicht staat. Zo krijgt de afstand tussen de ogen een eigen code, de afstand tussen de oren een eigen code, etc. Dit zorgt ervoor dat er referentiemateriaal, in de vorm van een codereeks, ontstaat waarmee nieuwe data kan worden vergeleken. Het referentiemateriaal kan bijvoorbeeld bestaan uit een database met gezichten en de daarbij behorende vastgestelde patronen (oftewel codes). Vervolgens ontstaat er een nieuwe scan met biometrische gegevens waar opnieuw een patroon/codereeks uit wordt gehaald. Een voorbeeld van een nieuwe scan is een foto van het gezicht van een persoon. Dit patroon kan worden vergeleken met de opgeslagen patronen die dienen als referentiemateriaal. Het biometrische systeem geeft vervolgens een matching score welke staat voor de mate van overeenkomst tussen het verkregen materiaal en het referentiemateriaal. Op deze manier bepaalt het systeem dan ook hoe aannemelijk het is dat twee lichaamskenmerken, in het geval van gezichtsherkenning gezichten, van dezelfde persoon afkomstig zijn (Grijpink, 2008; Leman-Langlois, 2003; Posthoorn, 2015; Veldhuis, 2014). In de figuur hieronder is het proces dat plaatsvindt met biometrische technieken eenvoudig weergegeven.



Figuur 1. Eenvoudige weergave van biometrische technieken

Geautomatiseerde gelaatsherkenning is een voorbeeld van een biometrische techniek. Het biometrische kenmerk dat hierbij wordt gebruikt is het gezicht. Door middel van de biometrische kenmerken die het gezicht bevat kan er identificatie of controle van een persoon plaatsvinden op basis van een digitaal beeld (foto) of een videobeeld (Melgaço, 2015; Van Welzen, 2011). Het gezicht bevat een aantal kenmerken die bruikbaar zijn bij het vergelijken van meerdere gezichten. Hierbij kan er gedacht worden aan de vorm en de structuur van het gezicht. Er wordt onder andere gekeken naar de vorm van de neus, de afstand tussen de ogen en oren, de vorm van de oogkassen, de afstand tussen de neus en mond en de vorm van de lippen. Wanneer geautomatiseerde gelaatsherkenning als biometrische techniek wordt toegepast resulteert dit in een lijst van respondenten met een percentage van gelijkenis. Dit houdt in dat het verkregen beeld wordt vergeleken met de referentielijst. De software zorgt ervoor dat er een lijst wordt opgesteld met de meest gelijkende gelaatsafbeeldingen (Politie, 2017). Van tevoren kan er een drempelwaarde worden ingesteld. Wanneer twee afbeeldingen of ook wel twee gezichten een gelijkenis vertonen die boven deze drempelwaarde ligt, komt dit beeld terecht in de lijst met meest gelijkende gelaatsafbeeldingen. De lijst wordt vervolgens in veel gevallen door een expert beoordeeld. Deze doet nog eens een handmatige toets en

kijkt, net als het systeem zelf, naar de overeenkomsten en verschillen tussen de afbeeldingen (Politie, 2012[7]; Politie, 2015[8]).

Vormen van geautomatiseerde gelaatsherkenning

Er zijn twee belangrijke vormen van geautomatiseerde gelaatsherkenning die gebruikt worden door de politie. Allereest één-op-één vergelijking waarbij het gaat om authenticatie van een persoon. Er wordt gekeken of een beeld van een bepaald persoon overeenkomt met een andere afbeelding. Bepaalde biometrische kenmerken worden vergeleken met de kenmerken van het eerder verkregen referentiemateriaal. Er wordt bekeken of de personen op twee afbeeldingen, dezelfde persoon zijn. Een tweede vorm is de één-op-veel vergelijking. Hierbij wordt er getracht om een persoon of subject te herkennen in een stroom of lijst van mensen. Met behulp van een videocamera of een bepaalde afbeelding wordt van het gezicht een aantal biometrische kenmerken bepaald. Deze wordt vervolgens vergeleken met referentiemateriaal dat opgeslagen is in een database. Hier gaat het om het vergelijken van het referentiemateriaal met meerdere gezichten, dit gebeurt vaak om de identiteit van een bepaald persoon vast te stellen (Politie, 2012).

Een ander belangrijk onderscheid dat gemaakt dient te worden is het toepassen van geautomatiseerde gelaatsherkenning op live beelden en het toepassen van geautomatiseerde gelaatsherkenning achteraf. Het verschil hiertussen is het makkelijkst uit te leggen aan de hand van voorbeelden. Een voorbeeld van geautomatiseerde gelaatsherkenning op live beelden is het voorbeeld van CSI, waarbij de meldkamer een bericht krijgt indien een bepaald persoon is herkend op bijvoorbeeld een station. Een ander voorbeeld zijn de toegangspoortjes op Schiphol welke direct een vergelijking maakt met de afbeelding op het paspoort en de persoon die door het poortje wilt. Het achteraf toepassen van geautomatiseerde gelaatsherkenning gebeurt bijvoorbeeld wanneer een foto van een verdachte wordt vergeleken met personen uit de database van de politie om te kijken of deze persoon al eerder in aanraking is gekomen met de politie en om informatie over deze persoon te vinden.

[7] Bron afkomstig van het Korps Landelijke Politiediensten (niet publiek toegankelijk)
[8] Bron afkomstig van de Landelijke Eenheid van de politie (niet publiek toegankelijk)

3. METHODE VAN ONERZOEK

In de eerste paragraaf van dit hoofdstuk zullen de gebruikte onderzoeksmethoden worden beschreven. Vervolgens worden de manieren van dataverzameling besproken. Hier zal per deelvraag worden besproken hoe deze beantwoord dienen te worden. Tevens wordt in dit hoofdstuk de gebruikte scenario's die in deze thesis onderzocht zijn met betrekking tot het formuleren van een antwoord op de vraag welke mogelijkheden en beperkingen er zijn op juridisch gebied. Ten slotte wordt dit hoofdstuk afgesloten met de manier van data-analyse.

Het inzetten van geautomatiseerde gelaatsherkenning in winkelcentra is op korte termijn niet reëel. Dit omdat dit volgens de wetgeving in Nederland niet zomaar is toegestaan. Allereerst moet er gekeken worden naar de voorwaarden waarbij geautomatiseerde gelaatsherkenning toegepast mag worden. Daarnaast kan de politie niet zomaar een sensor inzetten zonder dat hier verder onderzoek naar gedaan is. Doordat het inzetten van geautomatiseerde gelaatsherkenning, bij aanvang van dit onderzoek, niet mogelijk was, kan het daadwerkelijke effect op preventie en opsporing niet gemeten worden. Daarom is ervoor gekozen om allereerst andere effecten van geautomatiseerde gelaatsherkenning in kaart te brengen.

Door middel van het toepassen van geautomatiseerde gelaatsherkenning in een gecontroleerde omgeving, namelijk de werkplek van de medewerkers van Programma Sensing; Villa B, kan er allereerst worden gekeken naar de data die hierbij wordt verschaft. Voor dit onderzoek is er een geautomatiseerde gelaatsherkenningssysteem geplaatst bij de ingang van de werkplek van het Programma Sensing, Villa B. Doordat Villa B zich bevindt in een omgeving waarbij geen sprake is van veel voorkomende criminaliteit zoals dat in winkelcentra, kunnen de effecten op preventie en opsporing niet worden onderzocht. Echter streeft het ophangen van deze sensor een ander doel na. Op deze manier kan er, zoals eerdergenoemd, gekeken worden naar de informatie die wordt verschaft en welke mogelijke reacties dit oproept vanuit de medewerkers. Door de aanwezigheid van het systeem worden medewerkers zich bewust van wat geautomatiseerde gelaatsherkenning is en kunnen zij nadenken over wat zij van deze toepassing vinden. Zij worden vervolgens geïnterviewd over hun ervaring en mogelijke gedragingen die kunnen volgen op het toepassen van geautomatiseerde gelaatsherkenning. Vanuit het Programma Sensing is het nog niet wenselijk om, zo vroeg in het onderzoek naar het inzetten van een nieuwe sensor, de Nederlandse bevolking te bevragen naar eventuele ethische bezwaren. Dit omdat de mening van de burger pas wordt bevraagd nadat het Programma Sensing meer informatie heeft over de mogelijkheden en beperkingen van de sensor. Op deze manier kan het Programma eventuele vragen die vanuit burgers komen, bij het afnemen van een enquête of interview, meteen beantwoorden. Echter, voor het Programma Sensing is het wel van belang om het ethische aspect te onderzoeken. Daarom is ervoor gekozen om in dit onderzoek wel de mening van de medewerkers van het Programma Sensing te bevragen. Zij worden in de interviews niet bevraagd vanuit hun expertise maar vanuit hun rol als burger in de maatschappij. Aan de hand van deze interviews kan er een eerste inzicht worden verworven in eventuele ethische vraagstukken die zich voordoen bij het inzetten van geautomatiseerde gelaatsherkenning.

Dit onderzoek betreft een beschrijvend exploratief kwalitatief onderzoek. In dit onderzoek wordt gebruik gemaakt van zowel een literatuurstudie, interviews en wordt de professionele kennis van juristen, die werken voor het Programma Sensing, geraadpleegd wanneer het gaat om het vormen van een juridisch inzetkader.

3.1. Dataverzameling

Voor dit onderzoek zijn er verschillende manieren van dataverzameling gebruikt. In deze paragraaf wordt er per deelvraag besproken welke manier van dataverzameling is gebruikt om een antwoord te kunnen formuleren. De eerste deelvraag van dit onderzoek tracht een antwoord te vinden op de mogelijkheden en beperkingen van het toepassen van geautomatiseerde gelaatsherkenning wanneer het gaat om de wetgeving in Nederland. Hierbij zijn juridische kaders, bekend binnen het Programma Sensing, van andere sensoren gebruikt om inzicht te verwerven in de bestaande wetten en mogelijkheden voor het toepassen van deze sensoren. Daarnaast wordt deze deelvraag beantwoord met behulp van juristen welke binnen het Programma Sensing werkzaam zijn. Zij zijn de juridisch adviseurs binnen het programma en spelen een rol bij het vormen van juridische inzetkaders zodat duidelijk is in welke gevallen bepaalde sensoren toegepast mogen worden. Samen met hen wordt getracht een juridisch inzetkader te vormen voor verschillende scenario's. Met een juridisch inzetkader wordt gedoeld op een soort stappenplan die kan worden nagelopen en aan de hand waarvan duidelijk wordt of in een bepaald geval de sensor mag worden toegepast of niet. De scenario's zijn opgesteld naar aanleiding van de wensen van het Programma Sensing. Een scenario betreft een mogelijke omschrijving van een gebeurtenis. Vanuit het Programma Sensing zijn er een aantal gebeurtenissen omschreven waarin, volgens haar, geautomatiseerde gelaatsherkenning een oplossing kan bieden voor het probleem, in dit geval winkeldiefstal. Deze gebeurtenissen zijn verder omschreven in de geschetste scenario's. De vraag hierbij is, of in het geval van deze specifieke scenario's, geautomatiseerde gelaatsherkenning mag worden toegepast of niet. Aan de hand van de juridische inzetkaders zal, voor de gebruiker van het gelaatsherkenningssysteem, duidelijk worden onder welke omstandigheden geautomatiseerde gelaatsherkenning toegepast mag worden en onder welke niet. De gebruiker kan zowel een publieke partij, zoals de politie, of een private partij zijn, zoals de winkelier. Er wordt gewerkt vanuit scenario's, welke mogelijke situaties beschrijven waarin geautomatiseerde gelaatsherkenning toegepast kan worden. Deze scenario's worden getoetst aan de wetgeving, zodat uiteindelijk duidelijk is of geautomatiseerde gelaatsherkenning toegepast mag worden in deze gevallen. Allereerst wordt beschreven aan welke voorwaarden er moet worden voldaan wil geautomatiseerde gelaatsherkenning toegestaan zijn. Daarnaast worden de plichten die hieraan verbonden zijn benoemd. Ten slotte wordt er getoetst of de scenario's aan de voorwaarden voldoen en of deze te realiseren zijn wanneer het gaat om het toepassen van geautomatiseerde gelaatsherkenning binnen deze specifieke scenario's.

SCENARIO 1

Scenario 1 betreft een scenario in Villa B. Hierbij wordt geautomatiseerde gelaatsherkenning toegepast in een werkomgeving met het doel om de reacties op deze nieuwe sensor in kaart te brengen. Daarnaast wordt er getracht om op deze wijze medewerkers aan het denken te zetten zodat ethische vraagstukken, welke een rol spelen bij deelvraag 2, aan het licht komen en kunnen worden bevraagd in de interviews. De respondenten die in het systeem staan, die de zogenaamde 'referentielijst' vormen, staan hierin op basis van toestemming. De referentielijst staat in de referentiedatabase welke is benoemd in paragraaf 2.5.

SCENARIO 2

Scenario 2 betreft een scenario waarbij preventie het uiteindelijke doel is. Geautomatiseerde gelaatsherkenning wordt toegepast in winkelcentra ten behoeve van speciale preventie. Bij speciale preventie wilt men voorkomen dat een dader opnieuw de fout in gaat en een delict begaat (Ten Voorde, 2008). Binnen dit scenario wordt er onderscheid gemaakt tussen twee situaties. De eerste situatie (scenario 2.1) is die waarin een winkelcentrum of winkel eigendom is van een private partij. De tweede situatie (scenario 2.2) betreft de situatie waarin een winkelcentrum of winkel eigendom is van een publieke partij.

SCENARIO 3

Scenario 3 betreft het scenario waarbij geautomatiseerde gelaatsherkenning wordt gebruikt ten behoeve van de opsporing van daders van veel voorkomende criminaliteit in winkelcentra. Net zoals bij scenario 2 wordt ook binnen dit scenario onderscheid gemaakt tussen twee situaties. De eerste situatie (scenario 3.1) is dat waarbij er live beelden gebruikt worden ten behoeve van de opsporing. Dit kan gebruikt worden in de gevallen van heterdaad[9]. De tweede situatie (scenario 3.2) is die waarbij beelden achteraf worden gebruikt waarbij er een gezicht van de dader wordt 'uitgesneden' en waarna vervolgens geautomatiseerde gelaatsherkenning wordt toegepast om te zien of de dader al een bekende is en of er al informatie over deze persoon beschikbaar is.

Om uiteindelijk een antwoord te kunnen formuleren op de deelvraag, welke kijkt naar het juridische aspect van geautomatiseerde gelaatsherkenning, wordt de wet die hierop van toepassing is toegelicht. Omdat het in de scenario's gaat om twee verschillende gebruikers, namelijk particulieren/private gebruikers en de politie/publieke gebruikers, worden er twee wetten besproken, de Algemene verordening gegevensbescherming [AVG] en de Wet Politiegegevens [WPG]. De wetten worden kort besproken waarbij belangrijke begrippen worden toegelicht en waarbij de voorwaarden, waaronder geautomatiseerde gelaatsherkenning mag worden toegepast inzichtelijk worden gemaakt. Daarnaast zullen ook de plichten, die zowel de particulieren als de politie hebben, worden benoemd. Zo wordt er een beeld verschaft waarbij duidelijk zal worden op welke wijze geautomatiseerde gelaatsherkenning toegepast kan en mag worden en wanneer dit niet is toegestaan. Vragen zoals, welke personen in de referentielijsten mogen staan, hoelang de beelden bewaard mogen worden, wie de beelden mag gebruiken en wat er gebeurt na een hit komen

[9] Hiermee wordt de opsporing bedoeld die tijdens of kortstondig na de het plegen van het feit plaatsvindt door de politie of de betreffende opsporingsinstantie. Het gaat om het opsporen meteen na het ontdekken van het delict.

hierbij aan bod. Hierdoor zal voor de uiteindelijke gebruiker van het systeem duidelijk zijn in welke gevallen geautomatiseerde gelaatsherkenning toegepast mag worden, onder welke voorwaarden, welke plichten hieraan verbonden zijn en wanneer er van het inzetten van geautomatiseerde gelaatsherkenning zal moeten worden afgezien. Vervolgens zullen de verschillende scenario's getoetst worden aan deze voorwaarden. Zo is het duidelijk of in deze situaties geautomatiseerde gelaatsherkenning toegepast mag worden of niet.

Hieronder volgt een overzicht waarin de scenario's breder zijn uitgewerkt. Hierin zijn onder andere de doelen, gebruikers en situatiebeschrijvingen zichtbaar.

Tabel 1

Overzicht scenario 1

Scenario 1	
Samenvatting	Geautomatiseerde gelaatsherkenning wordt hier toegepast in Villa B binnen het Programma Sensing.
Doel	Het doel van het toepassen van geautomatiseerde gelaatsherkenning is om inzicht te verkrijgen in de mogelijkheden van het systeem en om medewerkers aan het denken te zetten met betrekking tot hun eigen mening over geautomatiseerde gelaatsherkenning.
Modaliteit	De sensor staat aan tijdens kantoortijden wanneer een van de verwerkers aanwezig is
Geautomatiseerde gelaatsherkenning door	Zelf samengestelde referentielijst met medewerkers van het Programma Sensing. Zij staan in deze lijst nadat zij hun toestemming voor medewerking hebben gegeven.
Verwerkingsverantwoordelijke	Programma Manager
Verwerker	Onderzoekster en begeleider onderzoek op locatie
Plaats van toepassing	Villa B, werkplek van de medewerkers van het programma Sensing

Uit tabel 1 blijkt dat scenario 1 betrekking heeft op een private partij welke geautomatiseerde gelaatsherkenning toepast met als doel het testen van een nieuwe sensor. Een vergelijkbaar scenario hierbij zou kunnen zijn dat een private partij geautomatiseerde gelaatsherkenning toepast ten behoeve van de veiligheid van hun gebouw. Denkbaar hierbij is dat geautomatiseerde gelaatsherkenning wordt toegepast om toegang te verlenen voor medewerkers, dit in plaats van een toegangspasje. Ook dit wordt in dit scenario bekeken en wordt in het hoofdstuk met de resultaten getoetst als mogelijkheid met betrekking tot de wet.

Tabel 2

Overzicht scenario 2

Scenario 2		
Samenvatting	Geautomatiseerde gelaatsherkenning wordt hier toegepast in winkelcentra ten behoeve van speciale preventie. Er is een onderscheid tussen het gebruik van geautomatiseerde gelaatsherkenning door private partijen en door publieke partijen.	
	Private partij (scenario 2.1)	**Publieke partij (scenario 2.2)**
Doel	Voorkomen van recidive van VVC in eigen omgeving of eigen winkel en het voorkomen van nieuwe daders van VVC.	Voorkomen van recidive voor VVC in winkelcentra in Nederland. Het terugdringen van VVC.
Modaliteit	Verschillende mogelijkheden: - Geautomatiseerde gelaatsherkenning ten tijde van de openingstijden van het winkelcentrum - Geautomatiseerde gelaatsherkenning 24/7 - Geautomatiseerde gelaatsherkenning 's nachts	Verschillende mogelijkheden: - Geautomatiseerde gelaatsherkenning ten tijden van de openingstijden van het winkelcentrum - Geautomatiseerde gelaatsherkenning 24/7 Geautomatiseerde gelaatsherkenning 's nachts
Geautomatiseerde gelaatsherkenning door/referentielijst bestaande uit	Een waarschuwingsregister met bekende daders die al bekend zijn onder de winkeliers. Het register is opgesteld door de winkeliers zelf en is in handen van de winkeliers.	Een antecedentenlijst van daders die bekend zijn bij de politie. Het gaat om een lijst met politiegegevens. Een voorbeeld hiervan is het systeem van de politie waarin daders staan van delicten zoals VVC of waarin processen verbaal staan van daders die zijn opgepakt voor VVC.
Verwerkingsverantwoordelijke	Er zijn hier twee mogelijke verwerkingsverantwoordelijken: - Eigenaar van het winkelcentrum - Winkelier/eigenaar van de winkel	Er zijn hier twee mogelijke verwerkingsverantwoordelijken: - Politie/justitie - Gemeente
Verwerker	Mogelijke verwerkers: - Winkelier - Camera operator	Mogelijke verwerkers: - Politie-agenten - Ambtenaren van de gemeente - OM
Plaats van toepassing	Verschillende mogelijkheden: - In- en uitgang winkelcentrum - Ingang winkel	Verschillende mogelijkheden: - In- en uitgang winkelcentrum - Ingang winkel - Begin en einde winkelstraat

Uit tabel 2 blijkt dat geautomatiseerde gelaatsherkenning ten behoeve van speciale preventie door zowel een publieke partij als een private partij toegepast kan worden. Vanuit Programma Sensing is het de vraag wat de mogelijkheden voor beide partijen zijn. Mag een private partij geautomatiseerde gelaatsherkenning inzetten en onder welke voorwaarden. Deze vragen spelen ook een rol voor publieke partijen. In het hoofdstuk van de resultaten wordt beschreven wat volgens de regels van de wet mogelijk is voor zowel een private als een publieke partij als het gaat om het inzetten van geautomatiseerde gelaatsherkenning zoals in scenario 2.

Tabel 3

Overzicht scenario 3

Scenario 3		
Samenvatting	Geautomatiseerde gelaatsherkenning gebruiken ten behoeve van de opsporing van bekende en nieuwe daders van veelvoorkomende criminaliteit in winkelcentra.	
Doel	Het zo snel mogelijk opsporen van daders van veel voorkomende criminaliteit	
	Heterdaad	**Buiten heterdaad**
Modaliteit	Tijdens of kortstondig na de daad. Dit gaat om het moment van plegen of het ontdekken van het delict. Het gaat om het meteen actie ondernemen na het ontdekken van het delict.	Na een melding van VVC.
Toelichting	Na melding van het incident wordt het gezicht van de dader uitgesneden op de videobeelden. Dit beeld wordt direct in de referentielijst gezet en zo wordt er gezocht of deze persoon nog terug te vinden is in het winkelgebied.	Na een melding worden de camerabeelden bekeken, indien de dader te zien is wordt hier een afbeelding van zijn/haar gezicht uitgesneden. Dit kan tegen de database worden gehouden om te zien of er al informatie over de dader bekend is.
Geautomatiseerde gelaatsherkenning door/referentielijst bestaande uit	Beeld van de dader op videobeelden.	Beeld van de dader op videobeelden.
Verwerkingsverantwoordelijke	Politie/justitie	Politie/justitie
Verwerker	Politie/justitie	Politie/justitie
Plaats van toepassing	Verschillende mogelijkheden: - In- en uitgang winkelcentrum - Ingang winkel - Begin en einde winkelstraat	Verschillende mogelijkheden: - In- en uitgang winkelcentrum - Ingang winkel - Begin en einde winkelstraat

In tabel 3 is scenario 3 verder uitgewerkt. Vragen zoals; mag de politie op deze manier geautomatiseerde gelaatsherkenning toepassen en waar moet zij hierbij rekening houden spelen een rol. Belangrijk is bijvoorbeeld met welke database de politie de beelden mag vergelijken. Dit zijn vragen die in het hoofdstuk van de resultaten worden beantwoord.

Deelvraag 2, welke kijkt naar ethische vraagstukken met betrekking tot geautomatiseerde gelaatsherkenning, wordt beantwoord aan de hand van literatuuronderzoek en interviews met medewerkers van Villa B. Omdat er nog relatief weinig onderzoek is gedaan naar het inzetten van geautomatiseerde gelaatsherkenningssystemen in winkelcentra in Nederland zal er gekeken worden naar welke ethische aspecten een rol kunnen spelen bij het inzetten van 'slimme systemen' of cameratoezicht in het werk van de politie. Relevante wetenschappelijke literatuur rondom ethische aspecten bij het inzetten van deze 'slimme systemen' en cameratoezicht door de politie zal worden bestudeerd. Om dit beeld aan te kunnen vullen en in te gaan op de ethische aspecten rondom het inzetten van geautomatiseerde gelaatsherkenning

worden er diepte-interviews[10] gehouden met medewerkers van het Programma Sensing. Zij worden, vanuit hun rol binnen het Programma Sensing, bevraagd naar mogelijke ethische dilemma's en naar hun persoonlijke mening en gevoelens bij het inzetten van geautomatiseerde gelaatsherkenning ten behoeve van opsporing en preventie van veel voorkomende criminaliteit in winkelcentra in Nederland. Hierdoor wordt ook deelvraag 3, welke kijkt naar de mening en ervaringen van medewerkers, beantwoord aan de hand van dit semigestructureerde diepte-interview. De vragen van dit interview zijn van tevoren opgesteld. Deze vragen waren een richtlijn, echter laten deze ruimte over voor het verhaal van de medewerker en is hierop verder gevraagd. De interviews zijn afgenomen bij de medewerkers, zie tabel 4 voor een overzicht van de duur van de interviews en de functies van de medewerkers, die mee wilden werken aan het onderzoek en welke een groot deel van hun werktijd in Villa B besteden, dit betreft totaal 14 interviews. De interviews zijn afgenomen in Villa B.

Tabel 4

Overzicht interviews

Respondent	Interviewduur	Functie
1	64 min	OPT Ram- en plofkraken
2	22 min	Privacy Jurist
3	39 min	Programma coördinator conceptontwikkeling
4	37 min	Programma manager Programma Sensing
5	38 min	Landelijk coördinator proeftuinen
6	39 min	TNO
7	27 min	Projectleider Bodycams
8	29 min	Expertteam ANPR
9	27 min	Functioneel beheerder ANPR
10	30 min	Projectondersteuner Programma Sensing
11	47 min	Communicatie
12	15 min	Office Manager
13	21 min	Adviseur informatiemanagement Sensing
14	38 min	Coördinator Evaluatie, onderzoek & benefits

Met behulp van de afgenomen interviews kan er inzicht verkregen worden in de grenzen die de medewerkers aan het systeem leggen. In welke gevallen mag geautomatiseerde gelaatsherkenning, naar hun mening, toegepast worden en wanneer wordt hierbij een grens overschreden? Waar ligt dit aan? In tabel 5 is een overzicht weergegeven met hierin de onderwerpen die zijn bevraagd in de interviews.

[10] Bijlage 1

Tabel 5

Interview topics

Topics	Vragen met betrekking tot
Informatief	- Rol binnen het programma - Achtergrond werk - Eerdere ervaring met geautomatiseerde gelaatsherkenning
Juridisch	- Mogelijke juridische basis
Ethisch	- Privacy - Negatieve en positieve kanten - Waarborgen
Grenzen	- Ernst van het delict - Soort toepassing

Van de interviews die zijn afgenomen worden uitgebreide verslagen gemaakt. Na het schrijven van de verslagen zullen de relevante uitspraken worden beschreven en zal er gekeken worden of de antwoorden van de verschillende medewerkers veel van elkaar afwijken en hoeveel medewerkers hun mening delen.

Deelvraag 4, welke betrekking heeft op de technische mogelijkheden en beperkingen, wordt beantwoord aan de hand van literatuur. Hierbij is voornamelijk het onderzoek van het National Institute of Standards and Technology [NIST] van belang. Deze instelling doet namelijk onderzoek naar geautomatiseerde gelaatsherkenning en de bestaande software die hiervoor op de markt is. Zij publiceert haar resultaten met betrekking tot technische mogelijkheden en beperkingen van de verschillende onderzochte softwareprogramma's. Hierbij wordt het meest recent gepubliceerde onderzoek gebruikt omdat sensoren snel ontwikkelen. Hierdoor veroudert de techniek snel en is het belangrijk om de meest recente resultaten weer te geven. Daarnaast worden de technische mogelijkheden en beperkingen besproken van het geautomatiseerde gelaatsherkenningssysteem welke in Villa B is gebruikt. Het analyseren van de verkregen data van het geautomatiseerde gelaatsherkenningssysteem wordt gedaan door middel van een applicatie. Het geautomatiseerde gelaatsherkenningssysteem is verbonden met een applicatie waarop eenvoudig te zien is welke medewerkers zijn herkend, welke niet en wat er in de omgeving is gebeurd. Op deze manier kunnen ook de reacties van medewerkers worden benoemd.

De laatste deelvraag, deelvraag 5, wordt beantwoord aan de hand van literatuuronderzoek. Deze deelvraag wordt beantwoord aan de hand van informatie dat verkregen is uit literatuur en uit krantenartikelen. Dit betreft een bespreking van verschillende mogelijke toepassingsvormen. Dit is van belang voor het Programma Sensing zodat duidelijk wordt op welke manieren geautomatiseerde gelaatsherkenning al wordt toegepast. Aan de hand hiervan kan het Programma informatie opvragen aan de verschillende partijen en zo informatie verkrijgen van de ervaringen van deze partijen.

3.2. Data-analyse

De juridische informatie is geanalyseerd door allereerst de belangrijkste bepalingen en grondslagen uit de AVG en de WPG uit te schrijven en te bespreken met de juristen van Programma Sensing. Deze uitwerkingen zijn opgesteld naar aanleiding van de wet, de handleiding behorende bij de wet en de juridische kaders welke door het Programma Sensing zijn verstrekt. Deze uitwerkingen zijn weergegeven in bijlage 2 en 3 van dit onderzoek. Vervolgens zijn er, aan de hand van deze uitgebreide bespreking van de toegepaste wetten, schema's gemaakt. De schema's die zijn opgesteld zijn terug te vinden in figuur 2 en 3 van dit onderzoeksverslag. Deze schema's zijn nogmaals nagelopen en gecontroleerd door de juristen van het Programma Sensing. Op deze manier wordt er voorkomen dat er informatie mist of dat informatie onjuist is. Aan de hand van deze schema's zijn de verschillende scenario's, welke zijn weergegeven in tabel 1 tot en met 3, uitgewerkt. De schema's vormen een stappenplan voor het toetsen van verschillende scenario's. Door het doorlopen van deze schema's kan er een antwoord geformuleerd worden op de vraag met betrekking tot de wettelijke mogelijkheden en beperkingen van het inzetten van gelaatsherkenning voor veel voorkomende criminaliteit. Tevens zijn deze toetsingen voorgelegd aan de juristen van het Programma Sensing om foutieve interpretatie van de wet te voorkomen.

De interviews zijn, na het vragen om toestemming van de respondent, vastgelegd door middel van een audio-opname. Na het afnemen van de interviews zijn de interviews zo nauwkeurig mogelijk uitgewerkt waarbij een uitgebreid verslag is geschreven naar aanleiding van de vooraf vastgestelde topics. Belangrijke citatenzijn vetgedrukt weergegeven.

Vervolgens zijn de interviews geanalyseerd aan de hand van open coderen. De verslagen zijn één voor één nagelezen waarbij belangrijke uitspraken en fragmenten per topic zijn gelabeld. Indien er onderwerpen in het interview naar voren kwamen die niet in de topic lijsten zijn opgenomen zijn deze gearceerd met een aparte kleur. Op deze manier zijn alle verslagen gelabeld naar aanleiding van de topics en is er een label met 'overig' gecreëerd. Vervolgens is er gekozen voor axiaal coderen waarbij de verschillende verslagen met elkaar zijn vergeleken en fragmenten die onder één en dezelfde groep behoorde onder elkaar zijn gezet. Dit is tevens gedaan aan de hand van de topics welke afgebeeld zijn in tabel 5. Ten slotte heeft selectief coderen plaatsgevonden waarbij de informatie die onder de topics vielen met elkaar zijn vergeleken. Op deze manier kan er inzicht worden verkregen in het aantal respondenten die dezelfde mening met elkaar delen en de respondenten die over bepaalde onderwerpen anders denken. Aan de hand hiervan is er getracht een antwoord te formulieren op deelvraag 2 en 3 van dit onderzoek.

Het literatuuronderzoek dat is uitgevoerd voor het beantwoorden van deelvraag 4 en 5 en voor een deel ook deelvraag 2, is uitgevoerd door allereerst een lijst met zoektermen op te stellen. Deze zoektermen betroffen onder andere, gelaatsherkenning, facial recognition, technische mogelijkheden gelaatsherkenning, gelaatsherkenning door winkels, gelaatsherkenning door politie, gelaatsherkenning door Koninklijke Marechaussee, gelaatsherkenning China, gezichtsherkenning, geautomatiseerde gezichtsvergelijking, geautomatiseerde gelaatsherkenning en toepassen gelaatsherkenning. Daarnaast is er contact gezocht met

alle Landelijke politiekorpsen om te vragen wat zij van gelaatsherkenning afweten en of zij al eerder hiermee hebben gewerkt. De informatie die hieruit is verzameld is genoteerd in een word bestand. Door middel van deze informatie ontstonden er nieuwe zoektermen en kon er verder gekeken worden naar de literatuur. Tevens is er, naar aanleiding van een korte presentatie over het onderzoek aan de medewerkers van Villa B, gevraagd naar relevante artikelen. Ook dit resulteerde in handige tips met betrekking tot zoektermen en een aantal internet links. Na het verzamelen van de literatuur is de literatuur bestudeerd en gearceerd op onderwerp. Op deze wijze kon inzichtelijk gemaakt worden welk artikel informatie bevatte over welk onderwerp. Ten slotte is, aan de hand van de kleurcodes die aan de artikelen zijn gegeven, een bespreking gemaakt per onderwerp om zo een antwoord te kunnen formuleren op de deelvragen.

3.3. Ethische aspecten

Omdat de interviews gevoelige informatie bevatten, het betreft immers uitspraken van respondenten binnen de politie, is er allereerst toestemming gevraagd om de interviews op te nemen. Vervolgens zijn de respondenten geanonimiseerd doordat er geen namen in het onderzoek worden gebruikt en doordat uitspraken niet gekoppeld worden aan uitspraken van respondenten. Hierdoor is niet duidelijk voor de lezer welke respondent welke uitspraak heeft gedaan. Daarnaast zijn de opnamen van de interviews beveiligd met een wachtwoord welke alleen bekend is bij de onderzoeker. Tevens worden de verslagen van de interviews niet toegevoegd als bijlage omdat de antwoorden op deze manier per respondent te herleiden zouden zijn.

De antwoorden op deelvraag 1 tot en met 5 worden weergegeven in hoofdstuk 4 tot en met 7 waarin de deelvragen apart behandeld worden. Naar aanleiding van de antwoorden op deze deelvragen zal er een antwoord kunnen worden geformuleerd op de onderzoeksvragen welke centraal staat in deze thesis.

4. WETTELIJK KADER

In dit hoofdstuk van deze thesis wordt antwoord gegeven op de deelvraag met betrekking tot de mogelijkheden en beperkingen wanneer het gaat om het inzetten van geautomatiseerde gelaatsherkenning volgens de wet in Nederland. Allereerst wordt een overzicht gegeven met de belangrijkste begripsbepalingen uit de WPG en de AVG, welke een rol spelen bij het inzetten van geautomatiseerde gelaatsherkenning. Dit is van belang omdat op deze manier voor de lezer duidelijk is wat de begrippen inhouden en zodat de lezer kan volgen waar het in het wettelijk kader over gaat. Vervolgens zal de wetgeving, welke een rol speelt bij het toepassen van geautomatiseerde gelaatsherkenning, kort worden besproken. Bij het bespreken van het wettelijk kader zal onderscheid gemaakt worden tussen de regels voor private partijen, zoals winkeliers, en die voor publieke partijen, zoals de politie. Dit onderscheid wordt gemaakt omdat de wetgeving omtrent het verwerken van biometrische gegevens door private en publieke partijen van elkaar verschilt. Tevens worden de scenario's in dit hoofdstuk getoetst aan de wetgeving. Aan de hand van de uitleg van de wet en de scenario's wordt bekeken onder welke omstandigheden de scenario's toegepast mogen worden en waar hierbij rekening gehouden dient te worden. In de derde paragraaf van het hoofdstuk worden de mogelijkheden en beperkingen met betrekking tot de wetgeving in Nederland besproken. Ten slotte volgt een overzicht van de verschillende scenario's met de daarbij behorende juridische kaders.

4.1. Begripsbepalingen

Persoonsgegevens

Persoonsgegevens worden gedefinieerd in artikel 4 lid 1 van de AVG. Het gaat hierbij om alle informatie die gaan over een geïdentificeerde of identificeerbare personen. Volgens artikel 4 lid 1 AVG kan een persoon aan de hand van persoonsgegevens direct of indirect worden geïdentificeerd. Deze informatie is herleidbaar naar één persoon. Voorbeelden zijn iemand zijn naam of woonplaats. Maar ook gegevens zoals iemand zijn/haar ras of godsdienst zijn persoonsgegevens, deze worden zelfs bijzondere persoonsgegevens genoemd (Autoriteit persoonsgegevens, z.j.). Persoonsgegevens zijn dan ook alle gegeven die betrekking hebben op een geïdentificeerde (1), of identificeerbare (2), natuurlijke personen (3). De gegevens moeten dan ook over een persoon gaan en wat over deze persoon zeggen. Ze moeten iets zeggen over een concreet persoon. Onder een geïdentificeerd persoon wordt verstaan dat deze persoon uniek van alle andere personen binnen een groep te onderscheiden is. Een persoon die identificeerbaar is, is een persoon die nog niet geïdentificeerd is maar waarbij dit wel mogelijk is. Een persoon kan geïdentificeerd worden aan de hand van identificatoren. Voorbeelden hiervan zijn lengte, haarkleur, economische kenmerken, IP-adressen, geboortedatum, adres etc. Het laatste kenmerk van een persoonsgegeven is dat het moet gaan om natuurlijke personen. Een organisatie geldt hierbij niet als natuurlijk persoon (tenzij het om een eenmanszaak gaat want dan zegt het wat over het inkomen van deze persoon). Bijzondere categorieën van persoonsgegevens zijn gevoeliger van aard. Het gaat om gegevens waaruit ras of etnische afkomst blijkt,

genetische gegevens, biometrische gegevens, gegevens over gezondheid, politie opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond en gegeven met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. De verwerking van bijzondere persoonsgegevens is in beginsel niet toegestaan tenzij er sprake is van een uitzondering (Ministerie van Veiligheid en Justitie, 2018).

Verwerking

Met het verwerken van persoonsgegevens worden alle bewerkingen bedoeld die betrekking hebben tot persoonsgegevens. Voorbeelden hierbij zijn het verzamelen, vastleggen, ordenen, opslaan, structureren, bijwerken/wijzigen, opvragen, raadplegen, gebruiken en verstrekken. De voorbeelden van verwerken worden zowel in de AVG als de WPG genoemd (art. 4 lid 2 AVG; art. 1 onder f WPG).

Bestand

Artikel 4 lid 6 luidt als volgt: "Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden verspreid". Een voorbeeld van een bestand is een verzameling naamkaartjes of een verzameling foto's (Ministerie van Veiligheid en Justitie, 2018). De WPG geeft eenzelfde definitie van het begrip bestand (art. 1 onder o WPG).

Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is de persoon die het doel van de verwerking vaststelt. Dit kan zowel een natuurlijk persoon als rechtspersoon zijn maar ook een overheidsinstantie of een ander orgaan dat het doel vaststelt (art. 4 lid 7 AVG). Degene die bepaalt welke persoonsgegevens worden verzameld, voor welk doel en de manier waarop dit plaatsvindt is de verwerkingsverantwoordelijke (Ministerie van Veiligheid en Justitie, 2018).

In tegenstelling tot de AVG stelt de WPG vast welke personen verwerkingsverantwoordelijke zijn. Deze zijn terug te vinden in artikel 1 sub f. Zo is de verwerkingsverantwoordelijke bij de politie de korpschef en bij de rijksrecherche het College van procureurs-generaal. Daarnaast is de verwerkingsverantwoordelijke van de Koninklijke marechaussee de Minister van Defensie.

Verwerker

Volgens artikel 4 lid 8 AVG is een verwerker "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt". De opdracht van de verwerker is afkomstig van de verwerkingsverantwoordelijke, de primaire opdracht is hier het verwerken van de persoonsgegevens (Ministerie van Veiligheid en Justitie, 2018).

Biometrische gegevens

Biometrische gegevens spelen een rol bij geautomatiseerde gelaatsherkenning. Het zijn "persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische

of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens" (art. 4 lid 14 AVG; art. 1 onder s WPG).

Politiegegevens

Politiegegeven wordt gedefinieerd in artikel 1 sub a van de WPG. Een politiegegeven is een persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak zoals deze is omschreven in de artikelen 3 en 4 van de Politiewet. Deze stellen onder andere dat de politie de taak heeft om volgens de geldende rechtsregels te zorgen voor de handhaving van de rechtsorde en voor het verlenen van hulp aan degene die deze behoeven en dat de politie de zorg draagt voor de beveiliging van luchtvaartterreinen. Een persoonsgegeven wordt in de WPG hetzelfde gedefinieerd als in de AVG. Het gaat namelijk om informatie dat gaat over een geïdentificeerde of identificeerbare natuurlijke personen (Art. 1 sub b WPG).

4.1.2. Wettelijk kader

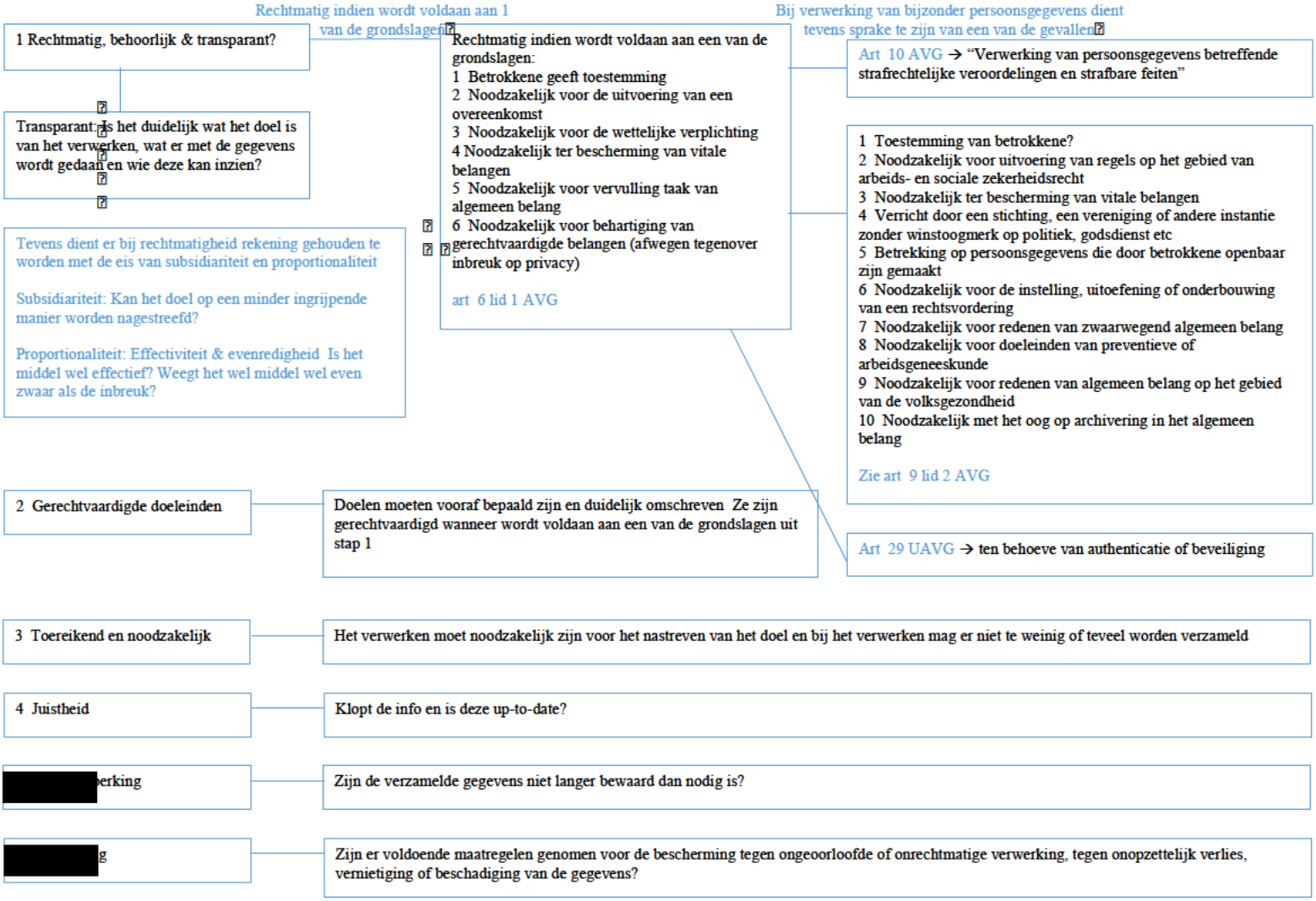
Wanneer er gebruik gemaakt wordt van nieuwe preventie- of opsporingsmiddelen is allereerst artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens [EVRM] van belang. Volgens dit artikel heeft iedereen recht op eerbiediging van het privé- en gezinsleven. Een inbreuk op de privacy is gerechtvaardigd indien de inbreuk bij de wet is voorzien en noodzakelijk is met het oog op één van de belangen die artikel 8 noemt. Zo is een belang bijvoorbeeld de nationale veiligheid of het voorkomen van strafbare feiten (Politie, 2010[11]). Er dient gekeken te worden of het gebruiken van geautomatiseerde gelaatsherkenning bij de wet voorzien is en of dit een van de belangen nastreeft die genoemd worden in artikel 8 EVRM.

In onderstaande paragrafen wordt er gekeken naar de regels omtrent het inzetten van nieuwe technieken, zoals geautomatiseerde gelaatsherkenning, door zowel private als publieke partijen. Allereerst wordt het wettelijk kader omtrent private partijen kort besproken waarna een toetsing op scenario 1 en scenario 2.1 volgen. Vervolgens wordt het wettelijk kader omtrent publieke partijen kort besproken waarna een toetsing op scenario 2.2, scenario 3.1 en scenario 3.2 volgen. Na de bespreking van de verschillende scenario's wordt een schematisch overzicht weergegeven in figuur 4 welke een samenvatting van de juridische inzetkaders bevat. Ten slotte zullen de mogelijkheden en beperkingen, welke naar voren komen aan de hand van de bespreking van de scenario's, kort worden besproken.

[11] Bron afkomstig van het Korps landelijke politiediensten van de politie (niet publiek toegankelijk)

4.1.2.1. Private partijen

Wanneer het gaat om het verwerken van persoonsgegevens door private partijen is de AVG van toepassing. De AVG stelt in artikel 5 dat er bij de verwerking van persoonsgegevens sprake moet zijn van rechtmatigheid, behoorlijkheid, transparantie, gerechtmatigde doeleinden, toereikendheid, noodzakelijkheid, juistheid van gegevens, beveiliging van gegevens en een redelijke bewaartermijn het onder omstandigheden toegestaan is dat persoonsgegevens worden verwerkt. Tevens stelt de AVG een aantal plichten voor de verwerkingsverantwoordelijke en de verwerker en geeft de AVG een aantal rechten voor betrokkenen. Om te bepalen of het verwerken van persoonsgegevens toegestaan is zijn er een aantal stappen die doorlopen kunnen worden. Deze zijn afgebeeld in figuur 2. Een uitgebreide uitleg van het wettelijke kader dat wordt gegeven in de AVG is terug te vinden in bijlage 2 van dit onderzoek.



Figuur 2. Schematisch overzicht van het wettelijk kader van private partijen omtrent het verwerken van bijzondere persoonsgegevens.

Tevens stelt de AVG een aantal plichten aan de verwerkingsverantwoordelijke en de verwerker. Wanneer er persoonsgegevens verwerkt worden dient hieraan te worden voldaan. In tabel 6 worden de plichten, met de daarbij behorende uitleg, van de verwerkingsverantwoordelijke kort weergegeven. Daarnaast is een uitgebreide uitleg van deze plichten terug te vinden in het wettelijk kader dat bijgevoegd is in bijlage 2.

Tabel 6

Overzicht plichten verwerkingsverantwoordelijke

Plicht	Uitleg
Registerplicht	Register met hierin de verwerkingsactiviteiten dient bijgehouden te worden.
Functionaris voor gegevensbescherming	Deze houdt toezicht op de toepassing en naleving van de Verordening.
Gegevensbeschermingseffectbeoordeling	Hiermee wordt de aard, de oorsprong en de ernst van risico's voor de bescherming van de vrijheden en rechten van betrokkenen geanalyseerd.
Voorafgaande raadpleging	Verwerking vooraf voorleggen aan de Autoriteit Persoonsgegevens
Privacy by design & default	Bescherming van privacy en gegevens wordt meegenomen in de ontwikkeling van het ontwerp
Beveiligingsmaatregelen	Een aantal beveiligingsmaatregelen die genomen dienen te worden.
Melden bij datalek	In het geval van een datalek dient dit gemeld te worden.
Afspraken met verwerkers	De verwerking met daarbij behorende afspraken dienen in een overeenkomst te worden opgenomen.

De plichten van de verwerker zijn terug te vinden in artikel 28 van de AVG. Allereerst moet de verwerker voldoende garanties kunnen bieden. Deze garanties hebben betrekking op de naleving van de Verordening. Ten tweede moet de verwerker een verwerkersovereenkomst tekenen waarin de afspraken met de verwerkingsverantwoordelijke staan. Verder moet de verwerker zijn of haar verwerkingsactiviteiten registeren. Een andere plicht die de verwerker heeft is dat hij of zij moet meewerken met de Autoriteit Persoonsgegevens (Ministerie van Veiligheid en Justitie, 2018).

Tevens stelt de AVG een aantal rechten vast voor betrokkenen. Zo hebben betrokkenen recht op informatie over de verwerking, recht op inzage in de gegevens, recht op correctie van de gegevens indien deze onjuist zijn, het recht om vergeten te worden, het recht op beperking van gegevensverwerking, het recht op verzet tegen gegevensverwerking, het recht op overdracht van zijn of haar gegevens en het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming (Ministerie van Veiligheid en Justitie, 2018). Ook hier dienen de partijen rekening mee te houden.

Aan de hand van het wettelijk kader dat hierboven is geschetst zullen scenario 1 en scenario 2.1 getoetst worden. Hierdoor wordt duidelijk of de scenario's wettelijk zijn en onder welke omstandigheden dit het geval is.

Scenario 1

Bij scenario 1 wordt geautomatiseerde gelaatsherkenning toegepast binnen Villa B om inzicht te verkrijgen in de mogelijkheden van het systeem en om medewerkers aan het denken te zetten over geautomatiseerde gelaatsherkenning. Het systeem staat hier louter aan op kantoortijden en wordt afgesloten wanneer de proef voorbij is. De referentielijst die wordt gebruikt bestaat uit medewerkers van het Programma Sensing die toestemming hebben verleend om deel te nemen aan de proef.

Dit scenario wordt toegepast door een werkgever, hierbij is het niet van belang dat deze werkgever in dit geval de politie is maar is het van belang dat de werkgever in deze situatie een private partij is. Hierdoor wordt er gekeken of dit scenario een juridisch draagvlak heeft aan de hand van het wettelijk kader voor private partijen. Allereerst dient er gekeken te worden of de verwerking rechtmatig, behoorlijk en transparant is. Bij rechtmatigheid van het verwerken van biometrische gegevens dient er sprake te zijn van een van de grondslagen uit artikel 6 AVG. Vervolgens dient er, doordat er sprake is van het verwerken van bijzondere persoonsgegevens, gekeken te worden of ook dit rechtmatig is. In deze situatie is er sprake van de grondslag van toestemmingverlening. De medewerkers hebben toestemming verleend waardoor de verwerking rechtmatig plaatsvindt. Tevens is er sprake van transparantie naar de deelnemers toe. Zij weten waarom zij deelnemen aan de proef en wat het doel van deze proef is. Dit is kenbaar gemaakt aan de hand van een email. Zo is deze manier van verwerking rechtmatig doordat er sprake is van art. 6 lid 1 onder a jo. art. 9 lid 2 onder a. Naast dat het scenario moet voldoen aan een van de grondslagen moet het tevens voldoen aan de eis van proportionaliteit en subsidiariteit. Aan beide eisen wordt in dit scenario voldaan. Aan de eis van subsidiariteit is voldaan doordat dit onderzoek op geen andere wijze kon worden uitgevoerd. Aan de eis van proportionaliteit is voldaan doordat de inbreuk proportioneel is. Dit doordat de personen toestemming hebben verleend en doordat de gegevens zijn verwijderd zodra deze niet langer nodig waren.

Een tweede stap is dat verwerking louter gedaan mag worden op grond van gerechtvaardigde doeleinden. De doeleinden zijn in dit geval gerechtvaardigd omdat de verwerking voldoet aan een van de grondslagen bij de wet voorzien. Een volgende vraag die speelt is of de verwerking toereikend en noodzakelijk is. Het verwerken van de biometrische gegevens moet in dit geval noodzakelijk zijn voor het nastreven van het doel. Tevens mag er bij de verwerking van de gegevens niet te veel of te weinig gegevens worden verzameld. Ook aan deze eis wordt voldaan. Zonder het toepassen van het geautomatiseerde gelaatsherkenningssysteem in Villa B is het namelijk niet mogelijk om inzicht te verkrijgen in de mogelijkheden van het systeem waardoor het doel, dat vooraf is opgesteld, niet kan worden nagestreefd. Daarnaast worden er niet te veel gegevens verzameld, het systeem staat immers alleen aan tijdens kantoortijden en gegevens van personen die niet aan de proef deelnemen worden elke dag verwijderd. Een volgende eis is de eis van juistheid; zijn de gegevens juist? De gegevens waren in het geval van deze situatie juist. De referentiedatabase betrof alleen foto's van de medewerkers met hierbij hun naam. Eis vijf is de eis van opslagbeperking. De gegevens mogen niet langer bewaard worden dan nodig. Ook aan deze eis is voldaan. Alle opgenomen beelden zijn tijdens de proef na een week verwijderd. Nadat alle interviews waren afgenomen en er inzicht was verkregen in hoe het systeem werkte en wat voor data er wordt

gegenereerd is het systeem losgekoppeld, zijn de gegevens verwijderd en zijn de applicaties verwijderd. De laatste eis is de beveiligingseis. In dit geval moeten er voldoende maatregelen zijn getroffen voor de bescherming tegen ongeoorloofde of onrechtmatige verwerking, tegen onopzettelijk verlies, vernietiging of beschadiging van de gegevens. Aan deze eis is niet voldaan. Tijdens de proef bleek dat de gegevens opgeslagen werden op een SD kaart. Deze SD kaart zat in het geautomatiseerde gelaatsherkenningssysteem en kon uit het systeem worden gehaald. Dit kon iedereen doen, hierdoor is niet voldaan aan eis 6.

Een vergelijkbaar scenario als dat van scenario 1 is dat een werkgever zijn of haar gebouw wil beschermen en medewerkers het gebouw laat betreden door middel van geautomatiseerde gelaatsherkenning in plaats van toegangspasjes. Dit is volgens het stappenplan dat is afgebeeld in figuur 2 mogelijk ondanks dat er geen sprake is van een van de grondslagen uit artikel 9 AVG. Op grond van artikel 6 lid 1 onder b jo. 29 UAVG is het voor private partijen mogelijk om biometrische gegevens te verwerken ten behoeve van authenticatie van personen of ten behoeve van de beveiliging. Dit is het geval bij een mogelijk scenario zoals hier beschreven.

Bij dit scenario geldt dat de verwerkingsverantwoordelijke en de verwerker zicht moeten houden aan een aantal plichten. Voor de verwerkingsverantwoordelijke geldt de verplichting met betrekking tot het hebben van een functionaris voor gegevensbescherming, het uitvoeren van een gegevenseffectbeoordeling, voorafgaande raadpleging, privacy by design & default, beveiligingsmaatregelen, melding bij datalek en afspraken met verwerkers. Omdat er sprake is van het verwerken van bijzondere persoonsgegevens is het nodig om een functionaris voor gegevensbescherming aan te wijzen welke adviseert en toezicht houdt op de naleving van de regels die gesteld zijn door de AVG. In scenario’s 1 is er geen sprake van een functionaris gegevensbescherming. Van zowel een gegevensbeschermingseffectbeoordeling en een voorafgaande raadpleging van de Autoriteit persoonsgegevens is geen sprake geweest. Dit had voorafgaand aan de verwerking wel gemoeten. Ook is er geen sprake geweest van het nemen van voldoende beveiligingsmaatregelen, het maken van schriftelijke afspraken met verwerkers en privacy by design & default. Er is dan ook niet voldaan aan de plichten die gesteld worden door de AVG.

Een eenvoudig overzicht van de hierboven genoemde afwegingen wordt weergegeven in tabel 7 op pagina 38 van dit onderzoek.

Tabel 7

Toetsing scenario 1

Beginsel	**Aan voldaan?**
Rechtmatig, behoorlijk & transparant	Ja. Rechtmatig door art. 6 lid 1 onder a jo. art. 9 lid 2 onder a. Transparant doordat er door middel van een email duidelijk is gemaakt wat het doel van de proef is. Tevens is hier sprake van proportionaliteit en subsidiariteit omdat dit onderzoek niet op basis van een ander inzetmiddel gedaan kon worden en doordat de inbreuk op de persoonlijke levenssfeer wordt geminimaliseerd door gegevens zo snel mogelijk te verwijderen.
Gerechtvaardigde doeleinden	Ja, art. 6 lid 1 onder a jo. art. 9 lid 2 onder a AVG.
Toereikend en noodzakelijk	Ja. Noodzakelijk omdat alleen op deze manier het doel kan worden nagestreefd. Toereikend omdat er niet meer gegevens worden verwerkt dan nodig.
Juistheid	Ja, deze is steeds bijgehouden.
Opslagbeperking	Ja. Zodra inzicht was verkregen in de mogelijkheden en de proef voorbij was zijn de gegevens verwijderd.
Beveiliging	Nee. Er hadden meer maatregelen genomen kunnen worden. Zo was het mogelijk om de SD kaart uit het systeem te halen en zo bezit te krijgen over de data.

Scenario 2.1

Het eerste scenario binnen scenario 2 is het scenario waarin een private partij, zoals een winkelier, geautomatiseerde gelaatsherkenning toepast ten behoeve van recidive van veel voorkomende criminaliteit in eigen omgeving of in de eigen winkel en het voorkomen van nieuwe daders van veel voorkomende criminaliteit. Geautomatiseerde gelaatsherkenning kan tijdens verschillende modaliteiten worden toegepast. Namelijk ten tijde van de openingstijden van de winkel, alleen 's nachts of gedurende de hele week. De referentielijst die hier wordt gebruikt bestaat uit afbeeldingen van personen die bekend zijn bij de winkelier en die zijn verkregen door de winkelier zelf. Dit door middel van bewakingsbeelden waarin de persoon in kwestie te zien is of doordat de persoon in kwestie eerder is aangesproken, een winkelverbod heeft en van deze persoon een foto is genomen. De verwerkingsverantwoordelijke is hier de eigenaar van de winkel of de eigenaar van het winkelcentrum die geautomatiseerde gelaatsherkenning in zijn of haar winkelcentrum toepast. Wie de verwerker mag zijn wordt tevens in dit scenario besproken.

Net zoals bij scenario 1 speelt hier het schema een rol dat is afgebeeld op figuur 2 van deze thesis. Allereerst dient de verwerking van biometrische gegevens rechtmatig, behoorlijk en transparant te zijn. Rechtmatigheid kan worden verkregen vanuit artikel 6 lid 1 onder f jo art. 10 AVG of door middel van artikel 6 lid 1 onder f AVG jo. art. 9 lid 2 onder g AVG jo. art. 29 UAVG. Met transparantie is het van belang dat het doel duidelijk gemaakt dient te worden, dit kan bijvoorbeeld door het ophangen van een bordje op de gevel van het gebouw 'let op hier wordt geautomatiseerde gelaatsherkenning toegepast ten

behoeve van de beveiliging'. Echter moet het hiernaast ook duidelijk zijn wie de gegevens kan inzien en wat er met deze gegevens wordt gedaan. Dit moet vooraf zijn vastgesteld en naar klanten duidelijk gemaakt worden. Dit kan door bijvoorbeeld een krantenbericht te plaatsen of een advertentie op de website van de winkelier met hierin het doel van de verwerking en de omschrijving. Omdat de verwerking rechtmatig is, is er sprake van een verwerking volgens gerechtvaardigde doeleinden. Een volgende eis is dat de verwerking toereikend en noodzakelijk dient te zijn. Bij de verwerking mogen niet teveel of te weinig gegevens worden verzameld. Daarbij is het van belang dat niet iedereens gezicht wordt opgeslagen maar dat er alleen wordt gekeken naar de personen met een match. Andere personen dienen uit het geautomatiseerde gelaatsherkenningssysteem vernietigd te worden. Daarnaast moet de winkelier een verschillende afwegingen maken. Zo moet hij of zij bepalen of de gegevens nog juist zijn, wanneer deze bijvoorbeeld van een aantal jaar geleden zijn kan de winkelier deze beter uit het systeem verwijderen. Dit geldt ook voor de eis van opslagbeperking. Wanneer de winkelier twijfelt of de gegevens nog wel nodig zijn moeten deze verwijderd worden, gegevens mogen immers niet langer bewaard worden dan nodig in overeenstemming met het vooropgestelde doel. Ook dient de winkelier voldoende beveiligingsmaatregelen te treffen tegen ongeoorloofde of onrechtmatige verwerking, tegen onopzettelijk verlies, vernietiging of beschadiging van de gegevens. Tevens dient de winkelier bij de eis van noodzakelijkheid te kijken naar wanneer hij of zij het geautomatiseerde gelaatsherkenningssysteem aanzet. Wanneer er alleen delicten worden gepleegd tijdens de openingstijden van de winkel dan is het belangrijk dat het geautomatiseerde gelaatsherkenningssysteem aan staat ten tijde van de openingstijden. Het is in dit geval niet noodzakelijk om het systeem ook 's nachts aan te laten. Hier speelt tevens de proportionaliteitseis een rol. Wanneer het niet nodig is om gegevens op bepaalde tijden van de dag te verwerken dient dit ook niet te gebeuren. Naast de proportionaliteitseis dient de winkelier een afweging te maken met betrekking tot de subsidiariteitseis. Wanneer hij of zij de winkel en de spullen kan beschermen door middel van een minder ingrijpend middel, zoals gewone camerabewaking, dient er voor het minst ingrijpende middel gekozen te worden.
Daarnaast dient de winkelier zowel te kijken naar de plichten van de verwerkingsverantwoordelijke en de verwerker (indien deze er is) wil de verwerking wettelijk zijn. Dit dient hij of zij te doen voordat de verwerking plaatsvindt.

Kortom, winkeliers mogen geautomatiseerde gelaatsherkenning toepassen mits zij hierbij duidelijke afwegingen hebben gemaakt en deze duidelijk hebben omschreven en het doel waarmee zij geautomatiseerde gelaatsherkenning toepassen bekend is. In tabel 8 wordt er een samenvatting gegeven met betrekking tot de conclusie op de stappen uit figuur 2.

Tabel 8

Toetsing scenario 2.1

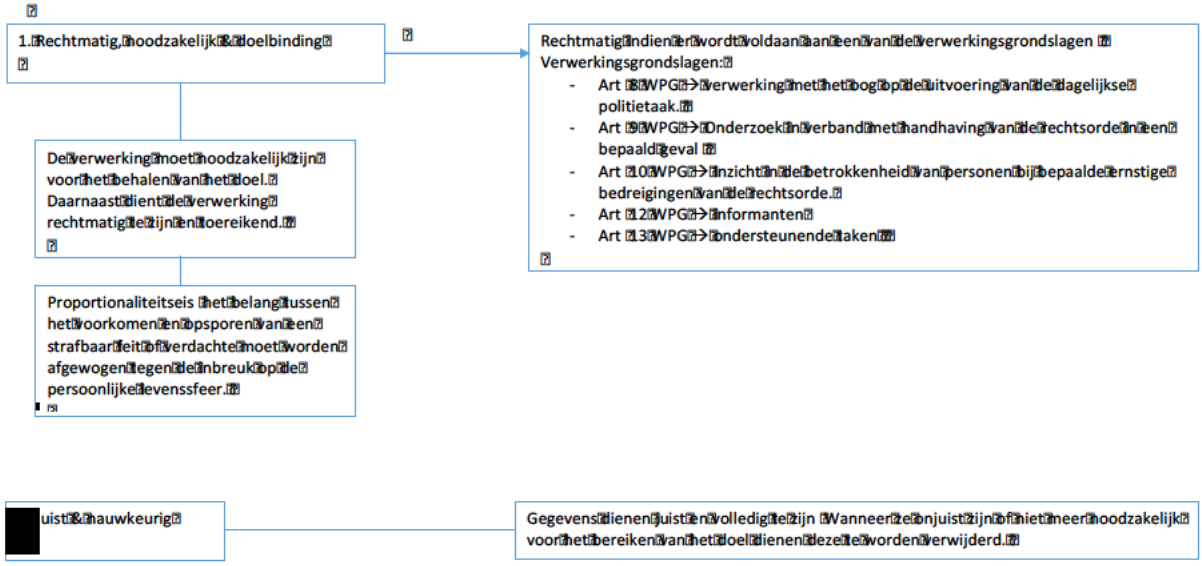
Beginsel	**Aan voldaan?**
Rechtmatig, behoorlijk & transparant	Ja. Rechtmatig door art. 6 lid 1 onder f jo. art. 10 AVG of door middel van art. 6 lid 1 onder f AVG jo. art. 9 lid 2 onder g AVG jo. art. 29 UAVG. Transparantie kan bereikt worden door middel van het plaatsen van een krantenbericht of advertentie en door een bordje op de gevel te plaatsen. Tevens dient er rekening gehouden te worden met de eis van proportionaliteit en subsidiariteit. Proportionaliteit kan bereikt worden door het systeem alleen aan te zetten tijdens tijden waarop bekend is dat er veel criminaliteit gepleegd wordt. Subsidiariteit kan bereikt worden door een afweging te maken tussen middelen. Wanneer er een minder ingrijpend middel is dient hiervoor gekozen te worden.
Gerechtvaardigde doeleinden	Ja, art. 6 lid 1 onder f jo. art. 10 AVG of door middel van art. 6 lid 1 onder f AVG jo. art. 9 lid 2 onder g AVG jo. art. 29 UAVG.
Toereikend en noodzakelijk	Afhankelijk van het geval. Noodzakelijk als er geen andere mogelijkheden meer zijn om te beveiligen. Toereikend als er niet meer gegevens worden verwerkt dan nodig en onschuldigen direct uit het systeem gehaald worden.
Juistheid	Indien de gegevens up-to-date gehouden worden.
Opslagbeperking	Hiervan is sprake indien gegevens niet langer bewaard worden in overeenstemming met het doel.
Beveiliging	Indien er voldoende beveiligingsmaatregelen genomen.

4.1.2.2. Publieke partijen

Wanneer de politie biometrische gegevens verwerkt voor haar politietaak is de WPG van toepassing. In deze wet staat beschreven op welke wijze de gegevens verwerkt mogen worden. Voor de politie geldt er een specifieke wetgeving omdat zij gegevens over burgers verwerkt die niet met toestemming zijn afgegeven (Politie, 2018[12]). Net als de AVG stelt de WPG een aantal beginselen waaronder de politie gegevens mag verwerken. Bij de verwerking moet er sprake zijn van rechtmatigheid, noodzakelijkheid, doelbinding, juistheid van de gegevens en volledigheid. Tevens stelt de WPG een aantal plichten voor de verwerkingsverantwoordelijke en de verwerking en geeft de WPG een aantal rechten voor betrokkenen. Net als bij het wettelijk kader voor private partijen is er een schema gemaakt met daarin de stappen die doorlopen kunnen worden wil een verwerking wettelijk zijn. Dit schema is afgebeeld in figuur 3. Daarnaast

[12] Bron afkomstig van de Politie – Gegevensautoriteit (niet publiek toegankelijk).

wordt een uitgebreide uitleg van het wettelijk kader voor publieke partijen gegeven in bijlage 3 van dit onderzoek.



Figuur 3. Schematisch overzicht van het wettelijk kader van publieke partijen omtrent het verwerken van bijzondere persoonsgegevens.

Tevens stelt de WPG een aantal plichten aan de verwerkingsverantwoordelijke en de verwerker. Wanneer er persoonsgegevens verwerkt worden dient hieraan te worden voldaan. In tabel 9 worden de plichten, met de daarbij behorende uitleg, van de verwerkingsverantwoordelijke kort weergegeven. Daarnaast is een uitgebreide uitleg van deze plichten terug te vinden in het wettelijk kader dat bijgevoegd is in bijlage 3.

Tabel 9

Overzicht plichten verwerkingsverantwoordelijke

Plicht	Uitleg
Gegevensbescherming door beveiliging en ontwerp	De verwerkingsverantwoordelijke dient passende technische en organisatorische maatregelen te treffen om te kunnen aantonen dat de gegevens alleen worden verwerkt in overeenstemming met het doel dat krachtens of bij de wet is bepaald.
Gegevensbescherming door standaardinstellingen	De verwerkingsverantwoordelijke dient ervoor te zorgen dat er passende technische en organisatorische maatregelen worden genomen dat standaard alleen de politiegegevens worden verwerkt die noodzakelijk zijn voor een specifiek doel.
Gegevensbeschermingseffectbeoordeling	Bij een hoog risico voor de rechten en vrijheden van personen dient er voorafgaand een beoordeling te worden uitgevoerd.
Autoritsatie	De verwerkingsverantwoordelijke is verantwoordelijk voor het bijhouden van de autorisaties.
Registerplicht	De verwerkingsverantwoordelijke heeft een registerplicht.
Documentatie	De verwerkingsverantwoordelijke draagt zorg voor de schriftelijke vastlegging van de doelen van het onderzoek.

Melden van datalek	In het geval van een datalek dient de verwerkingsverantwoordelijke een melding hiervan te doen bij de Autoriteit Persoonsgegevens.
Voorafgaande raadpleging	De verwerkingsverantwoordelijke is verantwoordelijke voor de voorafgaande raadpleging van de Autoriteit Persoonsgegevens.
Privacyfunctionaris	De privacyfunctionaris dienst benoemt te worden door de verwerkingsverantwoordelijke.
Functionaris voor gegevensbescherming	De verwerkingsverantwoordelijke dient een functionaris voor gegevensbescherming aan te wijzen.

Naast de plichten van de verwerkingsverantwoordelijke heeft de verwerker ook een aantal plichten. Zo moet ook de verwerker passende technische en organisatorische maatregelen treffen om aan te kunnen tonen dat gegevens louter worden verwerkt in overeenstemming met het doel. Daarnaast dient er een schriftelijke overeenkomst te zijn tussen de verwerkingsverantwoordelijke en de verwerker. Ook dient de verwerker een register bij te houden dat gegevens bevat die benoemd worden in artikel 31d WPG. Ook helpt de verwerker bij het bijhouden van de loggings waardoor duidelijk is hoe de verwerking plaatsvindt. Aan de hand van een logging kan worden gecontroleerd wie op welk moment inzage had in de persoonsgegevens. De logging bevat gegevens over de werknemer, die de gegevens geraadpleegd heeft, en het moment van inzage (Centrum informatiebeveiliging en privacybescherming, 2018).

Ook stelt de WPG een aantal rechten voor betrokkenen vast. Deze zijn terug te vinden in paragraaf 4 van de WPG. Zo dienen betrokkenen informatie te verkrijgen, hebben betrokkenen recht op inzage met betrekking tot de verwerking en de politiegegevens die verwerkt worden en recht op aanpassing en vernietiging van politiegegevens. Betrokkenen mogen deze rechten uitoefenen. Ook hier dient rekening mee gehouden te worden.

Aan de hand van het wettelijk kader dat hierboven is geschetst zullen scenario 2.2, scenario 3.1 en scenario 3.2 getoetst worden. Hierdoor wordt duidelijk of de scenario's wettelijk zijn en onder welke omstandigheden dit het geval is.

Scenario 2.2

Het tweede scenario binnen scenario 2 is het scenario waarin een publieke partij, zoals de politie, geautomatiseerde gelaatsherkenning toepast ten behoeve van het voorkomen van recidive voor veel voorkomende criminaliteit. Hierbij kan ervoor gekozen worden om het geautomatiseerde gelaatsherkenningssysteem aan te zetten ten tijde van de openingstijden van het winkelcentrum, 's nachts of altijd. De referentielijst bestaat hier uit daders en verdachten die bekend zijn bij de politie. Een voorbeeld is het HKS database. De verwerkingsverantwoordelijke wordt vastgesteld door de WPG. In het geval van dit scenario is de Korpschef de verwerkingsverantwoordelijke van de politie.

De WPG stelt, net als de AVG, de eis dat inzake verwerking van politiegegevens de verwerking rechtmatig en noodzakelijk dient te zijn. Daarnaast moet er sprake zijn van doelbinding. De verwerking van de gegevens dient noodzakelijk te zijn voor het behalen van het doel. Dit is alleen het geval indien er geen

andere mogelijkheden meer zijn om veel voorkomende criminaliteit terug te dringen. Dit komt dan ook overeen met de eis van subsidiariteit. Voordat geautomatiseerde gelaatsherkenning wordt toegepast dient allereerst te worden onderzocht of er geen milder alternatief is. Daarnaast geldt de eis van proportionaliteit. De impact van veel voorkomende criminaliteit dient afgewogen te worden tegenover de inbreuk op de persoonlijke levenssfeer. Dit zal per geval verschillend zijn. Wanneer er een bijvoorbeeld een winkelcentrum is waarin vaak veel voorkomende criminaliteit voorkomt en waardoor burgers zich onveiliger voelen dan zal deze afweging eerder naar het toepassen van geautomatiseerde gelaatsherkenning neigen. Echter, wanneer de impact van veel voorkomende criminaliteit op zowel de winkelende burger als de winkelier niet enorm groot is doordat de schade bijvoorbeeld te verwaarlozen is, dan zal deze afweging neigen naar een te grote inbreuk op de persoonlijke levenssfeer. De proportionaliteitseis en de noodzakelijkheidseis dienen per geval te worden bekeken. Van rechtmatigheid is er sprake indien er wordt voldaan aan één van de verwerkingsgrondslagen. In het geval van het winkelcentrum is er sprake van artikel 9 WPG. Er wordt een hoeveelheid gegevens verzameld die gericht zijn op een specifieke gebeurtenis, namelijk veel voorkomende criminaliteit in een winkel(centrum). Hierbij is het belangrijk dat de gegevens die worden verwerkt alleen bewaard worden indien dit noodzakelijk is voor het behalen van het doel. Een andere eis is de eis van juistheid en nauwkeurigheid. De politie moet in dit geval toezien op de juistheid van de gegevens die worden verworven. Ook dient de politie te voldoen aan een aantal plichten. Zo dient er sprake te zijn van gegevensbescherming door beveiliging en ontwerp, gegevensbescherming door standaardinstelling, draagt de verwerkingsverantwoordelijke zorgt voor de autorisatie, registerplicht, documentatie, het melden van datalekken, voorafgaande raadpleging, het benoemen van een privacyfunctionaris en een functionaris voor gegevensbescherming en dient er voorafgaand een gegevensbeschermingseffectbeoordeling te hebben plaatsgevonden.

Kortom, voor het verwerken van politiegegevens ten behoeve van het voorkomen van recidive voor veel voorkomende criminaliteit in winkelcentra is een verwerkingsgrondslag, namelijk artikel 9 WPG. Echter dient er per geval een afweging gemaakt te worden of de verwerking noodzakelijk is voor het behalen van het doel en of de verwerking voldoet aan de subsidiariteitseis en de proportionaliteitseis. Wanneer het effect van het voorkomen van criminaliteit bereikt kan worden door meer beveiligers of meer agenten op straat in te schakelen dient dit eerder te gebeuren omdat dit een minder grote inbreuk op de persoonlijke levenssfeer is. Waar en wanneer geautomatiseerde gelaatsherkenning toegepast wordt hangt tevens af van de omstandigheden van het geval. Wanneer er bij een winkel vaak wordt ingebroken is het waarschijnlijker om hier geautomatiseerde gelaatsherkenning toe te passen dan bij een winkel waar er nog nooit is ingebroken. Dit geldt tevens voor de tijd waarin geautomatiseerde gelaatsherkenning wordt toegepast.

Tabel 10

Toetsing scenario 2.2

Beginsel	Aan voldaan?
Rechtmatig, noodzakelijke en doelbinding	Rechtmatigheid vloeit voort uit artikel 9 WPG. Aan de eis van noodzakelijkheid wordt voldaan als er geen andere middelen zijn om het probleem van veel voorkomende criminaliteit tegen te gaan. Daarnaast dient het middel proportioneel te zijn en moet deze afweging per geval gemaakt worden.
Juist en nauwkeurig	Hieraan wordt voldaan als de gegevens juist en volledig zijn. Hierop moet controle zijn en dit moet worden bijgehouden.

Scenario 3.1 & scenario 3.2

Bij scenario 3 is het doel het zo snel mogelijk opsporen van daders van veel voorkomende criminaliteit. Dit kan zowel buiten heterdaad als op heterdaad. Buiten heterdaad wordt er achteraf gekeken of de persoon, die te zien is op de bewakingsbeelden, een bekende is van de politie. Op heterdaad wordt er gekeken of de persoon, welke te zien is op bewakingsbeelden, nog terug te vinden is in het winkelcentrum.

Om te bepalen of dit scenario binnen de kaders van de wet past dient er opnieuw een afweging te worden gemaakt tussen de noodzakelijkheid van het behalen van het doel en de inbreuk op de persoonlijke levenssfeer die plaatsvindt. In het geval van heterdaad is de inbreuk op de persoonlijke levenssfeer van onschuldige burgers hoog. Iedereen in het winkelcentrum wordt immers vergeleken met de persoon op de bewakingsbeelden. In het geval van buiten heterdaad is deze inbreuk lager. Dit komt doordat de persoon op de bewakingsbeelden als een verdachte is in de zin van art. 27 Sv. Onschuldige burgers worden in dit geval niet vergeleken met personen uit een database. Of de verwerking proportioneel is zal opnieuw afhangen van de omstandigheden van het geval. Hierbij is het aannemelijk dat wanneer er een eenmalig incident plaatsvindt de afweging tussen het inzetten van geautomatiseerde gelaatsherkenning in een winkelcentrum om deze dader op te sporen en de inbreuk op de persoonlijke levenssfeer zal neigen naar het niet inzetten van geautomatiseerde gelaatsherkenning. Dit omdat ernst van het feit niet opweegt tegen de inbreuk. Voor de rechtmatigheid dient er in dit geval gekeken te worden naar artikel 8 WPG. Het opsporen van daders en van delicten valt binnen de politietaak waardoor het verwerken van politiegegevens in dit geval zijn verwerkingsgrondslag vindt in artikel 8 WPG.

Bij scenario 3 is het volgens de WPG mogelijk om politiegegevens te verwerken op grond van artikel 8 WPG. Of dit verder noodzakelijk en proportioneel is hangt af van de omstandigheden van het geval. Dit geldt vooral voor het opsporen op heterdaad omdat hier de inbreuk op de persoonlijke levenssfeer van onschuldige burgers hoger ligt. Wanneer er gesproken wordt over opsporen buiten heterdaad is het wel mogelijk om binnen de kaders van de wet geautomatiseerde gelaatsherkenning toe te passen. Hierbij wordt geautomatiseerde gelaatsherkenning achteraf toegepast en zal de inbreuk op de persoonlijke levenssfeer nauwelijks een rol spelen.

4.1.2.3. Schematisch overzicht

In figuur 4 wordt een schematisch overzicht weergegeven van het juridische inzetkader van de verschillende scenario's.

	Scenario 1	Scenario 2.1	Scenario 2.2	Scenario 3.1	Scenario 3.2
Vorm van gebruik	Gelaatsherkenning in Villa B	Gelaatsherkenning in eigen pand/winkel	Gelaatsherkenning in winkels/winkelcentra	Gelaatsherkenning in winkelcentra, in de openbare ruimte	Gelaatsherkenning in winkelcentra, in de openbare ruimte
Juridisch kader	Art 6 lid 1 onder a jo. Art. 9 lid 2 onder a AVG	Art 6 lid 1 onder f jo. Art. 10 AVG of art. 6 lid 1 onder f AVG jo. Art. 9 lid 2 onder f AVG jo. Art 29 UAVG	Artikel 9 Wpg	Artikel 8 Wpg	Artikel 8 Wpg
Doelbinding	Gelaatsherkenning t.b.v. inzicht werven in de mogelijkheden en reacties van de medewerkers	Gelaatsherkenning t.b.v. speciale preventie van VVC in eigen omgeving (private partij)	Gelaatsherkenning t.b.v. speciale preventie van VVC door publieke partij	Gelaatsherkenning t.b.v. opsporing heterdaad	Gelaatsherkenning t.b.v. buiten heterdaad
Bevoegde autoriteit	Verwerkingsverantwoordelijke Villa B	Verwerkingsverantwoordelijke (winkelier of eigenaar pand)	Politie onder leiding van de Korpschef	Politie onder leiding van de Korpschef	Politie onder leiding van de Korpschef
Proportionaliteitsvereiste	Systeem staat alleen aan tijdens kantoortijden en ten tijde van de proef. Wanneer de het verwerken van gegevens niet langer noodzakelijk is stopt de verwerking en worden de beelden vernietigd	Systeem staat alleen aan op momenten waarop VVC voorkomt.	Systeem staat alleen aan op moment waarop VVC vaak voorkomt	Systeem gaat alleen aan op het moment dat er een melding is van een strafbaar feit. Er dient sprake te zijn van verdenking van een strafbaar feit.	Systeem wordt alleen gebruikt nadat er melding is gemaakt van een strafbaar feit en de dader in e database gezocht wordt. Er dient sprake te zijn van verdenking van een strafbaar feit.
Verwerkingstermijn	Zolang noodzakelijk voor het bereiken van het doel	Zolang noodzakelijk is voor het bereiken van het doel van de verwerking	Zolang noodzakelijk is voor het doel van de verwerking	Voor de duur van 5 jaar	Zolang noodzakelijk is voor het doel van de verwerking

Figuur 4. Juridische kaders (publiek/privaat) inzake gelaatsherkenning

4.3. Mogelijkheden en beperkingen

In de laatste paragraaf van dit hoofdstuk worden de mogelijkheden en beperkingen, welke naar voren zijn gekomen in de voorgaande paragrafen, beschreven. Welke mogelijkheden er zijn wordt aan de hand van paragraaf 4.2 uitgezet. De beperkingen worden besproken aan de hand van het geschetste wettelijke kader en geraadpleegde literatuur.

Mogelijkheden

Er zijn een aantal mogelijkheden met betrekking tot het inzetten van geautomatiseerde gelaatsherkenning. Voor elk van de scenario's geldt dat er een wettelijke grondslag is voor het inzetten van geautomatiseerde gelaatsherkenning. Vooral op het gebied van het verwerken van persoonsgegevens door private partijen zijn veel mogelijkheden. Dit omdat de verwerkingsgrondslagen wat ruimer zijn en niet bepaald worden door de wet. Hierbij wordt het doel door de partij zelf bepaald. Bij het inzetten van geautomatiseerde gelaatsherkenning door de politie is het wat minder eenvoudig. Zo speelt de eis van proportionaliteit en noodzakelijkheid hier juist een grote rol. Ondanks dat er verwerkingsgrondslagen zijn voor de verwerking dient er in elk afzonderlijk geval een afweging gemaakt te worden tussen de noodzakelijkheid van het inzetten van het middel en de inbreuk op de persoonlijke levenssfeer.

Beperkingen

Naast de mogelijkheden die in de paragraaf hierboven zijn genoemd zijn er juridisch ook beperkingen te benoemen wanneer het gaat om het inzetten van geautomatiseerde gelaatsherkenning. Zo is de juridische basis voor het gebruiken van technologie vaak onduidelijk en zijn de regels breed waardoor men eigen

invulling verwacht (Custers & Vergouw, 2015). Dit is ook terug te zien in het wettelijk kader dat in de eerste twee paragrafen van dit hoofdstuk is geschetst en die terug te vinden zijn in bijlage 2 en 3 van dit onderzoek. Er zijn mogelijkheden met betrekking tot het inzetten van geautomatiseerde gelaatsherkenning, echter zijn er veel bepalingen nog ruim en bieden ze mogelijkheid voor eigen interpretatie. Het is bijvoorbeeld niet duidelijk wanneer het inzetten van geautomatiseerde gelaatsherkenning proportioneel is, dit moet de verwerkingsverantwoordelijke zelf invullen en afwegen. Daarnaast is het begrijpelijk dat het voor een leek, zoals bijvoorbeeld een winkelier, lastig is om wetteksten te lezen en te begrijpen. Dit bemoeilijkt de plichten die de winkelier als gebruiker zou moeten uitvoeren. Een volgende beperking is dat er al veel verschillende camera's in het publieke en private domein zijn. Hierdoor zijn er verschillende eigenaren van zowel de camera's als de beelden. Deze camera's streven al een bepaald doel na. Camera's worden steeds gemeenschappelijker waardoor het lastig is te bepalen wie de beelden mag gebruiken. Het kan bijvoorbeeld zo zijn dat de camera eigendom is van de gemeente en op die plek hangt met een bepaald doel, mag de politie dan dezelfde camera gebruiken om hierop geautomatiseerde gelaatsherkenning toe te passen? Toezicht, zaaksbeveiliging en bestrijding van criminaliteit en overlast lopen hier door elkaar, hierbij moet er wel goed gekeken worden of de doelen ook daadwerkelijk nagestreefd worden en of het gebruik van de camera's wettelijk is. Dit is nog lastig te bepalen (Engberts & Copini, 2016).

5. ETHISCHE ASPECTEN

In dit hoofdstuk worden de antwoorden op deelvraag 2 en 3 van deze thesis besproken. Er wordt aan de hand van de bestudeerde literatuur bekeken welke ethische aspecten een rol spelen bij het inzetten van geautomatiseerde gelaatsherkenning door zowel private partijen, zoals een winkelier, en publieke partijen, zoals de politie. Vervolgens wordt er aan de hand van de afgenomen interviews besproken welke ethische aspecten, volgens de medewerkers van Villa B, een rol spelen. Hierbij wordt er een onderscheid gemaakt tussen de mening van de respondenten over het inzetten van geautomatiseerde gelaatsherkenning bij de preventie en bij de opsporing van veel voorkomende criminaliteit. Op deze manier kan er, op zowel deelvraag 2 als deelvraag 3, aan het einde van dit hoofdstuk een antwoord worden geformuleerd.

5.1. Literatuuroverzicht ethische aspecten geautomatiseerde gelaatsherkenning

Allereerst beschrijven Engberts en Copini (2016) dat met de komst van nieuwe sensoren het voor de burger steeds lastiger wordt om zichzelf te zijn. De burger wordt steeds meer in de gaten gehouden ondanks dat de inzet van deze sensoren wellicht binnen de kaders van de wet valt. Met geautomatiseerde gelaatsherkenning worden beelden gekoppeld aan persoonlijke data. Hierdoor zal het steeds lastiger worden om anoniem te kunnen bewegen, iedereen wordt voortdurend gezien. Deze herkenning zou kunnen leiden tot het sturen van bepaald gedrag, de burger houdt hiermee rekening (Olsthoorn, 2017). Zo kan iemand bijvoorbeeld een bepaalde route ontwijken omdat hier gelaatsherkenning wordt toegepast. Een volgend ethisch aspect wordt beschreven door Bouma en collega's (2014). Intelligente camera's, zoals camera's met geautomatiseerde gelaatsherkenning, kunnen een grotere impact hebben op de privacy van de burger dan de reguliere camera's. Dit zou zich negatief kunnen uiten. Zo kunnen er biases in het systeem zitten ten opzichte van bepaalde bevolkingsgroepen of kunnen de toezichthouders selecteren op huidskleur, kleding of gedrag. Het ethische aspect dat hier een rol speelt betreft het aspect van ongelijke behandeling. Een mogelijkheid om de privacy van burgers te beschermen is privacy-by-design waardoor in het systeem een methode wordt ingebouwd dat bijvoorbeeld mensen blurt bij niet-herkenning (Bouma et. al., 2014; Engberts & Copini, 2016). Naast dat intelligente camera's een grotere inbreuk hebben op de privacy van burgers wordt dit ook als een grotere inbreuk ervaren dan de waarneming van een opsporingsambtenaar. Beelden worden immers opgenomen en de waarneming van een opsporingsambtenaar niet (Politie, 2012).

Ondanks ethische bezwaren voor het inzetten van nieuwe sensoren is de verminderde privacy van burgers vrijwel onontkoombaar. Dit komt onder andere doordat er nieuwe ontwikkelingen op technisch gebied plaatsvinden. Deze ontwikkelingen worden door burgers zelf gebruikt, hierbij kan bijvoorbeeld gedacht worden aan het gebruik van Facebook of het inzetten van beveiligingscamera's. Een organisatie, zoals de politie, kan hierin vaak niet achterblijven en ontwikkelt zich daarom ook op technisch gebied. Camera's worden steeds beter en nieuwe sensoren worden ingezet. Daarnaast is er steeds meer informatie te vinden via social media. De burger gaat hierdoor voorzichtiger om met zijn of haar gegevens, ook omdat het vaak voor de burger niet duidelijk is wat er met de gegevens gebeurt. Tevens komen andere ethische

waarden zoals het recht op gelijke behandeling, menselijke waardigheid en autonomie ter discussie. Dit doordat geautomatiseerde gelaatsherkenningssystemen biases kunnen bevatten doordat het bijvoorbeeld de ene bevolkingsgroep beter herkent dan een andere bevolkingsgroep. Hierdoor zorgt geautomatiseerde gelaatsherkenning voor een ongelijke behandeling tussen bepaalde groepen. Wanneer een dader met een donkere huidskleur wel herkend wordt, doordat de software bijvoorbeeld beter is in het herkennen van donkere personen, en een persoon met een lichte huidskleur niet, dan is er sprake van ongelijke behandeling. Wanneer de software is ontwikkeld in een westers land zullen westerse burgers sneller worden herkend en zullen hierbij minder false positives[13] voorkomen dan niet-westerse burgers (Technologiescan, 2017; De Keizer, 2018). Autonomie komt ter discussie doordat de bewegingsvrijheid van de burger ter discussie komt. Zoals hierboven vermeld kan de burger geautomatiseerde gelaatsherkenning beleven op een manier waarbij de burger zich constant in de gaten gehouden voelt. Technologie kan de autonomie vergroten maar kan dit ook verminderen doordat de burger bijvoorbeeld geen optimale bewegingsvrijheid geniet of doordat de burger de technologie niet zelf in de hand heeft (Vonk & Dorrestijn, z.j.). Menselijke waardigheid wordt vaak gezien als het recht op privacy. Dit kan geschonden worden doordat met geautomatiseerde gelaatsherkenning het recht op privacy in het geding komt. Zo kan er bijvoorbeeld misbruik gemaakt worden van de beelden en kan identiteit gestolen worden. Dit kan de waardigheid aantasten (Amnesty International, z.j.). Daarnaast moet zowel de politie als de burger zich afvragen of het inzetten van geautomatiseerde gelaatsherkenning bij bepaalde vormen van criminaliteit ook wenselijk is. Het gaat in dit geval niet alleen om het kunnen en mogen maar ook om de wil van de burger en de mens in het algemeen. Het kan de veiligheid wel bevorderen en de criminaliteitscijfers naar beneden halen maar is de burger bereid om hiervoor zijn of haar privacy en een deel van zijn of haar vrije wil op te geven? Vindt de burger het wenselijk om constant in de gaten gehouden te worden? Een ander vraagstuk dat speelt is wie straks verantwoordelijk zal zijn voor de fouten die gemaakt kunnen worden. Wanneer er een false positive is of een false negative[14], wie wordt hier dan op aangesproken? In het geval van geautomatiseerde gelaatsherkenning is een software die zorgt voor de herkenning van een mogelijke dader. Wanneer achteraf blijkt dat de software de verkeerde persoon aanwijst als dader kan het lastig zijn te bepalen wie er schuldig is. Is dit dan de ontwikkelaar of het systeem zelf of wellicht een ander persoon? Daarnaast kan het de bewijslast vereenvoudigen maar ook bemoeilijken. Wanneer iemand op heterdaad wordt betrapt door een opsporingsambtenaar maar niet wordt herkend als dader door het gezichtsherkenningssysteem wordt het lastig om te bepalen op wat we dan moeten afgaan. Een andere vraag die speelt is of we ons wel moeten richten op het opsporen van strafbare feiten en het optreden achteraf. De verwachting is dat de oorzaken van crimineel gedrag steeds meer bekend zullen worden. Zo kunnen genetische afwijkingen of sociale omstandigheden leiden tot het vertonen van crimineel gedrag. Er zijn groepen die beargumenteren dat, bij het voorkomen van crimineel

[13] Wanneer het systeem een herkenning aangeeft terwijl deze fout is.
[14] Wanneer het systeem geen herkenning aangeeft terwijl het referentiemateriaal en het vergelijkingsmateriaal hetzelfde zijn.

gedrag, hierop gefocust moet worden in plaats van het inzetten van sensoren om achteraf op te treden (Technologiescan, 2017).

Een ander bezwaar is dat het niet duidelijk is hoe beelden bewaard worden en hoelang deze beelden bewaard worden. Het is niet bekend hoe de databank wordt bijgehouden en hoe de controle hierop werkt. Geautomatiseerde gelaatsherkenning mag toegepast worden indien de politie zich aan alle regels houdt en data wordt verwijderd wanneer dit verwijderd moet worden. Of dit echter zo gebeurt, is nog maar de vraag (Olsthoorn, 2017; Zenger, 2016). Ook heerst de angst voor een datalek[15] of misbruik van de software. Wat als het mogelijk is om door middel van een foto of een 3D-model gezichtsherkenning mogelijk is? (Olsthoorn, 2017). Een pincode of nieuw wachtwoord is zo aan te vragen. Een gezicht is echter niet zo eenvoudig te veranderen. In dit geval kan identiteitsfraude het slachtoffer zijn of haar hele leven lang volgen (Bijbel en Overheid, 2017).

Tenslotte beargumenteerd Zenger (2016) dat zowel de burger als de politie zich dient af te vragen waar de grens ligt. Omdat we iets kunnen moeten we dit nog niet persé willen. Als de samenleving op deze manier doorgaat kan straks alles in beeld worden gebracht. Ook wat de relatie van iemand is, waar de persoon is geweest en wat deze persoon koopt. Dit is ook een belangrijk vraagstuk voor het Programma Sensing (Programma Sensing, 2017).

Vanuit de literatuur zijn er een aantal ethische aspecten aan bod gekomen. Zo kunnen burgers het gevoel krijgen dat zij constant in de gaten gehouden worden wat de bewegingsvrijheid kan verminderen. Daarnaast is het mogelijk dat er ongelijke behandeling van bepaalde bevolkingsgroepen plaats kan vinden doordat er biases in systemen kunnen zitten. Een ander ethisch aspect is de inbreuk dat gemaakt wordt op de privacy van burgers. Deze is groter met geautomatiseerde gelaatsherkenning dan wanneer een opsporingsambtenaar een delict waarneemt, dit wordt immers niet opgenomen. Verder komen de rechten als menselijke waardigheid en autonomie ter discussie te staan. Vervolgens is het belangrijk om na te denken of het inzetten van geautomatiseerde gelaatsherkenning in de geschetste scenario's wel wenselijk is. Wanneer we dit kunnen en mogen hoeven we dit nog niet te willen. Wil de burger een deel van zijn of haar vrijheid opgeven voor dit specifieke doel? Daarnaast is het nog de vraag wie er verantwoordelijk is in het geval van een fout. Er zijn meerder partijen die bij geautomatiseerde gelaatsherkenning een rol spelen, van de ontwikkelaar tot de gebruiker, wie in dit geval verantwoordelijk is, is niet duidelijk. Daarnaast speelt hier de vraag of er niet meer aandacht moet naar factoren zoals de sociale omgeving of genetische factoren. Wellicht kan er, wanneer het gaat om het tegengaan van criminaliteit, meer bereikt worden door te kijken naar de oorzaken hiervan. Verder speelt het dilemma of de politie te vertrouwen is wanneer het gaat om het naleven van de regels omtrent het bewaren van data. Het is niet duidelijk wat de politie met de data doet en

[15] 'Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie' (https://autoriteitpersoonsgegevens nl/nl/onderwerpen/beveiliging/meldplicht-datalekken)

wanneer dit verwijderd wordt. Tenslotte is het nog de vraag of we ook alles moeten willen wat we kunnen. Gaat het inzetten van geautomatiseerde gelaatsherkenning niet te ver?

Uit bovenstaande blijkt dat er een aantal ethische vraagstukken steeds opnieuw naar voren komen. Deze ethische aspecten worden beschreven naar aanleiding van het inzetten van geautomatiseerde gelaatsherkenning in het algemeen. Of deze ethische aspecten hetzelfde zijn in elke situatie wordt aan de hand van de bestudeerde literatuur niet duidelijk. De aspecten kunnen wellicht anders zijn wanneer het gaat op opsporing of om preventie. Daarnaast kunnen deze aspecten verschillen ten behoeve van verschillende situaties of soorten delicten. Dit wordt niet in de literatuur beschreven. Specifieke casussen worden niet besproken. Om deze reden kan het interessant zijn om ethische aspecten niet alleen vanuit de literatuur te bekijken maar ook om deze te bestuderen aan de hand van interviews. Met een interview is inzicht verworven in de ethische aspecten in specifieke situaties. Aan de hand van de interviews met medewerkers van Villa B is getracht om eventuele verschillen in kaart te brengen.

5.2. Interviews met deelnemers Villa B over ethische aspecten van geautomatiseerde gelaatsherkenning

Aan de hand van interviews met de deelnemers van de proef met geautomatiseerde gelaatsherkenning in Villa B is er getracht een eerste beeld te schetsen over de ethische vraagstukken die een rol kunnen spelen bij het inzetten van geautomatiseerde gelaatsherkenning ten behoeve van het voorkomen en opsporen van veel voorkomende criminaliteit in winkelcentra. In totaal zijn er 14 respondenten geïnterviewd. Uit gesprekken met de coördinator evaluatie en onderzoek van het Programma Sensing (persoonlijke communicatie, 11 december 2018) blijkt dat het voor het Programma Sensing belangrijk is om, bij het inzetten van nieuwe sensoren, een verkenning te doen naar ethische vraagstukken. Zoals uit het methodehoofdstuk van deze thesis is gebleken is het, in dit stadium van het onderzoek, nog niet wenselijk om een enquête uit te zetten onder de gehele Nederlandse bevolking. Om toch een eerste verkenning naar mogelijke ethische aspecten te kunnen uitvoeren zijn medewerkers van het Programma Sensing bevraagd. Uit de interviews kunnen ethische aspecten naar voren komen waar de politie rekening mee dient te houden wil zij geautomatiseerde gelaatsherkenning toepassen voor het voorkomen en opsporen van veel voorkomende criminaliteit in winkelcentra. Wanneer het ethisch niet verantwoord blijkt te zijn en de acceptatie van de burger niet aanwezig is bij het inzetten van geautomatiseerde gelaatsherkenning kan dit een negatief effect met zich meebrengen. Vanuit het Programma Sensing is samenwerking met de burger belangrijk, zonder acceptatie kan dit de samenwerking belemmeren.

De respondenten die zijn bevraagd zijn bevraagd naar hun mening. Hierbij is er getracht een onderscheid te maken tussen de mening van de geïnterviewde als burger en de geïnterviewde als politieagent(e). De geïnterviewde respondenten doen mee aan het onderzoek in hun rol als werknemers, er wordt immers niet getracht een delict te voorkomen of op te sporen. Echter is er in de interviews ook bevraagd of de respondenten anders over het inzetten van geautomatiseerde gelaatsherkenning denken

wanneer het gaat om het vervullen van hun rol als politieagent(e). Zijn er andere ethische aspecten die een rol spelen wanneer de respondent een bepaald delict wilt voorkomen of opsporen en de respondent niet degene is waarop geautomatiseerde gelaatsherkenning wordt toegepast maar waarbij de respondent degene is de geautomatiseerde gelaatsherkenning gebruikt om zijn/haar werk te vergemakkelijken.

In de onderstaande paragrafen zullen de resultaten uit de interviews worden besproken. Deze worden besproken aan de hand van de topics, welke terug te vinden zijn in tabel 5. Vervolgens zal er een onderscheid gemaakt worden tussen geautomatiseerde gelaatsherkenning als opsporingsmiddel en geautomatiseerde gelaatsherkenning al preventiemiddel. Bij geautomatiseerde gelaatsherkenning als opsporingsmiddel wordt het systeem zowel achteraf toegepast als op live camerabeelden. Bij geautomatiseerde gelaatsherkenning als preventiemiddel wordt het systeem louter ingezet op live beelden. In onderstaande paragrafen wordt besproken of de mening van de respondenten hierin verschilt.

5.2.1. Juridische basis voor geautomatiseerde gelaatsherkenning

In de interviews is er onder andere gevraagd wat de respondenten verwachten dat de wettelijke mogelijkheden zijn voor het inzetten van geautomatiseerde gelaatsherkenning. De antwoorden op de vraag of zij een mogelijke juridische basis zien zijn terughoudend. Er zijn een aantal respondenten die denken dat er een juridische basis is voor het toepassen van geautomatiseerde gelaatsherkenning, het is immers ten behoeve van de opsporingstaak van de politie. Er zijn er echter ook een aantal respondenten die geen duidelijk antwoord weten te formuleren omdat zij geen jurist zijn of geen eerdere ervaring hebben met het gebruiken van sensoren bij de politietaak.

5.2.2. Ethisch aspecten van geautomatiseerde gelaatsherkenning

Allereerst is de mening van de respondenten gevraagd over het inzetten van geautomatiseerde gelaatsherkenning in scenario 1, in Villa B. Alle respondenten hebben toestemming gegeven om deel te nemen aan de proef. Bij het vragen naar de toestemming waren een aantal deelnemers niet meteen overtuigd. Het merendeel van de deelnemers deed mee aan de proef omdat het binnen de Villa plaatsvond en doordat het zich afspeelde ten behoeve van informatie verzamelen voor het onderzoek. De respondenten waren zich ervan bewust dat het systeem louter gebruikt werd ten behoeve van de proef, om te zien wat voor soort data er gegenereerd wordt en om de reacties van de medewerkers in kaart te brengen. De respondenten die in eerste instantie niet wilden deelnemen hadden hiervoor verschillende beweegredenen. Zo wilde een respondent in eerste instantie niet deelnemen omdat er volgens hem/haar al voldoende onderzoek naar geautomatiseerde gelaatsherkenning was gedaan. Waarom zou er nog een onderzoek hiernaar gedaan moeten worden? Een ander argument dat gebruikt werd is dat de respondent zich in de gaten gehouden zou voelen op zijn of haar werk. Dit doordat er altijd teruggekeken kan worden naar de beelden. Uiteindelijk hebben alle 14 respondenten toestemming verleend. Dit omdat zij nieuwsgierig waren

naar de resultaten van het onderzoek en omdat zij overtuigd waren van het feit dat de gegevens louter gebruikt werden voor de proef en vervolgens zouden worden verwijderd.

Vervolgens zijn de vragen gesteld met betrekking tot het inzetten van geautomatiseerde gelaatsherkenning in winkelcentra. Het merendeel van de respondenten is van mening dat het toepassen van geautomatiseerde gelaatsherkenning voor veel voorkomende criminaliteit een te grote inbreuk op de privacy van de burger met zich meebrengt. Slechts 4 van de respondenten zijn van mening dat geautomatiseerde gelaatsherkenning in alle omstandigheden en voor elk soort delict toegepast mag worden. Een argument dat vaak wordt gebruikt is dat wanneer een persoon onschuldig is en niets te verbergen heeft het niet erg is dat geautomatiseerde gelaatsherkenning wordt toegepast. Zij zijn van mening dat het niet erg is al wordt geautomatiseerde gelaatsherkenning toegepast, zij hebben immers niets te verbergen. Daarentegen wordt in de interviews ook meerdere keren beargumenteerd dat de respondenten zich juist gevolgd zullen voelen door het toepassen van geautomatiseerde gelaatsherkenning. Op deze manier kan er altijd teruggekeken worden waar iemand is geweest, dit zou het onveiligheidsgevoel juist kunnen vergroten. Daarnaast is het merendeel van de respondenten van mening dat wanneer geautomatiseerde gelaatsherkenning wel wordt toegepast de doelen hieromtrent duidelijk moeten zijn. Wanneer de doelen duidelijk zijn en het duidelijk is wat er gedaan wordt met de data, waar de data wordt opgeslagen, wanneer de data wordt verwijderd en onder welke voorwaarden het gezicht wordt opgeslagen dan zullen zij sneller accepteren dat geautomatiseerde gelaatsherkenning wordt toegepast.

Wanneer er gevraagd wordt naar de positieve kanten van het inzetten van geautomatiseerde gelaatsherkenning zijn er een aantal respondenten die juist denken dat geautomatiseerde gelaatsherkenning het veiligheidsgevoel van burgers kan vergroten. Daarnaast zijn er ook een aantal respondenten die verwachten dat de werkdruk voor de politie wordt verlaagd. Het werk ten behoeve van preventie en opsporing zal naar hun verwachting verminderen omdat het geautomatiseerde gelaatsherkenningssysteem een deel van het werk overneemt, er hoeven dan minder agenten op straat te worden ingezet. Echter wordt de werkdruk ook een aantal keren als negatieve kant van geautomatiseerde gelaatsherkenning benoemd. Wanneer geautomatiseerde gelaatsherkenning wordt toegepast zullen er meer meldingen komen waar opvolging op moet komen. Zonder geautomatiseerde gelaatsherkenning zal er niet altijd sprake zijn van ontdekking van een veel voorkomend delict of zal er niet altijd aangifte worden gedaan. Hierdoor heeft de politie minder werk doordat er minder strafbare feiten zijn waar de politie kennis van heeft. Wanneer geautomatiseerde gelaatsherkenning wordt toegepast zal het aantal meldingen stijgen doordat er meer verdachten worden herkend. Wanneer er geen opvolging volgt zal het middel uiteindelijk niet effectief zijn waardoor volgens deze respondenten de werkdruk juist wordt verhoogd. Het aantal bekende delicten zal immers hoger zijn.

Een ander punt waar veel respondenten het over eens zijn is dat er voor nu nog niet voldoende informatie beschikbaar is. Geautomatiseerde gelaatsherkenning is nog niet genoeg onderzocht om het effectief te kunnen inzetten. Vooraf dient er onderzocht te worden wat er met het systeem gedaan kan worden, welke data er verkregen wordt, wat er met de data gebeurd, wie de eigenaar is van de data, wanneer de data wordt verwijderd, enzovoort. Systemen moeten optimaal presteren waardoor het aantal foute meldingen nihil wordt. Op deze manier zullen onschuldige burgers er het minste last van

ondervinden. Er moet volgens de respondenten meer onderzoek gedaan worden willen zij duidelijke uitspraken kunnen doen of het middel ooit, voor welk delict dan ook, toegepast kan worden. Hierbij is het tevens belangrijk dat er een aantal respondenten zijn die menen nog niet genoeg vertrouwen te hebben in geautomatiseerde gelaatsherkenning. Er zouden nog te veel foute matches zijn waardoor het vertrouwen in het middel nog niet voldoende is. Dit is tevens een argument dat gebruikt wordt om tegen geautomatiseerde gelaatsherkenning te zijn totdat de software verbeterd wordt en voldoende werkt.

Tevens is er aan de respondenten gevraagd of zij anders denken over het inzetten van geautomatiseerde gelaatsherkenning wanneer zij, vanuit hun rol als politieagent(e), zelf degene zijn die geautomatiseerde gelaatsherkenning toepast. De twee respondenten die van mening waren dat geautomatiseerde gelaatsherkenning onder geen enkele omstandigheid wenselijk is blijven bij hun mening, ook wanneer zij de verwerker zouden zijn en het hun werk makkelijker zou maken. Er waren, zoals hierboven vermeld, 4 respondenten die geen enkel probleem hadden bij het inzetten van geautomatiseerde gelaatsherkenning, dit was voor hen niet anders wanneer zij de verwerker zouden zijn. Een groot deel van de overige respondenten vonden dit een lastige vraag. Dit omdat zij zelf geen ervaring hadden met politiewerk en zij vooral werken voor het Programma Sensing ten behoeve van communicatie, planning, onderzoek, strategie enzovoort. Zij konden zich moeilijk voorstellen hoe zij over geautomatiseerde gelaatsherkenning zouden denken wanneer dit hun werk zo vergemakkelijken. Twee van de respondenten beargumenteerden echter dat zij het, vanuit hun rol als politieagent(e), wel graag zouden willen toepassen. Dit zou volgens hen namelijk het werk makkelijker maken en zij zien hierbij ook minder tegenargumenten. De persoon in kwestie heeft immers wat gedaan of gaat wat doen dus waarom zou het dan niet toegepast mogen worden? Opvallend hierbij was dat zij anders over het inzetten van geautomatiseerde gelaatsherkenning dachten wanneer zij degene waren die als het ware in de gaten gehouden werden. Daarnaast was er een respondent die ook wel nadelen ziet in het toepassen van geautomatiseerde gelaatsherkenning. Wanneer een politieagent(e) getuige is van een delict en het geautomatiseerde gelaatsherkenningssysteem de dader niet herkent, terwijl de agent(e) zeker is van de schuld van de persoon, dit onnodige frustraties zal veroorzaken.

5.2.3. Grenzen van het inzetten van geautomatiseerde gelaatsherkenning

Wanneer er vragen worden gesteld die betrekking hebben op de grenzen van het inzetten van geautomatiseerde gelaatsherkenning lopen de meningen uiteen. Zo zijn er een viertal respondenten die vinden dat geautomatiseerde gelaatsherkenning toegepast mag worden voor welk delict dan ook. De rest van de respondenten zijn van mening dat geautomatiseerde gelaatsherkenning een te zwaar middel is voor veel voorkomende criminaliteit. Dit komt voornamelijk doordat de inbreuk op de persoonlijke levenssfeer hier niet opweegt tegenover de impact en de zwaarte van het delict. Dit hangt ook van het delict af, er is geen duidelijke grens aan te wijzen. Zo is er, aldus een respondent, namelijk een verschil tussen het stelen van een mars en het stelen van 40 Rolexen. Dit gaat tegelijkertijd gepaard met de impact op de burger en winkelier. Wanneer het gaat om een gewapende overval waarbij geld uit de kassa wordt gestolen is de

impact hoger waardoor de respondenten eerder geneigd zijn zwaardere opsporingsmiddelen, zoals geautomatiseerde gelaatsherkenning, in te zetten. Deze grens ligt bij iedere respondent anders. De ene respondent kan voor zichzelf duidelijk de grens aanwijzen tussen wanneer het wel geoorloofd is om geautomatiseerde gelaatsherkenning in te zetten en wanneer niet. De andere respondent vindt dit nog erg lastig en laat het afhangen van de omstandigheden van het geval en wat de toekomst ons zal leren over de mogelijkheden en onmogelijkheden van geautomatiseerde gelaatsherkenning. Wanneer het om terrorisme gaat zijn 12 van de 14 respondenten het met elkaar eens. In dit geval zal de politie alle middelen mogen inzetten om de terrorist te pakken of de aanslag tegen te gaan. Twee respondenten zijn het hier echter niet mee eens. Zij zijn van mening dat de wereld niet de goede kant opgaat wanneer er elke keer nieuwe sensoren en technologieën op de markt worden gebracht en worden ingezet. Volgens hen zou dit juist te veel gevaren met zich meebrengen en zullen er nieuwe vormen van criminaliteit kunnen ontstaan. Daarnaast zou dit lang niet altijd effectief werken. Een van de respondenten is zelfs van mening dat wanneer er nog meer technologieën worden ingezet de kwaliteit van het leven achteruit gaat. Het vermindert de bewegingsvrijheid van de mens, het vermindert sociale contacten. Deze respondent meende dan ook, samen met de andere respondent die tegen geautomatiseerde gelaatsherkenning is, dat onze samenleving zich niet moet richten op het inzetten van middelen achteraf. Nederland moet zich meer richten op sociale en genetische factoren die een oorzaak kunnen zijn voor het plegen van criminaliteit. Dit zal volgens hen goedkoper zijn en effectiever wanneer het gaat om preventie. Wanneer de agent op straat een praatje maakt met burgers of met personen die zich verdacht gedragen zal dit wellicht ook een positief effect hebben op de preventie en opsporing.

Daarnaast zijn er meerdere respondenten die geautomatiseerde gelaatsherkenning, indien het toegepast wordt, graag alleen toegepast zien worden door de politie. Dit komt doordat het vertrouwen in de politie hoger ligt dan het vertrouwen in private partijen. Zij zijn bang dat er bij private partijen eerder een datalek op zal treden of dat er misbruik wordt gebruikt van de data. Dit zou kunnen betekenen dat de partijen de data doorverkopen en hierdoor winst maken maar ook doordat er per ongeluk een datalek ontstaat en er misbruik kan worden gemaakt van persoonlijke gegevens. Er zijn meerdere respondenten die angst uiten voor identiteitsfraude. De respondenten zijn bang dat het ontstaan van een datalek sneller voorkomt bij een private partij doordat zij technisch vaak minder middelen hebben. Daarnaast is er een respondent die niet graag gegevens afstaat aan een private partij omdat hij of zij van mening is dat deze partij haar technologie kan verbeteren. Zo geeft de respondent het voorbeeld van het geautomatiseerde gelaatsherkenningssysteem in Villa B. Wanneer het systeem niet zeker was van een match werd dit bevraagd aan de verwerkers. Op deze manier kan het systeem haar algoritme verbeteren en was er steeds minder vaak sprake van een foutieve herkenning of niet-herkenning. Bij de politie is de controle volgens hen groter en is de kans op misbruik van de data kleiner.

Een volgende factor dat driemaal ter sprake kwam was dat het inzetten van geautomatiseerde gelaatsherkenning ook afhangt van de persoon die aan de macht is. Zo werd er een voorbeeld genoemd dat er in Nederland veel joden zijn vermoord tijdens de Tweede Wereldoorlog doordat in Nederland goed werd bijgehouden wie waar woonden. Ons bevolkingsregister was op orde. Hierdoor waren personen makkelijker te vinden. Een voorbeeld van zo'n database nu is CATCH. Hierin is informatie terug te vinden

over alle Vreemdelingen in Nederland. Wat gebeurt er als een persoon met kwade bedoelingen aan de macht komt en bij de data kan? Zien we geautomatiseerde gelaatsherkenning dan nog steeds als een goed middel?

Wanneer er gevraagd wordt naar het inzetten van geautomatiseerde gelaatsherkenning als toegangsmiddel op Schiphol, werk of bijvoorbeeld een telefoon zijn de meningen verdeeld. Ongeveer de helft van de respondenten is van mening dat wanneer een techniek zoals geautomatiseerde gelaatsherkenning het leven makkelijker maakt en processen versneld het geen probleem is dat het toegepast wordt. Ongeacht wie het systeem toepast. Transparantie is hierbij belangrijk. Het moet duidelijk zijn wat het doel is van de verwerking en het moet ook duidelijk zijn wat er met de data wordt gedaan. Andere zijn weer van mening dat ook dan geautomatiseerde gelaatsherkenning niet betrouwbaar genoeg is, juist omdat in deze gevallen het vaak onduidelijk is wat er met de data wordt gedaan en wie bij de data kan.

Bij het vragen naar verschillen in mening tussen het inzetten van geautomatiseerde gelaatsherkenning achteraf en geautomatiseerde gelaatsherkenning op live beelden zijn de meningen verdeeld. Wanneer de respondenten gesproken worden, welke van mening zijn dat in alle gevallen geautomatiseerde gelaatsherkenning toegepast mag worden, is er geen verschil tussen het toepassen achteraf en het toepassen op live beelden. Dit maakt volgens hen niet uit, zolang de veiligheid wordt vergroot maakt het niet uit in welke situatie geautomatiseerde gelaatsherkenning wordt toegepast. Andere respondenten zijn van mening dat de grens bij het achteraf toepassen van geautomatiseerde gelaatsherkenning wat lager ligt dan bij het toepassen op live beelden. Bij het gebruiken van live beelden is de impact en de inbreuk op de persoonlijke levenssfeer van burgers is groter. Het achteraf zoeken naar bepaalde personen op beelden is volgens hen sneller toelaatbaar, de impact op de onschuldige burgers is hier minder groot omdat zij niet tegenover een hele databank met personen worden gehouden. De respondenten die van mening zijn dat geautomatiseerde gelaatsherkenning en andere technologieën te ver gaan zijn van mening dat in zowel het geval van achteraf als in het geval van live beelden geautomatiseerde gelaatsherkenning niet wenselijk is. Tot nog toe heeft de politie het altijd gered zonder geautomatiseerde gelaatsherkenning dus waarom moet het dan nu wel worden ingezet?

Naast grenzen en de factoren die hierboven zijn genoemd delen de respondenten voornamelijk één en dezelfde mening. Deze bedraagt dat er meer onderzoek gedaan moet worden naar geautomatiseerde gelaatsherkenning wil het in de toekomst ingezet kunnen worden als opsporings- of preventiemiddel. Er dient onderzoek gedaan te worden naar de mogelijkheden van het systeem, de data die verkregen wordt, wat er met de data gedaan wordt, wanneer de data verwijderd wordt enzovoort. Hierbij is het tevens van belang dat er onder de bevolking een onderzoek plaatsvindt. Wanneer blijkt dat geautomatiseerde gelaatsherkenning technisch mogelijk is en dit binnen de kaders van de wet ook mag moeten we dit als samenleving nog wel willen. Hierbij zijn de woorden “niet kunnen en mogen, maar willen” erg belangrijk. Acceptatie van de burgers speelt een belangrijke rol.

5.2.4. Het inzetten van geautomatiseerde gelaatsherkenning bij preventie vs. opsporing

Tevens is er in de interviews gekeken naar het onderscheid tussen het inzetten van geautomatiseerde gelaatsherkenning bij de opsporing en bij de preventie. De respondenten die geen problemen hebben bij het inzetten van geautomatiseerde gelaatsherkenning door de politie, zijn van mening dat de politie geautomatiseerde gelaatsherkenning voor zowel de opsporing als de preventie van veel voorkomende criminaliteit in mag zetten. De respondenten die nog niet zo enthousiast zijn over het inzetten van geautomatiseerde gelaatsherkenning zijn minder tegen het middel wanneer het gaat om de opsporing. Er is een duidelijk onderscheid te maken tussen het inzetten van geautomatiseerde gelaatsherkenning in de opsporing en het inzetten van geautomatiseerde gelaatsherkenning bij de preventie. Wanneer het gaat om de opsporing zijn de respondenten sneller geneigd geautomatiseerde gelaatsherkenning als een mogelijk opsporingsmiddel te zien. Het argument dat hiervoor wordt gebruikt is dat bij de opsporing van veel voorkomende criminaliteit de inbreuk op de privacy minder is. In dit geval wordt namelijk niet iedere burger vergeleken met het referentiemateriaal maar alleen de persoon die gezocht wordt. Dit is volgens het merendeel van de respondenten toelaatbaarder. Dit hangt echter nog steeds af van de kwaliteit en de mogelijkheden van het systeem. Wanneer het systeem niet optimaal werkt zien zij niet in waarom geautomatiseerde gelaatsherkenning toegepast moet worden bij de opsporing of bij de preventie. Zo is de mening tevens hier dat er eerst goed onderzoek gedaan moet worden naar de mogelijkheden van het systeem en dat het systeem eerst moet werken met een zo klein mogelijk foutenpercentage.

Daarnaast zijn de twee respondenten, die van mening zijn dat er meer aandacht moet naar de oorzaken van crimineel gedrag en er minder gefocust moet worden op het inzetten van technologie, van mening dat dit bij zowel de opsporing als preventie geldt. Ook in het geval van opsporing moet er niet meteen gedacht worden aan geautomatiseerde gelaatsherkenning of een andere technologie.

Uit de interviews komt naar voren dat er nog niet voldoende vertrouwen is in geautomatiseerde gelaatsherkenning en dat veel respondenten van mening zijn dat geautomatiseerde gelaatsherkenning voor veel voorkomende criminaliteit een te zwaar en ingrijpend middel is. Sommige zien wel mogelijkheden in geautomatiseerde gelaatsherkenning als bijvoorbeeld toegangsmiddel of middel bij terrorisme omdat hiervan de impact hoger ligt en de grenzen van de inzetmogelijkheden daarmee ook. Dit geldt tevens voor het inzetten van geautomatiseerde gelaatsherkenning als opsporingsmiddel tegenover het inzetten van geautomatiseerde gelaatsherkenning als preventiemiddel of het inzetten van geautomatiseerde gelaatsherkenning achteraf tegenover het inzetten van geautomatiseerde gelaatsherkenning op live beelden. Indien geautomatiseerde gelaatsherkenning ingezet wordt als opsporingsmiddel is een groot deel van de respondenten eerder geneigd het middel te aanvaarden. Vanuit hun rol als politieagent zijn de meningen verdeeld. Het merendeel van de respondenten weet geen antwoord te geven op de vraag of zij anders denken over het inzetten van geautomatiseerde gelaatsherkenning wanneer zij degene zijn die het gebruiken of niet. Daarentegen zijn er ook een aantal respondenten die de voordelen van geautomatiseerde gelaatsherkenning inzien wanneer het gaat vanuit hun rol als politieagent(e). Toch zou dit ook voor frustaties kunnen zorgen. Echter, speelt ook hier de rol dat de inbreuk niet te groot moet zijn en dat het

middel goed moet werken. Daarnaast zijn de respondenten van mening dat, voordat geautomatiseerde gelaatsherkenning wordt ingezet, er eerst voldoende onderzoek gedaan dient te worden. Dit naar zowel de mogelijkheden van het systeem, de data die gegenereerd wordt en de gevolgen.

Ethische aspecten, die op dit moment aangedragen kunnen worden als argumenten tegen het inzetten van geautomatiseerde gelaatsherkenning zijn samengevat in onderstaand schema om voor de verwerker inzichtelijk te maken wat de aandachtspunten zijn op het gebied van ethiek.

Figuur 5. Schematisch overzicht van ethische aspecten tegen het inzetten van geautomatiseerde gelaatsherkenning

6. TECHNISCHE ASPECTEN

In dit hoofdstuk wordt een antwoord op deelvraag 4 geformuleerd. De eerste technische aspecten die belangrijk zijn bij het inzetten van geautomatiseerde gelaatsherkenning worden besproken. Hierbij wordt er gekeken naar de mogelijkheden en beperkingen op technisch gebied. Dit wordt voornamelijk gedaan aan het onderzoek van het National Institute of Standard and Technology. Belangrijk bij het onderzoek van NIST is dat het softwareprogramma's evalueert die ontwikkeld zijn tot 2015, programma's die na 2015 zijn ontwikkeld zijn hierin niet opgenomen. Daarnaast is het belangrijk te vermelden dat het onderzoek van NIST niet kijkt naar de weersomstandigheden waarin de afbeeldingen zijn verkregen of biases die bepaalde systemen kunnen bevatten. Tevens doet NIST geen onderzoek naar geautomatiseerde gelaatsherkenning op live beelden. Het maakt gebruik van geautomatiseerde gelaatsherkenning op opnames die meerdere keren kunnen worden gebruikt en waarbij het niet per se belangrijk is dat hits zo snel mogelijk worden weergegeven. Het onderzoek van NIST evalueert een aantal systemen die gebruik maken van geautomatiseerde gelaatsherkenning. Deze zullen hier niet uitzonderlijk worden besproken. Wat in dit hoofdstuk wel wordt besproken zijn de technische moeilijkheden waar de systemen nog mee kampen en de mogelijkheden die de systemen wel hebben.

Volgens het NIST (Grother, Ngan & Quinn, 2017) zijn er bij automatische geautomatiseerde gelaatsherkenning een aantal moeilijkheden. Zo is het vergelijkingsmateriaal vaak niet vrijwillig afgegeven. Het zijn vaak beelden waarin één of zelfs meerdere gezichten kunnen zitten. Het beeld betreft meerdere resoluties, poses en condities met betrekking tot verlichting. Daarnaast bewegen de personen op de beelden vaak waardoor afbeeldingen van gezichten wazig kunnen zijn. Verder kunnen delen van het gezicht bijvoorbeeld worden bedekt door andere personen of voorwerpen die in het beeld zichtbaar zijn. Een derde moeilijkheid is dat de resolutie van de beelden tevens door andere aspecten wordt beïnvloed. Hierbij kan gedacht worden aan het gezichtsveld, kosten van de camera's en diepte. Tenslotte is het mogelijk dat er een false positive ontstaat waardoor personen in het publieke domein worden beschuldigd terwijl ze wellicht niet dezelfde persoon zijn als die in de database. Uit het onderzoek blijkt verder dat er altijd een percentage gevallen zal zijn waarin personen niet worden herkend of ontdekt. Dit komt doordat deze personen van de camera wegkijken, hun gezicht bedekken met zonnebrillen, een hoed dragen, doordat er andere personen voor hen staan of bijvoorbeeld doordat een persoon naar een telefoon kijkt in plaats van voor zich uit. Wanneer gezichtsherkenning in een ruimte zo accuraat mogelijk moet zijn moet er rekening gehouden worden met de plaats van de camera. Vanuit een aantal punten is het vaak onmogelijk om een goede afbeelding van het gezicht te verwerven, gezichtsherkenning werkt immers het beste wanneer er een frontale afbeelding van het gezicht is. Daarom is het belangrijk dat er van tevoren wordt nagedacht over de plaats van de camera, de richting van de camera en de hoek die de camera in beeld heeft. Een ander technisch aspect waar rekening mee gehouden dient te worden is het geheugen van de computers waar de systemen op werken. Bij het verkrijgen en als het ware verwerken van een gezicht gebruikt het softwareprogramma veel geheugen. Daarnaast kan het enige tijd duren voordat de software alle gezichten in de database heeft vergeleken met die op het beeld. Gezichten uit beelden halen en deze vergelijken met

gezichten in een database duurt langer dan gezichten op een foto vergelijken met gezichten in een database. Dit komt doordat er als het ware meerdere foto's in een beeld zitten. Het programma moet hier het juiste beeld uithalen op de juiste tijd, pas dan kan de vergelijking plaatsvinden. Daarnaast duurt het vergelijken van gezichten langer naarmate er meer gezichten op een beeld zijn.

Uit het onderzoek van NIST blijkt verder dat geautomatiseerde gelaatsherkenning wel degelijk mogelijk is, ook op opnames van meerdere mensen. Echter blijkt ook uit het onderzoek dat hoe meer mensen op de opname staan des te minder accuraat de systemen werken. Het blijkt dat geautomatiseerde gelaatsherkenning goed werkt onder gecontroleerde omstandigheden waarbij foto's of opnamen precies zo gemaakt zijn zodat het systeem een goede vergelijking kan doen. Daarnaast werken zij ook met technieken die ervoor zorgen dat afbeeldingen van personen scherper worden waardoor deze beter bruikbaar zijn voor geautomatiseerde gelaatsherkenning. Wanneer dit ingebouwd zou kunnen worden in een geautomatiseerde gelaatsherkenningssyteem zijn de mogelijkheden met betrekking tot het toepassen van geautomatiseerde gelaatsherkenning groter.

Naast NIST zijn er nog een aantal andere onderzoekers die kijken naar de technische aspecten van geautomatiseerde gelaatsherkenning. Een aantal belangrijke punten hieruit worden hieronder besproken.

Mogelijkheden

Voordat geautomatiseerde gelaatsherkenning automatisch mogelijk was werd dit door forensisch specialisten gedaan. Vergelijking door forensische specialisten is erg tijdrovend, automatische gezichtsherkenning maakt het mogelijk dat er meerdere gezichten tegelijkertijd en dat gezichten sneller met elkaar kunnen worden vergeleken. Wanneer gezichtsherkenning toegepast wordt in een gecontroleerde omgeving is het percentage fouten dat de software maakt erg klein, in een gecontroleerde omgeving werkt gezichtsherkenning goed. Daarnaast blijkt het automatisch herkennen van gezichten accurater te zijn dan handmatige gezichtsherkenning doordat automatische gezichtsherkenning zelfs kan kijken naar het aantal sproeten, de hoeveelheid en plaats van de rimpels, missende stukjes tand enzovoort (Jain, Klare & Park, 2011).

Beperkingen

Van Welzen (2011) onderzoekt in zijn onderzoek de applicaties Picasa, Fotobounce en PittPatt Facesort. Deze programma's van gezichtsherkenning zijn voor iedereen te downloaden. Uit hun onderzoek blijkt dat de geautomatiseerde gelaatsherkenningssoftwares moeite hebben met het herkennen van gezichten wanneer personen een bril of hoofddeksel dragen. Ook wanneer het beeld onderbelicht of overbelicht is, is het herkenningspercentage lager dan bij een goed beeld. Dit geldt tevens voor wanneer het vergelijkingsmateriaal een foto betreft van de zijkant van iemand zijn/haar gezicht. Daarnaast wordt het herkenningspercentage hoger naarmate er meer referentiemateriaal wordt gebruikt.

Uit het onderzoek van Boume en collega's (2014) blijkt dat gezichtsherkenning beter werkt naarmate er meer vergelijkingsmateriaal is dat is waargenomen vanuit meerdere standpunten en dat gezichtsherkenning vooral werkt in een gecontroleerde omgeving waar medewerking kan worden

afgedwongen. Een voorbeeld hierbij zijn toegangspoortjes op Schiphol. Daarnaast maakt een grote massa mensen het voor de software lastiger om gezichten te herkennen. Dit doordat er zich veel mensen bevinden waarvan de gezichten allemaal door dezelfde of dezelfde paar camera's moeten worden waargenomen. Zo zal het ook lastig zijn om zakkenrollers te betrappen omdat zij dit juist vaak doen in een drukke omgeving.

Naast de beperkingen die hierboven zijn benoemd is er met geautomatiseerde gelaatsherkenning nog steeds kans op false positives en false negatives. Dit is een beperking van het systeem want het systeem werkt dan niet optimaal, er is nog steeds een percentage waarin de uitkomst van de vergelijking onjuist is. Daarnaast is het voor gezichtsherkenning belangrijk dat de kwaliteit van de beelden voldoende is en de camera op de juiste plaats hangt en de juiste hoek heeft. Dit is voor de verschillende softwareprogramma's anders. Wanneer hier geen sprake van is, werkt gezichtsherkenning niet optimaal (Melgaça, 2015). Echter zijn er ook programma's die de kwaliteit van de beelden kunnen verbeteren. Deze programma's kunnen bijvoorbeeld het beeld scherper maken of de belichting verbeteren, dit maakt het wellicht mogelijk om ook op de slechtere kwaliteit camera's gezichtsherkenning toe te passen (Jain et. al., 2011).

Een andere beperking is dat automatische gezichtsherkenning steeds minder goed werkt wanneer de afstand tussen de leeftijd van de persoon op het referentiemateriaal en de leeftijd van de persoon op het vergelijkingsmateriaal groter wordt (Jain et. al., 2011).

6.1. Preventie vs. opsporing

Uit de technische moeilijkheden en mogelijkheden, welke eerder in dit hoofdstuk besproken zijn, kan er geconcludeerd worden wat er mogelijk en niet mogelijk is in het kader van de opsporing en preventie van veel voorkomende criminaliteit in winkelcentra.

Vanuit de afschrikkingstheorie, welke is besproken in paragraaf 2.2 van dit onderzoek, kan er beargumenteerd worden dat de aanwezigheid van geautomatiseerde gelaatsherkenning een afschrikwekkende werking kan hebben op de crimineel. Echter is het voor alsnog lastig om geautomatiseerde gelaatsherkenning toe te passen op een grotere hoeveelheid personen. Hierdoor zal de melding dat er een crimineel is gesignaleerd, zoals omschreven in scenario 2, wellicht lastig waar te maken zijn. Dit doordat er bij een grote hoeveelheid mensen sprake is van meerdere gezichten in het beeld, geautomatiseerde gelaatsherkenningssystemen kunnen hieruit nog lastig één gezicht filteren. Daarnaast bewegen de personen op de beelden waardoor de beelden vaak wazig zijn en niet van optimale kwaliteit, geautomatiseerde gelaatsherkenning werkt immers het beste in een gecontroleerde omgeving onder optimale omstandigheden. Een ander aspect dat van belang is bij de preventie van delicten is tijd. Wanneer het gaat om het scannen van meerdere gezichten op een live beeld tegenover een database met meerdere gezichten is er als het ware sprake van een veel op veel vergelijking. Dit zal tijdrovend zijn terwijl het bij preventie van belang is om zo snel mogelijk te handelen. Een ander aspect is dat het waarschijnlijk is dat veel criminelen zo onopvallend mogelijk gekleed zijn, camera's zo veel mogelijk ontwijken en hun gezicht zo veel mogelijk bedekken door bijvoorbeeld een pet of bril te dragen. Geautomatiseerde gelaatsherkenning

werkt in deze gevallen minder goed dan wanneer er een foto van een bepaalde persoon tegenover de database wordt gehouden. Technisch is het, in het gewenste geval van preventie zoals in scenario 2, lastig om dit waar te maken.

Bij de opsporing zijn er meer mogelijkheden wanneer het op geautomatiseerde gelaatsherkenning gaat. Scenario 3 is uitgesplitst in twee scenario's waarbij het ene scenario uit gaat van opsporing op heterdaad en het andere van opsporing buiten heterdaad. Bij opsporing op heterdaad zullen dezelfde technische moeilijkheden naar voren komen als bij scenario 2. Er wordt immers gekeken of een bepaald persoon terug te vinden is in een massa bewegende mensen. Echter is er op dit moment geen sprake van een veel op veel vergelijking maar een één op veel vergelijking. Er is namelijk een beeld van de dader. Deze dader wordt gezocht in een massa mensen. In dit geval is er geen sprake van een grote referentiedatabase met gezichten die worden vergeleken met gezichten van meerdere bewegende mensen. Hierdoor kan het zijn dat de tijd, die het geautomatiseerde gelaatsherkenningssysteem nodig heeft om een persoon te vinden, anders is. Toch blijven de technische moeilijkheden met betrekking tot het beeld hetzelfde als bij scenario 2. De dader beweegt zich in een grotere groep mensen en zal waarschijnlijk zo veel mogelijk de camera's ontwijken of zichzelf vermommen. Wanneer het gaat om het toepassen van geautomatiseerde gelaatsherkenning buiten heterdaad kan er geconcludeerd worden dat er wel degelijk mogelijkheden zijn, mits het beeld van de dader van goede kwaliteit is. Wanneer er een beeld van de dader is doordat deze bijvoorbeeld is uitgesneden uit de beelden, kan dit beeld worden vergeleken met de personen in de bestaande database. Dit is wat er als het ware al gebeurd in Zoetermeer met CATCH (meer informatie hierover is terug te vinden in paragraaf 7.4). Zo kan er informatie worden gevonden betreffende de persoon, mits deze persoon een bekende is van de politie en in de database staat. Een kanttekening die hierbij geplaatst dient te worden is dat het verworven beeld wel van voldoende kwaliteit dient te zijn. Geautomatiseerde gelaatsherkenningssystemen werken immers het beste wanneer het gaat om een frontaal beeld, de lichtomstandigheden optimaal zijn, het beeld niet bewogen is en de persoon in kwestie weinig of geen vermommingsattributen draagt.

Uit bovenstaande blijkt dat er wel degelijk technische mogelijkheden zijn voor het inzetten van geautomatiseerde gelaatsherkenning. Vooral op afbeeldingen van de juiste kwaliteit werkt dit goed en wanneer dit achteraf plaatsvindt en zo min mogelijk personen vergeleken moeten worden. Of geautomatiseerde gelaatsherkenning ook goed en optimaal zal kunnen werken op massa's mensen en of dit realistisch is al wordt er gekeken naar kosten, tijd, beschikbaar geheugen en snelheid zal nog moeten blijken.

7. TOEPASSINGSVORMEN

In het laatste resultatenhoofdstuk van deze thesis worden de verschillende toepassingsvormen van geautomatiseerde gelaatsherkenning besproken. Zo zijn er verschillende mogelijkheden waarbij geautomatiseerde gelaatsherkenning gebruikt kan worden. Hierbij kan er gedacht worden aan het verschaffen van toegang tot gebouwen, het verschaffen van toegang tot computers of applicaties, het verschaffen van toegang tot het land en opsporing van bepaalde personen (Veldhuis, 2014).

Hieronder wordt besproken welke vormen van geautomatiseerde gelaatsherkenning in zowel het binnen- als het buitenland worden toegepast en hoe dit in zijn werk gaat. Op deze manier kan er inzicht worden verkregen in de mogelijke toepassingsvormen. Wanneer dit voor de politie als organisatie inzichtelijk is kan dit helpen bij verder onderzoek naar geautomatiseerde gelaatsherkenning. Zo wordt duidelijk welke partijen werken met geautomatiseerde gelaatsherkenning, welke proeven al zijn uitgevoerd en welke partijen benaderd kunnen worden om informatie in te winnen. Dit kan de politie veel tijd besparen door onderzoeken op te vragen welke door betreffende partijen al zijn uitgevoerd.

7.1. E-Gate

Een eerste voorbeeld van geautomatiseerde gelaatsherkenning zijn de e-gates die onder andere gebruikt worden op Schiphol, maar welke ook terug te vinden zijn op andere vliegvelden in de wereld. Hierbij wordt de foto op het paspoort vergeleken met het beeld dat te zien is op de camera. De persoon in kwestie gaat voor de camera staan, welke een digitaal beeld van het gezicht maakt. Dit beeld wordt vergeleken met de afbeelding op het paspoort. Op deze manier kan er gekeken worden of de persoon in kwestie ook de rechtmatige eigenaar van het paspoort of de identiteitskaart is. Wanneer er herkenning plaatsvindt gaan de poortjes open. Op deze manier is er automatische grenscontrole en zou de grenscontrole worden versneld (Brouwers, 2004; Del Rio, Moctezume, Conde, Martin de Diego & Cabello, 2016; Veldhuis, 2014). Bij Schiphol is het zo dat e-gates vrijwillig zijn, zo is het ook mogelijk om op de ‘normale’ wijze in te checken. Wanneer men voor inchecken via de e-gate kiest gaat dit geheel vrijwillig en staat men zijn of haar biometrische gegevens vrijwillig af. Bij registratie scant de betreffende persoon zijn/haar paspoort, instapkaart en gezicht. Wanneer dit overeenkomt gaat het poortje open. Na het boarden worden de gegevens van de passagier automatisch verwijderd en worden de biometrische gegevens niet opgeslagen (Schiphol, 2017). Om meer informatie te verkrijgen over de manier van werken met betrekking tot de e-gates op Schiphol is de communicatieafdeling geraadpleegd. Omdat Schiphol tot 2019 nog in de testfase zit van het toepassen van geautomatiseerde gelaatsherkenning kan er nog geen antwoord gegeven worden op vragen met betrekking tot databeheer, juridische en technische mogelijkheden en wat er na afloop gedaan wordt met de beelden. Informatie dat wel gedeeld is door de communicatieafdeling van Schiphol is dat de luchthaven bij hun testen met geautomatiseerde gelaatsherkenning samenwerkt met de overheid en verschillende luchtvaartmaatschappijen. Daarnaast wordt er bij het uitvoeren van de testen rekening gehouden met de privacywetgeving omtrent databeheer (persoonlijke communicatie, 10 december 2018).

7.2. Stadions

Gezichtsherkenning wordt tevens in verschillende stadions over de wereld toegepast. Niet alleen om mensen met een stadionverbod te weren maar ook om verdachte personen op te sporen (Mulder, 2018). In Nederland is de toepassing in stadions steeds vaker terug te vinden. Zo wordt gezichtsherkenning onder andere bij het stadion van FC Groningen toegepast om hooligans en bezoekers met een stadionverbod eruit te pikken. Deze personen worden bij de toegangspoortjes herkend en mogen het stadion niet betreden (RTVNoord, 2016). Tevens wordt gezichtsherkenning toegepast in de stadions van ADO Den Haag en PSV om mensen met een stadionverbod te weren. Deze stadions werken met toegangspoortjes die de mogelijkheid hebben om de foto en de persoon in kwestie te controleren (Trouw, 2007; Van Rooij, 2006; Veldhuis, 2014). Zo is er bij PSV een bestand aangemaakt (door de voetbalvereniging zelf) van pasfoto's van personen met een stadionverbod. Bij de toegangspoortjes wordt het gezicht dat te zien is in de camera vergeleken met dit bestand, wanneer er een match is wordt er een persoon met een stadionverbod herkent (Eindhovens dagblad, 2017). ADO Den Haag werkt daarnaast samen met de KNVB om personen met een stadionverbod te weren of uit de massa bezoekers te pikken. Zij hebben een zogenaamde blacklist opgesteld welke afbeeldingen van personen met een stadionverbod bevat. Deze afbeeldingen worden vergeleken met de beelden die bij de toegangspoortjes worden gemaakt. Hier is sprake van een private partij welke gebruik maakt van gezichtsherkenning (Algemeen dagblad, 2016).

7.3. Winkels, tankstations & horeca

In winkelcentra in Utrecht wordt gezichtsherkenning toegepast om mensen met een winkelverbod te weren (Veldhuis, 2014). Een voorbeeld van een winkel die gezichtsherkenning toepast is De Rode Winkel. De winkeliers van deze winkel hebben zelf het initiatief genomen om winkeldieven tegen te gaan. Omdat zij winkeldieven erg storend vonden en hiermee veel te maken hadden kozen zij ervoor om hun winkel te weren tegen winkeldieven. Een camera met gezichtsherkenning registreert bij binnenkomst alle bezoekers van de winkels. Vervolgens wordt er contact gemaakt met de database waarin de gezichten van winkeldieven zijn opgeslagen. Deze database is samengesteld door de winkeliers zelf en mag onderling (tussen andere winkels) niet worden uitgewisseld. Bij de vergelijking kan een hit ontstaan. Het idee van de eigenaren is, in het geval van een hit, de persoon in kwestie aan te spreken. Na het eerste jaar bleek dat het aantal winkeldiefstallen in hun winkels flink was afgenomen. Hier zijn het dan ook de winkeliers zelf, en niet de politie, die gezichtsherkenning toepassen en het initiatief hiervoor nemen (Haighton, 2004; Nu.nl, 2004;).

Niet alleen in winkels is gezichtsherkenning toegepast. Ook in tankstations in Rotterdam zijn gezichtsherkenningssystemen gebruikt. Het doel van het toepassen van gezichtsherkenning hierbij was om overvallen tegen te gaan en overvallers te weren. Wanneer iemand aan komt lopen registreert een camera dit gezicht, het gezicht wordt vergeleken met referentiemateriaal in een database. Wanneer de persoon wordt herkend gaat er een negatief signaal af en gaan de deuren niet open. Dit is getest bij juweliers en

tankstations maar zou ook gebruikt kunnen worden in supermarkten. Hierbij is samengewerkt met politie en het Openbaar Ministerie (Leonards, 2015).

7.4. Politie

10.2.c . Ook andere politieagenten kunnen een verzoek doen hiertoe wanneer dit noodzakelijk is voor de uitvoering van hun opsporingstaak. Hierbij kan het van belang zijn dat een subject zo snel mogelijk wordt geïdentificeerd, dit kan dan met behulp van geautomatiseerde gelaatsherkenning (Politie, 2012).

Een voorbeeld van een database die gebruikt wordt voor als referentie is het CATCH systeem. Deze database bestaat uit twee systemen met twee databases; de database van Verdachten en Veroordeelden en de database van Vreemdelingen. Opsporingsfoto's kunnen worden aangeboden voor zoekopdrachten in deze systemen (Politie, 2017).

Niet alleen de politie in Nederland maakt gebruik van gezichtsherkenning. Ook op andere plekken in de wereld, zoals bijvoorbeeld in Florida, maakt de politie gebruik van gezichtsherkenning om bijvoorbeeld te bevestigen met welke verdachte zij te maken heeft. Ook hier worden er foto's van meerder personen vergeleken met dat van de verdachte (Veldhuis, 2014).

[16] Wanneer er een hit is, is er een voldoende mate van gelijkenis geconstateerd tussen de foto welke gemaakt is door de opsporingsambtenaar van de DB&B en een foto in de database. Bij een no-hit is er geen sprake van voldoende gelijkenis met de foto en het referentiemateriaal (Politie, 2015).

7.5. Nederlands Forensisch Instituut

Ook bij het Nederlands Forensisch Instituut [NFI] wordt er gebruik gemaakt van gezichtsherkenning. Het NFI speelt hierbij een rol wanneer het gaat om identiteitsbepaling. Dit kan gebruikt worden voor bijvoorbeeld de opsporing in het geval van het zoeken naar verdachten, voor bewijsvoering wanneer het gaat om het koppelen van een persoon aan een misdrijf of om verificatie wanneer het gaat om het koppelen van een referentiebeeld aan een daderbeeld. Wanneer in een strafzaak de vraag naar voren komt of een persoon op een bepaalde afbeelding of een video overeenkomt met de verdachte kan het NFI gevraagd worden om hierin op te treden als deskundige. Het NFI kan hierbij gebruik maken van automatische gezichtsherkenning maar vaak maakt zij gebruik van vergelijking van gezichtsbeelden. Het belangrijke onderscheid hiertussen is dat het NFI vaak deskundige inzet om handmatig de gezichten met elkaar te vergelijken. De software van gezichtsherkenning wordt dan ook nauwelijks toegepast. Dit omdat de beelden die het NFI krijgt van bepaalde gebeurtenissen of verdachten vaak niet scherp genoeg zijn om automatische gezichtsherkenning op toe te passen. Belangrijk bij het onderzoek van het NFI is dat er nooit gesproken wordt van een 100% herkenning/overeenkomst. De deskundigen doen een uitspraak met betrekking tot aannemelijkheid. Zo kunnen zij concluderen dat het aannemelijker is dat de twee personen (de verdachte en de persoon op het beeld) dezelfde persoon zijn dan dat zij dit niet zijn, of andersom (Nederlands Forensisch Instituut, 2017).

7.6. Overige toepassingen

Hierboven zijn een aantal toepassingsvormen genoemd welke terug te zien zijn in de literatuur en in de kranten. Naast de toepassingsvormen kan gezichtsherkenning gebruikt worden als toegangskaartje. Wanneer het gezicht als toegangskaartje gebruikt wordt is het wellicht mogelijk om fraude met betrekking tot het doorgeven van kaartjes te verminderen (NOS, 2018). Verder wordt gezichtsherkenning gebruikt als toegangscode voor mobiele telefoons. Zo is het bij bijvoorbeeld iPhones mogelijk om de telefoon te ontgrendelen door middel van gezichtsherkenning (AD, 2018). Daarnaast experimenteert China met de mogelijkheid om te kunnen betalen door middel van gezichtsherkenning in plaats van ene pincode. In China zijn ze al veel verder met het toepassen van gezichtsherkenning. Zo wordt gezichtsherkenning gebruikt in de zogenaamde ‘slimme brillen’ van agenten, iets wat vergelijkbaar is met bodycams (Kist, 2018). Bij het lezen van krantenartikelen over de toepassing van gezichtsherkenning blijkt dat in China de toepassingsvormen verder gaan dan de toegangspoortjes op het vliegveld of het identificeren van personen. Zo zijn ze er zelfs mee bezig om via gezichtsherkenning boetes uit te kunnen schrijven aan burgers die bijvoorbeeld door rood lopen, de boetes zouden zij dan niet ontvangen in hun brievenbus maar krijgen zij toegestuurd via hun mobiele telefoon. Belangrijk om hierbij te vermelden is dat in China de wet en regelgeving anders is dan die in Nederland. China heeft zelfs hun wet aangepast om deze manieren van inzet mogelijk te maken. Omdat de wet en regelgeving anders is kan Nederland deze manier van inzetten niet zomaar overnemen (Security, 2018). Een andere mogelijke toepassing is een toepassingsvorm waar de

Koninklijke Marechaussee op Schiphol op dit moment onderzoek naar doet. Naast de e-gates is het een mogelijkheid om gezichtsherkenning toe te passen op de camera's op Schiphol of op de bodycams van de agenten op het vliegveld. Dit kan mogelijk de veiligheid op Schiphol vergroten doordat er hits naar de meldkamer worden gestuurd wanneer er een persoon wordt herkend die op de lijst met verdachte personen staat of als vermist of verdachte is geregistreerd. Op dit moment is de Koninklijke Marechaussee nog bezig met het onderzoeken van deze mogelijkheid en wordt dit nog niet daadwerkelijk toegepast (Strijbosch, 2017).

Zoals uit dit hoofdstuk is gebleken kan geautomatiseerde gelaatsherkenning voor meerdere doeleinden worden gebruikt. Geautomatiseerde gelaatsherkenning ten behoeve van de opsporing en preventie van veel voorkomende criminaliteit in winkelcentra is een mogelijkheid die onderzocht wordt door de politie. Echter blijkt uit bovenstaande dat geautomatiseerde gezichtsherkenning al op vele manieren en door verschillende organisaties wordt toegepast. Kennis van de verschillende toepassingsvormen kan inzicht verwerven wanneer het gaat om de mogelijkheden en beperkingen van geautomatiseerde gelaatsherkenningssystemen. Dit kan de politie, maar ook een andere mogelijke verwerkers, helpen bij de keuze voor het wel of niet inzetten van geautomatiseerde gelaatsherkenning in een bepaald geval. Daarnaast kan het bijdrage aan het doen van onderzoek hiernaar, zo wordt aan de hand van de verschillende toepassingsvormen duidelijk welke instanties benaderd kunnen worden om meer informatie over verschillende software te verkrijgen en om ervaringen met elkaar te delen. Daarnaast wordt duidelijk dat geautomatiseerde gelaatsherkenning geen nieuw fenomeen is dat de politie wil inzetten. Het wordt al gebruikt, ethische aspecten die bij de verschillende toepassingsvormen een rol spelen kunnen in kaart worden gebracht. Dit geldt tevens voor de juridische inzetkaders. Deze kunnen toekomstige verwerkers helpen bij het bepalen van hun inzetkader en het benaderen van ethische aspecten.

8. CONCLUSIE EN DISCUSSIE

8.1. Conclusie

Geautomatiseerde gelaatsherkenning is een techniek die voor veel doeleinden gebruikt wordt. Vanuit Programma Sensing is het de vraag of geautomatiseerde gelaatsherkenning kan bijdragen aan het aanpakken van een van de veiligheidsvraagstukken waar de politie mee kampt (Programma Sensing, 2017). Een van de veiligheidsstukken is de problematiek rondom veel voorkomende criminaliteit in winkelcentra. In dit onderzoek is gekeken of geautomatiseerde gelaatsherkenning toegepast kan worden als hulpmiddel bij de preventie en opsporing van deze vormen van criminaliteit. Daarnaast is gekeken of dit middel door zowel publieke partijen als door private partijen toegepast kan en mag worden.

Verschillende criminologische theorieën, zoals de routine activiteitentheorie, afschrikkingstheorie en de rationele keuzetheorie zijn gebruikt als onderbouwing voor het inzetten van geautomatiseerde gelaatsherkenning bij de opsporing en preventie van veel voorkomende criminaliteit in winkelcentra in Nederland. Voor het Programma Sensing is het van belang dat, voordat een nieuwe technologie wordt ingezet door de politie, deze eerst wordt onderzocht op zowel juridisch, technisch en ethisch vlak (Tweede Kamer, 2015). Daarom is de volgende onderzoeksvraag opgesteld:

'Wat zijn de mogelijkheden en beperkingen van het inzetten van geautomatiseerde gelaatsherkenning op basis van sensoren als preventie- en opsporingsmiddel voor veelvoorkomende criminaliteit in winkelcentra in Nederland door zowel private als publieke partijen?'

Om deze onderzoeksvraag te kunnen beantwoorden waren de volgende deelvragen geformuleerd:

- Welke mogelijkheden en beperkingen zijn er met betrekking tot de wetgeving in Nederland voor het inzetten van geautomatiseerde gelaatsherkenning bij de opsporing en preventie van veel voorkomende criminaliteit in winkelcentra?
- Met welke ethische vraagstukken dient rekening gehouden te worden met het inzetten van geautomatiseerde gelaatsherkenning als preventie- en opsporingsmiddel?
- Hoe denken de medewerkers van het Programma Sensing in Villa B over het toepassen van geautomatiseerde gelaatsherkenning in verschillende gevallen?
- Welke mogelijkheden en beperkingen zijn er op technisch gebied wanneer het gaat om geautomatiseerde gelaatsherkenning?
- Op wat voor manieren wordt geautomatiseerde gelaatsherkenning toegepast in zowel het binnen- als buitenland?

Ten eerste zijn de mogelijkheden en beperkingen op het gebied van de wetgeving onderzocht. Dit is gedaan aan de hand van drie scenario's die zijn opgesteld naar aanleiding van de wensen van het Programma Sensing. Aan de hand van de scenario's, welke gebeurtenissen omschrijven, wordt duidelijk voor welke

gevallen de politie of eventuele private partijen, geautomatiseerde gelaatsherkenning kan toepassen en onder welke omstandigheden dit dient te gebeuren. Uit het juridisch onderzoek komt naar voren dat er een aantal mogelijkheden zijn met betrekking tot het inzetten van geautomatiseerde gelaatsherkenning ten behoeve van preventie en opsporing van veel voorkomende criminaliteit in winkelcentra. Voor alle scenario's geldt dat er een juridische grondslag is voor het toepassen van geautomatiseerde gelaatsherkenning. Wanneer geautomatiseerde gelaatsherkenning wordt toegepast door private partijen is deze grondslag te vinden in de AVG. Wanneer het wordt toegepast door publieke partijen is deze grondslag terug te vinden in de WPG. In alle gevallen geldt de eis van proportionaliteit en subsidiariteit waar rekening mee gehouden moet worden wil de verwerking van bijzondere persoonsgegevens rechtvaardig zijn. Alle gevallen dienen apart behandeld te worden waarbij een afweging wordt gemaakt tussen de inbreuk op de persoonlijke levenssfeer en de noodzaak van het inzetten van het middel. Te allen tijde dient er gekozen te worden voor het minst ingrijpende middel wanneer er meerde middelen zijn met hetzelfde effect. Tevens stellen zowel de AVG als de WPG plichten waaraan de verwerker moet voldoen. Deze dienen nageleefd te worden en hierop dient controle te zijn. Wanneer er niet wordt voldaan aan een van de beginselen of plichten is de verwerking van de persoonsgegevens niet rechtvaardig. Wanneer het gaat om de eis van proportionaliteit en subsidiariteit is het denkbaar dat in het geval van scenario 3.3, waarbij geautomatiseerde gelaatsherkenning wordt toegepast in het licht van opsporing buiten heterdaad, sneller wordt voldaan aan deze eisen. Dit omdat in deze situatie niet alle burgers door het gelaatsherkenningssysteem gehaald worden. Hier wordt geautomatiseerde gelaatsherkenning louter toegepast op criminelen.

Concluderend zijn er op juridisch vlak wel degelijk mogelijkheden met betrekking tot het uitvoeren van de scenario's. Hierbij is het belangrijk dat er in elk apart geval een nieuwe afweging plaatsvindt en zijn normen breed omschreven waardoor er ruimte blijft voor interpretatie. Dit kan zowel gezien worden als een mogelijkheid, doordat de wet mogelijkheden biedt voor het inzetten van geautomatiseerde gelaatsherkenning, maar ook als een beperking doordat de normen breed zijn waardoor eigen interpretatie mogelijk is.

Vervolgens is, aan de hand van literatuur en interviews, gekeken welke ethische vraagstukken een rol spelen bij het inzetten van geautomatiseerde gelaatsherkenning. Uit de literatuur komen verschillende ethische vraagstukken naar voren die een rol spelen bij het inzetten van geautomatiseerde gelaatsherkenning. Zo dient de verwerker zich af te vragen of hij/zij geautomatiseerde gelaatsherkenning wel wil toepassen wanneer dit mogelijk blijkt te zijn. Daarnaast speelt het aspect van het gevoel van achtervolging een rol, de burger wordt op deze manier beperkt in zijn/haar bewegingsvrijheid. Ook de kans op biases wordt benoemd. Gelaatsherkenningssoftware kan biases bevatten waardoor de mogelijkheid bestaat tot oneerlijke behandeling van dezelfde gevallen. Daarnaast is geautomatiseerde gelaatsherkenning een grote inbreuk op de persoonlijke levenssfeer. Dit zijn aspecten die uit de literatuur meerdere malen naar voren komen. Uit de verschillende interviews blijkt dat medewerkers zich zorgen maken over wat er met data gebeurt en in welke omstandigheden onze maatschappij geautomatiseerde gelaatsherkenning wil toepassen. In veel gevallen gaat het hierbij niet om het kunnen en mogen maar om de wenselijkheid van het toepassen van geautomatiseerde gelaatsherkenning in bepaalde gevallen. Zo is gebleken dat een veel

voorkomend bezwaar van de respondenten is dat, in het geval van veel voorkomende criminaliteit, de inbreuk op de privacy en persoonlijke levenssfeer te groot is. Er zijn ook een aantal positieve punten benoemd door de respondenten. Zo zou geautomatiseerde gelaatsherkenning een bijdrage kunnen leveren aan het sneller opsporen van criminelen. Dit zou voor kunnen komen wanneer geautomatiseerde gelaatsherkenning wordt toegepast zoals in scenario 3.2 waarbij er een duidelijk afbeelding van de dader is en deze wordt vergeleken met bekende daders uit de database. Waar het merendeel van de respondenten het over eens is, is dat zij allen graag meer onderzoek naar geautomatiseerde gelaatsherkenning zien voordat het wordt ingezet. Zo is het vertrouwen in de techniek nog niet voldoende en moet er meer onderzoek uitgaan naar het verminderen van valse matches. Daarnaast is er een groot aantal respondenten die alleen de politie vertrouwd als verwerker. Wanneer een private partij geautomatiseerde gelaatsherkenning gebruikt als techniek dan zou de kans op een datalek en misbruik van de data volgens de respondenten groter zijn. Wanneer er een vergelijking wordt gemaakt tussen de ethische aspecten die uit de literatuur naar voren komen en de aspecten die naar voren komen uit de interviews blijkt dat zij een overeenkomst met elkaar hebben. Een aspect dat in beide delen naar voren komt is dat er meer aandacht moet naar andere factoren zoals genetische en sociale factoren bij het voorkomen van criminaliteit. Een verschil tussen de aspecten uit de literatuur en de aspecten uit de interviews is dat vanuit de interviews blijkt dat geautomatiseerde gelaatsherkenning onder bepaalde omstandigheden wel geaccepteerd zal worden. Dit komt doordat in de interviews bepaalde situaties worden beschreven waarbij de respondenten geautomatiseerde gelaatsherkenning acceptabel vinden door de ernst van het delict. In de interviews komt naar voren dat er bij het inzetten van geautomatiseerde gelaatsherkenning een afweging gemaakt dient te worden tussen de inbreuk op de persoonlijke levenssfeer en de ernst van het delict. Er zal altijd een toetsing plaats moeten vinden wil geautomatiseerde gelaatsherkenning acceptabel zijn.

Naast juridische mogelijkheden en ethische aspecten zijn de technische mogelijkheden en beperkingen in kaart gebracht. Hieruit is gebleken dat wanneer het gaat om een gecontroleerde setting, zoals een frontale foto dat vergeleken wordt met de database van CATCH, geautomatiseerde gelaatsherkenning in veel gevallen goed werkt. Wanneer geautomatiseerde gelaatsherkenning wordt toegepast op grotere groepen mensen is het lastig om de juiste afbeeldingen van de personen te verkrijgen, duurt het enige tijd voordat gegevens vergeleken zijn, zijn afbeeldingen vaak niet van goede kwaliteit en zijn niet alle gezichten duidelijk te zien doordat er overlapping in de beelden is of doordat personen zich vermommen. Wanneer de technologie, zoals deze in 2015 was, wordt toegepast zal deze niet voldoen aan de eisen die gesteld worden als het gaat om de opsporing en preventie van veel voorkomende criminaliteit. Dit doordat hits niet snel genoeg naar voren komen, niet iedereen wordt herkend en doordat afbeeldingen vaak niet onder de gewenste, gecontroleerde omstandigheden worden verkregen.

Ten slotte zijn er verschillende toepassingsvormen van geautomatiseerde gelaatsherkenning besproken. Zo wordt geautomatiseerde gelaatsherkenning al op verschillende manieren en in verschillende omstandigheden toegepast. Een voorbeeld dat genoemd is zijn de e-gates op luchthavens waarbij onder gecontroleerde omstandigheden toegang wordt verleend door middel van geautomatiseerde gelaatsherkenning. Een andere toepassingsvorm is het toepassen van geautomatiseerde gelaatsherkenning in stadions om mensen met een stadionverbod te weren. Daarnaast is geautomatiseerde gelaatsherkenning

ook meerdere keren toegepast in winkels, tankstations en horecagelegenheden. Ook de politie maakt al langere tijd gebruik van geautomatiseerde gelaatsherkenning. Zo maakt de DB&B gebruik van geautomatiseerde gelaatsherkenning bij de beveiliging van personen om te kijken of een bepaald, verdacht persoon in de database voorkomt. Naast de politie wordt geautomatiseerde gelaatsherkenning toegepast door het NFI. Echter gebeurt dit lang niet altijd geautomatiseerd maar komen hier vaak deskundigen bij kijken. Andere mogelijke toepassingsvormen zijn betalen door middel van gezichtsherkenning, het vinden van potentiële terroristen op luchthavens en het inzetten van geautomatiseerde gelaatsherkenning als toegangskaartje. Hieruit blijkt dat geautomatiseerd gelaatsherkenning op veel verschillende manieren toegepast kan worden en dat er wel degelijk mogelijkheden zijn wanneer het gaat om juridische inzetkaders en techniek.

Wanneer er gekeken wordt naar de specifieke mogelijkheden en beperkingen met betrekking tot de opsporing en de preventie van veelvoorkomende criminaliteit zijn er verschillende mogelijkheden en beperkingen aan te wijzen. Voor zowel de opsporing als de preventie, door zowel publieke als private partijen, is gebleken dat er een juridische grondslag is. Echter blijft het van de omstandigheden van het geval afhangen of de verwerking rechtmatig is of niet. Hierbij dient in alle gevallen een afweging gemaakt te worden tussen de inbreuk op de privacy en de noodzakelijkheid van het behalen van het doel. Subsidiariteit en proportionaliteit zijn twee belangrijke begrippen. Wanneer het gaat om ethiek is er een duidelijk onderscheid dat gemaakt kan worden tussen de opsporing en de preventie. In het geval van preventie zijn respondenten eerder geneigd te zeggen dat geautomatiseerde gelaatsherkenning, voor veel voorkomende criminaliteit, een te ingrijpend middel is. Wanneer het gaat om opsporing buiten heterdaad is een groot deel van de respondenten wat milder. In dit geval is de inbreuk op de persoonlijke levenssfeer minder groot doordat niet iedere burger te maken krijgt met geautomatiseerde gelaatsherkenning. Ten slotte zijn er ook verschillen in de mogelijkheden en beperkingen tussen opsporing en preventie wanneer het gaat om de techniek. Bij preventie blijft het, vooralsnog, technisch lastig om geautomatiseerde gelaatsherkenning toe te passen. Dit doordat geautomatiseerde gelaatsherkenning nog niet snel genoeg werkt, gezichten elkaar overlappen, personen zich vermommen, weersomstandigheden en belichting een rol spelen bij de kwaliteit van de beelden en doordat beelden vaak wazig zijn. Wanneer het gaat om opsporing buiten heterdaad is het eenvoudiger om geautomatiseerde gelaatsherkenning toe te passen. Dit wel onder de voorwaarde dat het beeld dat door de referentiedatabase wordt gehaald van voldoende kwaliteit is.

Vanuit de theorieën, die besproken zijn in hoofdstuk 2 van dit onderzoek, kan er aan de hand van de resultaten beargumenteerd worden dat geautomatiseerde gelaatsherkenning een bijdrage zou kunnen leveren aan het verminderen van veel voorkomende criminaliteit in winkelcentra. Vanuit de routine activiteitentheorie van Cohen en Felson (1979) wordt beargumenteerd dat wanneer de controle in een bepaald gebied toeneemt, het waarschijnlijk is dat de criminaliteit af zal nemen. Uit de interviews en de literatuur omtrent ethiek is gebleken dat burgers het gevoel kunnen hebben gevolgd te worden, vrij bewegen wordt lastiger (Olsthoorn, 2017). Dit zou ook voor de crimineel kunnen gelden wat, volgens de routine activiteiten theorie, kan leiden tot het verminderen van criminaliteit. Niet alleen vanuit de routine

activiteiten theorie zou geautomatiseerde gelaatsherkenning een bijdrage kunnen leveren aan het verminderen van crimineel gedrag. Ook vanuit de afschrikkingstheorie en de rationele keuze theorie kan er, aan de hand van de resultaten met betrekking tot ethiek, beargumenteerd worden dat geautomatiseerde gelaatsherkenning een bijdrage kan leveren aan het verminderen van criminaliteit. Wanneer een dader de subjectieve pakkans hoger acht en de verwachte kosten van het delict hoger zijn dan de baten zal de dader sneller van het delict afzien (Bentham en Beccaria in Goldenbeld, Morsink, Dragutinovic & Scheper, 2006, p. 7; Muller et. al., 2010). Zo zijn er enkele respondenten die verwachten dat het, met behulp van geautomatiseerde gelaatsherkenning, makkelijker is een dader te herkennen of op te sporen. Wanneer daders deze verwachting ook zullen hebben neemt de kans op criminaliteit, volgens de afschrikkingstheorie en rationele keuzetheorie, af.

Concluderend kan er beargumenteerd worden dat voor het inzetten van geautomatiseerde gelaatsherkenning bij veel voorkomende criminaliteit er op zowel juridisch, ethisch en technisch vlak wel degelijk mogelijkheden zijn. Er moet hierbij wel rekening gehouden worden met de beperkingen die op dit moment nog spelen. Tevens zijn er gronden waardoor er gedacht kan worden dat geautomatiseerde gelaatsherkenning een bijdrage kan leveren aan het aanpakken van het veiligheidsvraagstuk in dit onderzoek, namelijk het verminderen van veel voorkomende criminaliteit in winkelcentra. Echter moeten we ons, als politieorganisatie of andere verwerker, afvragen of geautomatiseerde gelaatsherkenning ook wenselijk is in het licht van dit veiligheidsvraagstuk of dat dit zal leiden tot een te grote inbreuk op de persoonlijke levenssfeer.

8.2. Discussie

Naar aanleiding van de gevonden resultaten en de geraadpleegde literatuur is er in de conclusie een antwoord op de onderzoeksvraag geformuleerd. Hieruit is gebleken dat er zowel mogelijkheden en beperkingen zijn wanneer het gaat om het inzetten van geautomatiseerde gelaatsherkenning voor veel voorkomende criminaliteit in winkelcentra. In deze paragraaf zullen de sterke punten en beperkingen van dit onderzoek worden benoemd en zullen er aanbevelingen worden gedaan voor vervolgonderzoek.

8.2.1. Sterke punten en beperkingen van het onderzoek

Een van de belangrijkste sterke punten van dit onderzoek is dat er zowel gekeken is naar techniek, wetgeving en ethiek omtrent geautomatiseerde gelaatsherkenning ten behoeve van preventie en opsporing van veel voorkomende criminaliteit in winkelcentra in Nederland. Daarnaast is de hulp ingeroepen van professionals op het gebied van privacy en is er naast een literatuurstudie gebruik gemaakt van interviews. Hierdoor zijn er meerdere onderzoeksmethoden gebruikt wat een completer beeld schetst over ethische aspecten omdat in de interviews vragen gesteld zijn die gericht zijn op een specifieke situatie. Voorafgaand aan dit onderzoek was er weinig tot geen onderzoek dat zich richt op het inzetten van geautomatiseerde

gelaatsherkenning op bewegende mensen en het onderzoek dat er wel is gedaan ligt erg verspreid. Hierdoor was er voorheen geen duidelijk overzicht van wat wel en niet mogelijk is. Met dit onderzoek is er getracht een duidelijker beeld te schetsen over de mogelijkheden en beperkingen. Daarnaast wordt door middel van dit onderzoek duidelijk welke aspecten om meer onderzoek vragen en welke stappen verder genomen dienen te worden. Er was tevens nog geen onderzoek dat zich richt op het inzetten van geautomatiseerde gelaatsherkenning ten behoeve van de opsporing en preventie van veel voorkomende criminaliteit in winkelcentra in Nederland. Dit onderzoek is daarom breed opgezet zodat dit een basis kan vormen voor vervolgonderzoek. Belangrijk is het om te beseffen dat het technisch onderzoek voornamelijk onderzoek betreft dat op het internet gepubliceerd is en technieken betreft die tot 2015 zijn onderzocht. Technologie verandert snel, dit betekent dat ten tijde van het schrijven van dit onderzoek er al nieuwe onderzoeken, op het gebied van techniek, plaatsvinden. Hierdoor kan het zijn dat er al andere mogelijkheden zijn wat betreft het inzetten van geautomatiseerde gelaatsherkenning op grote groepen mensen.

Een ander punt van discussie is terug te vinden op het ethische vlak. Hierbij is er louter gekeken naar onderzoek dat reeds bekend is en zijn er 14 respondenten geïnterviewd welke al meer ervaring hebben met sensoren dan de gemiddelde burger. Het beeld dat met de interviews wordt geschetst hoeft hierdoor niet alle ethische aspecten te belichten, het kan zijn dat andere respondenten andere ethische aspecten aan het licht brengen.

Concluderend bestaan er een aantal punten binnen dit onderzoek waar informatie kan missen wat kan zorgen voor vertekening van de resultaten. Om deze vertekening te voorkomen worden in de volgende paragraaf van dit hoofdstuk een aantal aanbevelingen gedaan.

8.2.2. Aanbevelingen

Aan de hand van bovenstaande kunnen aanbevelingen voor vervolgonderzoek worden gedaan. Dit onderzoek betreft een basis voor meer onderzoek naar het inzetten van geautomatiseerde gelaatsherkenning ten behoeve van preventie en opsporing van veel voorkomende criminaliteit in winkelcentra. Om meer informatie te vergaren omtrent ethiek is het raadzaam om een grotere steekproef te trekken. Wellicht zorgt dit voor nieuwe inzichten wat betreft ethiek. Dit kan van belang zijn voor het wel of niet inzetten van geautomatiseerde gelaatsherkenning. Op deze manier worden er meer ethische aspecten behandeld en kan eventuele kritiek dat kan volgen na het inzetten van geautomatiseerde gelaatsherkenning van tevoren worden aangepakt. Daarnaast kan het wellicht interessant zijn om mensen met verschillende achtergronden te bevragen. In Villa B werken de respondenten bij de politie en hebben zij meer ervaring met nieuwe sensoren en ethische kwesties omtrent het inzetten van nieuwe sensoren dan bijvoorbeeld een arts of een huisvader/moeder. Op dit moment doet het Rathenau Instituut onderzoek naar ethische aspecten omtrent het inzetten van sensoren door de politie. Dit onderzoek kan op het gebied van ethiek verder inzicht verschaffen. Een andere aanbeveling is een aanbeveling op het gebied van techniek. Zoals is gebleken verandert de techniek voortdurend en zijn onderzoeken hieromtrent snel verouderd. Een aanbeveling is om als onderzoeker zelf bij verschillende proeven aanwezig te zijn waarbij eigen input kan worden gegeven.

Op deze manier kan er gericht gekeken worden naar de manier van inzet die wenselijk is voor de verwerker. Is het bijvoorbeeld mogelijk om een grote hoeveelheid mensen langs een bepaalde camera te laten lopen die allemaal dezelfde haarkleur hebben of waarbij meerdere tweelingen meelopen. Hoe werkt geautomatiseerde gelaatsherkenning dan? Een andere aanbeveling dat gedaan kan worden is een aanbeveling wanneer blijkt dat geautomatiseerde gelaatsherkenning niet voldoende werkt. Wellicht kan geautomatiseerde gelaatsherkenning gecombineerd worden met andere sensoren om patronen en bewegingen van mensen in kaart te brengen. Zo kunnen loopsnelheid en richtingsverandering bijvoorbeeld indicatoren zijn die zakkenrollers onderscheiden van onschuldige burgers (Bouma et. al., 2015).

Ten derde een aanbeveling op het gebied van wetgeving. Dit onderzoek betreft een omschrijving van juridische inzetkaders waardoor duidelijk welke stappen ondernomen moeten worden wil het inzetten van geautomatiseerde gelaatsherkenning rechtvaardig zijn. Om een beter beeld te scheppen over de grenzen van het inzetten en de afweging van proportionaliteit en subsidiariteit is het raadzaam om een bepaalde situatie voor te leggen aan een aantal rechters. Op deze manier wordt inzichtelijker wat wel en niet houdt in de rechtbank en in welke situatie geautomatiseerde gelaatsherkenning toegepast kan worden en welke niet.

Ook aan de hand van het hoofdstuk betreffende de verschillende toepassingsvormen kunnen er een aantal aanbevelingen worden gedaan voor vervolgonderzoek. Dit onderzoek schetst een eerste beeld van de mogelijkheden van geautomatiseerde gelaatsherkenning. Deze kunnen een beginpunt zijn om verschillende aspecten in kaart te brengen. Aan de hand hiervan kunnen aspecten zoals databeheer, juridische aspecten, technische mogelijkheden en onmogelijkheden, verwijderen van data en mogelijk problemen bij de verschillende toepassingsvormen in kaart worden gebracht. Dit kan helpen bij het onderzoeken van de mogelijkheden wat betreft het inzetten van geautomatiseerde gelaatsherkenning ten behoeve van preventie en opsporing van veel voorkomende criminaliteit in winkelcentra.

Ten slotte een aanbeveling wat betreft het onderzoeksgebied. Dit onderzoek richt zich op Nederland en de Nederlandse wetgeving. Ondanks dat de wetgeving in andere landen anders is kunnen de onderzoeken in deze landen wel een bijdrage leveren aan vervolgonderzoek. Zo is het raadzaam om bijvoorbeeld te onderzoeken welke technieken China gebruikt en welke software zij toepast. Deze kan wellicht een mogelijkheid zijn in de gewenste scenario's.

Al met al heeft dit onderzoek betekenis. Zoals vermeld is dit één van de eerste onderzoeken die de mogelijkheden en beperkingen op verschillende gebieden in kaart brengt. Dit onderzoek vormt een uitgangspunt voor vervolgonderzoek en een duidelijk overzicht van de mogelijkheden en beperkingen op dit gebied.

LITERATUUR

Algemeen Dagblad. (9 mei 2016). Daders ADO op zwarte lijst. Geraadpleegd op 5 december 2018 via: https://www.ad.nl/nederlands-voetbal/daders-ado-op-zwarte-lijst~af1f4ae6/

Algemeen Dagblad. (1 oktober 2018). FBI dwingt man tot gezichtsherkenning iPhone. Geraadpleegd op 10 oktober 2018 via: https://www.ad.nl/buitenland/fbi-dwingt-man tot-gezichtsherkenningiphone~a45aefee/

Algemene verordening gegevensbescherming (2016, 4 mei). Geraadpleegd op 18 november 2018 via: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg

Amnesty International, (z.j.). Menselijke waardigheid, respect en mensenrechten. Geraadpleegd op 17 december 2018 via: https://www.amnesty.nl/encyclopedie/menselijke-waardigheid-en-mensenrechten

Akkermans, M. (2016). *Melding en aangifte van veelvoorkomende criminaliteit: Stand van zaken, trends en kenmerken.* CBS: Sociaaleconomische trends.

Autoriteit persoonsgegevens (z.j). Wat zijn persoonsgegevens? Geraadpleegd op 6 november 2018 via: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Beyens, H. (2007). Over de beperkte diepgang van de rationele keuzetheorie. *Tijdschrift voor Criminologie*, *49* (1), 87-92.

Burns, J.H., & Hart, L.H.A. (1996). *The collected works of Jeremy Bentham: An introduction to the principles of morals and legislation.* Clarendon Press.

Bijbel en Overheid. (2017, 13 september). 7. Biometrische gezichtsherkenning: zwaarwegende ethische dilemma's. Geraadpleegd op 17 december 2018 via: http://www.bijbelenoverheid.nl/uncategorized/7-biometrische-gezichtsherkenning-zwaarwegende-ethische-dilemmas/

Bouma, H, van Rest, J.H.C., Burghouts, G.J., Schutte, K., & Baan, J. (2014). Automatische gedragsanalyse voor effectiever cameratoezicht in de openbare ruimte. *Tijdschrift voor Veiligheid*, *4* (13), 20-34.

Brandhof, M. van den.(2007). Veelvoorkomende criminaliteit. Casestudie ten behoeve van het project veiligheid. WWR Wetenschappelijke raad voor het regeringsbeleid, 35, 1-49.

Brouwers, M. (2004). Het lichaam als wachtwoord. *Perspectief*. 45-47. Geraadpleegd op 17 december via: http://pubnpp.eldoc.ub.rug.nl/FILES/root/tijdschriftartikel/Idee/2004/Id2004_1p45Brouwers/Idee_2004_01_p45_Brouwers.pdf

Centraal Bureau voor de Statistiek. (z.j.). *Verdachten van misdrijven*. Geraadpleegd op 1 december 2018 via: https://www.cbs.nl/nl-nl/onze-diensten/methoden/onderzoeksomschrijvingen/korte onderzoeksbeschrijvingen/verdachten-van-misdrijven

Centrum informatiebeveiliging en privacybescherming, (12 februari 2018). *Privacyafspraken bij ketensamenwerking.* Geraadpleegd op 18 januari 2019 via:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwiV_fyojvffAhUP66QKHVkuDl8QFjACegQIBxAC&url=https%3A%2F%2Fwww.cip-overheid.nl%2Fwp-content%2Fuploads%2F2018%2F03%2F20180212-Privacyafspraken-in-ketensamenwerking-v1_0.pdf&usg=AOvVaw1FT_MF1V2lDpiMCyb7lLoy

Cohen, L.E., & M. Felson (1979), Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review 4 4 ,588-608.

Colder, J.C., & Nuijten-Edelbroek, E. G. M. (1988). *Het winkelcentraproject: Preventie van kleine criminaliteit.* Den Haag: SDU.

Cornish, D.B., & Clarke, R.V. (1989). Crime Specialisation, Crime Sisplacement and Rational Choice Theory. In: Wegener H., Lösel F., Haisch J. (eds) *Criminal behavior and the justice system* (pp. 103-117). Springer, Berlin, Heidelberg.

Custers, B., & Vergouw B. (2015). Promising policing technologies: Experiences, obstavles and police needs regarding law enforcement technologies. *Computer Law & Security Review, 31* (4). 518-526.

Del Rio, J. S., Moctezuma, D., Conde, C., de Diego, I. M., & Cabello, E. (2016). Automated border control egates and facial recognition systems. *computers & security*, *62*, 49-72.

De Keizer, C. (2018). De opening van de 'black box' van open source gezichtsherkenningssoftware; *Mogelijke voordelen in trainingsdatasets gebruikt door open source gezichtsherkenningssoftware*. Universiteit Utrecht, Utrecht. Geraadpleegd op 23-01-2019 via: https://dspace.library.uu.nl/handle/1874/367620

Eindhovens Dagblad. (11 april 2017). PSV: Proef met gezichtsherkenning nog onvoldoende. Geraadpleegd op 5 december 2018 via: https://www.ed.nl/overig/psv-proef-met-gezichtsherkenning-nog-onvoldoende~ad165030/

Eggen, A. T. J., & Goudriaan, H. (2010). Geregistreerde criminaliteit. *R. van der Vliet, J. Ooijevaar en A. Boerdam (red.), Jaarrapport Integratie*, 143-156.

Engberts, B., & Copini, F. (2016). Sensing door de politie en publiek-private samenwerking: operationele noodzaak. Het Tijdschrift voor de Politie, 7, 18-22.

Europees verdrag tot bescherming van de rechten van de mens (1950, 4 november). Geraadpleegd op 6 december 2018 via: https://maxius.nl/verdrag-tot-bescherming-van-de-rechten-van-de-mens-en-de-fundamentele-vrijheden-rome-04-11-1950/artikel8

Grijpink, J.H.A.M. (2008). Biometrie: wat is het, hoe werkt het.

Goldenbeld, C., Morsink, P., Dragutinovic, N., & Scheper, W. (2006). Veiliger verkeer door snelheidsbeheersing. Geraadpleegd op 2 juni 2018 via: https://www.researchgate.net/profile/Charles_Goldenbeld/publication/256195706_Veiliger_verkeer_door_snelheidsbeheersing/links/0deec521f49937f992000000.pdf

Grother, P.J., Ngan, M.L. & Quinn, G.W. (2017). Face In Video Evaluation (FIVE); Face Recognition of Non-Cooperative Subjects. *NIST Interagency/International Report (NISTIR) – 8173*. Geraadpleegd

op 30 oktober 2018 via: https://www.nist.gov/publications/face-video-evaluation-five-face-recognition-non-cooperative-subjects

Haighton, M. (16 oktober 2004). We zijn een merk op zichzelf geworden. *De Volkskrant.* Geraadpleegd op 15 juni 2018 via: https://www.volkskrant.nl/economie/-we-zijn-een-merk-op-zichzelf-geworden-~bab9f536/

Jain, A. K., Klare, B., & Park, U. (2011, March). Face recognition: Some challenges in forensics. In *Automatic Face & Gesture Recognition and Workshops (FG 2011), 2011 IEEE International Conference on* (pp. 726-733). IEEE.

Leman-Langlois, S. (2003). The myopic panopticon: The Social consequences of policing through the lens. *Policing and Society, 13*(1), 43-58.

Leonards, R. (01 april 2015). Camera met gezichtherkenning tegen overvallen. *Missethoreca.nl*. Geraadpleegd op 15 september 2018 via: https://www.missethoreca.nl/cafe/nieuws/2012/05/camera-met-gezichtsherkenning-tegen-overvallen-10184252?vakmedianet-approve-cookies=1?vakmedianet-approve-cookies=1

Melgaço, L. (2015). Meer camera's, meer veiligheid? Een analyse over de doeltreffendheid van videosurveillance. *Orde van de Dag,* 69, 43-52.

Ministerie van Justitie en Veiligheid (januari 2018). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming.* Geraadpleegd op 06-11-2018 via: https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

Mulder, T. (16 mei 2018). Hoe je door gezichtsherkenning of cameratoezicht in de problemen kan komen. *De monitor.* Geraadpleegd op 23 oktober 2018 via: https://demonitor.kro-ncrv.nl/artikelen/hoe-je-door-gezichtsherkenning-of-cameratoezicht-in-de-problemen-kan-komen

Muller, E. R., Van der Leun, J. P., Moerings, L. M., & Van Calster, P.J.V. (2010). Ruimtelijke verplaatsing van criminaliteit: theorie, methodologie en empirie. In *Criminaliteit en criminaliteitsbestrijding in Nederland* (pp. 375-394). Kluwer: Alpen aan den Rijn.

Nationale Politie. (2012). Inrichtingsplan nationale politie. *Den Haag: Rijksoverheid*. Geraadpleegd op 25 07-2018 via: https://www.mensenhandelweb.nl/en/system/files/documents/10%20feb%202014/blg-198145.pdf

Nederlands Forensisch Instituut, (18 oktober 2017). *Algemene onderzoeksmethode vergelijking van gezichtsbeelden*. Geraadpleegd op 20 september 2018 via: https://www.forensischinstituut.nl/over-het-nfi/publicaties/publicaties/2017/10/18/bijlage-vergelijking-gezichtsbeelden-versie

NOS. (29 juli 2018). *Gezichtsherkenning als toegangskaartje, mag dat?* Geraadpleegd op 30 juli 2018 via: https://nos.nl/artikel/2243694-gezichtsherkenning-als-toegangskaartje-mag-dat.html

Kist, R. (19 februari 2018). Gezichtsherkenning wordt mainstream. *NRC Handelsblad*. Geraadpleegd op 15 oktober 2018 via: https://www.nrc.nl/nieuws/2018/02/19/en-dat-scannen-is-straks-heel-gangbaar-a1592782

Olsthoorn, P. (2017, 8 januari). Gezichtsherkenning voltooit het digitale panopticum. *Netkwesties*.

Geraadpleegd op 17 december 2018 via: https://www.netkwesties.nl/947/gezichtsherkenning-voltooit-digitale.htm

Pauwels, L. (2015). Angst voor de negatieve gevolgen van criminaliteit, criminele geneigdheid en jeugddelinquentie. Wie laat zich bij het plegen van een delict leiden door percepties van de pakkans? *Handboek Politiediensten, afl. 116*, 24, september 2015, 227-251.

Politie (2010, 11 juni). Monitoren Top-X mbv ANPR [intern document]

Politie (2012, 24 oktober). Geautomatiseerde gelaatsherkenning RT [intern document]

Politie (2015, 1 mei). Juridische aspecten inzet automatische geautomatiseerde gelaatsherkenning bij DBB [intern document]

Politie (2016, maart). Verbeterplan Wet politiegegevens en informatiebeveiliging.

Politie (2017, maart). Factsheet Gelaatsvergelijking [intern document].

Politie (2018, mei). Wet politiegegevens; Praktijkhandboek [intern document].

Politie. (z.j.). *Mobiel banditisme*. Geraadpleegd op 3 juli 2018 via: https://www.politie.nl/themas/mobiel-banditisme.html

Politie. (z.j.). *Systeem voor geautomatiseerde gelaatsherkenning operationeel*. Geraadpleegd op 2 juli 2018 via: https://www.politie.nl/nieuws/2016/december/16/11-systeem-voor-geautomatiseerde gelaatsherkenning-operationeel.html

Politiewet (12 juli 2012). Geraadpleegd op 1 november 2018 via: https://wetten.overheid.nl/BWBR0031788/2018-09-19

Posthoorn, J. (2015). Biometrische veiligheid: Een overzicht van veelgebruikte methoden. Geraadpleegd op 31 mei 2018 via: https://docplayer.nl/20053418-Biometrische-veiligheid.html

Programma Sensing. (2017, 17 oktober). Governance en programma beheersing 2018 [intern document].

Programma Sensing. (2018, 25 januari). Programmaplan 2018-2019 [intern document].

Rooij, van, B.J. (1 december 2006). PSV: proef met gezichtsherkenning nog onvoldoende. *Eindhovens dagblad*. Geraadpleegd op 15 oktober 2018 via: https://www.ed.nl/overig/psv-proef-met-gezichtsherkenning-nog-onvoldoende~ad165030/

RTVNoord. (15 september 2016). FC Groningen start proef met gezichtsherkenning bij ticketcontrole. Geraadpleegd op 21 oktober via: https://www.rtvnoord.nl/nieuws/167783/FC-Groningen-start-proef-met-gezichtsherkenning-bij-ticketcontrole

Sajtos, J. (2009). Komt de woninginbreker weer op bezoek, of gaat hij liever naar de buren?: *Een kwantitatieve analyse naar herhaald slachtofferschap en risicobesmetting van woninginbraak* (Masterscriptie). Universiteit van Leiden, Leiden. Geraadpleegd op 12 april 2018 via: https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Woninginbraak/Documenten/Komt_de_woninginbreker_weer_op_bezoek_of_gaat_hij_liever_naar_de_buren/komt-de-woninginbreker-weer-op-bezoek.pdf

Schiphol (7 februari 2017). Test op Schiphol: snel en eenvoudig aan boord via gezichtsherkenning.

Geraadpleegd op 5 december 2018 via: https://nieuws.schiphol.nl/test-op-schiphol-snel-en-eenvoudig-aan-boord-via-gezichtsherkenning/

Security.nl. (28 maart 2018). China wil gezichtsherkenning inzetten om boetes via sms te versturen. Geraadpleegd op 24 oktober 2018 via: https://www.security.nl/posting/555977/China+wil+gezichtsherkenning+inzetten+om+boetes+via+sms+te+versturen

Strijbosch, V. (30 november 2017). Slimme snufjes op innovatiebeurs. *KMarMagazine*. Geraadpleegd op 23 juli 2018 via: https://magazines.defensie.nl/kmarmagazine/2017/10/01_purple_nectar_10-2017

Technologiescan, Veiligheid & Justitie (2017, 20 maart). Aanet voor een strategie om tegemoet te komen aan de 'smart'-uitdaging van het ministerie van Veiligheid en Justitie [intern document].

Ten Voorde, J. M. (2008). Strafrechtstheoretische bespiegelingen over afschrikking en generale preventie. Justitiële verkenningen, 34, 13.

Trouw. (8 februari 2007). ADO weert hooligans met gezichtsherkenning. Geraadpleegd op 30 juni 2018 via: https://www.trouw.nl/home/ado-weert-hooligans-met-gezichtsherkenning~a1aedc85/

Tweede Kamer (2015). Waarnemen met technische hulpmiddelen [Kamerbrief]. Geraadpleegd op 30 mei 2018 via: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z22421&did=2015D45494

Uitvoeringswet algemene verordening gegevensbescherming (2018, 25 mei). Geraadpleegd op 18 november 2018 via: https://wetten.overheid.nl/BWBR0040940/2018-05-25

Vaane, J. (2014). Ongewenst gedrag op de voetbalvereniging: Een onderzoek naar de samenhang *tussen sociale bindingen en de mate van ongewenst gedrag bij amateurverenigingen* (Masterscriptie). Universiteit Utrecht, Utrecht. Geraadpleegd op 12 april 2018 via: https://dspace.library.uu.nl/handle/1874/301427

Veldhuis, R.N.J. (2014). *Biometrie – op de grens tussen techniek en mens.* Universiteit van Twente.

Vonk, M., & Dorrestijn, S. (z.j.). Waardengericht ontwerpen en toepassen van zorgtechnologie. *Filosofie & Praktijk.*

Welzen, van, Y. (2011). Opsporing misbruik beeldmateriaal: prestaties van gezichtsherkenningssoftware. *KPB*, *11*, 1-27. Geraadpleegd via: https://dspace.library.uu.nl/handle/1874/205554

Wetboekboek van Strafvordering (2018, 16 oktober). Geraadpleegd op 6 december 2018 via: https://wetten.overheid.nl/BWBR0001903/2018-10-16

Wet politiegegevens (2017, 21 juli). Geraadpleegd op 01-12-2018 via: https://wetten.overheid.nl/BWBR0022463/2018-05-01

Winkels zetten gezichtsherkenning in tegen veelplegers (14 april 2002). *Nu.nl*. Geraadpleegd op 16 juni 2018 via: https://www.nu.nl/algemeen/307767/winkels-zetten-gezichtsherkenning-in-tegen-veelplegers.html

Zembla (25 april 2012). ICT-chef Nationale Politie vertrekt. Geraadpleegd op 1 december 2018 via:

https://zembla.bnnvara.nl/nieuws/ict-chef-nationale-politie-vertrekt

Zenger, R. (2016, 21 december). Wat als de mens het onmenselijke kan? *Bits of Freedom*. Geraadpleegd op 17 december 2018 via: https://www.bitsoffreedom.nl/2016/12/21/wat-als-de-mens-het-onmenselijke-kan/#comment-255639

BIJLAGEN

Bijlage 1

Interview om de eerste ethische aspecten in kaart te brengen.

Informatief

1. Wat is uw rol binnen het Programma Sensing? (functie)
2. Welke achtergrond heeft u qua werkervaring?
3. Was u voor dit onderzoek al bekend met geautomatiseerde gelaatsherkenning en zo ja, op welke manier?
4. Kunt u me wat vertellen over hoe u denkt dat geautomatiseerde gelaatsherkenning werkt?

Onderzoeksvragen

5. Denkt u dat er een juridische basis kan zijn voor het toepassen van geautomatiseerde gelaatsherkenning en hoe ziet u dit voor u?
6. Wat vindt u van geautomatiseerde gelaatsherkenning ten behoeve van:

Ten behoeve van:	**Positief**	**Negatief**	**Anders, namelijk**	**Waarom?**
Paspoortcontrole				
Toegang bij ADO				
Beveiliging personen				
Ontgrendelen telefoon				
Betalen bij winkels/bank				
Toegang tot gebouwen/werk				

7. Wat was uw eerste reactie toen bekend werd dat er met geautomatiseerde gelaatsherkenning gewerkt zou worden in Villa B? (situatie voor & na, kunt u nog herinneren wat uw gedachten waren)
    a. Negatief? Waarom dan wel toestemming?
    b. Positief? Waarom?
8. Wat vindt u goed aan geautomatiseerde gelaatsherkenning? (voorargumenten voor geautomatiseerde gelaatsherkenning)
9. Wat ziet u als problemen bij geautomatiseerde gelaatsherkenning?
10. Waar ziet u kansen voor het toepassen van geautomatiseerde gelaatsherkenning door de politie?
    a. Wat moet er dan gewaarborgd worden?
    b. Wat moet er gebeuren voordat het toegepast moet worden?
    c. Zijn er nog andere aspecten waar naar uw mening naar gekeken moet worden?
11. Wat vindt u van het idee dat de politie geautomatiseerde gelaatsherkenning zal inzetten in hun dagelijkse activiteiten? (opsporing & preventie)
    a. Negatief? In alle omstandigheden?
    b. Positief? Waarom juist goed?

BV ten behoeve van:	**Positief**	**Negatief**	**Anders, namelijk**	**Waarom?**
Terrorismebestrijding op Schiphol				
Terrorismebestrijding bij grote evenementen (bv. koningsdag)				
Opsporen dader van een ernstig delict (bv. moord, verkrachting, kinderporno)				
Voorkomen van VVC (bv. woninginbraak, diefstal (winkel, voertuigen)				
Opsporen dader van minder ernstig delict (bv. woninginbraak, winkeldiefstal, fietsendiefstal)				

Voorkomen van ernstig delict (bv. een buurt waar veel verkrachting of moord plaatsvindt)				
RTI (Real Time Identification), daders zsm identificeren met behulp van heimelijke beelden				

12. Stel, er kan een keuze gemaakt worden tussen een aantal alternatieven, voor welke kiest u en waarom?
    a. Geautomatiseerde gelaatsherkenning op basis van sensoren (zoals in de Villa)
    b. Automatische detectie van gedrag (sensoren 'pikken' als het ware verdacht gedrag op en zenden een melding)
    c. Herkenning op basis van menselijk geheugen (bv. winkelier die de dief herkent)
13. Wat zou u vinden van geautomatiseerde gelaatsherkenning wanneer:
    a. Het alleen werkt als de persoon enkele seconden stilstaat voor de camera (zoals bij Schiphol)
    b. Het de criminaliteitscijfers naar beneden haalt?
    c. Wanneer de politie een foto van iedereen als referentie wilt gebruiken?
    d. Wanneer het toegepast wordt op camera's die al aanwezig zijn?
14. Hebben uw antwoorden te maken met de ervaringen die u heeft mbt geautomatiseerde gelaatsherkenning?
    a. Zou u anders hebben gedacht wanneer u een 'normale' burger bent, bv. huisvrouw of man?
    b. Zou u anders hebben gedacht als winkelier zijnde waarbij constant sprake is van diefstal?
    c. Zou u anders hebben gedacht wanneer u zelf slachtoffers bent geweest van zakkenrollerij?
15. Nu we het verder besproken hebben, denkt u anders over geautomatiseerde gelaatsherkenning of heeft u een ander idee voor de juridische basis hiervan?

Bijlage 2

Wettelijk kader private partijen

Bij geautomatiseerde gelaatsherkenning wordt er gebruik gemaakt van biometrische gegevens (Leman-Langlois, 2003; Grijpink, 2008; Veldhuis, 2014; Posthoorn, 2015). Biometrische gegevens zijn volgens de AVG een bijzondere categorie van persoonsgegevens (Ministerie van Veiligheid en Justitie, 2018). Wanneer een private partij te maken heeft met (het verwerken van) persoonsgegevens is de AVG van toepassing. In deze bijlage zullen de belangrijke begrippen van de AVG worden uitgelegd en zullen de voorwaarden die de AVG stelt aan het gebruiken van persoonsgegevens en de plichten die hierbij komen worden toegelicht.

Artikel 2 lid 1 van de AVG bepaald wanneer de AVG van toepassing is, de wettekst luidt als volgt: "Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen".

Geautomatiseerde gelaatsherkenning is een geautomatiseerde verwerking van persoonsgegevens, en specifiek van biometrische gegevens. Het toepassen van geautomatiseerde gelaatsherkenning valt dan ook onder de regels die gesteld zijn door de AVG. Hieronder zullen er een aantal belangrijke begrippen uit de AVG worden omschreven.

Beginselen inzake verwerking persoonsgegevens

Hieronder worden de beginselen inzake de verwerking van persoonsgegevens besproken welke in de AVG worden genoemd. Vanuit deze beginselen wordt duidelijk wanneer geautomatiseerde gelaatsherkenning toegepast mag worden en onder welke omstandigheden. De beginselen worden in deze paragraaf apart besproken en zijn terug te vinden in artikel 5 van de AVG.

Rechtmatig, behoorlijk & transparant

Het eerste beginsel noemt dat de persoonsgegevens rechtmatig, behoorlijk en transparant worden verwerkt (art. 5 lid 1 onder a AVG). Het uitgangspunt hierbij is dat persoonsgegevens alleen verwerkt mogen worden voor gerechtvaardigde doeleinden. De verwerking moet hierbij noodzakelijk zijn bij het bereiken van een specifiek doel. Bij het rechtvaardig verwerken van persoonsgegevens moet dit vervolgens verantwoord gebeuren. Daarnaast moet duidelijk zijn voor welke doelen deze gegevens worden verwerkt en hoe dat gebeurt (Ministerie van Veiligheid en Justitie, 2018).

Het verwerken van persoonsgegevens is gerechtvaardigd wanneer aan een van de zes grondslagen, bij de wet genoemd, wordt voldaan. Deze grondslagen zijn terug te vinden in artikel 6 lid 1 van de AVG. Een overzicht van deze grondslagen, met daarbij hun uitleg, zijn hieronder terug te vinden.

Art. 6 lid 1 onder a

Artikel 6 lid 1 onder a luidt als volgt: "De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden".

Hierbij moet sprake zijn van een aantal voorwaarden. De toestemming moet vrij gegeven zijn, de persoon in kwestie moet ook kunnen weigeren. Verder moet de toestemming specifiek en geïnformeerd zijn. Het moet voor de toestemming verlenende persoon duidelijk zijn waarom de gegevens worden verwerkt (doel) en alle informatie die voor deze persoon van belang is moet duidelijk zijn. Daarnaast moet de toestemming ondubbelzinnig zijn. Dit houdt in dat er geen twijfel mag zijn over het feit dat de persoon in kwestie toestemming heeft verleend. Bij deze grondslag zijn er dan ook drie voorwaarden; vrije toestemming, specifieke en geïnformeerde persoon en ondubbelzinnigheid. Als verwerkingsverantwoordelijke moet u kunnen aantonen dat toestemming is verkregen. Hierbij moet het geven van toestemming op een duidelijke manier zichtbaar zijn en moet voor de betrokkene duidelijk zijn waarvoor hij/zij toestemming verleend. Ook geldt dat de betrokkene te allen tijde zijn toestemming mag intrekken. Wanneer de betrokkene nog geen 16 jaar is, moeten de ouders over degene die verantwoordelijk zijn voor de betrokkene, toestemming geven. Deze voorwaarden zijn terug te vinden in artikel 7 van de AVG en in de Handleiding Algemene verordening gegevens bescherming van het Ministerie van Justitie en Veiligheid (2018).

Art. 6 lid 1 onder b

"De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen".

Wanneer een consument bijvoorbeeld een product op het internet besteld mag de leverancier van dit product, gegevens verwerken zodat het product bij de consument geleverd kan worden. Dit is een voorbeeld van het verwerken van persoonsgegevens om aan de uitvoering van een overeenkomst te kunnen voldoen (Ministerie van Veiligheid en Justitie, 2018).

Art. 6 lid 1 onder c

"De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust".

De wettelijke plicht moet terug te vinden zijn in het recht van de Europese Unie of in het recht van de lidstaat. Hierin moet ook het doel van de verwerking staan. Een voorbeeld hierbij is dat een werkgever een kopie van hun werknemer zijn/haar identiteitskaart moet hebben (Ministerie van Veiligheid en Justitie, 2018).

Art. 6 lid 1 onder d

"De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen".

Deze grondslag kan alleen worden gebruikt wanneer er niet aan een van de andere grondslagen wordt voldaan. Een voorbeeld hierbij is wanneer betrokkene medische hulp nodig heeft. Hulpverleners mogen dan persoonsgegevens verwerken om noodzakelijke medische hulp te verlenen (Ministerie van Veiligheid en Justitie, 2018).

Art. 6 lid 1 onder e

"Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen".

De taak die hierin wordt omschreven dient een taak te zijn die voortvloeit uit Europees recht of uit het recht van de lidstaat. Ook hier moet het doel duidelijk zijn. Een voorbeeld hierbij is de Raad van de Kinderbescherming die voor de vervulling van haar taak persoonsgegevens moet verwerken (Ministerie van Veiligheid en Justitie, 2018).

Art. 6 lid 1 onder f

Artikel 6 lid 1 onder f noemt de laatste grondslag waarop persoonsgegevens verwerkt mogen worden, het artikel luidt als volgt:

> De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De gerechtvaardigde belangen dienen hierbij afgewogen te worden tegen de rechten, vrijheden en belangen van de betrokkenen. Pas wanneer de belangen zwaarder wegen mogen persoonsgegevens worden verwerkt (Ministerie van Veiligheid en Justitie, 2018).

De grondslagen die onder b tot en met f zijn staan zijn de noodzakelijkheidsgrondslagen. Alleen wanneer de verwerking noodzakelijk is voor het nastreven van de doelen die in de grondslagen zijn vermeld, is de verwerking gerechtvaardigd. Om te bepalen of de verwerking noodzakelijk is zijn de proportionaliteitseis en de subsidiariteitseis van toepassing. De verwerking moet proportioneel zijn. Deze eis bestaat uit twee elementen; effectiviteit en evenredigheid. Wanneer het verwerken van de gegevens niet het doel kan bereiken of dat het bereiken van dit doel onwaarschijnlijk is dan wordt er niet voldaan aan het element van de effectiviteit. Het element van evenredigheid houdt in dat het doel dat wordt nagestreefd in verhouding moet staan tot het feit dat daarvoor persoonsgegevens verwerkt moeten worden. Bij de subsidiariteitseis gaat het over de vraag of het doel niet op een andere, minder ingrijpende wijze kan worden bereikt (Ministerie van Veiligheid en Justitie, 2018).

De grondslagen die in artikel 6 lid 1 AVG staan gelden voor persoonsgegevens zoals gedefinieerd in artikel 4 lid 1 AVG. Wanneer het gaat om bijzondere persoonsgegevens, zoals biometrische gegevens die worden gebruikt bij geautomatiseerde gelaatsherkenning, gelden er andere grondslagen. Bijzondere persoonsgegevens mogen namelijk niet worden verwerkt (art. 9 lid 1 AVG). Echter, er zijn een aantal uitzonderingen die bepalen dat bijzondere persoonsgegevens wel verwerkt mogen worden. Deze staan in artikel 9 lid 2 AVG. In tabel 11 worden deze kort benoemd.

Tabel 11

Uitzonderingen voor het verwerken van bijzondere persoonsgegevens

Art. AVG	Uitzondering
9 lid 2 onder a	De betrokkene heeft uitdrukkelijk toestemming gegeven
9 lid 2 onder b	De verwerking is noodzakelijk in het kader van de uitvoering van regels op het gebied van arbeids- en sociale zekerheidsrecht
9 lid 2 onder c	De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een ander natuurlijke persoon
9 lid 2 onder d	De verwerking wordt verricht door een stichting, een vereniging of andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is.
9 lid 2 onder e	De verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt
9 lid 2 onder f	De verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsprekende bevoegdheid
9 lid 2 onder g	De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang
9 lid 2 onder h	De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondsheidszorgstelsels en –diensten of sociale stelsels en diensten
9 lid 2 onder i	De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid
9 lid 2 onder j	De verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden

Opmerking. Gegevens afkomstig uit de handleiding Algemene verordening gegevensbescherming van het Ministerie van Justitie en Veiligheid.

Naast artikel 9 lid 2 AVG bevat de Uitvoeringswet Algemene verordening gegevensbescherming [UAVG] ook een aantal uitzonderingen op het verbod inzake het gebruik van biometrische gegevens. Artikel 29 UAVG bepaald dat, indien de biometrische persoonsgegevens worden gebruikt voor de identificatie van personen met het doel authenticatie of beveiliging, het verwerken van biometrische gegevens wel is toegestaan.

Met transparantie wordt bedoeld dat de verwerker van de gegevens duidelijk moet maken voor welke doelen deze gegevens worden gewerkt en welke gegevens u precies verwerkt. Daarnaast moet duidelijk zijn of de persoonsgegevens worden gedeeld met andere partijen en hoelang de gegevens bewaard worden (Ministerie van Veiligheid en Justitie, 2018).

Gerechtvaardigde doeleinden

Artikel 5 lid 2 sub b benoemt dat het verwerken van persoonsgegevens alleen mag gebeuren voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Persoonsgegevens mogen niet zomaar verzameld worden met het idee dat deze in de toekomst nog bruikbaar kunnen zijn. De doelen, dit mogen er meerdere tegelijkertijd zijn, moeten duidelijk omschreven zijn en van tevoren bepaald. Verder is het doel gerechtvaardigd wanneer het gebaseerd is op één van de zes grondslagen die de Verordening noemt (Ministerie van Veiligheid en Justitie, 2018).

Toereikend & noodzakelijk

Het derde beginsel stelt dat het verwerken van persoonsgegevens toereikend en beperkt moet zijn tot wat noodzakelijk is voor het nastreven van de doelen. Er dient dus sprake te zijn van minimale gegevensverwerking (Art. 5 lid 1 onder c AVG). Dit houdt in dat gelet op het doel, niet te veel maar ook niet te weinig gegevens verwerkt mogen worden. Ook het te weinig verwerken van gegevens is niet toegestaan. Dit omdat dit kan zorgen voor een onvolledig beeld van de betrokkene (Ministerie van Veiligheid en Justitie, 2018).

Juistheid

Met het beginsel van juistheid wordt bedoeld dat alle persoonsgegevens die worden verwerkt en verzameld geactualiseerd dienen te worden. Alle redelijke maatregelen moeten worden genomen om de persoonsgegevens juist en up-to-date te hebben (art. 5 lid 1 onder d AVG).

Niet langer bewaard dan nodig

Dit beginsel wordt ook wel gezien als de opslagbeperking. Persoonsgegevens mogen niet langer bewaard worden dan dat noodzakelijk is. Wanneer het niet langer noodzakelijk is om de gegevens te bewaren moeten deze worden vernietigd (art. 5 lid 1 onder e AVG; Ministerie van Veiligheid en Justitie, 2018).

Beveiliging

Het laatste beginsel gaat in op de beveiliging van de persoonsgegevens. De persoonsgegevens moeten beveiligd zijn. Ze moeten beschermd worden tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Dit wordt ook wel de integriteit en vertrouwelijkheid genoemd (Art. 5 lid 1 onder f AVG; Ministerie van Veiligheid en Justitie, 2018).

Persoonsgegevens van strafrechtelijke aard

Naast bovengenoemde beginselen is het belangrijk om rekening te houden met artikel 10 van de AVG. Wanneer er namelijk persoonsgegevens worden verwerkt die betrekking hebben op strafbare feiten, strafrechtelijke veroordelingen of die verband houden met veiligheidsmaatregelen of persoonsgegevens die verkregen zijn door een verbod dat is opgelegd door de rechter, mogen deze alleen worden verwerkt onder toezicht van de overheid, voor zover is toegestaan in de uitvoeringswet en op basis van een gerechtvaardigde grondslag. Informatie van strafrechtelijke veroordelingen mogen dan ook alleen worden bijgehouden onder toezicht van de overheid. Er zijn echter een aantal uitzonderingsgronden op het verbod

om persoonsgegevens met strafrechtelijke aard te verwerken (Ministerie van Veiligheid en Justitie, 2018). Deze worden hieronder kort weergegeven in tabel 12.

Tabel 12

Uitzonderingen voor het verwerken van persoonsgegevens van strafrechtelijke aard

Uitzonderingsgrond
"Uitdrukkelijke toestemming van de betrokkene"
"Situaties waar de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of een ander natuurlijk persoon"
"Situaties waar de verwerking betrekking heeft op gegevens die door de betrokkene openbaar zijn gemaakt"
"Situaties waar de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een verordening"
"Gerechten die handelen in het kader van hun rechtsbevoegdheid"
"Situaties waar de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang"
"Situaties waar de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden en is voldaan aan alle toepasselijke voorwaarden uit de Verordening"
"Verwerkingen door verwerkingsverantwoordelijken die zijn belast met de toepassing van het strafrecht, of door verwerkingsverantwoordelijken die de gegevens op grond van de Wet politiegegevens of de Wet Justitiële en strafvorderlijke gegevens hebben gekregen"
"Verwerkingen door publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken wanneer dit noodzakelijk is voor de uitvoer van hun taken en passende waarborgen zijn getroffen"

In deze bijlage zijn de beginselen besproken die de AVG heeft gesteld wil het verwerken van persoonsgegevens volgens de wet mogen. Om een duidelijk beeld te geven is dit weergegeven in figuur 2 op pagina 34 van dit onderzoek.

Plichten van de verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is verplicht passende en effectieve maatregelen te nemen. De plichten worden genoemd in de Verordening. Daarnaast moet de verwerkingsverantwoordelijke ook kunnen aantonen dat deze plichten worden nageleefd. De maatregelen die genomen worden moeten in verhouding staan met het risico. Wanneer het risico voor de betrokkene hoger wordt, dan moeten de maatregelen strikter zijn, ook de verantwoordingsplicht is uitgebreider (Ministerie van Veiligheid en Justitie, 2018).

Er zijn een aantal maatregelen die een verwerkingsverantwoordelijke dient te treffen, deze worden hieronder besproken.

Registerplicht

De verwerkingsverantwoordelijke heeft een registerplicht. Dit houdt in dat er een register bij gehouden moet worden met de verwerkingsactiviteiten. Dit betreft informatie over de verwerking van de persoonsgegevens. Er is echter een uitzondering op de registerplicht. Namelijk wanneer een onderneming minder dan 250 medewerkers in dienst heeft dan geldt het registerplicht niet. Ook hier zijn weer uitzonderingen op. Wanneer het risico te hoog is of de verwerking niet-incidenteel is of wanneer er sprake van verwerking ban bijzondere persoonsgegevens of gegevens betreffende strafbare feiten, dan geldt ook voor deze ondernemingen het registerplicht. Het registerplicht en de gegevens die het register moet bevatten zijn terug te vinden in artikel 30 van de AVG (Ministerie van Veiligheid en Justitie, 2018).

Functionaris voor gegevensbescherming

Een functionaris voor gegevensbescherming houdt toezicht op de toepassing en naleving van de Verordening. Daarnaast adviseert hij/zij ook op deze punten de organisatie. Een functionaris voor gegevensbescherming dient aangewezen te worden, door de verwerkingsverantwoordelijke en de verwerker, wanneer er sprake is van een van de gevallen welke in artikel 37 lid 1 AVG worden genoemd. Het eerste geval betreft het geval waarin de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan. Het tweede geval betreft het geval waarin de verwerkingsverantwoordelijke of de verwerker voornamelijk is belast met verwerkingen die vanwege hun omvang, aard en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen. Van regelmatige en stelselmatige observatie is sprake wanneer er over een bepaalde periode betrokkenen worden gevolgd en van hen persoonsgegevens worden vastgelegd. Het derde en laatste geval betreft het geval waar de verwerkingsverantwoordelijke of verwerker belast is met het verwerken van bijzondere persoonsgegevens of persoonsgegevens van strafrechtelijke aard.

Gegevensbeschermingseffectbeoordeling

Met het vooraf uitvoeren van een gegevensbeschermingseffectbeoordeling wordt de aard, de oorsprong en de ernst van risico's voor de bescherming van de vrijheden en rechten van betrokkenen geanalyseerd (art. 35 AVG; Ministerie van Veiligheid en Justitie, 2018). Op deze manier kan er inzicht worden verkregen om te zien of de maatregelen die genomen worden wel voldoende zijn in het specifieke geval (Ministerie van Veiligheid en Justitie, 2018).

Voorafgaande raadpleging

Volgens artikel 36 lid 1 moet de verwerkingsverantwoordelijke de voorgenomen verwerking voorleggen aan de Autoriteit Persoonsgegevens wanneer uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een te hoog risico zou opleveren indien er niet voldoende maatregelen worden genomen. Autoriteit Persoonsgegevens geeft een oordeel over de voorgenomen verwerking. Pas wanneer deze positief is mag er begonnen worden met de verwerking (Ministerie van Veiligheid en Justitie, 2018).

Privacy by design & default

Privacy by design & default houdt in dat de bescherming van privacy en gegevensbescherming wordt meegenomen in de ontwikkeling van het ontwerp van een nieuw systeem waar persoonsgegevens mee worden verwerkt. Belangrijk hierbij is dat er een zo klein mogelijke inbreuk wordt gemaakt op de persoonlijke levenssfeer bij de verwerking van de persoonsgegevens (Ministerie van Veiligheid en Justitie, 2018).

Beveiligingsmaatregelen

Artikel 32 lid 1 AVG stelt dat er een beveiligingsniveau moet zijn welke een aantal aspecten moet omvatten. Deze zijn weergegeven in tabel 13.

Tabel 13

Waarborgen bij beveiliging

Art. AVG	Waarborg
Art. 32 lid 1 onder a	"Pseudonimisering en versleuteling van persoonsgegevens"
Art. 32 lid 1 onder b	"Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen"
Art. 32 lid 1 onder c	"Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen"
Art. 32 lid 1 onder d	"Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking"

Melden bij datalek

Artikelen 33 en 34 AVG bepalen dat indien er een datalek heeft plaatsgevonden, dit gemeld moet worden aan de Autoriteit Persoonsgegevens en aan de betrokkene. Er is sprake van een datalek wanneer de inbreuk op de beveiliging leidt tot vernietiging, verlies, wijziging, ongeoorloofde toegang of verstrekking van de persoonsgegevens (Ministerie van Veiligheid en Justitie, 2018).

Afspraken met verwerkers

Wanneer er gebruik gemaakt wordt van een verwerker dan moet de verwerking geregeld worden in een overeenkomst (art. 28 lid 3 AVG). Er dient een overeenkomst opgemaakt te worden waarin het onderwerp en de duur van de verwerking worden genoemd, de aard en het doel van de verwerking, het soort persoonsgegevens die worden verwerkt en de rechten en verplichtingen van de verwerkingsverantwoordelijke (Ministerie van Veiligheid en Justitie, 2018).

Plichten van de verwerker

Naast plichten voor een verwerkingsverantwoordelijke zijn er ook plichten verbonden aan de verwerker. Deze plichten zijn terug te vinden in artikel 28 van de AVG. Dit artikel stelt dat de verwerker aan een aantal plichten moet voldoen. Allereerst moet de verwerker voldoende garanties kunnen bieden, zo stelt

artikel 28 lid 1 AVG. Deze garanties hebben betrekking op de naleving van de Verordening. Als tweede moet de verwerker een verwerkersovereenkomst tekenen waarin de afspraken met de verwerkingsverantwoordelijke staan. Deze afspraken gaan bijvoorbeeld over de manier van omgaan met de gegevens. Verder mag de verwerker, volgens artikel 28 lid 2, een andere verwerker in dienst nemen. Dit mag alleen wanneer de verwerker hiervoor schriftelijke toestemming heeft gekregen van de verwerkingsverantwoordelijke. Ook hier moeten duidelijke afspraken worden gemaakt en moet een overeenkomst worden getekend. Verder moet de verwerker zijn of haar verwerkingsactiviteiten registeren. Een andere plicht die de verwerker heeft is dat hij of zij moet meewerken met de Autoriteit Persoonsgegevens (Ministerie van Veiligheid en Justitie, 2018).

Bijlage 3

Wettelijk kader publieke partijen

Wanneer de politie biometrische gegevens verwerkt voor haar politietaak is de WPG van toepassing. In deze wet staat beschreven op welke wijze de gegevens verwerkt mogen worden. Voor de politie geldt er een specifieke wetgeving omdat zij gegevens over burgers verwerkt die niet met toestemming zijn afgegeven (Politie, 2018[17]). In deze bijlage zullen de belangrijkste begrippen van de WPG worden uitgelegd en zullen de voorwaarden, voor het verwerken van politiegegevens, en de plichten die daarbij horen worden besproken.

Artikel 2 lid 1 van de WPG bepaald de reikwijdte van de wet en daarmee wanneer de wet van toepassing is. De wettekst luidt als volgt: "Deze wet is van toepassing op de verwerking van politiegegevens door een bevoegde autoriteit die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen". Net zoals de AVG heeft de WPG een aantal belangrijke begrippen die hieronder zullen worden besproken.

Beginselen inzake verwerking persoonsgegevens

Ook de WPG heeft een aantal beginselen inzake de verwerking van politiegegevens. Deze zullen in de volgende paragrafen worden besproken.

Rechtmatig, noodzakelijk & doelbinding

Allereerst geldt dat de verwerking alleen gebeurt voor zover dit noodzakelijk is voor het behalen van de doelen welke bij of krachtens de wet worden geformuleerd. Daarnaast vindt verwerking alleen plaats voor zover dit behoorlijk en rechtmatig is en dienen de gegevens toereikend te zijn. Ook stelt artikel 3 WPG dat de gegevens mogen worden verwerkt voor meerdere doelen mits deze zijn vastgesteld voor het nastreven van de politietaak en de verwerking in verhouding staat met dit doel. Tevens kunnen de gegevens voor een ander doel dan die van de politietaak worden verwerkt. Dit mag alleen wanneer het gaat om een zwaarwegend algemeen belang of is aangewezen in de wetgeving van de Europese Unie. Bij artikel 3 WPG is de proportionaliteitseis van belang. Het belang tussen het voorkomen en opsporen van een strafbaar feit of verdachte moet afgewogen worden tegen de inbreuk op de persoonlijke levenssfeer die gemaakt wordt ten opzichte van onschuldige burgers (Politie, 2015). Hierbij is het van belang wat het dreigingsniveau van nieuwe delicten is, het risico op incidenten speelt een belangrijke rol bij de afweging tussen het inzetten van een invasief middel, zoals geautomatiseerde gelaatsherkenning, en de privacy van burgers (Bouma, van Rest, Burghouts, Schutte & Baan, 2014).

Juistheid & volledigheid

Artikel 4 WPG stelt dat de gegevens juist en nauwkeurig dienen te zijn. De verwerkingsverantwoordelijke moet hiervoor de nodige maatregelen treffen. Wanneer de gegevens onjuist zijn moeten deze worden

[17] Bron afkomstig van de Politie – Gegevensautoriteit (niet publiek toegankelijk).

vernietigd worden aangepast. Daarnaast dienen de gegevens ook vernietigd te worden wanneer deze niet meer noodzakelijk zijn voor het doel waarvoor zij verwerkt worden.

Bijzondere categorieën persoonsgegevens

Bijzondere categorieën van politiegegevens, zoals biometrische gegevens, worden alleen verwerkt indien die onvermijdelijk is voor het doel van de verwerking (art. 5 WPG).

Plichten van de verwerkingsverantwoordelijke

Ook de WPG stelt een aantal plichten voor de verwerkingsverantwoordelijke. Deze worden hieronder besproken.

Gegevensbescherming door beveiliging en ontwerp

Naast juist dienen de gegevens goed beschermd te worden. Hierbij moet de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treffen om te kunnen aantonen dat de gegevens alleen worden verwerkt in overeenstemming met het doel dat krachtens of bij de wet is bepaald. Daarnaast moeten de gegevens doeltreffend worden verwerkt en moeten de rechten van betrokkenen in acht worden genomen. Technische maatregelen moeten genomen worden om het beveiligingsniveau van de gegevens te waarborgen, dit moet in verhouding staan tot het risico (art. 4a WPG).

Gegevensbescherming door standaardinstellingen

Artikel 4b WPG stelt dat de verwerkingsverantwoordelijke ervoor dient te zorgen dat er passende technische en organisatorische maatregelen worden genomen dat standaard alleen de politiegegevens worden verwerkt die noodzakelijk zijn voor een specifiek doel. De maatregelen betreffen hier de hoeveelheid van gegevens die verwerkt worden, de manier waarop zij verwerkt worden, de toegankelijkheid van de gegevens en de periode van opslag van de gegevens. De gegevens dienen daarnaast niet zonder tussenkomt van een natuurlijk persoon toegankelijk te worden gemaakt.

Gegevensbeschermingseffectbeoordeling

Wanneer de verweking een hoog risico voor de rechten en vrijheden van personen oplevert dient de verwerkingsverantwoordelijke vooraf aan de verwerking een beoordeling uit te voeren. Deze kijkt naar het effect van de verwerkingsactiviteiten en naar de bescherming van persoonsgegevens (Art. 4c WPG). De politie heeft een checklist opgesteld aan de hand waarvan kan worden bepaald of een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd. Dit moet worden gedaan indien er sprake is van een of meer van de criteria die in tabel 14 worden weergegeven.

Tabel 14

Criteria gegevenseffectbeoordeling

Criteria	Toelichting
Het beoordelen van mensen op basis van persoonskenmerken	Het maken van voorspellingen op basis van kenmerken zoals gedrag of persoonlijke voorkeuren.
Geautomatiseerde beslissingen	Gevolgen die zo wezenlijk zijn dat er sprake is van discriminatie.
Stelselmatige en grootschalige monitoring	Als er grootschalig gemonitord wordt in de openbare ruimte. Hierbij is het voor burgers onmogelijk om zich aan de verwerking te onttrekken.
Het verwerken van gevoelige gegevens, inclusief zeer persoonlijke gegevens	Hierbij gaat het om het verwerken van gevoelige gegevens.
Grootschalige gegevensverwerking	Wanneer gegevens grootschalig worden verwerkt. Er zijn een aantal criteria om dit te bepalen: - Hoeveelheid personen van wie gegevens worden verwerkt - Hoeveelheid en/of verscheidenheid aan gegevens die worden verwerkt - De tijdsduur van de gegevensverwerking - De geografische reikwijdte
Koppelen en combineren van politiegegevens	Gegevensverzameling die aan elkaar gekoppeld of met elkaar gecombineerd zijn
Het verwerken van gegevens over kwetsbare personen	Bijvoorbeeld gegevens van minderjarigen of verwarde personen.
Het gebruik maken van nieuwe technologieën	Wanneer nieuwe technologieën gebruikt worden, dit kan privacyrisico's met zich meebrengen.
Verwerkingen die leiden tot de blokkering van een recht, dienst of contract	Gegevensverwerkingen die ertoe leiden dat een recht niet meer uitgeoefend kan worden.

Autorisatie

Art. 6 WPG bepaald dat de verwerkingsverantwoordelijke verantwoordelijk is voor het bijhouden van de autorisaties. Hij of zij moet zorg dragen dat alleen de ambtenaren toegang hebben tot de politiegegevens die belast zijn met de uitvoering van de politietaak.

Registerplicht

Net zoals in de AVG stelt de WPG dat de verwerkingsverantwoordelijke een registerplicht heeft. De verwerkingsverantwoordelijke dient een register bij te houden met bepaalde gegevens die de wet noemt. Deze plicht geldt tevens voor de verwerker (art. 31d WPG).

Documentatie

De verwerkingsverantwoordelijke draagt zorg voor de schriftelijke vastlegging. Hierbij dienen de doelen van het onderzoek of de verwerking duidelijk te zijn vastgelegd en dient bepaald te zijn wie de verwerking uitvoert en wat er met de gegevens wordt gedaan. Daarnaast dient de verwerkingsverantwoordelijke een logging bij te houden waarin duidelijk is hoe de verwerking plaatsvindt en wat er met de data gebeurt. (art. 32 WPG; art. 32a WPG).

Melden van datalek

Artikel 33a WPG bepaald dat indien er sprake is van een datalek dit binnen 72 uur gemeld moet worden bij de Autoriteit Persoonsgegevens. Deze melding dient te voldoen aan een aantal eisen welke genoemd worden in artikel 33a lid 2 WPG.

Voorafgaande raadpleging

Net zoals de verwerkingsverantwoordelijke in een privaat scenario dient de verwerkingsverantwoordelijke en voorafgaande raadpleging van de Autoriteit Persoonsgegevens te laten uitvoeren.

Privacyfunctionaris

Artikel 34 WPG bepaalt dat de verwerkingsverantwoordelijke een of meer privacyfunctionarissen moet benoemen. Deze dient advies te geven met betrekking tot de verwerking van de politiegegevens.

Functionaris voor gegevensbescherming

Tevens dient er een functionaris voor gegevensbescherming te worden aangewezen. Deze persoon wordt aangewezen naar aanleiding van zijn of haar professionele kennis en is belast met een aantal taken welke de WPG noemt (art. 36 WPG).

Naast de plichten van de verwerkingsverantwoordelijke heeft de verwerker ook een aantal plichten. Zo moet ook de verwerker passende technische en organisatorische maatregelen treffen om aan te kunnen tonen dat gegevens louter worden verwerkt in overeenstemming met het doel. Daarnaast dient er een schriftelijke overeenkomst te zijn tussen de verwerkingsverantwoordelijke en de verwerker. Ook dient de verwerker een register bij te houden dat gegevens bevat die benoemd worden in artikel 31d WPG. Ook helpt de verwerker bij het bijhouden van de loggings waardoor duidelijk is hoe de verwerking plaatsvindt.

Verwerkingsgrondslagen

De WPG geeft een aantal verwerkingsgrondslagen met betrekking tot het verwerken van politiegegevens. Het doel waarvoor de politie de gegevens bewerkt, bepaalt op welke wijze deze gegevens mogen worden gebruikt en onder welke voorwaarden dit mag (Politie, 2018). De verwerkingsgrondslagen zijn terug te vinden in artikel 8, 9, 10, 12 en 13 van de WPG en zullen hieronder worden besproken.

Art. 8 WPG Uitvoering van de dagelijkse politietaak

Artikel 8 WPG stelt dat politiegegevens, uit de basisvoorziening handhaving [BVH], verwerkt mogen worden met het oog op de uitvoering van de dagelijkse politietaak. De BVH is een database dat informatie bevat over bekeuringen, processen-verbaal, observaties en andere handelingen van agenten (Zembla, 2012). De politietaak bestaat onder andere uit de handhaving van wetten, hulpverlening, surveillance, opsporingsonderzoeken en verkeerszaken. In dit geval mag de politie in het eerste jaar alles met de gegevens doen, de gegevens mogen zowel van verdachte als onverdachte personen zijn. Wanneer het eerste jaar voorbij is mogen de gegevens alleen nog worden verwerkt door gericht te zoeken, bijvoorbeeld op adres of kenteken. Ook dit is niet meer toegestaan nadat er 5 jaar is verstreken, dan worden de gegevens verwijderd en kunnen ze alleen nog worden geraadpleegd via een poortwachter[18]. Na 10 jaar worden de gegevens vernietigd en kunnen ze niet meer gebruikt worden (Politie, 2018).

Art. 9 WPG Onderzoek in verband met handhaving van de rechtsorde in een bepaald geval

Artikel 9 lid 1 WPG luidt als volgt: "Politiegegevens kunnen gericht worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval". Met dit soort verwerking worden er grote hoeveelheden gegevens verzameld die gericht zijn op bepaalde personen of op specifieke gebeurtenissen. Bij een artikel 9 verwerking kan er gedacht worden aan tappen of stelselmatige observatie. Een voorbeeld van een gericht onderzoek is bijvoorbeeld onderzoek naar overlast in een bepaalde wijk, het aanpakken van veelplegers of een verstoring van de openbare orde (Politie, 2018). Bij deze verwerking is het belangrijk dat het doel van het onderzoek binnen een week, na de start van de verwerking, duidelijk omschreven is en schriftelijk wordt vastgelegd (art. 9 lid 2 WPG). Daarnaast stelt artikel 9 lid 4 dat de gegevens alleen verwerkt mogen worden indien dit noodzakelijk is voor het doel van het onderzoek. Wanneer de gegevens niet meer noodzakelijk zijn worden ze verwijderd of voor nog maximaal een half jaar bewaard om te zien of er nog aanleiding is voor het instellen van een nieuw onderzoek.

Art. 10 WPG Inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde

Artikel 10 WPG stelt dat politiegegevens gericht verwerkt mogen worden om inzicht te krijgen in de betrokkenheid van personen in een bepaald aantal gevallen. De gevallen waar het hierom gaat worden opgesomd in art. 10 lid 1. Het gaat hierbij om het beramen of plegen van misdrijven, handelingen die hierop kunnen wijzen of handelingen die gezien hun aard, frequentie of georganiseerd verband een ernstige schending van de openbare orde vormen. Lid 2 tot en met 4 bepalen van welke personen de persoonsgegevens gebruikt mogen worden.

Artikel 11 WPG stelt dat zover het noodzakelijk is voor een onderzoek, zoals bedoeld in artikel 9 en 10 WPG, het mogelijk is om politiegegevens geautomatiseerd te verwerken. Gegevens kunnen geautomatiseerd worden vergeleken met andere politiegegevens.

---

[18] Een poortwachter is iemand die een speciale opleiding heeft genoten en wie toegang heeft tot verwijderde gegevens voor de in de wet genoemde doeleinden (Politie, 2016).

Art. 12 WPG Informanten

Volgens artikel 12 WPG mogen politiegegevens verwerkt worden met het oog op de controle en het beheer van een informant. De verwerking die hier plaatsvindt betreft informatie over de informant, personen waarover informanten informatie geven en/of ambtenaren van de politie of buitengewoon opsporingsambtenaren. De gegevens mogen gedurende een periode van vier maanden na de datum van de eerste verwerking ter beschikking worden gesteld voor verdere verwerking op grond van de artikelen 8, 9 of 10 WPG.

Art. 13 Ondersteunende taken

Dit artikel maakt het mogelijk om informatie dat is verwerkt op grond van artikel 8, 9 of 10 WPG verder te verwerken ter ondersteuning van de politietaak. Dit kan bijvoorbeeld om personen te signaleren of ten behoeve van identificatie of verificatie van personen. Artikel 13 gegevens worden vaak landelijk raadpleegbaar. De gegevens die raadpleegbaar zijn worden opgesplitst in twee categorieën. Namelijk een categorie die de hele politie mag raadplegen en een categorie die alleen geraadpleegd mag worden door bepaalde functionarissen (Politie, 2018). Een voorbeeld van een registratie van artikel 13 gegevens zijn de Herkenningsdienstsystemen [HKS]. Het HKS bevat gegevens over aangiftes van misdrijven en persoonsgegevens van de verdachten daarvan. Hierin staan personen tegen wie een proces-verbaal als verdachte is opgemaakt (CBS, z.j.).

Overige belangrijke aspecten

Een ander belangrijk punt is of er politiegegevens zijn die gebruikt kunnen worden bij het inzetten van geautomatiseerde gelaatsherkenning. Zo worden foto's van verdachten en veroordeelden opgenomen in de Strafrechtsketendatabank. Deze databank kan geraadpleegd worden bij het inzetten van geautomatiseerde gelaatsherkenning. Artikel 55c lid 4 van het Wetboek van Strafvordering [Sv] biedt de mogelijkheid om "foto's die zijn genomen in het kader van de identiteitsvaststelling ook te verwerken voor het voorkomen, opsporen en vervolgen van strafbare feiten" (Politie, 2015).