FACULTEIT
RECHT EN CRIMINOLOGIE

Smart CCTV en wetshandhaving: een ethisch verantwoorde tool voor politioneel gebruik?

Masterproef neergelegd tot het behalen van
de graad van Master in de Criminologische Wetenschappen
door (01708047) Melis Jayson

Academiejaar 2022-2023

Promotor :
Prof. Dr. Pauwels Lieven

Commissaris :
De Buck Ann

Aantal woorden: 15 940

UNIVERSITEIT
GENT

Abstract

While law enforcement agencies are showing a growing interest in smart CCTV technologies, the development of these intrusive surveillance instruments has led to complex ethical choices in terms of balancing the safety benefits for society in relation to the potential interference with fundamental rights of citizens. The current qualitative research project provides a critical reflection on the use of smart CCTV for law enforcement purposes, focussing particularly on perceived ethical issues and concerns. In addition, a distinction is made between the following key features of smart CCTV: automatic number plate recognition, abnormal behaviour recognition and live facial recognition. In order to gain insight into what is at stake when these advanced technologies are being implemented in our society, seven key informants from various professional backgrounds were interviewed by means of (online) semi-structured interviews. It will be argued that the perceived ethical issues go beyond privacy, while broader social consequences must be taken into account. One of those is the fact that the technology may not be free of bias which could lead to further discrimination of individuals with specific characteristics that are part of their identity. Nevertheless, it will be stated that the ethical problems and concerns cannot be separated from the social context in which they occur. Finally, the aim of the concluding section is to discuss whether the perceived issues outweigh the intended security value of smart CCTV applications, while also ending with a few recommendations.

Key words: smart CCTV, law enforcement, ethical concerns

Woord vooraf

Deze masterproef beoogt het sluitstuk van de opleiding Master of Science in de criminologische wetenschappen aan de Universiteit Gent te zijn. Hoewel het niet te ontkennen valt dat het afleveren van een kwaliteitsvol werk een uitdagende opdracht is, vormde het schrijven van deze masterproef zeker en vast een leerrijk proces. Alvorens het huidige onderzoek uiteengezet wordt, maak ik graag van deze gelegenheid gebruik om enkele personen in de bloemetjes te zetten. Zonder hun onvoorwaardelijke steun en betrokkenheid was het tenslotte niet mogelijk om dit eindresultaat in zijn huidige vorm tot stand te brengen.

Eerst en vooral wens ik mijn promotor, Prof. Dr. Lieven Pauwels, hartelijk te bedanken voor de nodige begeleiding, feedback en gouden raad. Een masterproef schrijven neemt toch wel enige tijd in beslag. Doorheen dit proces was u steeds bereid om vragen te beantwoorden en het onderzoek in goede banen te leiden.

Vervolgens wil ik mijn oprechte dank betuigen aan alle respondenten voor hun bereidwilligheid en tijd om aan dit onderzoek deel te nemen. Jullie kennis, professionele ervaring en antwoorden leverden de nodige inzichten op om het vooropgesteld doel van dit empirisch onderzoek te bereiken.

Tot slot is een woord van dank gericht aan mijn familie, vrienden en medestudenten op zijn plaats. Bij jullie kon ik steeds rekenen op mentale steun en terecht voor een luisterend oor. Bovendien kreeg ik dankzij mijn ouders de kans om een interessante opleiding te volgen en te vervolledigen. Zij namen ook de nodige tijd vrij om deze masterproef na te lezen.

Allen van harte bedankt.

Jayson Melis

Oudenaarde, mei 2023

Inhoudstafel

Lijst met afkortingen

AI	Artificiële Intelligentie
ANPR	Automatic Number Plate Recognition
CCTV	Closed-circuit television
COC	Controleorgaan op de Politionele Informatie
DPO	Data Protection Officer
EVRM	Europees Verdrag voor de Rechten van de Mens
IoT	Internet of Things
LFR	Live Facial Recognition
LMP	London Metropolitan Police
ML	Machine Learning
PbD	Privacy by Design
RDM	Research Data Management
WPA	Wet op het Politieambt

Lijst met figuren en tabellen

1. Inleiding

De moderne technologie grijpt steeds dieper in op onze dagelijkse levensstijl en heeft de manier waarop onze samenleving functioneert ingrijpend veranderd (Wolff, 2021). In de afgelopen paar decennia kregen alsmaar meer alledaagse voorwerpen de gelegenheid om met elkaar en het internet te verbinden. Dit netwerk van 'slimme' technologieën staat in de literatuur ook wel bekend als het Internet der Dingen (Internet of Things, IoT), en zal naar de toekomst toe alleen nog maar verder uitbreiden (van Berkel et al., 2017). Het tijdperk waarin enkel persoonlijke computers en laptops met het internet verbonden zijn, ligt tenslotte al ver achter ons (Gai et al., 2018).

Deze groei in diverse IoT-toepassingen valt niet enkel ten aanzien van de samenleving als geheel op te merken. Ook wetshandhavingsinstanties trachten voortdurend op zoek te gaan naar innovatieve technologieën om zowel de openbare veiligheid te garanderen als het opsporen en vervolgen van delinquenten op een efficiënte manier te bevorderen (Almeida et al., 2021). Zodoende is cameratoezicht in de loop der jaren niet alleen gegroeid tot één van de meest ingezette beeldtechnologieën door politiekorpsen, maar heeft het ook op technologisch vlak opmerkelijke stappen gezet (Custers & Vergouw, 2015; Held et al., 2012).

Een niet te negeren probleem ten aanzien van traditionele camerabewaking ligt in het feit dat er doorgaans meerdere beelden tegelijk gemonitord dienen te worden, terwijl CCTV operators slechts een beperkte aandachtspanne hebben. Hierdoor is het vrijwel onvermijdelijk dat cruciale informatie over het hoofd gezien wordt (Ferenbok & Clement, 2011). Daarenboven impliceert het belang van een continue monitoring een hoge personeelskost en tijdsinvestering (Hidayat et al., 2020).

Om aan deze beperkingen tegemoet te komen, hebben vorderingen op het vlak van artificiële intelligentie (AI) en *machine learning* (ML) geresulteerd in de komst van smart CCTV. Zo zijn slimme camera's in staat om real-time beelden automatisch te analyseren en te interpreteren op basis van patroonherkenning. Wanneer zich abnormale gebeurtenissen voordoen, kunnen operators eenvoudigweg door het systeem op de hoogte gesteld worden. Bijgevolg hoeven camerabeelden niet meer te allen tijde actief gemonitord te worden, waardoor politieambtenaren meer tijd in andere functionaliteiten kunnen investeren, zoals *community engagement* (Möllers & Hälterlein, 2012; Rahman, 2017).

Bovendien heeft de combinatie van beveiligingscamera's met AI geresulteerd in toepassings-mogelijkheden die zo goed als eindeloos zijn. Denk maar aan het louter detecteren van rook in

een welbepaalde ruimte tot één van de meest controversiële wetshandhavingstools van de eenentwintigste eeuw, met name automatische gezichtsherkenning in de publieke ruimte (Purshouse & Campbell, 2021).

1.1. Probleemstelling en onderzoeksvragen

Hoewel technologische ontwikkelingen op het vlak van camerabewaking een veelbelovende impact op de wetshandhaving kunnen betekenen, heeft de opkomst van dit toezichtinstrument op openbare plaatsen geleid tot een complex maatschappelijk debat, waarbij de vraag of de veiligheidswaarde van CCTV al dan niet het gepercipieerd privacyverlies kan rechtvaardigen op de voorgrond treedt. Over het algemeen suggereren voorstanders dat deze situationele preventiemaatregel effectief in staat is om criminele feiten op te helderen en terug te dringen, alsook veiligheidsgevoelens onder burgers te bevorderen. Tegenstanders daarentegen beweren dat de veiligheidswaarde van CCTV overschat wordt, en dat de impact van de toegenomen supervisie op de privacy opweegt tegen de vooropgestelde voordelen (Brey, 2004).

Daarenboven dient in geval van smart CCTV in het achterhoofd gehouden te worden dat het automatisch analyseren van camerabeelden aan de hand van Artificial Intelligence software bijkomende uitdagingen, bedreigingen en ethische problemen met zich meebrengt. Enerzijds vallen inbreuken op persoonsgegevens vanwege het risico op cyberaanvallen niet uit te sluiten (Costin, 2016; Khan et al., 2020). Anderzijds stellen tegenstanders evenzeer de accuraatheid van deze intrusieve technologie in vraag, en wijzen op de reële kans dat onschuldige burgers ten onrechte als criminelen geïdentificeerd kunnen worden (Brey, 2004; Lee et al., 2019).

Zo was er het verhaal van Robert Williams die in het bijzijn van zijn vrouw en dochters onrechtmatig voor winkeldiefstal gearresteerd werd. In het bijzonder had een winkeleigenaar wazige bewakingsbeelden van de verdachte ter beschikking gesteld, waarna deze beelden aan de hand van gezichtsherkenningssoftware gelinkt werden aan een rijbewijsfoto van Williams. Alvorens de politie van Detroit echter achterhaalde dat de gezichtsherkenningstechnologie Williams onterecht als verdachte geïdentificeerd had, was de 43-jarige man reeds dertig uur van zijn vrijheid beroofd (Perego, 2021).

Hoewel het merendeel van de bevolking zich er niet bewust van lijkt te zijn, wordt gezichtsherkenningstechnologie op verschillende plaatsen in de wereld reeds gehanteerd (Brey et al., 2004). Wat het gebruik daarvan in de Belgische context betreft, stuiten wetshandhavers vandaag de dag nog steeds op wettelijke beperkingen.

Zo ontbreekt er in de wet op het Politieambt (WPA) een afdoende wettelijke basis om gezichtsherkenning voor opdrachten van bestuurlijke of gerechtelijke politie te kunnen aanwenden (Controleorgaan op de Politionele Informatie, 2022a). Opdat een met gezichtsherkenning uitgeruste bewakingscamera effectief als wethandhavingstool kan functioneren, is het vanzelfsprekend dat een technische databank met biometrische gegevens aangelegd dient te worden (Rooseleers & Maesschalck, 2021). Echter heeft de wetgever bepaald dat camerabewaking wel degelijk met intelligente technologieën, zoals gezichtsherkenning, uitgerust kan worden, terwijl het opzetten van een technische gegevensbank enkel in het kader van automatische kentekenplaatherkenning (ANPR) wettelijk toegestaan is.[1]

Bovenstaande neemt echter niet weg dat de federale politie in 2019 trachtte te experimenteren met gezichtsherkenningssoftware op de luchthaven van Zaventem, waarbij biometrische gegevens van elke voorbijganger verzameld en opgeslagen werden. Vanwege het gebrek aan een wettelijke basis werd dit proefproject door het Controleorgaan op de Politionele Informatie (COC) dan ook stilgelegd, vermits fundamentele rechten in het gedrang kwamen (Controleorgaan op de Politionele Informatie, 2019). Tevens kwam uit een recenter rapport van het COC wederom aan het licht dat leden van de federale gerechtelijke politie meerdere malen een Amerikaanse gezichtsherkenningsapplicatie, genaamd *Clearview AI*, hanteerden in het kader van een lopend strafonderzoek naar kinderporno (Controleorgaan op de Politionele Informatie, 2022b; Cup, 2022).

Overigens dient opgemerkt te worden dat het politioneel gebruik van welbepaalde geavanceerde beeldtechnologieën inmiddels het voorwerp van wetsvoorstellen uitmaken. Zo ligt er reeds een voorstel op tafel om een wettelijk kader te voorzien voor ANPR-camera's met gezichtsherkenning ter detectie van elektronische apparaten achter het stuur.[2]

Het inzetten van gezichtsherkenningstechnologie als wetshandhavingstool is dus niet enkel en alleen maar een zorg voor de toekomst, maar dient vandaag de dag evenzeer onderwerp uit te maken van het actueel debat rond cameratoezicht. Bijgevolg is het dan ook opportuun om kritisch te reflecteren over de mate waarin en de bijzondere omstandigheden waaronder de geïntegreerde politie dergelijke camera's bij het uitoefenen van hun kerntaken mag hanteren, vermits fundamentele rechten en vrijheden van de mens in het gedrang komen.

[1] Art. 44/2, §3 WPA.
[2] Wetsvoorstel wat het actualiseren van de regelgeving inzake het verbod op elektronische communicatietoestellen in het verkeer betreft, *Parl. St.* Kamer 2021-22, nr. 1688/1.

Het huidige onderzoek beoogt een bijdrage te leveren aan het sociaalwetenschappelijk debat door vanuit een ethisch perspectief dieper in te gaan op gepercipieerde bezorgdheden en bedenkingen inzake het gebruik van slimme camera's voor wetshandhavingsdoeleinden. Deze doelstelling zal worden nagestreefd door semi-gestructureerde interviews met een aantal Belgische en Nederlandse professionele sleutelfiguren af te nemen, aangevuld met reeds bestaande kennis uit de wetenschappelijke literatuur.

Uitgaande van bovenstaande probleemstelling zal dit onderzoek zich primair focussen op het beantwoorden van de volgende centrale onderzoeksvraag, en de daarbij horende deelvragen:

1) In welke mate wegen de door professionele sleutelfiguren gepercipieerde ethische problemen rond slimme camera's al dan niet op tegen de beoogde veiligheidswaarde die deze AI gebaseerde technologie voor politioneel gebruik voorziet?
    a. Welke (privacy-)bezorgdheden en bedenkingen kaarten professionele sleutelfiguren jegens het politioneel gebruik van slimme camera's aan?
    b. In hoeverre worden specifieke toepassingen van slimme camera's door professionele sleutelfiguren gepercipieerd als al dan niet wenselijk en ethisch verantwoord voor politioneel gebruik?

Vermits de mogelijke toepassingen van slimme camera's zo goed als eindeloos zijn, is een concrete afbakening als dusdanig aan de orde. Zodoende stelt het huidige onderzoek volgende selectie van te bespreken toepassingen voorop:

- **Automatische kentekenplaatherkenning**: ANPR-camera's (automatic number plate recognition) beogen passerende kentekens van voertuigen te herkennen en vast te leggen. De gefotografeerde kentekens worden dan automatisch vergeleken met zogenaamde referentielijsten. Een dergelijke referentielijst of watchlist bevat gegevens van voertuigen en/of bestuurders die reeds bij de politie bekend zijn. Zo creëert het systeem de mogelijkheid om door de politie geseinde voertuigen (en inzittenden) te signaleren en te onderscheppen (Homburg et al., 2016). Het gebruik van ANPR-camera's door de Belgische politie is alvast onderworpen aan een duidelijk wettelijk kader en wordt inmiddels breed ingezet.[3]
- **Automatische gedragsherkenning**: Ten aanzien van slimme camerasystemen kunnen evenzeer algoritmen ontwikkeld worden die op basis van gedragsanalyse welbepaalde gedragingen van voorbijgangers trachten te herkennen, interpreteren en zelfs te voorspellen (Flight, 2016).

[3] Art. 44/11/3decies WPA.

- **Live gezichtsherkenning**: Bij gezichtsherkenningstechnologie wordt AI software aangewend om gezichten uit beeldmateriaal te detecteren en op basis van biometrische kenmerken te 'matchen' met eerder bewaarde afbeeldingen van individuen (Purshouse & Campbell, 2021). Hoewel het louter vergelijken van gezichtsafbeeldingen ter verificatie van de identiteit van een verdachte eveneens tot de bredere categorie van gezichtsherkenning behoort, focust het huidige onderzoek uitsluitend op automatische identificatie van individuen op openbare plaatsen. Daarbij wordt het door de camera waargenomen gezicht van elke voorbijganger gescand en vergeleken met digitale beelden van individuen die zich op een watchlist bevinden teneinde geseinde personen in real-time te identificeren (Purshouse & Campbell, 2021). Dermate beoogt de technologie niet alleen gekende criminelen of verdachten te monitoren en/of te arresteren, maar ook vermiste personen te lokaliseren (Brey, 2004). Deze subcategorie van gezichtsherkenning wordt in het Engels ook wel aangeduid met de term ***live facial recognition*** **(LFR)**. Zoals eerder aangehaald, ontbreekt er in België een afdoende wettelijke basis om geautomatiseerde gezichtsherkenningstechnologie voor opdrachten van bestuurlijke of gerechtelijke politie in te zetten.

Om een antwoord te formuleren op de vooropgestelde onderzoeksvragen vond zowel een grondige literatuurstudie als een empirisch kwalitatief onderzoek plaats. Het empirische luik bestond uit semi-gestructureerde interviews met professionele sleutelfiguren teneinde de thematiek vanuit een ethisch perspectief onder de loep te nemen en verscheidene standpunten in kaart te brengen. Hierbij stond niet het generaliseren van de bevindingen centraal, maar wel het in de diepte bespreken van de exacte problematiek en de mate waarin toepassingen van slimme camera's al dan niet wenselijk en verantwoord zijn voor politioneel gebruik.

Vermits een beperkt aantal professionele sleutelfiguren aan de studie participeerden, zit een beperking van het huidige onderzoek dan ook in de lage generaliseerbaarheid. Voorts dient evenzeer benadrukt te worden dat het om een perceptieonderzoek gaat. Er vindt geen effectiviteitsmeting van de vooropgestelde cameratoepassingen plaats. Bij het interpreteren van de resultaten dienen bovenstaande zaken in het achterhoofd gehouden te worden.

In wat volgt, worden bevindingen uit voorgaand onderzoek met betrekking tot het onderwerp toegelicht. Daaropvolgend vindt een uiteenzetting van de gehanteerde methodologie plaats, waarbij de rekrutering van respondenten, de ethische aspecten, de dataverwerking en data-analyse enige aandacht vereisen. Na het methodologisch luik spitsen we ons toe op de resultaten van het empirisch onderzoek die simultaan in verband gebracht worden met reeds bestaande

onderzoeksbevindingen. Tot slot beoogt men in het conclusie en discussie gedeelte een antwoord op de vooropgestelde onderzoeksvragen te formuleren en met enkele aanbevelingen af te ronden.

2. Bevindingen uit voorgaand onderzoek

Vermits ethische bezorgdheden inzake smart CCTV voortbouwen op de reeds bestaande problematiek rond traditionele camerabewaking, is het als onderzoeker van belang om een eerste inzicht te verwerven in de effectiviteit van reguliere camera's. De al dan niet gewenste impact die traditioneel cameratoezicht teweegbrengt, ligt tenslotte aan de basis van het maatschappelijk debat.

Om vertrouwd te geraken met het onderwerp vond een narratieve literatuurstudie plaats. Hierbij werd in de eerste plaats getoetst naar de effectiviteit van CCTV in de aanpak van criminaliteits- en overlastfenomenen. Echter worden de resultaten daarvan slechts beknopt besproken wegens het huidige onderzoek primair gericht is op intelligente camerabewaking. Dit neemt immers niet weg dat deze bevindingen van belang zijn bij de uiteindelijke afweging van de veiligheidswaarde en ethische bezorgdheden. In een daaropvolgende stap droeg de literatuurstudie evenzeer bij aan het verwerven van kennis omtrent ethische problemen rond smart CCTV. Daarbij lag de focus in hoofde op het gebruik ervan voor opdrachten van bestuurlijke of gerechtelijke politie.

2.1. CCTV: een oud fenomeen maar actueel debat

Hoewel CCTV doorheen de jaren reeds het voorwerp van talrijke studies uitmaakte, heerst er tot op vandaag nog steeds onenigheid over de vraag of het schenden van andermans privacy wel degelijk proportioneel is met de veiligheidswaarde die cameratoezicht biedt. In het discours staan de noties van privacy en veiligheid dan ook sterk gecentreerd (Brey, 2004). Doorgaans argumenteren voorstanders dat de implementatie van het toezichtinstrument een positieve bijdrage levert aan de reductie van criminele feiten en slechts een minimaal verlies aan privacy impliceert, waardoor eventuele privacyinbreuken in ieder geval gerechtvaardigd zijn. Een theoretische verklaring voor het beoogde preventieve effect kan gevonden worden in de '*rational choice theory*'. Deze theorie gaat ervan uit dat een potentiële dader zich omwille van de toegenomen supervisie mogelijks weerhoudt om feiten te plegen, mits geconcludeerd wordt dat de baten niet meer opwegen tegenover het risico op arrestatie (Melis, 2021).

Desalniettemin trekken tegenstanders niet enkel de conclusie dat fundamentele rechten en vrijheden in het gedrang komen, maar stellen tevens de effectiviteit van de technologie in vraag, vermits onderzoeksresultaten niet definitief zijn (Melis, 2021). Terwijl anderen het afschrikwekkend effect van camera's niet betwisten, uiten zij een zorg dat CCTV de

criminaliteit louter naar andere locaties verplaatst in plaats van deze effectief een halt toe te roepen (Melis, 2021).

Met dit discours in het achterhoofd wordt in het volgend luik beknopt stilgestaan bij de bevindingen van enkele relevante effectiviteitsstudies.

2.2. Effectiviteit reguliere CCTV

2.2.1. Objectieve veiligheid

Wegens camerabewaking wereldwijd in toenemende mate geïmplementeerd wordt, is het geen uitzondering dat de vraag naar de effectiviteit ervan dikwijls gesteld wordt. Ondanks het feit dat de effecten van CCTV verregaander zijn, heeft empirisch onderzoek zich in hoofde gericht op het criminaliteitsreducerend effect in de publieke ruimte. Een verbeterde objectieve veiligheid was dan ook het initiële doel die beleidsmakers voor ogen hadden (Melis, 2021).

Hoewel er effectiviteitsstudies zijn die een bescheiden maar significant preventief effect aantonen, kan men niet met de hand op het hart zeggen dat camera's criminaliteit voorkomen. Het preventieve effect zal in eerste instantie sterk afhangen van het type misdrijf dat men beoogt te reduceren. Zo zijn significante effecten vooral te wijten aan het terugdringen van voertuig-, vermogens- en drugscriminaliteit in parkeergarages en woonwijken. In geval van gewelds-delicten lijkt CCTV beduidend minder effectief te zijn (Caplan et al., 2011; Gerell, 2016; Piza et al., 2019).

Een potentiële verklaring hiervoor kan in het afschrikwekkend effect van CCTV gezocht worden. Doorgaans wordt er bij geweldsdelicten zonder voorbedachte rade gehandeld, waardoor daders zich er niet bewust van zijn dat hun handelingen door de camera geregistreerd worden. Vermogensdelinquenten daarentegen zijn eerder geneigd om vóór de daad een afweging tussen de baten en het risico op arrestatie te maken (De Pauw et al., 2013).

Desalniettemin dient over het algemeen geconcludeerd te worden dat onderzoeksbevindingen nopens effecten van CCTV weinig consistent zijn. Naast het type misdrijf zullen de vastgestelde effecten te allen tijde variëren naargelang de lokale context waarin de camera geïmplementeerd wordt, de aanwezigheid van andere preventiemaatregelen, alsook het al dan niet actief monitoren (Melis, 2021).

Zoals eerder aangehaald, kan camerabewaking leiden tot een toename van criminaliteit in de aangrenzende gebieden die niet van een dergelijk toezichtinstrument voorzien zijn. Het tegenovergestelde van het verplaatsingseffect valt immers ook niet uit te sluiten, wat in de

literatuur bekend staat als een diffusie van voordelen. Dit fenomeen impliceert dat het aantal gepleegde feiten niet uitsluitend daalt in de regio onder toezicht, maar ook in het aangrenzend gebied (Melis, 2021). Echter lijken beide fenomenen zich niet frequent voor te doen en leveren studies inzake neveneffecten tegenstrijdige resultaten op (Caplan et al., 2011; Cerezo, 2013; Dekker 2015; Waples et al., 2009). Daarenboven kan men dergelijke effecten niet met zekerheid toeschrijven aan de implementatie van CCTV, vermits deze beeldtechnologie frequent ingezet wordt naast tal van andere interventiestrategieën, waaronder verbeterde straatverlichting, politiepatrouilles, bewegwijzering, enzovoort (Melis, 2021).

2.2.2. Subjectieve veiligheid

In het bijzonder dient evenzeer belang gehecht te worden aan de mate waarin bewakings-camera's een invloed op de subjectieve veiligheid teweegbrengen. In tegenstelling tot het effectief terugdringen van het aantal gepleegde feiten (objectieve veiligheid), ligt de klemtoon uitdrukkelijk op de (on)veiligheidsbeleving van burgers (Melis, 2021).

Enkele studies hebben reeds aangetoond dat het merendeel van de respondenten zich als gevolg van de camera-implementatie veiliger is gaan voelen (Cerezo, 2013; Schreijenberg & Homburg, 2010). Desondanks valt niet uit te sluiten dat de toegenomen supervisie contraproductief werkt. Indien voorbijgangers de aanwezigheid van een camera opmerken, kan dit een verontrustend gevoel opwekken aangezien het toezicht met een reële kans op slachtofferschap geassocieerd wordt. Bijgevolg wordt de kans op slachtofferschap overschat en stelt men zich extra waakzaam op. Daartegenover is een situatie van schijnveiligheid ook denkbaar. Hierbij maken potentiële slachtoffers zich in een onder toezicht geplaatste buurt mogelijks minder zorgen, terwijl de objectieve veiligheid niet zozeer verbetert. Dit kan resulteren in een gebrek aan voorzorgs-maatregelen en waakzaamheid, waardoor de opportuniteit om feiten te plegen toeneemt (Melis, 2021).

2.2.3. Bijdrage aan ophelderingsgraad

Het wijdverspreid en toenemend gebruik van CCTV kan mede verklaard worden door het gebruik van beschikbare camerabeelden in het opsporingsonderzoek. In vergelijking met het criminaliteitsreducerend effect van camerabewaking, is het merkwaardig dat slechts een beperkt aantal studies zich toegespitst hebben op de waarde van dergelijke beelden in het ophelderen van criminaliteitsfenomenen (Melis, 2021).

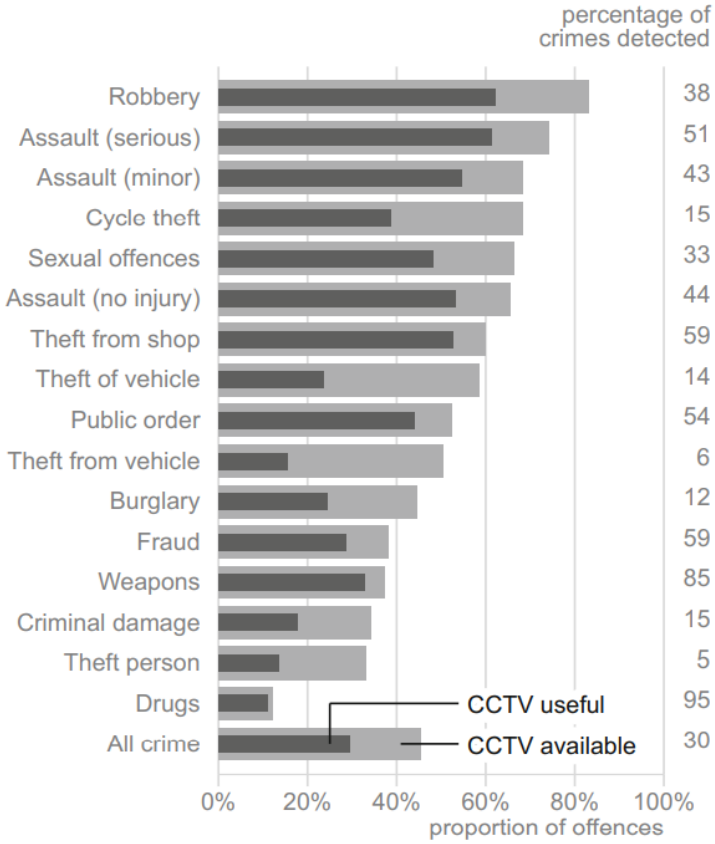
Doorgaans lijkt het immers niet evident om de effectiviteit ervan aan het licht te brengen, vermits de beelden vaak een indirecte rol spelen. Zo is het gebruik van camerabeelden als

doorslaggevend bewijsmateriaal eerder uitzondering dan regel. Nochtans kunnen ze onder meer aan het uitsluiten van een verdachte hebben bijgedragen. Daarnaast bevat het merendeel van de verrichte evaluatieonderzoeken weinig tot geen cijfermatige uitspraken over het belang ervan in het opsporingsonderzoek. Zo worden camerabeelden veelal aangewend om het onderzoek eenvoudigweg in een bepaalde richting te sturen, waardoor ze niet als bewijsmateriaal in het dossier opgenomen worden (Flight, 2016).

Desondanks hanteert het Australische evaluatieonderzoek van Morgan en Dowling (2019) politiedata van op het spoorwegnet gepleegde feiten. Ten aanzien van delicten waarbij CCTV-opnames voorhanden waren, werd een ophelderingspercentage van circa 25% geconstateerd, terwijl feiten zonder beschikbaar beeldmateriaal in 21% van de gevallen opgehelderd werden. Daarenboven blijken camerabeelden in het bijzonder waardevol wanneer de feiten gerelateerd zijn aan inbraak, diefstal of materiële schade (Morgan & Dowling, 2019).

Het feit dat dergelijke beelden een significante bijdrage leveren in het strafrechtelijk onderzoek naar inbraken en diefstallen, werd reeds eerder bevestigd in de studie van Ashby (2017). Een gedetailleerd overzicht omtrent de resultaten van dit empirisch onderzoek wordt in Figuur 1 weergegeven. In tegenstelling tot het onderzoek van Morgan en Dowling valt immers op dat cameratoezicht een adequaat hulpmiddel lijkt te zijn om daders van agressie of geweld te identificeren. Hoewel het opmerkelijk is dat beschikbaar beeldmateriaal in drugszaken relatief schaars is, blijken deze CCTV-opnames vrijwel altijd relevant in het ophelderen ervan (Ashby, 2017).

Figuur 1. Proportie misdrijven waarvoor CCTV-opnames in het onderzoek beschikbaar en nuttig waren.



Noot. Overgenomen uit "The value of CCTV surveillance cameras as an investigative tool: An empirical analysis," door M. P. J. Ashby, 2017, *European Journal on Criminal Policy and Research*, *23*(3), p. 448 (https://doi.org/10.1007/s10610-017-9341-6).

Echter dienen bovenstaande bevindingen met de nodige voorzichtigheid geïnterpreteerd te worden. Zowel in de studie van Ashby als die van Morgan en Dowling werd uitsluitend data gehanteerd met betrekking tot criminele feiten op het spoorwegnet, waardoor CCTV-opnames in een specifieke context geëvalueerd werden. Zo was de bestudeerde setting voorzien van een brede CCTV-dekking. Niettemin dient rekening gehouden te worden met het feit dat het gezichtsveld van een camera in een andere publieke ruimte tot slechts een deel van het gebied beperkt kan zijn. Bijgevolg valt het niet uit te sluiten dat camerabewaking op andere locaties in mindere mate bijdraagt aan het opsporingsonderzoek (Melis, 2021).

2.3. Van reguliere camera's naar smart CCTV

Een alom bekend probleem bij traditionele camerabewaking heeft betrekking op het actief monitoren van de beelden. Naast de alsmaar toenemende overvloed aan visuele informatie die cameratoezicht genereert, zijn humane operators ten opzichte van computers beperkt in hun concentratievermogen. Hierdoor wordt het voor een operator vrijwel onmogelijk om camera-beelden efficiënt te monitoren. Bovendien vereist het actief monitoren van camera's de nodige

politiecapaciteit die evengoed ten behoeve van andere functionaliteiten ingezet kan worden (Ferenbok & Clement, 2011; Koch et al., 2013).

Smart CCTV daarentegen biedt tal van voordelen om aan deze beperkingen tegemoet te komen. Zo wordt niet meer verwacht dat de beelden voortdurend in de gaten gehouden worden, maar brengt het systeem de operator eenvoudigweg op de hoogte van significante gebeurtennissen die eventueel tussenkomst of verdere monitoring vereisen (Ferenbok & Clement, 2011; Möllers & Hälterlein, 2012). Bovendien biedt het politiepatrouilles ondersteuning in het bepalen van de meest gepaste response en is men gedurende interventies beter voorbereid op potentiële bedreigingen (Rahman, 2017).

Door beveiligingscamera's met artificiële intelligentie te combineren, zijn de toepassings-mogelijkheden vrijwel eindeloos. In ieder geval behoren volgende zaken tot de meest voor de hand liggende karakteristieken van smart CCTV: gezichtsherkenning, detectie van afwijkend gedrag of onvoorziene objecten, kentekenplaatherkenning, het controleren van een menigte, en het volgen van personen of objecten (Rahman, 2017). Daarenboven dient de waarde ervan ten aanzien van *predictive policing* niet onderschat te worden. Zo kunnen algoritmen op basis van gedragsanalyse provocerend gedrag beogen te detecteren om te voorspellen of een bepaalde situatie al dan niet uit de hand dreigt te lopen (Koch et al., 2013). Tenslotte blijft het vooropgesteld doel immers niet langer beperkt tot het bestrijden van criminaliteitsfenomenen, maar kan de technologie evenzeer ingezet worden om vermiste personen te helpen lokaliseren (Brey, 2004).

Hoewel CCTV een relatief oud concept is dat meermaals aan wetenschappelijk onderzoek onderworpen werd, is smart CCTV een hedendaags en wereldwijd opkomend fenomeen. In tegenstelling tot traditionele camerabewaking, is er dan ook nog beduidend weinig objectief evaluatiemateriaal voorhanden omtrent de effectiviteit van smart CCTV-toepassingen. Echter is dit niet zo merkwaardig, vermits er tot op vandaag in veel landen een wettelijke grondslag ontbreekt die welbepaalde innovatieve AI-systemen voor wetshandhavingsdoelen reguleert. Daarnaast is het onder andere in België ook niet toegestaan om proefprojecten tot stand te brengen die bijvoorbeeld de accuraatheid van het politioneel gebruik van gezichtsherkennings-technologie trachten onder de loep te nemen (Controleorgaan op de Politionele Informatie, 2022a).

Alhoewel het niet te ontkennen valt dat smart CCTV op het vlak van wetshandhaving een veelbelovende innovatieve technologie kan zijn, komen tevens niet te negeren ethische problemen en bezorgdheden boven water.

2.4. Ethische problemen inzake smart CCTV

Naarmate het scala aan toepassingsmogelijkheden met behulp van smart CCTV verbreedt, nemen echter ook de daarmee gepaard gaande ethische bezorgdheden toe. Om het privacy versus security debat op een kritische manier te kunnen benaderen, is een beter inzicht vereist in wat er exact met intelligente camerabewaking op het spel staat, alsook welke maatschappelijke consequenties er uit het politioneel gebruik van deze technologie voortkomen. In het bijzonder staan we in dit luik stil bij vier ethische problemen die in de wetenschappelijke literatuur het meest frequent aangehaald worden. Deze bezorgdheden dienen evenzeer in rekening gebracht en in de mate van het mogelijke aangepakt te worden, alvorens smart CCTV voor wetshandhavingsdoeleinden in te zetten.

2.4.1. Privacy

In de huidige gedigitaliseerde samenleving heeft elk individu meer dan ooit nood aan eigen ruimte en eerbiediging van die persoonlijke levenssfeer. Zo staat het merendeel van de bevolking versteld wanneer aan het licht komt dat persoonlijke informatie zonder hun toestemming verzameld werd. Daarenboven wordt zelfs op openbare plaatsen verwacht dat de privacy optimaal gerespecteerd wordt (Brey, 2004). Bijgevolg nemen mensen dikwijls een kritische houding tegenover cameratoezicht in de publieke ruimte aan, vermits rechten en vrijheden van de mens in het gedrang dreigen te komen (Koch et al., 2013). In het bijzonder worden beeldtechnologieën die gebaseerd zijn op gedrags- of gezichtsherkenning beschouwd als controversiële toezichtmaatregelen, aangezien het systeem tal van persoonsgegevens kan onthullen zonder de betrokkene er iets van af weet (Laufs & Borrison, 2020; Perego, 2021).

Voorts is uit onderzoek gebleken dat de gepercipieerde privacybezorgdheden zich immers niet beperken tot het soort geregistreerde data, maar evenzeer gerelateerd zijn aan de doeleinden waarvoor ze initieel verzameld werden alsook door wie ze effectief gebruikt worden (Mariën & Poels, 2020; van Zoonen, 2016). Daarenboven impliceert het hanteren van AI software programma's dat het systeem mogelijks kwetsbaar is voor cyberaanvallen, met als gevolg dat het risico op inbreuken op persoonsgegevens reëel is. Het belang van cyber security en Privacy by Design (PbD) dient dan ook in de verf gezet te worden om de bescherming van persoons-gegevens te garanderen (Lee et al., 2019). Het achterliggend idee bij PbD is namelijk dat privacy niet uitsluitend door het naleven van reguleringsinstrumenten gewaarborgd kan worden

(European Group on Ethics in Science and New Technologies, 2014). In het bijzonder dienen proactieve maatregelen die de beveiliging van persoonsgegevens optimaliseren reeds bij de ontwikkeling van een welbepaald AI-systeem ingebouwd te zijn (Bu et al., 2020).

Aan de andere kant wordt beargumenteerd dat smart CCTV zelfs privacy bevorderend kan optreden. In deze context suggereert men dat het observeren van real-time camerabeelden door een humane operator juist hetgeen is dat een schending van iemands privacy vormt (Held et al., 2012). In principe kan elk individu die binnen het gezichtsveld van de camera valt door de operator geïdentificeerd worden. Hoewel dit probleem eigen is aan traditionele camera-bewaking, kan dit aan de hand van slimme camera's aangepakt worden (Koch et al., 2013). Zo wordt het beeldmateriaal door middel van algoritmes geanalyseerd en verwerkt, terwijl operators alleen maar beelden dienen te bekijken indien zich significante gebeurtenissen voordoen (Rahman, 2017).

Echter zal het al dan niet aantasten van iemands privacy sterk afhangen van hoe het systeem in de praktijk gehanteerd wordt. Het enigste realistische scenario waarbij smart CCTV de privacy kan bevorderen, is wanneer de beeldtechnologie beperkt blijft tot het filteren van informatie zodat enkel relevante feiten tot een beeldopname leiden of ter kennis van de operator komen. Daarbij is de operator nog steeds degene die opportune beslissingen neemt, waaronder het al dan niet overgaan tot interventie. Bovendien is het uitermate van belang dat het systeem niet meer valse positieven dan een humane operator genereert (Koch et al., 2013).

Desalniettemin dient opgemerkt te worden dat de ethische problemen nopens smart CCTV verregaander zijn dan enkel en alleen maar privacy-kwesties.

2.4.2. Error

Hoe dan ook dienen slimme camera's op openbare plaatsen te resulteren in de arrestatie van een aanzienlijk aantal delinquenten, terwijl slechts een geringe foutenmarge mag vastgesteld worden. Echter stellen tegenstanders evenzeer de accuraatheid van intelligente beeld-technologieën in vraag. Het probleem van error valt immers niet te negeren, vermits valse positieven aanleiding kunnen geven tot het lastigvallen en verhoren van onschuldige burgers door de politie (Brey, 2004).

Alvast waren specifieke cameratoepassingen uit proefprojecten van de Amsterdamse politie allesbehalve veelbelovend. Zo werd in 2008 reeds vastgesteld dat de technologie nog niet op punt stond om verdacht gedrag op parkeerterreinen automatisch te detecteren, vermits de gehanteerde software geen duidelijk onderscheid tussen normaal en afwijkend gedrag kon

maken (Flight, 2016). In een daaropvolgend experiment trachtte cameratoezicht op basis van audiocontentanalyse tekenen van agressie op te pikken, zoals angstschreeuwen, pistoolschoten, brekend glas, enzovoort. Niettemin bleken slechts twee van de honderd alarmen effectief betrekking te hebben op agressie (Flight, 2012). Hoewel de moderne technologie de afgelopen jaren vooruitgang geboekt heeft, blijken welbepaalde slimme cameratoepassingen tot op heden nog steeds veel valse positieven en valse negatieven op te leveren (Controleorgaan op de Politionele Informatie, 2022a). Een algoritme dat wel naar behoren lijkt te functioneren is automatische kentekenplaatherkenning, mits kwalitatief hoogwaardige ANPR-camera's ingezet worden (Flight, 2016; Gupta et al., 2020).

Daarnaast is er een groter risico op discriminatie ten aanzien van individuen met bepaalde karakteristieken (EU Fundamental Rights Agency, 2019; Van Brakel, 2015). De kans dat de technologie niet vrij is van bias kan mede verklaard worden aan de hand van ingebouwde vooroordelen in het gehanteerd algoritme (Perego, 2021). Zo heeft een algoritme namelijk de neiging om de vooringenomenheid van degene die het geschreven heeft te weerspiegelen (Almeida et al., 2021). Hierover wordt beargumenteerd dat algoritmen overwegend door blanke mannelijke ingenieurs geschreven worden, wat de ontwikkeling van beeldtechnologieën als dusdanig beïnvloedt.

In geval van gezichtsherkenning impliceert dit dat het systeem vooral op blanke gezichten van mannen getest wordt. Na verloop van tijd is de software dan ook getraind op een dataset die hoofdzakelijk uit dergelijke gezichten bestaat. Uiteindelijk resulteert dit in een algoritme dat burgers met een donkere huidskleur vaker incorrect identificeert dan degenen met een blanke huidskleur (Almeida et al., 2021; Perego, 2021). Zodoende heeft onderzoek reeds aangetoond dat gezichtsherkenningstechnologie minder accuraat is in het identificeren van Afro-Amerikaanse vrouwen (Fontes & Perrone, 2021; Grother et al., 2019). Dit brengt niet louter het recht op privacy van specifieke groepen verder in het gedrang, maar creëert ook een nadelig effect op het vertrouwen van burgers in wetshandhavers (Almeida et al., 2021; Safdar et al., 2016).

2.4.3. Function creep

Vermits wetshandhavingsinstanties ten aanzien van burgers het recht hebben om fysiek geweld en dwang uit te oefenen, wordt er per slot van rekening op vertrouwd dat de politie zowel rechtvaardig als rechtmatig optreedt (Schuilenburg et al., 2017). Niettemin impliceert een gebrek aan strikte regulering inzake smart CCTV dat het probleem van function creep als dusdanig niet uit te sluiten valt (Brey, 2004). In het bijzonder houdt dit fenomeen in dat

innovatieve technologieën niet meer exclusief in het kader van hun initieel doel gebruikt worden, maar omwille van hun flexibiliteit en effectiviteit uitbreiden naar andere doeleinden en functies (Safdar et al., 2016). Zo toont onderzoek aan dat function creep vrijwel altijd op de voorgrond treedt wanneer innovatieve technologieën geïmplementeerd worden (Brey, 2004).

In geval van smart CCTV wordt aan de hand van volgend voorbeeld geïllustreerd hoe dit fenomeen een negatieve impact op de privacy kan teweegbrengen. Zo kan de beeldtechnologie aanvankelijk worden ingezet om welbepaalde individuen, die reeds voor ernstige feiten veroordeeld werden, te identificeren in een menigte. Indien de politie vervolgens beslist om het systeem ook abnormaal gedrag te laten detecteren, is het denkbaar dat een significant hoger aantal personen geïdentificeerd worden. Echter kan specifiek gedrag door de ene groep geïnterpreteerd worden als een opkomst voor eigen rechten, terwijl anderen dit opvatten als een bedreiging. Wat onder antisociaal gedrag valt, is dan ook subjectief en gebonden aan bestaande sociale structuren, waarin gemarginaliseerde groepen vaak weinig inspraak hebben. Als gevolg daarvan zullen zij meer kans hebben om door het systeem geïdentificeerd te worden (Fontes & Perrone, 2021). Afgezien daarvan kan cameratoezicht leiden tot het zogenaamde 'chilling effect'. Wanneer mensen het gevoel krijgen dat ze bekeken worden, gaan ze zich vaak anders en mogelijks verdacht gedragen (Milligan, 1999). Bijgevolg detecteert de camera het afwijkend gedrag, waardoor burgers onrechtmatig door de politie lastig gevallen worden, en zelfs eventueel van hun vrijheid beroofd worden. Hoewel strikte regulering van smart CCTV function creep tot op een zekere hoogte kan beperken, kan dit fenomeen niet ten volle vermeden worden (Brey, 2004).

2.4.4. Transparantie

In het kader van slimme beeldtechnologieën voor wetshandhavingsdoeleinden dient evenzeer belang gehecht te worden aan het principe van transparantie. Aan de ene kant vormt het gebrek aan technologische transparantie van de door algoritmen aangestuurde systemen wellicht de grootste barrière om te doorbreken. Zo stelt het COC vast dat Belgische politie-instanties reeds moeilijkheden ondervinden om de werking van traditionele camerabewaking uit te leggen of zelfs te begrijpen, laat staan wanneer meer complexe beeldtechnologieën hun intrede doen (Controleorgaan op de Politionele Informatie, 2022a).

Aan de andere kant is het ten aanzien van rechtsonderhorigen uitermate van belang dat er transparant gecommuniceerd wordt over verscheidene aspecten van de ingezette technologie (Mariën & Poels, 2020). In het bijzonder dient er naar het brede publiek toe meer helderheid gecreëerd te worden in verband met de drijfveren waarom en de doelen waarvoor persoons-

gegevens verzameld en verwerkt worden (European Group on Ethics in Science and New Technologies, 2014). Het feit dat betrokkenen over de aanwezigheid van cameratoezicht adequaat geïnformeerd worden, volstaat in het geval van smart CCTV niet meer. Zo zijn voorbijgangers, die door de slimme camera gemonitord worden, zich niet bewust van het soort gedrag dat het systeem uitdrukkelijk tracht te detecteren. Vandaar kan het reeds eerder aangehaald chilling effect zich op het gedrag van burgers voordoen, vermits men bezorgd is om welbepaald verdacht gedrag te stellen (Koch et al., 2013).

Hierover transparant communiceren wil immers niet zeggen dat het gebruik van de technologie als het ware gerechtvaardigd is. Het is een stap in de goede richting maar dient in hoofde beschouwd te worden als een noodzakelijke voorwaarde om het debat inzake de rechtvaardiging ervan te kunnen aanvangen (European Group on Ethics in Science and New Technologies, 2014).

3. Methodologie

Vooraleer de resultaten van het huidige onderzoek uiteengezet en geïnterpreteerd worden in het licht van de vooropgestelde onderzoeksvragen en voorgaand onderzoek, dient de nodige aandacht naar de gehanteerde methodologie voor de dataverzameling uit te gaan teneinde de bevindingen op een correcte manier te kunnen interpreteren.

3.1. Onderzoeksmethode

Zoals eerder aangehaald, beoogt deze masterproef kritisch te reflecteren over de implementatie van smart CCTV voor wetshandhavingsdoeleinden, waarbij (privacy-)bezorgdheden en bedenkingen nopens welbepaalde toepassingen van deze beeldtechnologie in rekening gebracht worden. Hierbij dient opgemerkt te worden dat het niet de bedoeling is generaliseerbare uitspraken over de houding tegenover dit toezichtinstrument te doen, maar om met Belgische en Nederlandse professionele sleutelfiguren in de diepte stil te staan bij de exacte problematiek en de mate waarin het politioneel gebruik vanuit hun standpunt al dan niet wenselijk en ethisch verantwoord is. Zodoende werd dan ook geopteerd om de vooropgestelde doelstelling te bereiken aan de hand van een kwalitatief onderzoeksopzet met semi-gestructureerde interviews.

Deze flexibele, interactieve methode brengt enige zekerheid met zich mee dat alle relevante thema's aan bod komen, terwijl de volgorde van de vragen mede door het verloop van het gesprek en de gedachtegang van de respondent bepaald wordt (Beyens et al., 2016; Dearnley, 2005). Door het stellen van gerichte open vragen is de onderzoeker tenslotte in staat om respondenten te stimuleren tot het geven van exact die informatie die nodig is om de onderzoeksvragen adequaat te beantwoorden (Hardyns, 2019).

Bij elk interview werd een vooraf voorbereide topiclijst (zie Bijlage 4) als leidraad gehanteerd, opdat de te bespreken onderwerpen gegarandeerd aan bod zouden komen (Mortelmans, 2020). Ondanks het feit dat deze lijst de te behandelen onderwerpen in een welbepaalde volgorde weergeeft, was men niet noodzakelijk aan deze volgorde gebonden. Indien het verloop van het gesprek een onverwachte maar interessante wending nam, had de interviewer steeds de vrijheid om zich hieraan aan te passen (Magnusson, 2015).

De topiclijst bleef in de loop van het onderzoek steeds aan verandering onderhevig. Er valt immers niet uit te sluiten dat onvoorziene thema's aan bod komen die voldoende van belang lijken om ze aan de daaropvolgende interviews toe te voegen. Bovendien is het mogelijk dat bepaalde vragen en onderwerpen geherformuleerd of weggelaten dienen te worden (Adams, 2015).

Voorts is het van belang om enkele nadelen gebonden aan semi-gestructureerde interviews in het achterhoofd te houden. Vermits slimme camera's tot één van de meest intrusieve en controversiële wetshandhavingstools van de eenentwintigste eeuw behoren, valt de kans op sociaal wenselijk antwoorden immers niet uit te sluiten (Adams, 2015; Hardyns, 2019). Bijgevolg werd elke respondent bij de aanvang van het interview voldoende op de hoogte gebracht van de doelstelling van het onderzoek en het feit dat subjectief gekleurde antwoorden als dusdanig verwacht worden. Anderzijds kunnen kenmerken van de interviewer, zoals leeftijd, geslacht, taalgebruik en uiterlijk voorkomen, het verloop van het interview enigszins beïnvloeden en het opbouwen van een vertrouwensrelatie al dan niet bevorderen. Er al dan niet in slagen om een vertrouwensband op te bouwen, kan tenslotte de bereidheid van de respondent om voldoende open en transparant over de thematiek te communiceren in zekere mate beïnvloeden (Beyens et al., 2016).

Doorgaans lijkt het bij kwalitatief onderzoek niet vanzelfsprekend om de geloofwaardigheid en betrouwbaarheid na te gaan. Desondanks dien je als onderzoeker te streven naar het afleveren van een kwaliteitsvol werk. Het is dan ook van belang om zo transparant mogelijk over de aangewende methode te communiceren.

In het kader van het huidige onderzoek werd geopteerd om triangulatie toe te passen, wat impliceert dat zowel gegevens van respondenten als kennis uit de wetenschappelijke literatuur verzameld werden. Deze strategie werd oorspronkelijk naar voren geschoven om de validiteit van de resultaten te verhogen (Maesschalck, 2016). Inmiddels wordt het eerder gezien als een strategie om dieper inzicht in het bestudeerde topic te verkrijgen, waarbij reeds verworven kennis gerechtvaardigd en onderbouwd wordt door aanvullende kennis op te doen (Flick, 2004; Steinke, 2004).

Alvorens semi-gestructureerde interviews met professionele sleutelfiguren af te nemen, vond dan ook een narratieve literatuurstudie plaats om een eerste inzicht te verkrijgen in de ethische problemen rond slimme camera's voor opdrachten van bestuurlijke of gerechtelijke politie. Als onderzoeker is het namelijk relevant om op de hoogte te zijn van wat er over de exacte problematiek reeds geweten is. Met het oog op het verwerven van relevante literatuur werd beroep gedaan op verscheidene elektronische databanken, waaronder Google Scholar en Web of Science, alsook op de online catalogus van de Universiteitsbibliotheek Gent. Hierbij werden zoektermen als 'smart CCTV', 'intelligente camerabewaking', 'gezichtsherkenning', 'gedrags-herkenning' en 'ANPR' in combinatie met termen als 'privacy', 'ethische problemen',

‘bedenkingen’, ‘evaluatie’ en ‘wetshandhaving’ gehanteerd, zowel in het Nederlands als in de Engelse vertaling ervan.

Daarenboven werd de sneeuwbalmethode aangewend. Deze zoekstrategie houdt namelijk in dat alle literatuurverwijzingen van de reeds gevonden bronnen gecontroleerd worden om gerelateerde en relevante literatuur te identificeren (Hong et al., 2019).

Tot slot werd aan elke respondent de mogelijkheid geboden om het transcript van zijn/haar interview na te lezen, alvorens het in de rapportage opgenomen werd. Op deze manier kunnen respondenten feedback geven en verifiëren dat ze gezegd hebben wat ze effectief bedoelden (Dearnley, 2005; Maesschalck, 2016).

3.2. Selectie van respondenten

Vooraleer er met de dataverzameling aangevangen wordt, is het als onderzoeker noodzakelijk om evenzeer te reflecteren over de onderzoekseenheden die je in uw kwalitatieve steekproef wenst op te nemen. In het bijzonder werden professionele sleutelfiguren geselecteerd die reeds voldoende met de te behandelen thematiek vertrouwd zijn en als dusdanig zinvolle en betrouwbare informatie kunnen opleveren om de vooropgestelde onderzoeksvragen te beantwoorden. Het vooropstellen van specifieke selectiecriteria was in het kader van dit onderzoek niet aan de orde.

Aan de ene kant verliep de rekrutering van onderzoekseenheden met behulp van de sneeuwbal-methode, vermits er bij de aanvang van het onderzoek nog onvoldoende zicht was op wie er nu exact bruikbare informatie kan aanleveren. Hierbij werd er aan de reeds geïnterviewde actoren gevraagd of zij nog andere individuen aanbevelen die een significante bijdrage aan het onderzoek kunnen leveren (Merkens, 2004; Mortelmans, 2020). Aan de andere kant werden indicaties van relevante actoren uit de wetenschappelijke literatuur geput (Magnusson, 2015). Bovendien waren LinkedIn en ResearchGate behulpzame kanalen om met professionele sleutelfiguren in contact te komen.

De omvang van de steekproef was afhankelijk van een aantal factoren. Hoewel de bereidheid tot deelname aan het onderzoek een belangrijke rol speelt, beoogde men respondenten te blijven rekruteren tot het saturatiepunt bereikt werd. Dit houdt in dat de steekproef volledig is wanneer geen nieuwe informatie en inzichten meer vergaard worden, de onderzoeker kan voorspellen wat de respondent in zijn/haar antwoord zal beklemtonen en kan concluderen dat er voldoende materiaal ter beschikking is om de onderzoeksvragen te beantwoorden (Merkens, 2004;

Mortelmans, 2016). Om deze redenen werd de omvang van de steekproef niet op voorhand gespecificeerd.

Gedurende de periode maart - april van 2023 werden er in totaal zeven interviews afgenomen, waarvan één fysiek en zes online plaatsvonden. Hoewel een online interview de communicatie met geografisch gespreide respondenten faciliteert, kunnen non-verbale cues, zoals lichaamstaal, verloren gaan (James & Busher, 2016). Desalniettemin zijn de onderzoeksvragen van die aard dat het louter registreren van de letterlijke bewoording van respondenten volstaat. Derhalve doet het gebrek aan non-verbale communicatie geen afbreuk aan de resultaten. Voorts kenden de interviews een verschillende duur gaande van 47 tot 73 minuten.

Een voor het onderzoek belangrijk gegeven ligt in het feit dat de bevraagde onderzoeksubjecten zich van elkaar kunnen differentiëren naargelang hun professionele achtergrond. In het bijzonder namen twee senior beleidsadviseurs/onderzoekers gespecialiseerd in cameratoezicht, een voormalig voorzitter van de Gegevensbeschermingsautoriteit, de voorzitter van het Controleorgaan op de Politionele Informatie, een senior Data Protection Officer (DPO), een DPO/directeur van Dasprive vzw en een docent/postdoctoraal onderzoeker gespecialiseerd in AI en ethiek deel aan het huidige onderzoek. Het aantal jaren beroepservaring die de respondenten op het moment van het interview reeds verworven hadden, varieerde tussen de 19 en 42 jaar.

3.3. Ethische aspecten

Doorgaans is het geen uitzondering dat criminologen onderzoek naar gevoelige thema's doen. Het belang van een vrijwillige deelname aan het onderzoek dient dan ook in de verf gezet te worden. Zo is het de taak van de onderzoeker om potentiële respondenten voldoende te informeren over het doel van het onderzoek en de rol die participanten hierin vervullen, zodat eenieder een bewuste keuze kan maken om al dan niet deel te nemen (Hopf, 2004; Vander Laenen & O'Gorman, 2016). Om dit te kunnen garanderen, voorzag het huidige onderzoek zowel een informatiebrief (zie Bijlage 3) als *informed consent* (zie Bijlage 2) die voorafgaand aan het interview door de respondent in kwestie ondertekend werd. Hierbij werd evenzeer toegelicht dat eenieder het recht heeft hun medewerking aan het onderzoek op ieder moment stop te zetten. Bovendien werd er bij de aanvang van elk interview toestemming voor het gebruik van de opnameapparatuur verkregen.

Overigens beoogde men het vertrouwelijk karakter van het verkregen onderzoeksmateriaal te garanderen, alsook de anonimiteit en privacy van de respondenten in de mate van het mogelijke

te respecteren. In plaats van reële namen van participanten in de rapportage op te nemen, werd er vanaf de transcriptie geopteerd om pseudoniemen aan te wenden teneinde de identiteit van de persoon in kwestie te beschermen. Op deze manier is het voor derden namelijk onmogelijk om welbepaalde informatie verworven uit de interviews te associëren met een specifiek individu (Magnusson, 2015).

Daarenboven waren participanten zich bewust van de mogelijkheid om de transcriptie van hun eigen interview achteraf na te lezen en citaten aan te passen of zelfs verklaringen in te trekken waar ze dit nodig achten. Tenslotte wordt het verzameld onderzoeksmateriaal, conform het RDM-beleidskader van de Universiteit Gent, na een termijn van vijf jaar verwijderd en zal deze masterproef enkel en alleen maar openbaar gemaakt worden mits toestemming van de geïnterviewden.

Meer informatie met betrekking tot de dataverzameling, -verwerking en -opslag kan in het datamanagementplan (zie Bijlage 1) geraadpleegd worden.

3.4. Dataverwerking en -analyse

Het feit dat personen in het huidige onderzoek als bron fungeren, brengt met zich mee dat je een grote hoeveelheid aan diepgaande informatie op een relatief snelle manier ter beschikking kan hebben (Hardyns, 2019). Desalniettemin doet de dataverwerking en -analyse de tijd die je met de gegevensverzameling eventueel bespaart in sterke mate teniet (Mortelmans, 2017). Om de verzamelde data bij interpretatief onderzoek op een efficiënte manier te analyseren, volstaat het hanteren en beluisteren van interviewopnames met de daarbij horende aantekeningen immers niet (Magnusson, 2015). De onderzoeker dient namelijk in staat te zijn om de exacte bewoording van de respondent letterlijk te citeren (Beyens et al., 2016). Zodoende werden de audio-opnames van de interviews via transcriberen omgezet naar een schriftelijke neerslag, alvorens tot de analyse van de resultaten over te gaan. Hoewel het handmatig transcriberen van interviews een tijdrovend proces is, geraakt men op deze manier meer vertrouwd met de data en worden de eerste verbanden reeds automatisch gelegd (Decorte, 2016).

Uiteindelijk werden de transcripties met behulp van het softwarepakket NVivo gecodeerd en geanalyseerd, vermits een dergelijk kwalitatief onderzoeksprogramma u in staat stelt om het onderzoeksmateriaal op een gestructureerde manier te ordenen (Mortelmans, 2020). Hierbij werd de data in eerste instantie opgedeeld en gereduceerd door codes toe te wijzen aan stukken tekst die voor het onderzoek van belang lijken. Naderhand werden de codes aan elkaar

gerelateerd en categorieën opgebouwd teneinde verbanden tussen de diverse categorieën te kunnen leggen (Mortelmans, 2017).

Tot slot dient aangehaald te worden dat de uitvoering van het huidige onderzoek zich door een cyclisch verloop liet kenmerken, waarbij de processen van dataverzameling en -analyse tegelijkertijd plaatsvonden en elkaar continu afwisselden (Decorte, 2016). Zo werd het verzameld onderzoeksmateriaal kort na elk interview alvast getranscribeerd en geanalyseerd vooraleer een daaropvolgend interview plaatsvond. Op deze manier creëerde men ook de mogelijkheid om de topiclijst op regelmatige basis aan evaluatie te onderwerpen en waar nodig tijdig aan te passen.

4. Resultaten

In dit luik wordt een uiteenzetting gegeven van de resultaten die uit de zeven semi-gestructureerde interviews met zowel Belgische als Nederlandse professionele sleutelfiguren naar voren kwamen. Bij de aanvang van elk interview werd gepeild naar de houding van de respondent tegenover het politioneel cameragebruik in België of Nederland, met inbegrip van de uitrol van het ANPR-cameranetwerk. Daaropvolgend werd vanuit hun standpunt dieper ingegaan op (privacy-)bezorgdheden en bedenkingen ten aanzien van slimme camera's in het algemeen en welbepaalde toepassingen in het bijzonder.

In de eerste plaats zal niemand ontkennen dat (intelligent) cameratoezicht op openbare plaatsen een beduidende impact op ons recht op privacy teweegbrengt. Eenieder heeft namelijk het recht met rust te laten geworden en in vrijheid te functioneren, zonder inmenging van de overheid (Buil et al., 2023). Echter is dit fundamenteel grondrecht van burgers geen absoluut mensenrecht.[4] Conform internationale mensenrechtenverdragen valt een eventuele inmenging of beperking te rechtvaardigen, mits deze in overeenstemming is met de wet, een legitiem doel nastreeft en noodzakelijk is in een democratische samenleving (Fussey & Murray, 2019). Bovendien zijn privacy en gegevensbescherming niet de enige grondrechten die in het sociaalwetenschappelijk debat doorslaggevend kunnen zijn. Alvorens op de exacte problematiek in te gaan, dient evenzeer belang gehecht te worden aan het grondrecht op veiligheid en het feit dat de respondenten de meerwaarde van dit toezichtinstrument niet zozeer betwisten. Zo wezen vier van de zeven respondenten uitdrukkelijk op het operationele nut en de bijdrage ervan aan de waarheidsvinding.

> *"Het staat vast gewoon dat camerabeelden inderdaad dikwijls doorslaggevend zijn, of minstens het toelaten uw onderzoek te sturen in een bepaalde richting. En moest men het niet hebben, denk dat we mediagevoelige zaken kunnen opsommen waar het zeer moeilijk zou geweest zijn zonder camerabeelden." (P003)*

> *"Ik heb in de loop van moeten vaststellen dat het niet alleen bruikbaar is voor repressie, maar ook om uw onschuld te bewijzen. Ik heb ook moeten vaststellen dat dergelijke camerabeelden soms ook wel serieuze mistoestanden aan het licht konden brengen. (…) Het is ook een inbreuk natuurlijk op de bescherming van uw rechten en vrijheden wanneer u slachtoffer bent van een valse of onjuiste beschuldiging. En dan kan die verwetenschappelijking van de bewijsvoering u zelf helpen hé." (P002)*

[4] Art. 8 EVRM.

Hoewel het vertrouwen in camerabeelden op reactief vlak om onder meer daders te vatten en te veroordelen aan de relatief hoge kant lag, beargumenteerden twee respondenten dat ze niet overtuigd waren van het criminaliteitsreducerend effect van camera's.

> *"Ik geloof niet zozeer in het preventieve effect ervan. Dat is nog nooit aangetoond naar mijn weten. Maar het is ontegensprekelijk zo dat camera's zeer belangrijk zijn wat het gerechtelijk werk betreft. Denk dat je geen enkel serieus onderzoek meer hebt waar er geen camerabeelden meer opgevraagd worden, of waar men toch probeert te zoeken naar camerabeelden." (P003)*

> *"Wat je eigenlijk nu ziet gebeuren in België, is eind jaren '90 in het Verenigd Koninkrijk gebeurd. Dus een explosie van het aantal camera's. En als gevolg daarvan is er heel veel onderzoek gebeurd naar cameratoezicht in het kader van preventie. (...) Er is enorm veel gepubliceerd en wetenschappelijk onderzoek naar gedaan, waaruit is gebleken dat cameratoezicht in het kader van criminaliteitspreventie niet werkt. Buiten een klein effect in parkeergarages." (P007)*

Bovenstaande opvattingen stemmen overeen met de weinig consistente onderzoeksbevindingen nopens preventieve effecten en het feit dat wetenschappelijk onderzoek geen eenduidig antwoord oplevert. Het is tenslotte niet evident om een vastgestelde negatieve tendens van de criminaliteitscijfers toe te wijzen aan cameratoezicht, vermits camera's doorgaans in een context geïmplementeerd worden waar andere interventiestrategieën van kracht zijn, zoals politiepatrouilles, verbeterde straatverlichting, private bewakingsagenten, enzovoort (Melis, 2021).

Nochtans beweren politici dat slimme camera's een cruciaal toezichtinstrument in de criminaliteitsbestrijding vormen. Hoewel dergelijke camera's aan de ene kant een veelbelovende impact op de wetshandhaving kunnen betekenen, bekommerden de respondenten zich in ieder geval om het gebrek aan objectief bewijsmateriaal waarmee de overheid de noodzakelijkheid en effectiviteit ervan voor wetshandhavingsdoelen onderbouwt en aantoont. In welke mate kan men op een gepaste manier een proportionaliteitstoets doen als de exacte veiligheidswaarde niet geweten is? Er worden alsmaar meer camera's operationeel ingezet, maar het achteraf evalueren lijkt zich in de ogen van respondenten (N=3) zelden voor te doen. Derhalve rijst zich de vraag of er wel degelijk wordt ingezet op het garanderen van de veiligheid of er louter wordt ingespeeld op veiligheidsgevoelens van burgers.

"Het basisprobleem dat ik ermee heb, is dat de noodzaak niet fatsoenlijk wordt aangetoond. Men kan niet onderbouwen 'waarom doen we dit?'. Behalve met wat vage bewoordingen en, wat de politici natuurlijk niet vreemd is, proberen inspelen op populisme door aan te geven dat daarmee de veiligheid verhoogd wordt, zonder dat nu eens echt te kunnen onderbouwen. (...) Wat geven we op aan privacy en wat krijgen we ervoor terug? En die uitkomst is iets wat ik nog nooit fatsoenlijk uitgewerkt heb gezien." (P005)

Aan de andere kant is er uit de interviews wederom gebleken dat de risico's gerelateerd aan slimme cameratoepassingen verregaander zijn dan louter privacy-kwesties en een niet te negeren impact op onze samenleving impliceren. Zodoende verwezen drie respondenten uitdrukkelijk naar de neiging die burgers mogelijks ondervinden om hun gedrag aan te passen en te onderdrukken vanwege de aanwezigheid van camerasurveillance of de loutere perceptie die ze hebben van bekeken te worden. Dit fenomeen staat in de literatuur ook wel bekend als het chilling effect, en werd door één van de respondenten geïllustreerd met het voorbeeld van een burgerrechtenactivist die zich uit angst voor politiesurveillance weerhoudt om vreedzaam mee te lopen met een betoging.

Andere bezorgdheden waren inherent verbonden aan de manier waarop overheidsinstanties met de camerabeelden en de geregistreerde data omgaan teneinde privacy-risico's te minimaliseren. Hoewel het vertrouwen bij enkelen aan de relatief hoge kant lag, stelde het merendeel van de respondenten (N=5) de mate waarin dat vandaag de dag op een betrouwbare, verantwoorde en wettelijk conforme manier gebeurt in vraag. Hierbij werd onder meer het misbruiken van de beelden, de correctheid van de data in de politionele databanken, het niet respecteren van bewaartermijnen en beveiligingsniveaus, en de misinterpretatie van het recht op inzage aangekaart. Tevens werd in twijfel getrokken dat alle politiezones op een uniforme manier met camera's en privacy omgaan. Dergelijke issues leek men niet zozeer te wijten aan foute bedoelingen van wetshandhavers, maar eerder aan nalatigheid en gebrek aan expertise of ervaring van degenen die intern verantwoordelijk zijn voor de dataverwerking. Desalniettemin beargumenteerden twee respondenten dat hun wantrouwen in de private spelers opmerkelijk groter is, vermits commerciële ondernemingen onzorgvuldiger met onze persoonsgegevens lijken om te gaan.

"Aan de andere kant merk ik ook wel dat bedrijven een datahonger hebben die heel groot is. Heel veel private instanties hebben wel door dat zij met data heel veel kunnen, en die maken juist de afweging weer te veel naar economische belangen. En die zijn ook

belangrijk, maar die vind ik minder belangrijk dan veiligheid, gezondheid en een goed milieu. Dus dat bedrijven zo losgeslagen zijn in dataverzameling, dat vind ik wel een groot probleem." (P001)

Daarnaast haalden drie respondenten aan dat het cameragebruik doorgaans niet beperkt blijft tot zijn oorspronkelijke functie en er veelal de neiging bestaat om het voor andere doeleinden in te zetten. Aanvankelijk beoogden politici ANPR-camera's operationeel te benutten om zware misdadigers en terroristen op te sporen, alsook verkeersregels op autosnelwegen te handhaven. Echter stelden de respondenten vast dat we alsmaar meer zijn geëvolueerd naar het inzetten van ANPR-camera's voor minder ernstige feiten, zoals het niet verzekerd rondrijden, het toezicht aan de lage-emissiezones, de avondklok gedurende de coronapandemie, enzovoort.

"ANPR-camera's. Wat we daar zien, is dat dat dan in de tijd is geïmplementeerd in het kader van zware criminaliteit. Maar dat we nu al meer zijn afgegleden naar het gebruik van ANPR-camerabeelden door verzekeringsmaatschappijen en het opsporen van auto's die niet verzekerd zijn. (...) Het wordt in eerste instantie gemotiveerd voor een bepaald doel, waar de maatschappij gaat zeggen 'ah ja, dat is een belangrijk doel. Daarvoor kunnen we wel onze privacy een beetje opgeven'. Maar dan wordt het op termijn toch ook gebruikt voor minder serieuze dingen." (P007)

Zoals eerder vermeld, is function creep een inherent risico aan innovatieve surveillance-technologieën. Een strikte regulering ten aanzien van de desbetreffende technologie kan dit fenomeen tot op een zekere hoogte beperken, maar niet ten volle vermijden (Brey, 2004). Bovendien vonden twee respondenten het opvallend dat er niet alleen cijfers ontbreken die objectief de veiligheidswaarde aantonen, maar het tevens niet vanzelfsprekend en bijna onbestaande is dat cameratoezicht op een bepaalde plaats terug afgeschaft wordt wanneer het geen impact lijkt te hebben en de beelden niet meer voor begrijpelijke doeleinden benuttigd worden, met als gevolg dat rechten en vrijheden vrijwel onnodig in het gedrang komen.

"Wanneer gaan we dan nog eens een keer een stapje terugzetten? Want stapjes vooruit zetten, doet men heel graag. Maar camera's terugzetten als blijkt dat ze geen nut hebben. Dat heb ik nog nooit gezien." (P005)

"En het is best moeilijk om het cameratoezicht weer af te schaffen, want ofwel is de veiligheid in het gebied verbeterd en dan zegt iedereen 'ja, dat komt door die camera's'. Ofwel is de veiligheid niet verbeterd, en dan zegt iedereen 'ja, dan hebben we ze nog

steeds nodig'. Met andere woorden: als het cameratoezicht eenmaal begonnen is, is het heel moeilijk om ermee op te houden." (P006)

Voorts gaven drie van de zeven respondenten aan onvoldoende geïnformeerd te zijn over de data die van ons gecapteerd worden en wat er precies mee gebeurt. Daaraan voegden twee respondenten toe dat je ook niet weet of uw handelingen door een traditionele of slimme camera vastgelegd worden, met uitzondering van de ANPR-camera's waarbij de verplichting reeds bestaat om 'ANPR' in het pictogram te vermelden. Derhalve kan een gebrek aan kennis over wat het toezichtinstrument beoogt te detecteren wederom leiden tot een chilling effect op het gedrag van burgers, waarbij men zich anders gaat gedragen uit angst om verdacht over te komen (Koch et al., 2013). Hoewel er ruimte voor verbetering is, stelde één van de respondenten vast dat transparantie naar het brede publiek toe er in de afgelopen jaren op vooruitgegaan is.

"Ik heb wel gemerkt dat transparantie recent een beetje toegenomen is. Als je kijkt op de websites van de lokale politie zijn er nu veel die een overzicht geven van het gebruik van technologie door die zone. Een aantal jaren geleden was dat helemaal niet het geval. We wisten helemaal niet wat voor technologie de politie gebruikte. (...) Maar met de nieuwe soort camera's waarmee ze aan het experimenteren zijn rond objectherkenning, gedragsherkenning. Daar vind ik het bijzonder problematisch dat daar geen transparantie over is, en dat je niet weet of je door een traditionele camera wordt bekeken of door een slimme camera." (P007)

In de gevallen waar nieuwe technologieën aangewend worden en geheimhouding van het onderzoek centraal staat teneinde opsporingsbelangen te beschermen, beklemtoonde deze respondent dat de politie op zijn minst transparant dient te zijn jegens de toezichthoudende autoriteiten, wat ook niet altijd het geval blijkt. Hierbij werd onder meer verwezen naar het onrechtmatig gebruik van Clearview AI door de geïntegreerde politie en de experimenten met LFR op de luchthaven van Zaventem, die pas naderhand door het COC aan het licht kwamen en bijgevolg stilgelegd werden. Een andere respondent richtte zich eerder op het feit dat politici ook niet de indruk moeten geven dat we met slimme camera's alle handhaving rondkrijgen.

"Iets anders is natuurlijk de politieke communicatie rond het creëren van een ANPR-schild. Men had daarover van alles gezegd hé. 'We gaan daardoor misdrijven vermijden.' 'We gaan de zware criminaliteit bestrijden.' Ja, dat is natuurlijk maar een deeltje van het verhaal hé. De realiteit is dat het ANPR-schild helemaal niet preventief werkt." (P003)

Overigens heerste er gedurende de interviews een gevoel dat er niet alleen te weinig stilgestaan wordt bij de maatschappelijke consequenties, maar ook bij de impact van innovatieve beeldtechnologieën op de wetshandhavingsinstanties zelf.

> *"Het belangrijkste is 'wat doet ge met al die beelden?". Zijt ge operationeel wel nog in staat om dat allemaal te capteren? De politie klaagt over een enorme infobesitas en over de gigantische data die binnenkomen. Maar langs de andere kant blijft men natuurlijk wel camera's bijzetten, en dus meer data binnentrekken. Wij zien dat er toch nog te weinig over gereflecteerd wordt, en dat men al te gemakkelijk aanneemt dat men het nodig heeft." (P003)*

Dergelijke zaken dienen tevens in rekening gebracht te worden alvorens fundamentele beslissingen te nemen inzake het al dan niet operationeel inzetten van nieuwe en meer intrusieve camera's.

Tot slot dient in het achterhoofd gehouden te worden dat proportionaliteit niet louter draait rond de balans tussen grondrechten van burgers en het leveren van maatschappelijke veiligheid. Het gaat ook over het verantwoorden en onderbouwen waarom de desbetreffende technologie het minst intrusief is om het beoogde doel te realiseren (Fontes & Perrone, 2021). Zodoende vonden twee respondenten het essentieel om in eender welke context steeds minder privacy-intrusieve alternatieven voor slimme camerasystemen te overwegen waarmee hetzelfde legitieme doel bereikt kan worden. Hierbij verwoordde één van de respondenten als volgt hoe er in onze moderne samenleving nog al snel gegrepen wordt naar en lichtvaardig omgesprongen wordt met innovatieve technologieën, terwijl wetenschappelijk onderbouwde beleidsaanbevelingen onvoldoende in rekening gebracht worden:

> *"Er is zeker in het kader van misdaadpreventie een hele reeks criminologisch onderzoek met best practices. En ik heb de indruk sinds dat technologie zo geëxplodeerd is, dat dat soort onderzoek genegeerd wordt. En dat er geïnvesteerd wordt in technologie in plaats van beleidsstrategieën die wel werken, zoals bijvoorbeeld community policing." (P007)*

Hoewel bovenstaande issues inherent zijn aan slimme camerasystemen, zal de mate waarin een privacy-intrusief toezichtinstrument gepercipieerd wordt als al dan niet wenselijk en ethisch verantwoord sterk afhangen van wat het systeem exact beoogt te detecteren en de (sociale) context waarin het geïmplementeerd wordt. In wat volgt, wordt dan ook dieper ingegaan op de voornaamste bezorgdheden en bedenkingen van professionele sleutelfiguren die in het bijzonder gerelateerd zijn aan de vooropgestelde cameratoepassing.

4.1. Automatische kentekenplaatherkenning

Zowel in België als in Nederland worden ANPR-camera's reeds uitgebreid ingezet om kentekens van voertuigen te herkennen en vast te leggen. Hierbij beoogt het systeem waargenomen nummerplaten automatisch te vergelijken met zogenaamde referentielijsten bestaande uit gegevens van voertuigen en/of bestuurders die aandacht van de politie behoeven. In een wetshandhavingscontext worden dergelijke camera's onder meer geïmplementeerd bij trajectcontroles om snelheidsovertredingen vast te stellen, maar ook om gestolen of niet-verzekerde voertuigen, geseinde personen of individuen met openstaande verkeersboetes te lokaliseren en staande te houden (Homburg et al., 2016). Conform de WPA mogen de beelden voor een termijn van maximaal twaalf maanden bewaard worden.[5]

Ten opzichte van de andere besproken cameratoepassingen werd ANPR het meest positief geëvalueerd. In de eerste plaats gingen de respondenten (N=4) ervan uit dat de foutenmarge bij ANPR-camera's aan de relatief lage kant ligt, waardoor het aantal bestuurders die ten onrechte door de politie lastig gevallen en aangehouden worden gering is. Zo valt niet te betwijfelen dat de technologie onder gecontroleerde condities in laboratoria vrijwel 100% betrouwbaar is, aangezien kentekens gemaakt zijn om te lezen. Desondanks heeft onderzoek reeds aangetoond dat tal van factoren, waaronder slechte weersomstandigheden, lichtcondities, afbeeldingen met lage resolutie, afstand, vuile nummerplaten, enzovoort, kunnen leiden tot een hoger percentage valse positieven (Tang et al., 2022). In ieder geval beargumenteerde één van de respondenten dat kwalitatief hoogstaande ANPR-systemen met infraroodcamera's toch wel in staat zijn passerende kentekens op autosnelwegen in 95% van de gevallen foutloos te lezen, terwijl de technologie in stadscentra beduidend slechter presteert.

> *"Wat het beste werkt, is een ANPR-camera die specifiek is ingesteld voor het lezen van kentekens op een bepaalde plek. En die camera moet dat doen met het gewone spectrum, wat wij kunnen zien. Maar ook met infrarood, want de meeste kentekenplaten zijn infrarood geschikt. Dus je kan heel goed een infraroodbeeld koppelen aan het videobeeld en dan matchen. Dan wordt de kwaliteit veel beter. En je moet een radar hebben die bepaald hoe ver het kenteken van de camera af is. (...) Dat soort camera's werken heel erg goed, maar die zijn ook heel erg duur. Want die hebben radar aan boord om te schatten hoe ver iets van zich af is, en met welke snelheid dat voertuig naar ze toekomt." (P001)*

[5] Art. 44/11/3decies WPA.

"Dat werkt natuurlijk niet midden in een drukke binnenstad van [stad]. Dat lukt niet bij de grote markt, want dan rijden auto's met verschillende snelheden dwars door het hele straatbeeld. Daar kan je niet zeggen 'dat kenteken zit ongeveer altijd hier'. Dat kenteken kan overal zijn. En dan wordt het weer minder betrouwbaar." (P001)

Afgezien van de mate waarin ANPR-camera's kentekens foutloos lezen, erkende het merendeel van de respondenten (N=5) eveneens de (operationele) meerwaarde die het voor zowel wets-handhavers als voor onze samenleving kan betekenen. Bovendien werd daarbij aangegeven dat de privacy-consequenties eerder minimaal zijn, mits de verwerking van onze persoonsgegevens onderworpen is aan de nodige waarborgen teneinde datalekken te voorkomen.

"Als je zomaar camerabeelden maakt, moet je achteraf de data door en moet je er proberen betekenis aan te geven. Dat is heel inefficiënt werken. En een camera met ANPR maakt het veel makkelijker om deze te doorzoeken." (P001)

"Als mij een misdrijf overkomen is en ik weet dat de dader weggevlucht is in een auto met een bepaalde nummerplaat, dan vind ik het handig als de politie later kan opsporen waar die persoon is en kan aanhouden." (P006)

"Eigenlijk is dat nu niet zo'n grote inbreuk op mijn privacy. En als ik heel eerlijk ben. Als ik van tevoren heb gezien 'dit is een trajectcontrole', waar men ook nummerplaatherkenning doet. Ja, dan rij ik prima de snelheid. Dus het werkt." (P005)

Desalniettemin beargumenteerden twee respondenten dat je niet op een verantwoorde manier kan afwegen of de privacy-risico's van de toepassing, die strikt genomen beperkt zijn, in verhouding staan tot het legitieme doel. Dit omwille van het feit dat nametingen en evaluaties in termen van effectiviteit ontbreken en er onvoldoende met cijfers aangetoond wordt dat de uitrol van het ANPR-netwerk ook voldoet aan het wetshandhavingsdoel waarvoor we dergelijke camera's aan het implementeren zijn.

Overigens werd geconstateerd dat vooral vaste ANPR-camera's enorm veel hits genereren. Van zodra een gescand kenteken in een referentielijst voorkomt, spreken we van een hit. Echter is het ontegensprekelijk zo dat er onvoldoende capaciteit is om daar te allen tijde een operationeel gevolg aan te geven. Derhalve lijkt er vandaag de dag met zeer veel hits niets te worden gedaan. Vanuit een operationele invalshoek toont onderzoek namelijk aan dat er doorgaans geen capaciteit is om te reageren op signaleringen door vaste ANPR-camera's, terwijl er bij geplande politieacties effectief capaciteit is om direct in actie te komen van zodra een hit gegenereerd

wordt (Homburg et al., 2016). Zodoende suggereerde één van de respondenten dat het aantal referentielijsten dient afgestemd te worden op de hoeveelheid capaciteit beschikbaar voor de directe opvolging van hits.

> *"Als er niemand is om te reageren, moet je die referentielijsten uitzetten. Als er heel veel capaciteit is om te reageren, moet je de referentielijsten maximaal openzetten. En wat ik heb geleerd is dat het enige waarvoor de politie ANPR echt goed aan het gebruiken is, zijn specifieke controleacties. Het is vrijdagavond. We gaan op deze plek staan. Hier staat een kentekencamera, en daarachter staat de politie klaar om iedereen bij wie er een hit is meteen aan te houden. Dat werkt heel goed, want dan hebben ze capaciteit en aanbod op elkaar afgestemd." (P001)*

Daarenboven is het ten aanzien van gestolen voertuigen essentieel dat referentielijsten gelimiteerd blijven tot kentekens van voertuigen die slechts enkele dagen geleden gestolen zijn, vermits deze na verloop van tijd niet meer rondrijden, reeds naar het buitenland getransporteerd zijn, of van een valse nummerplaat voorzien zijn (Homburg et al., 2016). Op deze manier dragen beperkingen op de referentielijsten bij aan het minimaliseren van het risico op valse positieven.

Alvorens alsmaar meer dataverzamelingstechnieken in te zetten, dient er dus evenzeer gereflecteerd te worden over de impact die de technologie op onze wetshandhavingsinstanties kan hebben, waarbij de huidige politiecapaciteit in rekening gebracht moet worden.

4.2. Automatische gedragsherkenning

Een tweede toepassing die gedurende de interviews aan bod kwam, had betrekking op intelligente camerasystemen die automatisch abnormaal gedrag beogen te detecteren en te interpreteren. Hierbij dient opgemerkt te worden dat de focus uitsluitend op menselijk gedrag lag en niet op de manier waarop bewegende objecten, zoals voertuigen, zich in de tijd en ruimte verplaatsen. In een wetshandhavingscontext kan signalering gebaseerd zijn op een combinatie van vooraf gedefinieerde gedragingen of kenmerken die wijzen op of wellicht aanleiding geven tot inbraak, gauwdiefstal, rondhangen, rellen, geweld, enzovoort. Derhalve creëren dergelijke camerasystemen ruimte voor proactieve surveillance teneinde criminele feiten of ernstige bedreigingen te voorkomen en de heterdaadkracht te vergroten (Homburg et al., 2016; Vermeulen & Bellanova, 2013). Niettemin rijst zicht de vraag in welke mate de huidige technologie op punt staat om normaal van afwijkend gedrag te onderscheiden.

> *"Laten we het inderdaad even op het allerhoogste niveau mikken en dat is het begrijpen en interpreteren van gedrag. Dat is het moeilijkste te bereiken. Mijn ervaring is dat computers daar nu nog minder goed presteren dan een baby van zes maanden." (P001)*

Bovenstaande citaat vat op een ietwat uitgesproken manier samen hoe de respondenten in termen van accuraatheid het meest sceptisch tegenover deze toepassing stonden. In eerste instantie werd opgemerkt dat het niet evident is afwijkend gedrag van het normale gedrag concreet te definiëren. Wat onder antisociaal gedrag bijvoorbeeld verstaan wordt, is cultureel gebonden, subjectief van aard en zal naargelang de tijd en plaats op een verschillende manier geïnterpreteerd worden (Mabrouk & Zagrouba, 2018; Vermeulen & Bellanova, 2013). Daarbij voegde één van de respondenten toe dat computers vandaag de dag nog evenmin in staat zijn de betekenis van beelden en scènes te achterhalen als in de jaren vijftig.

> *"In het algemeen is mijn conclusie op basis van al dat onderzoek dat wat wij meteen als mens zien, is voor een computer tot nu toe nog niet mogelijk om te zien. Wij snappen de betekenis van gedrag. Wij snappen een scène. (…) Wij zijn vanaf onze geboorte getraind in het interpreteren van beelden." (P001)*

Zo is het voor een camera niet vanzelfsprekend om een loper die op klaarlichte dag aan zijn/haar conditie werkt te differentiëren van een individu die in de late avond in paniek wegloopt van een levensbedreigende situatie. Hoewel de technologie er de afgelopen jaren op vooruitgegaan is, waren de professionele sleutelfiguren het er unaniem over eens dat dergelijke systemen inaccuraat zijn en het aantal valse positieven opmerkelijk aan de hoge kant zouden liggen. Bijgevolg werd de effectiviteit ervan voor de veiligheid in onze samenleving weliswaar betwist, terwijl de ingrijpende consequenties voor de burger erkend werden.

In ieder geval zal de proportie valse positieven mede afhankelijk zijn van wat het systeem exact beoogt te detecteren. Indien dergelijke camera's gelimiteerd blijven tot het detecteren van zeer specifiek en eenvoudig te herkennen gedrag, zoals te lang blijven rondhangen of in de verkeerde richting lopen, kan slechts het gedrag van een beperkte doelgroep tot een signalering leiden. Wanneer het systeem zich verder uitbreidt naar moeilijker te identificeren gedrag die relatief veel voorkomt, zoals opstandig of antisociaal gedrag, zal het gedrag van een opmerkelijk hoger aantal voorbijgangers tot een (vals) alarm leiden. In dit laatste geval is het vrijwel onvermijdelijk dat er meer valse positieven zullen optreden waardoor te veel burgers onterecht door wetshandhavers lastig gevallen worden (Koch et al., 2013). Daarenboven kan het systeem tot verdere discriminatie van bepaalde individuen of sociale groepen leiden. Zo valt er immers

niet uit te sluiten dat afwijkend gedrag die frequent tot een signalering leidt mogelijks voortkomt uit specifieke bewegingen die bijvoorbeeld gerelateerd zijn aan eenieder die een bepaald geloof in de publieke ruimte beoefenen (Vermeulen & Bellanova, 2013). De reële bezorgdheid dat het non-discriminatiebeginsel in het gedrang dreigt te komen, werd door één van de respondenten als volgt beaamd:

> *"Iemand die er uit wordt gepakt met abnormaal gedrag, is iemand die bijvoorbeeld een fysieke stoornis heeft en spastische bewegingen maakt. Het algoritme gaat die eruit pakken als abnormaal gedrag, maar dat is iemand die al kwetsbaar is en vervolgens wordt die aanzien als iemand verdacht." (P007)*

Zodoende kan geconstateerd worden dat het aanwenden van gedragsherkenningssoftware in een wetshandhavingscontext gepercipieerd werd als ingrijpender op de persoonlijke levenssfeer dan het louter hanteren van referentielijsten bij ANPR.

Een andere respondent wees ook jegens deze toepassing op het feit dat dergelijke systemen ertoe kunnen leiden dat burgers hun gedrag gaan aanpassen. Daarbij werd tevens benadrukt dat we als maatschappij eens goed moeten nadenken over hoe ver we in dergelijke toezicht-instrumenten willen gaan.

> *"Het feit dat ik hier struikelde over dat steentje kan misschien geïnterpreteerd worden alsof ik klaar was om iemand een trap in het gezicht te geven, dus laat ik maar eens heel goed gaan opletten. Dan zit je weer in die context waar mensen hun gedrag beïnvloed worden door puur en alleen al de perceptie dat ze in de gaten gehouden worden." (P005)*

> *"En laten we ook niet vergeten dat we niet naar een soort minority report moeten gaan, waarin we puur op basis van wat een camera zegt 'deze persoon zal wel eens agressief kunnen worden'. Ja, ik ben toch echt onschuldig tot mijn schuld bewezen is." (P005)*

Afgezien daarvan dient er vanuit een operationele invalshoek evenzeer opgemerkt te worden dat een inaccuraat systeem de nodige politiecapaciteit en tijd gaat opeisen om de enorme hoeveelheid aan valse alarmen op een gepaste manier te corrigeren.

Rekening houdend met bovenstaande opvattingen, lijkt de conclusie dan ook te luiden dat het op dit moment niet wenselijk en onrealistisch is om intelligente camerasystemen met gedrags-herkenningssoftware operationeel in te zetten voor opdrachten van bestuurlijke of gerechtelijke politie.

4.3. Live gezichtsherkenning

Een laatste cameratoepassing die met de professionele sleutelfiguren besproken werd, had betrekking op live gezichtsherkenning in de publieke ruimte. Gezichtsherkenningsalgoritmen kunnen voor verscheidene toepassingen ontwikkeld worden. In de eerste plaats kan het eenvoudigweg de aanwezigheid van een gezicht in een afbeelding beogen te detecteren, zonder het aan een bepaald individu te koppelen. Een ietwat complexere toepassing houdt de verificatie (1-op-1 vergelijking) in waarbij twee biometrische templates vergeleken worden om na te trekken of het om dezelfde persoon gaat. Voorts kan de technologie evenzeer ingezet worden om individuen in bepaalde categorieën onder te brengen op basis van hun gezichtskenmerken. Overigens slaat de meest controversiële toepassing wellicht op het automatisch vergelijken van een biometrische template met digitale beelden uit een bestaande database (1-op-N vergelijking) teneinde individuen te identificeren (Keymolen et al., 2020; Madiega & Mildebrath, 2021).

LFR behoort tot deze laatste categorie van automatische gezichtsherkenning waarop het huidige onderzoek zich uitsluitend focust. Hierbij dient benadrukt te worden dat het inzetten van LFR gepaard gaat met de verwerking van biometrische persoonsgegevens. Dergelijke gegevens vallen onder de 'bijzondere categorieën' van persoonsgegevens, vermits unieke gezichtskenmerken van de persoon in kwestie vastgelegd worden die tot de kern van het privéleven behoren (Controleorgaan op de Politionele Informatie, 2022b). Dit brengt met zich mee dat dergelijk toezicht veel indringender is dan traditioneel cameratoezicht. Hoewel er in de jaren zeventig al experimenten met gezichtsherkenning plaatsvonden, valt pas sinds enkele jaren te constateren dat er wereldwijd gedebatteerd wordt over het al dan niet operationeel inzetten van LFR voor wetshandhavingsdoeleinden, en de maatschappelijke consequenties die daaruit voortkomen (Buil et al., 2023; Keymolen et al., 2020).

Zowel bij ANPR als bij LFR wordt een technische databank met persoonsgegevens aangelegd en eenieder automatisch gescand vooraleer er enige vermoedens zijn. Desondanks leek het draagvlak bij de professionele sleutelfiguren opvallend groter ten aanzien van ANPR. Een plausibele verklaring hiervoor kan mede gezocht worden in de manier waarop beide beeldtechnologieën zich van elkaar differentiëren in termen van gegevensverwerking en gepercipieerde accuraatheid. In vergelijking met de verwerking van biometrische persoonsgegevens vallen de verwerkte persoonsgegevens (kentekens) bij ANPR-camera's in principe in mindere mate te classificeren als gevoelig van aard. Zo kan het gezicht beschouwd worden als

één van de meest intieme eigenschappen van een persoon. Dit werd door één van de respondenten als volgt beargumenteerd:

> *"Het is mijn biometrische identiteit. Bij al die andere brokjes informatie kan ik nog zeggen 'dat was ik niet'. Dat geldt ook voor kentekens hé. Ik kan jou mijn auto uitlenen. Als mijn kenteken dan in verband gebracht wordt met een crimineel feit, kan ik zeggen 'ja, maar ik zat niet achter het stuur'. Maar bij je gezicht kan dat niet. Dat ben jij. Je gezicht is het meest individuele en persoonlijke wat we hebben." (P001)*

Afgezien daarvan dient de implementatie van ANPR en LFR in een wetshandhavingscontext te resulteren in de opsporing, arrestatie en/of vervolging van een significant aantal geseinde individuen, zonder grote aantallen valse positieven te genereren waarbij onschuldige burgers door de politie lastig gevallen worden (Brey, 2004). Echter waren de respondenten het ten aanzien van LFR unaniem over eens dat er vandaag de dag nog onvoldoende zekerheid over de fiabiliteit bestaat om dergelijke technologieën reeds in de publieke ruimte operationeel in te zetten.

> *"De beelden die je op straat kan capteren, zijn meestal echt niet van die kwaliteit dat je gezichten kan herkennen. (…) Als je gezichtsherkenning wilt doen, moet je de mensen kunnen laten fixeren dat die naar een bepaald punt kijken. (…) Dus als je iemand kan lootsen door zo een queue van security of border control, dan kan je dat doen. Maar niet in de openbare ruimte, omdat mensen daar at random bewegen." (P004)*

In ieder geval werd beaamd dat het een zeer ernstige aantasting van het recht op de eerbiediging van de persoonlijke levenssfeer met zich meebrengt. Hoewel er dankzij de ontwikkeling van zogenaamde deep learning algoritmen opmerkelijke vooruitgangen geboekt zijn (Keymolen et al., 2020), leek LFR in de ogen van de respondenten nog te veel valse positieven op te leveren. Bijgevolg dient in vraag gesteld te worden of de kans op arrestatie van enkele geseinde criminelen wel nog opweegt tegen de schade die het aan onschuldige burgers kan teweegbrengen.

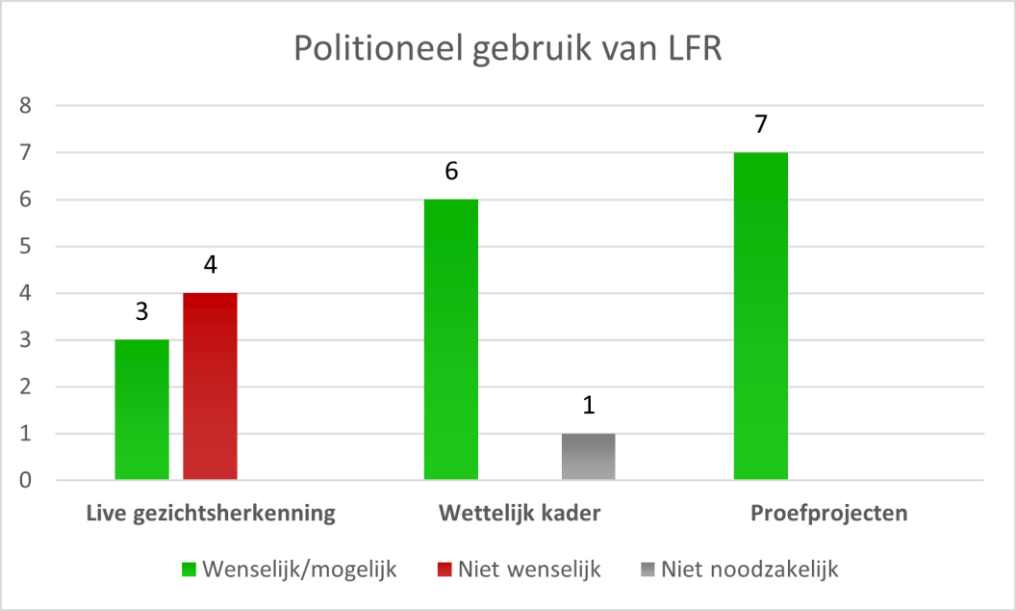
> *"Er wordt nogal dikwijls gegrepen naar slimme camera's, bijvoorbeeld gezichtsherkenning. Blijkt dus dat dat toch nog niet op punt staat hé. Dat daar nog heel wat valse positieven inzitten. En dus vind ik dat men daar toch wel verschrikkelijk goed moet mee opletten." (P002)*

"Je ziet dat ook in toepassingen van facial recognition in Amerika. Dat er toch zeer veel mislagen gebeuren. Soms met dramatische gevolgen. Mensen die, al is het een paar dagen, paar weken of maanden, ten onrechte worden opgesloten op basis van gezichtsherkenning, die dan nadien fout blijkt te zijn hé." (P003)

In deze context verwees één van de respondenten uitdrukkelijk naar het evaluatieonderzoek van Peter Fussey. Deze professor aan de universiteit van Essex voerde in 2019 het eerste en enige onafhankelijke onderzoek naar de werking van LFR bij de London Metropolitan Police (LMP). Hierbij stelde de LMP zelf een effectiviteit van 70% in relatie tot het opsporen van geseinde individuen voorop. Desalniettemin konden de onderzoekers slechts bij 8 van de 42 hits (19%) met absolute zekerheid vaststellen dat de technologie het juist had, terwijl de LMP er in de meeste gevallen van overtuigd was dat het systeem het bij het rechte eind had. Daarenboven kwamen niet te negeren operationele tekortkomingen aan het licht, waaronder inconsistenties in de manier waarop de LMP een hit verifieerde en met individuen omging (Fussey & Murray, 2019). Een andere respondent voegde daaraan toe dat iedere incorrecte match niet alleen gepaard gaat met nefaste gevolgen voor de maatschappij, maar het de politie tevens capaciteit kost om dergelijke misslagen op een gepaste manier te corrigeren.

In wat volgt, wordt getracht de diverse standpunten van professionele sleutelfiguren tegenover het politioneel gebruik van LFR op een overzichtelijke manier weer te geven.

Figuur 2. Live gezichtsherkenning: houding ten aanzien van LFR, de nood aan een wettelijk kader en proefprojecten.



Bovenstaande kolomdiagram dient alleszins met de nodige voorzichtigheid geïnterpreteerd te worden, vermits het bij kwalitatief onderzoek niet vanzelfsprekend is om de verkregen antwoorden uit interviews op een dergelijke manier te presenteren. Zodoende dient opgemerkt te worden dat het merendeel van de respondenten niet zo zwart-wit tegenover de operationele inzet van LFR stond als voorgesteld in de kolomdiagram. Enkele nuances dienen als dusdanig aangebracht te worden.

Rekening houdend met de huidige stand van de technologie leek er eerder unanimiteit te zijn over het feit dat LFR voor opdrachten van bestuurlijke of gerechtelijke politie op dit moment een brug te ver is. Hierbij werd aangegeven dat bevindingen uit onafhankelijke effectiviteits-studies allesbehalve veelbelovend zijn en de verhouding voor het aantal valse positieven te problematisch is. Niettemin staat technologie niet stil en ontwikkelt deze zich continu. Wat toekomstig gebruik betreft, zou er volgens zes van de zeven respondenten eventueel wel ruimte zijn om LFR in bijzondere omstandigheden aan te wenden. Desondanks neigde één respondent eerder in de richting van een permanent verbod op Europees niveau, vermits gezichts-herkenningstoepassingen vertekende resultaten opleveren en tot discriminatie jegens individuen met bepaalde karakteristieken leiden. De bezorgdheid van deze respondent dat het non-discriminatiebeginsel in het gedrang dreigt te komen, lijkt tenslotte volkomen terecht te zijn. Zo heeft onderzoek reeds meermaals aangetoond dat dergelijke technologieën niet vrij zijn van bias ten aanzien van geslacht, etniciteit, leeftijd of personen met een disability. Zodoende lijkt de identificatie jegens mannen met een lichte huidskleur accurater te zijn, terwijl Afro-Amerikaanse vrouwen doorgaans aan een hoger percentage valse positieven onderworpen zijn (Keymolen et al., 2020; Purshouse & Campbell, 2021). Ondanks het feit dat welbepaalde categorieën, zoals gezichten van blanke mannen, in de datasets oververtegenwoordigd zijn, stelde deze respondent vast dat dit een inherent probleem is dat tevens een reflectie van de bestaande maatschappelijke ongelijkheden is.

> *"En je kan wel zeggen van 'we gaan proberen die discriminatie, die bias eruit te halen', maar dat gaat niet lukken. Het is meer een maatschappelijk structureel probleem dat je moet aanpakken. Als je daar iets wil aan doen, moet je eerst etnisch profileren bij de veiligheidsdiensten aanpakken, en discriminatie in het algemeen in de maatschappij." (P007)*

Desalniettemin gingen drie respondenten ervan uit dat zowel de maatschappelijke aanvaard-baarheid als de betrouwbaarheid van gezichtsherkenningstechnologieën op termijn zal toe-nemen, waardoor LFR in een wetshandhavingscontext mogelijks niet tegen te houden valt.

Bijgevolg dient er vandaag de dag voldoende over gereflecteerd te worden teneinde LFR op een degelijke en afdoende manier te reguleren.

> *"Ik zou liever hebben dat men dat gebruik heel goed reguleert. Dat er daar een goeie wet wordt van gemaakt. (...) Ik denk dat veel van dat soort technologie je toch niet kan tegenhouden. (...) Langzaam aan zal het ook een technologie worden die steeds meer geaccepteerd wordt door de maatschappij, en daarom ben ik voorstander van dat eerder goed te gaan reguleren." (P005)*

Daarentegen beargumenteerde een andere respondent dat het tot stand brengen van een wettelijk kader rond LFR niet zozeer als een absolute prioriteit dient opgevat te worden. Zo dient men eerst andere issues aan te pakken die in hoofde gerelateerd zijn aan de politionele informatie-huishouding in België, alvorens nieuwe wetshandhavingstechnologieën toe te passen.

> *"Ik stel vast dat we criminaliteit bestrijden zonder dat dat allemaal bestaat in dit land. Ik stel ook vast dat we veel te weinig capaciteit hebben om met de huidige tools te kunnen doen wat we willen doen. (...) Altijd maar nieuwe technologieën, meer intrusieve technologieën, terwijl dat de basiscorrectheid van de informatie in de politionele databanken, dat daar nog zeer veel problemen zijn. (...) Eerst moet men dat probleem aanpakken en zeker zijn dat de informatie die verwerkt wordt, dat dat juist is. Dat dat vooral correct is en up-to-date gehouden wordt. Want dat is één van de grootste problemen bij de politie. Dat is dat bepaalde politionele vaststellingen niet meer relevant zijn na een bepaalde tijd of onjuist blijken te zijn na een bepaalde tijd, maar dat het allemaal niet gecorrigeerd wordt. Dat zijn dingen die eerst moeten aangepakt worden vooraleer we allerlei nieuwe technologieën ontwikkelen." (P003)*

Derhalve pleit het COC voor een tijdelijk moratorium op het gebruik van LFR tot er voldoende zekerheid bestaat nopens de betrouwbaarheid en accuraatheid, alsook het draagvlak bij de bevolking is toegenomen (Controleorgaan op de Politionele Informatie, 2022a). Hoe dan ook waren de respondenten het er unaniem over eens dat de geïntegreerde politie, onder strikte voorwaarden, effectief zou moeten kunnen experimenteren met gezichtsherkennings-technologie. Hoewel er voor de Nederlandse politie reeds ruimte is om hiermee te experimenteren, is dit in België nog niet toegelaten wegens biometrische persoonsgegevens verwerkt zouden worden waar momenteel geen wettelijke basis voor is. Een wettelijk kader die dergelijke proefprojecten toelaat is dan ook aan de orde.

"We moeten kunnen testen wat de waarde daarvan is. Weten wat de foutenmarge is. En dan een politieke beslissing nemen van 'ja, een foutenmarge van 5%, 10% of 15% aanvaarden we'. En als we dat aanvaarden, hoe gaan we dan omgaan met de mensen die we ten onrechte een uur, twee uur, een dag hebben vastgehouden?" (P003)

Over het algemeen kan geconcludeerd worden dat er unanimiteit was over het feit dat LFR op dit moment niet wenselijk is. Desondanks sluit het merendeel van de respondenten (N=6) toekomstig gebruik door de politie niet volledig uit, mits het alleen maar in uitzonderlijke omstandigheden gedurende een beperkte tijd ingezet wordt, het systeem door een onafhankelijke partij gecertifieerd is, de beelden in geval van no-hits direct verwijderd worden, en het niet in de publieke ruimte als massasurveillance maar slechts op specifieke plaatsen geïmplementeerd wordt, zoals luchthavens, restricted areas, ambassades, enzovoort.

In het kader van de desbetreffende thematiek wordt er sinds 2021 op Europees niveau reeds met de AI Act gepleit voor een principieel verbod op real-time gezichtsherkenning voor opdrachten van bestuurlijke of gerechtelijke politie in de publieke ruimte, met uitzondering van specifieke omstandigheden waarbij een zodanig zwaarwegend, maatschappelijk belang op het spel staat dat de risico's gerelateerd aan fundamentele rechten lijkt te rechtvaardigen. Dergelijke situaties kunnen onder meer betrekking hebben op het gericht zoeken naar potentiële slachtoffers van misdrijven, waaronder vermiste kinderen, alsook het voorkomen van een terroristische aanslag. In ieder geval is er voor de lidstaten van de EU ruimte om te beslissen of ze dergelijke uitzonderingen al dan niet wensen te implementeren in hun nationale wetgeving (Madiega & Mildebrath, 2021).

Tot slot dient opgemerkt te worden dat de aangekaarte (privacy-)bezorgdheden niet uitsluitend aan technologische aspecten te wijten vallen. De mate waarin privacy-risico's gerelateerd aan de vooropgestelde cameratoepassingen al dan niet opwegen tegenover de veiligheidswaarde is onlosmakelijk verbonden aan de sociale context waarin een intrusieve technologie geïmplementeerd wordt. Zodoende gaf één van de respondenten aan dat niet louter de technologie op zich, maar ook degenen die er in de praktijk mee omgaan een significante impact teweegbrengen.

"Als jij het implementeert op zo'n manier dat als het algoritme een alarm geeft, daar iemand zit die naar die persoon gaat op een heel vriendelijke manier. Dat is iets anders dan als daar een intimiderende veiligheidsagent naartoe gaat en op een agressieve manier tegen die persoon praat omdat die denkt dat dat iemand is die verdacht gedrag

vertoont. Dus heel veel heeft eigenlijk niet met de technologie te maken. (…) Want je kan zeggen dat de technologie met bias zit en niet werkt, maar als je dan ziet hoe ermee omgegaan wordt, dan valt het misschien nog wel mee." (P007)

Vermits de behoefte bij wetshandhavers en politici om alsmaar meer privacy-intrusieve wetshandhavingstools operationeel in te zetten steevast lijkt toe te nemen, neemt het belang van een opleiding bij de geïntegreerde politie die voldoende inzet op bewustmaking en expertise jegens AI toepassingen insgelijks toe. Zo dienen de nodige waarborgen genomen te worden om ervoor te zorgen dat wetshandhavers op een adequate, wettelijk conforme manier met de technologie en de data omgaan teneinde privacy-risico's te minimaliseren.

"De opleiding is essentieel. Ook geen blind vertrouwen hebben in systemen. Er goed van doordrongen blijven dat het een aanwijzing is, niet meer dan een aanwijzing. En dat is niet zo gemakkelijk hé. We hebben denk ik een menselijke reflex om de machine te geloven." (P003)

"Dus vóór je überhaupt discussie gaat voeren over meer verzamelen van gegevens, meer inzetten van technologie, denk ik dat het ook heel belangrijk is dat men intern eerst zorgt dat de mensen die daar gebruik van moeten maken en die gegevens mogen verwerken, dat die daar ook klaar voor zijn en dat die goed getraind zijn." (P005)

Dermate dienen wetshandhavers innovatieve beeldtechnologieën te allen tijde op een kritische manier te benaderen, over de nodige kennis en *knowhow* te beschikken om er op een gepaste manier mee om te gaan, en zich voldoende bewust te zijn van de foutenmarges. Zo is het cruciaal dat het vertrouwen bij de geïntegreerde politie in dergelijke technologieën getemperd wordt, zodat burgers die valselijk door het systeem geïdentificeerd worden niet in een ongunstige situatie terechtkomen waar ze niet meer uitkunnen.

5. Conclusie en discussie

In deze concluderende paragrafen wordt aan de hand van zeven semi-gestructureerde interviews met Belgische en Nederlandse professionele sleutelfiguren, aangevuld met reeds bestaande inzichten uit de wetenschappelijk literatuur, getracht een antwoord te bieden op de volgende centrale onderzoeksvraag: *"In welke mate wegen de door professionele sleutelfiguren gepercipieerde ethische problemen rond slimme camera's al dan niet op tegen de beoogde veiligheidswaarde die deze AI gebaseerde technologie voor politioneel gebruik voorziet?"*

Echter is het niet mogelijk een eenduidig antwoord op de gestelde onderzoeksvraag te formuleren, vermits tal van factoren een rol spelen die niet uitsluitend aan het intelligent camerasysteem gerelateerd zijn. Als we de thematiek vanuit een ethisch perspectief beogen onder de loep te nemen, volstaat het namelijk niet om alleen maar te kijken naar de beeldtechnologie en wat het beoogt te detecteren. De mate waarin ethische problemen inherent aan de desbetreffende technologie al dan niet de bovenhand nemen, is immers onlosmakelijk verbonden aan de sociale context waarin het geïmplementeerd wordt. De manier waarop wetshandhavers op een al dan niet betrouwbare, verantwoorde en wettelijk conforme manier met de technologie, de beelden en de data omgaan, zal tevens een onmiskenbare impact op onze grondrechten teweegbrengen.

Zodoende wordt met de eerste deelvraag *"Welke (privacy-)bezorgdheden en bedenkingen kaarten professionele sleutelfiguren jegens het politioneel gebruik van slimme camera's aan?"* stilgestaan bij de exacte problematiek rond intelligent cameratoezicht in het algemeen, alvorens de houding van professionele sleutelfiguren jegens specifieke toepassingen in kaart te brengen.

Zoals uit de wetenschappelijke literatuur naar voren komt, is uit de interviews wederom gebleken dat reële bezorgdheden over slimme camera's verregaander zijn dan louter privacy-kwesties. In eerste instantie beaamden enkele respondenten (N=3) dat de loutere perceptie van bekeken te worden ertoe kan leiden dat burgers geneigd zijn hun gedrag te onderdrukken en aan te passen. Deze impact die de aanwezigheid van cameratoezicht kan teweegbrengen, is in de literatuur een alombekend fenomeen en wordt vooropgesteld als het zogenaamde chilling effect (Milligan, 1999). Daarenboven werd vastgesteld dat er veelal de neiging bestaat om cameratoepassingen voor andere doeleinden in te zetten dan waarvoor ze oorspronkelijk geïmplementeerd werden. Ten aanzien van het initiële doel waarvoor een welbepaalde slimme cameratoepassing ingezet wordt, komen we als maatschappij mogelijks tot de conclusie dat de inmenging op grondrechten gerechtvaardigd is. Echter valt niet uit te sluiten dat deze privacy-

intrusieve beeldtechnologie op termijn ook voor minder ernsitge feiten ingezet zal worden. Deze vaststelling ligt in lijn met voorgaand onderzoek waarbij de gepercipieerde privacy-bezorgdheden niet louter gerelateerd waren aan de geregistreerde data, maar ook aan de doeleinden waarvoor deze initieel verzameld werden (Mariën & Poels, 2020; van Zoonen, 2016). Bovendien beaamt de studie van Brey (2004) dat function creep een inherent probleem aan de implementatie van innovatieve technologieën is.

Overigens trok het merendeel van de respondenten (N=5) de mate waarin overheidsinstanties vandaag de dag op een verantwoorde en wettelijk conforme manier met camerabeelden en geregistreerde data omgaan in twijfel. Hierbij gaven drie respondenten aan onvoldoende geïnformeerd te zijn over de persoonsgegevens die van burgers gecapteerd worden en waarvoor deze precies verwerkt worden, terwijl een andere respondent het eerder problematisch vond dat je niet weet of uw handelingen door een traditionele of slimme camera vastgelegd worden. Zodoende suggereert voorgaand onderzoek dat onwetendheid over wat het systeem exact beoogt te detecteren tot het eerder besproken chilling effect kan leiden vanwege de bezorgdheid om verdacht over te komen (Koch et al., 2013).

Vermits de balans tussen (privacy-)risico's en het leveren van maatschappelijke veiligheid tenslotte sterk afhangt van wat het camerasysteem exact beoogt te detecteren, luidt de tweede deelvraag als volgt: *"In hoeverre worden specifieke toepassinngen van slimme camera's door professionele sleutelfiguren gepercipieerd als al dan niet wenselijk en ethisch verantwoord voor politioneel gebruik?"* Hierbij werd in het bijzonder stilgestaan bij automatische kentekenplaatherkenning, automatische gedragsherkenning en live gezichtsherkenning.

In vergelijking met de andere cameratoepassingen leek het draagvlak bij de professionele sleutelfiguren opmerkelijk groter jegens ANPR. Zo lag het vertrouwen in de accuraatheid van het systeem op autosnelwegen aan de relatief hoge kant. Desalniettemin verschillen ANPR-camera's in grootte en kwaliteit naargelang de kostprijs, wat doorslaggevend is bij de mate waarin slechte weersomstandigheden en lichtcondities al dan niet tot een hoger percentage valse positieven leiden (Tang et al., 2022). Afgezien daarvan werd de aantasting van grondrechten eerder als minimaal gepercipieerd, mits de dataverwerking onderworpen is aan de nodige waarborgen teneinde datalekken te voorkomen. Desondanks stelden enkele professionele sleutelfiguren vast dat er met de uitrol van het ANPR-netwerk in België een aanzienlijke hoeveelheid ANPR-camera's op een relatief korte periode geïmplementeerd werden, terwijl er achteraf op een onvoldoende objectieve manier wordt aangetoond wat we nu als maatschappij

exact gewonnen hebben met het reeds geïmplementeerd ANPR-netwerk teneinde de inmenging op grondrechten te kunnen rechtvaardigen.

In de huidige stand van zaken waren de professionele sleutelfiguren het unaniem over eens dat het politioneel gebruik van intelligente camerasystemen uitgerust met gedragsherkennings-software onwenselijk is. Hoewel de technologie erop vooruitgaat, beargumenteerde één van de respondenten dat het voor een computer vrijwel onmogelijk is om de exacte betekenis van beelden en scènes te achterhalen, laat staan normaal gedrag van het afwijkende te differentiëren. Voorafgaande studies tonen tevens aan dat afwijkend gedrag subjectief van aard en cultureel gebonden is. Zodoende kan antisociaal gedrag naargelang de tijd en plaats op diverse manieren geïnterpreteerd worden (Mabrouk & Zagrouba, 2018; Vermeulen & Bellanova, 2013). Bijgevolg was het in de ogen van de professionele sleutelfiguren klaarblijkelijk dat dergelijke systemen onbetrouwbaar zijn. Volgens de bevraagde actoren zou de implementatie in de praktijk dan ook tot een aanzienlijk aantal valse alarmen leiden, waardoor te veel onschuldige burgers lastig gevallen worden door wetshandhavers. Tevens beweerde één van de respondenten dat dergelijke systemen discriminatoir van aard zijn. Zodoende kan verondersteld worden dat patiënten belast met een bewegingsstoornis en spasticiteit een hoger risico op signalering vormen. Ten aanzien van de Belgische politie benadrukte een andere respondent dat de issues gerelateerd aan de politionele informatiehuishouding allereerst dienen aangepakt te worden, alvorens alsmaar meer innovatieve wetshandhavingstechnologieën te implementeren.

Tot slot werd evenzeer stilgestaan bij wellicht de meest controversiële wetshandhavingstool van de eenentwintigste eeuw, met name live gezichtsherkenning in de publieke ruimte. Vanuit het standpunt van de professionele sleutelfiguren bestaat er vandaag de dag nog onvoldoende zekerheid over de fiabiliteit en is de verhouding voor het aantal valse positieven nog te problematisch om LFR reeds operationeel in te zetten. Deze vaststelling ligt in lijn met het eerste en enige onafhankelijke evaluatieonderzoek van Fussey & Murray (2019) naar de werking van LFR bij de London Metropolitan Police (LMP). Zo konden de onderzoekers slechts bij 8 van de 42 hits (19%) met de hand op het hart zeggen dat het systeem het bij het rechte eind had. Daarenboven beargumenteerde één van de respondenten dat de reeds bestaande maatschappelijke ongelijkheden door de bias in de technologie uitvergroot worden. Voorafgaand onderzoek heeft reeds meermaals aangetoond dat LFR-technologieën discriminatoir van aard zijn op grond van geslacht, etniciteit en leeftijd. Zo blijken Afro-Amerikaanse vrouwen bijvoorbeeld een groter risico op valse identificatie te lopen en worden dermate vaker door de overheid onterecht lastig gevallen (Fontes & Perrone, 2021; Grother et al., 2019; Keymolen et

al., 2020; Purshouse & Campbell, 2021). De noodzakelijkheid van LFR om de criminaliteit in onze hedendaagse samenleving te bestrijden, dient dan ook afdoende in vraag gesteld te worden. Desondanks sloot het merendeel van de respondenten (N=6) toekomstig gebruik van LFR in bijzondere omstandigheden niet uit, mits strikte garanties inzake de inachtneming van de rechten van de mens voorzien zijn.

Concluderend kan gesteld worden dat slimme camera's niet te negeren maatschappelijke consequenties met zich meebrengen, terwijl professionele sleutelfiguren de criminaliteits-preventieve effecten betwisten en duiden op het gebrek aan objectief bewijsmateriaal waarmee de overheid de noodzakelijkheid en effectiviteit aantoont. Desondanks kan het maatschappelijk draagvlak jegens een privacy-intrusieve beeldtechnologie die niet ten volle betrouwbaar is toenemen naargelang de omgeving er op een gepaste, wettelijk conforme manier mee omgaat, zich van de technologische tekortkomingen bewust is en het vertrouwen in het systeem als dusdanig niet absoluut is. In ieder geval dienen alternatieven die minder privacy-intrusief zijn en waarmee hetzelfde legitieme doel gerealiseerd kan worden steeds in overweging gebracht te worden.

Overigens zijn enkele beperkingen aan het huidige onderzoek verbonden waarmee rekening dient gehouden te worden teneinde bovenstaande bevindingen correct te interpreteren. Aan de ene kant zit een belangrijke beperking in de lage generaliseerbaarheid aangezien slechts een beperkt aantal professionele sleutelfiguren (N=7) aan de studie participeerden. Desondanks dient tevens opgemerkt te worden dat er jegens de bevraagde actoren afdoende diversiteit in termen van professionele achtergrond bestond, wat integratie van diverse standpunten en inzichten toeliet. Anderzijds is het evenzeer van belang te onthouden dat het om een perceptieonderzoek gaat. Zodoende vond geen effectiviteitsmeting van de vooropgestelde cameratoepassingen plaats.

Om af te ronden worden enkele praktijkgerichte (beleids-)aanbevelingen vooropgesteld. In de eerste plaats dient opgemerkt te worden dat het maken van een proportionaliteitstoets jegens slimme cameratoepassingen belemmerd wordt vanwege het door de respondenten vastgestelde gebrek aan kennis omtrent de effectieve veiligheidswaarde. Derhalve dienen afdoende onafhankelijke studies uitgevoerd te worden die innovatieve cameratoepassingen op een objectieve manier onder de loep nemen teneinde duidelijkheid te creëren rond de vraag wat we er als maatschappij exact mee gewonnen zijn.

In lijn met de vaststellingen van het COC (2022a) lijken we in België met een tijdelijk moratorium op het gebruik van gezichtsherkenningsalgoritmen gewonnen te zijn tot er meer zekerheid over de fiabiliteit van LFR-technologieën bestaat. Desondanks is het tot stand brengen van een wettelijk kader die de opstart van testomgevingen door de Belgische geïntegreerde politie toelaat van absolute meerwaarde. In een gecontroleerde omgeving en onder strikte voorwaarden dient geëxperimenteerd te kunnen worden om het ontwikkelen, testen en valideren van dergelijke beeldtechnologieën te bevorderen. Na een afdoende aantal testfases te hebben doorlopen, krijgt men dan beter inzicht in de prevalentie van valse positieven, valse negatieven en de mate waarin het systeem aan bias onderworpen is (Controleorgaan op de Politionele Informatie, 2022a). Hoewel het van belang is te debatteren over het foutenpercentage die we bereid zijn te aanvaarden, dient vooral de manier waarop we met valse identificaties gepast omgaan de aandacht op te eisen.

Tevens dient opgemerkt te worden dat de implementatie van proefprojecten rond LFR nieuwe vraagstukken met zich meebrengt. Hoe ga je bijvoorbeeld als wetshandhaver in het kader van dergelijke proefprojecten omgaan met hits? Zal er al dan niet geïntervenieerd worden als een hit betrekking heeft op een voortvluchtige schuldig bevonden aan ernstige criminele feiten? Over dergelijke kwesties zal dan ook uitvoerig gedebatteerd moeten worden.

Daarnaast werd door het COC reeds vastgesteld dat er over het algemeen een reëel expertiseprobleem bij de geïntegreerde politie heerst (Controleorgaan op de Politionele Informatie, 2022a). Indien alsmaar meer innovatieve en privacy-intrusieve toezicht-instrumenten hun intrede in onze maatschappij doen, dient de nodige aandacht naar het optimaliseren van de politieopleiding uit te gaan. Zodoende is het essentieel voldoende in te zetten op bewustmaking en expertise jegens AI toepassingen zodat wetshandhavers over de nodige kennis en *knowhow* beschikken om privacy-intrusieve beeldtechnologieën op een verantwoorde manier operationeel aan te wenden.

Alhoewel het niet zozeer te ontkennen valt dat innovatieve cameratoepassingen een veel-belovende impact op onze wetshandhaving kunnen betekenen, dient te allen tijde voldoende gereflecteerd te worden over de maatschappelijke consequenties en de vraag hoe ver we in dergelijke privacy-intrusieve toezichtsinstrumenten willen gaan. Waar leggen we jegens toekomstige AI-toepassingen voor wetshandhavingsdoeleinden de grens en tot op welke hoogte zijn we als maatschappij nog bereid een deel van onze rechten en vrijheden af te staan ten behoeve van het algemeen belang?

Bibliografie

Adams, W. C. (2015). Conducting semi-structured interviews. In K. A. Newcomer, H. P. Hatry, & J. S. Wholey (Eds.), *Handbook of practical program evaluation* (4e ed., pp. 492-505). Jossey-Bass.

Almeida, D., Shmarko, K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*, 377-387. https://doi.org/10.1007/s43681-021-00077-w

Ashby, M. P. J. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research*, *23*(3), 441-459. https://doi.org/10.1007/s10610-017-9341-6

Beyens, K., Kennes, P., & Tournel, H. (2016). Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview. In T. Decorte, & D. Zaitch (Reds.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 187-220). Acco.

Brey, P. (2004). Ethical aspects of facial recognition systems in public places. *Journal of Information, Communication & Ethics in Society*, *2*(2), 97-109. https://doi.org/10.1108/14779960480000246

Bu, F., Wang, N., Jiang, B., & Liang, H. (2020). "Privacy by Design" implementation: Information system engineers' perspective. *International Journal of Information Management*, *53*(5). https://doi.org/10.1016/j.ijinfomgt.2020.102124

Buil, M., Knops, K., & Zoetekouw, M. (2023). *Inzetkader gezichtsherkenningstechnologie politie: Een eerste kader ter toetsing van operationele inzetten*. Rijksoverheid. https://www.rijksoverheid.nl/documenten/rapporten/2023/02/24/tk-bijlage-inzetkader-gezichtsherkenningstechnologie-politie

Caplan, J. M., Kennedy, L. W., & Petrossian, G. (2011). Police-monitored CCTV cameras in Newark, NJ: A quasi-experimental test of crime deterrence. *Journal of Experimental Criminology*, *7*(3), 255-274. https://doi.org/10.1007/s11292-011-9125-9

Cerezo, A. (2013). CCTV and crime displacement: A quasi-experimental evaluation. *European Journal of Criminology*, *10*(2), 222-236. https://doi.org/10.1177/1477370812468379

Controleorgaan op de Politionele Informatie. (2019). *Tussentijds rapport met corrigerende maatregel betreffende de visitatie bij de federale politie van de luchthaven Zaventem door het controleorgaan op de politionele informatie met betrekking tot het gebruik van gezichtsherkenning op de nationale luchthaven van Zaventem* (DIO19005).

https://www.controleorgaan.be/files/DIO19005_Onderzoek_LPABRUNAT_Gezichtsherkenning_Publiek_N.PDF

Controleorgaan op de Politionele Informatie. (2022a). *Advies betreffende een voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen* (DA210029). https://www.controleorgaan.be/files/DA210029_Advies_N.pdf

Controleorgaan op de Politionele Informatie. (2022b). *Toezichtrapport van het controleorgaan op de politionele informatie met betrekking tot het gebruik van CLEARVIEW AI door de geïntegreerde politie* (DIO21006). https://www.controleorgaan.be/files/DIO21006_Toezichtrapport_Clearview_N_00050443.pdf

Costin, A. (2016). Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. *Proceedings of the 6th international workshop on trustworthy embedded devices* (pp. 45-54). Association for Computing Machinery. https://doi.org/10.1145/2995289.2995290

Cup, F. (2022, 10 maart). Belgische politie gebruikte omstreden software voor gezichtsherkenning. *Business AM*. https://businessam.be/belgische-politie-gebruikte-omstreden-software-voor-gezichtsherkenning/

Custers, B., & Vergouw, B. (2015). Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies. *Computer Law and Security Review*, *31*(4), 518-526. https://doi.org/10.1016/j.clsr.2015.05.005

Dearnley, C. (2005). A reflection on the use of semi-structured interviews. *Nurse Researcher*, *13*(1), 19-28. https://doi.org/10.7748/nr2005.07.13.1.19.c5997

Decorte, T. (2016). Kwalitatieve data-analyse. In T. Decorte, & D. Zaitch (Reds.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 463-510). Acco.

Dekker, L. (2015). Crime displacement through formal surveillance. *Forensic Research & Criminology International Journal*, *1*(3), 70-76. https://doi.org/10.15406/frcij.2015.01.00012

De Pauw, E., Deprins, F., Hardyns, W., Mortelé, J., & Vermeersch, H. (2013). *Cameratoezicht in de openbare ruimte : Ook wie weg is, is gezien?* Maklu.

EU Fundamental Rights Agency. (2019). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement* [Research report]. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

European Group on Ethics in Science and New Technologies. (2014). *Ethics of security and surveillance technologies* (Opinion no. 28). https://doi.org/10.2796/22379

Ferenbok, J. & Clement, A. (2011). Hidden changes: From CCTV to 'smart' video surveillance. In A. Doyle, R. Lippert, & D. Lyon (Eds.), *Eyes everywhere: The global growth of camera surveillance* (pp. 218-234). Devon Willan Publishing.

Flick, U. (2004). Triangulation in qualitative research. In U. Flick, E. von Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (B. Jenner, Trans.; pp. 178-183). Sage Publications. (Original source published in 2000)

Flight, S. (2012). *Agressiedetectie in Amsterdam Noord*. DSP-groep. https://www.dsp-groep.eu/wp-content/uploads/18sfnoorda_dsp-roep-rapport-agressiedetectie-amsterdam-noord.pdf

Flight, S. (2016). Politie en beeldtechnologie: Gebruik, opbrengsten en uitdagingen. *Justitiële verkenningen*, *42*(3), 68-94. https://doi.org/10.5553/JV/016758502015041002006

Fontes, C., & Perrone, C. (2021). *Ethics of surveillance: Harnessing the use of live facial recognition technologies in public spaces for law enforcement*. Institute for Ethics in Artificial Intelligence. https://ieai.mcts.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf

Fussey, P., & Murray, D. (2019). *Independent report on the London Metropolitan Police service's trial of live facial recognition technology*. Economic & Social Research Council. https://repository.essex.ac.uk/24946/

Gai, A., Azam, S., Shanmugam, B., Jonkman, M., & De Boer, F. (2018). Categorisation of security threats for smart home appliances. *Proceedings of the 2018 international conference on computer communication and informatics* (pp. 1-5). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICCCI.2018.8441213

Gerell, M. (2016). Hot spot policing with actively monitored CCTV cameras: Does it reduce assaults in public places? *International Criminal Justice Review*, *26*(2), 187-201. https://doi.org/10.1177/1057567716639098

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic effects* (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Gupta, S., Singh, R. S., & Mandoria, H. L. (2020). A review paper on automatic number plate recognition system. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(3), 955-966. https://doi.org/10.32628/CSEIT2063208

Hardyns, W. (2019). *Onderzoeksontwerp in de criminologie* [Ongepubliceerde cursus]. Institute for International Research on Criminal Policy.

Held, C., Krumm, J., Markel, P., & Schenke, R. P. (2012). Intelligent video surveillance. *Computer*, *45*(3), 83-84. https://doi.org/10.1109/MC.2012.97

Hidayat, F., Hamami, F., Dahlan, I. A., Supangkat, S. H., Fadillah, A., & Hidayatuloh, A. (2020). Real time video analytics based on deep learning and big data for smart station. *Journal of Physics: Conference Series*, *1577*. https://doi.org/10.1088/1742-6596/1577/1/012019

Homburg, G. H. J., Schreijenberg, A., van den Tillaart, J., & Bleeker, Y. (2016). *ANPR: Toepassingen en ontwikkelingen*. Regioplan Beleidsonderzoek. https://repository.wodc.nl/handle/20.500.12832/2079

Hong, Y., Tsang, K. K., & Liu, D. (2019). Conclusion: Research dilemma and feasible strategies. In K. K. Tsang, D. Liu, & Y. Hong (Eds.), *Challenges and opportunities in qualitative research: Sharing young scholar's experiences* (p. 155) [E-book]. Springer Nature Singapore. https://doi.org/10.1007/978-981-13-5811-1

Hopf, C. (2004). Research ethics and qualitative research. In U. Flick, E. von Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (B. Jenner, Trans.; pp. 334-339). Sage Publications. (Original source published in 2000)

James, N., & Busher, H. (2016). Online interviewing. In D. Silverman (Ed.), *Qualitative research* (4e ed., pp. 246-260). Sage Publications.

Keymolen, E., Noorman, M., van der Sloot, B., Cuijpers, C., Koops, B.-J., & Zhao, B. (2020). *Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*. Wetenschappelijk Onderzoek- en Documentatiecentrum. https://research.tilburguniversity.edu/en/projects/een-verkenning-van-gezichtsherkenning-en-privacyrisicos-in-horizo

Khan, P. W., Byun, Y.-C., & Park, N. (2020). A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics*, *9*(3). https://doi.org/10.3390/electronics9030484

Koch, H., Matzner, T., & Krumm, J. (2013). Privacy enhancing of smart CCTV and its ethical and legal problems. *European Journal of Law and Technology*, *4*(2). https://ejlt.org/index.php/ejlt/article/view/185/386

Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, *55*(4). https://doi.org/10.1016/j.scs.2020.102023

Lee, J. C., Kim, J. H., & Seo, J. T. (2019). Cyber attack scenarios on smart city and their ripple effects. *Proceedings of the 2019 international conference on platform technology and service* (pp. 1-5). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/PlatCon.2019.8669431

Mabrouk, A. B., & Zagrouba, E. (2018). Abnormal behavior recognition for intelligent video surveillance systems: A review. *Expert Systems with Applications*, *91*, 480-491. https://doi.org/10.1016/j.eswa.2017.09.029

Madiega, T., & Mildebrath, H. (2021). *Regulating facial recognition in the EU*. European Parliamentary Research Service. https://doi.org/10.2861/140928

Maesschalck, J. (2016). Methodologische kwaliteit in het kwalitatief onderzoek. In T. Decorte, & D. Zaitch (Reds.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 131-160). Acco.

Magnusson, E. (2015). *Doing interview-based qualitative research: A learner's guide* [E-book]. Cambridge University Press. https://doi.org/10.1017/CBO9781107449893

Mariën, S., & Poels, K. (2020). Een explorerend onderzoek naar de privacybezorgdheden en participatiebehoeften van inwoners van de smart city Antwerpen. *Tijdschrift voor Communicatiewetenschap*, *48*(1), 4-24. https://doi.org/10.5117/2020.048.001.002

Melis, J. (2021). *De effectiviteit van CCTV betreffende de preventie en ophelderingsgraad van criminaliteit* [Ongepubliceerde bachelorscriptie]. Universiteit Gent.

Merkens, H. (2004). Selection procedures, sampling, case construction. In U. Flick, E. von Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (B. Jenner, Trans.; pp. 165-171). Sage Publications. (Original source published in 2000)

Milligan, C. S. (1999). Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal*, *9*(1), 295-333. https://heinonline.org/HOL/Page?handle=hein.journals/scid9&div=7&g_sent=1&casa_token=&collection=journals

Möllers, N., & Hälterlein, J. (2012). Privacy issues in public discourse: The case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research*, *26*(1-2), 57-70. https://doi.org/10.1080/13511610.2013.723396

Morgan, A., & Dowling, C. (2019). Does CCTV help police solve crime? *Trends & issues in crime and criminal justice*, (576). https://www.aic.gov.au/publications/tandi/tandi576

Mortelmans, D. (2016). Het kwalitatief onderzoeksdesign. In T. Decorte, & D. Zaitch (Reds.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 81-128). Acco.

Mortelmans, D. (2017). *Kwalitatieve analyse met NVivo* (2e dr.). Acco.

Mortelmans, D. (2020). *Handboek kwalitatieve onderzoeksmethoden* (3e ed.). Acco.

Perego, A. (2021). A new age of surveillance: Facial recognition in policing and why it should be abolished. *Cardozo Journal of Equal Rights and Social Justice*, *28*(1), 79-104. https://heinonline.org/HOL/Print?collection=journals&handle=hein.journals/cardw28&id=89

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, *18*(1), 135-159. https://doi.org/10.1111/1745-9133.12419

Purshouse, J., & Campbell, L. (2021). Automated facial recognition and policing: A bridge too far? *Legal Studies*, *42*(2), 1-19. https://doi.org/10.1017/lst.2021.22

Rahman, M. F. B. A. (2017). *Smart CCTVS for secure cities: Potentials and challenges*. S. Rajaratnam School of International Studies. https://think-asia.org/handle/11540/7752

Rooseleers, L., & Maesschalck, J. (2021). Digitalisering in de lokale politie in Vlaanderen en Brussel: Waar staan we? *Panopticon*, *42*(5), 419-438. https://www.researchgate.net/publication/355585410_Digitalisering_in_de_lokale_politie_in_Vlaanderen_en_Brussel_Waar_staan_we

Safdar, M., Ullah, F., Khan, I., Ullah, F., & Khan, I. A. (2016). Function creep in surveillance techniques. *International Journal of Scientific Research in Science, Engineering and Technology*, *2*(2), 983-988. https://www.academia.edu/25501943/Function_Creep_in_Surveillance_Techniques

Schreijenberg, A., & Homburg, G. H. J. (2010). *Evaluatie cameratoezicht op openbare plaatsen: Viermeting*. Regioplan Beleidsonderzoek. https://www.publicspaceinfo.nl/media/uploads/files/REGIOBELEI_2010_0001.pdf

Schuilenburg, M., Besseling, B., & Uitendaal, F. (2017). Vertrouwen in de politie: Empirisch onderzoek naar de beleving van vertrouwen in de Rotterdamse wijk Bloemhof. *Justitiële verkenningen*, *43*(4), 47-63. https://doi.org/10.5553/JV/016758502017043004005

Steinke, I. (2004). Quality criteria in qualitative research. In U. Flick, E. von Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (B. Jenner, Trans.; pp. 184-190). Sage Publications. (Original source published in 2000)

Tang, J., Wan, L., Schooling, J., Zhao, P., Chen, J., & Wei, S. (2022). Automatic number plate recognition (ANPR) in smart cities: A systematic review on technological advancements and application cases. *Cities*, *129*(October 2022). https://doi.org/10.1016/j.cities.2022.103833

van Berkel, J. J., Pool, R. L. D., Harbers, M., Oerlemans, J. J., Bargh, M. S., & van den Braak, S. W. (2017). *(Verkeerd) verbonden in een slimme samenleving*. Wetenschappelijk Onderzoek- en Documentatiecentrum. https://repository.wodc.nl/handle/20.500.12832/186

Van Brakel, R. (2015). Iedereen verdacht? De effectiviteit en impact van het gebruik van preëmptieve surveillance voor publieke veiligheid. *Orde van de Dag*, *March*(69), 35-42. https://www.researchgate.net/publication/275770776_Iedereen_verdacht_De_effectiviteit_en_impact_van_het_gebruik_van_preemptieve_surveillance_voor_publieke_veiligheid

Vander Laenen, F., & O'Gorman, A. (2016). Ethische aspecten van het kwalitatief onderzoek. In T. Decorte, & D. Zaitch (Reds.), *Kwalitatieve methoden en technieken in de criminologie* (3e ed., pp. 555-585). Acco.

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480. https://doi.org/10.1016/j.giq.2016.06.004

Vermeulen, M., & Bellanova, R. (2013). European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination? *Security and Human Rights*, *23*(4), 297-311. https://doi.org/10.1163/18750230-99900034

Waples, S., Gill, M., & Fisher, P. (2009). Does CCTV displace crime? *Criminology & Criminal Justice*, *9*(2), 207-224. https://doi.org/10.1177/1748895809102554

Wolff, J. (2021). How is technology changing the world, and how should the world change technology? *Global Perspectives*, *2*(1). https://doi.org/10.1525/gp.2021.27353

Perstekst

Slimme camera's onder de loep: valt het Big Brother-gevoel nog te verantwoorden of niet?

Camera's die in één oogopslag uw nummerplaat, gezicht of zelfs gedrag beogen te detecteren. Werken ze écht? Of komen onze rechten en vrijheden voor niets in het gedrang? Een thesisonderzoek aan de Universiteit Gent evalueerde de perceptie rond het gebruik van deze camera's door de politie. Hiervoor vonden zeven (online) semi-gestructureerde interviews met experten plaats. De conclusie luidde dat deze camera's een enorme impact op onze samenleving hebben en er duidelijk veel meer op het spel staat dan alleen maar onze privacy. Toch is het van belang om alle privacy-risico's te bekijken in de sociale context waarin ze zich voordoen.

Nummerplaatherkenning (ANPR)

In vergelijking met de andere cameratoepassingen werd ANPR het meest positief geëvalueerd. Het vertrouwen in de accuraatheid van deze camera's op autosnelwegen lag relatief hoog, terwijl het verlies aan privacy eerder als minimaal aanschouwd werd. Toch heerste er onder de experten een groot gemis aan wetenschappelijk bewijs die duidelijk de noodzakelijkheid en effectiviteit van ANPR-camera's aantoont. Wanneer krijgen we eens objectieve cijfers voorgeschoteld waarmee de overheid daadwerkelijk aantoont wat we nu als maatschappij precies gewonnen hebben met de uitrol van het ANPR-cameranetwerk? Dit gebrek aan objectief bewijs brengt in principe met zich mee dat eventuele inbreuken op onze rechten en vrijheden, hoe minimaal ze ook mogen zijn, niet op een wetenschappelijk onderbouwde manier te rechtvaardigen vallen.

Gedragsherkenning

Daartegenover is het volgens experten glashelder dat camerasystemen met gedragsherkenning compleet onbetrouwbaar zijn. Computers lijken nog evenmin in staat te zijn de betekenis van beelden te achterhalen als normaal van afwijkend gedrag te onderscheiden. Camera's die op punt staan een onderscheid te maken tussen een loper die op klaarlichte dag aan zijn conditie werkt en iemand die in de late avond in paniek van een levensbedreigende situatie wegloopt, lijkt nog een absolute utopie te zijn. Aldus brengt zo'n inaccurate cameratoepassing enorm veel valse alarmen met zich, wat niet alleen een inmenging in het privéleven van onschuldige burgers impliceert maar ook politiecapaciteit opeist om die valse alarmen te corrigeren.

Live gezichtsherkenning

Wat het gebruik van gezichtsherkenning op openbare plaatsen betreft, leek het in de ogen van experten nog niet verantwoord om dit vandaag de dag in te zetten. Dit om de eenvoudige reden dat er nog onvoldoende zekerheid bestaat over de betrouwbaarheid, waarbij de kans dat onschuldige burgers vals beschuldigd worden reëel is. Deze bezorgdheid werd in 2019 al bevestigd door het eerste onafhankelijke onderzoek van surveillance-expert Peter Fussey naar de werking van gezichtsherkenningstechnologie bij de politiedienst van London. Bij slechts 8 van de 42 hits kon met absolute zekerheid gezegd worden dat het om een correcte match ging. Meer nog, gezichtsherkenningstechnologieën kunnen leiden tot verdere discriminatie op grond van geslacht, leeftijd en etniciteit. Zo lijkt de foutenmarge opvallend hoger te liggen bij personen met een donkere huidskleur, waardoor zij als onschuldige burger een hoger risico lopen om door de politie lastig gevallen te worden.

Zoals eerder gezegd, kunnen de privacy-risico's niet los gezien worden van de context. De actoren die met de technologie omgaan, spelen een belangrijke rol in dit hele verhaal. Zo is een camerasysteem mogelijks niet vrij van bias, maar als je ziet dat de politie over de nodige expertise beschikt en op een zorgvuldige en bedachtzame manier met de technologie omgaat, vallen de privacy-risico's in de praktijk misschien nog goed mee.

What's next?

Het onderzoek beoogde ook enkele aanbevelingen te formuleren. In de eerste plaats is er nood aan onafhankelijke studies die slimme cameratoepassingen op een objectieve manier onder de loep nemen. Hoewel we in België gebaat zijn met een tijdelijk moratorium op het gebruik van gezichtsherkenningsalgoritmen, is het toch van belang dat de politie de technologie in een gecontroleerde omgeving kan testen. Enkel op deze manier krijgen we inzicht in de foutenmarge en de mate waarin het systeem vertekende resultaten oplevert. Tot slot moet de politieopleiding ervoor zorgen dat wetshandhavers ten aanzien van AI toepassingen over de nodige kennis en *knowhow* beschikken, zodat er op een verantwoorde manier met slimme camera's omgegaan wordt.

Bijlagen

Bijlage 1: Data Management Plan

Thesis - Smart CCTV en wetshandhaving

A Data Management Plan created using DMPonline.be

Creator: Jayson Melis

Affiliation: Ghent University (UGent - UZ Gent)

Template: Faculty of Law & Criminology DMP +

ID: 197459

Start date: 01-09-2022

End date: 15-05-2023

Project abstract:

This qualitative research project aims to critically reflect on the use of smart CCTV by the police, focusing on perceived ethical issues primarily. In particular, semi-structured interviews with key informants will take place in order to discuss in depth specific concerns regarding this advanced technology, and the extent to which the use for law enforcement purposes is desirable and ethically justified from their point of view.

Last modified: 21-04-2023

Thesis - Smart CCTV en wetshandhaving
Law & Criminology DMP +

Administrative Data

Date of first version

March 2, 2023

Date of last update

April 21, 2023

1. Data Collection

1.1 What data will you collect or create?

Firstly, **audio recordings** will be made during the interviews with the consent of each participant (type of file format: AAC). In order to analyze the collected data in an efficient way, the audio recordings will be transcribed afterwards and saved as **text documents** (type of file format: DOCX). Eventually, the researcher chose to work with the software program NVivo to organize the data and facilitate the analysis, so a **NVivo file** will also be created (type of file format: NVP).

No third-party datasets will be reused.

1.2 How will the data be collected or created?

The audio recordings will be obtained by conducting (online) semi-structured interviews with key informants who can provide the necessary information to answer the research questions. The quality of the **recording equipment** will be **tested in advance** by the researcher himself.

After each interview, the audio recording will be transcribed into a written version. Afterwards, the transcripts will be coded and analyzed using NVivo.

All collected research material will be safely stored on the **central disk space** provided by Ghent University. We can assume that data stored on that infrastructure are properly secured under the responsibility of the educational institutions.

Regarding the structure and naming system for the files and folders, all files will be stored under the folder named 'Masterproef' where each Word document and audio recording is given a **neutral file name**, so that they cannot be linked to the identity of a particular respondent.

The audio recordings will be named ‘Audio Record_’ combined with the pseudonym given to the respondent (e.g. Audio Record_P001).

The transcription documents will be named ‘Transcript_’ combined with the pseudonym given to the respondent (e.g. Transcript_P001).

2. Data Documentation and Metadata

2.1 How will you document the data?

The collected data will be analyzed in NVivo.

After all, the data will eventually be deleted, meaning that third-parties will not be able to use the collected data. However, the data and the research findings will be brought together in a **master's thesis**.

3. Ethics, Legal Issues and Confidentiality

3.1 How will you manage ethics? Choose one of the options from the dropdown menu and briefly motivate your choice in the 'Comment' box below.

- Approval by the Ethical Committee of the Faculty is neither required nor desirable

Participants are not asked about personal information or experiences that could be considered sensitive in nature or that could cause a chance of emotional, physical, material or legal harm. They participate purely as experts to discuss the ethical issues associated with the implementation of smart CCTV for law enforcement purposes, and to argue whether or not the use of it by the police is ethically justified.

Potential participants are sufficiently informed about the purpose of the research project and the role they would play in it, so that they can make a voluntary decision whether or not to participate. The target group of potential participants does not belong to a vulnerable group. Each of them is in principle capable of freely giving informed consent.

3.2 How will you manage any confidentiality issues?

The personal data that is necessary to obtain the objective of the research project is kept to an absolute minimum. The participants will give their **name** and some information about their **professional background**. However, from the transcribing of the interviews, the identity of each participant will be protected by replacing real names with **pseudonyms**. This makes it impossible for third-parties to associate the collected data with a specific individual.

At the beginning of the interview, an **informed consent form** is provided that will be signed by the participant. In this way, the participant indicates that he/she is sufficiently informed about the research project whereby permission for the use of the recording equipment is also given.

Regarding the storage of data, **neutral file names** are given in order to protect the identity of participants. In addition, the data will be safely stored on the personal disk space **(H drive)** provided by Ghent University.

3.3 How will you manage intellectual property rights issues?

Before conducting (online) semi-structured interviews, a narrative review took place in order to gain insight into the ethical issues related to the use of smart CCTV for law enforcement purposes. This implies that a reference list will be included in the master's thesis and appropriate references will be made to the literature used.

The research material from the interviews are collected exclusively for the purpose of the current research project and will not be shared. At the end of the research project, all the data collected from the interviews will be safely stored for a period of five years and deleted afterwards.

4. Data Storage and Backup during Research

4.1 How will you store and backup data during research?

The data will be stored on the **H drive** provided by Ghent University. This personal disk space is accessible via Athena and secured by a personal login and password.

The risk of data loss is reduced by using this central disk space because the files can be accessed on any computer connected to the UGent network.

4.2 How will you ensure that stored data are secure?

In order to access the data stored on the personal H drive, it is required to give in my own **personal login** and **password** via Athena. No third-parties have knowledge of these login details.

5. Data Selection and Preservation after Research

5.1 Which data should be retained for preservation and/or sharing?

All the collected data from the interviews will be retained for a period of five years, which is in accordance with the Ghent University's RDM policy framework. This way, my research can be verified and reproduced.

5.2 What is the long-term preservation plan for the selected datasets?

The data will be safely stored on the **central disk space** provided by Ghent University. We can assume that data stored on that infrastructure are properly secured under the responsibility of the educational institutions.

6. Data Sharing

6.1 Are any restrictions on data sharing required?

Under no circumstances will the collected data be shared.

There is only the possibility for the participants to read the transcript of their own interview afterwards. This way they can make adjustments or even withdraw statements if desired.

6.2 How will you share data selected for sharing?

Not applicable.

7. Responsibilities and Resources

7.1 Who will be responsible for data management?

I, Jayson Melis, will be responsible for the data management.

Questions or ambiguities related to data management will be discussed with the supervisor of the master's thesis.

7.2 Will you need additional resources to implement your DMP?

No.

Thesis - Smart CCTV en wetshandhaving
GDPR Record

Collection and processing of personal data

1. Are you collecting or processing personal data?

- Yes

In the context of this master's thesis, (online) semi-structured interviews will be conducted with key informants who have sufficient knowledge of the current research topic and can therefore provide relevant and reliable information to answer the research questions.

Each participant will be asked to give their name and some information about their professional background. Contact details (e.g. mail adress, telephone number) will also be kept in order to communicate with participants. In addition, a recording of the interview is made.

2. In what format are you collecting or processing the personal data?

- Digital
- On paper

Digital:

- personal data will be collected via audio recording equipment.

On paper:

- at the beginning of each interview, an informed consent form will be signed in which participants fill in their name
- a list with contact details will also be kept in order to communicate with the participants.

3. Are you collecting or processing primary personal data and/or secondary personal data?

- Primary personal data

The data will be collected directly from the research subjects via (online) semi-structured interviews which will also be recorded exclusively for the purpose of the current research project.
No personal data that was collected previously will be reused.

4. If you are processing secondary personal data, will you inform the persons whose personal data are being processed or have they already been informed?

Not applicable.

5. If no, explain why it is impossible or why it would take a disproportionate effort to inform the persons whose personal data are being processed.

Not applicable.

6. How will the personal data be processed?

- Pseudonymised (explain below)

From the transcribing of the interviews, real names will be replaced by **pseudonyms** in order to respect the privacy and protect the identity of the participants. This makes it impossible for third-parties to associate the collected data with a specific individual.

7. If you are going to process personal data in a pseudonymised form, describe the method of pseudonymisation, where you will keep the key, and who has access to it.

From the transcribing of the interviews, directly identifiable data (e.g. real names) will be replaced by **pseudonyms** in order to respect the privacy and protect the identity of the participants. This makes it impossible for third-parties to associate the collected data with a specific individual.

The encrypted **key file** will be safely stored in a separate folder on the H drive provided by Ghent University, which can only be accessed by the researcher himself by entering a personal login and password via Athena. No third-parties have knowledge of these login details.

When the master's thesis is finished and scored sufficiently, all the collected data from the interviews (including the key file) will be safely stored for a period of five years in order to create the possibility to verify and reproduce my research. After this retention period, all the data will be deleted.

Categories of personal data & data subjects

8. Are you collecting/processing any of the following special categories of data?

- None of the above

9. Which other categories of personal data are you collecting/processing?

- Identification data (names, titles, addresses, phone numbers, passport numbers, IP addresses, cookies, electronic location data (GPS, mobile phone)…)
- Occupation and profession
- Audio and video recordings

10. Whose personal data are you collecting/processing?

- Others (please specify below)

Key informants who have sufficient knowledge of the current research topic and can therefore provide relevant and reliable information to answer the research questions.

11. Will your research be seriously hampered if the persons whose personal data are being collected/processed exercise their right to access, to rectification, to restriction of processing, to be forgotten, to data portability and/or to object?

- No

12. If yes, please justify the need to deviate from one or more of the rights mentioned in question 11. A justification is required for each deviation.

Not applicable.

Purpose(s) of the processing

13. What is/are the purpose(s) of the personal data processing?

The personal data (e.g. professional background) collected from the interviews will be processed in a master's thesis about the use of smart CCTV for law enforcement purposes.

Contact details of participants will only be used to contact and communicate with the research subjects. This personal data will not be mentioned in the master's thesis and will be deleted afterwards.

The possibility of associating data with a specific individual will be avoided at all times.

14. What is the legal ground for the processing? If the data are being processed for multiple purposes, you must describe the legal ground for each purpose.

- The individuals participating in the research have freely given their explicit consent for the processing of their personal data for one or more specific purposes.

15. If you are processing special categories of personal data (see question 8), on which exception is this based?

Not applicable.

GDPR responsibility

16. Which institution(s) is/are involved in the research?

- Ghent University

17. Is there another university, hospital, research institute or partner involved in the research (besides Ghent University and/or Ghent University Hospital)?

- No

18. Please specify who determines the purposes ('why') and the means ('how') of the research.

- This is determined within Ghent University: UGent is the data controller.

Data transfers & categories of recipients

19. Are you disclosing/sharing/transferring personal data beyond your project team, either with recipients in UGent or UZ Gent, or with external recipients during or after your research?

- No

20. If yes, to or with which categories of recipients are the personal data being disclosed/shared/transferred?

Not applicable.

21. If yes, where are the personal data being disclosed/shared/transferred to?

Not applicable.

22. What is/are the purpose(s) of the data transfer?

Not applicable.

23. What is the legal ground for the data transfer? If there will be multiple data transfers, you need to indicate the legal ground for each data transfer.

Not applicable.

Retention period

24. What is the envisaged retention period for the different categories of personal data? Please motivate.

In accordance with the Ghent University's RDM policy framework, the envisaged retention period of the personal data is five years after my master's thesis is finished and scored sufficiently. This way, my research can be verified and reproduced.

To protect the confidentiality of the data during this retention period, the audio recordings, transcripts and NVivo file will be safely stored on the H drive provided by Ghent University, which is only accessible to the researcher by entering a personal login and password via Athena.

Risk analysis

25. To analyse the possible risks associated with the processing of personal data, please tick the boxes that apply to this research.

Not applicable.

26. Does the research constitute a probable high-risk processing? If you ticked two or more boxes in question 25, the answer is 'yes'.

- No

Security measures

27. What technical and organisational security measures are in place to protect personal data?

- I hereby confirm that I carry out my research in accordance with the guidelines on information security of UGent and/or UZ Gent.

28. If you have motivated the need to deviate from one or more of the rights of the persons whose personal data you are collecting/processing in question 11 and 12, please describe which safeguards are put in place to protect their rights and freedoms.

Not applicable.

Bijlage 2: Informed Consent

FACULTEIT
RECHT EN CRIMINOLOGIE

FORMULIER 'INFORMED CONSENT'

Ik ondergetekende, …… , verklaar hierbij dat ik als participant aan het onderzoek naar het gebruik van slimme camera's door de politie, uitgevoerd in het kader van een masterproef aan de faculteit Recht en Criminologie van de Universiteit Gent:

(1) de informatiebrief heb gelezen en in kennis ben gesteld van de aard van de vragen en het doel van het onderzoek;
(2) op elk ogenblik de mogelijkheid heb om bijkomende informatie te verkrijgen;
(3) totaal vrijwillig deelneem aan het onderzoek;
(4) de toestemming geef aan de onderzoeker om mijn resultaten op anonieme wijze te bewaren, te verwerken en te rapporteren;
(5) de toestemming geef aan de onderzoeker om het interview door middel van opname-apparatuur te laten opnemen;
(6) op de hoogte ben van de mogelijkheid om mijn deelname aan het onderzoek op ieder moment stop te zetten;
(7) ervan op de hoogte ben dat ik een samenvatting van de onderzoeksbevindingen kan krijgen.

Gelezen en goedgekeurd te *(plaats)* ……

op datum van ……..

Handtekening van participant: ……..

UNIVERSITEIT
GENT

Bijlage 3: Informatiebrief

FACULTEIT
RECHT EN CRIMINOLOGIE

INFORMATIEBRIEF

MASTERPROEF JAYSON MELIS – SMART CCTV EN WETSHANDHAVING: EEN ETHISCH VERANTWOORDE TOOL VOOR POLITIONEEL GEBRUIK?

Beste deelnemer,

Alvast bedankt voor uw interesse in mijn onderzoek naar het gebruik van slimme camera's door de politie. Hieronder wordt toegelicht wat het onderzoek precies inhoudt zodat u voldoende geïnformeerd bent vooraleer deel te nemen. Indien u na het lezen van deze informatie nog vragen of opmerkingen heeft, wil ik u graag te woord staan. U kan mijn contactgegevens aan het einde van deze informatiebrief raadplegen.

Doel van het onderzoek

In het kader van mijn masteropleiding Criminologische wetenschappen aan de universiteit Gent wil ik met dit onderzoek kritisch reflecteren over de mate waarin het inzetten van slimme camera's voor opdrachten van bestuurlijke of gerechtelijke politie ethisch verantwoord is. Hierbij beoog ik een goed begrip te krijgen van wat er exact op het spel staat met deze beeldtechnologie, en welke gevolgen het politioneel gebruik ervan in de praktijk kan hebben.

Om het doel van mijn onderzoek te bereiken, ben ik op zoek naar personen die omwille van hun professionele achtergrond voldoende vertrouwd zijn met en kennis hebben over de thematiek.

Wat houdt deelname aan het onderzoek in?

Concreet houdt dit in dat er een interview met open vragen plaatsvindt waarin uw privacybezorgdheden en bedenkingen met betrekking tot slimme camera's besproken worden. Doorheen het interview wordt ook gepeild naar de mate waarin bepaalde toepassingen (*ANPR – gedragsherkenning – live gezichtsherkenning*) vanuit uw standpunt al dan niet wenselijk en verantwoord zijn voor politioneel gebruik.

Een volledige deelname aan het onderzoek zal ongeveer 60 minuten van uw tijd in beslag nemen. Normaliter vindt het interview plaats op een door ons beiden overeengekomen locatie. Indien gewenst is er ook de mogelijkheid om dit gesprek online te laten doorgaan. Uw deelname is tenslotte volledig vrijwillig, wat inhoudt dat u op ieder moment de medewerking aan het onderzoek mag stopzetten.

Wat gaat er met mijn antwoorden gebeuren?

Om de verkregen informatie op een nauwkeurige manier te kunnen verwerken, zal een audio-opname van het interview gemaakt worden. Uiteraard wordt ons gesprek enkel en alleen maar opgenomen indien u hiervoor toestemming verleent. De opname is uitsluitend voor mijzelf en de promotor toegankelijk en zal na afronding van het onderzoek verwijderd worden.

Als onderzoeker kan ik u garanderen dat uw anonimiteit en privacy te allen tijde gerespecteerd wordt. In geen geval zal de verkregen informatie uit de interviews gelinkt kunnen worden aan uw identiteit.

Indien gewenst is het mogelijk om de transcriptie van uw interview achteraf na te lezen en citaten aan te passen of zelfs verklaringen in te trekken waar u dit nodig acht. Na afronding van het onderzoek kan u ook een beknopte samenvatting van de resultaten ontvangen.

Uiteindelijk zal het verzameld onderzoeksmateriaal na afronding van het onderzoek verwijderd worden.

Waar kan ik met vragen of opmerkingen terecht?

Indien u vóór, tijdens of na het onderzoek met vragen of opmerkingen zit, sta ik u graag te woord. Hiervoor kan u contact opnemen met de verantwoordelijke van het onderzoek door te mailen naar Jayson.Melis@UGent.be.

Ik wil u alvast hartelijk bedanken voor het lezen van deze brief en uw bereidwilligheid tot deelname.

Met vriendelijke groeten,

Jayson Melis

Bijlage 4: Topiclijst

Topiclijst – Smart CCTV voor wetshandhavingsdoeleinden

Introductie
- Kennismaking
- Doelstelling onderzoek
- Informed consent

Personalia respondent
- Huidig beroep + vroegere werkervaring
- Aantal jaren beroepservaring

Cameratoezicht in België/Nederland
(afhankelijk van nationaliteit respondent)
- Bespreking cijfers
- Opinie t.a.v. toenemende investering/operationele inzet

Smart CCTV (algemeen)
- Reguliere camera's vs. slimme camera's
- Privacyconsequenties
  - Privacy bevorderend?
- Vertrouwen in de politie
  - Gegevensverzameling/-verwerking (anonimiteit)
  - Bewaartermijn
  - Gebruik voor andere doeleinden
  - Overheid vs. private ondernemingen
- Transparantie
  - Pictogram voldoende?
  - Over welke aspecten informeren?
- Bijkomende bezorgdheden (i.t.t. reguliere camera's)

Automatische nummerplaatherkenning (ANPR)
- Veiligheidswaarde
- Accuraatheid en juistheid
  - Beïnvloedbare factoren: weeromstandigheden, valse kentekens, kwaliteit referentielijsten
- Impact op rechten en vrijheden
- Andere doeleinden
  - Detectie gsm-gebruik achter het stuur
- Kosten-batenanalyse

Automatische gedragsherkenning
- Veiligheidswaarde (*predictive policing*)

- Accuraatheid en juistheid (normaal vs. afwijkend gedrag)
    - Beïnvloedbare factoren: soort te detecteren gedrag, chilling effect
- Impact op rechten en vrijheden
- Kosten-batenanalyse

Live gezichtsherkenning (LFR)

- Politioneel gebruik: mogelijk/wenselijk vs. permanent verbod
    - Impact op rechten en vrijheden
    - Vermoeden van (on)schuld?
- Nood aan wettelijk kader dat de technologie reguleert?
- Accuraatheid en juistheid
    - Vals positieven, vals negatieven, bias
    - Voorstander van proefprojecten om effectiviteit door politie te laten testen?
- Kosten-batenanalyse

Vergeten of onderbelichte zaken

- Andere bezorgdheden en/of bedenkingen
- Wilt u nog iets toevoegen?

Vragen/opmerkingen

Bedanking