Vraagstukken rond privacy: de zoektocht naar een wettelijk kader voor het gebruik van live facial recognition door de geïntegreerde politie in belgië

Aantal woorden: **46 283** (inclusief voetnoten en bibliografie)

Masterproef voorgelegd voor het behalen van de graad master in de rechten

Academiejaar: 2020- 2021

Deze masterproef is een examendocument dat niet werd gecorrigeerd voor eventueel vastgestelde fouten

**Abstract**

Reeds enige tijd heerst er twijfel of het wenselijk is dat politie gebruik kan maken van Live Facial Recognition (LFR) om personen te identificeren bij het uitoefenen van haar opdrachten. Uit een recent Voorstel van Verordening dat een regelgevend kader rond AI wil installeren op Europees niveau blijkt dat de Europese Commissie het over het algemeen niet wenselijk vindt dat LFR wordt gebruikt in publieke ruimtes. De vraag is nu in welke mate het wenselijk kan zijn om bepaalde toepassingen van LFR op een proportionele manier te gebruiken. Om deze vraag te kunnen beantwoorden moeten echter bepaalde vraagstukken nader worden bekeken.

De eerste vraag is hoe een concrete proportionaliteitstoets voor het gebruik van LFR door de politie eruit moet zien. Zo blijkt dat het momenteel erg onduidelijk is welke criteria in rekening moeten worden genomen om een beoordelingstoets te doen, omdat het moeilijk is een afbakening te maken tussen het recht op eerbiediging privéleven en het recht op bescherming persoonsgegevens. Bovendien stelt zich de vraag hoe en in welke mate de ontwikkeling van LFR hierbij in rekening moet worden genomen. Zo blijkt immers bij een uiteenzetting van de fasen die het gebruik van LFR voorafgaan dat de ontwikkelingsfase enerzijds reeds inperkingen inhoudt op het recht op bescherming persoonsgegevens en anderzijds ook andere problemen omvat, die in meer of mindere mate een impact hebben op de bescherming van privacy bij het latere gebruik van LFR door de politie.

Slechts wanneer deze vragen worden beantwoord kan men beoordelen welke concrete proportionele maatregelen die voorzien in het gebruik van LFR door de politie wenselijk zijn in een democratische samenleving.

[I. Dankwoord 4](#_Toc83303647)

[II. Intro 5](#_Toc83303648)

[III. Methodologie 6](#_Toc83303649)

[IV. Beperkingen van het onderzoek 16](#_Toc83303650)

[V. Wat is Live Facial Recognition? 16](#_Toc83303651)

[1. Drie vormen van gezichtsherkenning 16](#_Toc83303652)

[2. LFR: technologische basis 17](#_Toc83303653)

[3. Drie hoofdmechanismen van camera-surveillance 19](#_Toc83303654)

[VI. Gebruik van LFR bij de politie 19](#_Toc83303655)

[1. Organisatie binnen de geïntegreerde politie in België 20](#_Toc83303656)

[2. Opdrachten van de Belgische politie en hun link met LFR 20](#_Toc83303657)

[3. Werkwijze van LFR binnen bestuurlijke en gerechtelijke opdrachten 24](#_Toc83303658)

[VII. Wettelijk kader rond privacy 26](#_Toc83303659)

[1. Privacy: een moelijk begrip 26](#_Toc83303660)

[2. De wezenlijke inhoud van beide mensenrechten en andere perspectieven op “privacy” 32](#_Toc83303661)

[VIII. Welke rechtsinstrumenten zijn van toepassing bij het gebruik van LFR voor politionele doeleinden? 35](#_Toc83303662)

[1. Toepassingsgebied Richtlijn Politie en Justitie/Algemene Verordening Gegevensbescherming/Wet Bescherming Persoonsgegevens 35](#_Toc83303663)

[2. Politioneel kader: Camerawet/Wet op het Politieambt 38](#_Toc83303664)

[3. Belangrijke begrippen en actoren 39](#_Toc83303665)

[4. Toezichthoudende overheden 46](#_Toc83303666)

[IX. Vraagstuk rond de rechtsgrond van LFR in België 49](#_Toc83303667)

[1. Het debat rond LFR: is er nood aan een wettelijke basis? 49](#_Toc83303668)

[2. Is er een wettelijke basis? 50](#_Toc83303669)

[3. Is er een wettelijke basis voor proefprojecten? 54](#_Toc83303670)

[4. Aan welke inhoudelijke voorwaarden moet een rechtsgrond voldoen? 55](#_Toc83303671)

[X. Hoe beïnvloedt LFR privacy? 59](#_Toc83303672)

[1. Ontwikkelingsfase 59](#_Toc83303673)

[2. Fase van de aankoop 72](#_Toc83303674)

[3. Gebruik van LFR door de politie in de praktijk 79](#_Toc83303675)

[XI. Hoe beïnvloedt LFR verweven rechten? 100](#_Toc83303676)

[1. Het recht op een eerlijk proces 100](#_Toc83303677)

[2. Implicaties voor vrijheid van meningsuiting 101](#_Toc83303678)

[3. Non-discriminatiebeginsel 102](#_Toc83303679)

[XII. Enkele andere maatschappelijke problemen 103](#_Toc83303680)

[XIII. Conclusie 107](#_Toc83303681)

[XIV. Bibliografie 109](#_Toc83303682)

*“When we encounter something unprecedented, we automatically interpret it through the lenses of familiar categories, thereby rendering invisible precisely that which is unprecedented.” -Shoshana Zuboff, The Age of Surveillance Capitalism[[1]](#footnote-1)*

## Dankwoord

Ergens rond oktober 2019 sprong ik een gat in de lucht toen bleek dat ik een masterproef kon schrijven bij professor Eva Brems en Dr. Eline Kindt over live facial recognition. Bij het onderzoek in het anderhalf jaar dat volgde werd ik gesteund door een hele groep mensen, die ik in dit onderdeel van mijn masterproef wil bedanken.

Ik wil mijn promotors bedanken voor het vertrouwen en voor de aangename gesprekken. Ze stonden steeds open voor vragen, waar ik veel aan heb gehad.

Ik wil ook mijn respondenten bedanken om tijd te nemen voor een interview, om uitgebreid mijn vragen te beantwoorden en me informatie en contacten aan te reiken. Elk individueel gesprek zorgde zo voor nuttige inzichten die me hielpen bij mijn verder onderzoek.

Gust, Bente en mijn peter Ferre wil ik bedanken om het afgelopen anderhalf jaar te luisteren naar mijn uitingen van een gezonde interesse in alles wat met privacy te maken heeft. Mijn ouders wil ik bedanken voor alles.

Tenslotte wil ik mijn vrienden bedanken om een belangrijke bron te zijn van energie die ik kon investeren in mijn masterproef. Onder “vrienden” vallen leden van de ornitologische kring, enkele Wippelgemburgers, bezoekers van een trollenkelder, klanten van de Turkse bakker in de Dampoortstraat, mijn grote familie uit de Monterey, een groepje studenten-juristen wiens vriendschap op zich al een goeie reden was om rechten te studeren en een kleine potpourri van Europese bergbeklimmers.

## Intro

Met een boek met “mugshots” in de hand liet de Amerikaanse mathematicus Woody Bledsoe in 1964 voor het eerst een computer gezichten lezen.[[2]](#footnote-2) Het duurde nog tot 2014 voor Facebook met Deepface het eerste model trainde met een neuraal netwerk, wat een technologische en commerciële doorbraak betekende voor de technologie.[[3]](#footnote-3)

De vorm van automatische gezichtsherkenning of automated facial recognition (AFR)[[4]](#footnote-4) waar dit onderzoek op focust, is de vorm van AFR die personen identificeert aan de hand van bewegende camerabeelden: live facial recognition (hierna: LFR)[[5]](#footnote-5)

Naar aanleiding van een proefproject met LFR in Zaventem oordeelde het Controleorgaan op de politionele Informatie (hierna: COC) dat de huidige privacywetgeving een onvoldoende rechtsgrond biedt om de technologie te gebruiken.[[6]](#footnote-6) Dat betekent dat het voor private bedrijven momenteel wetenschappelijk mogelijk is om LFR-technologie te ontwikkelen en verkopen, maar voor politiediensten niet is toegestaan de LFR-functie te gebruiken.

Op nationaal niveau bestaat onduidelijkheid hoe een wettelijk kader dat de technologie reguleert er precies uit moet zien. Reden voor deze twijfel was dat de technologie enerzijds een mogelijke meerwaarde biedt voor de politie bij het beschermen van de nationale veiligheid, maar anderzijds risico’s met zich meebrengt voor mensenrechten, in de eerste plaats het recht op eerbiediging van privé-, familie en gezinsleven[[7]](#footnote-7) en het recht op de bescherming van persoonsgegevens.[[8]](#footnote-8)

De federale politie voert daarom momenteel een juridische analyse van LFR uit en onderzoekt bijkomende operationele behoeften bij het gebruik van biometrie. Minister van Binnenlandse Zaken Verlinden zal zich op dit onderzoek baseren om indien nodig wetgeving en regelgeving op te stellen voor het gebruik van LFR. Ze vermeldt hierbij dat de technologie van “bijzonder groot belang is in de strijd tegen terrorisme, georganiseerde criminaliteit en met het oog op de bescherming en de handhaving van de openbare veiligheid.” Het is volgens haar alvast de bedoeling om het gebruik van LFR uit te breiden “naar alle kritieke infrastructuren”.[[9]](#footnote-9)

Op Europees niveau bestond lange tijd dezelfde onduidelijkheid. Zo overwoog de EU in 2020 nog om een tijdelijk vijfjarig moratorium in te voeren voor gezichtsherkenning, maar kwam ze hier later van terug.[[10]](#footnote-10) Uiteindelijk leek de EU het aan de lidstaten over te laten om te beslissen of een wettelijk kader nodig was en hoe dat er dan moest uitzien. [[11]](#footnote-11) Kort voor het indienen van deze masterproef kwam er echter een belangrijke wending in de zoektocht naar een wettelijk kader. De Europese Commissie (hierna: EC) vaardigde immers een voorstel van Verordening rond AI uit, waarin uitgebreid de problematiek van (live) facial recognition wordt behandeld.

Aangezien de EU zich bevoegd acht live facial recognition te reguleren ontstaat een belangrijke wending in de zoektocht naar een wettelijk kader: het debat over de vorm en inhoud van een mogelijk wettelijk kader van LFR is immers geopend en wordt gevoerd op Europees niveau.[[12]](#footnote-12)

## Methodologie

#### Opzet en onderzoeksvragen van deze masterproef

In deze masterproef onderzocht ik in opdracht van de Liga voor Mensenrechten welke concrete maatschappelijke en juridische implicaties het gebruik van LFR door de geïntegreerde politie in België heeft voor mensenrechten. Ik focuste hierbij voornamelijk op Vlaanderen, gezien het in het kader van de masterproef niet mogelijk was om uitgebreid zowel Vlaamse als Waalse politiezones te interviewen.

Om dit opzet te verwezenlijken, behandelde ik de volgende onderzoeksvragen:

1. Wat is de maatschappelijke en juridische impact van de toepassing van LFR gebruikt door de Belgische geïntegreerde politie op mensenrechten?
	1. Deelvraag: Wat zijn de mogelijke toepassingen van LFR voor politie in België?
	2. Deelvraag: Hoe beïnvloedt zulke toepassing van LFR de privacy (het recht op bescherming persoonsgegevens[[13]](#footnote-13) en het recht op eerbiediging van privé-, familie en gezinsleven).[[14]](#footnote-14)
2. In welke mate kunnen schendingen van de betrokken mensenrechten bij de toepassing van LFR door de geïntegreerde politie in België vermeden worden?

Uit dit onderzoek leidde ik enkele vraagstukken af die richting kunnen geven aan het ruimere (Europese) debat over toekomstige wetgeving.

#### Concrete bijdragen van de masterproef in het licht van het nieuwe voorstel van verordening

Dit onderzoek hoopt het volgende te kunnen bijdragen:

* Een beschrijving van wat LFR inhoudt en enkele mogelijke toepassingen ervan in de Belgische politionele context. Hieruit kan men afleiden welke vormen van LFR wel en niet onder het verbod vallen dat de EC voorstelt.
* Een overzicht van de manier waarop gebruik van LFR voor politionele doeleinden privacy beïnvloedt.
* Via de toets aan het recht op bescherming persoonsgegevens/het recht op eerbiediging privéleven geeft het bovendien een overzicht van de ruimere problemen met betrekking tot verweven rechten en maatschappelijke problemen.
* Een toets van een mogelijk gebruik van LFR aan het bestaande wettelijk kader draagt bij aan een overzicht van de raakpunten van LFR aan verschillende (nationale) juridische materies.

#### Onderzoeksproces

* Stap 1: Literatuuronderzoek

Ter voorbereiding van de materie voerde ik een bureau-onderzoek, waarbij ik me inlas in de bestaande literatuur. Op basis daarvan stelde ik een stand van zaken samen van de materie van LFR. De bronnen die ik hierbij gebruik bestaan ten eerste uit de wetgeving op Europees, Belgisch en Vlaams niveau. Ten tweede gebruikte ik rechtspraak van het EHRM, het Europees Hof van Justitie (hierna: HvJ) en het Grondwettelijk Hof. Verder bestaat een groot deel van de bronnen in dit onderzoek uit zogenaamde “grijze literatuur:” richtlijnen, aanbevelingen, rapporten van (officiële) instanties, (interne) documenten en krantenartikels.[[15]](#footnote-15) Door de snel evoluerende inhoud van de materie bestaan er ontzaglijk veel van dit type bronnen en was het niet mogelijk om deze allemaal te behandelen binnen het kader van deze masterproef. Ik heb me dan ook beperkt tot enkele autoriteiten m.b.t. regelgeving rond AI, LFR en privacywetgeving. Er dient te worden opgemerkt dat er verschillende autoriteiten zijn in de context van gegevensbescherming. Ik koos deze organisaties omdat dit de instanties zijn die richtlijnen creëren rond en verder vorm geven aan de wetgevende instrumenten die ik gebruik.

Ik maakte voornamelijk gebruik van bronnen van de volgende gegevensbeschermingsautoriteiten: de Fundamental Rights Agency (FRA), European Data Protection Supervisor (EDPS), de European Data Protection Board (EDPB) die de voormalige Artikel 29-Werkgroep (of Working Party 29, hierna: WP29) vervangt. Bovendien gebruikte ik ook de “Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data bij Verdrag 108” bij de Raad van Europa. Op nationaal niveau boden de adviezen en rapporten van het COC nuttige richtlijnen bij het oplossen van de onderzoeksvraag van deze masterproef.

Op basis van dit literatuuronderzoek stelde ik een voorlopige structuur samen van mijn onderzoek, om zo een overzicht te krijgen van de stand van zaken en de voornaamste lacunes in de bestaande literatuur rond LFR.

* Stap 2: kwalitatief onderzoek: interviews

##### Verantwoording van de methode

In een tweede fase van het onderzoek nam ik een reeks **semi- gestructureerde interviews** af met experten binnen hun terrein. Gezien de materie van LFR vele raakpunten heeft,[[16]](#footnote-16) behoren de respondenten van de interviews tot een heterogene groep. De resultaten uit de interviews werden in de eerste plaats gebruikt als leidraad voor verder literatuuronderzoek naar de vraagstukken met LFR. In de tweede plaats gebruikte ik de interviews om respondenten te parafraseren doorheen deze masterproef, waar dit relevant is. Omdat het politioneel gebruik van LFR in België momenteel nog hypothetisch is, vond ik het relevant om ruimte te laten voor verschillende visies op een mogelijk wettelijk kader.

De respondenten die ik interviewde zijn de volgende:

|  |  |  |
| --- | --- | --- |
| **Naam** | **Functie** | **Verslag** |
| Nele Krols | DPO[[17]](#footnote-17) bij een aantal Antwerpse Politiezones[[18]](#footnote-18). | MS Teams-opname, transcriptie, notities |
| Piet De Vulder | DPO bij PZ VLAS[[19]](#footnote-19), Westkust[[20]](#footnote-20), Polder[[21]](#footnote-21), Riho [[22]](#footnote-22) | MS Teams-opname, transcriptie, notities |
| Jan Vandenkerchove | DPO bij PZ Gent | Geluidsopname, transcriptie, notities |
| Kurt Verstockt | DPO bij PZ Donder-Schelde | Notities |
| Mart Coenen | DPO bij PZ’s Limburg | MS-Teams-opname |
| Stéphanie Witters | adjunct-DPO bij PZ Oostende, leraar postgraduaat-opleiding tot DPO aan Howest, Business Consultant bij Privaco | MS-Teams-opname, transcriptie, notities |
| Ruben Vansevenant | Diensthoofd ICT bij PZ Gent. | MS-Teams-opname. |
| Nick Noël | Directeur Operaties bij politiezone Rupel | MS-Teams-opname, transcriptie, notities. +notities van rondleiding in PZ Rupel |
| Frank Schuermans | Lid-Raadsheer bij het Controleorgaan op de Politionele Informatie (COC) | MS-Teams-opname, transcriptie, notities |
| Anke Stakenborg | Beleidsadviseur van de Commissaris Generaal bij de federale politie, onderzoekt momenteel de mogelijkheden met technologieën die biometrische persoonsgegevens verwerken (zoals LFR) | MS-Teams-opname, transcriptie, notities |
| Bart Schoenmaekers | Diensthoofd Financiën en Middelen bij PZ Gent | MS-Teams-opname, transcriptie, notities |
| Yves Moreau | Gewoon hoogleraar aan KULeuven in de ingenieurswetenschappen. Voert onderzoek naar “computational biology for genomic medicine”. Onderwees bovendien ook een vak binnen de faculteit over ethiek en bio-informatica. | MS-Teams-opname, notities |
| Wim Hardyns | Hoofddocent aan UGent in Criminologie, bij het Institute for International Research on Criminal Policy (IRCP) | MS-Teams-opname, transcriptie, notities |
| Koen Luykx | Regional Sales Manager binnen de BENELUX bij Avigilon, Motorola Solutions, dat onder andere LFR verkoopt aan publieke en private klanten. | MS-Teams-opname, transcriptie, notities |
| Ella Jakubowska | Policy and Campaigns Officer bij European Digital Rights (EDRi). EDRi is een Europees netwerk van privacyen burgerrechtenorganisaties in 19 verschillende landen.[[23]](#footnote-23) | MS Teams-opname, transcriptie |
| Peter van Schelven | Zelfstandig Juridisch Adviseur in Nederland, met uitgebreide ervaring binnen het gegevensbeschermingsrecht, o.a. binnen posities als DPO en als leraar binnen de opleiding tot DPO. | Notities |
| Stephen Lernout | Chief Strategy and Innovation bij Nalantis, een Belgisch bedrijf dat AI-taalmodellen ontwikkelt. | MS-Teams-opname |

Aanvullend voerde ik ook een telefoongesprek met een persoon met ervaring bij de Financiën bij de federale politie, die me meer vertelde over de praktijk van het aankoopbeleid van innovatieve technologieën op federaal niveau. Deze wenste liever anoniem te blijven.

##### Methodologie bij het interviewen

De aanpak die ik hanteerde om interviews af te nemen bestond concreet uit **4 verschillende fasen**: contacteren van respondenten, voorbereiden van het interview, interviews afnemen en de resultaten voorbereiden voor verdere verwerking.

###### *Fase 1: Respondenten contacteren*

Om respondenten te contacteren gebruikte ik in de eerste plaats **Linkedin**:[[24]](#footnote-24) ik stuurde connect-verzoekjes naar professoren van wie ik les had (en geen les had) en had zo snel toegang tot hun netwerk van onderzoekers. Via Wim Hardyns, professor in de criminologie, was het gemakkelijk om een netwerk uit te bouwen binnen de politie. In de tweede plaats probeerde ik respondenten te vinden via de **officiële kanalen**, zoals de contactpagina op de website van federale en lokale politiezones. De respons via deze weg hing heel erg af van de contactpersoon. Ik vond het in het algemeen moeilijker om via de officiële kanalen, in het bijzonder die van de federale politie, te werken.

Een derde hele waardevolle manier om respondenten te vinden was via de **sneeuwbalmethode**. Dit wil zeggen dat ik de personen die ik contacteerde vroeg of zij mensen (of organisaties, onderzoeksgroepen,…) kenden die interessant zouden kunnen zijn voor mijn onderzoek. Op die manier kreeg ik gemakkelijk de contactgegevens van andere respondenten, die ik dan vaak uit naam van de ander kon contacteren. Ik paste deze methode ook toe in mailverkeer wanneer de persoon die ik contacteerde afwijzend reageerde omdat die niet wilde of kon meewerken aan het onderzoek.

In de eerste communicatie met de respondent zette ik vervolgens kort het opzet van mijn masterproef uiteen en de reden waarom een interview met deze persoon relevant zou zijn voor mijn onderzoek (eventueel de manier waarop ik de contactgegevens van de persoon had gevonden). Ik probeerde het zo te doen klinken dat het ook interessant zou kunnen zijn voor hen om hierover een gesprek te hebben. (vb.:“Ik ben erg benieuwd naar de visie die u heeft op deze vraagstukken vanuit uw positie/ervaring als X”)

In deze eerste communicatie voegde ik mijn onderzoeksplan toe in de bijlage, zodat men een gedetailleerder overzicht kreeg van het onderzoek, van wie ik nog zou interviewen, de manier waarop ik data zou verwerken,… Daarnaast vermeldde ik ook steeds de mogelijkheid om anoniem te blijven.

Ik zorgde er steeds voor dat ik erg beschikbaar was wanneer ik respondenten contacteerde. Zodra een moment was vastgelegd, stuurde ik een MS Teams-nodiging via mail met daarin nog eens heel kort het doel van het interview en en de mededeling dat het interview waarschijnlijk een uur in beslag zou nemen.

###### *Fase 2: Respondenten contacteren*

Op basis van de voorlopige structuur die ik samenstelde uit het literatuuronderzoek, kon ik een indeling maken van de voornaamste thema’s die ik wilde bevragen. Dit zag er toen uit als volgt:

|  |  |  |
| --- | --- | --- |
| **Thema** | **Vragen en bijvragen (genummerd)** | **Relevantie van de vraag** |
| 1. Mogelijke toepassingen van LFR in België |  |  |
| 2. Mogelijke problemen |  |  |
| a. Aankopen van technologie |  |  |
| b. Privacy |  |  |
| c. Discriminatie |  |  |
| 3. Mogelijke oplossingen |  |  |

De concrete afbakening van de thema’s in het schema evolueerde gaandeweg door het onderzoek. Zo had ik in eerste instantie naast privacy ook het non-discriminatiebeginsel als uitgangspunt voor mijn onderzoek. De antwoorden op de vragen die ik stelde binnen dit thema bleken echter grotendeels te kaderen binnen het belang van privacy, dat zelf al garanties blijkt te bieden voor de bescherming van het non-discriminatiebeginsel. Om deze reden en omdat een onderzoek naar de impact van LFR op het non-discriminatiebeginsel als recht op zich voldoende informatie biedt voor een tweede masterproef, besloot ik het non-discriminatiebeginsel uitsluitend te onderzoeken in het licht van de eerbiediging van het privéleven/het recht op bescherming persoonsgegevens.

In bovenstaand schema vulde ik per thema vragen in die toetsten naar de lacunes in het bestaande literatuuronderzoek, zodat ik in totaal 10 vragen had. Bovendien bereidde ik ook enkele bijvragen voor. Die vragen peilden ~~bovendien~~ naar de ervaring en kennis van iedere individuele respondent en de informatie die ik verwachtte te kunnen verzamelen uit een gesprek met de persoon. Alweer bood Linkedin hier een handig hulpmiddel, aangezien ik zo snel een helder overzicht had van de opleiding en werkervaring van iedere respondent en het belang van hun positie voor mijn onderzoek.

Ten slotte printte ik de interviewgids en nam goed de vragen door zodat ik tijdens het gesprek mijn vragen achter de hand had en gemakkelijk kon inspelen op wat de respondent vertelde.

###### *Fase 3: Interviews afnemen*

De meeste van mijn interviews gingen door via MS Teams en 2 respondenten sprak ik “offline”. Oorspronkelijk was de bedoeling om al mijn respondenten in het echt te ontmoeten in een café en hen een koffie of taartje te trakteren. Deze methode was mogelijk wat twijfelachtig qua onderzoeksethiek, dus gelukkig stak corona daar een stokje voor. Via MS Teams kon ik me erg toegankelijk opstellen en kon ik gemakkelijk het gesprek opnemen via de opnamefunctie.

Ik startte elk gesprek door mezelf voor te stellen en de respondent te begroeten en te bedanken om tijd vrij te maken voor een gesprek. Vervolgens zette ik het opzet van mijn masterproef uiteen en het concrete opzet van het interview (bijvoorbeeld: “In dit gesprek wil ik toetsen naar de standaardpraktijken rond privacygaranties bij het gebruik van bestaande technologieën”). Ik vertelde de persoon over de mogelijkheid om achteraf de resultaten van mijn onderzoek te lezen en aanpassingen te doen aan de citaten uit het interview die ik zou gebruiken in de masterproef. Daarna vroeg ik of de respondent zelf nog bepaalde vragen had of bedenkingen over het interview. Voor ik uiteindelijk begon vroeg ik ook toestemming om het gesprek op te nemen voor eigen gebruik en notities te maken tijdens het gesprek.

Het interview zelf begon ik steeds met een hele open vraag (bijvoorbeeld: “Wat zijn volgens u de mogelijke toepassingen van LFR voor de politie in België?”). Door deze ruime vraagstelling begon de respondent meestal over thema’s die deze zelf belangrijk vond. Op deze manier konden zij zelf aanhalen wat zij interessant vonden en maakten ze associaties die ik niet had kunnen voorspellen.

Wat zij vertelden sloot steeds aan bij een van de thema’s die ik had voorbereid, waardoor ik aan de hand van mijn vragenlijst gemakkelijk kon inpikken met vragen over het thema dat zij relevant achten bij de mogelijke toepassingen van LFR. Afhankelijk van wat de respondent vertelde, vroeg ik door met speficieke bijvragen. De gevoelige vragen (bijvoorbeeld rond discriminatie en de verantwoordelijkheid van de politie) stelde ik pas op het einde.

Tijdens het gesprek noteerde ik voor mezelf de nummers (of het belangrijkste woord) van de vragen die ik vervolgens wilde stellen en doorstreepte ik de nummers van vragen die ik reeds stelde. Op deze manier verloor ik geen tijd met zoeken naar de gepaste vragen.

Tussendoor noteerde ik de voornaamste bevindingen in sleutelwoorden.

Eens ik al mijn vragen had gesteld, rondde ik af door te bedanken voor de informatie/het gesprek. Ik vroeg of de respondent zelf nog vragen had en vroeg vervolgens of deze nog andere personen kende die ik zou kunnen interviewen/bronnen die ik kon gebruiken. Vervolgens herhaalde ik de mogelijkheid om de masterproef na te lezen en de citaten daarin aan te passen waar ze dit zouden nodig vinden (en eventueel de mogelijkheid om het gesprek te anonimiseren) en gaf ik hen de datum waarop ik het onderzoek plande door te sturen.

###### *Fase 4: Resultaten voorbereiden voor verdere verwerking*

Na het interview downloadde ik de opname van het interview de dag zelf om het op te slaan op mijn laptop, op een stick en in de Onedrive van de UGent. Vervolgens typte ik in een word-document een kort verslag van het interview. In dat verslag beschreef ik kort hoe het interview was verlopen (bijvoorbeeld: de respondent leek gestresseerd, was vriendelijk, respondent viel weg in het midden van het gesprek,…).

Ik gebruikte dit verslag vervolgens bij het transcriberen van het interview, waarvoor ik in een apart document woordelijk het gesprek uittypte. In dit verslag reflecteerde ik over mijn aanpak bij het interviewen. Op deze manier wist ik wat ik zelf beter kon doen in een volgend interview. Zo zorgde mijn gebruik van het begrip “facial recognition” in plaats van “live facial recognition” voor verwarring doorheen een volledig interview en had ik dit pas achteraf goed door. Zo wist ik dat ik dit begrip in een volgend gesprek goed moest afbakenen.

Bij het transcriberen onderlijnde ik in Word ook de belangrijkste informatie, die ik dan achteraf kort structureerde in het verslagdocument. Zo had ik een overzicht van wat ik verder kon onderzoeken, in literatuuronderzoek, maar ook in verdere interviews, waarin ik dan specifieker vragen kon stellen die verder gingen op wat ik reeds leerde.

Op het einde van het verslag lijstte ik de personen op naar wie de respondent me eventueel doorverwees.

Zowel het document met de transcriptie, het verslag van het interview, als de opname van het interview sloeg ik vervolgens op in een map met een nummer en de naam van de respondent in een map “Interviews”.

* Stap 3: Plaatsbezoek aan de PZ Rupel

Om in de praktijk een overzicht te krijgen van de werking van de (lokale) politie kreeg ik een rondleiding van de Directeur Operaties bij politiezone Rupel, Nick Noël. Hierbij kreeg ik een overzicht van de praktijken met camera’s en bestaande technologieën en privacywaarborgen in de praktijk. Ik kon uitgebreid vragen stellen aan verschillende personen die camerabeelden monitorden en ANPR-camera’s hanteerden.

* Stap 4: Verder literatuuronderzoek aan de hand van de resultaten over LFR

Vervolgens verwerkte ik de resultaten uit de interviews en onderwierp ik deze aan verder literatuuronderzoek. Hetzelfde type bronnen werd hiervoor gebruikt als in de eerste fase van literatuuronderzoek.

Een leidraad bij de verwerking van de resultaten van de interviews en verder literatuuronderzoek is de praktijk van het gebruik van Automatic Number Plate Recognition (hierna: ANPR), dat ik gebruikte als case study.

ANPR-technologie wordt immers reeds uitgebreid ingezet door de politie ~~wordt~~ om nummerplaten te herkennen. Het linkt beelden van nummerplaten aan nummerplaten in een databank van auto’s die worden gezocht door de politie.[[25]](#footnote-25) ANPR en LFR hebben elk verschillende consequenties voor mensenrechten, in die zin bijvoorbeeld dat LFR gevoelige biometrische persoonsgegevens en ANPR voornamelijk persoonsgegevens (nummerplaten) verwerkt die niet per se gevoelig zijn.[[26]](#footnote-26) Desalniettemin is ANPR een goed voorbeeld van een innovatieve technologie die als precedent kan dienen voor andere “slimme” technologieën, zoals LFR. Zo is LFR net als ANPR een innovatieve technologie die werkt met een (technische) databank[[27]](#footnote-27) met persoonsgegevens en ingezet wordt door de politie in België.[[28]](#footnote-28) ANPR-gebruik door de politie heeft intussen een duidelijk wettelijk kader en wordt breed ingezet ingevolge het beleidsplan van Jan Jambon om een nationaal cameraschild in te voeren. Dit plan kwam er na de aanslagen in Parijs en Brussel en zorgt ervoor dat er tegen 2022 zo’n 3465 ANPR-camera’s in België geïnstalleerd zullen zijn.[[29]](#footnote-29)

Om die reden wordt ANPR als analoge case-study gebruikt doorheen deze masterproef, in het bijzonder bij Deel VI, Fase 2: aankoopbeleid en Fase 3: Gebruik LFR door politie in de praktijk.

## Beperkingen van het onderzoek

De resultaten uit dit onderzoek zijn niet-exhaustief, om verschillende redenen. Ten eerste situeert het zich in een snel veranderende context, zowel op wetgevend, technologisch als politiek vlak. Zeker in het licht van het voorstel van Verordening zal in de (nabije) toekomst zowel harde als zachte wetgeving de materie van LFR omkaderen. De relevantie van het doel van deze masterproef om een overzicht te bieden van de privacyvraagstukken over een mogelijk wettelijk kader is dan ook van tijdelijke aard.

Ten tweede bevindt LFR zich op een kruispunt van verschillende onderzoekdomeinen. Gezien mijn juridische achtergrond en gebrek aan technologische kennis belicht dit onderzoek voornamelijk de juridische en minder de technologische vraagstukken. Wanneer ik bevindingen neerschrijf van technische aard, baseerde ik me op voor mij toegankelijke bronnen en gesprekken met experts.

Ten derde was de keerzijde van de keuze voor een onderzoek in de breedte- in die zin dat het een overzicht biedt van de vraagstukken rond LFR- dat het geen diepgaand onderzoek levert op éen of bepaald(e) specifiek(e) thema(‘s). Het is dan ook aangewezen om bij het lezen van dit onderzoek te beseffen dat elk onderdeel een masterproef op zich waard is.

## Wat is Live Facial Recognition?

### Drie vormen van gezichtsherkenning

Live facial recognition (hierna: LFR) behoort tot de bredere categorie van automatische gezichtsherkenning (hierna: AFR).[[30]](#footnote-30) Binnen deze categorie bestaan er verschillende subcategorieën van gezichtsherkenning. Zo is er gezichtsherkenning die verifieert, catalogiseert en identificeert. Binnen **verificatie** worden twee afbeeldingen van een gezicht vergeleken om te controleren of het dezelfde persoon is. [[31]](#footnote-31) Dit wordt al uitgebreid toegepast bij grenscontroles in luchthavens, ook in België:[[32]](#footnote-32) de betrokkene scant zijn paspoort en dan wordt er een live afbeelding genomen van het gezicht van de betrokkene.[[33]](#footnote-33)

De **catalogisering** maakt het mogelijk om personen op basis van hun gezicht toe te wijzen aan een bepaalde categorie, zoals bijvoorbeeld gender, leeftijd of etnische origine. Hierbij worden betrokkenen niet noodzakelijk geïdentificeerd.[[34]](#footnote-34) Ten slotte is er gezichtsherkenning die afbeeldingen van een gezicht vergelijkt met foto’s van gezichten in een database om zo een persoon te identificeren. Dit is de **identificatie**functie van gezichtsherkenning.[[35]](#footnote-35)

**LFR** valt binnen deze laatste categorie, aangezien het personen probeert te identificeren.[[36]](#footnote-36) De vorm van AFR die dit doet aan de hand van bewegende videobeelden is de focus van dit onderzoek.[[37]](#footnote-37)

### LFR: technologische basis

De technologie van LFR bestaat uit **software** en een camera.[[38]](#footnote-38) Men kan een bestaande “domme” camera in staat stellen gezichten te herkennen, door een deel hardware toe te voegen aan het camerasysteem. Op deze manier kunnen op de bestaande camera AI-applicaties zoals LFR worden geïnstalleerd.[[39]](#footnote-39) Momenteel maakt de politie in België gebruik van verschillende soorten camera’s. Zo zijn er de klassieke CCTV[[40]](#footnote-40)-camera’s, die kunnen voorkomen in statische of mobiele vorm en al dan niet rondom rond kunnen draaien of inzoomen. Sommige types CCTV-camera’s kunnen in het donker filmen en deze beelden omzetten in zichtbaar beeld, anderen kunnen bovendien ook geluid opnemen.[[41]](#footnote-41) Zulke CCTV-camera’s kunnen als bewakingscamera worden ingezet door de politie,[[42]](#footnote-42) door private actoren en door de overheid.[[43]](#footnote-43) In België worden CCTV-camera’s al uitgebreid ingezet voor politiedoeleinden.[[44]](#footnote-44)

Bovendien gebruikt de politie ook steeds vaker bodycams, die agenten dragen bij interventies[[45]](#footnote-45) en dashcams, die gebruikt worden in politiecombi’s.[[46]](#footnote-46) Deze verschillen in functionaliteiten en types van camera’s hebben een invloed op de mate waarin het filmen met die camera intrusief is voor privacy.[[47]](#footnote-47) Door aan deze camera’s een deel hardware en LFR-software toe te voegen wordt het mogelijk om de beelden van 24/7 filmende bestaande camera’s te gebruiken voor automatische analyses achteraf.[[48]](#footnote-48) Die automatische analyses worden uitgevoerd door algoritmes en kunnen bijvoorbeeld bestaan uit patroonherkenning, maar ook uit LFR. [[49]](#footnote-49)

Naast de mogelijkheid om op “domme camera’s” software te installeren kan men ook camera’s inzetten die zelf al de mogelijkheid bezitten om AI-applicaties zoals gezichtsherkenning toe te passen.[[50]](#footnote-50) In dat geval kan men gewoon het Application Program Interface (of API) installeren, dat wordt aangeboden als model-as-a service.[[51]](#footnote-51) Camera’s die zo LFR kunnen toepassen worden in België reeds gebruikt, zonder dat echter de LFR-functie mag worden aangezet.[[52]](#footnote-52) Zulke “intelligente” camera’s worden wel reeds gebruikt voor andere doeleinden, zoals voor nummerplaatherkenning. Automatic Number Plate Recognition-camera’s (hierna: ANPR) worden gebruikt in elk van de **lokale politiezones** die in het kader van dit onderzoek werden geïnterviewd,[[53]](#footnote-53) alsook door de Federale Politie.[[54]](#footnote-54) Bovendien wordt door politiezones ook gebruik gemaakt van camera’s die voorwerpen kunnen herkennen en daardoor personen sneller kunnen opsporen aan de hand van bijvoorbeeld het type trui dat ze droegen.[[55]](#footnote-55)

### Drie hoofdmechanismen van camera-surveillance

Voor LFR is met andere woorden steeds een camera nodig, die het mogelijk maakt de realiteit om te zetten naar een zichtbaar beeld voor de gebruiker van de camera. LFR kent dan ook gelijkaardige toepassingen als bestaande bewakingscamera’s.

De bewakingscamera’s die worden ingezet bij de politie kennen momenteel drie hoofdmechanismen: **heden, verleden en toekomst**.[[56]](#footnote-56)

De **heden**-functie houdt in dat een persoon, zoals een politieambtenaar of private bewakingsagent,[[57]](#footnote-57) de verdachte activiteit of een misdrijf monitort zodat men personen op heterdaad kan betrappen.[[58]](#footnote-58) Op die manier kan het bijvoorbeeld ingezet worden om een grote massa te monitoren (crowd control) of om een politiebureau te bewaken. De **verleden**-functie (of “retroactief kijken”[[59]](#footnote-59)) houdt in dat men eerder gefilmde en opgeslagen camerabeelden kan bekijken.[[60]](#footnote-60)

De **toekomst-**functie slaat dan weer op de mogelijkheid om met camera’s criminaliteit te vermijden door misdadigers het gevoel te geven dat ze gecontroleerd worden.[[61]](#footnote-61) Uit onderzoek blijkt dat deze functie weinig effectief is. Er zou slechts een minieme meerwaarde kunnen worden aangetoond voor de preventie van criminaliteit en dat slechts op verschillende plaatsen. Bovendien zouden er verplaatsingseffecten optreden, wat wil zeggen dat de criminaliteit zich gewoon verschuift naar plekken waar minder camera’s hangen.[[62]](#footnote-62) Hoewel CCTV-camera’s desondanks breed worden ingezet door politie haalden de respondenten (inclusief medewerkers bij de politie) in dit onderzoek deze toekomstfunctie niet aan als mogelijke functie voor LFR. De vraag stelt zich bovendien of LFR in vergelijking met bestaande CCTV-camera’s een wezenlijk verschil in effectiviteit zou maken binnen deze functie. De toekomstfunctie van LFR zal dan ook geen deel uitmaken van dit onderzoek.

## Gebruik van LFR bij de politie

### Organisatie binnen de geïntegreerde politie in België

Eerst en vooral is het belangrijk te schetsen wat wordt verstaan onder “politie” en waarvoor zij LFR kan inzetten. De organisatie van de geïntegreerde politie wordt geregeld in de Wet Geïntegreerde Politie.[[63]](#footnote-63) In België wordt de politie georganiseerd als een **geïntegreerde politie**, die is opgedeeld in een operationeel kader en een administratief en logistiek kader.[[64]](#footnote-64) Het operationele kader bestaat uit politieambtenaren, maar ook uit agenten van politie, beveiligingsassistenten van politie en beveiligingsagenten van politie, die in tegenstelling tot de politieambtenaar geen operationele taken kunnen uitvoeren.[[65]](#footnote-65)

De geïntegreerde politie bestaat uit 2 niveaus: het lokaal en het federaal niveau.[[66]](#footnote-66) Het **lokale** niveau bestaat uit 185 politiezones, verdeeld over het hele grondgebied.[[67]](#footnote-67) Afhankelijk van het aantal gemeenten waaruit de zone is opgebouwd, is de politiezone een één- of meergemeentezone. In een eengemeentezone wordt de lokale politie bestuurd door een burgemeester, gemeenteraad en schepencollege, waar dit in een meergemeentezone gebeurt door de politieraad en het politiecollege.[[68]](#footnote-68)

Op het **federale** niveau staat de politie onder gezag van de minister van Binnenlandse Zaken en de minister van Justitie.[[69]](#footnote-69) De federale politie bestaat uit het commissariaat-generaal, 3 algemene directies, centrale directies, diensten in Brussel en gedeconcentreerde directies en diensten in arrondissementen.[[70]](#footnote-70) Binnen de Algemene Directie bestuurlijke politie valt ook de Luchtvaartpolitie, die controle en toezicht houdt aan de buitengrenzen van de 6 Schengenluchthavens in België.[[71]](#footnote-71)

### Opdrachten van de Belgische politie en hun link met LFR

Om te bepalen waarvoor LFR-camera’s kunnen worden aangewend in politionele context, is het belangrijk te kaderen welke de **bevoegdheden** en **doeleinden** zijn van de politie.

#### Algemene opdracht

De politiefunctie kan algemeen worden gezien als een institutioneel beschermende en regulerende functie van sociale orde die erop gericht is de **uitoefening van de fundamentele rechten** mogelijk te maken en de ontregeling van deze orde te voorkomen of te herstellen.[[72]](#footnote-72)

De politiefunctie dient m.a.w. de handhaving van de sociale, openbare orde.[[73]](#footnote-73) Belangrijk hierbij is dat het naleven en het beschermen van de individuele rechten en vrijheden en de democratische ontwikkeling van de maatschappij steeds als leidraad dienen voor het optreden van politiediensten.[[74]](#footnote-74) Zo bepaalt **artikel 1 van de Wet op het Politieambt** dat de politiediensten waken over de naleving en bijdragen tot de bescherming van de individuele rechten en vrijheden, evenals tot de democratische ontwikkeling van de maatschappij. De bevoegdheid van de politie mag dus niet als doel op zich worden beschouwd, maar moet een middel zijn om de maatschappelijke orde te verzekeren.

Een belangrijk argument voor het gebruik van LFR door de politie in België is dat het de **openbare veiligheid** ten goede zou komen.[[75]](#footnote-75) Het zou immers voordelen bieden qua effectiviteit en efficiëntie in vergelijking met bestaande technologie voor het nakomen van politionele doeleinden, zoals het bestrijden van terrorisme en de handhaving van de openbare orde.[[76]](#footnote-76) Directeur Operaties bij PZ Rupel **Nick Noël** stelt dat camera’s alleen niet de oplossing zijn, maar dat ze wel kunnen bijdragen tot een subjectief veiligheidsgevoel, bewijsvoering, pakkans,…

Een voordeel van LFR is bijvoorbeeld dat het een relatief goedkoop product is omdat het voornamelijk op software eerder dan op hardware gebaseerd is.[[77]](#footnote-77) **Nick Noël** voegt hieraan echter toe dat dit niet opgaat voor ANPR: hoewel ANPR net als LFR voornamelijk op software is gebaseerd, is het toch niet goedkoop, gezien de nodige modelgoedkeuring, ijking, plaatsing, herijking,… nodig zijn.

Daarnaast maakt het ook identificatie op afstand mogelijk, wat in vergelijking met bestaande vormen van bijvoorbeeld vingerafdrukherkenning een snelle vorm van identificatie is[[78]](#footnote-78) en bovendien voordelen heeft in een (corona-)pandemie.[[79]](#footnote-79) Ten slotte zien **Piet de Vulder** en **Nick Noël** ook een mogelijk voordeel in LFR omdat het toepassen van dergelijke vorm van identificatie ook personeelsbesparend kan zijn.[[80]](#footnote-80)

#### LFR en (niet-) operationele opdrachten

* Bestuurlijke en gerechtelijke opdrachten

De taken van de politie kunnen algemeen worden opgedeeld in **bestuurlijke en gerechtelijke** taken.[[81]](#footnote-81) De **bestuurlijke** opdrachten gaan uit van een preventief oogmerk,[[82]](#footnote-82) zoals de handhaving van de openbare orde, het voorkomen van misdrijven en bescherming van personen en goederen, bijstandverlening aan ieder die in gevaar verkeert, algemeen toezicht en controles op plaatsen waar ze wettelijk toegang toe hebben, verslag uitbrengen en andere maatregelen van bestuurlijke politie[[83]](#footnote-83). De bestuurlijke politie omvat m.a.w. het geheel van opdrachten dat de openbare orde verzekert.[[84]](#footnote-84) Hoewel het begrip “openbare orde” moeilijk te definiëren valt,[[85]](#footnote-85) verwijst men er algemeen mee naar de drie wezenlijke bestanddelen: openbare rust (geen oproer of wanordelijkheden), openbare veiligheid (vermijden van ongelukken of gevaar voor ongelukken aan personen of goederen) en openbare gezondheid (de afwezigheid van ziektes of ziekterisico’s).[[86]](#footnote-86)

LFR kan in deze context voornamelijk preventief worden ingezet om misdrijven te voorkomen, bijvoorbeeld op grote evenementen zoals sport-of muziekwedstrijden[[87]](#footnote-87) of andere massa-bijeenkomsten.[[88]](#footnote-88) Bovendien kan men met LFR in real time monitoren en op heterdaad personen betrappen en identificeren. Daarnaast kan men ook bijvoorbeeld vermiste kinderen opsporen[[89]](#footnote-89) en de luchtvaartpolitie zou er gebruik van kunnen maken bij grenscontroles.[[90]](#footnote-90)

De opdrachten van **gerechtelijke** politie zijn dan weer traditioneel repressief: dit gaat over het opsporen van misdaden, wanbedrijven en overtredingen, de bewijsverzameling…[[91]](#footnote-91) Binnen de gerechtelijke politie-opdrachten biedt LFR de mogelijkheid om personen op te sporen op bestaande opgeslagen camerabeelden.

* Niet-operationele taken

Naast deze categorieën van operationele taken, kent de politie ook enkele **niet-operationele opdrachten**, met betrekking tot werkomstandigheden en arbeidsprestaties van het personeel van politiediensten. Afzonderlijke videobewaking regelt de controle op de werknemers. De regelgeving hierrond dient geregeld te worden in het huishoudelijk reglement van de politiezone of dienst van de federale politie.[[92]](#footnote-92) In die zin valt de controle van het eigen personeel met LFR in politiekantoren ook binnen de bevoegdheden van de politie.

De Directeur van Financiën bij PZ Gent **Bart Schoenmakers** ziet een mogelijk niet-operationeel gebruik van LFR voor de toegangsbeveiliging van bepaalde lokalen.

Bovendien hangen momenteel ook camera’s aan de politiekantoren en de **inkomhal** of het **onthaal** van het politiecommissariaat.[[93]](#footnote-93) **Nele Krols** ziet hierin een eventuele mogelijkheid om LFR te gebruiken ter identificatie van personen die binnenkomen in het politiecommissariaat.[[94]](#footnote-94)

Ook in de **cellen** kunnen camera’s worden gebruikt om te bewijzen dat een opsluiting rustig dan wel problematisch is verlopen. In de eerste plaats heeft dit als doel om gevangenen tegen elkaar te bewaken en te waken over hun gezondheid.[[95]](#footnote-95)

In het kader van dit onderzoek zullen vooral de operationele opdrachten van LFR worden onderzocht.

### Werkwijze van LFR binnen bestuurlijke en gerechtelijke opdrachten

Bij het gebruik van LFR worden de beelden van CCTV-camera’s in real time gestreamed naar het LFR-systeem, waarbij politieambtenaren in een controle-kamer de software monitoren.[[96]](#footnote-96) Zodra er een match is met een persoon op een watchlist, wordt een signaal gegeven en worden zowel het live beeld als het gezicht van de watchlist getoond aan de politieambtenaar.[[97]](#footnote-97) De camerabeelden kunnen hierbij afkomstig zijn van een vaste CCTV-camera of een mobiele camera op een wagen. Het is echter ook mogelijk dat LFR software wordt geïnstalleerd op bodycams.[[98]](#footnote-98) Hieruit blijkt dat er steeds politieambtenaren nodig zijn om te monitoren en als interventie-team in te grijpen in het kader van bestuurlijke opdrachten.

 Zoals hierboven beschreven kan men in het kader van gerechtelijke opdrachten ook LFR gebruiken om achteraf personen te identificeren op camerabeelden van bestaande CCTV-netwerken.

Het onderscheid tussen de hoofdmechanismen van camera’s (heden/verleden/toekomst) en tussen de bestuurlijke en gerechtelijk opdrachten hangt niet samen. Het is immers niet zo dat de gerechtelijke politie enkel repressief gebruik kan maken van camera’s omdat haar taken eerder repressief gericht zouden zijn. In het kader van de bestuurlijke opdrachten hoeft dan weer niet noodzakelijk enkel gebruik te worden gemaakt van de heden-functie van camera’s.

Men kan immers niet altijd een duidelijk onderscheid maken tussen gerechtelijke en bestuurlijke opdrachten,[[99]](#footnote-99) waardoor er niet steeds een concrete afbakening kan worden gemaakt tussen de heden en de verleden-functie van LFR.

Bovenop deze onduidelijk afbakening komt nog eens het proactief gebruik van camera’s.[[100]](#footnote-100) [[101]](#footnote-101) Dit hangt samen met de bijzondere opsporingsmaatregelen die worden omschreven in de BOM-wet.[[102]](#footnote-102) Zulke maatregelen worden gekenmerkt door hun **heimelijk** karakter[[103]](#footnote-103) en hebben een gerechtelijke finaliteit.[[104]](#footnote-104) Ze hebben als doel om daders van misdrijven te vervolgen, en om gegevens en inlichtingen op grond van een redelijk vermoeden van te plegen of reeds gepleegde maar nog niet aan het licht gebrachte strafbare feiten die worden gepleegd (o.a.) in het kader van een criminele organisatie op te sporen, te verzamelen, registreren en verwerken.[[105]](#footnote-105) Een voorbeeld van een bijzondere opsporingsmaatregel is de stelselmatige observatie met een technisch hulpmiddel. Hieronder vallen camera’s, met zicht op een openbare plaats of in een private plaats of met zicht op een woning.[[106]](#footnote-106)

De BOM-wet bepaalt echter dat bijzondere opsporingsmaatregelen zowel binnen het opsporingsonderzoek als binnen een gerechtelijk onderzoek kunnen worden genomen. In die zin kunnen zowel het opsporingsonderzoek als het gerechtelijk onderzoek binnen de proactieve recherche kaderen.[[107]](#footnote-107) Men kan m.a.w. proactief werken zowel binnen bestuurlijke als binnen gerechtelijke opdrachten.

De beelden van een match genereerd door LFR kunnen vervolgens worden bijgehouden of verwijderd.[[108]](#footnote-108)

## Wettelijk kader rond privacy

### Privacy: een moelijk begrip

#### Twee fundamentele rechten: Recht op eerbiediging privéleven[[109]](#footnote-109)/Recht op bescherming persoonsgegevens

Het recht op eerbiediging van het privéleven kwam voor het eerst in het internationale mensenrechtendiscours in 1948 in de **Universele Verklaring voor de Rechten van de Mens.** [[110]](#footnote-110) Vervolgens werd het opgenomen in art. 8 van het **Europees Verdrag Voor de Rechten van de Mens** (Hierna: EVRM)[[111]](#footnote-111) als “Recht op eerbiediging van privé-, familie-, en gezinsleven.” Een beperking van dit recht door een publieke overheid is verboden, behalve wanneer deze in overenstemming is met de wet, een legitiem belang nastreeft en noodzakelijk is in een democratische samenleving.[[112]](#footnote-112)

Toen informatietechnologie zich ontwikkelde en steeds belangrijker werd, groeide de noodzaak om regels aan te nemen om de bescherming van persoonsgegevens van individuen te beschermen.[[113]](#footnote-113) In de EU begonnen in de jaren ’70 verschillende EU- staten de controle op verwerking van persoonsgegevens door publieke overheden en grote bedrijven te reguleren.[[114]](#footnote-114) De Raad van Europa nam in 1981 het **Verdrag 108**[[115]](#footnote-115) aan, dat tot op de dag van vandaag het enige bindende internationale instrument is met betrekking tot de bescherming van persoonsgegevens.[[116]](#footnote-116) Het verdrag heeft betrekking op de verwerking van persoonsgegevens door zowel de publieke als private sector.[[117]](#footnote-117) Recent werd een Aanvullend Protocol aangenomen tot wijziging van het originele verdrag. Vandaag wordt naar de gewijzigde versie verwezen als Gemoderniseerd Verdrag 108 (of Verdrag 108+).[[118]](#footnote-118)

Bij het aannemen van het Handvest van de Grondrechten van de Europese Unie (hierna: HEU) werd naast een recht dat het respect voor privé-en familieleven beschermt[[119]](#footnote-119) ook een afzonderlijk recht ingevoerd, dat de **bescherming van persoonsgegevens** garandeert.[[120]](#footnote-120) Dit wordt gezien als een modern en actief afdwingbaar recht voor de betrokkene wiens gegevens worden verwerkt.[[121]](#footnote-121)

De verwerking van persoonsgegevens kan aanleiding geven tot een schending van het recht op eerbiediging van het privéleven afhankelijk van de specifieke context, maar valt sowieso onder het toepassingsgebied van het recht op bescherming van persoonsgegevens.[[122]](#footnote-122) Er vindt dus veel sneller een inperking plaats van het recht op de bescherming persoonsgegevens dan op het recht op eerbiediging privéleven.

De verwevenheid van beide rechten wordt duidelijk aangetoond in de (belangrijke) zaak *Digital Rights/Ierland* voor het Hof van Justitie.[[123]](#footnote-123) In deze zaak werd de verplichte periode van retentie van data door telecommunicatiediensten aangevochten, die in de toenmalige e-Privacyrichtlijn werd voorgeschreven. Eerst stelt het Hof dat er een inmenging is in het recht op privéleven uit art. 7 HEU, omdat de combinatie van de gegevens geleverd door telecommunicatiediensten kan leiden tot zeer precieze conclusies over iemands **privéleven**.[[124]](#footnote-124) Dit is dus een schending van het recht op eerbiediging privéleven. Vervolgens stelt het Hof dat de retentie van data op zich een **verwerking van persoonsgegevens** vormt, wat dan weer een schending van het fundamenteel recht op bescherming van persoonsgegevens inhoudt.[[125]](#footnote-125)

Dit laatste Europese recht[[126]](#footnote-126) wordt uiteengezet in enkele **Europeesrechtelijke instrumenten**: de Algemene Verordening Gegevensbescherming[[127]](#footnote-127), de Richtlijn Politie en Justitie[[128]](#footnote-128), de e-privacyRichtlijn[[129]](#footnote-129) en Verordening 45/2001, die de verwerking van persoonsgegevens door de EU-instanties en organen verzorgt.[[130]](#footnote-130)

In het kader van deze masterproef zijn voornamelijk de AVG en Richtlijn Politie en Justitie belangrijk, die de uitwerking vormen van art. 8 HEU vormen voor de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens.[[131]](#footnote-131) De Richtlijn Politie en Justitie geldt voor zulke verwerkingen wanneer deze gedaan worden door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.[[132]](#footnote-132)

Op Belgisch niveau worden beide instrumenten overgenomen of omgezet in de Belgische Wet Bescherming Persoonsgegevens.[[133]](#footnote-133)

#### De toets van de gerechtvaardigde schending

Hoewel het ‘moderne’ recht op bescherming persoonsgegevens[[134]](#footnote-134) een apart recht is dat onderscheiden dient te worden van het recht op eerbiediging privéleven [[135]](#footnote-135) in art. 7 en 8 HEU erkent het Hof van Justitie (hierna: HvJ) dat art. 7 en art. 8 HEU gelijkaardige rechten inhouden, nauw aan elkaar **gelinkt** zijn[[136]](#footnote-136) en beiden **gelijkaardige waarden** willen beschermen.[[137]](#footnote-137) Het zijn bovendien beiden grondvoorwaarden voor andere fundamentele mensenrechten, zoals bijvoorbeeld het recht op vrijheid van meningsuiting.[[138]](#footnote-138)

Daarnaast blijkt de verwevenheid van het recht op eerbiediging privéleven en het recht op persoonsgegevens ook uit de rechtvaardigingstoets die **art. 52(1) HEU** voorziet wanneer een inbreuk van een van beide rechten dient te worden beoordeeld. Dit houdt in dat elke beperking van een mensenrecht in het Handvest bij wet voorzien moet zijn, de **wezenlijke inhoud** van de rechten moet eerbiedigen, noodzakelijk moet zijn en aan de Unie erkende doelstellingen van algemeen belang of aan eisen van de bescherming van rechten en vrijheden van anderen beantwoorden.

Bovendien stelt **art. 52(3)** HEU dat het HvJ de rechten die zowel in het EVRM als in het Handvest staan, op een zelfde manier dient te interpreteren. Art. 8 EVRM en art. 7 HEU voorzien bijgevolg in eenzelfde recht op eerbiediging privéleven en zouden dus volgens de interpretatie van het EHRM moeten beoordeeld worden.[[139]](#footnote-139) Art. 8 Handvest heeft echter geen direct equivalent in een artikel van het EHRM. Dit belet niet dat het Hof toch de criteria van art. 8 EVRM in aanmerking mag nemen bij de beoordeling van art. 8 Handvest. Evenmin belet dit dat het EHRM de voorwaarden voor een gerechtvaardigde schending in art. 8 HEU in aanmerking mag nemen.[[140]](#footnote-140) Bovendien vermeldt de Toelichting bij het Handvest[[141]](#footnote-141) dat dit laatste recht gebaseerd is op het Verdrag 108 van de Raad van Europa en art. 8 EVRM.[[142]](#footnote-142) Hieruit volgt dat ook de rechtspraak van het EHRM met betrekking tot art. 8 EVRM in rekening moet worden genomen bij de interpretatie van art. 8 Handvest.

Deze complexe relatie tussen beide rechten heeft tot gevolg dat het HvJ hen in haar rechtspraak m.b.t. gegevensbescherming in onderling verband beoordeelt of verwijst naar rechtspraak van het EHRM bij haar beoordeling.[[143]](#footnote-143) Dit zorgt ervoor dat voor een beoordeling van een schending niet enkel de klassieke drie-stapstoets van het EHRM of enkel de rechtvaardigingstoets uit art. 52 Handvest moet worden gebruikt, maar een onderling verweven toets die bovendien ook Verdrag 108 (+) (waarover het in se geen judiciële supervisie heeft)[[144]](#footnote-144) in rekening neemt en de AVG en Richtlijn Politie en Justitie niet achterwege laat voor de uiteenzetting van art. 8 HEU. Het probleem is dus dat er geen duidelijke proportionaliteitstoets is. De vraag stelt zich **hoe een inbreuk op het recht op bescherming persoonsgegevens en het ermee verweven recht op eerbiediging privéleven** preciesdient te worden beoordeeld?

In de zaak ***Digital Rights/Ireland***werd (ongeveer) dezelfde vraag gesteld in de vorm van een prejudicieel verzoek aan het HvJ.*[[145]](#footnote-145)* Het HvJ maakte in deze zaak echter geen gebruik van de mogelijkheid om enige duidelijkheid te scheppen in de relatie tussen beide rechten en beantwoordde de vraag niet. In deze zaak werd geoordeeld dat de Dataretentierichtlijn die telecombedrijven verplichtte om persoonsgegevens te bewaren voor een zekere periode vernietigd moest worden omdat ze in strijd was met het evenredigheidsbeginsel voorzien in art. 7, 8 en art. 52 HEU.[[146]](#footnote-146) Bijgevolg vond het Hof het verder niet nodig bovenstaande prejudiciële vraag nog te beantwoorden.[[147]](#footnote-147)

Uit de opbouw van haar redenering om tot de ongeldigheid van de Dataretentierichtlijn te besluiten valt ook geen duidelijke lijn te trekken in de vereisten van een duidelijke proportionaliteitstoets: het Hof vermeldt art. 52 (lid 1) HEU,[[148]](#footnote-148) toetst de wezenlijke inhoud van art. 7 HEU[[149]](#footnote-149) en van art. 8 HEU,[[150]](#footnote-150) controleert of er een algemeen belang bestaat[[151]](#footnote-151) en toetst of de inbreuk evenredig is[[152]](#footnote-152) aan de hand van vaste rechtspraak van het HvJ (voor legitieme doelstellingen en niet verder dan geschikt en noodzakelijk).[[153]](#footnote-153) Voor de beoordeling van de discretionaire marge en de minimale vereisten van de maatregel haalt het HvJ dan weer EHRM-rechtspraak aan.[[154]](#footnote-154)

Om aan dit gebrek aan duidelijkheid[[155]](#footnote-155) te verhelpen, werkte de **EDPS** een **stappenplan** dat wetgevers kunnen volgen om aan mensenrechtenvoorwaarden te voldoen.[[156]](#footnote-156) Deze moet worden gelezen in combinatie met de Necessity Toolkit die de EDPS eerder al uitwerkte[[157]](#footnote-157) en andere bestaande richtlijnen van EU-instellingen rond deze beoordelingstoets.[[158]](#footnote-158) Hoewel de EDPS deze richtlijnen van andere organen reeds in rekening nam en bovendien een synthese geeft van voorwaarden uit EHRM-rechtspraak, geeft het zelf aan dat het niet als definitieve proportionaliteitsbeoordeling mag worden beschouwd voor een specifieke maatregel.[[159]](#footnote-159) Het zorgt wel voor een duidelijk en gedetailleerd overzicht van de voorwaarden die een maatregel moet vervullen. [[160]](#footnote-160) [[161]](#footnote-161)

Aangezien van een concrete maatregel met LFR in België momenteel nog geen sprake is, wordt in het kader van deze masterproef niet stap voor stap het plan gevolgd, maar worden doorheen de masterproef de voorwaarden onderzocht waaraan LFR moet voldoen om proportioneel te kunnen worden ingezet.

### De wezenlijke inhoud van beide mensenrechten en andere perspectieven op “privacy”

####  De“wezenlijke inhoud” van privacy: een recht op informationele zelfbeschikking?

In haar beoordeling van een mogelijke schending van het recht op eerbiediging privéleven/recht op bescherming van persoonsgegevens, gaat het HvJ geregeld na of er een inbreuk is op de “**wezenlijke inhoud**” van deze rechten. Art. 52 (1) HEU bepaalt immers dat de wezenlijke inhoud van de rechten en vrijheden moet worden eerbiedigd wanneer rechten in het Handvest worden ingeperkt.

Het feit dat het HvJ gebruik maakt van art. 52(3) HEU om beperkingen van het recht op bescherming persoonsgegevens te beoordelen aan de hand van het recht op eerbiediging privéleven in het EVRM,[[162]](#footnote-162) wijst erop dat het HvJ de beide rechten in zekere zin een zelfde inhoud en reikwijdte toekent.

De vraag is echter wat deze wezenlijke inhoud precies is. Het lijkt terug te gaan op een interpretatie van het begrip “**privacy**”.[[163]](#footnote-163) De invulling van dit begrip, waar de Europese rechtsinstrumenten zich deels op baseerden,[[164]](#footnote-164) stamt uit een uitspraak van het Duitse Grondwettelijk Hof in 1983.[[165]](#footnote-165) Het Hof erkende daarin een “**recht op informationele zelfbeschikking**” dat voortvloeide uit het recht op de menselijke waardigheid en persoonlijkheidsrechten in de Duitse Grondwet.[[166]](#footnote-166)

Het recht op informationele zelfbeschikking berust met andere woorden op de universele en onvervreemdbare menselijke waardigheid.[[167]](#footnote-167) Hoewel het recht de mogelijkheid erkent van individuen om op basis van hun eigen autonomie te kiezen in welke mate ze hun persoonsgegevens kunnen vrijgeven,[[168]](#footnote-168) heeft de wezenlijke inhoud van privacy ook betrekking op de rechten van anderen. Het recht op zelfdeterminatie is immers een grondvoorwaarde voor een democratische samenleving die steunt op de solidariteit tussen burgers.[[169]](#footnote-169)

Hoewel de wezenlijke inhoud van privacy met andere woorden ook een zeker collectief element lijkt te bevatten, kunnen de fundamentele rechten op privacy en bescherming persoonsgegevens in het EVRM en HEU slechts worden ingeroepen door individuele betrokkenen.[[170]](#footnote-170)

#### Relativiteit van de invulling van de wezenlijke inhoud van privacy

Met de opmars van observatie-en monitoring technologieën zoals CCTV en LFR lijkt deze invulling van “privacy” die gebaseerd is op menselijke autonomie **onder druk** gezet[[171]](#footnote-171) omdat ze onvoldoende garanties geeft aan de “privacy” van de gemeenschap. Op die manier brengen technologieën als LFR niet enkel risico’s met zich mee voor het individuele recht op eerbiediging privéleven en het recht op de bescherming van persoonsgegevens, maar ontstaan ook risico’s voor “privacy” als grondvoorwaarde voor een democratische samenleving.[[172]](#footnote-172)

Een van deze risico’s is **mass surveillance**, een begrip dat wordt uitgewerkt door de rechtspraak van het EHRM en het HvJ.[[173]](#footnote-173) Doorheen die rechtspraak ontwikkelen de hoven bepaalde garanties ter bescherming van de “privacy”, die case per case dienen worden toegepast om te bepalen of er sprake is van mass surveillance. Zo bepaalde het HvJ in *Digital Rights/Ireland (en in Schrems I)[[174]](#footnote-174)* voor het eerst enkele modaliteiten die bepalen of een maatregel een inbreuk vormt op de wezenlijke inhoud van deze rechten.[[175]](#footnote-175)

Zo oordeelde het HvJ in die zaak ten eerste dat de retentie van telecommunicatiegegevens geen inbreuk vormde op de **wezenlijke inhoud van het recht op eerbiediging privéleven** omdat de maatregel het niet mogelijk maakte om kennis te nemen van de inhoud van die communicatie en enkel metadata verzamelde.[[176]](#footnote-176) Het HvJ ging met andere woorden uit van een begrip van “privacy” dat meer bescherming biedt aan de inhoud van communicatiegegevens dan aan metadata, zoals de datum, het tijdstip en het uur van de communicatie.[[177]](#footnote-177) Deze aanpak kan echter worden betwist: de retentie van metadata kan immers in verregaande mate (gevoelige) persoonsgegevens vrijgeven. Zo maakt een database met metadata van telecommunicatie het mogelijk om te zien wie allemaal een psycholoog of gespecialiseerde arts heeft gecontacteerd.[[178]](#footnote-178) Bovendien maakt metadata het mogelijk om hele bevolkingsgroepen te catalogiseren, wat niet mogelijk is aan de hand van enkel de inhoud van communicatie.[[179]](#footnote-179)

Hieruit volgt dat het recht op bescherming persoonsgegevens en het recht op eerbiediging privéleven niet in de weg staan aan de retentie van metadata in grote hoeveelheden[[180]](#footnote-180) (big data), die een impact kan hebben op de (collectieve) “privacy” van een bevolkingsgroep. [[181]](#footnote-181)

Ten tweede oordeelde het HvJ in *Digital Rights/Ireland* dat ook de **wezenlijke inhoud van het recht op bescherming persoonsgegevens** niet werd aangetast door de maatregel ter retentie van metadata. De maatregel die voorzag in deze retentie bepaalde immers dat hierbij steeds alle beginselen van gegevensbescherming en-beveiliging moesten worden gerespecteerd.[[182]](#footnote-182) Het HvJ lijkt er hier dan ook van uit te gaan dat de gegevensbeschermingsbeginselen de wezenlijke inhoud van privacy (voldoende) beschermen.

Uit deze uiteenzetting van het HvJ volgt m.a.w. nog geen concrete afbakening van de modaliteiten om de wezenlijke inhoud van “privacy”te toetsen. Door de inhoud van communicatie een hogere bescherming te geven dan metadata, gaat het Hof bij de toets aan de wezenlijke inhoud van het recht op eerbiediging privéleven immers uit van een traditionele individuele opvatting van privacy[[183]](#footnote-183) terwijl privacy ook een collectief aspect lijkt te omvatten.[[184]](#footnote-184)

Dit traditionele uitgangspunt van “privacy” lijkt dan ook een mogelijke verklaring te bieden voor de hierboven beschreven problematiek met de proportionaliteitstoets. Het HvJ lijkt zelf niet goed te weten in welke mate het recht op bescherming persoonsgegevens en het recht op eerbiediging privéleven de wezenlijke inhoud van “privacy” omvatten. Zo geeft het Hof het recht op bescherming persoonsgegevens soms een te minimalistische invulling als zijnde een recht beperkt tot veiligheidsmaatregelen, terwijl het meer is dan enkel dat.[[185]](#footnote-185) Zo oordeelde het zelf dat ook alle gegevensbeschermingsbeginselen moeten worden nageleefd die de uitwerking vormen van het recht op eerbiediging privéleven, het recht op bescherming persoonsgegevens en grondvoorwaarden bieden voor andere fundamentele rechten.[[186]](#footnote-186)

Er wordt door verschillende rechtsgeleerden en ethici dan ook steeds meer gezocht naar deze wezenlijke inhoud van “privacy” en naar manieren om dit begrip werkbaar te maken. Zo wordt nagedacht over een fundamenteel recht op “group privacy”[[187]](#footnote-187) of een uiteenzetting van privacy als “contextuele privacy”, waarbij de mate waarin “privacy” moet worden gegarandeerd afhangt van de concrete context waarin men zich bevindt.[[188]](#footnote-188)

## Welke rechtsinstrumenten zijn van toepassing bij het gebruik van LFR voor politionele doeleinden?

Zoals hieronder zal blijken zijn er verschillende fases die het gebruik van LFR door de politie voorafgaan, zoals de ontwikkelingsfase van LFR en de aankoopfase. Omdat deze een impact hebben op de manier waarop het gebruik van LFR privacy beïnvloedt, worden deze in het kader van deze masterproef ook uiteengezet.

### Toepassingsgebied Richtlijn Politie en Justitie/Algemene Verordening Gegevensbescherming/Wet Bescherming Persoonsgegevens

#### Algemene Verordening Persoonsgegevens

De **AVG** is van toepassing op elke geheel of gedeeltelijk geautomatiseerde verwerking en op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen (materieel toepassingsgebied).[[189]](#footnote-189) De verordening geldt voor iedere verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie (personeel toepassingsgebied), ongeacht of de verwerking al dan niet in de Unie plaatsvindt.[[190]](#footnote-190)

Bovendien is de verordening ook van toepassing op verwerkingen door niet in de EU gevestigde verwerkingsverantwoordelijken of verwerkers wanneer de verwerking gegevens inhoudt van betrokkenen in de EU en de verwerking verband houdt met het aanbieden van goederen of diensten aan betrokkenen in de EU of het monitoren van gedrag in de EU van de betrokkene (territoriaal toepassingsgebied).[[191]](#footnote-191) Dit is een relevante bepaling voor LFR, gezien de bedrijven die LFR verkopen aan politie niet noodzakelijk in de EU gevestigd zijn. Een bedrijf als Clearview AI dat LFR maakt en haar software aanbiedt aan overheden in de EU is zelf gevestigd in de Verenigde Staten.[[192]](#footnote-192)

Door deze ruime werking van het toepassingsgebied van de AVG lijken bedrijven die LFR ontwikkelen en daarbij persoonsgegevens verwerken (van betrokkenen in de EU) **in principe** te moeten voldoen aan de beginselen in de AVG. Doorheen deze masterproef wordt de relativiteit van dit principe echter **in vraag gesteld** omdat verschillende bepalingen uit de AVG niet afgestemd lijken op software-ontwikkelaars.[[193]](#footnote-193)

#### Richtlijn Politie en Justitie

De **Richtlijn Politie en Justitie** is dan weer van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten (personele toepassingsgebied) met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. (materiële toepassingsgebied).[[194]](#footnote-194)

Tot die bevoegde autoriteiten behoren volgens de Belgische Wet Bescherming Persoonsgegevens (hierna: WBP) de **politiediensten**,[[195]](#footnote-195) zijnde de federale politie en de korpsen van de lokale politie.[[196]](#footnote-196) Bovendien behoren ook de **gerechtelijke overheden**, zoals de hoven en rechtbanken en het openbaar ministerie hiertoe.[[197]](#footnote-197) In het kader van LFR is dit relevant voor de identificaties verkregen via LFR die dienen als bewijs in gerechtelijke procedures. Gerechtelijke overheden zullen dus aan dezelfde beginselen qua bescherming van persoonsgegevens moeten voldoen als politiediensten.[[198]](#footnote-198)

#### Onderscheid tussen AVG en Richtlijn Politie en Justitie

Zoals verder wordt uiteengezet, ontstaan door het mogelijke gebruik van LFR in een politionele context onduidelijkheden in het onderscheid tussen de AVG en de Richtlijn Politie en Justitie. Hoewel de WBP zowel de AVG als de Richtlijn Politie en Justitie integreert, is er een verschil in de mate waarin de basisbeginselen van gegevensbeschermingsrecht en de rechten van betrokkenen worden ingevuld. Dit verschil is afhankelijk van het onderscheid tussen Titel 1,[[199]](#footnote-199) dan wel van Titel 2 WBP dat van toepassing is op verwerkingen voor politionele doeleinden.[[200]](#footnote-200)

Dit blijkt vooral bij de voorwaarde van **privacy by design** een probleem te vormen.[[201]](#footnote-201)

#### Wet Bescherming Persoonsgegevens

Op nationaal niveau vormt de WBP de **implementatie** van zowel de AVG als van de Richtlijn Politie en Justitie. Het toepassingsgebied van deze wet omvat dus zowel politionele[[202]](#footnote-202) als niet-politionele verwerkers.[[203]](#footnote-203) Bovendien omvat de WBP ook **inlichtingen-en veiligheidsdiensten** terwijl zowel de AVG als de Richtlijn Politie en Justitie deze uitsluiten van hun toepassingsgebied.[[204]](#footnote-204) Door deze diensten onder de WBP te brengen,[[205]](#footnote-205) ontstaat een vervagend onderscheid tussen politiediensten en inlichtingendiensten.[[206]](#footnote-206) In het kader van deze masterproef zal enkel het gebruik van LFR door politiediensten worden besproken.

Het personele toepassingsgebied van de Richtlijn Politie en Justitie beperkt zich echter niet tot de bevoegde overheden belast met het opsporen, voorkomen en vervolgen van strafbare feiten,[[207]](#footnote-207) maar strekt ook tot andere autoriteiten die openbaar gezag uitoefenen.[[208]](#footnote-208)

In Belgische context worden de bevoegde autoriteiten bedoeld in de Richtlijn Politie en Justitie opgelijst in de Wet Bescherming Persoonsgegevens.[[209]](#footnote-209) De vraag stelt zich of deze **autoriteiten** LFR zouden kunnen gebruiken voor de doeleinden bepaald in het materiële toepassingsgebied onder dezelfde voorwaarden als wanneer de politiediensten dit zouden mogen.

### Politioneel kader: Camerawet/Wet op het Politieambt

De garanties van gegevensbescherming vloeien nog verder voort in verschillende nationale wetten. Zo worden verschillende beginselen van gegevensbescherming geïntegreerd in de **camerawetten**: de Wet op het Politieambt[[210]](#footnote-210) die het gebruik regelt van politiecamera’s en de Camerawet van 21 maart 2007[[211]](#footnote-211) die het gebruik regelt van alle andere camera’s, zoals de inzet van camera’s door gemeenten, particulieren en ondernemingen.[[212]](#footnote-212)

Een eerste manier om camera’s in te delen is aan de hand van de drie categorieën plaatsen waar gefilmd mag worden. Een eerste categorie is de **niet-besloten** plaats die vrij toegankelijk is voor het publiek.[[213]](#footnote-213) Een tweede is de voor het publiek **toegankelijke** **besloten** plaats die wordt afgebakend door een omsluiting maar bestemd is voor het gebruik door het publiek waar diensten worden verstrekt.[[214]](#footnote-214) Ten laatste is er de **niet voor het publiek toegankelijke** **besloten** plaats: hieronder valt elk gebouw of door een omsluiting afgebakende plaats uitsluitend bestemd voor het gebruik door gewoonlijke gebruikers.[[215]](#footnote-215) Het onderscheid tussen deze verschillende toepassingen is zeer relevant gezien het Voorstel voor Verordening rond AI uitdrukkelijk het gebruik van LFR in “publieke ruimtes” uitsluit.[[216]](#footnote-216)

Hierbij is de definitie van EDRi (European Digital Rights) relevant om te vermelden. EDRi baseert zich op de definitie van UNESCO[[217]](#footnote-217) waar het ook online plaatsen aan toevoegt. Naast online plaatsen vallen volgens EDRi ook de volgende plaatsen onder het begrip “**publieke ruimtes**”: straten, parken, hospitalen, private eigendommen die publiek toegankelijk zijn zoals winkelcentra, stadia, openbaar transport en andere plaatsen waar diensten worden geleverd van openbaar belang.[[218]](#footnote-218) Hoewel de Belgische beleidsmaker reeds een duidelijke afbakening maakt in categorieën van puliek plaatsen waar camera’s kunnen worden geplaatst, lijkt het relevant om te blijven evalueren wat precies wordt verstaan onder “publiek.”

Een tweede belangrijk indeling van camerabewaking is het **zichtbaar** en het niet- zichtbaar gebruik van camera’s. Zichtbare camera’s worden steeds aangegeven met een pictogram.[[219]](#footnote-219) Niet-zichtbare camera’s zijn niet kenbaar voor de burger. Dit zijn bijvoorbeeld ANPR- camera’s op anonieme politievoertuigen.[[220]](#footnote-220) Niet-zichtbaar gebruik van camera’s is slechts mogelijk in enkele omstandigheden voor zowel gerechtelijke als bestuurlijke opdrachten,[[221]](#footnote-221) zoals bij de voorbereiding van acties van gerechtelijke politie of bij handhaving van de openbare orde tijdens deze acties.[[222]](#footnote-222)

Het heimelijk gebruik van camera’s is dan weer een bijzondere opsporingsmethode die wordt geregeld in de BOM-wet en het wetboek van strafvordering.[[223]](#footnote-223)

Het zal m.a.w. belangrijk zijn om de locatie en zichtbaarheid van het gebruik van LFR duidelijk af te bakenen in mogelijke wetgeving.

### Belangrijke begrippen en actoren

#### Verwerking

Opdat het gegevensbeschermingsrecht van toepassing is, dient er eerst een verwerking te zijn.[[224]](#footnote-224) Een **verwerking** is “de bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.”[[225]](#footnote-225) De bescherming van persoonsgegevens geldt voor “de geheel of gedeeltelijk geautomatiseerde” verwerking, wat betekent dat de gegevens worden verwerkt met behulp van een computer, mobile device of router.[[226]](#footnote-226)

Zowel in de fase van ontwikkeling[[227]](#footnote-227) als in de gebruiksfase van LFR gebeuren een hele reeks verwerkingen.[[228]](#footnote-228)

#### (Biometrische) persoonsgegevens

Een **persoonsgegeven** is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.[[229]](#footnote-229) Op basis van deze definitie kunnen ook metadata zoals locatie- en tijdgegevens als persoonsgegevens kwalificeren indien deze het mogelijk maken een individu direct of indirect te identificeren. [[230]](#footnote-230)

Het arrest ***Lindqvist***zorgde hierbij voor een lage drempel van “identificeerbaarheid”, waardoor metadata snel als persoonsgegevens kunnen kwalificeren en ook zelfs werkomstandigheden of persoonsgegevens kunnen uitmaken.[[231]](#footnote-231) Om te beoordelen of metadata kwalificeren als persoonsgegevens moet rekening worden gehouden met de redelijke mogelijkheid om op basis van de stand van de technologie (en alle objectieve factoren) de persoon te identificeren.[[232]](#footnote-232) Zoals hierboven beschreven kan de verwerking van dergelijke metadata een grote impact hebben op privacy, hoewel dit als dusdanig niet steeds zo wordt erkend.[[233]](#footnote-233)

Een **bijzondere categorie** van persoonsgegevens zijn de “gevoelige” persoonsgegevens waaruit onder meer ras, etnische afkomst, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijk persoon en gezondheidsgegevens kunnen worden afgeleid.[[234]](#footnote-234) Deze soorten persoonsgegevens behoren omwille van hun gevoeligheid tot een bijzondere categorie die een hogere bescherming vereist.[[235]](#footnote-235) De vraag is in welke mate bijvoorbeeld een camerabeeld dat een donkere huidskleur toont een rasgegeven uitmaakt en een camerabeeld dat een brildrager toont een gezondheidsgegeven uitmaakt.[[236]](#footnote-236)

De biometrische persoonsgegevens die tot deze categorie behoren hebben betrekking op fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk persoon, resulteren uit een specifieke technische verwerking en hebben tot doel om een natuurlijk persoon te identificeren.[[237]](#footnote-237)

Wanneer een verwerkingsverantwoordelijke zoals een software-ontwikkelaar zulke persoonsgegevens wil verwerken bij het **ontwikkelen** van software moet die daarvoor een duidelijke rechtsgrond in de AVG kunnen aanduiden.[[238]](#footnote-238) Zoals hieronder zal blijken bestaan echter onduidelijkheden over welke rechtsgrond kan worden gebruikt in de ontwikkelingsfase en over de vraag of het wel aan de ontwikkelaar zelf is om een rechtsgrond in te roepen.[[239]](#footnote-239)

In de **gebruiksfase** van LFR is een verwerking van zulke gevoelige persoonsgegevens door de politie volgens de Richtlijn Politie en Justitie dan weer enkel toegelaten indien het toegestaan is bij Unierecht of lidstatelijk recht, noodzakelijk is om de vitale belangen van de betrokkene of andere natuurlijke persoon te beschermen of indien die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.[[240]](#footnote-240) De vraag is welke rechtsgrond politiediensten kunnen inroepen om de verwerking van gevoelige persoonsgegevens door LFR op te baseren.[[241]](#footnote-241)

#### Verwerkingsverantwoordelijke

##### In de ontwikkelingsfase

De verwerkingsverantwoordelijke (hierna: VWV) is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoons­gegevens vaststelt.[[242]](#footnote-242)

In eerste instantie lijkt de ontwikkelaar dus VWV wanneer hij persoonsgegevens verwerkt bij het ontwikkelen van LFR-software, gezien hij het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt voor de specifieke verwerkingen in het ontwikkelingsproces.[[243]](#footnote-243) Het is echter onduidelijk wat precies dat doel is waarvoor de ontwikkelaar persoonsgegevens ontwikkelt. Moet dit doel gezien worden als het doel van de ontwikkelaar om software te ontwikkelen voor de latere verkoop ervan of dient het latere gebruik van de software voor politionele operationele opdrachten als doel voor de ontwikkelaar?[[244]](#footnote-244)

In een poging om hierop een antwoord te geven, stelt de Raad van Europa in haar Recommendation “Unboxing Artificial Intelligence: 10 steps to protect Human Rights” dat alle AI die in de private sector wordt ontwikkeld aan dezelfde standaarden moet voldoen als die ontwikkeld in de publieke sector zodra er een intentie is om te werken met publieke entiteiten.[[245]](#footnote-245) Hieruit volgt dat de ontwikkelaar software moet ontwikkelen die voldoet aan de standaarden voor LFR in de gebruiksfase, wanneer software wordt ontwikkeld met het oog op later gebruik ervan in de publieke sector (hier: voor politionele doeleinden). In deze interpretatie is het dus niet de ontwikkelaar die het uiteindelijke doel van de verwerking bepaalt, maar de politiedienst die beslist hoe en voor welke doeleinden LFR persoonsgegevens zal verwerken.

Men kan zich bijgevolg afvragen in welke mate de ontwikkelaar kan gezien worden als VWV in de zin van de AVG. **Peter van Schelven**[[246]](#footnote-246) is van mening dat software-ontwikkelaars door de mazen van het net glippen omdat de verplichtingen in de Europese rechtsinstrumenten uitsluitend gericht zouden zijn op de eindgebruiker van technologie en niet op de ontwikkelaars ervan.

##### In de gebruiksfase

Het begrip “**bevoegde overheid**” dat wordt gebruikt om het personele toepassingsgebied van gegevensbeschermingsinstrumenten af te bakenen dient te worden onderscheiden van het begrip “**VWV**”.[[247]](#footnote-247) De VWV is immers de bevoegde autoriteit die de doeleinden van en de middelen voor de verwerking van persoonsgegevens met LFR vaststelt.[[248]](#footnote-248)

Binnen de gebruiksfase van LFR ontstaat onduidelijkheid in de wet over wie de **VWV** precies is.[[249]](#footnote-249) Het COC zet dit begrip uiteen als een functioneel begrip “bedoeld om verantwoordelijkheden te leggen op de plaats waar de **feitelijke invloed** ligt.”[[250]](#footnote-250) Dit wil zeggen dat de entiteit die beslist over het “hoe” en “wat” van de gegevensverwerking volgens het COC de VWV is “onafhankelijk van de status, de positie of het statuut die deze entiteit binnen diens organisatie is toebedeeld.”[[251]](#footnote-251)

Dit wil echter niet zeggen dat de **specifieke politieambtenaar** die LFR hanteert, zal kwalificeren als VWV. Het COC stelt immers dat er bij het definiëren van het begrip “VWV” best een onderscheid wordt gemaakt tussen het materieel politierecht en het gegevensbeschermingsrecht omdat deze andere doelstellingen beogen. Ze moeten samen worden gelezen om de functie van VWV te bepalen.

Hieruit volgt dat dit voor de bijzondere en lokale technische gegevensbank, (waarvan de aanleg noodzakelijk is voor het gebruik van LFR)[[252]](#footnote-252) steeds de korpschef zal zijn.[[253]](#footnote-253)

**Nick Noël** geeft aan dat bij het bepalen van een VWV bij ANPR-camera’s in de praktijk ook onduidelijkheden bestaan. Hoewel in vele gevallen de korpschef de feitelijke en wettelijke verantwoordelijke van de verwerking is, komt het geregeld voor dat hij zelfs niet op de hoogte is van het bestaan van een camera die geplaatst werd door de gemeente.[[254]](#footnote-254) De wettelijke vereiste voor de gemeente om advies te vragen bij het plaatsen van een nieuwe camera wordt volgens **Nick Noël** immers niet steeds vervuld, waardoor het mogelijk is dat de korpschef niet op de hoogte is van het bestaan van bepaalde camera’s. **DPO bij PZ Antwerpen Nele Krols** voegt daaraan toe dat ook onduidelijkheid bestaat over de verwerkingsverantwoordelijkheid voor de ANPR-camera’s bij de uitrol van het nieuwe Cameraschild.[[255]](#footnote-255) Dit Cameraschild koppelt de lokale ANPR- camera’s aan een algemene nationale gegevensbank met ANPR-gegevens en doet de vraag rijzen: is de federale politie VWV wanneer lokale camera’s beelden opnemen die naar de algemene gegevensbank worden verzonden of is het de lokale politie omdat die gebruik maakt van de lokale camera’s?

Daarnaast is er ook de vraag of **eigenaarschap** van de camera een bepalende factor is voor wie VWV is. Hoewel de civielrechtelijke eigenaarschap in se niet bepalend is voor de kwalificatie als verwerkingsverantwoordelijkheid kan men zich afvragen of de financiering van lokale politiezones door gemeenten geen impact heeft op het bepalen van het doel en de middelen van de verwerkingen met die camera.[[256]](#footnote-256) [[257]](#footnote-257) In welke mate speelt er in zo’n geval een **gezamenlijke** verwerkingsverantwoordelijkheid?[[258]](#footnote-258)

De onduidelijkheid in dit vraagstuk rond wie de VWV is bij technologieën die reeds door de politie worden ingezet is erg relevant voor LFR, gezien LFR-software kan geïnstalleerd worden op CCTV-camera’s, ANPR-camera’s, bodycams en mogelijks op drones.[[259]](#footnote-259)

#### Verwerker

Een ander belangrijk begrip is dat van de **verwerker**. (hierna: VW) Dit is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de VWV persoonsgegevens verwerkt.[[260]](#footnote-260)

##### In de ontwikkelingsfase

Wanneer een ontwikkelaar persoonsgegevens verwerkt in opdracht van de politiedienst zou hij kunnen worden beschouwd als VW die in opdracht van de politiedienst persoonsgegevens[[261]](#footnote-261) verwerkt om software te ontwikkelen die gebruikt zal worden voor politionele doeleinden.[[262]](#footnote-262) Het is dan de politiedienst die als eindgebruiker het doel en de middelen bepaalt van de uiteindelijke verwerkingen met LFR en deze kwalificeert dus als VWV. De ontwikkelaar zal dan handelen volgens de instructies van de VWV,[[263]](#footnote-263) die worden vastgelegd in een **verwerkersovereenkomst**.[[264]](#footnote-264) Uit deze overeenkomst volgt dat de verwerker zelf voldoende garanties moet kunnen bieden opdat de vereisten van de Richtlijn Politie en Justitie zijn voldaan.[[265]](#footnote-265)

Zoals hierboven werd gesteld, is niet steeds duidelijk of de ontwikkelaar kwalificeert als **VWV** binnen het toepassingsgebied van de AVG of niet. Indien dit wel het geval zou zijn, betekent dat dat de ontwikkelaar als VWV aan de verplichtingen in de AVG[[266]](#footnote-266) dient te voldoen en als VW aan de verplichtingen voor verwerkers binnen de Richtlijn Politie en Justitie.[[267]](#footnote-267) Aangezien deze verplichtingen niet volledig gelijklopen,[[268]](#footnote-268) stelt zich de vraag aan welke vereisten met betrekking tot gegevensbescherming de ontwikkelaar precies dient te voldoen.

##### In de gebruiksfase

Het begrip verwerker is bovendien ook van belang in de gebruiksfase, aangezien politiediensten naast camerabeelden van politie-camera’s ook toegang kunnen krijgen tot beelden van **particuliere** camera’s.[[269]](#footnote-269)

Wanneer particulieren bewakingscamera’s installeren, moeten ze die **aangegeven** bij de politie,[[270]](#footnote-270) zodat de politie vervolgens beelden kan opvragen in het kader van haar gerechtelijke of bestuurlijke opdrachten.[[271]](#footnote-271) Vervolgens worden deze camera’s in het cartografisch systeem “CamElia” opgenomen. Dit systeem is echter niet accuraat en laat niet toe om te controleren in welke mate deze camera’s wettelijk zijn geplaatst.[[272]](#footnote-272)

In de context van mogelijke toepassing van LFR, zou de politie enerzijds beelden kunnen opvragen om vervolgens op die beelden personen te gaan identificeren met LFR in het kader van haar gerechtelijke taken.[[273]](#footnote-273) Anderzijds zou het ook mogelijk zijn om bewakingscamera’s van ondernemers in real time te verbinden met politiediensten mits een samenwerkingsovereenkomst werd gesloten.[[274]](#footnote-274)

Dit is erg relevant, gezien ondernemingen zoals De Lijn en verschillende voetbalstadia zelf LFR gebruiken.[[275]](#footnote-275) Op die manier kan de politie gebruik maken van LFR wanneer zij zulke camerabeelden opvragen of live monitoren.

De vraag is in welke mate particulieren kwalificeren als VW van de verwerking met LFR voor politionele doeleinden. Een mogelijke kwalificatie van de particulier als verwerker kan namelijk consequenties hebben voor de verwerker m.b.t. verantwoordelijkheid en verplichtingen van gegevensbescherming.[[276]](#footnote-276) De Wet op het Politieambt stelt echter duidelijk dat het gebruik van camera’s gebeurt op beslissing en onder de verantwoordelijkheid van de politieambtenaar, die waakt over de naleving van de proportionaliteits-en subsidiariteitsbeginselen.[[277]](#footnote-277) De vraag is of en in welke mate de particulier precieze verplichtingen heeft naast de verplichtingen van de politieambtenaar om bij het gebruik van LFR privacyvoorwaarden te respecteren.

### Toezichthoudende overheden

De AVG en Richtlijn Politie en Justitie vereisen elk dat een onafhankelijke overheidsinstantie toezicht houdt op de toepassing van deze rechtsinstrumenten.[[278]](#footnote-278) In België bestaan verschillende entiteiten die deze rol op zich nemen.

#### Controleorgaan op de Politionele Informatie (COC)

Zo is er het Controleorgaan op de Politionele Informatie (COC), dat bevoegd is voor de controle op de bescherming van persoonsgegevens door de rechtshandhaving.[[279]](#footnote-279) Het COC is ten eerste belast met de politionele **informatiehuishouding**[[280]](#footnote-280) en met de **controle** van de verwerking van de operationele informatie persoonsgegevens, inclusief de bestaande politionele gegevensbanken en de gemeenschappelijke gegevensbanken terrorisme en extremisme.[[281]](#footnote-281)

Ten tweede is het de **gegevensbeschermingsautoriteit voor de geïntegreerde politie**en houdt het toezicht op de toepassing van titel II GBW ten aanzien van de politie, de Algemene Inspectie van de Federale en de Lokale Politie (AIG) en de passagiers informatie-eenheid.[[282]](#footnote-282)

Ten derde krijgt het opdrachten door of krachtens andere wetten verleend. Hierdoor is het bijvoorbeeld bevoegd voor de regels inzake het zichtbaar en niet-zichtbaar gebruik van camera’s door politiediensten.[[283]](#footnote-283)

Ten slotte ziet het ook toe op gegevensbescherming bij niet-operationele opdrachten door politie.[[284]](#footnote-284) Hierbij dient opgemerkt te worden dat personeelszaken onder de AVG vallen en niet onder de Richtlijn Politie en Justitie.[[285]](#footnote-285)

Het COC benadrukt dat het naast elementen van privacy en gegevensbescherming ook aandacht heeft voor elementen als **efficiëntie en effectiviteit** van het politieoptreden en dus steeds in haar publicaties een gepaste belangenafweging maakt tussen beide aspecten.[[286]](#footnote-286)

#### Gegevensbeschermingsautoriteit

De **Gegevensbeschermingsautoriteit** (hierna: GBA) is dan weer de algemeen bevoegde autoriteit voor het toezicht op de naleving van de grondbeginselen van de bescherming van de persoonsgegevens, in het kader van de Wet tot Oprichting Gegevensbeschermingsautoriteit en van de wetten die bepalingen bevatten inzake de bescherming van de verwerking van persoonsgegevens.[[287]](#footnote-287) De GBA is bevoegd wanneer geen andere wet anders bepaalt en heeft dus een residuaire bevoegdheid.[[288]](#footnote-288) De controle op het politioneel cameragebruik valt niet binnen de bevoegdheid van de GBA, maar van het COC. [[289]](#footnote-289)

Aangezien het echter niet altijd gemakkelijk is een onderscheid te maken in het toepassingsgebied van de AVG of de Richtlijn Politie en Justitie[[290]](#footnote-290) zijn de bevoegdheden tussen het COC en de GBA soms moeilijk te onderscheiden.[[291]](#footnote-291) Zo is de vraag of de fase van ontwikkeling van LFR door private ontwikkelaars onder de bevoegdheid van de GBA of onder die van het COC valt. Het is immers niet duidelijk of de ontwikkelaar die LFR ontwikkelt om dit te verkopen aan politie bij de ontwikkeling van de software rekening moet houden met de voorwaarden uit de AVG of die uit de Richtlijn Politie en Justitie.[[292]](#footnote-292)

#### Andere

Daarnaast zijn er nog het **Comité I** en het **Comité P.** Comité I is aangewezen als gegevensbeschermingsautoriteit belast met de controle van de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten en hun verwerkers.[[293]](#footnote-293) Binnen dat kader ziet het toe op de verwerking van gegevens voor de ‘nationale veiligheid.”[[294]](#footnote-294) Bovendien is het samen met het COC bevoegd voor de controle op de gemeenschappelijke gegevensbanken “terrorist fighters en haatpropagandisten”*.*[[295]](#footnote-295) In het geval hier m.o.o. de regulering van LFR een wijziging gebeurt aan deze databanken zullen bijgevolg zowel het COC als het Comité I hun toestemming hiervoor moeten geven.[[296]](#footnote-296) Het Comité P houdt toezicht op alle mogelijke politiediensten. Samen met het Comité I deelt het een verantwoordelijkheid voor de gegevensbescherming bij verwerkingen door het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en zijn verwerkers.[[297]](#footnote-297)

Naast deze federale toezichthouders zijn er nog enkele **deelstatelijke** actoren: zo is er de Vlaamse Toezichtscommissie (hierna: VTC),[[298]](#footnote-298) de Brusselse Controlecommissie en de Commission Wallonie-Bruxelles de contrôle des échanges de données.[[299]](#footnote-299) De VTC is in principe verantwoordelijk voor het toezicht op de toepassing van de AVG door de Vlaamse bestuursinstanties en is dus niet bevoegd voor de private sector.[[300]](#footnote-300)

Samengevat zijn er dus verschillende mogelijke toezichtsautoriteiten betrokken bij de controle op gegevensverwerking door LFR bij gebruik door de politie, wat kan leiden tot een onduidelijke **bevoegdheidsverdeling** in het toezicht ervan.

Ten slotte is het belangrijk om te vermelden dat de toezichtsautoriteiten van verschillende lidstaten onderbemand zijn en te weinig financiering krijgen.[[301]](#footnote-301) Het COC bestaat bijvoorbeeld uit een beperkt aantal leden: een voorzitter/magistraat, een lid-raadsheer/parketmagistraat en een lid-raadsheer/deskundige. Daarnaast is er een Dienst Onderzoeken met twee leden afkomstig van de politie en een deskundige en een Dienst Steun met éen jurist, éen informaticus en éen directie-assistent.[[302]](#footnote-302) Hieruit blijkt dat men dus prioriteiten moet stellen wegens de kleine bemanning van de organisatie.[[303]](#footnote-303)

**Frank Schuermans**[[304]](#footnote-304) geeft aan dat hij het belangrijk vindt dat men bij het COC bij het uitvoeren van opdrachten kan samenwerken met politiemensen omdat zij weten hoe de dagdagelijkse processen lopen en enkel zij de systemen, applicaties en software kennen of bronnen binnen de politie hebben die externen niet kunnen hebben. Dit wijst weer op de afweging die het COC maakt tussen gegevensbescherming en effectiviteit en veiligheid.

## Vraagstuk rond de rechtsgrond van LFR in België

### Het debat rond LFR: is er nood aan een wettelijke basis?

Ongeacht of men voor of tegen het gebruik van LFR voor politionele doeleinden is, bleken alle respondenten bij het afnemen van de interviews het eens dat er nood is aan een wettelijk kader.

In het maatschappelijk debat hierrond dient echter een duidelijk **onderscheid** te worden gemaakt tussen de vraag of LFR gebruikt mag worden tout court en het debat rond de proportionaliteit van een mogelijk wettelijk kader.

Deze eerste vraag naar de **maatschappelijke wenselijkheid** rond LFR werd reeds (in beperkte mate) in het Belgisch federaal parlement besproken. In een voorstel van resolutie voor een driejarig moratorium op het gebruik van gezichtsherkenningssoftware stelden Écolo, Groen en Défi in 2020 de vraag: “Willen we dat met AI uitgeruste software adviezen uitbrengt of zelfs beslissingen neemt in hoogst heikele aangelegenheden als gezondheid, openbare veiligheid, justitie of migratie?”[[305]](#footnote-305) De positie van de initiatiefnemende partijen is met het voorgestelde moratorium dan ook duidelijk “nee”.

Naast dit wetsvoorstel wordt gezichtsherkenning in de parlementaire stukken voorlopig enkel vermeld in het kader van de mogelijke uitgaven van de begroting waarbij minister Verlinden zoals eerder vermeld eerst het onderzoek van de federale politie naar de mogelijkheden van biometrische technologieën afwacht alvorens het debat rond de wenselijkheid van LFR te willen voeren.[[306]](#footnote-306)

Binnen de respondenten binnen dit onderzoek stelde **Ella Jakubowska**[[307]](#footnote-307)erg duidelijk dat het gebruik van LFR niet wenselijk is en zij is dan ook voor een permanent verbod dat LFR verbiedt. Lid-Raadsheer bij het COC **Frank Schuermans** vindt dat een verbod of moratorium te overwegen valt, maar stelt dat er eerst een uitgebreid parlementair debat over moet worden gevoerd.

**Anke Stakenborg**[[308]](#footnote-308) vindt dan weer dat er eerst een wettelijk kader moet zijn dat proefprojecten met LFR mogelijk maakt alvorens er een debat kan worden gevoerd over de wenselijkheid en mogelijke toepassing van LFR voor operationele doeleinden.

Vanuit het idee dat het nodig is een zicht te krijgen op de vraag of en in welke mate proportioneel gebruik van LFR mogelijk is alvorens een duidelijk standpunt kan worden ingenomen over de wenselijkheid van LFR in de maatschappij, biedt deze masterproef een overzicht van de vraagstukken in deze proportionaliteitsbeoordeling.

### Is er een wettelijke basis?

#### Huidige Voorstel van Verordening rond AI

De EC acht de EU **bevoegd** om een Verordening rond AI uit te vaardigen op grond van art. 114 van het verdrag van de werking van de Europese Unie (hierna: VWEU),[[309]](#footnote-309) wat betekent dat het harmonisatiemaatregelen kan nemen rond het functioneren van de interne markt.[[310]](#footnote-310) Op die manier zou de EU regels kunnen vaststellen rond de ontwikkeling, het op de markt plaatsen en het gebruik van producten die AI-systemen gebruiken[[311]](#footnote-311) en probeert de EU enkele problemen te remediëren.[[312]](#footnote-312)

Bovendien baseert het zich ook op art. 16 VWEU, op grond waarvan de EU de bevoegdheid heeft om regels vast te stellen rond gegevensbescherming.[[313]](#footnote-313)

In het voorstel verklaart de EC dat een **risk-based approach** moet worden gevolgd om een onderscheid te maken tussen gebruik van AI-systemen dat 1) een onaanvaardbaar risico, 2) een hoog risico en 3) een laag of minimaal risico vormt.[[314]](#footnote-314) Het gebruik van AI-systemen die een onaanvaardbaar risico inhouden, worden verboden.

De EC meent dat het gebruik van AI-systemen als “remote biometric identification” van personen in publiek toegankelijke ruimtes een **hoog risico** inhouden.[[315]](#footnote-315) Dit omvat zowel het in real time filmen met LFR als de analyse van camerabeelden met LFR achteraf.[[316]](#footnote-316) Het voorstel verbiedt in het bijzonder het gebruik van zulke biometrische identificatie in real time voor rechtshandhaving, tenzij in zeer beperkte uitzonderingen.[[317]](#footnote-317)

#### Aan welke voorwaarden dient een rechtsgrond te voldoen?

Opdat een inbreuk gerechtvaardigd is en LFR in België dus zou kunnen worden toegepast, dient er in de eerste plaats een **rechtsgrond** te zijn in het Belgische recht die de maatregel voorziet.[[318]](#footnote-318) Gezien hier de voorwaarden van het EHRM in rekening moeten worden genomen,[[319]](#footnote-319) moet de rechtsgrond toegankelijk zijn en voorzienbaar. Omdat het gebruik van LFR als surveillancemaatregel kwalificeert,[[320]](#footnote-320) stelt het EHRM uitdrukkelijk dat de rechtsgrond voldoende duidelijk moet zijn.[[321]](#footnote-321)

Dat er een wettelijke basis nodig is, vloeit bovendien voort uit artikels 8 Richtlijn Politie en Justitie, 11 Richtlijn Politie en Justitie en artikels 34 en 35 WBP die voorzien dat er Unierechtelijk of lidstatelijk recht voorhanden moet zijn opdat een bevoegde overheid gevoelige persoonsgegevens mag verwerken obv **geautomatiseerde besluitvorming**.[[322]](#footnote-322)

#### Voldoende aan het bestaande wettelijke kader als rechtsgrond voor LFR?

##### “Wettelijk kader”

In de eerste rechtszaak over LFR diende de **High Court of Justice** in het Verenigd Koninkrijk te oordelen over de vraag of het bestaande wetgevende kader voldoende was om als wettelijke basis te dienen voor het gebruik van LFR.[[323]](#footnote-323) Dit kader bestond uit de nationale Data Protection Act, Surveillance Camera Code of Practice en beleidsdocumenten van de politie die cumulatief als rechtsgrond werden beschouwd voor het gebruik van LFR,[[324]](#footnote-324) dat op verschillende plaatsen in het VK werd getest.[[325]](#footnote-325) De rechter besloot dat er **geen nood was aan nieuwe wetgeving** in verband met gezichtsherkenning,[[326]](#footnote-326) maar in de aanleg van de Court of Appeal werd dit enigszins herroepen.[[327]](#footnote-327)

In België oordeelde het COC in haar rapport over het proefproject in Zaventem dat het gebruik van LFR **strijdig** was met de Wet op het Politieambt en het oordeelde op basis daarvan dat het project diende te worden stilgelegd.[[328]](#footnote-328) Wanneer de politie nieuwe technologieën wenst in te zetten is het volgens het COC haar **verantwoordelijkheid om de juiste juridische basis aan te duiden**.[[329]](#footnote-329) De vraag is in welke mate er reeds een rechtsgrond in het Belgisch recht die in het gebruik van LFR voorziet.[[330]](#footnote-330)

##### Wettelijk kader in België

Zowel in de WPA[[331]](#footnote-331) als in de Camerawet[[332]](#footnote-332) wordt in de mogelijkheid voorzien om “**intelligente** **camera’s**” te gebruiken. De wettelijke omschrijving van dit begrip lijkt ook de toepassing van LFR te kunnen omvatten: “de camera die ook onderdelen en software bevat, die al dan niet gekoppeld aan registers of bestanden, de verzamelde beelden al dan niet autonoom kunnen verwerken.”[[333]](#footnote-333) Op dit moment is echter qua intelligente camera’s enkel het gebruik van ANPR-camera’s toegestaan.[[334]](#footnote-334)

Ook het artikel 44/2, §3 WPA lijkt in eerste instantie het gebruik van intelligente camera’s als LFR toe te staan: “Wanneer in de uitvoering van de opdrachten van bestuurlijke en gerechtelijke politie technische hulpmiddelen worden gebruikt om automatisch persoonsgegevens en informatie van technische aard te verzamelen, zodanig gestructureerd dat zij rechtstreeks kunnen worden teruggevonden, worden deze gegevens verwerkt in een technische gegevensbank.” Het artikel gaat echter verder: “Een technische gegevensbank wordt gecreëerd ingevolge het gebruik van: 1° intelligente camera's voor de automatische nummerplaatherkenning; 2° intelligente systemen voor de automatische nummerplaatherkenning.”

Bijgevolg is enkel het gebruik van ANPR-camera’s toegestaan en niet het gebruik van LFR door de politie. Toen in 2018 de vraag werd gesteld waarom er niet, net zoals voor ANPR voorzien werd in een technische databank voor gezichtsherkenning, antwoordde toenmalig minister van Justitie **Koen Geens** dat er gezien het massale aantal persoonsgegevens dat wordt verzameld, voor elke specifieke technologie een **parlementair debat** dient te worden gehouden.[[335]](#footnote-335) Bovendien bleek het toen nog te vroeg om dit debat te voeren omdat de technologie nog lang niet op punt stond en het nog jaren zou duren vooraleer men er zinvol gebruik van zou kunnen maken.[[336]](#footnote-336)

Een bijkomende juridische drempel voor het gebruik van LFR is dat biometrische gegevens van enkele **categorieën** personen enkel mogen worden verwerkt mits toestemming van de betrokkenen of mits dit nodig is om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen.[[337]](#footnote-337) Dit geldt voor de getuigen van een strafbaar feit en de slachtoffers van een strafbaar feit.[[338]](#footnote-338) LFR maakt echter geen onderscheid en verwerkt ieders persoonsgegevens op een gelijke manier. Deze bepaling staat dus in de weg van een mogelijk gebruik van LFR door de politie.

Hoewel het gebruik van intelligente niet-ANPR-camera’s dus nog geen rechtsgrond heeft, wordt in verschillende politiezones software zoals **Briefcam**[[339]](#footnote-339) gebruikt die in real time objecten herkent.[[340]](#footnote-340) Men kan zich afvragen wat precies de rechtsgrond is voor zulke technologie in het Belgisch recht.

### Is er een wettelijke basis voor proefprojecten?

Naar aanleiding van het proefproject in Zaventem concludeerde het COC dat ook voor proefprojecten van LFR een wettelijk kader ontbreekt.[[341]](#footnote-341) **Frank Schuermans**[[342]](#footnote-342)vindt dat er wel enige mogelijkheid zou moeten zijn om proefprojecten met gezichtsherkenning te laten doorgaan om de technologie te testen,[[343]](#footnote-343) maar stelt vast dat ook bij het testen van de technologie onvermijdelijk persoonsgegevens worden verwerkt.

Niettemin kan een proefproject handig zijn om de effectiviteit, het gebruik en de doelstellingen van de technologie te onderzoeken met het oog op mogelijk toekomstig gebruik ervan. In enkele EU-lidstaten wordt LFR wel al getest.[[344]](#footnote-344) **Anke Stakenborg**[[345]](#footnote-345)vindt het beter dat de effectiviteit en praktijken met LFR getest zouden kunnen worden, zodat de politie kan oordelen wat de voor-en nadelen zijn van de technologie. Enkel op deze manier kan volgens haar een goed publiek debat worden gevoerd. Ze zegt: “Laat ons eerst testen, dan een dossier opbouwen dat argumentatie geeft waarom we het willen doen en dan het wettelijk kader in orde brengen. Als we eerst altijd moeten wachten, moeten we blind een juridisch kader opstellen, omdat we te weinig weten wat de toepassingsmogelijkheden en concrete werkingsmodaliteiten zijn van deze nieuwe technologie.”

Verschillende zaken dienen in zo’n rechtsgrond voorzien worden opdat proefprojecten geen inbreuk vormen op de privacy van betrokkenen.[[346]](#footnote-346) Zo rijst de vraag welke watchlists men gaat gebruiken: **Anke Stakenborg**[[347]](#footnote-347) geeft aan dat in het proefproject op Zaventem een watchlist werd gebruikt met daarin personen uit een algemene most-wanted lijst die vrij beschikbaar is op het internet. De vraag is in welke mate de vrije beschikbaarheid van persoonsgegevens online de verwerking ervan rechtvaardigt.[[348]](#footnote-348) Daarnaast werden ook afbeeldingen gebruikt van politieambtenaren die vrijwillig wilden meewerken met het project.

**Frank Schuermans** vindt het bovendien belangrijk om bij proefprojecten vast te leggen in welke mate politie in het kader van een proefproject gevolgen mag hechten aan hits met LFR: kan men een verdachte van terrorisme aanhouden wanneer het gebruik van LFR nog in een testfase zit?

Bovendien stelt zich de vraag **welke vereisten van gegevensbescherming** precies van toepassing zijn op een proefproject: zo dient volgens Fussey een duidelijk onderscheid te worden gemaakt tussen toestemming gegeven voor onderzoek en toestemming voor politieoperaties.[[349]](#footnote-349) De vraag is dan ook in welke mate de betrokkene redelijke verwachtingen van privacy kan hebben. Zo werd een man in het Verenigd Koninkrijk beboet omdat hij verdacht overkwam toen hij zijn gezicht afschermde om niet gefilmd te worden.[[350]](#footnote-350) Dat de politie dit als verdacht gedrag zou beschouwen, ondermijnt de onderliggende waarde van geïnformeerde toestemming van de betrokkene voor het proefproject.[[351]](#footnote-351)

### Aan welke inhoudelijke voorwaarden moet een rechtsgrond voldoen?

#### Enkele basisbeginselen

Om een beoordeling te maken van de manier waarop LFR mogelijks art. 8 EHRM en art. 7 en 8 HEU schendt, wordt hieronder het gebruik van LFR getoetst aan de basisbeginselen van het gegevensbeschermingsrecht. Het is belangrijk om hierbij in aanmerking te nemen dat deze beginselen niet concreet kunnen worden afgebakend, maar met elkaar overlappen en elkaar aanvullen. Zo is het beginsel van doelbinding bijvoorbeeld heel nauw gelinkt aan het beginsel van transparantie: als het doel voldoende duidelijk en precies wordt omschreven, versterkt dat ook de transparantie van de verwerking.[[352]](#footnote-352)

De basisbeginselen zijn de volgende:

* Rechtmatigheid, behoorlijkheid en transparantie[[353]](#footnote-353)

Deze basisbeginselen worden regelmatig samengenomen en houden in dat een verwerking een duidelijke verwerkingsgrond moet hebben dat de verwerking vervolgens geen onvoorzienbare negatieve effecten mag hebben en dat de VWV de betrokkene in duidelijke taal moet informeren onder meer over de doeleinden van de verwerking.[[354]](#footnote-354)

* Doelbinding[[355]](#footnote-355)

Elke verwerking moet gebeuren voor een specifiek doel en enkel voor aanvullende doeleinden die overeenstemmen met het originele doel. Bovendien moeten de doelen van de verwerking worden vastgelegd voordat de verwerking begint.[[356]](#footnote-356)

* Beginsel van minimale gegevensverwerking of “dataminimalisatie”[[357]](#footnote-357)

De verwerkingen moeten worden beperkt tot wat noodzakelijk is om het legitieme doel van de verwerking na te komen. Zulke verwerkingen van persoonsgegevens mogen enkel plaats vinden als dit niet kan gebeuren door middel van andere redelijke middelen en de verwerking mag niet disproportioneel zijn ten aanzien van de betrokken belangen, rechten en vrijheden.[[358]](#footnote-358)

* Nauwkeurigheid[[359]](#footnote-359)

Doorheen alle verwerkingsprocessen moeten inaccurate persoonsgegevens worden gewist en moeten persoonsgegevens regelmatig worden gecheckt en geüpdatet om accuraatheid van de verwerking te bewerkstelligen.[[360]](#footnote-360)

* Opslagbeperking[[361]](#footnote-361)

Persoonsgegevens moeten worden gewist of geanonimiseerd zodra ze niet langer nodig zijn voor de doelen van de verwerking waarvoor ze werden verzameld.[[362]](#footnote-362)

* Verantwoordelijkheid en verantwoordingsplicht

De VWV en VW hebben verantwoordelijkheden en verplichtingen (verantwoordelijkheid)[[363]](#footnote-363) en moeten actief maatregelen nemen om de gegevensbescherming te garanderen gedurende hun verwerkingsactiviteiten (verantwoordingsplicht).[[364]](#footnote-364)

* Integriteit en vertrouwelijkheid[[365]](#footnote-365)

Er moeten bij verwerkingen veiligheidsmaatregelen worden getroffen om negatieve gevolgen voor de betrokkene te voorkomen.[[366]](#footnote-366)

De invulling van deze basisbeginselen **verschilt** in zekere mate afhankelijk van de context waarin deze moeten worden toegepast. Zo kan bijvoorbeeld het beginsel van transparantie in de context van politionele opdrachten proportioneel worden ingeperkt om de politionele doeleinden niet tegen te werken. Bij verwerkingen voor niet-politionele opdrachten kan dit niet zomaar. [[367]](#footnote-367)

#### Omkaderen van geautomatiseerde individuele besluiten, inclusief profilering

Geautomatiseerde beslissingen zijn beslissingen die worden gemaakt door automatische middelen, zonder enige vorm van menselijke tussenkomst.[[368]](#footnote-368) Hieronder valt ook profilering, waarbij bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name de bedoeling aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.[[369]](#footnote-369) Verwerkingen die uitsluitend op geautomatiseerde beslissingen steunen, zijn verboden.[[370]](#footnote-370) Slechts onder bepaalde strikte voorwaarden, waaronder het recht op menselijke tussenkomst, is dit toch mogelijk.[[371]](#footnote-371)Een beslissing genomen o.b.v. de bijzondere categorieën persoonsgegevens is verboden tenzij er passende maatregelen worden genomen. Dit is echter absoluut verboden wanneer de verwerking leidt tot discriminatie.[[372]](#footnote-372)

Zoals verder wordt beschreven bestaat er bij de toepassing van LFR zowel in de ontwikkelings-als gebruiksfase een risico op profiling.[[373]](#footnote-373)

#### Bescherming van de rechten van de betrokkene

Naast deze basisbeginselen worden ook bepaalde **rechten** voorzien in de AVG[[374]](#footnote-374) en de Richtlijn Politie en Justitie. Zo biedt de AVG de bescherming van het recht op inzage, recht op rectificatie, recht op gegevenswissing, recht op beperking van de verwerking, recht op overdraagbaarheid van persoonsgegevens en het recht van bezwaar tegen geautomatiseerde individuele besluitvorming.[[375]](#footnote-375) Deze rechten worden niet in dezelfde mate voorzien in de Richtlijn Politie en Justitie als in de AVG wanneer verwerkingen plaatsvinden voor politionele doeleinden.[[376]](#footnote-376) Zo bestaat er geen verzet tegen automatische individuele beslissingen zoals bij de AVG.[[377]](#footnote-377)

Bovendien is het onduidelijk in welke mate de rechten binnen het kader van de Richtlijn Politie en Justitie moeten worden gezien als rechten die actief inroepbaar zijn voor de betrokkene, dan wel dat dit “passieve” rechten zijn, die eerder een verplichting voor de overheid creëren.[[378]](#footnote-378) **Nele Krols** (DPO bij PZ Antwerpen)geeft aan dat er verwarring bestaat bij de burger in welke mate de betrokkene via het COC onrechtstreeks haar rechten kan uitoefenen dan wel rechtstreeks bij de DPO terecht kan. Voor de uitoefening van het recht op inzage m.b.t. camerabeelden lijkt het volgens haar evenwel vanzelfsprekend te zijn dat de burger zich rechtstreeks tot de politiedienst moet kunnen wenden.

Het is naast de actieve uitoefening van rechten ook mogelijk dat het COC passief toeziet dat rechten van de betrokkene worden gerespecteerd. Dit is bijvoorbeeld het geval wanneer het nodig is om rechten te beperken om de politionele doeleinden te vrijwaren.[[379]](#footnote-379) Op vraag van de betrokkene zal het COC dan onderzoeken of en hoe de rechten van de betrokkene werden gerespecteerd.[[380]](#footnote-380) De vraag is in welke mate deze individuele uitoefening van rechten effectief zijn om “privacy” (wezenlijke inhoud van het recht op eerbiediging privéleven en het recht op bescherming persoonsgegevens) te garanderen aangezien dit dus ook een collectief element omvat.[[381]](#footnote-381)

Bovendien stelt zich in het kader van LFR ook de vraag hoe je praktisch het recht op inzage, recht op rectificatie e.d. bij beeldmateriaal regelt.[[382]](#footnote-382)

## Hoe beïnvloedt LFR privacy?

Bij de ontwikkeling van LFR gebeuren al verschillende verwerkingen van persoonsgegevens.[[383]](#footnote-383) Hieronder zal worden opgelijst hoe en welke persoonsgegevens worden verwerkt en welke beginselen daarbij mogelijk in het gedrang komen.

###  Ontwikkelingsfase

#### Convolutioneel neuraal netwerk (CNN)

Om personen te kunnen identificeren maakt LFR gebruik van een **convolutioneel neuraal netwerk**.[[384]](#footnote-384) Zo’n neuraal netwerk wordt gebruikt in verschillende AI-systemen en wordt hier gebruikt voor **computer vision** om de menselijke mogelijkheid om te “zien” na te bootsen.[[385]](#footnote-385) Men voedt een netwerk met een bepaalde input en dat netwerk filtert de input in verschillende lagen om vervolgens een bepaalde output te genereren.[[386]](#footnote-386) Als er bijvoorbeeld een eend op een foto staat, zal het neuraal netwerk in een eerste laag bepaalde lijnen en kleuren filteren, waarna in een volgende laag snavel en ogen worden geselecteerd. Zo gaat het beeld door **verschillende** lagen die steeds gesofisticeerder worden tot het systeem voldoende indicatoren heeft om te zeggen dat het een eend is op de foto.[[387]](#footnote-387)

#### CNN: Een reeks verschillende verwerkingen van persoonsgegevens

##### Input

Om een gezicht te kunnen herkennen heeft het neuraal netwerk input nodig. Deze input bestaat uit “**digital images**”, een tweedimensionaal beeld in digitale vorm. In het geval van LFR worden deze gereconstrueerd uit bewegende beelden.[[388]](#footnote-388)[[389]](#footnote-389)

De opslag van persoonsgegevens in de vorm van digital images, wordt “**ruwe data”** genoemd. Een belangrijk kenmerk van die ruwe data is dat het de mogelijkheid biedt om ook de bron te herkennen waar de persoonsgegevens (namelijk een foto van het gezicht) vandaan komen.[[390]](#footnote-390)

Hoewel de Europese privacyinstrumenten uitdrukkelijk verwijzen naar gezichtsafbeeldingen als biometrische persoonsgegevens,[[391]](#footnote-391) stelt de WP29 dat een **onderscheid** **moet worden gemaakt tussen de ruwe data en biometrische persoonsgegevens** op zich. De ruwe data wordt immers gebruikt als bron voor de verzameling van biometrische persoonsgegevens en dit kwalificeert als dusdanig niet zelf als biometrische persoonsgegevens.[[392]](#footnote-392)

Pas wanneer uit de ruwe data een biometrische template wordt samengesteld, kwalificeren de gebruikte persoonsgegevens als **biometrische persoonsgegevens**.[[393]](#footnote-393) Een **biometrische template** ontstaat wanneer bepaalde kenmerken uit de ruwe vorm van data worden gehaald en worden opgeslagen voor latere verwerking.[[394]](#footnote-394) Het genereren van een template kan niet ongedaan worden gemaakt om er terug de ruwe biometrische data uit te halen: het is een “one-way process”. [[395]](#footnote-395)

Deze laatste stap maakt het menselijk gezicht “machine readable” zodat LFR in staat is om een gezicht te “lezen” en het te vergelijken met andere gezichten om zo de identiteit van een persoon af te leiden. Het feit dat er een zekere probabiliteit is dat er effectief identificatie zal plaatsnemen (bijvoorbeeld als LFR er niet in slaagt een persoon te herkennen en de juiste uitkomst te geven) is van geen belang voor de kwalificatie van een biometrische template als biometrische data.[[396]](#footnote-396)

##### Lagen[[397]](#footnote-397)

Om van ruwe data tot een bepaald resultaat, namelijk het herkennen van een bepaald gezicht te komen, gaat die verzamelde ruwe data door **verschillende lagen** heen. In elk laag gebeurt een bepaalde verwerking van de digital image die als input wordt gebruikt:

* + - 1. Convolutional layer: Deze laag deelt de template op in verschillende lagen die elk een deeltje van het beeld voorstellen.
			2. Pooling layer: De convolutionele laag gaat door een volgende laag die het beeld vertaalt in een voor de computer verstaanbaar beeld.
			3. Filters: in een volgende stap wordt een filter gebruikt die herkent wat dit deeltje van de input voorstelt. vb.: het deeltje dat de neus op de foto voorstelt “is een neus”.
			4. Fully connected: de data verkregen door al deze filters worden in een laatste stap opgesomd waardoor de computer herkent wie op de biometrische template wordt afgebeeld.

De verzamelde persoonsgegevens in de vorm van een biometrische template worden met andere woorden **verwerkt** in verschillende stappen doorheen het proces van de ontwikkeling van software. Men kan zich afvragen of deze verwerkingen ieder individueel of slechts de ontwikkelingsfase als geheel moeten worden gerechtvaardigd aan de hand van de gegevensbeschermingsbeginselen.

##### Machine learning

Om de laatste stap in de “fully connected layer” tot een goed einde te brengen moet men de computer voeden met een **grote hoeveelheid foto’s** en deze labelen. Elke biometrische template dient verbonden te zijn met een naam of nummer dat de LFR in staat stelt om de juiste identificatie van het individu te geven.[[398]](#footnote-398) Op die manier leert de computer wie wie is en kiest het zelf het neuraal netwerk met de grootste slaagkans om een gezicht te herkennen.[[399]](#footnote-399) Dit is het “machine learning” gedeelte van LFR. De software die de uitkomst vormt van dit proces kan worden aangekocht en geïnstalleerd op bestaande systemen van de eindgebruiker[[400]](#footnote-400) of op een camera die als LFR-camera wordt verkocht.[[401]](#footnote-401)

#### Hoe beïnvloedt LFR privacy in de ontwikkelingsfase?

##### Proportionaliteitstoets van verwerkingen in de ontwikkelingsfase

Vooraleer de gegevensbeschermingsbeginselen in de ontwikkelingsfase te bespreken, is het belangrijk om te duiden dat niet zeker is in welke mate de ontwikkelaar hieraan dient te voldoen. De ontwikkelaar valt immers waarschijnlijk niet onder het (personele) toepassingsgebied van de **privacywetgeving**. Dit blijkt niet alleen uit de onduidelijke positie van de ontwikkelaar als VWV en verwerker,[[402]](#footnote-402) maar zal verder ook blijken uit de manier waarop de basisbeginselen zijn opgebouwd.[[403]](#footnote-403) Dat de ontwikkelaar tussen de mazen van het net glipt, zorgt er voor dat de **verplichtingen** om de voorwaarden van privacy te voldoen[[404]](#footnote-404) niet van toepassing zijn op de ontwikkelaar. Er zullen met andere woorden op een andere manier privacygaranties (contractueel) moeten worden ingebouwd voor de verwerking van persoonsgegevens in de ontwikkelingsfase.[[405]](#footnote-405)

De onduidelijkheid rond de vraag in welke mate ontwikkelaars verantwoordelijk zijn voor de naleving van privacywetgeving lijkt te maken te hebben met de discussie rond **horizontale werking** van het Handvest van de Europese Grondrechten.[[406]](#footnote-406) Mensenrechten worden immers traditioneel beschouwd als verticale rechten die men kan inroepen tegen de overheid.[[407]](#footnote-407) Door de uitwerking van het recht op bescherming persoonsgegevens in art. 8 HEU in de AVG, kunnen ook bijvoorbeeld particuliere ondernemingen aansprakelijk worden gesteld voor een inperking van het recht op bescherming persoonsgegevens. In die zin krijgt het recht in zekere zin een horizontale dimensie.

De proportionaliteitstoets van art. 52 (1) HEU zorgt er bovendien voor dat de **beoordeling** van zo’n inperking gebeurt aan de hand van de rechtspraak van het EHRM rond de inperking van art. 8 EVRM.[[408]](#footnote-408) Dit recht op eerbiediging privéleven in het EVRM heeft echter een verticale werking, wat ervoor zorgt dat erg onduidelijk is welke rechtspraak en principes van het EHRM toepasselijk zijn bij de beoordeling van een inperking door een particulier.

Hoewel het bestaande wetgevende privacykader niet van toepassing lijkt op de ontwikkelaar, bespreekt deze masterproef toch in welke mate de ontwikkelingsfase voldoet aan de voorwaarden van privacy die blijken uit deze wetgeving.[[409]](#footnote-409) Op deze manier wordt aan de hand van de bestaande privacyvoorwaarden in de fase van gebruik van LFR, die volgens het HvJ de wezenlijke inhoud vormen van privacy, besproken hoe de “privacy” van betrokkenen in de ontwikkelingsfase wordt aangetast. Hieruit blijkt enerzijds dat er reeds inperkingen zijn van het recht op privacy in de ontwikkelingsfase, anderzijds bestaan er problemen die consequenties hebben voor de mate waarin privacy wordt beschermd in de latere fase van het gebruik van LFR.

##### Rechtmatigheid, behoorlijkheid, transparantie

###### Rechtmatigheid en behoorlijkheid

Om LFR te ontwikkelen is het nodig om voldoende trainingsdata ter beschikking te hebben.[[410]](#footnote-410) De vraag is **hoe** men aan zo’n grote hoeveelheid data komt en welke **rechtsgrond** men hiervoor gebruikt.

###### *Clearview Case*

Hierbij is het interessant de casus te bespreken van Clearview, het Amerikaans bedrijf dat het nieuws haalde toen het een app ontwikkelde die de gebruiker in staat stelt een foto te nemen van iemand om een persoon te identificeren (d.i. de niet-live versie van facial recognition).[[411]](#footnote-411) Het gebruikte hiervoor de techniek van internet scraping om een dataset op te bouwen waarmee men de software (Clearview AI) kan trainen.[[412]](#footnote-412) Dit wil zeggen dat het gegevens van sociale netwerkplatformen als Facebook “schraapte” en verzamelde in een database. Verdere verwerking van zulke gegevens leidde al eerder tot controverse in het Cambridge Analytica-schandaal, toen er geen duidelijke wettelijke basis was om de persoonsgegevens te verwerken voor hele andere doeleinden dan voor de werking van het platform.[[413]](#footnote-413)[[414]](#footnote-414) Hoewel Facebook nog steeds persoonsgegevens doorverkoopt, beweerde het bedrijf in het geval van Clearview AI dat het internet scraping voor de ontwikkeling van gezichtsherkenning expliciet had verboden in haar privacyverklaring. Ook Twitter, Instagram, Youtube en Linkedin verboden Clearview AI deze data te gebruiken.[[415]](#footnote-415) **Peter van Schelven**, die juridisch adviseur is in gegevensbeschermingsrecht vraagt zich af in welke mate een platformbezoeker als Clearview echter gebonden is aan zulke eenzijdige verklaringen van de platformen.

Clearview kon zich dus niet op de **toestemming** van de privacyverklaring door de betrokkenen beroepen als rechtmatigheidsgrond voor de verdere verwerking van persoonsgegevens ter samenstelling van een database. Het bedrijf riep dan ook het **publieke karakter** van foto’s op sociale media in als rechtmatigheidsgrond.[[416]](#footnote-416) Op basis van art. 9, e) AVG kan dit effectief als rechtsgrond dienen voor de verwerking van gevoelige persoonsgegevens zoals biometrische templates wanneer die kennelijk openbaar werden gemaakt door de betrokkene. Deze rechtmatigheidsgrond is in het geval van Clearview omstreden; de vraag stelt zich of profielfoto’s en andere persoonsgegevens vrijgegeven op sociale media effectief publieke gegevens zijn. Men kan zich immers afvragen of de toestemming tot openbaarmaking door de betrokkenen van hun persoonsgegevens zo ver reikt dat ook het gebruik van internet scraping erbinnen valt.[[417]](#footnote-417)

Om als rechtmatigheidsgrond te worden gebruikt, dient die toestemming vrij te zijn, specifiek, geïnformeerd, ondubbelzinnig, aantoonbaar, moet het een actieve handeling zijn en moet het te allen tijde mogelijk zijn voor de betrokkene om de toestemming in te trekken.[[418]](#footnote-418) Bovendien moet rekening worden gehouden met de **redelijke verwachtingen** van de betrokkene t.a.v. de verwerkingen van diens persoonsgegevens op basis van de verhouding met de VWV.[[419]](#footnote-419) Hoewel in deze Facebook en andere sociale mediaplatformen beweerden dat er geen enkele samenwerking was tussen hen en Clearview lijkt het relevant te weten wat de redelijke verwachting van “privacy” is van betrokkenen t.a.v. hun persoonsgegevens op sociale media. [[420]](#footnote-420)

Kortom, in het geval van Clearview is het erg omstreden of er een legitieme rechtmatigheidsgrond was om op zulke grote schaal gegevens te verwerken. De **EDPB** reageerde in een brief gericht aan het Europees Parlement op het gebruik van Clearview AI door de politie, maar sprak zich over de ontwikkeling van zulke tools in die korte eerste reactie niet uit.[[421]](#footnote-421)

###### *Wetenschappelijk onderzoek*

Een andere mogelijke rechtmatigheidsgrond waar ontwikkelaars zich op kunnen beroepen is die van de **verdere verwerking voor wetenschappelijk onderzoek**. Een relevante casus in deze context is die van IBM, dat in 2019 de grote dataset Dif (Diversity in Faces) beschikbaar maakte voor onderzoek om het risico op bias in toepassingen met facial recognition terug te dringen.[[422]](#footnote-422) De foto’s uit de database maakten deel uit van een grotere database YFCC-100M die online stond onder een **Creative Commons Licence**. Dit is een online auteursrechtelijke overeenkomst die toestaat afbeeldingen te kopiëren en te gebruiken voor academische en commerciële onderzoeksdoeleinden.[[423]](#footnote-423)

Het idee achter Creative Commons is dat vrij gebruik van publiek toegankelijke informatie de innovatie ten goede komt. Ook hier stelde zich echter het probleem dat foto’s van een sociale media-site (Flickr) werden gehaald en dat de gebruikers van het platform geen expliciete toestemming hadden gegeven.[[424]](#footnote-424) Bovendien is onduidelijk wiens foto’s in de dataset zitten, waardoor het moeilijk is een recht van bezwaar[[425]](#footnote-425) uit te oefenen tegen zulke praktijken.[[426]](#footnote-426) De CEO van het bedrijf is ervan overtuigd dat **strikte copyright-regels niet** het goede middel zijn om privacy te beschermen, onderzoeksethiek vorm te geven of het gebruik van online surveillance tools te reguleren.[[427]](#footnote-427)

Om van zulke databanken gebruik te maken, kan een onderzoeker zich beroepen op de uitzondering in de AVG die stelt dat een verwerking van persoonsgegevens is toegestaan wanneer dit wordt gedaan met het doel die persoonsgegevens verder te gebruiken voor **wetenschappelijk onderzoek**.[[428]](#footnote-428) In dat geval wordt de verdere verwerking a priori geacht in overeenstemming te zijn met het oorspronkelijke doel van de verwerking.[[429]](#footnote-429)

Het is bijgevolg belangrijk te weten of de ontwikkeling van LFR al dan niet onder de noemer van “wetenschappelijk onderzoek” valt en wie als **onderzoeker** kwalificeert. Vallen de activiteiten van de afdeling research & development (R&D) van een privé-bedrijf ook binnen dit begrip? Om deze vraag te beantwoorden is een duidelijke definitie nodig van wat kwalificeert als “wetenschappelijk onderzoek,” want in de AVG ontbreekt een duidelijke omschrijving. Volgens de **Europese** Copyright Richtlijn van 2019[[430]](#footnote-430) moet in deze context een onderscheid worden gemaakt tussen **verschillende onderzoeksentiteiten**: zo zijn er **non-profit-instellingen** of instellingen met een doel van **publiek belang** en instellingen met een **commercieel belang**. Tot de eerste categorie behoren universiteiten, instellingen van hoger onderwijs en hun bibliotheken en entiteiten die publiek gesubsidieerd zijn of onderzoek doen gebaseerd op nationale wetten of publieke contracten.[[431]](#footnote-431) De tweede bestaat uit entiteiten met commerciële invloeden en wordt niet gezien als een organisatie die wetenschappelijk onderzoek doet. Deze opdeling in categorieën is echter enkel van toepassing binnen het kader van deze Copyright richtlijn [[432]](#footnote-432) en het is dus onduidelijk of deze categorieën doorgetrokken kunnen worden om een antwoord te bieden op bovenstaande vragen m.b.t. gegevensbeschermingsrecht.

Indien het effectief toegestaan is voor private R&D-onderzoekers om van deze uitzondering gebruik te maken, is er nog steeds een rechtmatigheidsgrond nodig om dit te doen. Het gaat immers om biometrische persoonsgegevens die tot de bijzondere categorieën persoonsgegevens behoren, waardoor de rechtmatigheidsgronden van artikels 6 en 9 AVG moeten worden gecombineerd.

###### *Kan een ontwikkelaar een rechtmatigheidsgrond aanduiden voor gevoelige persoonsgegevens?*

De vraag is in welke mate een software-ontwikkelaar zelf die rechtsgrond **kan aanduiden.** De rechtsgrond voor verwerkingen bij het uiteindelijke gebruik met LFR wordt immers vastgelegd door de eindgebruiker wanneer die het specifieke doel van LFR bepaalt. Of een ontwikkelaar vooraf al het doel van het uiteindelijke gebruik van LFR kent, is afhankelijk van de manier waarop de LFR aan de eindgebruiker wordt aangeboden: gebeurt dit als software as a service (SaaS) of wordt het “off the shelf” aangeboden?[[433]](#footnote-433)

In het eerste geval kan de ontwikkelaar rekening houden met de doelen en rechtmatigheidsgrond van het gebruik van LFR door de eindgebruiker. Wanneer LFR echter wordt ontwikkeld om “off the shelf” te worden aangeboden als afgewerkt product, dan zijn de ontwikkelings- en gebruiksfase erg van elkaar afgescheiden en lijkt een afzonderlijke rechtsgrond nodig voor de verwerking van persoonsgegevens in de ontwikkelingsfase.[[434]](#footnote-434)

Dit toont aan dat de ontwikkelaars niet echt binnen het personele toepassingsgebied van de privacywetgeving vallen. Ze lijken immers niet als VWV te kunnen kwalificeren. De vraag is dan ook hoe de rechtmatigheid van de verwerking van persoonsgegevens in de ontwikkelingsfase dan wél kan worden gegarandeerd.

###### Transparantie

Een probleem met algoritmes is momenteel de zogenaamde **black box**.In zijn boek “The Black Box society” beschreef Pasquale voor de eerste keer hoe we allemaal onderworpen zijn aan de manier waarop algoritmes functioneren zonder dat we goed begrijpen hoe die werken.[[435]](#footnote-435)

De term black box verwijst m.a.w. naar de **conceptuele, methodologische en epistemologische uitdagingen** bij het bestuderen van algoritmes.[[436]](#footnote-436) Het feit dat we “software niet kunnen kennen”[[437]](#footnote-437) vormt een probleem voor het beginsel van transparantie[[438]](#footnote-438) dat vereist dat VWV en verwerker de gepaste maatregelen nemen om te verzekeren dat de betrokkene geïnformeerd is over de manier waarop hun persoonsgegevens worden verwerkt.[[439]](#footnote-439) Dit moet gebeuren op een verstaanbare manier, zodat de betrokkenen weet voor welke doeleinden hun persoonsgegevens worden verwerkt.[[440]](#footnote-440) Door de zeer complexe logica van algoritmes, is dit **recht op transparante informatie**[[441]](#footnote-441) zeer moeilijk te garanderen in de context van LFR (en AI in het algemeen) Het is dan ook moeilijk te voorspellen welke data voor welke doeleinden zal worden gebruikt.[[442]](#footnote-442)

Hoewel er wordt gewerkt aan manieren om de verwerking met algoritmes verstaanbaar te maken (zoals Explainable AI (XAI))[[443]](#footnote-443) lijkt het moeilijk om de black box te “openen.” De vraag stelt zich dan ook of de aanpak van een recht op een transparante uitleg wel een oplossing biedt voor het onderliggende probleem.[[444]](#footnote-444) Bucher houdt een pleidooi om minder te focussen op het **openen van de black box** en ziet transparantie niet meteen als iets noodzakelijks.[[445]](#footnote-445) Een recht op een transparante uitleg lijkt op deze manier impliciet een methode in te houden om de black box te openen, wat mogelijks leidt tot “meaningless consent,” waarbij de betrokkene niet begrijpt waarmee die toestemt.[[446]](#footnote-446) De zoektocht naar een werkbaar recht dreigt volgens sommigen ook te leiden tot een “transparency fallacy”: de misvatting dat het mogelijk is transparante algoritmes te creëren.[[447]](#footnote-447)

##### Doelbinding

Het beginsel van transparantie hangt nauw samen met het de doelbeperking. Belangrijk is dat het beginsel van doelbeperking op haar beurt nauw samenhangt met het beginsel van **transparantie en voorzienbaarheid**.[[448]](#footnote-448)

Elk doel dient best zo precies mogelijk te worden afgebakend.[[449]](#footnote-449) Men kan zich afvragen in welke mate elke stap in het proces hierbij apart moet worden beoordeeld dan wel dat het hele ontwikkelingsproces onder hetzelfde doel moet worden beschouwd. Bovendien is dus onduidelijk in welke mate de ontwikkelaar rekening moet houden met de uiteindelijke politionele doeleinden, dan wel met de doeleinden van de ontwikkeling. In het laatste geval kan men zich afvragen wat dan precies die doeleinden zijn.

Deze vragen zijn relevant gezien het **materiële toepassingsgebied** van de Richtlijn Politie en Justitie afhangt van de politionele doeleinden.[[450]](#footnote-450)

##### Dataminimalisatie

Het beginsel van dataminimalisatie is de verplichting om enkel die persoonsgegevens te verwerken die **adequaat, relevant en niet-excessief** zijn voor het doel waarvoor ze worden verzameld en/of verder verwerkt.[[451]](#footnote-451)

Dit beginsel zou ertoe moeten leiden dat slechts een minimum aantal personen wordt geraakt door de verwerking.[[452]](#footnote-452) Die vereiste van dataminimalisatie lijkt echter moeilijk verenigbaar met de aard van big data, die technologiebedrijven gebruiken als input bij softwareontwikkeling. Een kenmerk van **big data** is immers dat het een grote hoeveelheid gegevens omvat.

Hoewel er geen precieze definitie bestaat van het begrip “big data” kan het worden beschreven als de technologische mogelijkheid om nieuwe kennis te verkrijgen, verzamelen, verwerken uit een grote hoeveelheid data (volume), die uit een ruime diversiteit van bronnen afkomstig is (variety), en ook op verschillende snelheden werken (velocity).[[453]](#footnote-453) Het begrip omvat dus zowel de bronnen van gegevens als het het verwerken/analyseren van gegevens (big data analytics).[[454]](#footnote-454)

De vereiste van dataminimalisatie in dit proces lijkt dan ook inherent tegengesteld aan de aard van big data.[[455]](#footnote-455) Gezien nieuwe technologieën zoals LFR **leren door big data analyses**[[456]](#footnote-456) stelt zich de vraag in welke mate het beginsel van dataminimalisatie kan worden nageleefd.

##### Nauwkeurigheid

###### Nauwkeurige resultaten:

Momenteel blijkt LFR nog niet op punt te staan. De resultaten van LFR in het proefproject op Zaventem waren volgens **Anke Stakenborg**[[457]](#footnote-457) voor zo’n zeventig procent accuraat. Tijdens de testfase werd bijvoorbeeld een jongedame als grijsaard bestempeld.[[458]](#footnote-458) Zo zijn er ook problemen met de herkenning van personen met een bril[[459]](#footnote-459) en kwamen er in de proefprojecten met LFR in het Verenigd Koninkrijk veel verkeerde matches uit de bus van de zogenaamde “**lambs**” of “**frequent** **hitters**”: mensen met een specifiek gezicht dat vaak een hit oplevert.[[460]](#footnote-460) Bovendien kan men zich afvragen of personen die plastische chirurgie ondergaan, een baard laten staan,… nog herkend zullen worden.[[461]](#footnote-461)

###### Risico op profilering/inperking non-discriminatiebeginsel[[462]](#footnote-462)

Een eerste mogelijke risico op verboden profilering (waarbij een geautomatiseerde beslissing wordt genomen zonder menselijke tussenkomst) bestaat bij oude mensen en kinderen die slecht zouden kunnen worden herkend. Dit komt doordat hun gezichten een **verouderingsproces** ondergaan. De tijd die tussen het nemen van een foto en de herkenning met LFR zit, heeft een negatieve impact op de nauwkeurigheid van de herkenning. Er is meer wetenschappelijk bewijs nodig voor de betrouwbaarheid van een match wanneer meer dan 5 jaar verliep tussen beide.[[463]](#footnote-463) Een accurate herkenning komt dus zeker in het gedrang voor kinderen, wiens gezicht snel veranderingen ondergaat, maar ook voor ouderen is er onduidelijkheid over het level van nauwkeurigheid van de resultaten.[[464]](#footnote-464)

Een tweede risico blijkt dat mensen met **donkere huidskleur** slechter worden herkend dan mensen met een lichte huidskleur. Zwarte **vrouwen** worden het slechtst herkend.[[465]](#footnote-465) Hierdoor ontstaat het risico op valse positieven, wat wil zeggen dat zij vaak verkeerd worden geïdentificeerd als een persoon op een watchlist van gezochte personen.[[466]](#footnote-466) Er bestaan verschillende mogelijke verklaringen voor deze “bias” of vooringenomenheid in de software:

-“Raw Data is an Oxymoron”:[[467]](#footnote-467) Dit wil zeggen dat de resultaten van AI maar zo goed zijn als de **kwaliteit van de ruwe data**.[[468]](#footnote-468) Zoals boven uiteengezet worden bepaalde kenmerken van een gezicht die een persoon kunnen identificeren uitgelicht om een biometrische template samen te stellen. Er moeten m.a.w. keuzes worden gemaakt over hoe een gezicht is samengesteld. Huidige LFR-systemen blijken voornamelijk gecodeerd op basis van fenotypische kenmerken (zoals huidskleur, ogen, neus) van witte mannen.[[469]](#footnote-469) Een mogelijke verklaring hiervoor is dat de AI-sector momenteel overwegend uit mannen bestaat. Slechts 15% van het onderzoekspersoneel bij Facebook is vrouw, bij Google is dit 10%.[[470]](#footnote-470) Slechts 2,5% van Google’s medewerkers is zwart, bij Facebook en Microsoft is dit 4%.[[471]](#footnote-471) Volgens de Raad van Europa zouden staten moeten waarborgen dat betrokken werknemers voldoende diverse achtergronden hebben, zodat bewuste of onbewuste bias (vooringenomenheid) wordt vermeden bij het ontwikkelen van software.[[472]](#footnote-472)

-**Diversiteit in database**: ImageNet, een van de meest gebruikte datasets voor computer vision-systemen[[473]](#footnote-473) bestaat voor 6% uit beelden van zwarte piet (“blackface”).[[474]](#footnote-474) De databank blijkt bovendien zeer weinig foto’s van zwarten en andere niet-witte mensen te bevatten.[[475]](#footnote-475) Toen Google Photos, dat foto’s in uw persoonlijke digitale foto-bibliotheek labelt, openbaar werd, bleek dat deze tool die ontwikkeld werd op basis van de Imagenet database[[476]](#footnote-476) foto’s van een zwart koppel herkende als “gorilla’s”.[[477]](#footnote-477) Er bestaat met andere woorden een probleem met het gebrek aan diversiteit in datasets die worden gebruikt voor machine learning.[[478]](#footnote-478)

-Pas in de jaren ’90 bracht Kodak een camera uit die in staatwas om de details van niet-witte huid op camera te vatten. Onder de titel “To Photograph the Details of a Dark Horse in Low Light” liet het bedrijf weten dat de nieuwe camera in staat was om ook zwarten of Aziatische mensen te fotograferen (nadat producenten van donkere meubels of zwarte chocolade hadden geklaagd dat ze hun producten niet op foto kregen).[[479]](#footnote-479) De default van camera-instellingen is meestal nog steeds zo ingesteld om beter een lichtere huid te vatten. Er moet bij het gebruik van LFR dan ook worden rekening gehouden met de standaardinstellingen en de technologische mogelijkheden van de camera waarmee wordt gefilmd. [[480]](#footnote-480)

### Fase van de aankoop

#### Bevoegde aankoper van LFR

Een aankoop van een product als LFR door de geïntegreerde politie kan gebeuren via een **overheidsopdracht**[[481]](#footnote-481) of een **raamovereenkomst**. Kenmerkend aan een raamovereenkomst is dat deze gesloten wordt voor een bepaalde periode. In het kader van de raamovereenkomst kunnen vervolgens de prijzen en hoeveelheden van de opdrachten worden vastgelegd.[[482]](#footnote-482)

Volgens **een ervaringsdeskundige bij Financiën van de federale politie in België** (die liever anoniem wenste te blijven),[[483]](#footnote-483) zal LFR waarschijnlijk centraal worden aangekocht op federaal niveau, met name door de Centrale Directie van technische en wetenschappelijke politie (DJT). Hiermee doelt die op de bevoegdheid van deze federale politiedienst om via het federaal aankoopmodel een openbare aanbesteding uit te schrijven.[[484]](#footnote-484) Dit aankoopmodel houdt in dat een Strategisch Aankoopoverleg (SFA) dat bestaat uit de belangrijkste federale instellingen de gemeenschappelijke behoeften bepaalt van publieke instellingen[[485]](#footnote-485) en een gemeenschappelijke overeenkomst kan uitschrijven.[[486]](#footnote-486) De federale en lokale politiediensten kunnen hier vervolgens op inschrijven.[[487]](#footnote-487)

#### Mededingingswetgeving

Doorheen zulke aankoopprocedures moet steeds de regelgeving van de **wetgeving inzake overheidsopdrachten** worden gevolgd. Zo moeten ondernemers op een gelijke en transparante wijze worden behandeld[[488]](#footnote-488) en mag men niet bepaalde ondernemers benadelen of bevoordelen.[[489]](#footnote-489)

Deze vereisten van **eerlijke mededinging staan in zekere zin in de weg aan een optimale privacybescherming**.[[490]](#footnote-490)

Ten eerste worden sommige producten die bij private bedrijven “on the shelf” bestaan in “ready-made”-vorm aangeboden aan de politie.[[491]](#footnote-491) Hoewel **Bart Schoenmaekers**[[492]](#footnote-492) aangeeft dat hierbij enkel binnen de zwaarste veiligheidsprotocollen wordt gewerkt, zijn de mogelijkheden om de ontwikkeling van software te beïnvloeden voor doeleinden van de politie beperkt. Zo meldt **Koen Luykx**[[493]](#footnote-493) dat LFR als product in dezelfde vorm wordt verkocht aan private als publieke entiteiten. De mogelijkheden om aanpassingen te doen aan de software bestaan volgens hem dan ook vooral uit mogelijkheden om suggesties te doen voor toekomstige software, eerder dan aanpassingen te doen aan bestaande software.[[494]](#footnote-494)

Ten tweede merkt **Stéphanie Witters**[[495]](#footnote-495)op dat er privacyrisico’s bestaan met bestaande raamcontracten. Zo kan men immers nieuwe software aankopen binnen een ruimere raamovereenkomst, waarbij er niet opnieuw een aankoopprocedure moet gebeuren.[[496]](#footnote-496) Het is daarbij mogelijk dat raamovereenkomsten dateren van vóór 2018 toen de AVG, Richtlijn Politie en Justitie en de WBP werden geïmplementeerd die o.a. bovenstaande privacygaranties invoerden.

Op die manier kunnen nieuwe aankopen binnen een raamovereenkomst gebeuren zonder dat enige garanties voorzien in de privacywetgeving in rekening worden genomen.[[497]](#footnote-497) Dit is relevant om mee rekening te houden met het oog op mogelijke toekomstige wijzigingen aan de privacywetgeving.[[498]](#footnote-498) Bovendien geeft **Stéphanie Witters** ook aan dat momenteel in het kader van de mededingingsprocedure geregeld gebruik wordt gemaakt van een template, een kopie van een bestaande opdracht die als leidraad wordt gebruikt die vaak nog niet volledig is aangepast aan de bestaande privacywetgeving.[[499]](#footnote-499)

Een derde manier waarop belangen van privacy in zekere mate tegenover de belangen van mededinging staan, komt volgens **Anke Stakenborg**[[500]](#footnote-500)voortuit de onmogelijkheid om op voorhand LFR te gaan testen en aan te passen aan de specifieke behoeften en privacybelangen van de politie. Zijen **Nick Noël**[[501]](#footnote-501) geven aan dat ze graag reeds vóór de aankoop zouden willen kunnen samenwerken met ontwikkelaars. Op deze manier zouden ze al in de fase van ontwikkeling de behoeften van de politie kunnen communiceren met de ontwikkelaar, maar zouden ze de technologie ook bijvoorbeeld kunnen testen op effectiviteit. Momenteel staat echter in België de mededingingswetgeving hieraan in de weg.[[502]](#footnote-502) Het is volgens **Anke Stakenborg** immers moeilijk om een bepaald bedrijf te overtuigen te experimenteren met technologie, te testen voor de doeleinden van de politie en al in R&D fase samen te zitten, omdat dit tegen het gelijkheidsheidsbeginsel ingaat.[[503]](#footnote-503)

Een laatste risico volgens **Koen Luykx**[[504]](#footnote-504)i.v.m. de mededingingswetgeving is dat het een monopoliepositie zou kunnen creëren voor bepaalde bedrijven.[[505]](#footnote-505) Zo werd voor de uitrol van het nationaal cameraschild met ANPR-camera’s een raamovereenkomst gesloten met Proximus en Trafiroad,[[506]](#footnote-506)[[507]](#footnote-507) waardoor volgens hem andere bedrijven voor een bepaalde periode hun producten voor dezelfde doeleinden niet kunnen aanbieden.[[508]](#footnote-508)

#### Privacygaranties in aankoopfase

##### Privacy by design

Er bestaan verschillende instrumenten die tijdens de aankoopfase moeten voorkomen dat privacy wordt ingeperkt. Zo is er de voorwaarde van privacy by design, die vereist dat reeds in de ontwikkelingsfase privacygaranties worden ingebouwd.[[509]](#footnote-509)

De vereiste van privacy by design is echter gericht op de **eindgebruiker** die LFR gaat gebruiken[[510]](#footnote-510) en bijgevolg niet op de ontwikkelaar. Deze zal dan ook in de aankoopovereenkomst de voorwaarden en behoeften bepalen waaraan de LFR moet voldoen. Op het moment dat een aankoopprocedure wordt gestart, is de software echter reeds ontwikkeld.

Verkoper van AI-software **Koen Luykx** zegt dat producten op dit moment in dezelfde vorm worden verkocht aan de publieke als aan de private sector en dat er qua functionaliteiten dus geen onderscheid wordt gemaakt in de hoedanigheid van de cliënt. Dit wil zeggen dat er geen rekening wordt gehouden met het verschil in inhoud van de gegevensbeschermingsbeginselen in de Richtlijn Politie en Justitie dan wel de AVG.[[511]](#footnote-511) Het lijkt dan ook belangrijk voor de R&D-afdeling om vooraf te weten voor welke doeleinden[[512]](#footnote-512) LFR uiteindelijk zal worden ingezet en aan welke (privacy) voorwaarden en behoeften dit moet voldoen.

Hier dient opgemerkt te worden dat het gebruik van LFR voor **niet-politionele doeleinden** dat moet voldoen aan de privacygaranties in de AVG even goed risico’s op schendingen van mensenrechten inhoudt.[[513]](#footnote-513) Men kan zich dan ook afvragen in welke mate ingebouwde privacy by design-garanties van LFR-software dienen af te hangen van de hoedanigheid van de eindgebruiker en dus zouden moeten verschillen wanneer LFR voor politionele, dan wel voor niet-politionele doeleinden wordt gebruikt. Om hier een antwoord op te vinden, lijkt het nuttig om te onderzoeken wat de precieze verschillen zijn in risico’s van LFR voor publiek dan wel privaat gebruik.

##### Derdeverwerkersovereenkomst

In de verwerkersovereenkomst die wordt gesloten tussen de private ondernemer en de aanbestedende overheid worden privacyvoorwaarden vastgelegd waaraan de private onderneming als verwerker moet voldoen.[[514]](#footnote-514) **Nick Noël** geeft echter aan dat deze overeenkomst niet steeds een waarborg biedt dat met privacygaranties wordt rekening gehouden. Hij stelt dat nog niet elk bedrijf de maturiteit heeft inzake informatieveiligheid en gegevensbescherming die de privacywetgeving vooropstelt, waardoor bij verschillende bedrijven het gevaar bestaat dat de garanties in de derdeverwerkersovereenkomst dode letter blijven.[[515]](#footnote-515)

##### Certificering

De AVG maakt het mogelijk voor VWVn om een certificering te krijgen, waarmee verwerkers en VWV aantonen dat ze voldoen aan de voorwaarden in de AVG.[[516]](#footnote-516) In dit opzicht is het relevant dat in een aanbesteding van ondernemingen kan worden vereist dat ze **ISO-waarden** kunnen voorleggen.[[517]](#footnote-517) De International Organization for Standardization (ISO) is een non-gouvernementele organisatie die in samenspraak met experten marktgerelateerde standaarden ontwikkelt per type product of dienst die bedrijven kunnen implementeren.[[518]](#footnote-518) In ruil voor het toepassen van die standaarden, krijgen ze een ISO-certificaat, waaruit blijkt dat ze bepaalde garanties in acht nemen.[[519]](#footnote-519)

De organisatie ontwikkelde verschillende standaarden die relevant zijn in de context van LFR. Zo zijn er ISO 27001-normen, die een stappenplan uitschrijven voor ondernemingen om een Information Security Management System (ISMS) te implementeren, waarbinnen de onderneming maatregelen kan nemen ter bescherming van informatie-veiligheid.[[520]](#footnote-520) Deze normen, die worden beschreven als “common language for organizations around the world” op het vlak van informatieveiligheid,[[521]](#footnote-521) worden aangevuld met ISO-27002-normen, die een overzicht bieden van veiligheidsmaatregelen.[[522]](#footnote-522)

Recent werden ook de ISO 27701-normen gecreëerd, die richtlijnen en waarborgen bieden ter bescherming van privacy. De bedoeling is dat ondernemingen en publieke entiteiten een Privacy Information Management System (PIMS) installeren, dat verschillende privacygaranties inhoudt.[[523]](#footnote-523)

Deze normen vormen dus in zekere zin de uitwerking van het beginsel van veiligheid[[524]](#footnote-524) en privacy by design[[525]](#footnote-525) en kunnen in informatie-systemen bepaalde waarborgen garanderen.

##### Gegevensbeschermingseffectbeoordeling

In elk geval waarin de verwerking gelet op de aard, reikwijdte, context of doeleinden ervan een hoog risico inhoudt voor rechten en vrijheden van natuurlijke personen oplevert, dient vóór de verwerking een gegevensbeschermingseffectbeoordeling (hierna: GEB) of Data Protection Impact Assessment (DPIA) te gebeuren.[[526]](#footnote-526)

Een GEB dient steeds te gebeuren vóór de eerste verwerking. De vraag is hier wat kwalificeert als de eerste verwerking: als pas een GEB wordt gedaan wanneer de technologie is aangekocht zit men al snel met het probleem dat het niet meer mogelijk is dit te remediëren in de onderhandelingsfase.[[527]](#footnote-527) Zo stelt **Peter van Schelven** dat het moeilijk is om reeds een GEB te maken vóór de aankoop van de technologie, omdat dit mogelijks een inbreuk vormt op het gelijkheidsbeginsel voorzien in de Wet inzake Overheidsopdrachten. Men zou immers voor elke onderneming een GEB moeten doen om alle ondernemers op gelijke manier te behandelen.[[528]](#footnote-528)

De **vraag** is in welke mate het huidige aankoopproces volstaat om bestaande inperkingen op “privacy” te identificeren en remediëren.

#### Een mogelijke oplossing: innovation procurement?

* Publiek-private samenwerking

Om enkele van de beschreven moeilijkheden in het aankoopproces te remediëren zou “innovation procurement” een oplossing kunnen bieden.[[529]](#footnote-529) Deze methode om openbare aankopen te organiseren werd ontwikkeld door de Europese Commissie in het kader van de Digital Single Market[[530]](#footnote-530) en voorziet verschillende **innovatieve methoden** voor een betere **publiek-private samenwerking**. [[531]](#footnote-531)

Zo stelt het de methode van pre-commercial procurement voorop, waarbij geïnvesteerd wordt in R&D vooraleer technologie op de markt kan komen. Op deze manier wil men garanderen dat enkel de minst risicovolle en meest effectieve producten zullen verkocht worden.[[532]](#footnote-532) Dit maakt het bovendien ook mogelijk om reeds in de aankoopfase de concrete doelen van de uiteindelijke verwerking te communiceren met de ontwikkelaar, wat bijvoorbeeld nuttig kan zijn m.o.o. de vereiste van privacy by design.[[533]](#footnote-533)

**Nick Noël** vermeldt dat de Nederlandse politie reeds langer inzet op zulke publiek-private samenwerking waarbij politieambtenaren reeds vanaf de ontwikkelingsfase samen aan tafel zitten met ontwikkelaars om de belangen, behoeften en (privacy)verplichtingen van de politie te communiceren.[[534]](#footnote-534) Het lijkt dan ook aangewezen om te kijken naar bestaande praktijken hieromtrent bij de Nederlandse politie.

* Quadruple Helix

Bovendien kan het interessant zijn om bij zulke publiek-private samenwerking uit te gaan van de Quadruple Helix (hierna: QH). Dit is een **organisatorisch model** waarin de overheid, industrie, de academische wereld en burgerparticipanten samenwerken rond innovatie.[[535]](#footnote-535) Het model voorziet een democratische aanpak van innovatie, doordat de besluitvorming en strategie rond technologie wordt blootgesteld aan feedback van verschillende belanghebbenden.[[536]](#footnote-536)

Een recent voorbeeld in België van een vorm van samenwerking tussen de academische wereld en publieke sector is het onderzoek van de UGent en KULeuven naar oorbiometrie in samenspraak met de federale politie.[[537]](#footnote-537) QH zou hieraan ook de private sector en een vertegenwoordiger van de civiele maatschappij toevoegen.

Het model maakt het in de context van innovative procurement mogelijk om reeds bij het bepalen van de mogelijke functionaliteiten van LFR in de **ontwikkelingsfase** rekening te houden met de precieze (privacy) belangen van de burger, de behoeften van de politie en de doeleinden van het gebruik met LFR.

* Smart policing

Ook de tendens richting “**smart policin**g” lijkt te kaderen binnen deze evolutie van publiek- private samenwerking en innovation procurement. Zo organiseert de Belgische politie “hackatons” waarbij teams problemen worden voorgelegd die zij proberen oplossen[[538]](#footnote-538) en de winnaars hun innovatief project vervolgens verder kunnen ontwikkelen. Met het oog op de problemen in de aankoopfase van LFR zou het interessant kunnen zijn om de winnende bedrijven van zulke wedstrijden hun product te laten ontwikkelen en te laten afstemmen op de concrete verwachtingen van de politie.

Een dergelijke aanpak van publiek-private samenwerking kent reeds een precedent in het portaal van **Smart Ports Entrepeneurial Ecosystem Development** (SPEED). Dit portaal biedt een platform voor havens om probleemgerichte opdrachten uit te schrijven waar bedrijven en onderzoekers kunnen inschrijven om die vervolgens te gaan ontwikkelen.[[539]](#footnote-539) Zo heeft de haven van Antwerpen bijvoorbeeld recent een “challenge” uitgeschreven voor bedrijven en onderzoeksgroepen om het “data management” binnen de haven te optimaliseren.[[540]](#footnote-540)

### Gebruik van LFR door de politie in de praktijk

#### Welke persoonsgegevens worden verwerkt?

Het gebruik van LFR houdt de verwerking in van **verschillende persoonsgegevens** voor verschillende doeleinden.[[541]](#footnote-541)

1. Eerst worden “**facial images”** samengesteld wanneer de camera filmt. Vervolgens worden gezichtskenmerken geanalyseerd om er een **biometrische templates** uitsamen te stellen. De biometrische template op zich vormt een verwerking van gevoelige fysieke persoonsgegevens, nog los van het feit of deze vergeleken wordt met een watchlist.[[542]](#footnote-542)

Bovendien is het hierbij relevant dat verschillende vormen van AFR worden getest in medische toepassingen om diagnoses te stellen aan de hand van een gezichtsscan.[[543]](#footnote-543) De vraag rijst dan ook in welke mate de biometrische template ook gezondheidsgegevens kan bevatten, die kwalificeren als gevoelige persoonsgegevens.[[544]](#footnote-544)

1. **Metadata:** Om de verzamelde persoonsgegevens te linken aan tijd en plaats wordt ook metadata verzameld, zodat de politie niet enkel de persoon kan identificeren, maar deze ook kan plaatsen in tijd en ruimte.[[545]](#footnote-545) Zoals hierboven beschreven kan metadata kwalificeren als (gevoelige) persoonsgegevens, wanneer de VWV via wettelijke middelen in staat is om het individu te identificeren met behulp van aanvullende informatie.[[546]](#footnote-546)

Gezien het doel van LFR is om individuen te identificeren en de VWV hierbij gegevens over locatie en tijd kan combineren met zowel biometrische persoonsgegevens via LFR als persoonsgegevens verzameld door middel van andere bestaande technieken lijkt de toets van identificeerbaarheid van metadata hier voldaan. Op die manier kwalificeren metadata ook als persoonsgegevens.

1. **Watchlist**: Om een watchlist samen te stellen worden digital images gebruikt. Deze kunnen ofwel van een bestaande databank afkomstig zijn ofwel van een nieuw samengestelde databank bedoeld voor LFR door de bevoegde overheid. Zoals hierboven vermeld,[[547]](#footnote-547) moet een onderscheid worden gemaakt tussen de digitale beelden van gezichten die de “ruwe data” vormen en de biometrische templates die hieruit worden samengesteld.[[548]](#footnote-548) Een watchlist met digital images zal dus anders worden beoordeeld dan een watchlist met biometrische templates.[[549]](#footnote-549)

Door het gegeven van de **black box**[[550]](#footnote-550) kan niet duidelijk worden aangetoond welke gegevens het algoritme precies gebruikt voor welke doeleinden, wat ingaat tegen de redelijke verwachtingen van de betrokkene.[[551]](#footnote-551)

#### Enkele processtappen waarbij reeds persoonsgegevens verzameld worden vóór het eigenlijke gebruik van LFR

##### Stap 1: Databank creëren

###### Watchlist samenstellen uit foto’s in een databank

Om gebruik te maken van LFR ter identificatie van personen heeft men allereerst een **databank** nodig, waaruit men een lijst kan samenstellen van personen die men wil identificeren in het kader van gerechtelijke of bestuurlijke opdrachten. De Belgische politiediensten maken gebruik van verschillende soorten **gegevensbanken**.[[552]](#footnote-552)Zo zijn er bijvoorbeeld de **gemeenschappelijke gegevensbanken**[[553]](#footnote-553) die de gegevensbank Terrorist Fighters omvatten waarin persoonsgegevens staan die kunnen gebruikt worden ter voorkoming of bestrijding van terrorisme.[[554]](#footnote-554)

De **technische** gegevensbanken[[555]](#footnote-555) werden dan weer opgericht speciaal voor het gebruik van ANPR-camera’s[[556]](#footnote-556) en dienen ter opslag van de persoonsgegevens die nodig zijn voor het gebruik van intelligente technologieën.[[557]](#footnote-557) Ze maken het mogelijk om grote hoeveelheden gegevens van verschillende omvang te verwerken die verkregen zijn uit technische hulpmiddelen. Het laat dus toe om te werken met big data.[[558]](#footnote-558)

Een van de redenen dat het proefproject op Zaventem werd stilgelegd was dat het opslaan van “snapshots” van mensen op de luchthaven in feite neerkwam op het aanleggen van een technische gegevensbank met biometrische gegevens, waardoor het COC het onwettig bevond.[[559]](#footnote-559)Zoals hoger vermeld kunnen technische gegevensbanken[[560]](#footnote-560) immers momenteel enkel voor ANPR worden samengesteld.[[561]](#footnote-561) Zo bestaan er het federale ANPR management system (AMS)[[562]](#footnote-562) en de lokale technische gegevensbanken die aan elkaar worden gekoppeld om gegevens te delen binnen de geïntegreerde politie. [[563]](#footnote-563)

###### Welke databanken kan men gebruiken voor een watchlist?

Niet elke foto is geschikt om een watchlist mee samen te stellen. Het is namelijk belangrijk dat foto’s “**machine readable**”en duidelijk zijn. Zo hangt het af van elementen als lichtinval en de houding van de betrokkene of LFR de afbeelding van een gezicht in een database kan lezen.[[564]](#footnote-564) Bovendien kunnen ook veranderingen in het gelaat, zoals bijvoorbeeld **ouderdom** een impact hebben: hoe minder tijd er tussen de vergeleken afbeeldingen zit, hoe beter LFR zal presteren.[[565]](#footnote-565)

Andere factoren die een impact hebben op de prestatie van LFR zijn: gezichtsuitdrukking, het dragen van een bril of een mondmasker op de afbeelding,...[[566]](#footnote-566) De kwaliteit van de inputdata is m.a.w. van belang om een **accuraat** resultaat te kunnen krijgen.

De vraag stelt zich dan ook of men zich voor het aanleggen van watchlists kan baseren op afbeeldingen van personen in **bestaande gegevensbanken**. **Anke Stakenborg**[[567]](#footnote-567) geeft aan dat ze zelf niet weet of deze geschikt zijn voor gebruik en dat het proefproject op Zaventem te kort was om dit te kunnen testen.

##### Stap 2: Watchlist aanleggen

Wanneer men een databank heeft, kan men op basis van de gegevens in de databank een lijst aanleggen met de personen die men wil identificeren. Dit noemt men ook wel de “watchlist”[[568]](#footnote-568), “blacklist”[[569]](#footnote-569) of “negatieve lijst.”[[570]](#footnote-570)

Een belangrijke vraag die zich stelt is wie op deze lijst zal komen te staan. Dit moet worden beoordeeld op basis van de urgentie van de maatregel voor het publiek belang.[[571]](#footnote-571) Belangrijk hierbij is dat het HvJ oordeelt dat “covert large scale surveillance” (heimelijk) enkel kan worden gerechtvaardigd voor **serieuze** misdrijven.[[572]](#footnote-572) Art. 6 Richtlijn Politie en Justitie **verplicht** lidstaten bij de verwerking een duidelijk onderscheid te maken tussen categorieën personen, zoals personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen, personen die voor een strafbaar feit zijn veroordeeld, slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit of andere personen die bij een strafbaar feit betrokken zijn.

Om deze categorieën van elkaar te onderscheiden, ontwikkelde de UK South Wales Police een **kleurensysteem** waarbij vier watchlists elk een kleur kregen afhankelijk van het risico of de bedreiging geassocieerd met de betrokkene.[[573]](#footnote-573) De rode watchlist bevatte betrokkenen die een serieuze bedreiging vormden voor de publieke veiligheid. Geelbruin (‘amber’) stond voor individuen met eerdere veroordelingen voor serieuze misdrijven en groen voor individuen in wie de politie geïnteresseerd zou kunnen zijn, maar die geen onmiddellijke bedreiging vormen voor de publieke veiligheid.[[574]](#footnote-574)

#### Hoe beïnvloedt LFR privacy in de gebruiksfase?

##### Mass surveillance

Vooraleer een concrete beoordeling te maken van de mate waarin LFR de basisbeginselen van gegevensbescherming respecteert, is het belangrijk om een onderscheid te maken tussen surveillance en **mass surveillance**. Door LFR te koppelen aan bewakingscamera’s (of bewakingscamera’s te installeren met ingebouwde LFR) behoort LFR immers tot de categorie van surveillancemaatregelen.[[575]](#footnote-575) Het risico bestaat echter dat zulke maatregelen ontaarden in mass surveillance, wat slechts in heel uitzonderlijke omstandigheden is toegestaan.

Het **begrip “mass surveillance**” kent geen vaststaande juridische inhoud en wordt uiteengezet in de rechtspraak van het HvJ en het EHRM.[[576]](#footnote-576) Hieruit kan men bepaalde criteria afleiden om te toetsen of een concrete maatregel al dan niet kwalificeert als **toegestane surveillance**. Belangrijk bij de criteria afgeleid uit de rechtspraak is dat de principes van “covert surveillance”, ook van toepassing zijn op “overt surveillance”.[[577]](#footnote-577) Hierdoor zal zowel voor zichtbare als niet zichtbare camera’s (al dan niet met LFR) die op grote schaal surveilleren rekening moeten worden gehouden met de rechtspraak rond covert surveillance. [[578]](#footnote-578)

Hoewel doorheen de uiteenzetting van de basisbeginselen hieronder de criteria uit de mass surveillance rechtspraak in rekening worden genomen waar mogelijk, zal de proportionaliteit van de concrete maatregel met LFR moeten worden beoordeeld o.b.v. een case-by-case benadering.[[579]](#footnote-579)

##### Rechtmatigheid, behoorlijk, transparantie

###### Behoorlijkheid

Het behoorlijkheidsbeginsel heeft voornamelijk betrekking op de relatie tussen de VWV en de betrokkene.[[580]](#footnote-580) De betrokkenen moeten **bewust** worden gemaakt van de risico’s, regels, waarborgen en rechten in verband met de verwerking van hun persoonsgegevens en de manier waarop zij hun rechten kunnen uitoefenen.[[581]](#footnote-581) In dat opzicht is het relevant dat een betrokkene geen expliciete toestemming kan geven om gefilmd te worden met LFR wanneer die zich in het openbaar begeeft.[[582]](#footnote-582) Hierbij is de vraag in welke mate men redelijke verwachtingen van privacy kan hebben in openbare ruimtes.[[583]](#footnote-583)

Hier lijkt het onderscheid tussen **niet-besloten plaatsen**, toegankelijk besloten plaatsen en niet voor het publiek toegankelijke besloten plaatsen belangrijk, gezien de redelijke verwachtingen van betrokkene minder relevant worden geacht in publieke ruimtes omdat men zich intentioneel begeeft in ruimtes waar wordt gefilmd.[[584]](#footnote-584) Dit dient echter te worden onderscheiden van het systematische filmen in de publieke ruimte, wat dan wel weer ingaat tegen privébelangen.[[585]](#footnote-585)

Ookhetpictogram dat betrokkenen erop moet wijzen dat gefilmd wordt met zichtbare camera’s[[586]](#footnote-586) valt binnen dit transparantiebeginsel. Er zijn bepaalde regels vastgesteld rond het gebruik van pictogrammen: zo moet het bord groter zijn op een niet-besloten plaats dan op een besloten plaats. Bovendien moet het pictogram vóór de camera staan, zodat bij het gebruik van bijvoorbeeld ANPR-camera’s de verwerking wordt aangekondigd vóórdat de nummerplaatgegevens worden verwerkt.[[587]](#footnote-587)

**Nick Noël** geeft aan dat er in de praktijk binnen zijn politiezone veel problemen bestaan rond de juiste plaatsing van pictogrammen. Zo staan er soms geen pictogrammen of staan ze op de verkeerde plek, waar ze bijvoorbeeld niet zichtbaar zijn. Bovendien bevatten verschillende pictogrammen de foute informatie.[[588]](#footnote-588)

###### Rechtmatigheid[[589]](#footnote-589) en transparantie

De behoorlijkheid die het gebrek aan toestemming bij het filmen met LFR in een openbare ruimte[[590]](#footnote-590) compenseert, hangt samen met het beginsel van **rechtmatigheid**. Op basis van dit beginsel moet de verwerking op een expliciete en legitieme grond worden gestoeld.[[591]](#footnote-591) De betrokkene dient **geïnformeerd** te worden over o.a. de identiteit en de contactgegevens van de verantwoordelijke, de verwerkingsdoeleinden en de legitieme verwerkingsgrond, de bewaartermijn voor de gegevens en de contactgegevens van de DPO.[[592]](#footnote-592)

Bovendien moet de betrokkene ook geïnformeerd worden over de **rechten** die hij kan uitoefenen: het recht om toegang te verzoeken tot en rectificatie van of wissing van persoonsgegevens.[[593]](#footnote-593) Belangrijk hierbij is dat de informatie moet worden verstrekt voordat de gegevens worden verzameld, opgeslagen, geanalyseerd of gebruikt.

In deze context is ten eerste de bestaande praktijk met betrekking tot ANPR relevant. Het gedeelte van de Gemeenschappelijke richtlijn **MFO-3**[[594]](#footnote-594) die de signalementen bepaalt van personen die mogen worden gezocht met ANPR is immers deels geheim.[[595]](#footnote-595) Het openbare gedeelte van de MFO-3 betreft een Ministeriële Omzendbrief dat een algemeen kader bevat met betrekking tot de verwerking van persoonsgegevens en informatie. De toegangsregels tot de politionele gegevensbanken, waaronder de technische gegevensbanken (met ANRP-gegevens) en de profielen maken echter deel uit van de interne en niet-openbare richtlijnen van de politie.[[596]](#footnote-596) Het **COC** stelt dat dit afbreuk doet aan de transparantie zoals die blijkt uit de grondrechten en verplichtingen opgenomen in art. 8 EVRM en art. 7 en 8 HEU.[[597]](#footnote-597) Bovendien meent het COC dat het een pijnpunt is dat deze MFO-3 sinds ettelijke jaren niet up to date wordt gehouden.[[598]](#footnote-598) Recent werden vier ontwerpen van richtijn opgesteld die deze MFO-3 zouden aanvullen/vervangen, maar het COC stelt vast dat deze dit pijnpunt niet remediëren.[[599]](#footnote-599)

Ten tweede is er het probleem van de **black box.**[[600]](#footnote-600) De black box veroorzaakt een gebrek aan transparantie in het algoritme dat dreigt wantrouwen te wekken tegenover het algoritme[[601]](#footnote-601) en dat daardoor het vertrouwen in de politie negatief beïnvloedt.[[602]](#footnote-602)

Ten derde bleek uit een survey waarin Londenaars bevraagd werden over hun bezorgdheden omtrent het gebruik van LFR ook het gebrek aan **transparantie** op andere vlakken een impact te hebben op het vertrouwen in de politie. Zo bleek een grote bezorgdheid dat er onduidelijkheid bestond wie de politie precies beschouwde als “people of interest” en welke groepen die zou targeten. Een aantal personen vroeg zich ook af of regelgeving rond LFR de politie in staat zou stellen om een bredere groep personen te monitoren en data door te spelen aan derden.[[603]](#footnote-603)

De Raad van Europa stelt dan ook in haar “Guidelines on Facial Recognition” voor dat entiteiten die LFR gebruiken **transparantie** in acht nemen op verschillende vlakken.[[604]](#footnote-604) In een ongecontroleerde omgeving (zoals een publieke ruimte) dient de autoriteit een gelaagde aanpak te volgen. Zo moet een eerste laag voorzien dat in de nabije omgeving van de technologie alle informatie in leesbare vorm beschikbaar is over de doeleinden, de VWV, de duur van de verwerking en de perimeter waarin de technologie wordt toegepast. In een tweede laag van transparantie voorziet de autoriteit dat alle noodzakelijke informatie beschikbaar is bij de ingangspunten van de plaats waar LFR wordt ingezet. [[605]](#footnote-605)

De South Wales Police, die LFR reeds uitgebreid testte, paste bij elk proefproject de volgende reeks **maatregelen** toe:

* Vooraf aan elk gebruik kondigde de politie op Facebook en Twitter het gebruik van LFR aan, waarbij ze de exacte locatie vermeldde en een uitnodiging om in gesprek te gaan met de politieambtenaren die de technologie gebruiken.
* Op de politiewagens op de site en in een 100 meter radius rond de LFR-camera’s werden “Fair Processing Notices” geplaatst op A-2 formaat.
* Mededelingen ter grootte van een postkaart werden uitgedeeld aan het publiek in de nabijheid van elk gebruik van LFR-camera’s en aan elke persoon die werd aangehouden voor een interventie. Bovendien was er informatie beschikbaar op de website van de politie.[[606]](#footnote-606)

Ten slotte is het volgens de London Policing Ethics Panel essentieel voor transparantie dat de resultaten over het gebruik van LFR worden gepubliceerd in de publieke statistieken van de politie.[[607]](#footnote-607)

##### Verantwoordelijkheidsbeginsel en verantwoordingsplicht

* Beginsel

Het **verantwoordelijkheisbeginsel** verwijst naar de verantwoordelijkheid die de VWV heeft om de verwerkingen in overeenstemming te laten gebeuren met de andere beginselen van dataverwerking. De VWV moet hierbij kunnen aantonen dát dit gebeurt en hoe dit gebeurt (verantwoordingsbeginsel).[[608]](#footnote-608) De Richtlijn Politie en Justitie stelt enkele verplichtingen vast die de VWV moet naleven om dit beginsel te vervullen.

Zo heeft hij bijvoorbeeld de **algemene verplichting**[[609]](#footnote-609) om passende technische en organisatorische maatregelen te nemen opdat de verwerking in overeenstemming is met de beginselen in de Richtlijn Politie en Justitie,[[610]](#footnote-610) de verplichting om te voldoen aan de vereisten van privacy by design en privacy by default,[[611]](#footnote-611) om een register van de verwerkingsactiviteiten bij te houden, logbestanden bij te houden en de verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren. Bovendien moet de VWV ook maatregelen nemen ter **beveiliging** van persoonsgegevens[[612]](#footnote-612) en een **functionaris voor gegevensbescherming** aanwijzen.[[613]](#footnote-613)

###### Privacy by design

Om te garanderen dat in beide fases gegevensbescherming wordt gegarandeerd, heeft de VWV de verplichting om **privacy by design**[[614]](#footnote-614) **en privacy by default**[[615]](#footnote-615) te voorzien.[[616]](#footnote-616)

Hoewel de mogelijkheid om gegevensbescherming in te bouwen in de technologie zich voordoet in de fase van ontwikkeling valt de verplichting om dit te voorzien onder de verantwoordelijkheid van de VWV in de gebruiksfase, zijnde de politie. Zoals hierboven bleek[[617]](#footnote-617) heeft de politie als eindgebruiker echter vaak weinig invloed op de fase van ontwikkeling. Men kan zich dus afvragen in welke mate de politie **verantwoordelijk** is voor verwerkingen van persoonsgegevens bij de ontwikkeling van de technologie. **Peter van Schelven** herkent hierin een fout van de Europese wetgever om enkel een verplichting van privacy by design te voorzien voor de eindverantwoordelijke.[[618]](#footnote-618)

###### Verplichtingen

De VWV dient de **passende technische en organisatorische maatregelen** te nemen om te waarborgen en aan te tonen dat de verwerking werd verricht in overeenstemming met de basisbeginselen.[[619]](#footnote-619) [[620]](#footnote-620)Dit betekent dat de VWV maatregelen neemt om de nodige waarborgen in te bouwen in de verwerking om de basisbeginselen te voldoen.[[621]](#footnote-621)

Er bestaan verschillende mogelijke technische maatregelen. Deze kunnen concreet bijvoorbeeld bestaan uit het gebruik van encryptie ter beveiliging[[622]](#footnote-622) of pseudonimisering.[[623]](#footnote-623) De gepaste **methode** voor een technische maatregel hangt af van de concrete kenmerken van een bepaald systeem.[[624]](#footnote-624) Om een juiste afweging te maken tussen veiligheids- en privacybelangen is dan ook specifieke expertise op het vlak van engineering vereist zodat men het privacy by design-principe kan vertalen in technische oplossingen.[[625]](#footnote-625) De gebruikte methode garandeert echter vaak geen volledige anonimiteit[[626]](#footnote-626) of een remedie voor een inperking van het recht op bescherming persoonsgegevens.

Dit werpt dan ook verschillende vragen op: is een verwerking sowieso onrechtmatig als er onvoldoende technische of organisatorische bescherming is?[[627]](#footnote-627) In welke mate zijn technische maatregelen überhaupt in staat om (disproportionele) inperkingen van het recht op bescherming persoonsgegevens te remediëren? Een inherent kenmerk van LFR is immers dat het massaal persoonsgegevens verwerkt om te kunnen functioneren. Camera’s met LFR filmen namelijk zonder onderscheid voorbijgangers en analyseren hun biometrische kenmerken. Kunnen technische maatregelen bijvoorbeeld verhinderen dat het beginsel van dataminimalisatie wordt aangetast wanneer het doel van LFR net is om zoveel mogelijk persoonsgegevens te verwerken?

EDRi zegt dat privacy by design-maatregelen in de ontwikkelingsfase geen baat hebben voor de bescherming van grondrechten bij het latere gebruik van de technologie.[[628]](#footnote-628) **Ella Jakubowska**[[629]](#footnote-629) is dan ook van mening dat LFR inherent een inperking inhoudt van mensenrechten.[[630]](#footnote-630)

###### Gegegevensbeschermingseffectbeoordeling (GEB)

Zoals reeds hoger uiteengezet[[631]](#footnote-631) is de VWV verplicht om een GEB[[632]](#footnote-632) uit te voeren wanneer de verwerking een hoog risico inhoudt.[[633]](#footnote-633)

Om te beoordelen of er sprake is van een “**hoog risico**” dient men rekening te houden met een reeks van criteria. [[634]](#footnote-634) Omwille van het feit dat LFR een nieuwe technologie inhoudt die op grote schaal persoonsgegevens verwerkt (o.a. van kwetsbare personen zoals kinderen) op basis van geautomatiseerde individuele besluitvorming en daardoor in staat is om systematisch te monitoren, overschrijdt de technologie de twee criteria-drempel om een verplichte GEB uit te voeren.[[635]](#footnote-635)

Het is ook belangrijk dat de GEB voor mogelijk gebruik van LFR steeds publiek wordt gemaakt en open ter consultatie.[[636]](#footnote-636)

###### Functionaris voor de gegevensbescherming (DPO)

Een derde verplichting voor de VWV is om een **functionaris voor gegevensbescherming** of data protection officer (hierna: DPO)[[637]](#footnote-637) aan te wijzen.[[638]](#footnote-638) Een DPO wordt per politiezone aangewezen op grond van zijn professionele kwaliteiten en aangesteld door de ministers van Binnenlandse Zaken en van Justitie. [[639]](#footnote-639) Hoewel hij merkte dat er eind februari 2021 nog enkele politiezones waren zonder DPO is **Frank Schuermans** in het algemeen positief over de aanstelling van DPO’s in de Belgische politiezones (hoewel Vlaamse politiezones volgens hem al iets verder lijken te staan qua privacybeleid en aanstelling van kwaliteitsvolle DPO’s dan Waalse).[[640]](#footnote-640)

De DPO dient een reeks taken te vervullen binnen diens politiezone. Zo controleert deze de verwerkingen van persoonsgegevens door politie, geeft die adviezen en fungeert als contactpunt voor de externe toezichthoudende autoriteit.[[641]](#footnote-641) Volgens **Stéphanie Witters** en **Nele Krols**,die beide (adjunct-) DPO zijn in lokale politiezones vervult een DPO een **complexe positie**. Er is immers kennis vereist van verschillende domeinen: kennis van privacywetgeving, maar ook IT-kennis, kennis van de organisatie en ook ervaring met de werking van de organisatie zijn van belang.

Dat is waarom de Politiezone van Antwerpen werkt met een Data Protection Office, waarbij zowel juristen als IT’ers als politieambtenaren werken.[[642]](#footnote-642) **Frank Schuermans** moedigt dit soort structuren aan bij lokale politiezones.

Om dezelfde reden kiest **Stéphanie Witters** ervoor om in de opleiding postgraduaat tot DPO aan Howest een multidisciplinair lespakket samen te stellen.[[643]](#footnote-643)

##### Doelbeperking

###### Function creep bij cameragebruik

Wanneer de doelen van de verwerking niet voldoende specifiek zijn afgebakend bestaat het risico van “**function creep”**.[[644]](#footnote-644) Dit verwijst naar het feit dat bestaande infrastructuur en systemen nieuwe mogelijkheden kunnen creëren waardoor mogelijks een (verdere) inperking ontstaat van rechten.[[645]](#footnote-645) Een goed voorbeeld van dit risico zijn de vele CCTV-camera’s die na het uitdrukkelijke rapport van het COC over het proefproject met LFR op Zaventem[[646]](#footnote-646) momenteel **geen LFR mogen toepassen, maar dit wel kunnen**.

Een tweede voorbeeld zijn de ANPR-camera’s, die soms zo’n scherpe foto’s maken dat de personen achter het stuur kunnen worden herkend.[[647]](#footnote-647) **Nick Noël** geeft aan dat het ook kan gebeuren dat ANPR-camera’s bijvoorbeeld een misdrijf filmen op straat. Vanuit zijn functie als Directeur Operaties bij PZ Rupel stelt hij dat de politie dit ook als bewijs verzamelt en dat het aan de rechters bij een gerechtelijk onderzoek is om de bewijswaarde hiervan te evalueren.

Bijgevolg moet de **Antigoon-leer** in het achterhoofd worden gehouden bij het afbakenen van de doelen van de verwerking met LFR. De vraag stelt zich in welke mate deze leer die geldt voor onrechtmatig verkregen bewijs in het strafrecht[[648]](#footnote-648) ook van toepassing is wanneer bij het verzamelen van bewijs met LFR de Richtlijn Politie en Justitie werd overtreden.[[649]](#footnote-649) Het lijkt in die zin belangrijk om vooraf vast te leggen in welke mate zulke beelden mogen worden gebruikt voor andere doeleinden dan waarvoor ze in essentie zijn bedoeld. Is dit enkel zo voor zwaardere misdrijven zoals doodslag of moord of ook voor bijvoorbeeld een vechtpartij, dealen van joints,…?

###### Legislatieve function creep

Het risico van function creep bij de praktische toepassingen van LFR hangt samen met de legislatieve function creep. Ook bij de juridische afbakening van het begrip “openbare orde” is er immers een risico op function creep. De inhoud van het begrip openbare orde in de ruime zin is **evolutief** en varieert naargelang de maatschappelijke omstandigheden.[[650]](#footnote-650) De openbare orde in de enge zin berust op verschillende regelgevende kaders waarin de lokale besturen de mogelijkheid hebben om hun eigen reglement op te stellen en om autonoom te bepalen welke gedragingen ze strafbaar stellen. Bovendien kunnen lokale besturen de openbare orde ruimer handhaven dan enkel op grond van de bevoegdheid van bestuurlijke politie. [[651]](#footnote-651) Op deze manier hebben zij ruime discretionaire bevoegdheden die verschillen per ordehandhavingsaangelegenheid.[[652]](#footnote-652)

Het lijkt dan ook aangewezen de discretionaire beoordelingsmarges in kaart te brengen waarmee beleidsgevers in staat zijn om doelen uit te breiden om een duidelijk en precies begrip van “ordehandhaving” te definiëren bij het bepalen van de doelstellingen van mogelijk gebruik van LFR.[[653]](#footnote-653)

###### Function creep in de aankoopfase

Ook in de **aankoopprocedure** bestaat bij een mogelijke aankoop van LFR een risico op function creep. Er kan immers tijdens de procedure worden overeengekomen dat automatisch updates zullen worden uitgevoerd aan het systeem wanneer deze door het bedrijf beschikbaar worden gesteld. Zo geeft **Bart Schoenmaekers** (Diensthoofd Financiën en Middelen bij PZ Gent) aan dat het belangrijk is om full-onderhoudscontracten af te sluiten. Op deze manier kan in de behoeftebepaling worden geschreven dat men zowel het initiële product als bijkomende toekomstige updates als éen pakket aankoopt. Dit mag er echter niet toe leiden dat de doeleinden waarvoor de technologie kan worden ingezet, worden verruimd wanneer men bijvoorbeeld een update uitvoert die ruimere mogelijkheden heeft dan het wettelijke doel voorziet.[[654]](#footnote-654)

De globale **corona**-pandemie lijkt dit risico op function creep in zekere mate te vergroten. Vele lidstaten zetten immers surveillancesystemen in die de mogelijkheid hebben veel verder te gaan dan wat nodig is voor de bestrijding van de pandemie of het handhaven van de corona-maatregelen.[[655]](#footnote-655) Private bedrijven ontwikkelen ook software voor CCTV-camera’s die in staat is te herkennen of iemand een mondmasker draagt, of personen voldoende afstand houden enzovoort.[[656]](#footnote-656) Er zijn ook verschillende bedrijven die LFR combineren met temperatuurmeting om te controleren of iemand koorts heeft.[[657]](#footnote-657) **Koen Luykx** die AI- software verkoopt in de Beneluxgeeft aan dat zulke updates met nieuwe functionaliteiten automatisch kunnen gebeuren voor iedereen die reeds klant is bij het private bedrijf dat deze updates ontwikkelt en hiervoor de juiste apparatuur bezit.

##### Dataminimalisatie

De massale verwerking van persoonsgegevens door het gebruik van LFR gaat in tegen het beginsel van **dataminimalisatie**. Op grond daarvan mogen enkel die persoonsgegevens worden verwerkt die noodzakelijk zijn ter identificatie van de gezochte personen.[[658]](#footnote-658)

Wanneer LFR wordt ingezet in een bepaalde ruimte filmt deze iedereen die zich in die ruimte begeeft.[[659]](#footnote-659) Niet enkel worden personen gefilmd, maar er worden ook **templates** gemaakt voor iedere voorbijganger die worden vergeleken met de afbeeldingen van de gezochte personen. Ten slotte worden de gegevens van een mogelijke match ook opgeslagen.[[660]](#footnote-660) Uit een rapport over het proefproject van South Wales Police bleek dat deze verwerkingen op heel grote schaal gebeurden: zo kon de gebruikte LFR tien gezichten per frame verwerken en dertig frames per seconde. Dit wil zeggen dat ze in theorie driehonderd gezichten per seconde konden analyseren.[[661]](#footnote-661)

Belangrijk hierbij is dat de verwerking niet enkel op grote schaal gebeurt, maar ook dat dit gebeurt **zonder onderscheid**: elke voorbijganger wordt immers gefilmd.[[662]](#footnote-662) Dit betekent dus dat niet enkel gezochte personen worden gefilmd (en diens gezichten geanalyseerd), voor wie een inperking van hun recht op bescherming persoonsgegevens gerechtvaardigd zou kunnen zijn in het licht van de politionele doeleinden, maar ook personen die niet worden gezocht worden aan dezelfde maatregel onderworpen. De vereiste dat politie een onderscheid moet maken in **categorieën** van personen (zoals verdachten, veroordeelden, slachtoffers of betrokkenen bij een strafbaar feit) kan dan ook niet worden nageleefd.[[663]](#footnote-663) Bovendien worden ook persoonsgegevens van kwetsbare personen zoals kinderen verwerkt, wat ingaat tegen de hogere bescherming die kinderen vereisen onder het gegevensbeschermingsrecht.[[664]](#footnote-664)

Dit “untargeted” verwerken zonder onderscheid is een fundamenteel kenmerk van **mass surveillance**.[[665]](#footnote-665) De Europese rechtspraak rond dataretentie en mass surveillance bepaalt een reeks van strikte voorwaarden waaraan een surveillancemaatregel dient te voldoen[[666]](#footnote-666) om niet als mass surveillance te kwalificeren.[[667]](#footnote-667) Het HvJ formuleerde bijvoorbeeld in ***Tele2Sverige*** de voorwaarde dat een surveillancemaatregel beperkt moet zijn tot zowel een geografisch gebied, beperkt moet zijn in de tijd en beperkt moet zijn tot bepaalde personen of tot een bepaald publiek.[[668]](#footnote-668) De surveillance van een hele bevolking is immers niet toegestaan. Dit principe werd later nogmaals bevestigd in ***Quadrature du Net.***[[669]](#footnote-669)

De rechtspraak formuleert zo nog een reeks andere **discriminanten**, die ervoor moeten zorgen dat er niet zomaar willekeurig kan worden gesurveilleerd.[[670]](#footnote-670) De keerzijde hiervan is echter dat zulke discriminanten zouden kunnen leiden tot verboden profilering of verboden discriminatie.[[671]](#footnote-671) Er blijkt m.a.w. een spanningsveld te zijn tussen het beginsel van dataminimalisatie[[672]](#footnote-672) en het verbod op profilering en non-discriminatie.[[673]](#footnote-673)

Een voorstel van Vermeulen om te onderzoeken hoe deze tegenstrijdigheid kan worden geremedieerd is om te brainstormen over mogelijke discriminanten in de volgende onderverdeling: ratione informationis (het type informatie dat wordt beschreven), ratione personae (karakteristieken van de getargete persoon), ratione loci (verblijfplaats of aanwezigheid van de getargete persoon), ratione itineris (route die de data flows afleggen), ratione temporis (de getargete periode), ratione instrumenti (personen die bepaalde communicatiemiddelen gebruiken).[[674]](#footnote-674)

##### Opslagbeperking

De opslagbeperking bepaalt hoe lang de **bewaartermijnen** zijn voor verwerkte persoonsgegevens. Zo mogen camerabeelden van ANPR- camera’s,[[675]](#footnote-675) van zichtbaar gebruikte politiecamera’s[[676]](#footnote-676) en niet-zichtbaar gebruikte politiecamera’s[[677]](#footnote-677) in principe twaalf maanden worden bewaard.[[678]](#footnote-678) Als deze gegevens in bepaalde operationele databanken zouden worden opgenomen, gelden de bewaartermijnen voor dat type databanken.[[679]](#footnote-679) De bewaartermijn van beelden van gewone bewakingscamera’s, die de politie in real time kan ontvangen, kan dan weer onderling overeengekomen worden in de samenwerkingsovereenkomst tussen particulieren en politie.[[680]](#footnote-680)

Toen de bewaartermijnen van persoonsgegevens door de politie aan juridische controle van het Grondwettelijk Hof onderworpen werden, erkende het Hof dat er een **evenwicht** moet zijn tussen de privacybelangen van personen en de nagestreefde doeleinden van ordehandhaving en misdaadbestrijding.[[681]](#footnote-681) Het moet voor de politiediensten immers mogelijk zijn om bepaalde vaststellingen te doen voor hun operationele doeleinden, maar anderzijds bestaat het risico dat lichtzinnig met deze persoonsgegevens wordt omgegaan, wat een inbreuk kan betekenen op de privacy van betrokkenen.[[682]](#footnote-682)

Het Grondwettelijk Hof oordeelde dat **de regeling van toegang** tot de camerabeelden een belangrijk element is bij de beoordeling van dit evenwicht. Zo moet de toegang steeds worden gemotiveerd en is toegang tot gegevens in principe enkel mogelijk tijdens de eerste bewaarmaand. Nadien is toegang slechts mogelijk in bijzondere omstandigheden en met machtigingen.[[683]](#footnote-683) Dit wordt geregeld in de camerawetten en er worden ook protocollen over afgesloten op het niveau van de politiezone. [[684]](#footnote-684)

De vraag is in hoeverre voor het gebruik van LFR nieuwe bewaartermijnen moeten worden geregeld. Er bestaan immers verschillen tussen bestaande (ANPR-)camera’s en LFR in de mate waarin de verwerking een impact heeft op privacy van de betrokkene. Zo worden bijvoorbeeld door LFR in verregaande mate biometrische gegevens gecapteerd,[[685]](#footnote-685) wat een impact heeft op de intrusiviteit van de verwerking. Dit maakt het moeilijk om zomaar de bestaande bewaartermijnen over te nemen voor LFR. Technologie die in die zin meer aansluit bij LFR is vingerafdrukherkenning, DNA-onderzoek en irisscans, gezien zij ook biometrische gegevens verwerken.[[686]](#footnote-686)

Het lijkt bijgevolg relevant om een **specifieke beoordeling** te maken van de bewaartermijnen voor LFR waarbij rekening moet worden gehouden met het evenwicht tussen privacy enerzijds en ordehandhaving en misdaadbestrijding anderzijds. Hoewel analogieën kunnen worden getrokken met bestaande technologieën dient men deze beoordeling te maken voor elke aparte technologie.[[687]](#footnote-687)

##### Nauwkeurigheid

Zoals hierboven uiteen gezet, bestaan momenteel nog verschillende problemen met de accurate herkenning met LFR. De oorzaak van deze inaccuraatheid ligt voornamelijk in de ontwikkelingsfase,[[688]](#footnote-688) maar ook de gebruiksfase heeft een impact op deze resultaten.

###### FAR/FRR

De “**similarity score**” van LFR heeft een invloed op de nauwkeurigheid. Deze score geeft de waarschijnlijkheid aan dat gezichten zullen matchen: een grotere waarde houdt in dat er een grotere waarschijnlijkheid is dat gezichten matchen.[[689]](#footnote-689)

Indien die waarde te hoog wordt gelegd, is er een risico op een hoge “false alarm rate” (FAR), wat het percentage van verkeerdelijk geïdentificeerde matches aangeeft. Een hoge “false reject rate” (FRR) geeft daarentegen het percentage aan van echte matches die niet geïdentificeerd werden door de software.[[690]](#footnote-690) Hoe hoger of lager deze drempelwaardes worden gelegd, hoe meer of minder matches de LFR zal weergeven. Deze drempelwaardes worden aanbevolen door de ontwikkelaar en worden gericht op het eindgebruik van de LFR, maar in vele systemen is het mogelijk voor de eindgebruiker om de drempelwaardes aan te passen.[[691]](#footnote-691) Het lijkt volgens **Frank Schuermans**[[692]](#footnote-692)dan ook aangewezen om een publiek debat te voeren over deze drempelwaardes.

Bovendien is het ook belangrijk vast te leggen **hoe politieambtenaren omgaan** **met vals positieve meldingen**. Het kan immers zijn dat operatoren verschillend reageren bij een match van een verkeerdelijk geïdentificeerde betrokkene die deel uitmaakt van een minderheidsgroep [[693]](#footnote-693) dan wanneer die niet tot een minderheidsgroep behoort. Het feit dat mensen met donkere huidskleur door LFR slechter worden herkend dan mensen met lichte huidskleur in combinatie met de drempelwaarde die zelf kan worden gelegd, zorgt ervoor dat meer mensen met donkere huidskleur incorrect zullen worden herkend dan mensen met lichte huidskleur.[[694]](#footnote-694)

###### Menselijke tussenkomst

In deze context is het **recht op menselijke tussenkomst** relevant. Dit betekent dat er een mens kan tussenkomen om zelf een besluit te nemen wanneer het systeem individuele geautomatiseerde besluiten kan nemen die een nadelige impact kunnen hebben op de betrokkene.[[695]](#footnote-695) In het geval van LFR kan een match bijvoorbeeld leiden tot een aanhouding of een mogelijke arrestatie.[[696]](#footnote-696) Een beslissing door LFR kan dus een nadelige impact hebben voor de betrokkene. Het lijkt relevant om bij een publiek debat rond een wetgevend kader van LFR de mogelijke nadelige gevolgen van volledig LFR in kaart te brengen.

Een mogelijk probleem bij die menselijke tussenkomst is dat operatoren **geloof** hechten aan de effectiviteit van het systeem zonder dat ze iets zien dat er niet is.[[697]](#footnote-697) Het is dan ook belangrijk dat politieambtenaren de juiste **training** krijgen om LFR te hanteren en juiste beslissingen te nemen.[[698]](#footnote-698)

Uit een studie in de Verenigde Staten bleek dat er een gebrek was aan **getraind personeel** om LFR te hanteren, waardoor de helft van de tijd een verkeerde beslissing werd genomen over een potentiële match.[[699]](#footnote-699) Dit risico speelt ook in België, waar wegens geldgebrek vaak iemand wordt ingezet zonder expertise zoals laaggeschoolde bewakingsagenten of soms zelfs jobstudenten.[[700]](#footnote-700)

Bovendien wordt de training van politieambtenaren in België voor het gebruik van ANPR geregeld in de aankoopfase. Hierbij wordt regelmatig het train-the-trainer principe gehanteerd, wat wil zeggen dat het private bedrijf een of meerdere agenten traint, die dan op hun beurt anderen kunnen trainen.[[701]](#footnote-701) Men kan zich afvragen in welke mate deze training de hoger aangekaarte risico’s behandelt.

###### Ongecontroleerde omstandigheden

Een volgende element dat invloed uitoefent op de nauwkeurigheid van matches met LFR zijn de omstandigheden waarin deze worden ingezet. In een gecontroleerde omgeving, waar o.a. de lichtomstandigheden, camera-afstand, achtergrond en de filmrichting van de camera kunnen worden gecontroleerd heeft LFR immers relatief accurate resultaten. In een ongecontroleerde omgeving presteert LFR echter slechter.[[702]](#footnote-702) Daar kunnen lichtomstandigheden en dergelijke niet of moeilijker worden gecontroleerd en in een publieke ruimte zorgt ook bijvoorbeeld het hoge aantal gezichten in een publieke ruimte voor onnauwkeurigheden.[[703]](#footnote-703) Zo vertelt **Ruben Vansevenant**[[704]](#footnote-704) dat bijvoorbeeld de lichtinval van de zon soms een probleem vormt bij de huidige ANPR-camera’s: wanneer de zon in de lens schijnt, gaat de nauwkeurigheid van de herkenningen achteruit.

Deze aspecten van onnauwkeurigheid dienen in rekening te worden genomen wanneer men zou beslissen om LFR in te zetten in een bepaalde **ruimte**. In niet-besloten ruimtes vrij toegankelijk voor het publiek zal de omgeving waarschijnlijk minder gecontroleerd zijn dan in niet voor het publiek toegankelijke besloten plaatsen, waar men de omstandigheden die een invloed hebben op de resultaten al wat meer kan controleren. Zo zou men bijvoorbeeld op de luchthaven bij de grenscontrole een laan kunnen afsluiten waar slechts een persoon tegelijk kan passeren in een ruimte waar de verlichting wordt gecontroleerd.[[705]](#footnote-705)

## Hoe beïnvloedt LFR verweven rechten?

### Het recht op een eerlijk proces

In de zaak *Big Brother* *Watch/Verenigd Koninkrijk* oordeelde het EHRM dat er ook steeds **objectief bewijs** dient te zijn alvorens in bulk persoonsgegevens te verzamelen. Dit moet het mogelijk maken een publiek te identificeren wiens gegevens **vermoedelijk** een link hebben met een ernstig strafbaar feit en op een of andere manier bijdragen aan de bestrijding van zware criminaliteit of de preventie van een ernstig risico voor de openbare veiligheid. Er hoeft echter geen redelijke verdenking te zijn.[[706]](#footnote-706)

Uit deze rechtspraak kan men afleiden dat de bescherming van het recht op bescherming persoonsgegevens een grondvoorwaarde kan zijn voor het recht op een eerlijk proces. Een inperking van het recht op bescherming persoonsgegevens kan immers aanleiding geven tot een inperking van het recht op een eerlijk proces.[[707]](#footnote-707) Zo komt door de massale verwerking van persoonsgegevens met LFR mogelijk het **vermoeden van onschuld** van de betrokkene in het gedrang.[[708]](#footnote-708) Doordat iedereen systematisch wordt gefilmd en diens facial images geanalyseerd, wordt elke voorbijganger immers als verdachte beschouwd. Dit betekent in zekere zin een omkering van het vermoeden van onschuld: iedereen wordt geacht verdacht te zijn tot het tegendeel wordt bewezen.[[709]](#footnote-709) In het Belgische politionele rechtskader wordt dit vermoeden van onschuld op verschillende plaatsen gegarandeerd. Zo moet er in het kader van proactieve recherche een **redelijke verdenking** van een misdrijf zijn voordat men een maatregel kan nemen. Bij gerechtelijk taken is hiervoor een **redelijk gegrond vermoeden** nodig dat een misdrijf werd gepleegd of zal gepleegd worden.[[710]](#footnote-710)

Wanneer men LFR zou inzetten bij gezochte personen is er geen inbreuk op het vermoeden van onschuld van de gezochte persoon: er was immers een redelijk vermoeden om aan te nemen dat de persoon schuldig was.[[711]](#footnote-711) LFR houdt echter geen rekening met het vermoeden van onschuld van alle voorbijgangers die ook worden gefilmd. Er is met andere woorden een risico dat LFR een disproportionele last vormt op andere personen dan de dader, verdachte of andere gezochte persoon.[[712]](#footnote-712)

Wanneer LFR puur **preventief** wordt ingezet voordat enig misdrijf is gepleegd en zonder enige verdenking, is er sowieso een omkering van het vermoeden van onschuld.[[713]](#footnote-713) Alle voorbijgangers worden immers gefilmd en diens gezichten geanalyseerd zonder dat voor het verwerken van hun persoonsgegevens enige verdenking bestaat. Zij worden dus gesurveilleerd alvorens ze een misdrijf zullen plegen (als ze al een misdrijf zullen plegen).[[714]](#footnote-714) Op deze manier wordt iedere voorbijganger behandeld alsof die schuldig zou zijn aan een misdrijf, ook al is er geen aanwijzing dat zij enig misdrijf hebben gepleegd, zullen plegen of dat zij de openbare orde zouden verstoren.[[715]](#footnote-715)

Ten slotte bestaat door het gebruik van LFR een **machtsonevenwicht** dat het moeilijk maakt voor de betrokkene om diens onschuld te bewijzen: burgers worden steeds transparanter voor de overheid en bedrijven, terwijl de algoritmen en methoden van de overheid en van bedrijven volledig niet-transparant zijn.[[716]](#footnote-716) Op die manier wordt het voor de betrokkene mogelijk moeilijk om het met LFR verkregen bewijs te weerleggen.

### Implicaties voor vrijheid van meningsuiting

In ***Tele2/Sverige*** stelde het HvJ dat de retentie van metadata een impact kan hebben op het recht op de bescherming van de vrijheid van meningsuiting. [[717]](#footnote-717) In deze zaak waarin het Hof oordeelde over de verplichte retentie van communicatiedata door telecommunicatiediensten lijkt het Hof dan ook een link te leggen tussen het recht op bescherming persoonsgegevens en het recht op vrijheid van meningsuiting.[[718]](#footnote-718)

Door het gebruik van LFR is het mogelijk dat een **chilling effect** bestaat van het recht van vrijheid van meningsuiting en de vrijheid van vergaderen.[[719]](#footnote-719) Het zou immers kunnen dat personen uit schrik voor negatieve consequenties minder snel op straat komen om te protesteren en hun rechten onder het recht op vrijheid van meningsuiting uitoefenen.[[720]](#footnote-720) De omkering van het vermoeden van onschuld door het gebruik van LFR zorgt er immers gemakkelijk voor dat iedereen als verdacht wordt beschouwd.[[721]](#footnote-721)

Het zou ook kunnen dat personen schrik krijgen omdat ze de politiesurveillancemaatregel zelf als te fysiek en psychologisch intrusief beschouwen.[[722]](#footnote-722)

### Non-discriminatiebeginsel

Ook het recht op non-discriminatie komt in het gedrang door het gebruik van LFR. Het verbod van discriminatie houdt immers in dat iedereen op een gelijkwaardige moet worden behandeld.[[723]](#footnote-723) Bepaalde kwetsbare groepen in de maatschappij blijken echter bovengemiddeld vaak het doelwit van surveillancetechnologieën.[[724]](#footnote-724) Zo verwijst **Ella Jakubowska** bijvoorbeeld naar het Verenigd Koninkrijk waar LFR bijvoorbeeld werd ingezet op Nottinghil Carnival, waar voornamelijk zwarte mensen aan deelnemen.[[725]](#footnote-725)

Door proportioneel gezien vaker LFR in te zetten op aangelegenheden met **kwetsbare groepen**, riskeert men dat bovenmatig veel meer personen van deze kwetsbare groepen in databanken van verdachten of daders terecht komen.[[726]](#footnote-726) Men kan zich inbeelden dat dit een impact kan hebben op de criminaliteitscijfers omdat bijvoorbeeld bovenmatig veel personen met een donkere huidskleur in deze registers terecht komen. In dit kader is het relevant dat AFR momenteel voornamelijk wordt ingezet aan grenscontroles op de luchthaven waar personen die onwettig de grens oversteken meteen in een databank terecht komen en zo gemakkelijk te traceren vallen.[[727]](#footnote-727)

## Enkele andere maatschappelijke problemen

##### Ethisch vraagstuk rond LFR

Vooraleer een rechtsgrond rond LFR kan worden opgesteld, moet men eerst beoordelen of hier wel een **maatschappelijke noodzaak** voor bestaat.[[728]](#footnote-728) Hoewel dit criterium door de EDPS wordt geformuleerd in het kader van een juridische beoordelingstoets is dit in de eerste plaats niet meteen een juridisch vraagstuk. Zo stelt de Raad van Europa in haar “Guidelines on Facial Recognition” dat het vaststellen van de maatschappelijke noodzaak van LFR ook een **ethisch** vraagstuk is:[[729]](#footnote-729) is het gebruik van LFR ethisch gezien wenselijk?

Er bestaat momenteel reeds een ruime discipline van **AI Ethics**[[730]](#footnote-730) waarin ook zulke ethische kwesties rond LFR worden onderzocht.[[731]](#footnote-731) De discipline blijkt echter momenteel onderhevig aan enige politieke invloed en de impact van private bedrijven, wat het moeilijk maakt deze vraagstukken te beantwoorden.[[732]](#footnote-732)

Hoogleraar in de ingenieurswetenschappen **Yves Moreau**[[733]](#footnote-733)geeft aan dat er ook nood is aan **ethisch toezicht** in de ontwikkelingsfase van software zoals LFR.[[734]](#footnote-734) Hij trekt de analogie met “human subject research” dat mensen als onderzoeksvoorwerp heeft en waarbij het wettelijk verplicht is om een ethische commissie te voorzien.[[735]](#footnote-735) Hij meent dat dit ook voor IT-onderzoek belangrijk is. Men kan zich bovendien afvragen in welke mate het analyseren van biometrische digital images op zich al behoort tot zulk onderzoek met mensen als onderzoeksvoorwerp. Dit is zeker zo gezien LFR ook wordt ingezet om bijvoorbeeld genetische of medische aandoeningen te identificeren in een geneeskundige context.[[736]](#footnote-736)

Een goed voorbeeld van onafhankelijk wetenschappelijk ethisch onderzoek naar de implicaties van het gebruik van LFR is de studie van de **London Policing Ethics Panel**.[[737]](#footnote-737) Dit onafhankelijke ethische panel werd samengesteld in opdracht van de Mayor of London om ethisch advies te geven in zaken die het publiek vertrouwen kunnen ondermijnen.[[738]](#footnote-738) Het panel deed een survey naar het vertrouwen van de Londense burger in het gebruik van LFR door de politie en stelt op basis daarvan ethische voorwaarden op waaraan toekomstige proefprojecten met LFR zeker moeten voldoen.[[739]](#footnote-739)

##### Wetenschappelijk onderzoek

Een tweede moeilijkheid is dat onderzoek naar de effectiviteit van de technologie vaak gebeurt door de politie zelf of dat de effectiviteit ervan wordt vastgesteld door de ontwikkelaar.[[740]](#footnote-740) Hierbij bestaat het risico dat de politie voornamelijk technische middelen onderzoekt en niet de niet-technische middelen, wat een onvolledig resultaat kan opleveren.[[741]](#footnote-741)

Het private bedrijf Amazon manipuleerde de accuraatheid van haar AFR-product door een hogere drempel te hanteren om de performantie van het systeem te checken, ook al werkten hun klanten bij politie met een veel lagere drempel.[[742]](#footnote-742) Het lijkt dan ook aangewezen dat vooraf een drempelwaarde en **methode van berekening** van effectiviteit worden vastgelegd.

Bovendien kan ook hier het model van Quadruple Helix worden gebruikt. Door de aanwezigheid van universiteiten en onafhankelijke onderzoeksinstanties bij besluitvorming in de fase van ontwikkeling, stimuleert de QH dat de besluitvorming rond functionaliteiten voor mogelijk gebruik van LFR steeds op wetenschappelijk onderzoek zijn gefundeerd.[[743]](#footnote-743)

Een goed voorbeeld van onafhankelijk onderzoek naar het politionele gebruik van LFR is dat van **Peter Fussey bij de London Metropolitan Police**.[[744]](#footnote-744)

##### Effectiviteit en efficiëntie meten

Het meten van de effectiviteit en efficiëntie van LFR om de veiligheid te garanderen is een zeer **complexe** bezigheid. Niet alleen is **veiligheid** een complex en abstract begrip met verschillende invullingen,[[745]](#footnote-745) bovendien is het ook onduidelijk welke methode men kan gebruiken om de “**effectiviteit**” van bewakingscamera’s te meten.[[746]](#footnote-746) Voor CCTV- en ANPR-camera’s bestaan bijvoorbeeld momenteel geen sluitende resultaten die kunnen aantonen dat ze effectief zijn voor het voorkomen van criminaliteit.[[747]](#footnote-747)

Het is ook moeilijk te meten in welke mate LFR “**efficiënt**” is. Hoe kan men bijvoorbeeld controleren of LFR personeelsbesparend is? Men moet hierbij in rekening nemen dat er ook **personeel** nodig is dat LFR hanteert. LFR maakt immers geautomatiseerde individuele beslissingen, wat (gespecialiseerde) menselijke controle vereist. Bovendien is er voor de heden-functie van LFR ook steeds een politieambtenaar nodig die monitort en een team dat interventies kan doen naar aanleiding van een mogelijke match.[[748]](#footnote-748)

Nick Noël voegt hier nog aan toe dat ook extra personeel nodig is dat het mogelijk maakt voor betrokkenen om hun rechten uit te oefenen. Zo moet een belangenafweging worden gemaakt tussen de belangen van het onderzoek en de bescherming van de openbare orde en het individuele belang van de betrokkene.[[749]](#footnote-749)

Om te berekenen of de maatregel met LFR een efficiëntiewinst inhoudt, zal men rekening moeten houden met een hele reeks van variabelen: met de oorspronkelijke investering, maar ook met continue kosten van onderhoud en kosten van personeel om de camera’s te bemannen.[[750]](#footnote-750) Er zal onderzocht moeten worden wat de beste methode is om van de technologie een kosten-batenanalyse te maken en welke elementen daarbij in rekening moeten worden genomen. Het kan dan ook interessant zijn om bij het bepalen van de rechtsgrond met het **voorzorgsbeginsel** (of “precautionary principle”) rekening te houden, dat zegt dat het beter is te werken met een geverifieerde IT-tool dan met een IT-tool waarvan de effectiviteit nog niet volledig is getest.[[751]](#footnote-751)

Hieruit blijkt dat het wenselijk kan zijn om in bepaalde gevallen **proefprojecten** toe te staan met LFR om de effectiviteit ervan te meten. De maatschappelijke en juridische voorwaarden voor proefprojecten met LFR worden uiteengezet in het onderzoek van de London Policing Ethics Panel.[[752]](#footnote-752)

## Conclusie

Live Facial Recognition maakt het mogelijkheden om automatisch gezichten te herkennen. Het gebruik ervan biedt **mogelijkheden** voor de Belgische geïntegreerde politie bij het vervullen van haar politionele opdrachten. Het is belangrijk om hierbij het hoger doel van de politie in rekening te nemen om te waken over de individuele mensenrechten en de democratische ontwikkeling van de maatschappij na te streven. Het lijkt echter aangewezen om aan de hand van onafhankelijk ethisch en wetenschappelijk onderzoek te bestuderen in welke mate het gebruik van LFR de politie effectief kan helpen om op een efficiënte manier haar opdrachten uit te oefenen.

Er bestaat een risico dat door het gebruik van LFR (door de politie) het **recht op eerbiediging privéleven en het recht op bescherming persoonsgegevens** worden ingeperkt. Bovendien dreigen daardoor ook andere verweven grondrechten zoals het recht op de vrijheid van meningsuiting, het recht op een eerlijk proces en het non-discriminatiebeginsel in het gedrang te komen.

Momenteel is er een gebrek aan een **wettelijk kader** dat het gebruik van LFR reguleert en is het niet toegelaten voor de politie om de technologie te gebruiken. Het voorstel van verordening van de Europese Commissie wil verschillende mogelijkheden van LFR uitsluiten, waardoor nu wordt gezocht naar de mogelijkheden voor een wettelijk kader dat het gebruik van LFR reguleert. In die zoektocht is het belangrijk een onderscheid te maken tussen de **wenselijkheid** van een maatregel die voorziet in het gebruik van LFR door de geïntegreerde politie en de proportionaliteit van zulke maatregel.

Het antwoord op de eerste vraag naar **wenselijkheid** hangt af van het antwoord op de tweede die toetst naar de mate waarin een concrete maatregel proportioneel is. Om de vraag naar proportionaliteit te beantwoorden moeten eerst enkele vraagstukken rond privacy worden opgelost.

Ten eerste **stelt zich de vraag hoe een concrete proportionaliteitsbeoordeling van een maatregel die in het gebruik van LFR voorziet eruit moet zien**. Door de strikte verwevenheid van het recht op bescherming persoonsgegevens en het recht op eerbiediging privéleven is het op dit moment namelijk erg onduidelijk met welke vereisten men hierbij allemaal rekening moet houden. Beide rechten blijken voort te vloeien uit een gedeelde **wezenlijke inhoud**, die verschillende interpretaties kent. Het lijkt aangewezen om te zoeken naar een werkbaar begrip van deze wezenlijke inhoud, waardoor men de fundamentele rechten van privacy (het recht op eerbiediging privéleven en het recht op bescherming persoonsgegevens) zo kan toepassen dat ze de “wezenlijke inhoud” kunnen beschermen tegen het risico dat het filmen zonder onderscheid met LFR ontaardt in mass surveillance.[[753]](#footnote-753)

Een **tweede belangrijke vraag is hoe en in welke mate een proportionaliteitsbeoordeling de ontwikkeling van LFR hierbij in rekening moet nemen**. Zo blijkt immers dat in de ontwikkelingsfase reeds **inperkingen** gebeuren van privacy van betrokkenen. Zo wordt immers een grote hoeveelheid gevoelige persoonsgegevens verwerkt om LFR mee te trainen. Om de wenselijkheid van het gebruik van LFR te beoordelen lijkt het dan ook aangewezen om af te wegen in welke mate de inperkingen op privacy in de ontwikkelingsfase proportioneel waren. Gebeurde het verzamelen van de persoonsgegevens bijvoorbeeld met toestemming of werden deze inperkingen op een andere manier geremedieerd?

Tegelijkertijd blijkt dat er zich in de ontwikkelingsfase ook verschillende **problemen voordoen die consequenties** hebben voor de mate waarin LFR privacy inperkt in de gebruiksfase. Een gebrek aan diversiteit in de trainingsdatasets van LFR zorgt bijvoorbeeld voor een inperking van het beginsel van nauwkeurigheid in de gebruiksfase. Zo worden ook functionaliteiten van LFR ontwikkeld zonder daarbij de concrete doeleinden van het uiteindelijke gebruik in rekening te nemen, wat een risico op function creep creëert. De bestaande privacygaranties bij de aankoop van LFR lijken niet voldoende succesvol om inperkingen op privacy bij later gebruik te kunnen voorkomen. De vraag is in welke mate methoden zoals innovation procurement hierbij meer garanties kunnen bieden.

Het probleem bij zowel de inperkingen in de ontwikkelingsfase zelf (die ook gevolgen kunnen hebben bij het gebruik) en de problemen die consequenties kunnen hebben voor de gebruiksfase is dat er **weinig** **juridische mogelijkheden** zijn om de proportionaliteit van deze verwerkingen te beoordelen. Het recht op bescherming persoonsgegevens en het recht op eerbiediging privéleven hebben immers horizontale werking en de ontwikkelaar lijkt niet binnen het toepassingsgebied te vallen van de privacywetgeving die van beide rechten de uitwerking vormt.

Het lijkt dan ook aangewezen om de privacyvoorwaarden in het **gegevensbeschermingsrecht** ook van toepassing te maken op de ontwikkelaar. Men zal echter moeten bepalen in welke mate de proportionaliteit van een mogelijke inperking van privacy in de ontwikkelingsfase moet worden beoordeeld vanuit de **proportionaliteitsbeoordeling van het latere gebruik** ervan of in een **proportionaliteitsbeoordeling van de ontwikkelingsfase op zich.**

In de zoektocht naar een wettelijk kader rond het gebruik van LFR lijkt het met andere woorden noodzakelijk om twee vraagstukken te beantwoorden:

1. Hoe moet een proportionaliteitsbeoordeling worden gemaakt van het gebruik van LFR?
2. Hoe en in welke mate dienen daarbij te worden beoordeeld: a) de inperkingen op privacy in de ontwikkelingsfase en b) de problemen in de ontwikkelingsfase die een impact hebben op de bescherming van privacy bij het latere gebruik van LFR?

Enkel wanneer men deze vraagstukken beantwoordt, lijkt het mogelijk om een proportionaliteitsbeoordeling te maken van het gebruik van LFR, wat nodig is om te bepalen of en welk concreet gebruik van LFR precies wenselijk is in een democratische samenleving.

## Bibliografie

1. **Wetgeving**
2. Internationaal
* *Harde wetgeving*

RVE, Verdrag van 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden, *BS,* 19 augustus 1955.

RVE, ETS. no 108 Convention of 28th of January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

EG, Verordening nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlĳke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrĳe verkeer van die gegevens, *Pb. L.* 12 januari 2001, afl. 8.

EG, Richtlĳn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlĳke levenssfeer in de sector elektronische communicatie (richtlĳn betreffende privacy en elektronische communicatie), *Pb.L* 31 juli 2002, afl. L 201.

EU, Verdrag betreffende de werking van de Europese Unie (geconsolideerde versie), C 326/49, *Publicatieblad van de Europese Unie,* 26 oktober 2012.

EU, Handvest van de grondrechten van de Europese Unie van 26 oktober 2012, *Pb.L* C326.

Verordening (EU) 2016/679 van het Europees parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb. L.* 4 mei 2016, afl. 119.

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, *Pb.L.* 4 mei 2016, afl. 119.

RVE, Convention of 18th of May 2018 for the protection of individuals with regard to the processing of personal data.

EUROPEES PARLEMENT, RAAD, Richtlijn (EU) 2019, 790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG.

Zachte wetgeving

Europees

EC, “Tool #28. Fundamental Rights & Human Rights” (datum niet vermeld).

WP29, “Opinion 04/2007 on the concept of personal data”, 2007.

WP29, “Opinion 02/2012 on facial recognition in online and mobile services”, 2012.

WP29, “Opinion 03/2012 on developments in biometric technologies”, 2012.

WP29, “Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector”, 2014.

EDPS, Opinion 7/2015, “Meeting the challenges of big data, a call for transparency, user control, data protection by design and accountability”, 2015.

RVE, “Fundamental Rights Compatibility- Guidelines for Council preparatory bodies”, *Publications Office European Union,* 2015.

WP29, “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”*,* 2017.

WP29, Guidelines on consent under Regulation 2016/679, 2018.

FRA, “Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level-Guidance”,2018.

AI HLEG, “Ethics Guidelines for Trustworthy AI”, *AI HLEG,* 2018.

EDPS, “Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data”, *EDPS* 2019.

RvE, COMMISSARIS VOOR MENSENRECHTEN, “Unboxing Artificial Intelligence: 10 steps to protect Human Rights”, 2019.

EC, “White Paper-On Artificial Intelligence-A European approach to excellence and trust, 2020.

EDPS, “A preliminary opinion on data protection and scientific research”, 2020.

EDPB, “EDPB response to MEPs Sophie in ‘t Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI.”, 2020.

RvE, “Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems”, 2020.

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA- CONVENTION 108*-*“Guidelines on Facial Recognition”, *Directorate General of Human Rights and Rule of Law*, 2021.

EC, “Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts”, nr. 2021/0106 (COD), *EU,* 2021.

EC, “Annexes accompanying the Proposal for a Regulation of the European Parliament and of the Council”, nr. SWD (2021) 84 final, 2021.

Andere landen

CNIL, facial recognition, for a debate living up to the challenges, *CNIL,* 2019.

UK Surveillance Camera Commissioner, “Facing the Camera, Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist in Public Places in England & Wales”, 2020.

1. Nationaal
* Harde wetgeving

Wetboek van 17 november 1808 van strafvordering, *BS* 27 november 1808.

Wet van 5 augustus 1992 op het Politieambt, *BS* 22 december 1992.

Nieuwe Gemeentewet van 24 juni 1988, *BS* 3 september 1988.

Wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, *BS* 5 januari 1999.

Gemeenschappelijke richtlijn MFO-3 van 14 juni 2002 van de Ministers van Justitie en van Binnenlandse Zaken betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie, *BS* 18 juni 2002.

Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 mei 2003.

Wet van 10 juli 2006 betreffende de analyse van de dreiging, *BS* 20 juli 2006.

KB van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie, *BS* 23 november 2006.

Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera’s, *BS* 31 mei 2007.

Wet van 7 mei 2014 inzake experimenten op de menselijke persoon, *BS,* 18 mei 2014.

Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS* 10 januari 2018.

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.

KB van 22 december 2017 inzake de federaal gecentraliseerde overheidsopdrachten in het kader van het federaal aankoopbeleid, *BS,* 16 januari 2018.

KB van 28 mei 2018 tot wijziging van het koninklijk besluit van 10 februari 2008 tot vaststelling van de wijze waarop wordt aangegeven dat er camerabewaking plaatsvindt, *BS* 1 juni 2018.

KB van 6 december 2018 tot vaststelling van de plaatsen waar de verwerkingsverantwoordelijke zijn bewakingscamera’s kan richten op de perimeter rechtstreeks rond de plaats, de beelden van de bewakingscamera’s gedurende drie maanden kan bewaren en toegang in real time tot de beelden kan geven aan de politiediensten, *BS* 18 december 2018.

Zachte wetgeving

COC, “Aanbeveling nr. 06/2011 van 6 juli 2011 betreffende installatie en gebruik van bewakingscamera’s in opsluitingsplaatsen (cellen en arrestantenlokalen) en andere plaatsen van het commissariaat (CO-AR-2010-04)”, *Aanbevelingen COC*, 12/13.

COC, “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, Visitatie-toezichtrapport, executive summary publieke versie, betreft”, DIO19005, 2020.

COC, “Advies van 22 september 2020 nr.DA200008 betreffende een Gemeenschappelijke richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de toegangsregels van de leden van de politiediensten tot de algemene nationale gegevensbank en de basis-, bijzondere en technische gegevensbank (richtlijn toegangsregels)”, *Adviezen COC*, 2020.

COC, “Advies nr. DD200026 van 11 februari 2021 uit eigen beweging mbt de vraag wie de verwerkingsverantwoordelijke is voor gegevensverwerkingen door de politiediensten in het kader van de uitvoering van politionele opdrachten enerzijds en voor gegevensverwerkingen onder de AVG anderzijds”, *Advies COC*, 2021.

1. Deelstatelijk

Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, *BS* 29 oktober 2008.

Decreet houdende de aanpassing van de decreten aan de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming.), *BS* 26 juni 2018.

1. **Voorbereidende werken en parlementaire stukken**

Wetsontwerp op het Politieambt van 4 juni 1991, nr. 1637/1.

Wetsontwerp van 12 maart 2002 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St. Kamer*, 2001-02, nr. 1688/1.

Toelichtingen van 14 december 2007 bij het Handvest van de Grondrechten, *Pb.L* 14 december 2007, afl. C 303/02.

Parl. St. DOC 54, n° 2855/003 van 2 maart 2018.

Voorstel van Resolutie DOC 55/1349/001 van 16 juni 2020 over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en- algoritmen in vaste of mobiele beveiligingscamera’s in openbare en privéplaatsen.

Wetsontwerp van 10 december 2020 houdende de Algemene uitgavenbegroting voor het begrotingsjaar 2021, *DOC 55 1578/023*.

1. **Rechtspraak**
2. Europees

EHRM, 6 september 1978, nr. 5029/71, *Klass en anderen.*

EHRM, 6 december 1988, nr. 10590/83, Barberà, Messegué en Jabardo/ Spanje.

EHRM, 20 maart 2001, nr. 33501/96, Telfner/Oostenrijk.

EHRM, 25 december 2001, P. G. en J. H./ Verenigd Koninkrijk.

HvJ, 17 juni 2010, nr.C-92/02, C-93/02, Volker und Markus Schecke GbR/Land Hessen.

HvJ, 17 oktober 2013, nr. C-291/12, *Schwarz/Stadt Bochum*, ECLI:EU:C:2013:670.

HvJ 8 april 2014, nrs.C‑293/12 en C‑594/12, *Digital Rights Ireland Ltd./ Minister for Communications, Marine and Natural Resources en anderen en Kärntner Landesregierung en anderen*, ECLI:EU:C:2014.

HvJ, 13 mei 2014, nr. C-131/12, *Google Inc/AEPD,* ECLI:EU:2014:317.

HvJ Schrems, 6 oktober 2015, C-362/14, *Schrems/Data Protection Commissioner,* ECLI: EU: C:2015:650.

EHRM, 12 januari 2016, nr. 37138/14, *Szabó en Vissy/Hongarije.*

HvJ 19 oktober 2016, nr. C-582/14, Patrick Breyer/Bundesrepublik Deutschland, ECLI:EU:C:2016:779.

HvJ, 21 december 2016, *Tele2Sverige/Secretary of State for the Home Department,* ECLI:EU:C:2016:970.

EHRM, 24 januari 2019, nr. 43514/15, *Catt/Verenigd Koninkrijk.*

EHRM, 4 februari 2019, nrs. 58170/13, 62322/14, 24960/15, Big Brother Watch e.a./Verenigd Koninkrijk.

HvJ, 6 oktober 2020, nrs. C-511/18, C-512/18 en C-520/18, *Quadrature du Net*, ECLI: ECLI:EU:C:2020:791.

Belgisch

Grondwettelijk Hof, 20 februari 2020, nr. 27/2020.

1. Buitenlands

High Court of Justice, 04/09/2019, nr. CO/4085/2018, The Queen Bridges/Chief Constable of South Wales Police and others.

Royal Court of Justice, Court of appeal (civil division), 11 augustus 2020, nr. C1/2019/2670, R/The Chief Constable of South Wales Police.

Bundesverfassungsgericht, 15 december 1983, nr. BvR 209/83, Volkszählungsurteil.

1. **Rechtsleer**
	1. Boeken

FRA, *Handbook on European data protection law,* Luxemburg, Imprimerie Centrale in Luxembourg 2018, 402.

GUTWIRTH, G., POULLET, Y., DE HERT, P., e.a. (eds.), *Reinventing Data Protection?,* Springer, 2009, 371.

GOOSSENS, F., (ed.), *Dragers van de politiefunctie- een dwarsdoorsnede van de reguliere politie, de Veiligheid van de staat, de bijzondere politiediensten en de private politie*, Kluwer Belgium, Mechelen 2012, 358.

LEENS, R., VAN BRAKEL, R., GUTWIRTH, S., DE HERT, P., *Data Protection and Privacythe age of intelligent machines*, HART Publishing, Bloomsbury Publishing Plc., Oxford, 2017.

MEESE, J.,“Onrechtmatig verkregen bewijs in strafzaken” in J. MEESE, *Bewijsnood na het vernieuwde bewijsrecht,* Mortsel, Intersentia, 2020,X+176.

TAYLOR, L., FLORIDI, L., VAN DER SLOOT, B., *Group Privacynew challenges of Data Technologies,* Springer International Publishing, 2017, XIII, 237.

WARNEZ, B., *De lokale bestuurlijke ordehandhaving in Vlaanderen. Een kritische analyse van de actoren en hun bevoegdheden*, Brugge, die Keure/la Charte, 2020; 336.

* 1. Artikels

AERTS, A., “Onderzoek over gebruik dna-analyse in strafonderzoeken legt pijnpunten bloot”, *De Juristenkrant,* 2018.

BRKAN, M., “The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core”, *European Constitutional Law Review,* 2018.

BRKAN, M., “The essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning”, *German Law Journal, Special issue 6: Interrogating the Essence of EU Fundamental Rights,* 2019.

BRKAN, M., “Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond”, *International Journal of Law and Information Technology,* 2019.

CEYHAN, A., “Analyser la sécurité: Dillon, Waever, Williams et les autres”, *Cultures & Conflits,* 1998.

EDWARDS, L., VEALE, M., “Slave to the algorithm? Why a “right to an explanation” is probably not the remedy you are looking for”, [16 Duke Law & Technology Review 18, 2017](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855).

DE SCHEPPER,T., DE HERT, P., “Versoepeling Camerawet grondwettelijk getoetst. De doelgroepen kunnen rustig werken, terwijl camera’s draaien, rijden, vliegen en gelinkt worden met politiedatabanken.”, *NjW* 2020, afl. 669 e.v.

DE SCHEPPER, T., “Welke regels gelden voor de verwerking van ANPR-data?”, *Politeia Uitgeverij,* 2020.

DWARDS, L., VEALE, M., “Slave to the algorithm? Why a “right to an explanation” is probably not the remedy you are looking for”, [*16 Duke Law & Technology Review 18,* 2017](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855).

FRANTZIOU, E., “The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality”, *European Law Journal,* 2015.

HENDERSON, S., E., “Expectations of Privacy in Social Media”, *Mississippi College Law Review,* 2012.

KAMMOURIEH, L., BAAR, T., BERENS, J., e.a., “Group Privacy in the Age of Big Data”, *Philosophical Studies Series,* 2016.

MAES, E., PANZAVOLTA, M., “Op zoek naar normatief principe voor uitsluiting van onrechtmatig verkregen bewijs in tijdperk van “mass data gathering””, *de Juristenkrant,* 2021.

MELGAÇO, L., “Meer camera’s, meer veiligheid? Een analyse over de doeltreffendheid van videosurveillance”, *Orde van de Dag,* 2015.

MITTELSTADT, B., “From individual to group privacy in Big Data Analytics”, *Philosophy & Technology,* 2017.

MOREHAM, N., A., “Privacy in Public Places”, *The Cambridge Law Journal,* 2006.

NISSENBAUM, H., “Privacy as Contextual Integrity”, *Washington Law Review* 2004.

RISACK, L., “Mogen Belgische politieagenten een bodycam dragen?”, *Rechtenkrant,* 12 februari 2020

SAJFERT, J., QUINTEL, T., “Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities”, *Edward Elgar Publishing,* 2019.

SOLOVE, D., J., ““I’ve got nothing to hide” and Other Misunderstandings of Privacy”, *San Diego Law Review* 2007.

VAN BRAKEL, R., “Een reflectie over het huidige toezicht van het gebruik van surveillancetechnologie door de lokale politie in België”, *Cahiers Politiestudies,* 2020.

VERMEULEN, G., “Non-Paper-Workshop ‘Targeted surveillance and selective data retention’”, *International Intelligence Oversight Forum (IIOF2017) ‘The Road Ahead*. *Dilemmas and Best Practices in Democratic Intelligence Oversight’ Brussels*, 2017.

WARNEZ, B., “Het beginsel van kenbaarheid en de lokale bestuurlijke ordehandhaving”, *Tijdschrift voor Wetgeving,* 2019.

* 1. Rapporten en grijze literatuur

CDEI, “Snapshot Series: Facial Recognition Technology”, *CDEI,* 2020.

DATATILSYNET, (Noorse GBA), “Report on Artificial intelligence and privacy”, 2018.

DIRECTIE ONDERZOEK EN DOCUMENTATIE, “Themafiche Bescherming van persoonsgegevens”, *HVJ,* 2020.

FRA, “Facial recognition technology: fundamental rights considerations in the context of law enforcement”, *FRA Focus* 2019.

GALLE, J., WITTERS, S., “Template Risico-Analyse DPIA”, *Postgraduaat DPO Howest,* 2021.

KENNISCENTRUM DATA EN MAATSCHAPPIJ, “Rapport over bevoegdheden in het delen van gegevens-automatische kentekenplaatherkenning (ANPR) als toepassingsgeval”, *Kenniscentrum Data en Maatschappij,* 2021.

LIGA VOOR MENSENREHTEN, “Mensenrechten-Een kennismaking”, *Liga voor Mensenrechten,* 2009.

RvE, Guide on article 8 of the European Convention of Human Rights.

1. Blogs

GATTA, F. L., “Social media and applications to the ECtHR: connecting people in the name of human rights?”, *Strasbourg Observers,* 2020.

VOGIATZOGLOU, P., “Mass Surveillance and the European Courts”, *KULeuven CiTiP,* 2017.

X, “Big brother may continue watching you”, *Strasbourg Observers,* 2018.

**Wetenschappelijke literatuur**

Boeken

CARAYANNIS, E., G., CAMPBELL, D.F., J, *Mode 3 Knowledge Production in Quadruple Helix Innovation Systems, 21st-Century Democracy, Innovation, and Entrepeneurship for Development,* Springer, New York, 2012, VI, 63.

CALDER, A., “Implementing Information Security based on ISO 27001/ISO 27002”, *Van Haren,* 2011.

CHUN, W.H.K., *Programmed Visions: Software and Memory*, Cambridge, MA: MIT Press*,* 2011, 239p.

COHN, A., G., THOMAS, J., R., *Artificial Intelligence and Its Applications,* John Wiley and Sons, Warwich University, 1986, 306p.

GATES, K. A., *Our Biometric Future- Facial Recognition Technology and the Culture of Surveillance,* New York University Press, 2011, 274p.

GITELMAN, L., *Raw Data is an oxymoron*, Cambridge, Massachusetts, MIT Press, 2013, 192p.

PASQUALE, F., *The Black Box Society, The Secret Algorithms that control money and information*,Harvard University Press, Cambridge Massachusetts, 2015, 320p.

KUBITSCHKO, S.A., KAUN, A., *Innovative Methods in Media and Communication Research*, London: Palgrave Macmillan, 2017, 82. 330p.

LI, S., Z., JAIN, A., K., *Handbook of Face Recognition*, Springer, New York, 2005, 714p.

RODENHUIS, W., *Basisboek Integrale Veiligheid,* Boom Uitgevers, Den Haag, 2011, 545p.

STALLINGS, W., *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices,* Addison-Wesley Professional, 2019*,* 70, 528.

SUDMANN, A., (ed.), *The Democratization of Artificial lntelligence Net Policies in the Era of Learning Algorithms*, Transcript Verlag, Bielefeld, 2019, 331p.

VON SILVIA-TARUCA LARSEN, B, *Setting the Watch: Privacy and the Ethics of CCTV Surveillance,* London: Hart Publishing, 2011, 226p.

ZUBOFF, S., *The Age of Surveillance Capitalism,* Public Affairs New York, 2019, 704p.

1. Rapporten

BUOLAMWINI, J., GEBRU, T., “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification”, *Proceedings of Machine Learning Research,* 2018.

DAVIES, B., DAWSON, A., INNES, M., “An evaluation of South Wales Police’s Use of Automated Facial Recognition”, *Universities’ Police Science Institute, Crime & Security Research Institute Cardiff University,* September 2018.

FUSSEY, P., MURRAY, D., “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Technology”, *The Human Rights, Big Data and Technology Project,* 2019.

GARVIE, C., BEDOYA, A., FRANKLE, J., “The perpetual line-up: unregulated police face recognition in America”, *Georgetown Law- Center on Law and Technology,* 2016.

GARVIE, C., “Garbage in, garbage out, face recognition on flawed data”, *Georgetown Law Center on Privacy & Technology,* 2019.

HOMBURG, G., SCHREIJENBERG, A., VAN DEN TILLAART, H., BLEEKER, Y., “ANPR: Toepassingen en ontwikkelingen”, *Wetenschappelijk Onderzoeks-en Documentatiecentrum (WODC),* 2016, 1, 11.

INTRONA, L., D., NISSENBAUM, H., “Facial Recognition Technology-A Survey of Policy and Implementation Issues”, *New York University, CCPR- Center for Catastrophic preparedness and response,* 2009.

LONDON POLICING ETHICS PANEL, “Final Report on Live Facial Recognition”, in opdracht van de Mayor of London, 2019.

ODSC-Open Data Science, “The impact of racial bias in facial recognition software”, *ODSC,* 2018.

UNIVERSITEIT VAN TILBURG, “Op het eerste gezicht: een verkenning van gezichtsherkenning en privacyrisico’s in horizontale relaties”, *WODC,* 2020.

WEST, S., M., WHITTAKER, M., CRAWFORD, K., “Discriminating systems, Gender, Race, and Power in AI”, *AI Now Institute,* 2019.

1. Artikels

BALLANTYNE, M., BOYER, R.S., HINES, L., “Woody Bledsoe His Life and Legacy”, *AI Magazine,* 1996.

CAVALLINI, S., SOLDI, R., e.a., “Using the Quadruple Helix Approach to Accelerate the Transfer of Research and Innovation Results to Regional Growth”, *EU* 2016.

DISTERER, G., “ISO/IEC 27000, 27001 and 27002 for Information Security Management”, *Journal of Information Security,* 2013.

GÜRSES, S., TRONCOSE, C., DIAZ, C., “Engineering Privacy by Design”, *KULeuven, gepresenteerd op Conference on Computers, Privacy & Data Protection,* 2011.

HICKOK, M.,” Lessons learned from AI ethics principles for future actions”, *AI and Ethics* 2020.

HURST, A., C., E., “Facial recognition software in clinical dysmorphology”, *Current Opinion in Pediatrics,* 2018.

INTRONA, L., D., WOOD, D., “Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems”, *Surveillance & Society,* 2004.

ISAAC, J., HANNA, M., J., “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection”, *IEEE,* 2018.

KOSILEK, R., P., FROHNER, R., WÜRTZ, R., P., “Diagnostic use of facial image analysis software in endocrine and genetic disorders: review, current results and future perspectives”, *European Journal of Endocrinology,* 2015.

MARTINEZ-MARTIN, N., “What are important ethical implications of using facial recognition technology in health care?”, *AMA Journal of Ethics,* 2019.

RABIA, S.-H., SCHNEIDER, H., NAVARRO, E., e.a., “Automatic recognition of the XLHED phenotype from facial images”, *American Journal of Medical Genetics,* 2017.

RAJI, I.D., FRIED, G., “About Face: a survey of Facial Recognition Evaluation”, *Research Gate,* 2021.

RADTKE, T.,“The concept of joint control under the data protection law enforcement directive 2016/680 in contrast to the GDPR.”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* 2020.

SHARIF, M., NAZ, F., “Face Recognition: A Survey”, *Journal of Engineering Science and Technology Review* 2017.

RAI, A., “Explainable AI: from black box to glass box”, *Journal of the Academy of Marketing Science,* 2020.

RAIJI, I., D., GEBRU, T., MITCHELL, M., BUOLAMWINI, J., e.a., “Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing”, *AIES’ 2020: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society,* 2020.

WELSH, B., C., D. FARRINGTON, P., “Crime prevention effects of closed-circuit television: a systematic review”, *Home Office Research,* 2002.

ZIMMER, M., ““But the data is already public”: on the ethics of research in Facebook”, *Ethics and Information Technology,* 2010.

**Nieuwsartikels**

BREWSTER, S., “How Google’s new photos app can tell cats from dogs”, *Wired,* 6 maart 2015.

BREWSTER, “Drones with Facial Recognition Are Primed to Fly-But The World Isn’t Ready Yet”, *Forbes,* 2021.

BURGESS, M., “Facial Recognition Tech used by UK police is making a ton of mistakes”, *Wired,* 2018.

CLERIX, K.,“Knack onderzoekt: “Het ANPR-cameraschild riskeert zich tegen de politie te keren”, *Knack,* 18 maart 2020.

COOSEMANS, D., “Vanaf morgen mag de politie u filmen met dashcams en bodycams”, *Gazet van Antwerpen,* 24 mei 2018.

DEARDEN, L., “Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested”, *Independent,* 31 januari 2019.

DEARDEN, “L., Facial Recognition wrongly identifies public as potential criminals 96% of time, figure reveals”, *Independent,* 7 mei 2019.

DOBBELAERE-WELVAERT, “Slimme camera’s gericht op de voorkant van wagens? Weg naar China is geplaveid met naïeve bedoelingen”, *Knack,* 28 november 2019.

ESPINOZA, J., “EU backs away from call for blanket ban on facial recognition tech”, *Irish Times,* 12 februari 2020.

HILL, K., “The secretive company that might end privacy as we know it”, *The New York Times,* 2020.

HSU, H.-J., CHEN, K.-T., “Face Recognition on drones”, *Conference: the first workshop,* 2015; T.

KAV, “Aantal camera’s in België vervijfvoudigt: op ruim 47 000 plaatsen wordt u gefilmd”, *De Morgen,* 12 augustus 2017

MARR, B., “Facial Recognition Technology: Here are the Important Pros and Cons”, *Forbes,* 2019

NAAFS, S., “Gezichtsherkenning rukt op: kunnen we weldra niet meer anoniem over straat?”, *Knack,* 21 augustus 2019.

POKHARNA, H., “For Dummies-The Introduction to Neural Networks we all need! (Part 1)”, *Medium,* 2016.

PORTER J., “Facebook and Linkedin are latest to demand Clearview stop scraping images for facial recognition tech”, *The Verge,* 2020.

PTI, “Delhi: Facial recognition system helps trace 3000 missing children in 4 days”, *Times of India,* 22 april 2018.

SCHUERMANS, F.,“Een vernieuwde speler in het politielandschap”, *Blue Trends,* 2019.

STRUYS, B., “2 jaar na invoering laat De Crem gebruik bodycams door politie onderzoeken: “Er moet een kader komen””, *De Morgen,* 4 juli 2020.

VANHECKE, N., “Éen stap van gezichtsherkenning verwijderd: Kortrijk vindt in geen tijd de man in de rode trui”, *De Standaard,* 24 mei 2019.

VANMELDERT, D., “Steeds meer camera’s in het straatbeeld: “Ze voorkomen criminaliteit niet, de samenleving wordt er niet beter van”, *Vrt Nws,* 25 maart 2021.

VANRENTERGHEM, A.,“U wordt gefilmd: nieuwe camerawet maakt onder meer bodycams, drones en een slim cameraschild mogelijk”, *Vrt Nws,* 13 maart 2018.

WARD, J., SOTTILE, C., “A facial recognition company wants to help with contact tracing. A senator has questions.”, *NBC News,* 1 mei 2020.

1. **Websites[[754]](#footnote-754)**

<https://www.rug.nl/language-centre/communication-training/academic/hacv/handboek/schriftelijk/student/bronnen-literatuur/onderzoek>.

<https://www.linkedin.com/company/european-digital-rights/>.

<https://www.europarl.europa.eu/infographic/legislative-procedure/index_nl.html>.

<https://docs.aws.amazon.com/rekognition/latest/dg/faces-sqs-video.html>.

<https://www.avigilon.com/products/video-infrastructure/ai-nvr>.

<https://www.avigilon.com/products/cameras-sensors/h5a-cr>.

<https://www.politieantwerpen.be/jaarboek/anpr>.

<https://www.pzvlas.be/nieuws/article/detail/gestolen-voertuig-met-drugsdealer-aan-het-stuur-gestopt-dankzij-hit-met-anpr-camera>.

<https://www.jobpol.be/nl/administratieve-jobs/functioneel-beheerder-dienst-informatie-analyse-en-kennisbeheer>.

<https://www.politie.be/5998/nl/over-ons/geintegreerde-politie/voorstelling>.

<https://www.politie-oostende.be/lokaal-informatiekruispunt-lik>.

<https://www.politie.be/5379/nieuws/pz-kanton-borgloon-en-politie-limburg-regio-hoofdstad-kopen-twee-anpr-cameras-aan>.

<https://www.politie.be/5998/nl/over-ons/federale-politie>.

<https://www.politie.be/5998/nl/over-ons/bestuurlijke-politie/luchtvaartpolitie>.

<https://www.amazon.com/Recognition-Temperature-Measurement-Detection-Comparison/dp/B087NQXND2>.

[https://www.controleorgaan.be/nl/politiediensten/camerawetgeving#](https://www.controleorgaan.be/nl/politiediensten/camerawetgeving).

<https://www.comiteri.be/index.php/nl/vast-comite-i>.

<https://www.comiteri.be/index.php/nl/vast-comite-i/acht-taken-mainmenu-61>.

<https://cirb.brussels/fr/nos-solutions/infrastructure-solutions/portlet-fidus/commission-de-controle-bruxelloise>.

<https://www.controleorgaan.be/nl/controleorgaan/samenstelling-van-de-organisatie>.

<https://comitep.be/wie-controleren-wij.html>.

<https://www.dekamer.be/kvvcr/showpage.cfm?section=none&language=nl&cfm=/site/wwwcfm/search/search_new.cfm?db=searchpdf>.

<https://www.europarl.europa.eu/doceo/document/E-8-2018-005624_EN.html>.

<https://www.briefcam.com/who-we-serve/law-enforcement/>.

<https://cs231n.github.io/convolutional-networks/#overview>.

<https://developer.twitter.com/en/developer-terms/more-on-restricted-use-cases>.

<https://www.politie.be/5998/nl/over-ons/centrale-directies/centrale-directie-van-technische-en-wetenschappelijke-politie>.

<https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg/deelnemers-aan-federaal-aankoopmodel>.

<https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg/gemeenschappelijke-overeenkomsten-go-passieve>.

<https://www.proximus.be/en/id_b_cl_axis_partner_award/companies-and-public-sector/blog/news-blog/news/axis-partner-award.html>.

<https://www.iso.org/about-us.html#2>.

<https://www.27000.org/background.html>.

<https://www.iso.org/standard/42103.html>.

<https://ec.europa.eu/digital-single-market/en/innovation-procurement>.

<https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html>.

<https://ec.europa.eu/digital-single-market/en/public-procurement-innovative-solutions>.

<https://www.politieacademie.nl/thema/politieleiderschap/Advanced%20Programmes/Paginas/Columbus-VIII.aspx>.

<https://ec.europa.eu/digital-single-market/en/open-innovation-20>.

<https://www.politie.be/5998/nl/over-ons/centrale-directies/centrale-directie-van-technische-en-wetenschappelijke-politie>.

<https://police-hackathon.be/nl/>.

<https://speed.wazoku.com/#/community/b6e9b42e2627478ba8cc9b5a17357428/home-page>.

<https://news.belgium.be/nl/gemeenschappelijke-gegevensbank-terrorist-fighters>.

<https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security>.

<https://www.politieantwerpen.be/privacyverklaring>.

<https://www.howest.be/nl/opleidingen/postgraduaat/data-protection-officer/praktisch#Waaruit-bestaat-uit-het-programma>.

<https://www.avigilon.com/solutions/covid-19-resources/no-face-mask-detection>.

<https://www.danners.com/security/covid-19-security-solutions/>.

1. **Blogs**

C. BURT, “Dermalog and Pensees roll out computer vision temperature check systems for access control”, *Biometric Update.com,* 2020; <https://www.biometricupdate.com/202004/dermalog-and-pensees-roll-out-computer-vision-temperature-check-systems-for-access-control>.

R. MERKLEY, “Use and Fair Use: Statement on shared images in facial recognition AI”, *Creative Commons,* 2019; <https://creativecommons.org/2019/03/13/statement-on-shared-images-in-facial-recognition-ai/>.

SMITH, J. R., “IBM Research releases ‘Diversity in Faces’ Dataset to Advance Study of Fairness in Facial Recognition Systems”, *IBM,* 2019.

[https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.`](https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.%60)

1. **Andere**

DORMAELS , A., (VIAS INSTITUTE), “Presentatie ‘Belangrijkste bevindingen uit omgevingsanalyse en knelpuntennota’”, gepresenteerd op 19 november 2020 tijdens de ‘Webinar ANPR-camera’s: slimmer dan gedacht’

FEDERALE POLITIE, “Jaarverslag 2015”, <https://www.politie.be/5998/nl/jaarverslag-2015>, 8.

VERHEYDEN, T., “Privacy & Ik”, *Vrt,* 2021.

Presentatie Willem Debeuckelaere, “Gegevensbescherming in België na de GDPR/AVG**”,** 3 maart 2020, binnen het vak “Gegevensbeschermingsrecht” UGent.

1. S. ZUBOFF, *The Age of Surveillance Capitalism,* Public Affairs New York, 2019, 12. [↑](#footnote-ref-1)
2. I. D. RAJI, G. FRIED, “About Face: a survey of Facial Recognition Evaluation”, *Research Gate,* 2021, 2; <https://www.researchgate.net/publication/348958353_About_Face_A_Survey_of_Facial_Recognition_Evaluation>; M. BALLANTYNE, R. S. BOYER, L. HINES, “Woody Bledsoe His Life and Legacy”, *AI Magazine,* 1996, 7; K. A. GATES, *Our Biometric Future- Facial Recognition Technology and the Culture of Surveillance,* New York University Press, 2011, 28-29. [↑](#footnote-ref-2)
3. Ibid 2, 3. [↑](#footnote-ref-3)
4. Rapport van European Union Agency on Fundamental Rights, “Facial recognition technology: fundamental rights considerations in the context of law enforcement”, *FRA Focus* 2019, 7. [↑](#footnote-ref-4)
5. Ibid 4, 7. [↑](#footnote-ref-5)
6. Het COC houdt toezicht op de gegevensbescherming bij politiediensten. COC, “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, Visitatie-toezichtrapport, executive summary publieke versie, betreft”, DIO19005, 2020; <https://www.controleorgaan.be/files/DIO19005_Onderzoek_LPABRUNAT_Gezichtsherkenning_Publiek_N.PDF>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-6)
7. Hierna zal ik voor dit recht de term “het recht opeerbiediging privéleven” gebruiken. Wanneer ik het woord privacy gebruik, verwijs ik zowel naar de eerbiediging van het privéleven als naar het recht op bescherming persoonsgegevens. Dit begrip moet worden onderscheiden van “privacy” (tussen aanhalingstekens) waarbij ik verwijs naar de wezenlijke inhoud van beide fundamentele rechten, de inhoud van privacy. [↑](#footnote-ref-7)
8. Ibid 4, 7. [↑](#footnote-ref-8)
9. Wetsontwerp van 10 december 2020 houdende de Algemene uitgavenbegroting voor het begrotingsjaar 2021, *DOC 55 1578/023*, 125. [↑](#footnote-ref-9)
10. J. ESPINOZA, “EU backs away from call for blanket ban on facial recognition tech”, *Irish Times,* 12 februari 2020. [↑](#footnote-ref-10)
11. Europese Commissie, “White Paper-On Artificial Intelligence-A European approach to excellence and trust, 2020. (Europese Commissie, hierna EC) (hierna: White Paper). [↑](#footnote-ref-11)
12. EC, “Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts”, nr. 2021/0106 (COD), *EU,* 2021, 6; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021SC0084&qid=1619447658825>;(geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-12)
13. Art. 7 (en 8) EU, Handvest van de grondrechten van de Europese Unie van 26 oktober 2012, *Pb.L* C326. (hierna: HEU) [↑](#footnote-ref-13)
14. Art. 8 EVRM, art. 7 HEU. [↑](#footnote-ref-14)
15. Bronnen voor literatuuronderzoek; <https://www.rug.nl/language-centre/communication-training/academic/hacv/handboek/schriftelijk/student/bronnen-literatuur/onderzoek>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-15)
16. Het is immers zowel juridische als technische materie. Bovendien raakt het ook aan ethische en sociologische problematieken. [↑](#footnote-ref-16)
17. Data protection officer/functionaris voor gegevensbescherming. [↑](#footnote-ref-17)
18. Hierna: PZ. [↑](#footnote-ref-18)
19. Kortrijk, Kuurne, Lendelede. [↑](#footnote-ref-19)
20. De Panne, Koksijde, Nieuwpoort. [↑](#footnote-ref-20)
21. Kortemark, Koekelare, Houthulst, Diksmuide. [↑](#footnote-ref-21)
22. Roeselare, Izegem, Hooglede. [↑](#footnote-ref-22)
23. <https://www.linkedin.com/company/european-digital-rights/>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-23)
24. Linkedin was voor mij niet enkel een handig hulpmiddel om respondenten te zoeken, maar ook om bij te blijven met literatuuronderzoek en beleidsontwikkelingen. Mijn Linkedin- netwerk telde immers verschillende (gezaghebbende) onderzoekers die bezig waren met mijn onderzoeksonderwerp, en regelmatig onderzoek, soft law en evenementen deelden die interessante informatie bevatten voor mijn onderzoek. [↑](#footnote-ref-24)
25. G. HOMBURG, A. SCHREIJENBERG, J. VAN DEN TILLAART, Y. BLEEKER, “ANPR: Toepassingen en ontwikkelingen”, *Wetenschappelijk Onderzoeks-en Documentatiecentrum (WODC),* 2016, 1, 11. [↑](#footnote-ref-25)
26. Dit dient echter genuanceerd te worden: de kentekenplaat van een bekend persoon bijvoorbeeld zou eventueel wel als gevoelig kunnen worden beschouwd. De kwalificatie “gevoelig” hangt erg af van de context. [↑](#footnote-ref-26)
27. Zie voor een uiteenzetting van de werking van LFR met databanken: Deel X, 3, b. [↑](#footnote-ref-27)
28. Art. 44/2 §3 Wet van 5 augustus 1992 op het Politieambt, *BS,* 22 december 1992; M. DOBBELAERE-WELVAERT, “Slimme camera’s gericht op de voorkant van wagens? Weg naar China is geplaveid met naïeve bedoelingen”, *Knack,* 28 november 2019. [↑](#footnote-ref-28)
29. K. CLERIX, “Knack onderzoekt: “Het ANPR-cameraschild riskeert zich tegen de politie te keren”, *Knack,* 18 maart 2020; Bronnen van de documentaire T. VERHEYDEN, “Privacy & Ik”, *Vrt,* 2021, verkregen via eindredacteur Maarten Boone, die dit opvraagde bij de federale politie. [↑](#footnote-ref-29)
30. Automatic Facial Recognition. [↑](#footnote-ref-30)
31. Rapport van European Union Agency on Fundamental Rights, “Facial recognition technology: fundamental rights considerations in the context of law enforcement”, *FRA Focus* 2019, 7; <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>; <https://www.europarl.europa.eu/doceo/document/E-8-2018-005624_EN.html>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-31)
32. FEDERALE POLITIE, “Jaarverslag 2015”, <https://www.politie.be/5998/nl/jaarverslag-2015>, 8. [↑](#footnote-ref-32)
33. Ibid 31, 7. [↑](#footnote-ref-33)
34. Ibid 31, 8. [↑](#footnote-ref-34)
35. Ibid 31, 8 ; <https://www.europarl.europa.eu/doceo/document/E-8-2018-005624_EN.html>; (geraadpleegd op: 16 mei 2021).

 Automatic Facial Recognition. [↑](#footnote-ref-35)
36. Ibid 34 [↑](#footnote-ref-36)
37. Ibid 34. [↑](#footnote-ref-37)
38. P. FUSSEY, D. MURRAY, “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Technology”, *The Human Rights, Big Data and Technology Project,* 2019, 19. [↑](#footnote-ref-38)
39. <https://docs.aws.amazon.com/rekognition/latest/dg/faces-sqs-video.html>; <https://www.avigilon.com/products/video-infrastructure/ai-nvr>., (geraadpleegd op: 16 mei 2021); B. VON SILVIA-TARUCA LARSEN, “Does Public CCTV Violate Anonymity Interests?” in *Setting the Watch: Privacy and the Ethics of CCTV Surveillance,* London: Hart Publishing, 2011, 42; uitleg uit interview met Koen Luykx, Regional Sales Manager binnen de BENELUX bij Avigilon, Motorola Solutions. [↑](#footnote-ref-39)
40. CCTV staat voor closed circuit television surveillance. [↑](#footnote-ref-40)
41. Voor een duidelijk overzicht van verschillende types CCTV-camera’s en hun functies: B. VON SILVA-TAROUCA LARSEN, ibid 39, 42-47. [↑](#footnote-ref-41)
42. Art. 25/1 e.v. Wet op het Politieambt. [↑](#footnote-ref-42)
43. Art. 6,2 lid 1 en 7, 2 lid 1 Camerawet. De overheid kan deze bijvoorbeeld inzetten om sluikstorten te controleren (<https://mooimakers.be/kenniswijzer/artikel/inzet-van-cameras-tegen-sluikstort-onderzoek>). Ook private en bijzondere veiligheidsdiensten kunnen gebruik maken van camera’s. Dit wordt geregeld in de Wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *BS* 31 oktober 2017. (hierna: Wet op de private en bijzondere veiligheid). [↑](#footnote-ref-43)
44. KAV, “Aantal camera’s in België vervijfvoudigt: op ruim 47 000 plaatsen wordt u gefilmd”, *De Morgen,* 12 augustus 2017; <https://www.demorgen.be/nieuws/aantal-camera-s-in-belgie-vervijfvoudigt-op-ruim-47-000-plaatsen-wordt-u-gefilmd~b0b88288/>. [↑](#footnote-ref-44)
45. L. RISACK, “Mogen Belgische politieagenten een bodycam dragen?”, *Rechtenkrant,* 12 februari 2020; <https://rechtenkrant.be/mogen-belgische-politieagenten-een-bodycam-dragen/>; B. STRUYS, “2 jaar na invoering laat De Crem gebruik bodycams door politie onderzoeken: “Er moet een kader komen””, *De Morgen,* 4 juli 2020; <https://www.demorgen.be/nieuws/2-jaar-na-invoering-laat-de-crem-gebruik-bodycams-door-politie-onderzoeken-er-moet-een-kader-komen~b1fbf6a5/>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-45)
46. D. COOSEMANS, “Vanaf morgen mag de politie u filmen met dashcams en bodycams”, *Gazet van Antwerpen,* 24 mei 2018; <https://www.gva.be/cnt/dmf20180524_03527247>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-46)
47. B. VON SILVIA-TARUCA LARSEN, ibid 39, 42 e.v., 62 e.v. [↑](#footnote-ref-47)
48. Ibid 38, 20. [↑](#footnote-ref-48)
49. Ibid 38, 20. [↑](#footnote-ref-49)
50. <https://www.avigilon.com/products/cameras-sensors/h5a-cr>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-50)
51. I. D. RAJI, G. FRIED, ibid 2, 4. [↑](#footnote-ref-51)
52. N. VANHECKE**,** “Éen stap van gezichtsherkenning verwijderd: Kortrijk vindt in geen tijd de man in de rode trui”, *De Standaard,* 24 mei 2019;<https://www.standaard.be/cnt/dmf20190523_04420266>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-52)
53. Zijnde PZ Antwerpen, PZ VLAS (Kortrijk, Kuurne, Lendelelede), PZ Gent, PZ Oostende, Politiezones Limburg. [↑](#footnote-ref-53)
54. <https://www.politieantwerpen.be/jaarboek/anpr>; <https://www.pzvlas.be/nieuws/article/detail/gestolen-voertuig-met-drugsdealer-aan-het-stuur-gestopt-dankzij-hit-met-anpr-camera> ; <https://www.jobpol.be/nl/administratieve-jobs/functioneel-beheerder-dienst-informatie-analyse-en-kennisbeheer>; <https://www.politie-oostende.be/lokaal-informatiekruispunt-lik>; <https://www.politie.be/5379/nieuws/pz-kanton-borgloon-en-politie-limburg-regio-hoofdstad-kopen-twee-anpr-cameras-aan>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-54)
55. Ibid 52. [↑](#footnote-ref-55)
56. Onderverdeling uit: L. MELGAÇO, “Meer camera’s, meer veiligheid? Een analyse over de doeltreffendheid van videosurveillance”, *Orde van de Dag,* 2015, 46. [↑](#footnote-ref-56)
57. Art. 115, 3°, b) Wet op de private en bijzondere veiligheid. [↑](#footnote-ref-57)
58. Ibid 56, MELGAÇO, 46. [↑](#footnote-ref-58)
59. Dit is gangbare terminologie onder politieambtenaren, volgens Nick Noël. [↑](#footnote-ref-59)
60. Ibid 58. [↑](#footnote-ref-60)
61. Ibid 58. [↑](#footnote-ref-61)
62. B. C. WELSH, D. P. FARRINGTON, “Crime prevention effects of closed-circuit television: a systematic review”, *Home Office Research,* 2002, 7, 41 e.v. [↑](#footnote-ref-62)
63. Wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, *BS* 5 januari 1999. (vanaf hier: Wet Geïntegreerde Politie). [↑](#footnote-ref-63)
64. Art. 116, art. 118 Wet Geïntegreerde Politie. [↑](#footnote-ref-64)
65. Art. 117 Wet Geïntegreerde Politie. [↑](#footnote-ref-65)
66. Art. 3 Wet Geïntegreerde Politie. [↑](#footnote-ref-66)
67. <https://www.politie.be/5998/nl/over-ons/geintegreerde-politie/voorstelling>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-67)
68. F. GOOSSENS (ed.), *Dragers van de politiefunctie- een dwarsdoorsnede van de reguliere politie, de Veiligheid van de staat, de bijzondere politiediensten en de private politie*, Kluwer Belgium, Mechelen 2012, 30. [↑](#footnote-ref-68)
69. Art. 4 Wet Geïntegreerde Politie; <https://www.politie.be/5998/nl/over-ons/federale-politie>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-69)
70. <https://www.politie.be/5998/nl/over-ons/federale-politie>; (geraadpleegd op: 16 mei 2021). Zie ook KB van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie, *BS* 23 november 2006. [↑](#footnote-ref-70)
71. <https://www.politie.be/5998/nl/over-ons/bestuurlijke-politie/luchtvaartpolitie>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-71)
72. Art. 1 Wetsontwerp op het Politieambt van 4 juni 1991, nr. 1637/1. [↑](#footnote-ref-72)
73. Ibid 68, 9. [↑](#footnote-ref-73)
74. Ibid 68, 10. [↑](#footnote-ref-74)
75. Dit wordt immers als argument aangehaald door minister Verlinden in het Wetsontwerp houdende de Algemene uitgavenbegroting, ibid 9.

 Interview met Nick Noël, Directeur Operaties PZ Rupel: “Privacy wordt vaak als mensenrecht naar voren geschoven, maar veiligheid is minstens even belangrijk als mensenrecht. Dat is de hele insteek met camera’s: dat het veiliger wordt, dat we efficiënter kunnen werken, dat het gewoon gemakkelijker gaat voor iedereen.” Hoofddocent aan UGent in Criminologie Wim Hardyns haalt dan weer aan dat LFR een mogelijke oplossing biedt voor het handmatig identificeren van personen, wat veel capaciteit vraagt. Zie ook bijvoorbeeld de website van Clearview AI die dit argument aanhaalt ter promotie van LFR-product Clearview: <https://clearview.ai/>. [↑](#footnote-ref-75)
76. Ibid 9, Wetsontwerp Uitgavenbegroting, 125. [↑](#footnote-ref-76)
77. Ibid 56, MELGAÇO, 49. [↑](#footnote-ref-77)
78. B. MARR, “Facial Recognition Technology: Here are the Important Pros And Cons”, *Forbes,* 2019; <https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-78)
79. N-VA’er Steven Vandeput haalt facial recognition aan als mogelijk technisch hulpmiddel bij de bestrijding van corona. (Ibid 9) Zie hierbij ook deel X, 3, d): doelbinding en risico op function creep. [↑](#footnote-ref-79)
80. Piet de Vulder is DPO bij DPO bij verschillende lokale politiezones. Nick Noël is de Directeur Operaties van PZ Rupel. Nick Noël zegt over het zonaal veiligheidsplan van PZ Rupel: “We gaan capaciteit moeten besparen door in te zetten op technologie. “Da’s goed, kleef er eens een doelstelling op”, zegt hij (red: de korpschef). Ik zeg “(…)tegen 2025 hoop ik vijf percent van het personeel te besparen door het personeel in te zetten op technologie”. [↑](#footnote-ref-80)
81. Dit is de traditionele ruime onderverdeling van politie-opdrachten. Voor een gedetailleerdere uiteenzetting van (de relativiteit van) dit onderscheid, zie: B. WARNEZ, De lokale bestuurlijke ordehandhaving in Vlaanderen. Een kritische analyse van de actoren en hun bevoegdheden, Brugge, die Keure/la Charte, 2020. [↑](#footnote-ref-81)
82. B. WARNEZ, *De lokale bestuurlijke ordehandhaving in Vlaanderen. Een kritische analyse van de actoren en hun bevoegdheden*, Brugge, die Keure/la Charte, 2020, 14. [↑](#footnote-ref-82)
83. Art. 14 Wet van 5 augustus 1992, *BS* 22 december 1992 (hierna: Wet op het Politieambt in tekst/WPA in voetnoten). [↑](#footnote-ref-83)
84. Ibid 68, GOOSSENS, 14. [↑](#footnote-ref-84)
85. Ibid 68, GOOSSENS, 9. [↑](#footnote-ref-85)
86. Art. 135 §2 Nieuwe Gemeentewet van 24 juni 1988, *BS,* 3 september 1988; Ibid 82, B. WARNEZ, 21; Ibid 9, Wetsontwerp, 57. Zie ook: De promotie voor Amazons’ “non contact” LFR-technologie die bovendien temperatuur meet: <https://www.amazon.com/Recognition-Temperature-Measurement-Detection-Comparison/dp/B087NQXND2>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-86)
87. B. DAVIES, A. DAWSON, M. INNES, “An evaluation of South Wales Police’s Use of Automated Facial Recognition”, *Universities’ Police Science Institute, Crime & Security Research Institute Cardiff University,* September 2018, 9. [↑](#footnote-ref-87)
88. Ibid 31, FRA, 11. [↑](#footnote-ref-88)
89. PTI, “Delhi: Facial recognition system helps trace 3000 missing children in 4 days”, *Times of India,* 22 april 2018; <https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-89)
90. Ibid 31, 3. [↑](#footnote-ref-90)
91. Art. 15 WPA. [↑](#footnote-ref-91)
92. COC, “Aanbeveling nr. 06/2011 van 6 juli 2011 betreffende installatie en gebruik van bewakingscamera’s in opsluitingsplaatsen (cellen en arrestantenlokalen) en andere plaatsen van het commissariaat (CO-AR-2010-04)”, *Aanbevelingen COC*, 12/13. [↑](#footnote-ref-92)
93. Deze vorm van camerabewaking wordt geregeld in het Koninklijk besluit van 14 september 2007 betreffende de minimumnormen, de inplanting en de aanwending van de door de politiediensten gebruikte opsluitingsplaatsen ("cellenbesluit"), *BS 16 oktober 2007*. [↑](#footnote-ref-93)
94. Nele Krols is DPO bij een aantal Antwerpse politiezones. Belangrijke nuance: Nele Krols stelt dat zulke operationele toepassingen van LFR eerst een impact- en risicoanlyse zullen moeten vooraf gaan. Bovendien stelt ze de nood voorop aan een parlementair debat en een wetgevend kader rond LFR alvorens de toepassingen operationeel kunnen worden. [↑](#footnote-ref-94)
95. De videobewaking van politiecellen wordt eveneens geregeld door het cellenbesluit (ibid 93); Ibid 92, COC, 4/13. [↑](#footnote-ref-95)
96. Ibid 38, FUSSEY, 19 e.v. [↑](#footnote-ref-96)
97. Ibid 38, FUSSEY, 19. [↑](#footnote-ref-97)
98. Ibid 97. [↑](#footnote-ref-98)
99. Ibid 82, WARNEZ, 14 e.v. [↑](#footnote-ref-99)
100. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 669 e.v. [↑](#footnote-ref-100)
101. Aangezien het proactief gebruik van camera’s gaat over de manier waarop een camera wordt gebruikt door bestuurlijke en gerechtelijke politiediensten eerder dan de inherente mogelijkheden van de camera zelf, wordt het proactief gebruik van camera’s hier besproken en niet in het onderdeel V. 3): hoofdmechanismen. [↑](#footnote-ref-101)
102. Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS,* 12 mei 2003 (hierna: BOM-wet). [↑](#footnote-ref-102)
103. Wetsontwerp van 12 maart 2002 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St. Kamer*, 2001-02, nr. 1688/1, 8. [↑](#footnote-ref-103)
104. Art. 47 ter §1 Wetboek van 17 november 1808 van strafvordering, *BS,* 27 november 1808. (hierna: Sv). [↑](#footnote-ref-104)
105. Art. 28 bis, §2 Sv. [↑](#footnote-ref-105)
106. Art. 47 sexies, lid 1 Sv.; Ibid 103, Wetsontwerp, 32. [↑](#footnote-ref-106)
107. Art. 28 bis Sv. [↑](#footnote-ref-107)
108. Ibid 38, FUSSEY, 20. [↑](#footnote-ref-108)
109. Hierna zal ik voor dit fundamentele recht dat vervat zit in verschillende rechtsinstrumenten (EVRM, HEU,…) de term “recht op eerbiediging privéleven” gebruiken. Wanneer ik het woord privacy gebruik, verwijs ik naar zowel de eerbiediging van het privéleven als naar het recht op bescherming persoonsgegevens. Dit begrip moet worden onderscheiden van “privacy” (tussen aanhalingstekens) waarbij ik verwijs naar de wezenlijke inhoud van beide fundamentele rechten, de inhoud van privacy. [↑](#footnote-ref-109)
110. Universele Verklaring van de Rechten van de Mens van 10 december 1948 (UVRM); Het recht op eerbiediging privéleven bevindt zich in art. 12 UVRM; FRA, *Handbook on European data protection law,* Luxemburg, Imprimerie Centrale in Luxembourg 2018, 18 [↑](#footnote-ref-110)
111. RAAD VAN EUROPA, Verdrag van 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden, *BS,* 19 augustus 1955 (hierna: RVE), (hierna: EVRM). [↑](#footnote-ref-111)
112. Art. 8, lid 2 EVRM. [↑](#footnote-ref-112)
113. FRA, *Handbook on European data protection law,* Luxemburg, Imprimerie Centrale in Luxembourg 2018, p. 24. [↑](#footnote-ref-113)
114. Ibid 113, FRA, *Handbook*, 18. [↑](#footnote-ref-114)
115. RVE, ETS. no 108 Convention of 28th of January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (in werking sinds 1 oktober 1985) (Hierna: Verdrag 108). [↑](#footnote-ref-115)
116. Ibid 113, FRA, *Handbook*, 24. [↑](#footnote-ref-116)
117. Art. 3, lid 1 Gemoderniseerd Verdrag 108. [↑](#footnote-ref-117)
118. RVE, Convention of 18th of May 2018 for the protection of individuals with regard to the processing of personal data. (Hierna: Gemoderniseerd Verdrag) Zie voor het een overzicht van de wijzigingen in dit verdrag: <https://www.coe.int/en/web/data-protection/convention108/modernised>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-118)
119. Art. 7 HEU. [↑](#footnote-ref-119)
120. Art. 8, lid 1 HEU. [↑](#footnote-ref-120)
121. HvJ, 17 juni 2010, nr.C-92/02, C-93/02, Volker und Markus Schecke GbR/Land Hessen, Opinie Advocaat-Generaal Sharpston, §71. [↑](#footnote-ref-121)
122. Ibid 113, FRA, *Handbook*, 20. [↑](#footnote-ref-122)
123. HvJ 8 april 2014, nrs.C‑293/12 en C‑594/12, *Digital Rights Ireland Ltd./ Minister for Communications, Marine and Natural Resources en anderen en Kärntner Landesregierung en anderen*, ECLI:EU:C:2014:238. [↑](#footnote-ref-123)
124. Ibid 123, §§26, 27, 29. [↑](#footnote-ref-124)
125. Ibid 123, §36. [↑](#footnote-ref-125)
126. Art. 8 HEU. [↑](#footnote-ref-126)
127. Verordening (EU) 2016/679 van het Europees parlement en de raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb. L.* 4 mei 2016, afl. 119. (Hierna: AVG) [↑](#footnote-ref-127)
128. Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, *Pb.L.* 4 mei 2016, afl. 119. (Hierna: Richtlijn Politie en Justitie) [↑](#footnote-ref-128)
129. Richtlĳn (EG) 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlĳke levenssfeer in de sector elektronische communicatie (richtlĳn betreffende privacy en elektronische communicatie), *Pb.L* 31 juli 2002, afl. L 201. Zou in de toekomst vervangen worden door de e-Privacyverordening. Een voorstel voor zulke verordening werd in 2017 gedaan, maar de onderhandelingen lopen nog. [https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacyand-electronic-communications](https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications) (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-129)
130. Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlĳke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrĳe verkeer van die gegevens, *Pb. L.* 12 januari 2001, afl. 8. [↑](#footnote-ref-130)
131. Overweging 1 AVG; Overweging 1 Richtlijn Politie en Justitie; art. 2 AVG, art. 2 Richtlijn Politie en Justitie. [↑](#footnote-ref-131)
132. Art. 1, lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-132)
133. Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018 (hierna: Wet Bescherming Persoonsgegevens in tekst, WBP in voetnoten). [↑](#footnote-ref-133)
134. Gemoderniseerd Verdrag 108, art. 8 Handvest. [↑](#footnote-ref-134)
135. Ibid 121, Volker und Markus, §47; ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27 februari 2014, 3. (Hierna: WP29) [↑](#footnote-ref-135)
136. Opinie Advocaat-Generaal Sharpston bij HvJ, 17 juni 2010, nr.C-92/02, C-93/02, *Volker und Markus Schecke GbR en Eifert/Land Hessen*, ECLI:EU:C:2010:662, §71. [↑](#footnote-ref-136)
137. Zie Deel VII, 2 voor een bespreking van de wezenlijke inhoud van beide rechten. [↑](#footnote-ref-137)
138. Zie bijvoorbeeld: HvJ, 21 december 2016, C‑203/15, C‑698/15, *Tele2Sverige/Post-och telestyrelsen,* Secretary of State for the Home Department/Tom Watson, ECLI:EU:C:2016:970, §101; Ibid 113, FRA, *Handbook*, 19. Voor een uiteenzetting van mensenrechten waarvoor art. 7, 8 HEU grondvoorwaarde biedt: deel XI. [↑](#footnote-ref-138)
139. WP29, “Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector”, 27 februari 2014,4, §2.1; EDPS, “Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit”, *EDPS* 2017, 6-9; <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf>. (geraadpleegd op: 16 mei 2021)**.** [↑](#footnote-ref-139)
140. Ibid 113, FRA, *Handbook*, 52. [↑](#footnote-ref-140)
141. Art. 8 Toelichtingen van 14 december 2007 bij het Handvest van de Grondrechten, *Pb.L* 14 december 2007, afl. C 303/02. [↑](#footnote-ref-141)
142. Toen nog: RvE, Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, inmiddels aangevuld met het Aanvullend Protocol aangenomen dat het Verdrag en gewijzigd naar Gemoderniseerd Verdrag 108 (ibid 118). [↑](#footnote-ref-142)
143. HvJ, 17 oktober 2013, nr. C-291/12, *Schwarz/Stadt Bochum*, ECLI:EU:C:2013:670, §25; Ibid 123, *Digital Rights*, §47. Deze verwevenheid blijkt o.a. ook uit HvJ, 13 mei 2014, nr. C-131/12, *Google Inc/AEPD,* ECLI:EU:2014:317, §§3, 58,66, 68, 81, 97, 99. Ook in Schrems is een duidelijke link te zien tussen beide rechten: HvJ Schrems, 6 oktober 2015, C-362/14, *Schrems/Data Protection Commissioner,* ECLI: EU: C:2015:650, §§38, 39. Voor een overzicht van rechtspraak mbt art. 7 Handvest, zie: DIRECTIE ONDERZOEK EN DOCUMENTATIE, “Themafiche Bescherming van persoonsgegevens”, *HVJ,* 2020; <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_nl.pdf>. (geraadpleegd op: 16 mei 2021); Zie ook: Ibid 135, WP29, *Opinion 01/2014*, 4. [↑](#footnote-ref-143)
144. Ibid 113, FRA, *Handbook*, 25. [↑](#footnote-ref-144)
145. *“Kunnen, gelet op artikel 52, lid 3, van het Handvest, de vijfde alinea van de preambule en de toelichting op artikel 7 van het Handvest, volgens welke de in artikel 7 gewaarborgde rechten corresponderen met de rechten die in artikel 8 EVRM zijn gewaarborgd, aan de rechtspraak van het Europees Hof voor de Rechten van de Mens inzake artikel 8 EVRM criteria worden ontleend voor de uitlegging van artikel 8 van het Handvest, die de uitlegging van laatstgenoemd artikel beïnvloeden?” ;* in Ibid 123, Digital Rights, §21,2,e). [↑](#footnote-ref-145)
146. Ibid 123, §§69, 71. [↑](#footnote-ref-146)
147. Ibid 123, §72. [↑](#footnote-ref-147)
148. Ibid 123, §38. [↑](#footnote-ref-148)
149. Ibid 123, §39. Het toetst om precies te zijn “de wezenlijke inhoud van het fundamentele recht op eerbiediging van het privéleven en de andere door artikel 7 van het Handvest erkende rechten.” Hiermee verduidelijkt ze geenszins wat het onderscheid precies is tussen het recht op privéleven en die andere rechten in art. 7 Handvest. Zie ook Deel V, 2. [↑](#footnote-ref-149)
150. Ibid 123, §40. [↑](#footnote-ref-150)
151. Ibid 123, §§41-44. [↑](#footnote-ref-151)
152. Ibid 123, §45 e.v. [↑](#footnote-ref-152)
153. Ibid 123, §46. [↑](#footnote-ref-153)
154. Ibid 123, 6§47,54, 55. [↑](#footnote-ref-154)
155. EDPS, “Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data”, *EDPS* 2019, 10; <https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf>; (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-155)
156. Ibid 155. [↑](#footnote-ref-156)
157. Ibid 139, EDPS, “Necessity Toolkit”. [↑](#footnote-ref-157)
158. Zo heeft de Europese Commissie een tool: EC, “Tool #28. Fundamental Rights & Human Rights”; <https://ec.europa.eu/info/files/better-regulation-toolbox-28_en>, (datum niet vermeld), de Raad van Europa: RVE, “Fundamental Rights Compatibility- Guidelines for Council preparatory bodies”, *Publications Office European Union,* 2015; <https://www.consilium.europa.eu/media/30209/qc0214079enn.pdf> en de FRA: FRA, “Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level-Guidance”, *FRA,* 2018; <http://fra.europa.eu/en/publication/2018/national-guidance-application-eu-charter> (geraadpleegd op: 16 mei 2021). [↑](#footnote-ref-158)
159. Ibid 155, EDPS, “Guidelines on assessing proportionality”, 4. [↑](#footnote-ref-159)
160. Ibid 155, EDPS, “Guidelines on assessing proportionality”, 12- 13. [↑](#footnote-ref-160)
161. Gezien er op dit moment nog geen duidelijkheid bestaat over een concrete rechtsgrond en maatregelen met LFR, worden de concrete stappen van de toets niet gevolgd in deze volgorde. De garanties uit de toets waarmee rekening moet worden gehouden, worden echter zoveel mogelijk verwerkt in Deel X rond de invloed van LFR op privacy. [↑](#footnote-ref-161)
162. Zie supra Deel III, 1. [↑](#footnote-ref-162)
163. Vanaf hier gebruik ik het woord “privacy” om te verwijzen naar de wezenlijke inhoud van het recht op eerbiediging privéleven (d.i. het recht op eerbiediging van privé-, familie- en gezinsleven) en het recht op de bescherming van persoonsgegevens. [↑](#footnote-ref-163)
164. Ibid 113, FRA, *Handbook*, 18. [↑](#footnote-ref-164)
165. Bundesverfassungsgericht, 15 december 1983, nr. BvR 209/83, Volkszählungsurteil; <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html>; K. ADENAUER-STIFTUNG, “English translation of essential parts of the German ““Volkszählungsurteil” from 15 December 1983, which established in Germany the Basic Right on Informational Self-Determination.”, <https://freiheitsfoo.de/files/2013/10/Census-Act.pdf>; (geraadpleegd op 16 mei 2021); Ibid 113, FRA, *Handbook*, 18. [↑](#footnote-ref-165)
166. De bescherming van de menselijke waardigheid wordt ook voorzien in art. 1 HEU; A. ROUVROY, Y. POULLET, “Chapter 2: the Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy”, in G. GUTWIRTH, Y. POULLET, P. DE HERT e.a. (eds.), *Reinventing Data Protection?,* Springer, 2009, 45. [↑](#footnote-ref-166)
167. EDRi, “Ban Biometric Mass Surveillance- A Set of fundamental rights demands for the European Commission and EU Member States”, *EDRi,* 2020, 22. [↑](#footnote-ref-167)
168. Ibid 166, ROUVROY e.a., 45-47. [↑](#footnote-ref-168)
169. Ibid 165. [↑](#footnote-ref-169)
170. LIGA VOOR MENSENREHTEN, “Mensenrechten-Een kennismaking”, *Liga voor Mensenrechten,* 2009, 9, 38; FRA, Handbook DPRights, 19. Dit blijkt ook uit Hoofdstuk III AVG en Hoofdstuk III Richtlijn Politie en Justitie waarin rechten worden opgesomd die het individu kan uitoefenen. [↑](#footnote-ref-170)
171. Ibid 166, ROUVROY e.a., 46. [↑](#footnote-ref-171)
172. Ibid 165. [↑](#footnote-ref-172)
173. Zie deel X, 3, c). [↑](#footnote-ref-173)
174. Ibid 123, *Digital Rights*, §38-41. Zie ook: Ibid 143, *Schrems/Data Protection Commissioner*, §94 e.v. [↑](#footnote-ref-174)
175. M. BRKAN, “The essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning”, *German Law Journal, Special issue 6: Interrogating the Essence of EU Fundamental Rights,* 2019, Titel B) II. [↑](#footnote-ref-175)
176. Ibid 123, *Digital Rights*, §39. [↑](#footnote-ref-176)
177. Ibid 123, *Digital Rights*, §26 geeft een opsomming van de metadata die werden verplicht dienden worden bijgehouden door de Dataretentierichtlijn. [↑](#footnote-ref-177)
178. CONCLUSIE VAN ADVOCAAT-GENERAAL H. SAUGMANDSGAARD ØE van 19 juli 2016 in HvJ, 21 december 2016, C‑203/15, C‑698/15, *Tele2Sverige/Post-och telestyrelsen,* Secretary of State for the Home Department/Tom Watson, ECLI:EU:C:2016:970, §257-259. [↑](#footnote-ref-178)
179. Ibid 178, Conclusie Saugmandsgaard, §256, 259. [↑](#footnote-ref-179)
180. Big data, zie infra deel X, 1, c): dataminimalisatie. [↑](#footnote-ref-180)
181. Ibid 178, Conclusie Saugmandsgaard, §256, 259. [↑](#footnote-ref-181)
182. Ibid 123, *Digital Rights*, §40. [↑](#footnote-ref-182)
183. M.-P. GRANGER, K. IRION, “The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection”, *European Law Review,* 2014, 30. [↑](#footnote-ref-183)
184. Ibid 181. [↑](#footnote-ref-184)
185. Ibid 175, BRKAN, Titel D) I; Zie ook deel IX, 4) van deze masterproef. [↑](#footnote-ref-185)
186. Zie deel VIII voor de rechtsinstrumenten die het recht op eerbiediging privéleven /recht op bescherming persoonsgegevens uitwerken en de basisbeginselen voorzien. Zie deel IX, 4 voor de basisbeginselen, deel XI voor verweven rechten. [↑](#footnote-ref-186)
187. Zie bijvoorbeeld: L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT, *Group Privacynew challenges of Data Technologies,* Springer International Publishing, 2017; B. MITTELSTADT, “From individual to group privacy in Big Data Analytics”, *Philosophy & Technology,* 2017; L. KAMMOURIEH, T. BAAR, J. BERENS, e.a., “Group Privacy in the Age of Big Data”, *Philosophical Studies Series,* 2016. [↑](#footnote-ref-187)
188. H. NISSENBAUM, “Privacy as Contextual Integrity”, *Washington Law Review* 2004. [↑](#footnote-ref-188)
189. Art. 2, lid 1 AVG. [↑](#footnote-ref-189)
190. Art. 3 AVG. [↑](#footnote-ref-190)
191. Ibid 191. [↑](#footnote-ref-191)
192. #  EDPB, “EDPB response to MEPs Sophie in ‘t Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI.”, 2020, 3.

 [↑](#footnote-ref-192)
193. Zie o.a. Deel VI, fase 3 doelbeperking, Deel VI, fase 2: fase van de aankoop, samengelezen met Deel VI, 3, verantwoordelijkheidsbeginsel. [↑](#footnote-ref-193)
194. Art. 1, lid 1; art. 2 lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-194)
195. Art. 26, 7°, a) WBP. [↑](#footnote-ref-195)
196. Art. 2, 2° Wet Geïntegreerde Politie. [↑](#footnote-ref-196)
197. Art. 26, 7°, b) WBP. [↑](#footnote-ref-197)
198. Art. 25 juncto art. 26, 7°, b) WBP. [↑](#footnote-ref-198)
199. Dat min of meer de uitwerking vormt van de voorwaarden van de AVG. [↑](#footnote-ref-199)
200. Dat min of meer de uitwerking vormt van de Richtlijn Politie en Justitie. Zie voor de verschillende mate van bescherming van deze beginselen en rechten deel IX, lid 4, deel X, 1, c), deel X, 3, c. [↑](#footnote-ref-200)
201. Zie deel VI, fase 2: fase van de aankoop, samengelezen met Deel VI, 3, verantwoordelijkheidsbeginsel. [↑](#footnote-ref-201)
202. Titel II WBP. [↑](#footnote-ref-202)
203. Titel I WBP. [↑](#footnote-ref-203)
204. Art. 2 AVG, overweging 16 AVG, art. 2 Richtlijn Politie en Justitie. [↑](#footnote-ref-204)
205. Titel 3, Ondertitel 1: art. 72- art. 104 WBP. België is deel van een hele reeks lidstaten die dit deden: J. SAJFERT, T. QUINTEL, “Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities”, *Edward Elgar Publishing,* 2019, 4. [↑](#footnote-ref-205)
206. Ibid 205, SAJFERT en QUINTEL, 4. [↑](#footnote-ref-206)
207. Art. 3, 7°, a) Richtlijn Politie en Justitie. [↑](#footnote-ref-207)
208. Dit wil zeggen dat gemengde rechtshandhavingsautoriteitendie zowel inlichtingen-als politionele bevoegdheden uitvoeren, voor hun politionele bevoegdheden onder de Richtlijn Politie en Justitie vallen. (overweging 11 en art. 3, 7°, b) Richtlijn Politie en Justitie.) [↑](#footnote-ref-208)
209. Art. 26, 7° WBP. [↑](#footnote-ref-209)
210. Wet van 5 augustus 1992 op het Politieambt, *BS,* 22 december 1992. (hierna: Wet op het Politieambt in tekst, WPA in voetnoten). [↑](#footnote-ref-210)
211. Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera’s, *BS,* 31 mei 2007. (hierna: Camerawet) [↑](#footnote-ref-211)
212. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 658. [↑](#footnote-ref-212)
213. Art. 25/2, 4° WPA [↑](#footnote-ref-213)
214. Art. 25/5, 5° WPA [↑](#footnote-ref-214)
215. Art. 25/5, 6° WPA. Dit onderscheid heeft o.a. te maken met de mate waarin toestemming kan worden gegeven door de betrokkene die wordt gefilmd: CDEI, “Snapshot Series: Facial Recognition Technology”, *CDEI,* 2020, 22. [↑](#footnote-ref-215)
216. Zie EC, “Annexes accompanying the Proposal for a Regulation of the European Parliament and of the Council”, nr. SWD (2021) 84 final, 41, 2021. [↑](#footnote-ref-216)
217. UNESCO, “Inclusion through Acces to Public Spaces”, *UNESCO*, 2019; <http://www.unesco.org/new/en/social-and-human-sciences/themes/urban-development/migrants-inclusion-in-cities/good-practices/inclusion-through-access-to-public-space/>. [↑](#footnote-ref-217)
218. Ibid 167, EDRi, “Ban Biometric Mass Surveillance”, 9. [↑](#footnote-ref-218)
219. Bovendien zijn operationele ambtenaren steeds herkenbaar aan een waarschuwing, herkenbaar voertuig van de politie… (art. 25/2, §2, lid 1 WPA) Voor LFR is dit relevant voor het operationele interventieteam dat live matches opvolgt. [↑](#footnote-ref-219)
220. [https://www.controleorgaan.be/nl/politiediensten/camerawetgeving#](https://www.controleorgaan.be/nl/politiediensten/camerawetgeving); (geraadpleegd op 16 mei 2021); Belangrijk hierbij is dat de regeling rond het niet-zichtbaar gebruik van ANPR- camera’s o.a gebeurt door (geheime) circulaire omzendbrieven. Zo bijvoorbeeld de geheime circulaire Omzendbrief n° 3/2019 inzake BOM-bijzondere opsporingsmethoden-ANPR-camera’s, 26 juni 2019. [↑](#footnote-ref-220)
221. art. 46/4-art. 46/6 WPA. [↑](#footnote-ref-221)
222. art. 46/7-art. 46/8 WPA. Zie ook art. 46/9-art. 46/10 Wet op het Politieambt en art. 46/11 Wet op het Politieambt. [↑](#footnote-ref-222)
223. Zie: [https://www.controleorgaan.be/nl/politiediensten/camerawetgeving#](https://www.controleorgaan.be/nl/politiediensten/camerawetgeving) (geraadpleegd op 16 mei 2021) en Ibid 92, COC, “Aanbeveling nr. 06/2011”, 12/13. [↑](#footnote-ref-223)
224. art. 2 lid 1 AVG, art. 1, lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-224)
225. art. 4, lid 2 AVG; art. 3, 2) Richtlijn Politie en Justitie; art. 2 Gemoderniseerd Verdrag 108. [↑](#footnote-ref-225)
226. Ibid 113, FRA, *Handbook,* 99. [↑](#footnote-ref-226)
227. Zie deel X, 1. [↑](#footnote-ref-227)
228. Zie deel X, 1. [↑](#footnote-ref-228)
229. art. 4, lid 1 AVG, art. 3, lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-229)
230. art. 3, lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-230)
231. HvJ 6 november 2003, nr. C-101/0, ECLI: EU:2003:596, Lindqvist, 27. [↑](#footnote-ref-231)
232. Overweging 21 Richtlijn Politie en Justitie. [↑](#footnote-ref-232)
233. Deel VII, 2. [↑](#footnote-ref-233)
234. art. 9 Richtlijn Politie en Justitie. [↑](#footnote-ref-234)
235. art. 9 AVG, art. 10 Richtlijn Politie en Justitie, art. 6 Gemoderniseerd Verdrag 108. [↑](#footnote-ref-235)
236. Vraagstelling van Peter van Schelven. [↑](#footnote-ref-236)
237. art. 3, 13° Richtlijn Politie en Justitie, art. 4, 14 AVG. [↑](#footnote-ref-237)
238. Voor de verwerking van gevoelige gegevens moet een van de rechtmatigheidsgronden uit art. 6 AVG worden gecombineerd met die uit art. 9 AVG, dat voorziet in “strengere” rechtmatigheidsgronden voor biometrische en andere gevoelige persoonsgegevens. Zie ook deel X, 1, c, beginsel van rechtmatigheid. [↑](#footnote-ref-238)
239. Zie deel X, 1, c, rechtmatigheid. [↑](#footnote-ref-239)
240. art. 10 Richtlijn Politie en Justitie. [↑](#footnote-ref-240)
241. Zie infra deel X, 3, c, rechtmatigheid. De keuze van een rechtmatigheidsgrond zal het voorwerp moeten uitmaken van een concrete proportionaliteitsbeoordeling: Ibid 155, EDPS, “Guidelines on assessing proportionality”, 11. [↑](#footnote-ref-241)
242. art. 4 lid 7 AVG. [↑](#footnote-ref-242)
243. Zie deel X, 3, c, doelbinding. [↑](#footnote-ref-243)
244. Zie Deel X, 1, c, doelbinding. [↑](#footnote-ref-244)
245. RvE, COMMISSARIS VOOR MENSENRECHTEN, “Unboxing Artificial Intelligence: 10 steps to protect Human Rights”, 2019, 6. [↑](#footnote-ref-245)
246. Zelfstandig Juridisch Adviseur in Nederland, met uitgebreide ervaring binnen het gegevensbeschermingsrecht. [↑](#footnote-ref-246)
247. Deze definitie is nagenoeg hetzelfde in art. 3, lid 8 Richtlijn Politie en Justitie; art. 4, lid 7 AVG; art. 26, lid 8 WBP. [↑](#footnote-ref-247)
248. Zie deel X, 3, a: welke persoonsgegevens worden verwerkt. [↑](#footnote-ref-248)
249. Dit is bijvoorbeeld zo voor de bewaring van camerabeelden: COC, “Advies nr. DD200026 van 11 februari 2021 uit eigen beweging mbt de vraag wie de verwerkingsverantwoordelijke is voor gegevensverwerkingen door de politiediensten in het kader van de uitvoering van politionele opdrachten enerzijds en voor gegevensverwerkingen onder de AVG anderzijds”, *Advies COC*, 2021, 3. [↑](#footnote-ref-249)
250. Ibid 249, COC, Advies DD200026 2021, 6. [↑](#footnote-ref-250)
251. Ibid 250. [↑](#footnote-ref-251)
252. Zie infra:Deel X, 3, b, databanken. [↑](#footnote-ref-252)
253. Ibid 249, Advies DD200026, 11. [↑](#footnote-ref-253)
254. art. 5 §2 Camerawet. Nick Noël is Directeur Operaties bij PZ Rupel. [↑](#footnote-ref-254)
255. A. VANRENTERGHEM, “U wordt gefilmd: nieuwe camerawet maakt onder meer bodycams, drones en een slim cameraschild mogelijk”, *Vrt Nws,* 13 maart 2018. [↑](#footnote-ref-255)
256. art. 38 e.v. Wet op de Geïntegreerde Politie. [↑](#footnote-ref-256)
257. Zie voor een overzicht van de mogelijke regelingen rond ANPR-camera’s de presentatie van A. DORMAELS (VIAS INSTITUTE), “Presentatie ‘Belangrijkste bevindingen uit omgevingsanalyse en knelpuntennota’”, gepresenteerd op 19 november 2020 tijdens de ‘Webinar ANPR-camera’s: slimmer dan gedacht’. *Nele Krols zegt hierover : Maar de eerste discussie die zich dan al begint te stellen en waar precies niemand een antwoord op kan geven is: “Wie is de verwerkingsverantwoordelijke van die ANPR-camera?” Is dat de federale politie als we gebruik maken van de camera voordat we die beelden richting nationale server sturen? Of zijn dat de lokale besturen? En dan komen er van die deelvragen: “Wie betaalt die camera?” Dat doet eigenlijk niet ter zake, want wij gebruiken die beelden voor onze lokale politionele doeleinden. Dan is eigenlijk de politie toch de verwerkingsverantwoordelijke.”* [↑](#footnote-ref-257)
258. art. 26 AVG. [↑](#footnote-ref-258)
259. H.-J. HSU, K.-T. CHEN, “Face Recognition on drones”, *Conference: the first workshop,* 2015; T. BREWSTER, “Drones With Facial Recognition Are Primed to Fly-But The World Isn’t Ready Yet”, *Forbes,* 2021. [↑](#footnote-ref-259)
260. art. 3, lid 9) Richtlijn Politie en Justitie. [↑](#footnote-ref-260)
261. De vraag naar de juiste kwalificatie van ontwikkelaars als verwerker of verwerkingsverantwoordelijke speelt in de ontwikkelingsfase uiteraard enkel wanneer deze daarbij persoonsgegevens verwerkt. Dit is bij LFR het geval: de software moet worden getraind a.d.h.v. afbeeldingen van gezichten. Zie deel X, 1). [↑](#footnote-ref-261)
262. art. 22 Richtlijn Politie en Justitie. [↑](#footnote-ref-262)
263. art. 23 Richtlijn Politie en Justitie. [↑](#footnote-ref-263)
264. art. 22, lid 3 Richtlijn Politie en Justitie. [↑](#footnote-ref-264)
265. art. 22 lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-265)
266. Hoofdstuk IV AVG. [↑](#footnote-ref-266)
267. Hoofdstuk IV Richtlijn Politie en Justitie. [↑](#footnote-ref-267)
268. Zo is bijvoorbeeld de vereiste van transparantie in de Richtlijn Politie en Justitie niet even belangrijk als transparantie in de AVG. Zie: T. RADTKE, “The concept of joint control under the data protection law enforcement directive 2016/680 in contrast to the gdpr.”, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* 2020, 245. Bovendien worden ook de rechten van betrokkenen niet op dezelfde manier gegarandeerd. Vergelijk Hoofdstuk III AVG, Hoofdstuk III Richtlijn Politie en Justitie. [↑](#footnote-ref-268)
269. art. 9 lid 4 Camerawet, art. 25/4 WPA. Dit geldt ook voor camera’s op plaatsen met een bijzonder veiligheidsrisico: het gaat over publiek toegankelijk plaatsen met een bijzonder veiligheidsrisico, zoals bijvoorbeeld treinstations. Om toegang in real time te krijgen tot deze beelden van deze plaats dient een overeenkomst te worden gesloten met de beheerder van de plaats die werd afgesloten. (art. 2 KB van 6 december 2018 tot vaststelling van de plaatsen waar de verwerkingsverantwoordelijke zijn bewakingscamera’s kan richten op de perimeter rechtstreeks rond de plaats, de beelden van de bewakingscamera’s gedurende drie maanden kan bewaren en toegang in real time tot de beelden kan geven aan de politiediensten, *BS 18 december 2018.)* [↑](#footnote-ref-269)
270. art. 5 §2, art. 6 §2, art. 7 §2 Camerawet. [↑](#footnote-ref-270)
271. art. 9 lid 4 Camerawet. [↑](#footnote-ref-271)
272. Plaatsbezoek PZ Rupel. Met “wettelijk geplaatst” wordt bedoeld dat alle voorwaarden en de procedure van de verwerkersovereenkomst werden nageleefd. [↑](#footnote-ref-272)
273. art. 9, lid 4 Camerawet. [↑](#footnote-ref-273)
274. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 667. [↑](#footnote-ref-274)
275. S. NAAFS, “Gezichtsherkenning rukt op: kunnen we weldra niet meer anoniem over straat?”, *Knack,* 21 augustus 2019; <https://www.knack.be/nieuws/belgie/gezichtsherkenning-rukt-op-kunnen-we-weldra-niet-meer-anoniem-over-straat/article-longread-1499451.html>. (geraadpleegd op 16 mei 2021) Voor een uitgebreide uiteenzetting van de mogelijkheden en het gebruik van LFR door particulieren, (door de private sector), zie: UNIVERSITEIT VAN TILBURG, “Op het eerste gezicht: een verkenning van gezichtsherkenning en privacyrisico’s in horizontale relaties”, *WODC,* 2020. [↑](#footnote-ref-275)
276. art. 22 Richtlijn Politie en Justitie. [↑](#footnote-ref-276)
277. art. 25/5 WPA. [↑](#footnote-ref-277)
278. art. 41 Richtlijn Politie en Justitie; art. 51 AVG. [↑](#footnote-ref-278)
279. art. 27 Richtlijn Politie en Justitie, art. 71 §1, 1° WBP, art. 44/1 tot en met art. 44/11/13 WPA, art. 4 § 2 Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS 10 januari 2018.* (hierna: Wet oprichting GBA) [↑](#footnote-ref-279)
280. art. 71 WBP. [↑](#footnote-ref-280)
281. art. 71, §1, 2°; F. SCHUERMANS, “Een vernieuwde speler in het politielandschap”, *Blue Trends,* 2019, 2. [↑](#footnote-ref-281)
282. art. 71 WBP. [↑](#footnote-ref-282)
283. art. 71 WBP; <https://www.controleorgaan.be/nl/controleorgaan/nationale-activiteiten>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-283)
284. art. 71 WBP. [↑](#footnote-ref-284)
285. art. 2, lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-285)
286. Ibid 6, COC, “Tussentijds rapport over LFR op Zaventem”, 2. [↑](#footnote-ref-286)
287. art. 4 §1 Wet oprichting GBA. [↑](#footnote-ref-287)
288. KENNISCENTRUM DATA EN MAATSCHAPPIJ, “Rapport over bevoegdheden in het delen van gegevens-automatische kentekenplaatherkenning (ANPR) als toepassingsgeval”, *Kenniscentrum Data en Maatschappij,* 2021, 25 ; <https://data-en-maatschappij.ai/uploads/publications/20210201_Rapport-Bevoegdheden_ANPR.pdf>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-288)
289. Ibid 288, KENNISCENTRUM DATA EN MAATSCHAPPIJ, Rapport ANPR, 25. [↑](#footnote-ref-289)
290. Dit blijkt uit deel VIII, 2, d, verwerkingsverantwoordelijke, in de ontwikkelingsfase; deel VIII, 2, d, verwerker, in de ontwikkelingsfase; deel VIII, 3, b, bevoegdheden GBA; deel X, 1, c, doelbinding; deel X, 2, c, privacy by design. [↑](#footnote-ref-290)
291. Zie infra deel X, 2, c, wie is VWV voor privacy by design-verplichting? [↑](#footnote-ref-291)
292. Aan welke wetgeving dient een software-ontwikkelaar te voldoen: de basisbeginselen uit de AVG of Richtlijn Politie en Justitie? Dit onderscheid loopt verder in de WBP, die in Titel II de gegevensbescherming bij verwerkingen voor politionele doeleinden regelt; Ibid 290. [↑](#footnote-ref-292)
293. art. 95 WBP; <https://www.comiteri.be/index.php/nl/vast-comite-i>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-293)
294. Ibid 293, comité i. [↑](#footnote-ref-294)
295. Ibid 294. [↑](#footnote-ref-295)
296. <https://www.comiteri.be/index.php/nl/vast-comite-i/acht-taken-mainmenu-61>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-296)
297. art. 15, 16 van de wet van 10 juli 2006 betreffende de analyse van de dreiging, *BS,* 20 juli 2006; <https://comitep.be/wie-controleren-wij.html>. [↑](#footnote-ref-297)
298. Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, *BS,* 29 oktober 2008. [↑](#footnote-ref-298)
299. <https://cirb.brussels/fr/nos-solutions/infrastructure-solutions/portlet-fidus/commission-de-controle-bruxelloise>; (geraadpleegd op 16 mei 2021); Deze autoriteit bestaat echter voornamelijk op papier. Presentatie Willem Debeuckelaere, “Gegevensbescherming in België na de GDPR/AVG**”,** 3 maart 2020, binnen het vak “Gegevensbeschermingsrecht” UGent. [↑](#footnote-ref-299)
300. #  Opgericht door Decreet houdende de aanpassing van de decreten aan de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming.), *BS,* 26 juni 2018; [Ibid 288, KENNISCENTRUM DATA EN MAATSCHAPPIJ, 25](https://ugentbe-my.sharepoint.com/personal/lledgrae_degraeve_ugent_be/Documents/Werkversies%20thesis/Ibid%20288%2C%20KENNISCENTRUM%20DATA%20EN%20MAATSCHAPPIJ%2C%2025); <https://overheid.vlaanderen.be/vlaamse-toezichtcommissie>.; (geraadpleegd op 16 mei 2021).

 [↑](#footnote-ref-300)
301. L. EDWARDS, M. VEALE, “Slave to the algorithm? Why a “right to an explanation” is probably not the remedy you are looking for”, [16 Duke Law & Technology Review 18, 2017](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855), 75. [↑](#footnote-ref-301)
302. <https://www.controleorgaan.be/nl/controleorgaan/samenstelling-van-de-organisatie>; (geraadpleegd op 16 mei 2021); Ibid 281, SCHUERMANS, 2. [↑](#footnote-ref-302)
303. art. 231 WBP; Ibid 302, SCHUERMANS. [↑](#footnote-ref-303)
304. Lid-Raadsheer bij het COC. [↑](#footnote-ref-304)
305. Dit voorstel werd ingediend door Gilles Vanden Burre (Écolo), Jessika Soors (Groen), Francçois De Smet (Défi). Voorstel van Resolutie DOC 55/1349/001 van 16 juni 2020 over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en- algoritmen in vaste of mobiele beveiligingscamera’s in openbare en privéplaatsen, 3. [↑](#footnote-ref-305)
306. Ibid 9, Wetsontwerp, 125; overzicht van vermeldingen naar “facial recognition” binnen de Kamer: <https://www.dekamer.be/kvvcr/showpage.cfm?section=none&language=nl&cfm=/site/wwwcfm/search/search_new.cfm?db=searchpdf>. [↑](#footnote-ref-306)
307. Policy and Campaigns Officer bij European Digital Rights (EDRi). [↑](#footnote-ref-307)
308. Beleidsadviseur van de Commissaris-Generaal bij de federale politie. [↑](#footnote-ref-308)
309. EU, Verdrag betreffende de werking van de Europese Unie (geconsolideerde versie), C 326/49, *Publicatieblad van de Europese Unie,* 26 oktober 2012 (hierna: VWEU). [↑](#footnote-ref-309)
310. art. 114 VWEU. [↑](#footnote-ref-310)
311. Ibid 12, EC, Proposal for Artificial Intelligence Act, 6. [↑](#footnote-ref-311)
312. Deze problemen worden beschreven in Deel VI, 1) van deze masterproef. De vraag is nog maar in welke mate dit prille voorstel van verordening erin slaagt om deze problemen te remediëren. Peter van Schelven betreurt dat een algemene regeling van AI wordt vooropgesteld en geen sectorspecifieke aanpak van AI. Hij vraagt zich af of er niet moet nagedacht worden over bijvoorbeeld sectorspecifieke regelgeving voor AI bij de politie. [↑](#footnote-ref-312)
313. art. 16 lid 2 VWEU. [↑](#footnote-ref-313)
314. Ibid 12, EC, Proposal for Artificial Intelligence Act, 12. [↑](#footnote-ref-314)
315. Ibid 216, Annexes accompanying proposal for Artificial Intelligence Act, 41. [↑](#footnote-ref-315)
316. Ibid 12, EC, Proposal for Artificial Intelligence Act, 26. [↑](#footnote-ref-316)
317. Ibid 12, EC, Proposal for Artificial Intelligence Act, 13. [↑](#footnote-ref-317)
318. art. 52(1) HEU. [↑](#footnote-ref-318)
319. Zie deel VII, 1, d); Art. 52(3) HEU; Ibid 155, EDPS, “Guidelines on assessing proportionality”, 7. [↑](#footnote-ref-319)
320. Ibid 31, FRA, Rapport over Facial recognition technology, 3; <https://www.europarl.europa.eu/doceo/document/E-8-2018-005624_EN.html>. [↑](#footnote-ref-320)
321. EHRM, 4 februari 2019, nrs. 58170/13, 62322/14, 24960/15, Big Brother Watch e.a./Verenigd Koninkrijk, §306. [↑](#footnote-ref-321)
322. Zie deel IX, 4. [↑](#footnote-ref-322)
323. High Court of Justice, 04/09/2019, nr. CO/4085/2018, *The Queen Bridges/Chief Constable of South Wales Police and others.* [↑](#footnote-ref-323)
324. Ibid 323, *The Queen Bridges/Chief Constable* § 85-97. [↑](#footnote-ref-324)
325. Zie voor een overzicht van de testen in het Verenigd Koninkrijk: Ibid 87, DAVIES. [↑](#footnote-ref-325)
326. Ibid, High Court of Justice, *The* *Queen Bridges/Chief Constable,* §134. [↑](#footnote-ref-326)
327. Royal Court of Justice, Court of appeal (civil division), 11 augustus 2020, nr. C1/2019/2670, R/The Chief Constable of South Wales Police, §53. De wetgeving antwoordde volgens de Court of Appeals niet op de vragen wie op een watchlist wordt geplaatst (“who question”) en waar de technologie kan worden ingezet (“where question”). Zonder zulke regelgeving konden politieagenten dit immers discretionair zelf beoordelen. (§91) [↑](#footnote-ref-327)
328. Ibid 6, COC, “Tussentijds rapport over LFR op Zaventem”, 4; Interview met Frank Schuermans, Lid-Raadsheer bij het COC. [↑](#footnote-ref-328)
329. Bovendien moet de politie in dat geval ook de noodzakelijke en gepaste risico-en impactanalyse op het vlak van bescherming van persoonlijke levenssfeer en bescherming van persoonsgegevens voorleggen aan het COC, gekoppeld aan een adequaat en concreet veiligheidsplan. (Ibid 6, COC, Tussentijds rapport LFR op Zaventem, 5). [↑](#footnote-ref-329)
330. Ibid 6, COC, “Tussentijds rapport over LFR op Zaventem”, 5. [↑](#footnote-ref-330)
331. art. 25/3 WPA, art. 46/4 WPA. [↑](#footnote-ref-331)
332. art. 8/1 Camerawet. [↑](#footnote-ref-332)
333. art. 25/2 WPA. [↑](#footnote-ref-333)
334. art. 44/2 §3 WPA. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 665. [↑](#footnote-ref-334)
335. Parl. St. DOC 54, n° 2855/003 van 2 maart 2018, 74. [↑](#footnote-ref-335)
336. Ibid 335. [↑](#footnote-ref-336)
337. art. 44/1, art.44/5, §3, 7°-9° WPA. [↑](#footnote-ref-337)
338. art.44/5, §3, 7°-9° WPA. [↑](#footnote-ref-338)
339. <https://www.briefcam.com/who-we-serve/law-enforcement/>*.* [↑](#footnote-ref-339)
340. Interview Kurt Verstockt (DPO bij PZ Donder-Schelde), Ruben Van Sevenant (Diensthoofd ICT bij PZ Gent). [↑](#footnote-ref-340)
341. Ibid 6, COC, “Tussentijds rapport over LFR op Zaventem”, 5. [↑](#footnote-ref-341)
342. Lid-Raadsheer bij het COC. [↑](#footnote-ref-342)
343. Interview met Frank Schuermans, Lid-Raadsheer bij het COC. [↑](#footnote-ref-343)
344. Ibid 31, FRA, Rapport over Facial recognition technology, 3. [↑](#footnote-ref-344)
345. Beleidsadviseur van de Commissaris Generaal bij de federale politie. [↑](#footnote-ref-345)
346. Voor een overzicht van het ethische kader rond proefprojecten met LFR: LONDON POLICING ETHICS PANEL, “Final Report on Live Facial Recognition”, in opdracht van de Mayor of London, 2019, 36-39. Voor een stappenplan om een proefproject op te stellen met privacygaranties: UK Surveillance Camera Commissioner, “Facing the Camera, Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist in Public Places in England & Wales”, 2020; <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf> , 70 en CNIL, facial recognition, for a debate living up to the challenges, p.9-10; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-346)
347. Beleidsadviseur van de Commissaris Generaal bij de federale politie. [↑](#footnote-ref-347)
348. Peter van Schelven geeft het voorbeeld van persoonsgegevens van een sollicitant die beschikbaar zijn op internet, die volgens de praktijk in Nederland niet zonder meer mogen worden verwerkt door de werkgever in de sollicitatie-fase. [↑](#footnote-ref-348)
349. Ibid 38, FUSSEY, MURRAY, “Independent Report”, 12. [↑](#footnote-ref-349)
350. L. DEARDEN, “Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested”, *Independent,* 31 januari 2019. [↑](#footnote-ref-350)
351. Ibid 349. [↑](#footnote-ref-351)
352. Ibid 31, FRA, *Handbook,* 122. [↑](#footnote-ref-352)
353. art. 5, lid 1, a) AVG, de rechtmatigheidsgronden staan in art. 6 AVG, (juncto art. 9 AVG voor de gevoelige persoonsgegevens); overweging 26 Richtlijn Politie en Justitie, art. 8 Richtlijn Politie en Justitie, art. 13 Richtlijn Politie en Justitie; art. 5, lid 4, b) Gemoderniseerd Verdrag 108. [↑](#footnote-ref-353)
354. Ibid 31, FRA, *Handbook,* 117. [↑](#footnote-ref-354)
355. art. 5, lid 1, b) AVG, art. 4, lid 1, b) Richtlijn Politie en Justitie. [↑](#footnote-ref-355)
356. Ibid 31, FRA, *Handbook*, 122. [↑](#footnote-ref-356)
357. art. 5, lid 1, c) AVG, art. 4, lid 1, c) Richtlijn Politie en Justitie. [↑](#footnote-ref-357)
358. Ibid 31, FRA, Handbook, 125. [↑](#footnote-ref-358)
359. art. 5, lid 1, d) AVG, art. 5, lid 4, d) Gemoderniseerd Verdrag 108, art. 4, lid 1, d) Richtlijn Politie en Justitie. [↑](#footnote-ref-359)
360. Ibid 31, FRA, *Handbook,* 127. [↑](#footnote-ref-360)
361. art. 5, lid 1, e) AVG, art.5, lid 4, e) Gemoderniseerd Verdrag 108, art. 4, lid 1, e) Richtlijn Politie en Justitie. [↑](#footnote-ref-361)
362. Ibid 31, FRA, *Handbook,* 129. [↑](#footnote-ref-362)
363. Hoofdstuk IV Richtlijn Politie en Justitie. [↑](#footnote-ref-363)
364. art. 5, lid 2 AVG, art. 10, lid 1 Gemoderniseerd Verdrag 108, art. 4 (4) Richtlijn Politie en Justitie. [↑](#footnote-ref-364)
365. art. 5, lid 1, f) AVG, art. 32, lid 1 AVG, art. 7 Gemoderniseerd Verdrag 108, art. 4, lid 1, f) Richtlijn Politie en Justitie. [↑](#footnote-ref-365)
366. Ibid 31, FRA, *Handbook,* 131. [↑](#footnote-ref-366)
367. Ibid 31, FRA, *Handbook,* 248. [↑](#footnote-ref-367)
368. Overweging 71, art. 22 AVG; Overweging 38, art. 3, lid 4, art. 11 Richtlijn Politie en Justitie. [↑](#footnote-ref-368)
369. art. 3, lid 4 Richtlijn Politie en Justitie. [↑](#footnote-ref-369)
370. art.11, lid 1 Richtlijn Politie en Justitie. [↑](#footnote-ref-370)
371. art. 11, lid 2 Richtlijn Politie en Justitie. [↑](#footnote-ref-371)
372. art. 11, lid 2 en 3 Richtlijn Politie en Justitie. [↑](#footnote-ref-372)
373. Zie deel X, 1, c, deel X, 3, c. [↑](#footnote-ref-373)
374. Zie Hoofdstuk III, AVG; Hoofdstuk III, Richtlijn Politie en Justitie. [↑](#footnote-ref-374)
375. Hoofdstuk III, art. 12-art. 21 AVG. [↑](#footnote-ref-375)
376. Hoofdstuk III, Richtlijn Politie en Justitie. [↑](#footnote-ref-376)
377. Hoofdstuk III: rechten van de betrokkene, art. 22 e.v. AVG. [↑](#footnote-ref-377)
378. art. 46, 47 Richtlijn Politie en Justitie; M. BRKAN, “Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond”, *International Journal of Law and Information Technology,* 2019, 99. [↑](#footnote-ref-378)
379. art. 13 lid 3, 15 lid 3, art. 15, 16 lid 4. [↑](#footnote-ref-379)
380. art.17 Richtlijn Politie en Jusitie. Art. 4, §2 Wet oprichting GBA. [↑](#footnote-ref-380)
381. Zie Deel VII, 2, wezenlijke inhoud. [↑](#footnote-ref-381)
382. Opmerking o.a. van Peter van Schelven. [↑](#footnote-ref-382)
383. <https://cs231n.github.io/convolutional-networks/#overview>. [↑](#footnote-ref-383)
384. Ibid 31, FRA, *Handbook,* 9. [↑](#footnote-ref-384)
385. Ibid 383. [↑](#footnote-ref-385)
386. [Ibid](https://cs231n.github.io/convolutional-networks/%22%20%5Cl%20%22overview) 383. [↑](#footnote-ref-386)
387. S. BREWSTER, “How Google’s new photos app can tell cats from dogs”, *Wired,* 6 maart 2015; <https://www.wired.com/2015/06/how-googles-new-photos-app-can-tell-cats-from-dogs/>*;* <https://cs231n.github.io/convolutional-networks/#overview>; (geraadpleegd op 16 mei 202&). [↑](#footnote-ref-387)
388. WP29, “Opinion 02/2012 on facial recognition in online and mobile services”, 2012, 1. [↑](#footnote-ref-388)
389. Ibid 31, FRA, Handbook, 1; <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-389)
390. WP29, “Opinion 03/2012 on developments in biometric technologies”, 27 april 2012,4. [↑](#footnote-ref-390)
391. Art. 3, 13) Richtlijn Politie en Justitie en art.4, 14) AVG. [↑](#footnote-ref-391)
392. WP29, “Opinion 04/2007 on the concept of personal data”, 2007, 9; <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. [↑](#footnote-ref-392)
393. art. 13 Richtlijn Politie en Justitie, art. 4, 14 AVG; Ibid 390. [↑](#footnote-ref-393)
394. Ibid 390. [↑](#footnote-ref-394)
395. Ibid 394. [↑](#footnote-ref-395)
396. Ibid 390. [↑](#footnote-ref-396)
397. [Ibid](https://cs231n.github.io/convolutional-networks/%22%20%5Cl%20%22overview) 383.; H. POKHARNA, “For Dummies-The Introduction to Neural Networks we all need! (Part 1)”, *Medium,* 2016; <https://medium.com/technologymadeeasy/for-dummies-the-introduction-to-neural-networks-we-all-need-c50f6012d5eb>. [↑](#footnote-ref-397)
398. R. VAN BRAKEL, “Een reflectie over het huidige toezicht van het gebruik van surveillancetechnologie door de lokale politie in België”, *Cahiers Politiestudies,* 2020, 142; Ibid 383, POH. [↑](#footnote-ref-398)
399. [↑](#footnote-ref-399)
400. Ibid FUSSEY, MURRAY, “Independent Report”, 19.

 <https://docs.aws.amazon.com/rekognition/latest/dg/faces-sqs-video.html>*;* (geraadpleegd op 16 mei 2021); Zie ook Deel V, 2: technologische basis. [↑](#footnote-ref-400)
401. Zie deel V, 2. [↑](#footnote-ref-401)
402. Zie deel VIII, 2, c, d. [↑](#footnote-ref-402)
403. Zie bijvoorbeeld deel X, 1, c, rechtmatigheidsgrond, Zie ook Ibid 290. [↑](#footnote-ref-403)
404. De privacyvoorwaarden die voortvloeien uit de Richtlijn Politie en Justitie, AVG, WBP. [↑](#footnote-ref-404)
405. Zie deel X, 1, c, wetenschappelijk onderzoek: privacygaranties via copyrightregels. Zie deel X, 2: garanties in de aankoopfase. [↑](#footnote-ref-405)
406. Discussie over horizontaliteit van mensenrechten in het algemeen: E. FRANTZIOU, “The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality”, *European Law Journal,* 2015. [↑](#footnote-ref-406)
407. Ibid 170, LIGA VOOR MENSENREHTEN, “Mensenrechten-Een kennismaking”, 9, 38; Ibid 113, FRA, *Handbook*, 15. [↑](#footnote-ref-407)
408. Zie deel VII, 1, b). [↑](#footnote-ref-408)
409. Zie deel IX, 4. [↑](#footnote-ref-409)
410. UNIVERSITEIT VAN TILBURG, “Op het eerste gezicht: een verkenning van gezichtsherkenning en privacyrisico’s in horizontale relaties”, *WODC,* 2020, 57. [↑](#footnote-ref-410)
411. #  Ibid 192, EDPB “EDPB response”, 2-3.

 [↑](#footnote-ref-411)
412. K. HILL, “The secretive company that might end privacy as we know it”, *The New York Times,* 2020. [https://www.nytimes.com/2020/01/18/technology/clearview-privacyfacial-recognition.html](https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html)*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-412)
413. #  J. ISAAC, M. J. HANNA, “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection”, *IEEE,* 2018; <https://ieeexplore.ieee.org/abstract/document/8436400>. Voor een overzicht van de Cambridge Analytica-affaire, zie ook de documentaire “The Great Hack”.

 [↑](#footnote-ref-413)
414. Art. 11, lid 1, Gemoderniseerd Verdrag 108, art. 4, lid 2, a) en art. 9, lid 1 Richtlijn Politie en Justitie, art. 6 lid 4 AVG. [↑](#footnote-ref-414)
415. <https://developer.twitter.com/en/developer-terms/more-on-restricted-use-cases>, J. PORTER, “Facebook and Linkedin are latest to demand Clearview stop scraping images for facial recognition tech”, *The Verge,* 2020; <https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-415)
416. Ibid 412, K. HILL, “The secretive company”. [↑](#footnote-ref-416)
417. M. ZIMMER, ““But the data is already public”: on the ethics of research in Facebook”, *Ethics and Information Technology,* 2010; [https://link.springer.com/article/10.1007%2Fs10676-010-9227-5](https://link.springer.com/article/10.1007/s10676-010-9227-5); (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-417)
418. Art. 7 AVG. Voor meer richtlijnen over de voorwaarden voor een geldige toestemming: WP29, Guidelines on consent under Regulation 2016/679, 2018. [↑](#footnote-ref-418)
419. overweging 47 AVG. [↑](#footnote-ref-419)
420. F. L. GATTA, “Social media and applications to the ECtHR: connecting people in the name of human rights?”, *Strasbourg Observers,* 2020; <https://strasbourgobservers.com/2020/06/04/social-media-and-applications-to-the-ecthr-connecting-people-in-the-name-of-human-rights/>; (geraadpleegd op 16 mei 2021); S. E. HENDERSON, “Expectations of Privacy in Social Media”, *Mississippi College Law Review,* 2012. (dit gaat over privacy in Amerikaans recht) [↑](#footnote-ref-420)
421. #  Ibid 192, EDPB, “EDPB response”.

 [↑](#footnote-ref-421)
422. J. R. SMITH, “IBM Research releases ‘Diversity in Faces’ Dataset to Advance Study of Fairness in Facial Recognition Systems”, *IBM,* 2019; <https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-422)
423. Ibid 410, UNIVERSITEIT VAN TILBURG, “Op het eerste gezicht”, 58. [↑](#footnote-ref-423)
424. Ibid 424. [↑](#footnote-ref-424)
425. art. 21 AVG. [↑](#footnote-ref-425)
426. Ibid 424. [↑](#footnote-ref-426)
427. R. MERKLEY, “Use and Fair Use: Statement on shared images in facial recognition AI”, *Creative Commons,* 2019; <https://creativecommons.org/2019/03/13/statement-on-shared-images-in-facial-recognition-ai/>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-427)
428. Art. 5 lid 1, juncto art. 89 lid 1 AVG. [↑](#footnote-ref-428)
429. Art. 5 lid 1 AVG, art. 4, b) Richtlijn Politie en Justitie, art. 5 lid, b) Gemoderniseerd Verdrag 108. Passende waarborgen (zoals anonimisering, encryptie of pseudonimisering, beperkingen tot toegang tot persoonsgegevens) blijven echter in dit geval noodzakelijk. (Art. 5 lid 1 AVG, art. 5 lid 4, b) Gemoderniseerd Verdrag 108, art. 4, lid 3 Richtlijn Politie en Justitie). [↑](#footnote-ref-429)
430. Overweging 12, EUROPEES PARLEMENT, RAAD, Richtlijn (EU) 2019, 790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG. [↑](#footnote-ref-430)
431. Ibid 430, Richtlijn inzake auteursrechten. [↑](#footnote-ref-431)
432. Gezien de EDPS in haar Preliminary Opinion dit onderscheid hanteert bij het definiëren van het begrip, hanteer ik deze opdeling van entiteiten ook in het kader van dit onderdeel. De EDPS heeft als onafhankelijke autoriteit opgericht door de Europese als taak om EU- instellingen raad te geven en samenwerking met nationale gegevensbechermingsautoriteiten te bevorderen. Het heeft dus een belangrijke autoriteit mbt gegevensbescherming op Europees niveau. (EDPS, “A preliminary opinion on data protection and scientific research”, 2020, 10.) [↑](#footnote-ref-432)
433. Peter van Schelven wees me op dit onderscheid. Zie voor een verdere uiteenzetting Deel X, 2. [↑](#footnote-ref-433)
434. De vraag is echter in welke mate de ontwikkelaar deze rechtsgrond kan aanduiden. Zie deel X, 1, c, rechtmatigheid. [↑](#footnote-ref-434)
435. F. PASQUALE, *The Black Box Society, The Secret Algorithms that control money and information*,Harvard University Press, Cambridge Massachusetts, 2015. [↑](#footnote-ref-435)
436. T. BUCHER, [Neither black nor box: ways of knowing algorithms](https://link.springer.com/chapter/10.1007/978-3-319-40700-5_5), In: S. A. KUBITSCHKO, A. KAUN, (eds.) *Innovative Methods in Media and Communication Research*, London: Palgrave Macmillan, 2017, 82. [↑](#footnote-ref-436)
437. W.H.K. CHUN, *Programmed Visions: Software and Memory*, Cambridge, MA: MIT Press*,* 2011, 54. [↑](#footnote-ref-437)
438. art. 5 AVG, art. 12 AVG, art. 8, art. 9 Gemoderniseerd Verdrag 108. [↑](#footnote-ref-438)
439. art. 12 AVG. [↑](#footnote-ref-439)
440. overweging 39 AVG. [↑](#footnote-ref-440)
441. art. 12 AVG. [↑](#footnote-ref-441)
442. EDPS, Opinion 7/2015, “Meeting the challenges of big data, a call for transparency, user control, data protection by design and accountability”, 2015, 4. [↑](#footnote-ref-442)
443. DATATILSYNET, (Noorse GBA), “Report on Artificial intelligence and privacy”, 2018, 27. [↑](#footnote-ref-443)
444. Ibid 301, EDWARDS, VEALE, “Slave to the algorithm?”, 2017, 16. [↑](#footnote-ref-444)
445. Ibid 436, 81-89. [↑](#footnote-ref-445)
446. Ibid 301, EDWARDS, VEALE, “Slave to the algorithm?”, 2017, 81. [↑](#footnote-ref-446)
447. Ibid 301, EDWARDS, VEALE, “Slave to the algorithm?”, 2017, 65 e.v. [↑](#footnote-ref-447)
448. FRA, *Handbook on European data protection law,* Luxemburg, Imprimerie Centrale in Luxembourg 2018, 122. [↑](#footnote-ref-448)
449. Ibid 135, WP29, “Opinion 01/2014”, 2014, 21. [↑](#footnote-ref-449)
450. Zie Deel VIII, 1, toepassingsgebied Richtlijn Politie en Justitie. [↑](#footnote-ref-450)
451. Het begrip krijgt invulling door art. 5, 1) c) AVG, art. 4, 1) c) en art. 20 Richtlijn Politie en Justitie en art. 5, 4) c) Gemoderniseerd Verdrag 108. Zie: Ibid, 113, FRA, *Handbook*, 125. [↑](#footnote-ref-451)
452. art. 4, 1, c) Richtlijn Politie en Justitie, art. 5, 1, c) AVG, art. 5, 1 Gemoderniseerd Verdrag 108. [↑](#footnote-ref-452)
453. Ibid, 113, FRA, *Handbook*, 350. [↑](#footnote-ref-453)
454. Ibid 453. [↑](#footnote-ref-454)
455. Ibid, 113, FRA, *Handbook*, 125, 356. [↑](#footnote-ref-455)
456. Ibid, 113, FRA, *Handbook*, 125, 351. [↑](#footnote-ref-456)
457. Beleidsadviseur van de Commissaris Generaal bij de federale politie. [↑](#footnote-ref-457)
458. Proefprojecten met facial processing technology tussen 2016 en 2018 bleken voor 96% personen verkeerdelijk te identificeren als verdachten van criminele feiten; L. DEARDEN, “Facial Recognition wrongly identifies public as potential criminals 96% of time, figure reveals”, *Independent,* 7 mei 2019; <https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-458)
459. Ibid 6, COC, “Tussentijds rapport LFR op Zaventem”, 3. [↑](#footnote-ref-459)
460. Ibid 87, DAVIES, e.a., “Rapport South Wales Police”, 5, 25. [↑](#footnote-ref-460)
461. Deze vraag komt van Peter van Schelven. [↑](#footnote-ref-461)
462. art. 21 HEU; Ibid 38, FUSSEY, MURRAY, “Independent Report”, 20-23, 40. [↑](#footnote-ref-462)
463. Ibid 31, FRA, *Rapport over Facial Recognition Technology,* 2. [↑](#footnote-ref-463)
464. <https://ec.europa.eu/jrc/en/publication/study-face-identification-technology-its-implementation-schengen-information-system>; Ibid 31, FRA, *Rapport over Facial Recognition Technology,* 29. [↑](#footnote-ref-464)
465. J. BUOLAMWINI, T. GEBRU, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification”, *Proceedings of Machine Learning Research,* 2018, 3. e.v. [↑](#footnote-ref-465)
466. Ibid 465, BUOLAMWINI, GEBRU, “Gender Shades”, 3. e.v. [↑](#footnote-ref-466)
467. L. GITELMAN, *Raw Data is an oxymoron*, Cambridge, Massachusetts, MIT Press, 2013. [↑](#footnote-ref-467)
468. C. GARVIE, “Garbage in, garbage out, face recognition on flawed data”, *Georgetown Law Center on Privacy & Technology,* 2019; [https://www.law.georgetown.edu/privacytechnology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/](https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/); (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-468)
469. Ibid 465, BUOLAMWINI, GEBRU, “Gender Shades”, 4. [↑](#footnote-ref-469)
470. Over transgender en andere-gender medewerkers is momenteel geen of weinig publieke data beschikbaar. [↑](#footnote-ref-470)
471. S. M. WEST, M. WHITTAKER, K. CRAWFORD, “Discriminating systems, Gender, Race, and Power in AI”, *AI Now Institute,* 2019, 3. [↑](#footnote-ref-471)
472. RvE, “Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems”, 2020, 8, 3.4, 10, §5.3 [↑](#footnote-ref-472)
473. A. SUDMANN (ed.), *The Democratization of Artificial lntelligence, Net Policies in the Era of Learning Algorithms*, Transcript Verlag, Bielefeld, 2019, 197. [↑](#footnote-ref-473)
474. De dataset werd intussen aangepast, maar de dataset bevat nog steeds bestaat nog steeds voor een aanzienlijk deel uit foto’s van zwarte piet; Ibid 473, SUDMANN, *The Democratization of Artificial Intelligence*, 198. [↑](#footnote-ref-474)
475. Ibid 473, SUDMANN, *The Democratization of Artificial Intelligence,* 197. [↑](#footnote-ref-475)
476. Er moet worden opgemerkt dat ze niet enkel deze, maar ook andere datasets gebruikten. Ibid 475. [↑](#footnote-ref-476)
477. Ibid 473, SUDMANN, *The Democratization of Artificial Intelligence,* 197. [↑](#footnote-ref-477)
478. I. D. RAJI, G. FRIED, “About Face: a survey of Facial Recognition Evaluation”, 2021, 7, <https://www.researchgate.net/publication/348958353_About_Face_A_Survey_of_Facial_Recognition_Evaluation>; <https://arxiv.org/abs/2102.00813>. [↑](#footnote-ref-478)
479. Ibid 473, SUDMANN, *The Democratization of Artificial Intelligence,* 195. [↑](#footnote-ref-479)
480. Ibid 456, BUOLAMWINI, GEBRU, “Gender Shades”, 11-12. [↑](#footnote-ref-480)
481. art. 2, 17° Wet van 17 juni 2016 inzake overheidsopdrachten, *BS,* 14 juli 2016 (hierna: wet overheidsopdrachten). [↑](#footnote-ref-481)
482. art. 2, 35° Wet overheidsopdrachten. [↑](#footnote-ref-482)
483. Deze persoon wenste liever anoniem te blijven, maar haalde deze informatie uit het interne zogezegde telefoonboek van de politie, waar Facial Recognition vermeld staat als bevoegdheid van de Centrale Directie van technische en wetenschappelijke politie (DJT). De DJT die o.a. bevoegd is voor de Gerechtelijke Identificatie o.b.v. video-analyse, <https://www.politie.be/5998/nl/over-ons/centrale-directies/centrale-directie-van-technische-en-wetenschappelijke-politie>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-483)
484. <https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg/deelnemers-aan-federaal-aankoopmodel>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-484)
485. <https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg>*.* [↑](#footnote-ref-485)
486. <https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg/gemeenschappelijke-overeenkomsten-go-passieve>*.* [↑](#footnote-ref-486)
487. art. 2, §1 Koninklijk besluit van 22 december 2017 inzake de federaal gecentraliseerde overheidsopdrachten in het kader van het federaal aankoopbeleid, *BS,* 16 januari 2018, <https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg/gemeenschappelijke-overeenkomsten-go-passieve>. De achterliggende redenering achter deze strategie is dat aankopen worden gecentraliseerd, waardoor het mogelijk wordt om het aankoopbeleid o.a. duurzamer te doen verlopen. <https://www.publicprocurement.be/nl/federale-diensten/het-federaal-aankoopoverleg/gemeenschappelijke-overeenkomsten-go-passieve>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-487)
488. art. 4 Wet overheidsopdrachten. [↑](#footnote-ref-488)
489. art. 5 Wet overheidsopdrachten. [↑](#footnote-ref-489)
490. Zie interview Peter van Schelven, mailverkeer met Stéphanie Witters. [↑](#footnote-ref-490)
491. Zie interview Frank Schuermans, Lid-Raadsheer bij het COC: *“Dus men kijkt wat er on the shelf bestaat, zoals dat heet. Dus wat de privésector kan aanbieden en of dat dan bruikbaar is voor politie-doeleinden.”* [↑](#footnote-ref-491)
492. Hoofd van de afdeling Financiën en Logistiek bij PZ Gent. [↑](#footnote-ref-492)
493. Regional Sales Manager binnen de BENELUX bij Avigilon, Motorola Solutions. [↑](#footnote-ref-493)
494. Koen Luykx vermeldt dat Avigilon een “suggestion box” openstelt op haar website, waar klanten suggesties kunnen doen voor toekomstige functionaliteiten. Bovendien communiceren sales managers zoals Luykx met klanten zoals lokale politiezones over de behoeften voor toekomstige software. De resultaten hiervan worden vervolgens meegenomen in de ontwikkeling van nieuwe software. [↑](#footnote-ref-494)
495. Adjunct-DPO bij PZ Oostende, leraar postgraduaat-opleiding tot DPO aan Howest, Business Consultant bij Privaco. [↑](#footnote-ref-495)
496. art. 2, 35° Wet overheidsopdrachten. [↑](#footnote-ref-496)
497. art. 2, 35°, art. 43 Wet overheidsopdrachten. [↑](#footnote-ref-497)
498. Dit is niet onwaarschijnlijk, zeker gezien het nieuwe Voorstel van verordening van de Commissie dat ook privacygaranties inhoudt. [↑](#footnote-ref-498)
499. Zie gesprek met Stéphanie Witters, Adjunct-DPO bij PZ Oostende, leraar postgraduaat-opleiding tot DPO aan Howest en Business Consultant bij Privaco. [↑](#footnote-ref-499)
500. Beleidsadviseur van de Commissaris Generaal bij de federale politie. [↑](#footnote-ref-500)
501. Directeur Operaties bij politiezone Rupel. [↑](#footnote-ref-501)
502. Zie infra: Deel V, 2: proefprojecten, Deel VI, e, meten effectiviteit. [↑](#footnote-ref-502)
503. art. 4 Wet overheidsopdrachten. [↑](#footnote-ref-503)
504. Regional Sales Manager binnen de BENELUX bij Avigilon, Motorola Solutions. [↑](#footnote-ref-504)
505. Interview met Koen Luykx, Regional Sales Manager binnen de BENELUX bij Avigilon, Motorola Solutions; interview met Nick Noël, Directeur Operaties bij PZ Rupel; VERHEYDEN, T., “Privacy & Ik”, *Vrt,* 2021.. [↑](#footnote-ref-505)
506. <https://www.proximus.be/en/id_b_cl_axis_partner_award/companies-and-public-sector/blog/news-blog/news/axis-partner-award.html>. [↑](#footnote-ref-506)
507. Koen Luykxmeent dat deze raamovereenkomst in zekere zin ingaat tegen de Wet Overheidsopdrachten. Hij vertelt dat het bij de aanbesteding van de ANPR-camera’s zeer moeilijk was voor Avigilon om te wedijveren met die twee spelers, gezien er heel grote bedragen werden vereist om attesten te verkrijgen die de camera’s homologeerden. [↑](#footnote-ref-507)
508. In het kader van de continue verbetering van software, is het relevant dat ook software-updates deel kunnen uitmaken van zo’n raamovereenkomst. Deze gebeuren immers in het ene bedrijf al sneller dan in het andere. Men kan zich dus afvragen in welke mate het mogelijk is om op voorhand voorwaarden te voorzien in de raamovereenkomst die ook voor latere software-updates privacygaranties voorzien. Zie deel X, 3, c) doelbinding en function creep in de aankoopfase. [↑](#footnote-ref-508)
509. art. 20 Richtlijn Politie en Justitie, art. 25 AVG, art. 20 §1, 9° WBP. [↑](#footnote-ref-509)
510. art. 20 Richtlijn Politie en Justitie, art. 20 §1, 9° WBP. [↑](#footnote-ref-510)
511. Of titel I en titel II WBP; Deel IV, 2, c, en Deel VII, 3. Zie ook infra: Deel VI, 3, c, verantwoordelijkheidsbeginsel. [↑](#footnote-ref-511)
512. Hierbij is in eerste instantie belangrijk om te weten of het voor politionele dan wel niet-politionele doeleinden zal worden ingezet. Daarnaast is het ook belangrijk om de concrete doeleinden van het gebruik van LFR voor een bepaalde politionele operatie belangrijk. [↑](#footnote-ref-512)
513. Zie voor een omstandig overzicht van deze risico’s: Ibid 410, UNIVERSITEIT VAN TILBURG, “Op het eerste gezicht”. [↑](#footnote-ref-513)
514. art. 22, lid 3 Richtlijn Politie en Justitie; zie Deel VI, 2, c. [↑](#footnote-ref-514)
515. Hij vat de praktijk samen als volgt: *“Hebben we een derdeverwerkersovereenkomst?”, dan ben je geslaagd!* (lacht) *En dat is wel belangrijk, maar ja, dan heb je nog geen garantie dat die mensen dat überhaupt doen, want die werken dan soms express wat tegen. En dat duurt dat wat langer. Ofwel zeggen die: “Ik zal tekenen, maar ik doe toch mijn goesting.”* [↑](#footnote-ref-515)
516. art. 42 AVG. [↑](#footnote-ref-516)
517. Mailverkeer met Stéphanie Witters, adjunct-DPO PZ Oostende. [↑](#footnote-ref-517)
518. <https://www.iso.org/about-us.html#2> *;* <https://www.27000.org/background.html>; (geraadpleegd op 16 mei 2021). G. DISTERER*, “ISO/IEC 27000, 27001 and 27002 for Information Security Management”, Journal of Information Security, 2013.* [↑](#footnote-ref-518)
519. G. DISTERER, “ISO/IEC 27000, 27001 and 27002 for Information Security Management”, *Journal of Information Security,* 2013. [↑](#footnote-ref-519)
520. <https://www.iso.org/standard/42103.html>*;* A. CALDER, “Implementing Information Security based on ISO 27001/ISO 27002”, *Van Haren,* 2011, 2; W. STALLINGS, *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices,* Addison-Wesley Professional, 2019*,* 70, 295. [↑](#footnote-ref-520)
521. Ibid 519, DISTERER, “ISO/IEC 27000, 27001 and 27002 for Information Security Management”, *Journal of Information Security,* 2013. [↑](#footnote-ref-521)
522. Ibid 520, CALDER, “Implementing Information Security”*,* 2011,2; Ibid 520, STALLINGS, *Information Privacy Engineering and Privacy by Design,* 70. [↑](#footnote-ref-522)
523. <https://www.iso.org/standard/71670.html>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-523)
524. art. 29 e.v. Richtlijn Politie en Justitie. [↑](#footnote-ref-524)
525. art. 20 Richtlijn Politie en Justitie, art. 25 AVG. [↑](#footnote-ref-525)
526. art. 27 lid 1 Richtlijn Politie en Justitie, art. 23 lid 2 WBP. [↑](#footnote-ref-526)
527. Interview Peter Van Schelven, (Zelfstandig Juridisch Adviseur in Nederland); Interview Stéphanie Witters, adjunct-DPO PZ Oostende. [↑](#footnote-ref-527)
528. art. 4 Wet overheidsopdrachten. [↑](#footnote-ref-528)
529. <https://ec.europa.eu/digital-single-market/en/innovation-procurement>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-529)
530. Hiermee wilde de EC een strategie lanceren voor de organisatie van de Europese digitale markt: <https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-530)
531. Ibid 529. [↑](#footnote-ref-531)
532. <https://ec.europa.eu/digital-single-market/en/public-procurement-innovative-solutions>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-532)
533. Deel X, 2, b). [↑](#footnote-ref-533)
534. In het Columbus- opleidingsprogramma voor leidinggevenden bij de politie en uit zijn persoonlijke ervaring bij de Nederlandse politie leerde Nick Noël dat de Nederlandse politie zulke methoden reeds meer toepast dan de Belgische politie. Het Columbus-programma dat innovatieve opleidingen geeft aan leidinggevende politieambtenaren in België en Nederland lijkt in dit opzicht interessant; <https://www.politieacademie.nl/thema/politieleiderschap/Advanced%20Programmes/Paginas/Columbus-VIII.aspx>. [↑](#footnote-ref-534)
535. <https://ec.europa.eu/digital-single-market/en/open-innovation-20>; (geraadpleegd op 16 mei 2021); S. CAVALLINI, R. SOLDI, J. FRIEDL, M. VOLPE, “Using the Quadruple Helix Approach to Accelerate the Transfer of Research and Innovation Results to Regional Growth”, *EU* 2016, 5. [↑](#footnote-ref-535)
536. E. G. CARAYANNIS, D. F. J. CAMPBELL, “Mode 3 Knowledge Production in Quadruple Helix Innovation Systems”, in E. G. CARAYANNIS, D. G. J. CAMPBELL, *Mode 3 Knowledge Production in Quadruple Helix Innovation Systems, 21st-Century Democracy, Innovation, and Entrepeneurship for Development,* Springer, New York, 2012, 1; <https://doi.org/10.1007/978-1-4614-2062-0_1>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-536)
537. <https://www.politie.be/5998/nl/over-ons/centrale-directies/centrale-directie-van-technische-en-wetenschappelijke-politie>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-537)
538. <https://police-hackathon.be/nl/>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-538)
539. <https://speed.wazoku.com/#/community/b6e9b42e2627478ba8cc9b5a17357428/home-page>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-539)
540. <https://speed.wazoku.com/#/challenge/ebd3daa145df45f4ae8ba178da50e91a?scrollTo=scrollDisco&entities=idea&sort=-relevancy&page=3&pageSize=15&parentType=challenge&parentId=ebd3daa145df45f4ae8ba178da50e91a&communityId=b6e9b42e2627478ba8cc9b5a17357428&query=antwerpen&filters=%7B%22show_archived%22:true%7D>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-540)
541. Opsomming van de gebruikte persoonsgegevens in: Ibid 323, *The Queen Bridges/Chief Constable*, 13. [↑](#footnote-ref-541)
542. Ibid 31, FRA, “Rapport over facial recognition technology”, 25; Ibid 390, “Opinion 03/2012”, 2012, 4. [↑](#footnote-ref-542)
543. Zie voor een aantal voorbeelden: A. C. E. HURST, “Facial recognition software in clinical dysmorphology”, *Current Opinion in Pediatrics,* 2018 ; https://journals.lww.com/co-pediatrics/Fulltext/2018/12000/Facial\_recognition\_software\_in\_clinical.3.aspx?casa\_token=RNiJH\_BbBX8AAAAA:Q-SJNUB9JgFDzpNE1DFppcHFJVU-rOYoTN0l0lxEZsA3D05vjhAAo\_Bd4AbckLi6ERkG5N4\_IK3h9xZlbb2iwCiq8\_qQCt1JbVXp (geraadpleegd op 16 mei 2021).; S.- H. RABIA, H. SCHNEIDER, E. NAVARRO, e.a., “Automatic recognition of the XLHED phenotype from facial images”, *American Journal of Medical Genetics,* 2017; <https://onlinelibrary.wiley.com/doi/full/10.1002/ajmg.a.38343?casa_token=0KMLGA2oy2UAAAAA%3AzwMvxdGsdTIir2b5vyLlOiwcLjuc8UNUvvj4hxfAIOg_uoI65Qo4pq4KZrjnjcR9MHG1kzUXKSyHpbOy>; (geraadpleegd op 16 mei 2021); R. P. KOSILEK, R. FROHNER, R. P. WÜRTZ, “Diagnostic use of facial image analysis software in endocrine and genetic disorders: review, current results and future perspectives”, *European Journal of Endocrinology,* 2015. [↑](#footnote-ref-543)
544. Dit is “informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel, met inbegrip van genetische gegevens en biologische monsters; en informatie over bijvoorbeeld ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron, zoals bijvoorbeeld een arts of een andere gezondheids­ werker, een ziekenhuis, een medisch hulpmiddel of een in-vitrodiagnostiek.” (Overweging 35 AVG). [↑](#footnote-ref-544)
545. Ibid 323, *Queen Bridges/Chief constable*, §41. [↑](#footnote-ref-545)
546. HvJ 19 oktober 2016, nr. C-582/14, Patrick Breyer/Bundesrepublik Deutschland, ECLI:EU:C:2016:779, §49. [↑](#footnote-ref-546)
547. Deel VIII, 2, b). [↑](#footnote-ref-547)
548. Ibid 31, FRA, “Rapport over Facial Recognition Technology”, 25. [↑](#footnote-ref-548)
549. Ibid 548. [↑](#footnote-ref-549)
550. Deel X, 1, c), transparantie. [↑](#footnote-ref-550)
551. overweging 47 AVG: redelijke verwachtingen van de betrokkene. [↑](#footnote-ref-551)
552. De Algemene Nationale Gegevensbank (ANG) is de politionele gegevensbank die de gegevens bedoeld in artikel 44/5 en de informatie bevat die voor het geheel van de politiediensten nodig zijn om hun opdrachten uit te oefenen(…). (art. 44/7 WPA). De basisgegevensbanken dienen dan weer voor het geheel van de geïntegreerde politie en heeft als doel om de opdrachten van bestuurlijke en van gerechtelijke politie uit te oefenen door de erin vervatte persoonsgegevens en informatie te exploiteren en door de bevoegde overheden te informeren over de uitoefening van deze opdrachten. (art. 44/11/2 WPA) De bijzondere gegevensbanken kunnen worden opgericht in specifieke omstandigheden om bijzondere behoeften te vervullen. (art. 44/11/3 WPA). [↑](#footnote-ref-552)
553. art.44/11/3bis e.v WPA. Deze dienen voor de gezamenlijke uitoefening van de opdrachten. [↑](#footnote-ref-553)
554. art. 4/11/3 quater; <https://news.belgium.be/nl/gemeenschappelijke-gegevensbank-terrorist-fighters>. [↑](#footnote-ref-554)
555. art. 44/11/3 sexies e.v WPA. [↑](#footnote-ref-555)
556. art. 44/2, §3 WPA. [↑](#footnote-ref-556)
557. art. 44/11/3decies WPA. [↑](#footnote-ref-557)
558. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, afl. 670. [↑](#footnote-ref-558)
559. Ibid 6, COC, “Tussentijds rapport over LFR op Zaventem”, 4. [↑](#footnote-ref-559)
560. Art. 44/2§3 WPA. [↑](#footnote-ref-560)
561. art. 44/2, §3, 44/11/3sexies-44/11/3decies WPA. [↑](#footnote-ref-561)
562. T. DE SCHEPPER, “Welke regels gelden voor de verwerking van ANPR-data?”, *Politeia Uitgeverij,* 2020; [https://politeia.be/nl/artikels/252507-welke+regels+gelden+voor+de+verwerking+van+anpr-data%3f](https://politeia.be/nl/artikels/252507-welke%2Bregels%2Bgelden%2Bvoor%2Bde%2Bverwerking%2Bvan%2Banpr-data%3F)*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-562)
563. Ibid 562. [↑](#footnote-ref-563)
564. Ibid 2, RAJI, FRIED, “About Face”, 3. [↑](#footnote-ref-564)
565. L.D. INTRONA, H. NISSENBAUM, “Facial Recognition Technology-A Survey of Policy and Implementation Issues”, *New York University, CCPR- Center for Catastrophic preparedness and response,* 2009, 3. [↑](#footnote-ref-565)
566. M. SHARIF, F. NAZ, “Face Recognition: A Survey”, *Journal of Engineering Science and Technology Review* 2017; <https://www.semanticscholar.org/paper/Face-Recognition%3A-A-Survey-Sharif-Naz/bb86bed5f8b98c65a4f882858523bb8ee12ad6ba>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-566)
567. Beleidsadviseur van de Commissaris Generaal bij de federale politie. [↑](#footnote-ref-567)
568. Ibid 87, DAVIES, e.a., “Rapport South Wales Police”, 12. [↑](#footnote-ref-568)
569. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 666. [↑](#footnote-ref-569)
570. Interview Frank Schuermans, Lid-Raadsheer bij het COC. [↑](#footnote-ref-570)
571. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 16. [↑](#footnote-ref-571)
572. Ibid 138, *Tele2Sverige/Secretary of State for the Home Department,* §232. [↑](#footnote-ref-572)
573. Ibid 87, DAVIES, e.a., “Rapport South Wales Police”, 12. [↑](#footnote-ref-573)
574. Ibid 87, DAVIES, e.a., “Rapport South Wales Police”, 12. [↑](#footnote-ref-574)
575. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA- CONVENTION 108*-* “Guidelines on Facial Recognition”, *Directorate General of Human Rights and Rule of Law*, 2021, 6. Dit is momenteel (naast het voorstel voor een verordening rond AI van de EC) een van de weinige bronnen op Europees niveau die richtlijnen uitvaardigt rond gezichtsherkenning zowel in de publieke als private sector. [↑](#footnote-ref-575)
576. EHRM, 6 september 1978, nr. 5029/71, *Klass en anderen*, § 42; EHRM, 12 januari 2016, nr. 37138/14, *Szabó en Vissy/Hongarije,* §54; P. VOGIATZOGLOU, “Mass Surveillance and the European Courts”, *KULeuven CiTiP,* 2017. [↑](#footnote-ref-576)
577. EHRM, 24 januari 2019, nr. 43514/15, *Catt/Verenigd Koninkrijk,* §§108, 114. [↑](#footnote-ref-577)
578. Ibid 577, 114. [↑](#footnote-ref-578)
579. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 11. [↑](#footnote-ref-579)
580. art. 5 (4) a) Gemoderniseerd Verdrag 108, Overweging 26 Richtlijn Politie en Justitie. [↑](#footnote-ref-580)
581. Overweging 26 Richtlijn Politie en Justitie. [↑](#footnote-ref-581)
582. Ibid 215, CDEI, “Snapshot Series”, 22. [↑](#footnote-ref-582)
583. N.A. MOREHAM, “Privacy in Public Places”, *The Cambridge Law Journal,* 2006, 1.

<https://www.jstor.org/stable/pdf/4509242.pdf?refreqid=excelsior%3A52025066a0e315e9287b9d059c557bf7>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-583)
584. EHRM, 25 december 2001, P. G. en J. H./ Verenigd Koninkrijk, §57. [↑](#footnote-ref-584)
585. Ibid 584. [↑](#footnote-ref-585)
586. art. 25/2, §2, lid 1 WPA. [↑](#footnote-ref-586)
587. Deze regels zijn terug te vinden in KB van 28 mei 2018 tot wijziging van het koninklijk besluit van 10 februari 2008 tot vaststelling van de wijze waarop wordt aangegeven dat er camerabewaking plaatsvindt, *BS* 1 juni 2018. [↑](#footnote-ref-587)
588. Plaatsbezoek Politiezone Rupel onder begeleiding van Nick Noël, Directeur Operaties bij PZ Rupel. [↑](#footnote-ref-588)
589. De rechtmatigheid van verwerkingen met LFR hangt o.a. samen met het vooropgestelde legitieme belang en de concrete doelen waarvoor deze zullen worden ingezet. Zie voor enkele mogelijke doelen: deel VI, 2. [↑](#footnote-ref-589)
590. Deze toestemming wordt geacht impliciet gegeven te zijn wanneer men zich in een openbare ruimte begeeft. Om dit gebrek aan toestemming te compenseren, hanteert men het begrip van de redelijke verwachtingen van privacy;

Ibid 583, MOREHAM, “Privacy in Public Places”, 1. [↑](#footnote-ref-590)
591. art. 8 Richtlijn Politie en Justitie. [↑](#footnote-ref-591)
592. art. 13 Richtlijn Politie en Justitie. Zie ook de verplichting in het voorstel voor een Verordening voor AI, p.14-15. [↑](#footnote-ref-592)
593. art. 13, lid 1 en 2 Richtlijn Politie en Justitie. [↑](#footnote-ref-593)
594. Gemeenschappelijke richtlijn MFO-3 van 14 juni 2002 van de Ministers van Justitie en van Binnenlandse Zaken betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie, *BS* 18 juni 2002. (hierna: MFO-3) [↑](#footnote-ref-594)
595. Interview met Anke Stakenborg, Beleidsadviseur van de Commissaris-Generaal bij de federale politie. Frank Schuermans, Lid- Raadsheer bij het COC zegt hierover: “*Dus een belangrijke omzendbrief is de MFO-3. Dat is een geheime omzendbrief, maar daarin worden verschillende profielen uit de doeken gedaan. Het is niet de bedoeling dat iedereen toegang heeft tot alles, uiteraard. Dus dat is ook bij de politie zo en dat is ook bij die camera’s zo. Dus daar moet een beleid rond ontwikkeld worden. Dikwijls is dat nog niet voorhanden, bij de goeien is dat wel al voorhanden. En in dat beleid zal men bepalen wie daar toegang toe heeft, dat men ook altijd een reden van raadpleging moet invoeren enzoverder enzovoort. Idem ditto voor het nationale AMS-systeem: daar zal de directeur of de directeur-generaal een profielenbeleid, een toegangsbeleid moeten vaststellen.”* [↑](#footnote-ref-595)
596. COC, “Advies nr.DA200008 van 22 september 2020 betreffende een Gemeenschappelijke richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de toegangsregels van de leden van de politiediensten tot de algemene nationale gegevensbank en de basis-, bijzondere en technische gegevensbank (richtlijn toegangsregels)”, *Adviezen COC*, 2020, 5/9- 6/9. [↑](#footnote-ref-596)
597. Ibid 596, COC, “Advies nr. DA200008”, 6/9. [↑](#footnote-ref-597)
598. Ibid 597. [↑](#footnote-ref-598)
599. Ibid 597. [↑](#footnote-ref-599)
600. Dit is een bezorgdheid van Anke Stakenborg,beleidsadviseur van de Commissaris Generaal bij de federale politie. [↑](#footnote-ref-600)
601. A. RAI, “Explainable AI: from black box to glass box”, *Journal of the Academy of Marketing Science,* 2020; <https://link.springer.com/article/10.1007/s11747-019-00710-5>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-601)
602. Deel X, 1, c, transparantie. Deel X, 3, a). [↑](#footnote-ref-602)
603. Ibid 346, LONDON POLICING ETHICS PANEL, “Final Report on Live Facial Recognition”, 26. [↑](#footnote-ref-603)
604. Ibid 575, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA- CONVENTION 108*, “*Guidelines on Facial Recognition”, 11. [↑](#footnote-ref-604)
605. Met “alle noodzakelijke informatie” wordt hier bedoeld alle informatie opgesomd in art. 8 Verdrag 108: de identiteit van de verwerkingsverantwoordelijke, de rechtmatigheidsgrond, de categorieën persoonsgegevens die worden verwerkt, de ontvangers van de persoonsgegevens, de methoden om zijn rechten uit te oefenen en “aanvullende informatie die moet verzekeren dat de persoonsgegevens fair en transparant worden verwerkt.” Ibid 575, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA- CONVENTION 108*, “*Guidelines on Facial Recognition”, 11-12. [↑](#footnote-ref-605)
606. Ibid 323, *The Queen Bridges/Chief Constable of South Wales Police*, §39-40. [↑](#footnote-ref-606)
607. Ibid 603, 11. [↑](#footnote-ref-607)
608. art. 10 (1) Gemoderniseerd Verdrag 108, art. 4 (4) Richtlijn Politie en Justitie, Ibid 113, FRA, *Handbook,* 134. [↑](#footnote-ref-608)
609. Hoofdstuk IV Richtlijn Politie en Justitie. [↑](#footnote-ref-609)
610. Titel II WBP. [↑](#footnote-ref-610)
611. Gegevensbescherming door ontwerp en door standaardinstellingen. [↑](#footnote-ref-611)
612. Hoofdstuk IV, afdeling 2 Richtlijn Politie en Justitie. [↑](#footnote-ref-612)
613. Hoofdstuk IV, afdeling 3 Richtlijn Politie en Justitie, art. 32 Richtlijn Politie en Justitie. [↑](#footnote-ref-613)
614. Het beginsel van gegevensbescherming door ontwerp. [↑](#footnote-ref-614)
615. Het beginsel van gegevensbescherming door standaardinstellingen. [↑](#footnote-ref-615)
616. art. 20 Richtlijn Politie en Justitie, art. 25 AVG. [↑](#footnote-ref-616)
617. Deel X, 2) fase van de aankoop. [↑](#footnote-ref-617)
618. Interview Peter van Schelven, Zelfstandig Juridisch Adviseur in Nederland, met uitgebreide ervaring binnen het gegevensbeschermingsrecht. [↑](#footnote-ref-618)
619. art. 19 Richtlijn Politie en Justitie, art. 50 WBP. [↑](#footnote-ref-619)
620. Dit hangt samen met het basisbeginsel van vertrouwelijkheid en integriteit (art. 29 e.v. Richtlijn Politie en Justitie.) en de vereiste van privacy by design of gegevensbescherming door ontwerp (art. 20 Richtlijn Politie en Justitie). [↑](#footnote-ref-620)
621. art. 20 lid 1 Richtlijn Politie en Justitie [↑](#footnote-ref-621)
622. S. GÜRSES, C. TRONCOSE, C. DIAZ, “Engineering Privacy by Design”, *KULeuven, gepresenteerd op Conference on Computers, Privacy & Data Protection,* 2011, 1. [↑](#footnote-ref-622)
623. art. 20 lid 1 Richtlijn Politie en Justitie [↑](#footnote-ref-623)
624. Ibid 622. [↑](#footnote-ref-624)
625. Ibid 622. [↑](#footnote-ref-625)
626. Ibid 622. [↑](#footnote-ref-626)
627. Zie ook: <https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security> over de “state of the art” van de technische maatregelen die bedrijven kunnen gebruiken voor hun IT beveiliging. [↑](#footnote-ref-627)
628. Ibid 167, EDRi, “Ban Biometric Mass Surveillance”, 35. [↑](#footnote-ref-628)
629. Policy and Campaigns Officer bij European Digital Rights (EDRi). [↑](#footnote-ref-629)
630. *“It’s going to, by definition, scan any person that walks by, even if their data is subsequently discarded after ten seconds or you know, even ten milliseconds*. *It already infringed their right to privacy, data protection, anonymity and you know with the potential impact on a load of other fundamental rights, just by the fact that it’s capturing people’s data as they go. Very sensitive personal data if… they’re going about in public. So that, by definition, is inherently disproportionate and unnecessary.”* [↑](#footnote-ref-630)
631. Deel X, 2, c. [↑](#footnote-ref-631)
632. Voor een duidelijk voorbeeld van hoe zo’n GEB eruit ziet: J. GALLE, S. WITTERS, “Template Risico-Analyse DPIA”, *Postgraduaat DPO Howest,* 2021. [↑](#footnote-ref-632)
633. art. 27 Richtlijn Politie en Justitie, art. 23 Wet Bescherming Persoonsgegevens. [↑](#footnote-ref-633)
634. WP29, “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”*,* 2017; <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>*.* [↑](#footnote-ref-634)
635. Ibid 634, 28. [↑](#footnote-ref-635)
636. Ibid 575, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA- CONVENTION 108*, “*Guidelines on Facial Recognition”, 14. [↑](#footnote-ref-636)
637. Data Protection Officer. [↑](#footnote-ref-637)
638. Hoofdstuk IV, afdeling 3 Richtlijn Politie en Justitie, art. 32 Richtlijn Politie en Justitie. [↑](#footnote-ref-638)
639. art. 44/11/3 quinquies WPA. [↑](#footnote-ref-639)
640. Frank Schuermans, Lid-Raadsheer bij het COC zegt: “En dat begint wel, dus ik ben vrij positief over de ontwikkeling. Er is nog veel werk, maar er is een enorme awareness aan de gang, ook bij de politie over het feit dat dataprotectie nu eenmaal bestaat, dat niet noodzakelijk tegenstrijdig hoeft te zijn aan hun operationele doelstellingen: de veiligheidsdoelstellingen, de opsporingsdoelstellingen, maar dat het bestaat en dat ze ermee moeten rekening houden…. Het gaat beter, vind ik in het noorden van het land dan in het zuiden van het land. Bijvoorbeeld, de politiezone Antwerpen: die hebben echt een Data Protection Office. Dat is een model voor mij (…).” [↑](#footnote-ref-640)
641. art. 34 Richtlijn Politie en Justitie, art. 65 WBP. [↑](#footnote-ref-641)
642. <https://www.politieantwerpen.be/privacyverklaring>*.* [↑](#footnote-ref-642)
643. <https://www.howest.be/nl/opleidingen/postgraduaat/data-protection-officer/praktisch#Waaruit-bestaat-uit-het-programma>*.* [↑](#footnote-ref-643)
644. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 17. [↑](#footnote-ref-644)
645. Ibid 644. [↑](#footnote-ref-645)
646. N. VANHECKE, “Éen stap van gezichtsherkenning verwijderd: Kortrijk vindt in geen tijd de man in de rode trui”, *De Standaard,* 24 mei 2019;<https://www.standaard.be/cnt/dmf20190523_04420266>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-646)
647. D. FIERS, J. TRUYTS, “ANPR-camera’s fotograferen niet enkel nummerplaat”, *vrt nws,* 2017; <https://www.vrt.be/vrtnws/nl/2017/02/08/anpr-camera_s_fotograferennietenkelnummerplaat-1-2886393/>; (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-647)
648. J. MEESE, “Onrechtmatig verkregen bewijs in strafzaken” in J. MEESE, *Bewijsnood na het vernieuwde bewijsrecht,* Mortsel, Intersentia, 2020, 61. [↑](#footnote-ref-648)
649. Voor een overzichtelijk artikel over de huidige stand van zaken in België rond de kwestie van onrechtmatig verkregen bewijs in de context van “mass data gathering”, zie: E. MAES, M. PANZAVOLTA, “Op zoek naar normatief principe voor uitsluiting van onrechtmatig verkregen bewijs in tijdperk van “mass data gathering””, *de Juristenkrant,* 2021. [↑](#footnote-ref-649)
650. F. GOOSSENS (ed.), *Dragers van de politiefunctie- een dwarsdoorsnede van de reguliere politie, de Veiligheid van de staat, de bijzondere politiediensten en de private politie*, Kluwer Belgium, Mechelen 2012, 14. B. WARNEZ, De lokale bestuurlijke ordehandhaving in Vlaanderen. Een kritische analyse van de actoren en hun bevoegdheden, Brugge, die Keure/ la Charte, 2020, 20. [↑](#footnote-ref-650)
651. B. WARNEZ, *De lokale bestuurlijke ordehandhaving in Vlaanderen. Een kritische analyse van de actoren en hun bevoegdheden,* Brugge, die Keure/la Charte, 2020, 13. Voor een schematisch overzicht van de bestuurlijke ordehandhaving door lokale besturen in Vlaanderen: zie: B. WARNEZ, 36-37. [↑](#footnote-ref-651)
652. B. WARNEZ, “Het beginsel van kenbaarheid en de lokale bestuurlijke ordehandhaving”, *Tijdschrift voor Wetgeving,* 2019, 6. Een voorbeeld hiervan is de grote beoordelingsbevoegdheid van de Koning om de plaatsen, die een bijzonder veiligheidsrisico inhouden te bepalen. Zie: Grondwettelijk Hof, 20 februari 2020, nr. 27/2020, A5. [↑](#footnote-ref-652)
653. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 16. [↑](#footnote-ref-653)
654. Dit is louter een toepassing van de definitie van function creep. [↑](#footnote-ref-654)
655. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 17. [↑](#footnote-ref-655)
656. <https://www.avigilon.com/solutions/covid-19-resources/no-face-mask-detection> ; <https://www.danners.com/security/covid-19-security-solutions/> ; J. WARD, C. SOTTILE, “A facial recognition company wants to help with contact tracing. A senator has questions.”, *NBC News,* 1 mei 2020. [↑](#footnote-ref-656)
657. C. BURT, “Dermalog and Pensees roll out computer vision temperature check systems for access control”, *Biometric Update.com,* 28 april 2020; <https://www.biometricupdate.com/202004/dermalog-and-pensees-roll-out-computer-vision-temperature-check-systems-for-access-control>*.*  [↑](#footnote-ref-657)
658. Zie omschrijving van het beginsel van dataminimalisatie hierboven. [↑](#footnote-ref-658)
659. CNIL, “Facial Recognition-For a debate living up to the challenges”, *CNIL,* 2019, 7. [↑](#footnote-ref-659)
660. Ibid 659. [↑](#footnote-ref-660)
661. Ibid 87, DAVIES, e.a., “Rapport South Wales Police”, 17. [↑](#footnote-ref-661)
662. En diens persoonsgegevens geanalyseerd, opgeslagen,… [↑](#footnote-ref-662)
663. art. 6 Richtlijn Politie en Justitie. [↑](#footnote-ref-663)
664. overweging 50, overweging 51 Richtlijn Politie en Justitie. [↑](#footnote-ref-664)
665. RvE, “Factsheet on Mass Surveillance”, *RvE,* 2018, 1. [↑](#footnote-ref-665)
666. Zie voor rechtspraak van het EHRM o.a.: EHRM, 6 september 1978, nr. 5029/71, *Klass en anderen;* EHRM, 12 januari 2016, nr. 37138/14, *Szabó en Vissy/Hongarije;* EHRM, 4 februari 2019, nrs. 58170/13, 62322/14, 24960/15, Big Brother Watch e.a./Verenigd Koninkrijk. (een overzicht in: RvE, “Factsheet on Mass Surveillance”, *RvE,* 2018); Voor rechtspraak van het HvJ: HvJ 8 april 2014, nrs.C‑293/12 en C‑594/12, *Digital Rights Ireland Ltd./ Minister for Communications, Marine and Natural Resources en anderen en Kärntner Landesregierung en anderen*, ECLI:EU:C:2014, HvJ, 6 oktober 2015, C-362/14, *Schrems/Data Protection Commissioner,* ECLI: EU: C:2015:650, HvJ, 21 december 2016, *Tele2Sverige/Secretary of State for the Home Department,* ECLI:EU:C:2016:970, HvJ, 26 juli 2017, doc. 62015CV0001(01), Advies van het hof 1/15 omtrent de Canada PNR Agreement, ECLI:EU:C:2017:592; zie ook: Ibid 576, VOGIATZOGLOU. [↑](#footnote-ref-666)
667. G. VERMEULEN, “Non-Paper-Workshop ‘Targeted surveillance and selective data retention’”, *International Intelligence Oversight Forum (IIOF2017) ‘The Road Ahead*. *Dilemmas and Best Practices in Democratic Intelligence Oversight’ Brussels*, 2017, 4. [↑](#footnote-ref-667)
668. Ibid 666, HvJ, *Tele2Sverige,* §106. [↑](#footnote-ref-668)
669. HvJ, 6 oktober 2020, nrs. C-511/18, C-512/18 en C-520/18, *Quadrature du Net*, ECLI: ECLI:EU:C:2020:791. [↑](#footnote-ref-669)
670. Een duidelijke opsomming van deze criteria wordt gegeven in G. VERMEULEN, “Non-Paper-Workshop ‘Targeted surveillance and selective data retention’”, *International Intelligence Oversight Forum (IIOF2017) ‘The Road Ahead*. *Dilemmas and Best Practices in Democratic Intelligence Oversight’ Brussels*, 21 november 2017, 4: Andere voorwaarden zijn bijvoorbeeld dat de maatregel niet willekeurig mag zijn en de verwerking niet mag gebeuren op een algemene basis, deze mag niet willekeurig zijn, mag geen bulkverzameling zijn en moet worden beperkt tot wat strikt noodzakelijk is. Bovendien geldt een beperking of uitzondering slechts in het licht van het nagestreefde doel. De verwerking moet gericht zijn (althans niet volledig ongericht, ruimte voor ‘relatively untargeted'). Daarnaast moet de verwerking worden beperkt tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of op een kring van bepaalde personen en moet die gelimiteerd zijn wat betreft de categorieën gegevens die moeten worden bewaard én de beïnvloede communicatiemiddelen én de bewaartermijn die is vastgesteld én de “betrokken personen” of “het publiek dat mogelijk wordt geaffecteerd”. Ook moet moet worden gedefinieerd op basis van objectief bewijs dat het mogelijk is een persoon te identificeren wiens gegevens: vermoedelijk een link met een ernstig strafbaar feit zullen opleveren, minstens een onrechtstreekse, en op de een of andere manier bijdragen aan de bestrijding van zware criminaliteit of het voorkomen van een ​​ernstig risico voor de openbare veiligheid. Dit hoeft geen 'redelijke verdenking' te zijn.” [↑](#footnote-ref-670)
671. art. 10 en 11 Richtlijn Politie en Justitie, overweging 38 Richtlijn Politie en Justitie; Ibid 667, VERMEULEN, 5. [↑](#footnote-ref-671)
672. Ibid 667, VERMEULEN, 6. [↑](#footnote-ref-672)
673. art. 11 Richtlijn Politie en Justitie. [↑](#footnote-ref-673)
674. Ibid 672. [↑](#footnote-ref-674)
675. art. 44/11/3decies WPA. [↑](#footnote-ref-675)
676. art. 25/6 WPA. [↑](#footnote-ref-676)
677. art. 46/12 lid 1 WPA. [↑](#footnote-ref-677)
678. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 668. [↑](#footnote-ref-678)
679. 44/9 WPA, (art. 44/2 WPA). [↑](#footnote-ref-679)
680. Ibid 100, DE SCHEPPER, DE HERT, “Versoepeling Camerawet”, 667. [↑](#footnote-ref-680)
681. Grondwettelijk Hof, 20 februari 2020, nr. 27/2020, B9.10. [↑](#footnote-ref-681)
682. Ibid 681, B9.9, B.9.10. [↑](#footnote-ref-682)
683. Ibid 681, B9.9, A6. [↑](#footnote-ref-683)
684. art. 44/11/4- art.44/11/14, art. 46/12-art. 46/14 WPA, art. 9 Camerawet. [↑](#footnote-ref-684)
685. Zie deel VIII, 2, b); deel X, lid 1, c), deel X, lid 3, c). [↑](#footnote-ref-685)
686. B. AERTS, “Onderzoek over gebruik dna-analyse in strafonderzoeken legt pijnpunten bloot”, *De Juristenkrant,* 2018, 9;

<https://www.jurisquare.be/en/journal/djk/2018-379/onderzoek-over-gebruik-dna-analyse-in-strafonderzoeken-legt-pijnpunten-bloot-interview-met-bertrand-/index.html#page/9/search/DNA-database%20politie>*.* [↑](#footnote-ref-686)
687. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 11. [↑](#footnote-ref-687)
688. Deel X, 1, c, nauwkeurigheid. [↑](#footnote-ref-688)
689. High Court of Justice, 4 september 2019, nr. CO/4085/2018, The Queen Bridges/Chief Constable of South Wales Police and others, §9. [↑](#footnote-ref-689)
690. Ibid 689. [↑](#footnote-ref-690)
691. Ibid 689. [↑](#footnote-ref-691)
692. Lid-Raadsheer bij het COC. [↑](#footnote-ref-692)
693. L. MELGAÇO, “Meer camera’s, meer veiligheid? Een analyse over de doeltreffendheid van videosurveillance”, *Orde van de Dag,* 2015, 50. [↑](#footnote-ref-693)
694. ODSC-Open Data Science, “The impact of racial bias in facial recognition software”, 2018; L. D. INTRONA, D. WOOD, “Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems”, *Surveillance & Society* 2004, 192. [↑](#footnote-ref-694)
695. art. 11 Richtlijn Politie en Justitie. [↑](#footnote-ref-695)
696. C. GARVIE, A. BEDOYA, J. FRANKLE, “The perpetual line-up: unregulated police face recognition in America”, *Georgetown Law- Center on Law and Technology,* 2016; <https://www.perpetuallineup.org/>*;* (geraadpleegd op 16 mei 2021). [↑](#footnote-ref-696)
697. Ibid 694, INTRONA, WOOD, 192. Lid-Raadsheer bij het COC Frank Schuermans zegt hierover: *“Dus, qua opleiding van de mensen die daarmee moeten werken…het gevaar met geautomatiseerde systemen is altijd dat politie-ambtenaren er gemakshalve…of het is een menselijke reflex waarschijnlijk van uitgaan dat wat dat ding zegt ook de waarheid is, dat dat ook correct is allemaal.”* [↑](#footnote-ref-697)
698. Ibid 696. [↑](#footnote-ref-698)
699. Ibid 696. [↑](#footnote-ref-699)
700. R. VAN BRAKEL, “Een reflectie over het huidige toezicht van het gebruik van surveillancetechnologie door de lokale politie in België”, *Cahiers Politiestudies,* 2020, 142. [↑](#footnote-ref-700)
701. Interview Bart Schoenmaekers, Hoofd van de afdeling Financiën en Logistiek bij PZ Gent. S. PANCUCCI, “Train the trainer: The Bricks in the Learning Community Scaffold of Professional Development”, *World Academy of Science, engineering and Technology,* 2007. [↑](#footnote-ref-701)
702. Ibid 565, INTRONA, NISSENBAUM, “Facial Recognition Technology”, 3. [↑](#footnote-ref-702)
703. T. HUANG, Z. XIONG, Z. ZHANG, “Chapter 16: Face Recognition Applications”, in S. Z. LI, A. K. JAIN, *Handbook of Face Recognition*, Springer, New York, 2005, 375-376. [↑](#footnote-ref-703)
704. Diensthoofd ICT bij PZ Gent. [↑](#footnote-ref-704)
705. Ibid 703, 375. [↑](#footnote-ref-705)
706. In het geval van *Big Brother Watch/Verenigd Koninkrijk* was sprake van de willekeurige verzameling van communicatie en van gerelateerde communicatiedata in bulk door National Security Agencies van de Verenigde Staten voor de Amerikaanse PRISM en UPSTREAM programma’s. Voor een uiteenzetting over deze zaak: X, “Big brother may continue watching you”, *Strasbourg Observers,* 2018. [↑](#footnote-ref-706)
707. art. 6 EVRM. [↑](#footnote-ref-707)
708. art. 6 lid 2 EVRM; art. 48 HEU. [↑](#footnote-ref-708)
709. Ibid 716, EDRi, “Ban Biometric Mass Surveillance”, 21. [↑](#footnote-ref-709)
710. art. 28 bis Sv.; Ibid 650, F. GOOSSENS, 16. [↑](#footnote-ref-710)
711. Dit is natuurlijk enkel zo als aan alle waarborgen voor het vermoeden van onschuld is voldaan: zie EHRM, 6 december 1988, nr. 10590/83, Barberà, Messegué en Jabardo/ Spanje, §77. [↑](#footnote-ref-711)
712. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 20. [↑](#footnote-ref-712)
713. EHRM, 20 maart 2001, nr. 33501/96, Telfner/Oostenrijk, §13-15. [↑](#footnote-ref-713)
714. RvE, “Factsheet on Mass Surveillance”, *RvE,* 2018, 1. [↑](#footnote-ref-714)
715. Ibid 709. [↑](#footnote-ref-715)
716. Ibid 700, VAN BRAKEL, 142. [↑](#footnote-ref-716)
717. Ibid 666, *Tele2Sverige,* §101. [↑](#footnote-ref-717)
718. Ibid 666, *Tele2Sverige*, Titel III, A), B), §101. [↑](#footnote-ref-718)
719. P. FUSSEY, D. MURRAY, “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Technology”, *The Human Rights, Big Data and Technology Project,* 2019, 36 e.v. [↑](#footnote-ref-719)
720. Ibid 718, 36-37. [↑](#footnote-ref-720)
721. Zie deel XI, 1). [↑](#footnote-ref-721)
722. Ibid 719, 38. [↑](#footnote-ref-722)
723. art. 21 HEU; Ibid 71, 20-23, 40. [↑](#footnote-ref-723)
724. Ibid 700, 142. [↑](#footnote-ref-724)
725. M. BURGESS, “Facial Recognition Tech used by UK police is making a ton of mistakes”, *Wired,* 2018; <https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>; Ella Jakubowska, Policy and Campaigns Officer bij EDRi zegt hierover: *“Added in this part about arbitrarily targeting, because we wanted to make sure that it’s clear that indiscriminate doesn’t mean that it’s not discriminatory. You know, these technologies could be deployed against a black community for example, and it would still be biometric mass surveillance. So a good example of that is the London Metropolitan Police a few years ago deployed live facial recognition at the Nottinghil Carnival, which is a famous celebration of black, African, carribean culture in London and that was very much…the fact that they chose that black community event as the place to try all these very invasive technologies was kind of both indiscriminate and arbitrarily targeted in the sense that it was scanning everyone that was attending the carnival, but it was also targeted against the black community in London.”* [↑](#footnote-ref-725)
726. Ibid 716, EDRi, “Ban Biometric Mass Surveillance”, 13. [↑](#footnote-ref-726)
727. FRA, Rapport van European Union Agency on Fundamental Rights, “Facial recognition technology: fundamental rights considerations in the context of law enforcement”, *FRA Focus* 2019, 13. [↑](#footnote-ref-727)
728. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, 17. [↑](#footnote-ref-728)
729. Ibid 575, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA- CONVENTION 108*, “*Guidelines on Facial Recognition”, 15. [↑](#footnote-ref-729)
730. Verschillende internationale instanties schreven reeds ethische richtlijnen rond het gebruik van artificiële intelligentie in het algemeen: AI HLEG, “Ethics Guidelines for Trustworthy AI”, *AI HLEG,* 2018; CAHAI van de Raad van Europa schreef verschillende studies en richtlijnen rond AI Ethics: <https://www.coe.int/en/web/artificial-intelligence/cahai>. [↑](#footnote-ref-730)
731. Zie bijvoorbeeld: I. D. RAIJI, T. GEBRU, M. MITCHELL, J. BUOLAMWINI, e.a., “Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing”, *AIES’ 2020: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society,* 2020. [↑](#footnote-ref-731)
732. M. HICKOK, ”Lessons learned from AI ethics principles for future actions”, *AI and Ethics* 2020; <https://link.springer.com/article/10.1007/s43681-020-00008-1?fbclid=IwAR2B_GFLBvN_R8RLem4uV7oF2DvbPSan019_sjPSXgeMz3QKLsolqk9wqc8>. [↑](#footnote-ref-732)
733. Gewoon hoogleraar aan KULeuven in de ingenieurswetenschappen. [↑](#footnote-ref-733)
734. Voor een overzicht van ethische en andere problematieken rond de ontwikkeling van en het onderzoek naar AI, zie interview met Yves Moreau, Gewoon hoogleraar aan KULeuven in de ingenieurswetenschappen. Drie uur luisterplezier gegarandeerd. [↑](#footnote-ref-734)
735. art. 2, 4°, art. 4, art. 10 Wet van 7 mei 2014 inzake experimenten op de menselijke persoon, *BS,* 18 mei 2014; Voor een overzicht van de wettelijke voorwaarden rond klinische experimenten op mensen: <https://www.famhp.be/en/human_use/medicines/medicines/research_development/ethic_committee>; Voor een uiteenzetting van de plichten van een ethische commissie: L. GELLING, “Role of the research ethics committee”, *Nurse Education Today,* 1999; <https://pubmed.ncbi.nlm.nih.gov/10808899/>*.* [↑](#footnote-ref-735)
736. N. MARTINEZ-MARTIN, “What are important ethical implications of using facial recognition technology in health care?”, *AMA Journal of Ethics,* 2019; <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6634990/>*.* [↑](#footnote-ref-736)
737. LONDON POLICING ETHICS PANEL, “Final Report on Live Facial Recognition”, in opdracht van de Mayor of London, 2019. [↑](#footnote-ref-737)
738. Ibid 737, 6-7. [↑](#footnote-ref-738)
739. Ibid 737, 30 e.v. [↑](#footnote-ref-739)
740. P. FUSSEY, D. MURRAY, “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Technology”, *The Human Rights, Big Data and Technology Project,* 2019, 6. [↑](#footnote-ref-740)
741. Ibid 740, 6. [↑](#footnote-ref-741)
742. I. D. RAJI, G. FRIED, “About Face: a survey of Facial Recognition Evaluation”, 2021, 7; <https://www.researchgate.net/publication/348958353_About_Face_A_Survey_of_Facial_Recognition_Evaluation>. [↑](#footnote-ref-742)
743. EUROPEES COMITE VAN DE REGIO’S, “Using the Quadruple Helix Approach to Accelerate the Transfer of Research and Innovation Results to Regional Growth”, *EU,* 2016, 13. [↑](#footnote-ref-743)
744. Ibid 740*,* 2019. [↑](#footnote-ref-744)
745. A. CEYHAN, “Analyser la sécurité: Dillon, Waever, Williams et les autres”, *Cultures & Conflits,* 1998, §6. De meetbaarheid van veiligheid valt bovendien uiteen in de subjectieve meetbaarheid en de objectieve meetbaarheid. G. VANDERVEEN, S. PLEYSIER, W. RODENHUIS, “Meten van onveiligheid”, in W. RODENHUIS, *Basisboek Integrale Veiligheid,* Boom Uitgevers, Den Haag, 2011, 91. [↑](#footnote-ref-745)
746. Ibid 693, MELGAÇO, 44. [↑](#footnote-ref-746)
747. D. VANMELDERT, “Steeds meer camera’s in het straatbeeld: “Ze voorkomen criminaliteit niet, de samenleving wordt er niet beter van”, *Vrt Nws,* 25 maart 2021;[https://www.vrt.be/vrtnws/nl/2021/03/23/privacyen-ik-camerasurveillance/](https://www.vrt.be/vrtnws/nl/2021/03/23/privacy-en-ik-camerasurveillance/); Ibid 746. [↑](#footnote-ref-747)
748. Zie hoger: Deel VI, 3, werkwijze. [↑](#footnote-ref-748)
749. De voorwaarden voor de uitoefening van de rechten van betrokkenen mbt camerabeelden is voorzien in art. 25/7 Wet op het Politieambt en art. 12 Camerawet. [↑](#footnote-ref-749)
750. L. MELGAÇO, “Meer camera’s, meer veiligheid? Een analyse over de doeltreffendheid van videosurveillance”, *Orde van de Dag,* 2015, 44. [↑](#footnote-ref-750)
751. Ibid 155, EDPS, “Guidelines on assessing the proportionality”, 2019, [↑](#footnote-ref-751)
752. Ibid 737. [↑](#footnote-ref-752)
753. De EDPS biedt een mooi overzicht van de bestaande criteria voor een proportionaliteitsbeoordeling uit de rechtspraak van de Europese hoven. [↑](#footnote-ref-753)
754. Allen een laatste keer geraadpleegd op 16 mei 2021. [↑](#footnote-ref-754)