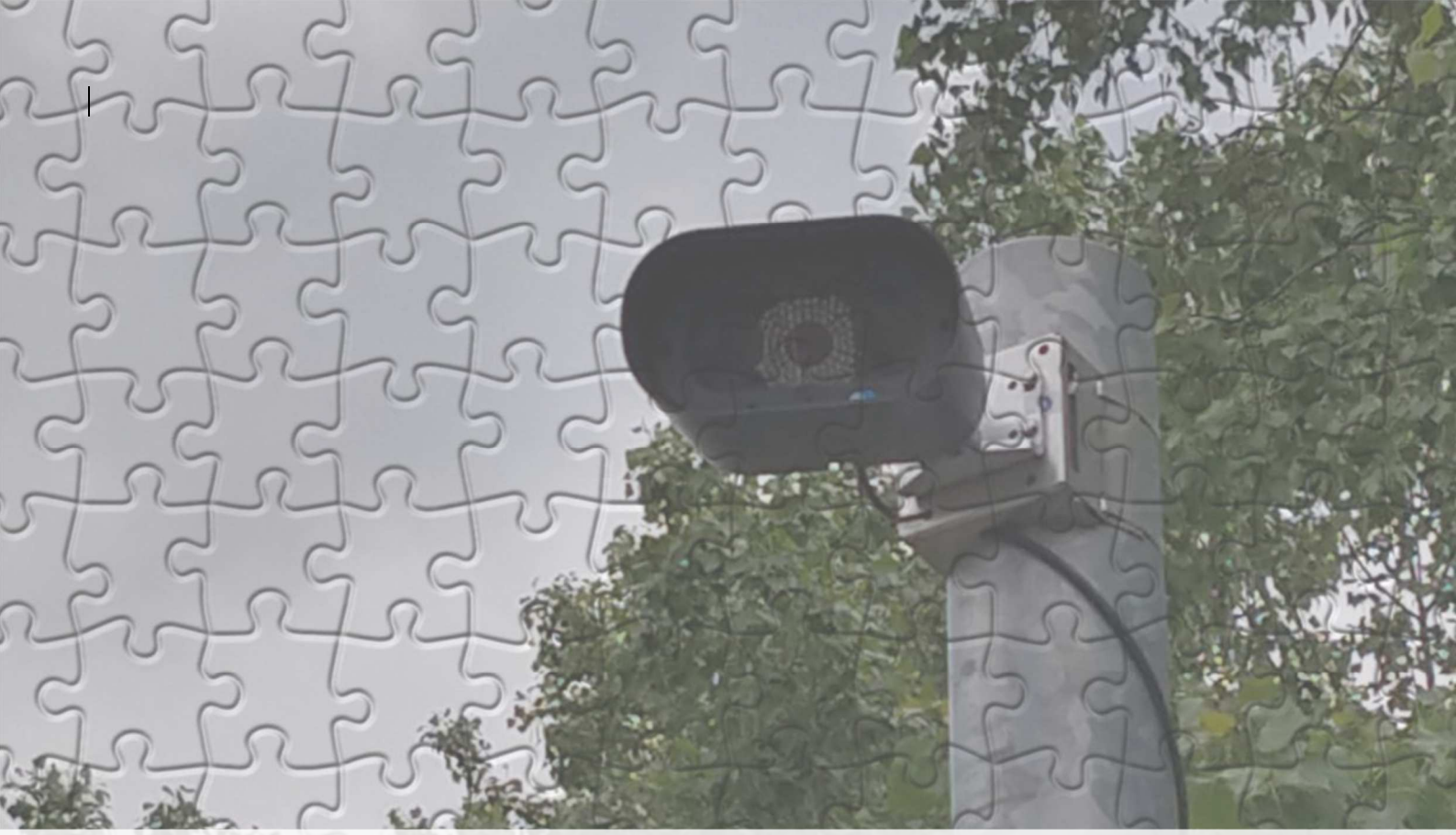


Rapport nr. 2020-02-NL

Omgevingsanalyse en knelpuntennota rond de ontwikkeling van een toegankelijk ANPR-data platform voor lokale besturen

VAS institute
crowell moring
AGENTSCHAP INNOVEREN & ONDERNEMEN
stad TURNHOUT
Stad KORTRIJK
MECHELEN

Omgevingsanalyse en knelpuntennota rond de ontwikkeling van een toegankelijk ANPR-data platform voor lokale besturen

Rapport nr. 2020-02-NL
Auteurs: Dormaels Arne, Verwee Isabel, Nieuwkamp Ricardo, Van Remoortel Frederik, Jamaels Evelien
Verantwoordelijke uitgever: Genoe Karin
Uitgever: Vias institute – Dept. Veiligheid en Preventie
Publicatiedatum: 24/04/2020
Wettelijk depot: D/2020/0779/11
Gelieve naar dit document te verwijzen als volgt: Dormaels Arne, Verwee Isabel, Nieuwkamp Ricardo, Van Remoortel Frederik, Jamaels Evelien, Omgevingsanalyse en knelpuntennota rond de ontwikkeling van een toegankelijk ANPR-data platform voor lokale besturen , Brussel, België: Vias institute – Dept. Veiligheid en Preventie

Inhoudsopgave

1 Executive summary

Steden en gemeenten die aan de slag willen gaan met Automatic Number Plate Recognition (ANPR)-camera's, om bijvoorbeeld het concept van een *smart city* te implementeren of diensten willen aanbieden voor hun burgers en bezoekers, botsen op verschillende uitdagingen: juridische onduidelijkheid, de (al dan niet) interoperabiliteit van systemen en tot slot onduidelijkheid over de inplanting en eigenaarschap van ANPR-camera's.

In dit project werden verschillende onderzoeksvragen bestudeerd door middel van twee analyses: een omgevings- en technische analyse en een juridische analyse. In deze analyses staan drie thema's centraal: 1) welke actoren zijn er vandaag betrokken in het ANPR-netwerk en hoe verhouden zij zich ten opzichte van elkaar?; 2) hoe zit het juridisch kader in elkaar en wat zijn juridische vereisten om een datadeling mogelijk te maken met lokale overheden? en; 3) welke technische vereisten zijn er nodig om ANPR-data te delen met derden?

Om een antwoord te bieden op deze onderzoeksvragen werden twee methodes gehanteerd: enerzijds werden de antwoorden uit een online survey geanalyseerd – een kwantitatieve methode – en anderzijds vonden diepgaande interviews plaats – de kwalitatieve methode. De online survey werd verstuurd naar Vlaamse politiezones, Vlaamse Steden en Gemeenten, enkele havens en parkings. De antwoorden van 139 respondenten werden gebruikt voor analyse. De kwalitatieve analyse bestaat uit 18 interviews die werden afgenomen bij een diversiteit aan actoren die betrokken zijn in het ANPR-verhaal/landschap.

Er zijn veel actoren betrokken in het ANPR-verhaal: (cf supra), onder andere:

- opdrachtgevers (zoals de lokale of federale politie, Agentschap Wegen en Verkeer (AWV));
- leveranciers van de camera's (bv. Macq, Tattile, Jenoptik);
- telecomoperatoren (Proximus, Telenet Business);
- beheersoftware van de camera's (bv. Macq, Myriade);
- datacenters (Communicatie en Informatiecentra (CIC), Directie van de politionele Informatie (DRI));
- Informatie Vlaanderen;
- toezichtsorganen (bv. Gegevensbeschermingsautoriteit (GBA), Vlaamse Toezicht commissie (VTC), Controleorgaan voor politioneel Informatiebeheer (COC)).

Het groot aantal actoren wijst op een bepaalde mate van complexiteit. Verschillende organisaties kunnen de opdracht geven om een ANPR-portaal te laten plaatsen, voor een specifieke finaliteit. Zo kan een lokaal bestuur bijvoorbeeld beslissen op een ANPR-portaal te installeren met het oog op criminaliteitsbestrijding maar bijvoorbeeld ook met het oog op het handhaven van een lage emissiezone. Een laag van complexiteit wordt toegevoegd door het aanbod van ANPR-camera's van verschillende merken met verschillende bijbehorende software. Voorts, kan men ervoor kiezen om de data afkomstig van deze camera's op te slaan op een lokale, gewestelijke, provinciale of een federale server als backoffice.

In België inspireerde de aankoop van ANPR-camera's tussen 2003 en 2006 door een paar lokale politiezones andere lokale politiezones om hier gebruik van te maken (Easton, 2019). Veel lokale politiezones beschikken vandaag dan ook over een eigen ANPR-cameranetwerk (Simons, 2014). De lokale zones en/of het lokaal bestuur is doorgaans de eigenaar en de data staan op de lokale backoffice.

Meer en meer inspanningen worden gedaan om boven aangehaalde complexiteit te stroomlijnen. Dit stroomlijnen gebeurt door het opzetten van raamcontracten en/of openbare aanbestedingen evenals het uitwerken van een geïntegreerde visie voor een geïntegreerde politie. Het geloof dat de dader niet stopt aan de grens van een gemeente of politiezone enerzijds en de nood om politionele datadeling efficiënt en effectief te structureren op een centraal niveau anderzijds bekrachtigt het belang van een geïntegreerde visie. Deze visie kwam er onder meer door de vaststelling dat het ANPR-netwerk versnipperd is over België wat de regering na de aanslagen van Parijs in 2015 noopte tot het opzetten van één nationaal ANPR-netwerk (Billiet & Colenbie, 2017). De opzet van dit nationaal netwerk gebeurt in twee fases: in de eerste fase plaatst de federale politie eigen camera's op grensovergangen en autosnelwegen. De tweede fase wordt momenteel uitgerold, namelijk de implementatie van één

nationale backoffice waarop alle door de politie gebruikte ANPR-camera's of voor politie bruikbare camera's worden geconnecteerd. Het databeheer systeem of het ANPR Managed Services (AMS) is de centrale backoffice van de federale politie.

Belangrijk en cruciaal is dat artikel 44/11/3sexies §2 Wet op het Politieambt bepaalt dat alle ANPR-data die worden verzameld (ongeacht wie de eigenaar is), worden hergebruikt voor politionele doeleinden en doorgestuurd worden naar het AMS. Dit maakt een nationale datadeling mogelijk voor politionele doeleinden en impliceert dat een lokale politiezone ANPR-data kan vragen bij de federale politie.

Op basis van de kwalitatieve interviews werd informatie verzameld over deze vorm van politionele datadeling. De meerwaarde van de ontwikkeling van het AMS situeert zich op meerdere niveaus. Zo is vooreerst het stroomlijnen cruciaal binnen een context van informatie gestuurde politiezorg. Een centrale actor die lokale, bovenlokale, nationale en internationale data-uitwisseling mogelijk maakt is cruciaal. De opslagtermijn van ANPR-data bij de federale politie wordt als een belangrijke meerwaarde beschouwd. De federale politie houdt de data 12 maanden bij terwijl dit bij de lokale politie één maand is. De federale backoffice is schaalbaar, flexibel, kan meegroeien met nieuwe gebruikers en nieuwe aansluitingen van camera's. Er rijzen echter ook wel technische bekommernissen. De grootste bekommernis is dat het vandaag moeilijk is om de lokale backoffices te verbinden met de federale backoffice. Het feit dat het federale platform niet volledig operationeel is, stuit op kritiek en is geen evidentie als een lokaal bestuur investeerde of wenst te investeren in de integratie met het federale platform. Lokale besturen willen een *return on investment* maar als blijkt dat technische beperkingen in de weg zitten, komt dit de geloofwaardigheid niet ten goede. Behalve een technisch probleem is het bovendien wachten op ministeriële richtlijnen die bepalen hoe de politie met deze ANPR-data kan en mag werken.

De meerderheid van de bevraagde lokale zones prefereert daarenboven het behoud van een eigen lokale backoffice. De betaler speelt hier uiteraard een rol in. Het lokaal bestuur – vaak de betaler – verwacht transparantie en verantwoording over wat er met de ANPR-camera's gebeurt en hoe deze data worden aangewend, hoe efficiënt en effectief deze camera's zijn. Behalve het gegeven dat dit "*al van oudsher*" wordt gebruikt, is de snelle en accurate data die men ter beschikking heeft een toegevoegde waarde. Het gebruik van een lokale backoffice biedt bovendien fijnmazigheid, wat toelaat om beleidsmatig de politiediensten aan te sturen. De prioriteiten van de lokale politie zijn bovendien niet altijd dezelfde als deze van de federale politie. Een eigen systeem laat een eigen lokale monitoring toe om zowel de politiediensten aan te sturen op beleidsmatig niveau maar biedt evenzeer zicht op het gebruik van de databank: Wie logt in op welk moment? Welke informatie wordt opgezocht?

Drie vierde van de bevraagde respondenten via de online survey maakt gebruik van ANPR-camera's. Er heerst onduidelijkheid over het totaal aantal camera's: deze vaststelling geldt zowel bij aanvang als bij afsluiting van dit project. Dit geldt evenzeer voor de locaties van ANPR-camera's. Op de vraag wie eigenaar is van de ANPR-camera's zijn de frequentst aangeduide eigenaars de politiezone (56,3%), het lokaal bestuur (20,7%) en het Vlaams Gewest (16,3%). De politie staat meestal in voor de coördinatie ervan. Het hebben van een eigen ANPR-cameranetwerk impliceert niet (meer) automatisch dat de data enkel (eigendom) van deze entiteit is. Door artikel 44/11/3sexies §2 Wet op het Politieambt worden lokale politiezones verplicht data door te sturen naar het federale AMS, wat geen uniek eigenaarschap meer impliceert.

Zes op tien respondenten maakt structureel gebruikt van ANPR-data en vijf op tien respondenten maakt er eerder sporadisch gebruik van. Niet-anonieme ANPR-data worden frequenter gebruikt (44,7%) in vergelijking met anonieme ANPR-data (19,7%). Bijna twee op de drie (63,2%) respondenten maakt gebruik van beeldmateriaal en minder dan één op vier (23,7%) van de respondenten maakt gebruik van afgeleide data. Het vaakst wordt criminaliteitsbestrijding (50,0%) en verkeershandhaving (33,3%) als finaliteit genoemd. 52 respondenten delen informatie. ANPR-data worden voornamelijk gedeeld met federale politie (28,3%), andere politiezone (25,8%), eigen politiezone (21,7%) of eigen organisatie (11,7%). Van deze 52 respondenten, gebruikt 34,7% een protocol, 65,3% gebruikt geen protocol (soms via een andere modaliteit) om data te kunnen delen.

Het Vlaamse ANPR-netwerk wordt geconfronteerd met een ware versnippering waarbij zowel lokale als federale backoffices ANPR-data genereren. Deze versnippering wordt door sommige geïnterviewden geproblematiseerd en anderen beschouwen dit als niet-problematisch. Zo wensen veel zones een eigen

lokale backoffice te behouden. Het huidige versnipperde landschap is één van de belangrijkste redenen waarom een centralisering zich opdringt. De centralisering stelt allerhande instanties voor een diversiteit aan technische en juridische uitdagingen. Technische en juridische vereisten gaan hand in hand.

Een belangrijke technische vereiste om goede datadeling mogelijk te maken tussen allerhande politionele en niet-politionele actoren betreft een doordacht IT-securitybeleid. Het gegeven dat er een diversiteit is aan leveranciers, cameramerken, software, etc. wordt door veel respondenten in de interviews als weinig problematisch ervaren. Dit impliceert wel vaak een integratiekost. Alle door de politie gebruikte of voor politie bruikbare ANPR-camera's dienen data door te sturen naar het AMS. Dit betekent dat alle lokale backoffices verbonden worden met het AMS. De geïnterviewden halen voor wat betreft dit onderwerp behoorlijk wat technische vereisten aan:

- Het AMS dient flexibel te zijn;
- Het AMS moet bereid zijn om verschillende systemen hierop toe te laten;
- Het AMS dient voldoende voorbereid te zijn;
- Om alle door de politie bruikbare of politie gebruikte ANPR-camera's aan te sluiten, zijn er resources nodig;
- De meeste data komt real time binnen op het AMS, wat een performant systeem noodzaakt met veel opslagcapaciteit. Aangaande opslagcapaciteit wordt er een onderscheid gemaakt tussen: Opslag en verwerking van data;
- De processorcapaciteit moet voldoende krachtig zijn;
- Er moet voldoende kennis en *know how* zijn voor het lezen, het bepalen van de foutenmarge…;
- Het AMS moet beschikken over goede gebruiks- en gebruikersregels (bijvoorbeeld hoeveel mensen kunnen tegelijkertijd opzoekingen doen in het systeem, hoeveel gegevens kan men maximaal opzoeken…);
- Data moet real time van de lokale politie naar de federale politie gaan en vice versa;
- Aangaande de controle: Moet een surveillance- en controlefunctie uitgewerkt worden die bepaalt wie de toegang krijgt en wie niet? De data over wie inlogt op welk moment op welk systeem moet de lokale politie ter beschikking worden gesteld voor beleids- als integriteitsdoeleinden.

Eén van de kernvragen van dit project is: mocht er ontsluiting van ANPR-data zijn met lokale overheden, wat de technische vereisten hiertoe zijn? Op basis van de antwoorden in sommige interviews blijkt dat reeds data worden gedeeld met de lokale overheden, in het kader van bijvoorbeeld lage emissiezones (LEZ) of autoluwe zones. De data worden vaak van de politionele backoffice geanonimiseerd en doorgestuurd naar de lokale overheden. Bij LEZ speelt Informatie Vlaanderen een specifieke rol in enkele steden: zo koppelen zij ANPR-data aan DIV-gegevens (zij hebben hiervoor een decretale machtiging). Andere lokale entiteiten delen geen data maar stellen doorgaans dat er weinig belemmeringen zijn om te delen. Zo blijkt uit één van de interviews dat: "*Het is niet omdat iets technisch kan, dat het juridisch ook kan en mag*", en vormt een belangrijke rode draad doorheen dit project. De finaliteit waarvoor deze data aangewend worden en door wie ze worden gebruikt, is en blijft een belangrijke premisse.

Het depersonaliseren van ANPR-data is een belangrijke vereiste alvorens deze gedeeld kunnen worden met lokale overheden. ANPR-data zijn immers politionele data die niet ter beschikking kunnen gesteld worden van andere doeleinden dan politionele. De politie is dé instantie die volgens meerdere bevraagden instaat voor het depersonaliseren van de ANPR-data. Vanuit juridisch oogpunt wordt anonimisering boven pseudonimisering verkozen, omdat er bij anonieme data geen enkele link is naar de identificatiegegevens van het voertuig. Echter, om anonieme data te delen met lokale overheden moeten die uit het politioneel netwerk worden gehaald. Een piste die bij menig respondent op bijval rekent, is dat de gewesten een centrale rol krijgen toebedeeld in dit verhaal. De federale politie – die toch alle data verzamelen in het AMS – kan anonieme data doorsturen naar Informatie Vlaanderen dat op zijn beurt instaat voor de dispatching van anonieme gegevens naar de geïnteresseerde lokale overheden. Anonieme ANPR-data staan als het ware ter beschikking op een centraal platform, wat een uniforme datadeling mogelijk maakt. Volgens meerdere respondenten is Informatie Vlaanderen het

best geplaatst voor deze dispatching. De meest cruciale technische vereiste is uiteraard dat alle lokale backoffices geconnecteerd staan met het AMS.

De relevante wetgeving, zijnde (i) de GDPR en de Belgische uitvoeringswet (ii) de Camerawet, en (iii) de wet op het politieambt (WPA), vormt een strikt wettelijk kader omtrent het gebruik van ANPR-camera's en het gebruik en delen van ANPR-data. Het vandaag bestaand wettelijk kader laat geen ontsluiting toe van politionele gegevens, met inbegrip van ANPR-gegevens, naar niet-politionele overheden/instanties voor niet-politionele/justitiële doeleinden. Er bestaat dus geen wettelijke grondslag voor het ontsluiten van ANPR-data aan lokale besturen voor algemene beleidsdoeleinden zoals mobiliteit, milieu, klimaat, leefbaarheid, etc.

Teneinde die wettelijke basis te voorzien, lijkt de meest aangewezen optie een wijziging van de WPA, en in het bijzonder aanvulling van het huidig artikel 44/11/9 WPA.

Artikel 44/11/9 WPA zou zodanig kunnen uitgebreid worden dat de openbare overheden (waarvan reeds sprake in de huidige versie van artikel 44/11/9 en waaronder dus ook steden en gemeenten vallen) niet louter met betrekking tot hun opdrachten van toepassing van de strafwet of wettelijke verplichtingen inzake de openbare veiligheid, maar ook met betrekking tot mobiliteit-, milieu-, leefbaarheidsbeleid, etc. toegang kunnen krijgen tot de gegevens in de zin van de WPA.

Vanuit juridisch oogpunt is het ons inziens meest werkbare kader voor het delen van ANPR-data met lokale besturen, in de zin van een op die wijze gewijzigd artikel 44/11/9 WAP, te werken met een centraal systeem (en niet met decentrale systemen).

Als men ervan uitgaat dat één centraal systeem zou bestaan met ANPR-gegevens dat geconsulteerd kan worden door de lokale besturen, dan stelt zich nog de vraag hoe een lokaal bestuur dan aan de gegevens kan die het nodig heeft om een bepaald project te realiseren? Een suggestie is het oprichten (via een uitvoeringsbesluit van de WPA (gewijzigd artikel 44/11/9)) van een kruispuntbank die instaat voor (i) het anonimiseren/pseudonimiseren van de ANPR-data en (ii) het verdelen van de gegevens aan de lokale besturen conform de wettelijk bepaalde doeleinden.

Uiteraard blijft de GDPR en de Belgische uitvoeringswet van toepassing telkens wanneer persoonsgegevens verwerkt worden voor die aangelegenheden die niet door bijzondere wetgeving worden geregeld. Het opzetten van een kruispuntbank of enige ander initiatief wijzigt de verplichtingen van lokale besturen op dat vlak niet. Dit betekent dat de verwerking van de gegevens (minstens de gepseudonomiseerde gegevens, aangezien de GDPR niet van toepassing is op louter anonieme gegevens) moet plaatsvinden conform de basisprincipes van de GDPR. Elke verwerking moet proportioneel zijn, de verwerkingsverantwoordelijke (lokaal bestuur) moet transparant zijn, etc. Bovendien moet een lokaal bestuur nog steeds, indien zij meent dat een verwerking een hoog risico inhoudt voor de vrijheden van natuurlijke personen, een DPIA (Gegevensbeschermingseffectbeoordeling) uitvoeren voorafgaand aan de verwerking van de gegevens, wat evenwel ook kan worden opgenomen in bijzondere wetgeving.

2 Omgevingsanalyse en knelpuntennota

2.1 Context

De toenemende informatie- en communicatietechnologie transformeerde traditionele methodes van stedelijk management en infrastructuurplanning de laatste twee decennia (Havadi, Buldeo Rai, Verlinde, Huang, Macharis, Guns, 2018). Om dagelijkse operaties te monitoren, wenst men meer gebruik te maken van real time data en analyses, zoals bijvoorbeeld de bewegingen van voertuigen in steden om verkeer te monitoren en de verkeerslichten en snelheidslimieten hierop in te stellen (Dodge & Kitchin, 2007). Heel veel bronnen van informatie kunnen hiervoor gebruikt worden en dit is evenzeer het geval voor Automatic Number Plate Recognition (ANPR-)data.

Steden en gemeenten die aan de slag willen gaan met ANPR-camera's – of de data hiervan - om bijvoorbeeld het concept van een *smart city* te implementeren of diensten willen aanbieden voor hun burgers en bezoekers botsen op verschillende uitdagingen: juridische onduidelijkheid, de (al dan niet) interoperabiliteit van systemen en onduidelijkheid over de inplanting en eigenaarschap van ANPR-camera's.

2.2 Onderzoeksvragen

In dit project werden verschillende onderzoeksvragen bestudeerd door middel van twee analyses: een omgevings- en technische analyse en een juridische analyse.

In deze analyses stonden drie thema's centraal: 1) welke actoren zijn er vandaag betrokken in het ANPR-netwerk en hoe verhouden zij zich ten opzichte van elkaar?; 2) hoe zit het juridisch kader in elkaar en wat zijn juridische vereisten om een datadeling mogelijk te maken met lokale overheden? en; 3) welke technische vereisten zijn er nodig om ANPR-data te delen met derden?

2.3 Methodologie

Om een antwoord te bieden op bovenstaande onderzoeksvragen werden twee (belangrijke) methodes gehanteerd: enerzijds werd een online survey opgemaakt – een kwantitatieve survey – en anderzijds vonden diepgaande interviews plaats – de kwalitatieve interviews.

Door middel van een online vragenlijst die werd verstuurd naar Vlaamse politiezones, Vlaamse Steden en Gemeenten, enkele havens en parkings, werd informatie digitaal opgevraagd en geanalyseerd. De online survey leverde een respons op van 139 ingevulde vragenlijsten die bruikbaar waren voor de analyse. De vragenlijsten werden in hoofdzaak ingevuld ofwel door een gemeente of stad (n = 66) of door een politiezone (n = 65). De overige vragenlijsten werden ingevuld door een haven (n = 7) en een treinstation (n = 1). De meerderheid van de politiezones betreft meergemeentezones (78,5%) ten opzichte van 21,5% ééngemeentezones. De respons van de politiezone ten opzichte van het totaal aangeschreven Vlaamse politiezones is vrij hoog, namelijk 60,7%.

De kwalitatieve analyse bestaat uit 18 interviews die werden afgenomen bij een diversiteit aan actoren die betrokken zijn in het ANPR-verhaal, zoals onder meer lokale en federale politie, Informatie Vlaanderen, Viapass, Dienst Inschrijving Voertuigen (DIV), netwerkproviders, leveranciers van camera's... Daarnaast werden toezicht- en controleorganen geïnterviewd zoals de Gegevensbeschermingsautoriteit (GBA), Vlaamse Toezicht commissie (VTC), Controleorgaan voor politioneel informatiebeheer (COC)... Van sommige organisaties kregen wij een schriftelijk antwoord op de door ons gestelde vragen in het interview.

Het rapport beschrijft de resultaten van de kwantitatieve survey en de kwalitatieve interviews. Bij de beschrijvende onderzoeksresultaten van de kwalitatieve interviews wordt er een onderscheid gemaakt tussen de actoren, de frequent aangehaalde thema's door de respondenten en de technische vereisten. Er wordt een apart luik beschreven met de juridische analyse.

De belangrijkste onderzoeksresultaten worden navolgend samengevat en de knelpunten worden aangehaald. De resultaten en de knelpunten lopen frequent door elkaar. Door middel van de kwantitatieve survey werden statistische data verzameld en door middel van diepgaande interviews werd kwalitatieve informatie verzameld. Beide vormen van dataverzameling genereren tevens specifieke resultaten als knelpunten.

2.4 Historiek

Enkele Belgische lokale politiezones raken begin 2000 geïnspireerd door de automatische nummerplaatherkenning toepassingen uit de UK. Ze kopen een ANPR-portaal aan en inspireren heel wat andere politiezones en autoriteiten (Easton, 2019). Het eerste politionele gebruik van ANPR-technologie in België situeert zich tussen 2003 en 2006.

In 2012 brengt het Agentschap Wegen en Verkeer (AWV) een raamcontract uit waarbij trajectcontrolecamera's, evenals andere camera's, kunnen aangekocht worden volgens een lokaal concept. De data van deze ANPR-camera's worden verzameld op een lokale backoffice die enerzijds instaat voor politionele toepassingen en anderzijds voor kandidaat-overtreders van trajectcontroles. Dit raamcontract liep eerst vier jaar en werd uiteindelijk verlengd tot vijf jaar.

Na het raamcontract van AWV, wordt er een opvolgcontract uitgeschreven door de federale politie. Dat deze materie bij de federale politie terechtkomt, komt door de aanslagen in Parijs in 2015. Men komt op dat moment tot de vaststelling dat er geen geïntegreerde visie is omtrent ANPR, evenals geen nationaal initiatief of centrale backoffice. De idee dat er heel wat niet-geïnterconnecteerde eilanden zijn, versnipperde provinciale initiatieven wordt sterk bekritiseerd evenals het gebrek aan federaal politioneel bruikbare ANPR-camera's. Dit leidde tot de ontwikkeling van één nationaal ANPR-netwerk (Billiet & Colenbie, 2017).

2.5 Veel actoren in een complexe puzzel

2.5.1 Inleiding

Er zijn bijzonder veel actoren betrokken in het ANPR-verhaal, meer bepaald opdrachtgevers (zoals de lokale of federale politie, Agentschap Wegen en Verkeer (AWV)), leveranciers (Macq, Tattile, Jenoptik, …), telecomoperatoren (Proximus, Telenet Business), beheersoftware (Macq, Myriade…), datacenters (Communicatie en InformatieCentra (CIC), Directie van de politionele Informatie (DRI)), Informatie Vlaanderen, toezichtsorganen zoals Gegevensbeschermingsautoriteit (GBA), Vlaamse Toezicht commissie (VTC), Controleorgaan voor politioneel Informatiebeheer (COC)… . Het aantal actoren dat betrokken is, is dus bijzonder groot, wat wijst op een bepaalde mate van complexiteit. Het maken van de puzzel is dus niet eenvoudig. Verschillende organisaties kunnen de opdracht geven om een ANPR-portaal te laten plaatsen, voor een specifieke finaliteit. Zo kan een lokaal bestuur bijvoorbeeld beslissen op een ANPR-portaal te installeren met het oog op criminaliteitsbestrijding maar bijvoorbeeld ook met het oog op het handhaven van een lage emissiezone. Een laag van complexiteit wordt toegevoegd door het aanbod van ANPR-camera's van verschillende merken met verschillende bijbehorende software. Voorts, kan men ervoor kiezen om de data afkomstig van deze camera's op te slaan op een lokale, gewestelijke, provinciale of een federale server als backoffice.

Meer en meer inspanningen worden gedaan om dit geheel te stroomlijnen. Dit stroomlijnen gebeurt door het opzetten van raamcontracten en/of openbare aanbestedingen evenals het uitwerken van een geïntegreerde visie voor een geïntegreerde politie. Het geloof dat de dader niet stopt aan de grens van een gemeente of politiezone enerzijds en de nood om politionele datadeling efficiënt en effectief te structureren op een centraal niveau anderzijds bekrachtigt het belang van een geïntegreerde visie. De informatie die ANPR-camera's immers genereert is bijzonder waardevol: "*Intelligente camera's (ANPR) zijn een ware jackpot aan informatie voor de politie. Als de mogelijkheid tot het gebruik van die kennis niet bij enkelen ligt, maar korps breed wordt uitgerold en overal gebruikt kan worden, is het volgens mij hét instrument voor de komende jaren*" (Crispel, 2020, p. 107).

2.5.2 Interesse alom

De aankoop van ANPR-camera's is inmiddels sterk ingeburgerd bij veel lokale politiezones, als instrument ter bestrijding van criminaliteit evenals voor verkeerscontrole. Het aankopen van een ANPR-portaal impliceert enerzijds keuzes maken en anderzijds een diversiteit van actoren betrekken.

Er is niet alleen veel politionele interesse in deze data maar meer en meer niet-politionele interesse, denk bijvoorbeeld aan lokale overheden, gewestelijke overheden, havenbedrijven, luchthavens, parkeerbedrijven, afvalintercommunales, kenniscentra... Terwijl het een geroutineerd gegeven is voor de lokale en federale politie, zijn veel (niet-politioneel) geïnteresseerden zoekende naar hoe zij ANPR-camera's en de data ervan kunnen aanwenden voor doeleinden van controle, mobiliteit, leefmilieu, stadsontwikkeling, kennisverzameling, …

De diversiteit aan actoren die betrokken zijn in deze puzzel maakt een optimaal gebruik van ANPR-data een complexe uitdaging. Dit doet allerlei vragen rijzen zoals: Wie is eigenaar van de camera's? Wie is eigenaar van de data? Wie beheert de data? Bij wie kan ik terecht als ik data wil krijgen? Wie doet wat? Er zijn bovendien talrijke onduidelijkheden op juridisch en technisch niveau: Kunnen data gedeeld worden? Binnen welke juridische context kunnen data gedeeld worden? Hoe dien ik een aanvraag in te dienen? Bij wie kan ik terecht? Wat zijn technische vereisten om data te delen?... Weinig mensen hebben een zicht op wat er kan en wat er mag inzake politionele en niet-politionele datadeling.

2.5.3 De federale politie

De vaststelling dat het ANPR-netwerk versnipperd is over België noopte de regering na de aanslagen van Parijs in 2015 tot het opzetten van één nationaal ANPR-netwerk. Dit is één van de 18 regeringsmaatregelen in de strijd tegen terrorisme.[1] De opzet van dit nationaal netwerk gebeurt in twee fases: in de eerste fase plaatst de federale politie eigen camera's op grensovergangen en autosnelwegen. Enkele ANPR-camera's van AWV die op de gewestwegen staan worden geïntegreerd in het nationale ANPR-netwerk, evenals de camera's van een aantal luchthavens.

De tweede fase wordt momenteel uitgerold, namelijk de implementatie van één nationale backoffice waarop alle door de politie gebruikte ANPR-camera's of voor politie bruikbare camera's worden geconnecteerd. Het databeheer systeem of het ANPR Managed Services (AMS) is de centrale backoffice van de federale politie. De lokale zones worden verplicht (artikel 44/11/3sexies §2 Wet op het Politieambt) om zich met hun reeds bestaande camera's aan te sluiten op het AMS. Zij kunnen daarnaast nieuwe camera's aankopen door middel van het federale raamcontract en zich direct aansluiten op het AMS.

De federale politie maakte een berekening van de door de politie gebruikte of bruikbare ANPR-camera's. Er werden in totaal 3.465 camera's geïdentificeerd die in aanmerking komen om zich te koppelen aan het AMS, waarvan er reeds 800 camera's gekoppeld zijn.

Het AMS stelt een aantal cruciale pijlers centraal: *"Optillen van de ANPR-technologie naar het nationale niveau om de samenleving nog beter te dienen, criminaliteit te voorkomen en de transparantie te verbeteren.*

De AMS zullen de bestaande systemen vervangen om:

- *De toegang tot de gegevens op een nationale schaal mogelijk te maken;*
- *de ANPR-functionaliteit te standaardiseren in heel het land;*
- *een beter datamanagement en een integratie met andere politietoepassingen op te zetten;*
- *een volledige transparantie te bieden;*
- *een gebruiksvriendelijke, veerkrachtige en « future proof » service te realiseren;*

[1] Zie: https://www.premier.be/nl/strijd-tegen-terrorisme-%E2%80%93-maatregelen-van-de-federale-regering-toespraak, geraadpleegd op 21 april 2020.

- *een toegang tot de ANPR-tools mogelijk te maken voor alle politie- en inlichtingendiensten;*
- *een samenwerking met bestuurlijke overheden op te zetten voor een beter mobiliteitsmanagement* "[AMS, presentatie Vias institute, 13/03/2020].

Belangrijk en cruciaal is dat artikel 44/11/3sexies §2 Wet op het Politieambt bepaalt dat alle ANPR-data die worden verzameld (ongeacht wie de eigenaar is) worden hergebruikt voor politionele doeleinden en doorgestuurd worden naar het AMS. Dit maakt een nationale datadeling mogelijk voor politionele doeleinden en impliceert dat een lokale politiezone ANPR-data kan vragen bij de federale politie.

Het AMS staat in nauwe verbinding met de gedeconcentreerde coördinatie- en steundirecties van de federale politie, meer bepaald met de Informatie en Communicatiecentra (CIC) van de Communicatie- en informatiedienst van het arrondissement (SICAD). Aan het hoofd van deze directies staat een directeur-coördinator die op bovenlokaal niveau de gebeurtenissen en initiatieven coördineert. Hij vormt de scharnierfunctie tussen de lokale en federale politie. Deze directie staat tevens in voor het beheer van het CIC. De CIC's worden uitgerust met werkstations die ANPR-data ontvangen. De CIC's staan in voor de verwerking van deze data en het optimaal delen ervan met politionele instanties. Een kritische bemerking aangehaald in de interviews is dat de federale politie geconfronteerd wordt met capaciteitsproblemen, evenals logistieke en huisvestingsproblemen. Indien deze werkstations optimaal dienen te functioneren en een datadeling mogelijk gemaakt wordt, dienen deze problemen ook idealiter te worden aangepakt.

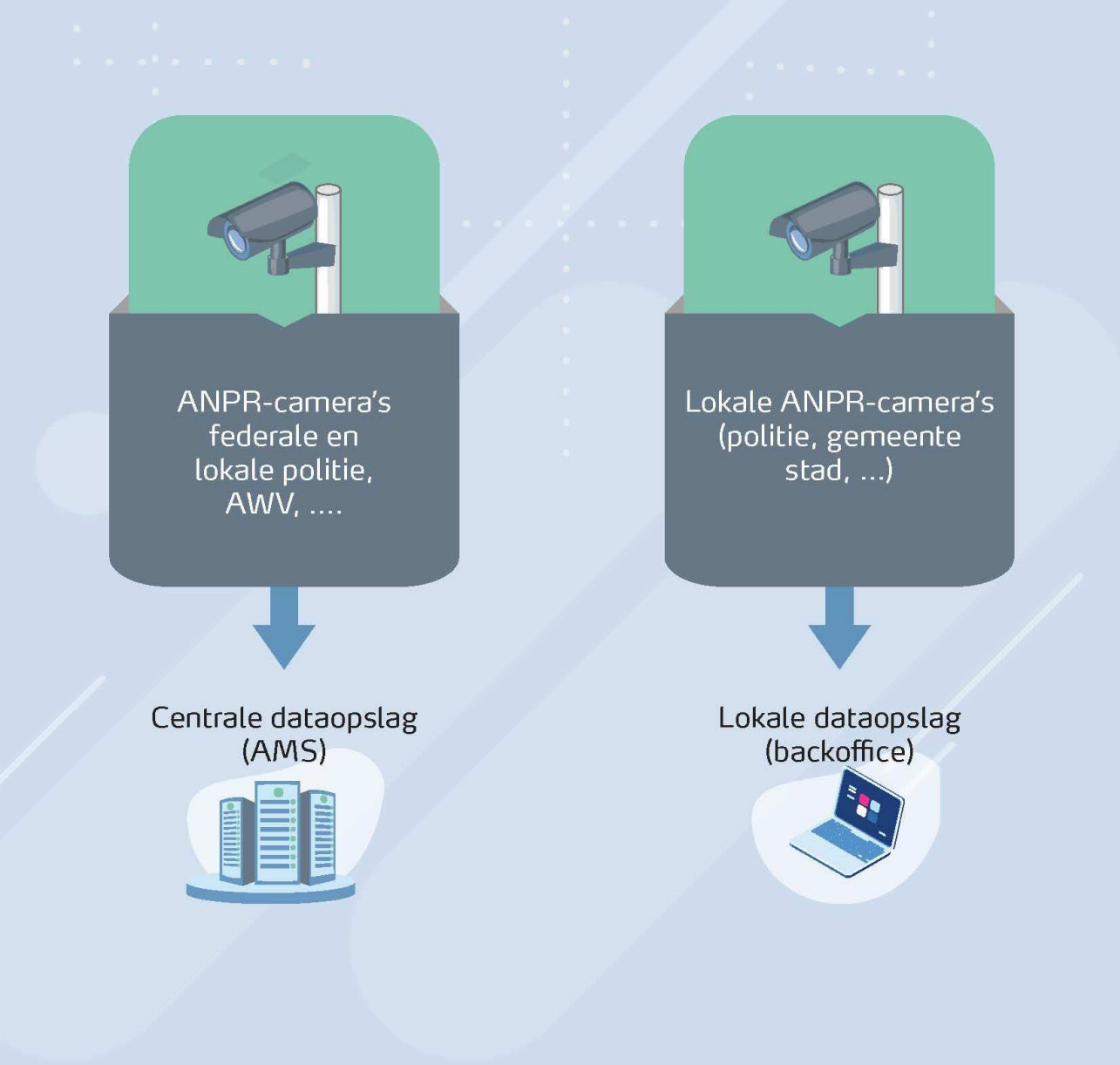
2.5.4 Lokale politie

De aankoop van ANPR-camera's tussen 2003 en 2006 door een paar lokale politiezones inspireerde andere lokale politiezones om hier gebruik van te maken. Veel lokale politiezones beschikken vandaag dan ook over een eigen ANPR-cameranetwerk (Simons, 2014). De lokale zones en/of het lokaal bestuur is doorgaans de eigenaar en de data staan op de lokale backoffice. De ANPR-data worden aangewend voor trajectcontroles, voor criminaliteitsbestrijding, in politioneel gerechtelijk onderzoek, en in enkele zones wordt er samengewerkt in het kader van de controles op lage emissiezone[2], autoluwe zone... Er zal straks ingezoomd worden op het gebruik en aantal ANPR-camera's, hoe de ANPR-data gebruikt worden en waarvoor deze gebruikt worden (cfr. finaliteit).

2.5.5 AS IS situatie

De actuele situatie (AS IS) wordt weergegeven in onderstaande figuur. Links van de figuur wordt de datastroom weergegeven waarbij de ANPR-data zowel komen van federale ANPR-camera's, AWV-camera's als lokale zones die zich aansluiten op het AMS. Deze data worden centraal opgeslagen in het AMS. In de figuur rechts worden de lokale ANPR-camera's van de politiezones, steden, gemeenten… visueel voorgesteld. De data van deze camera's worden doorgegeven aan de lokale backoffices.

[2] Zie: https://www.vlaanderen.be/lage-emissiezones-lez, geraadpleegd op 21 april 2020.



2.5.6 Lokale en federale politie: integratie op AMS

"Op dat moment is er geen centraal concept, geen nationaal initiatief of centrale backoffice en ontbreekt een integratievisie omtrent dit ANPR-gebeuren", is één van de grootste vaststellingen na de terreuraanslagen in Parijs in november 2015. Net deze vaststelling noopte de regering tot de ontwikkeling en implementatie van een nationaal ANPR-netwerk waarin de federale politie een geïntegreerde vorm van ANPR-datadeling mogelijk maakt.

Op basis van de kwalitatieve interviews werd veel informatie verzameld over deze politionele datadeling. Er worden navolgend zowel onderzoeksresultaten gepresenteerd, evenals kritische bemerkingen waarom het niet evident is als lokale politiezone om zich aan te sluiten op het AMS. Uiteraard wordt er door velen ook ingegaan op de meerwaarde waarbij de ontwikkeling van een nationaal ANPR-netwerk, zoals het AMS, gevolgen heeft op meerdere niveaus.

2.5.6.1 Meerwaarde van de integratie

Het gegeven dat politionele data versnipperd aanwezig zijn in het landschap genereert ook politionele consequenties. Zo wordt in eerste instantie de versnippering en de eilandvorming gehekeld, waardoor het cruciale karakter van informatiedeling wordt onderschreven. De criminaliteit stopt immers niet aan

de grens van een lokale politiezone of gemeente/stad waardoor het fundamenteel is om een gestroomlijnde ANPR-informatiedeling mogelijk te maken. Als informatie gestuurde politiezorg hoog in het vaandel wordt gedragen dan is dit stroomlijnen vanuit een nationaal AMS een belangrijke conditie. Deze centrale actor staat in voor de lokale, bovenlokale, nationale maar ook internationale data-uitwisseling.

De opslagtermijn van ANPR-data bij de federale politie wordt als een belangrijke meerwaarde beschouwd. De federale politie houdt de data 12 maanden bij, volgens artikel 25/6 WPA, terwijl dit bij de lokale politie één maand is.

De federale backoffice is schaalbaar, flexibel en kan meegroeien met nieuwe gebruikers, nieuwe aansluitingen van camera's…. Het federale raamcontract werd opgemaakt zodat de diversiteit aan camera's, software… gestroomlijnd werd zodat alles geïntegreerd en uniform in het AMS terechtkomt. De informatie van oude camera's moet uiteraard geïntegreerd kunnen worden in de nationale backoffice. Dit raamcontract biedt met andere woorden een bepaalde garantie dat de verschillende systemen afgestemd kunnen worden op het AMS.

2.5.6.2 Geen evidente integratie

De wettelijke verplichting om de lokale data door te sturen naar de federale backoffice wordt door velen beschouwd als een meerwaarde maar er rijzen wel wat technische bekommernissen. De grootste bekommernis is dat het vandaag moeilijk is om de lokale backoffices te verbinden met de federale backoffice. Het feit dat het federale platform niet volledig operationeel is, stuit op kritiek en is geen evidentie als een lokaal bestuur investeerde of wenst te investeren in de integratie met het federale platform. Lokale besturen willen een *return on investment* maar als blijkt dat technische beperkingen in de weg zitten, komt dit de geloofwaardigheid niet ten goede. Naast een technisch probleem is het bovendien wachten op ministeriële richtlijnen die bepalen hoe de politie met deze ANPR-data kan en mag werken.

In volgende instantie prefereert de meerderheid van de bevraagde lokale zones het behoud van een eigen lokale backoffice. De betaler speelt hier uiteraard een rol in. Het lokaal bestuur – vaak de betaler – verwacht transparantie en verantwoording over wat er met de ANPR-camera's gebeurt en hoe deze data worden aangewend, hoe efficiënt en effectief deze camera's zijn…. Met andere woorden, zij investeren en willen hiervoor een *return on investment*.

Een andere reden waarom lokale zones een eigen backoffice prefereren is van historische aard, bijvoorbeeld omdat "*er al van oudsher*" op deze wijze gewerkt wordt. Een meer fundamentele reden dan de historische is de snelle en accurate data die men ter beschikking heeft. Het gebruik van een lokale backoffice biedt bovendien fijnmazigheid, wat toelaat om beleidsmatig de politiediensten aan te sturen. Sommige politiezones maken gebruik van lokale lijsten die geverifieerd worden met ANPR-data. Deze lijsten worden gekenmerkt door een belangrijke "*couleur locale*" die men vreest te verliezen eenmaal alles gestroomlijnd wordt op het federale niveau. De prioriteiten van de lokale politie zijn bovendien niet altijd dezelfde als deze van de federale politie. Op het federaal niveau wenst men ANPR-camera's in te zetten voor bovenlokale fenomenen zoals terrorisme terwijl er op lokaal niveau vaak successen geboekt worden door op lokale fenomenen in te werken. Omwille van deze reden wenst men een eigen backoffice te behouden, als het ware als veiligheidsmechanisme.

Een eigen systeem laat een eigen lokale monitoring toe om zowel de politiediensten aan te sturen op beleidsmatig niveau maar biedt evenzeer zicht op het gebruik van de databank: Wie logt in op welk moment? Welke informatie wordt opgezocht?… Dit is belangrijke informatie in het kader van controle- en integriteitdoeleinden voor bijvoorbeeld een Dienst Intern Toezicht.

2.5.7 Informatie Vlaanderen

Naast de lokale en federale politie, is Informatie Vlaanderen een andere belangrijke speler in het ANPR-verhaal. Informatie Vlaanderen van de Vlaamse Overheid ondersteunt de Vlaamse overheden bij het in de markt zetten, digitaliseren en verbeteren van dienstverlening (Informatie Vlaanderen, 2020).[3]

[3] Zie: https://overheid.vlaanderen.be/informatie-vlaanderen, 3 april 2020.

Er wordt binnen Informatie Vlaanderen actief onderzocht hoe datasets kunnen ontsloten worden voor *smart city* doeleinden, meer specifiek hoe bijvoorbeeld geanonimiseerde of gepseudonimiseerde ANPR-data kunnen ontsloten worden met geïnteresseerde partners in Vlaanderen, overheidsadministraties, steden en gemeenten… Informatie Vlaanderen bevroeg in 2019 Vlaamse overheden en administraties aangaande welk soort ANPR-data zij wensen en hoe deze ter beschikking kunnen worden gesteld. Deze oefening werd ook verbonden aan de ter beschikking zijnde data van DIV en verder werd bestudeerd wat nuttig en haalbaar is vanuit privacy-aspect. Deze bevraging resulteerde in use cases.

Informatie Vlaanderen onderzoekt niet alleen wat mogelijkheden kunnen zijn om data-ontsluiting mogelijk te maken voor *smart city* doeleinden maar heeft binnen het ANPR-verhaal ook een specifieke rol. Zij bieden namelijk ondersteuning aan de steden Antwerpen en Gent in het kader van de controle op lage emissiezones. Informatie Vlaanderen maakt een koppeling tussen de door ANPR-camera's geregistreerde nummerplaten in deze steden en de data van DIV. Informatie Vlaanderen voorziet de politie van deze gekoppelde data voor de verwerking van de boetes.

Een groot aantal respondenten in dit onderzoek wijzen Informatie Vlaanderen een belangrijke rol toe in dit project. Zo zouden zij een geanonimiseerde (of gespeudonimiseerde) ANPR-dataset kunnen ontvangen van de federale politie (AMS) en deze op haar beurt versturen naar de lokale geïnteresseerde overheden (steden/gemeenten/…). We komen later in deze samenvatting hier nog op terug. Het is belangrijk volgens meerdere respondenten om deze dispatchrol te centraliseren. De versnippering van het aantal partners en instanties bemoeilijkt de transparantie en het borgen van de privacy van de burger. Deze rol wordt Informatie Vlaanderen toebedeeld omdat zij de 'databoite' van de Vlaamse overheid zijn als het ware. Zij doen aan *e-governance* en stellen reeds data ter beschikking aan lokale overheden in het kader van het rijksregister, kruispunt sociale zekerheid, … evenals in de domeinen van financiën, onderwijs, tewerkstelling. Zij zijn tevens decretaal gemachtigd en hebben aldus een wettelijke opdracht om dergelijke informatiedoorstroming te faciliteren. Deze decretale machtiging wordt erkend voor de materies Kruispunt Sociale Zekerheid, Financiën maar de vraag stelt zich in hoeverre dit kan voor politionele informatie.

2.5.8 Andere spelers in het veld

Naast de lokale en federale politie en Informatie Vlaanderen zijn er nog een aantal andere spelers in het ANPR-verhaal belangrijk. Zij worden kort even toegelicht.

De Dienst Inschrijving Voertuigen (DIV) is een eerste belangrijke speler. Alle personen die in België wonen zijn verplicht hun voertuig in te schrijven bij de Dienst Inschrijving Voertuigen.[4] De informatie-uitwisseling met DIV is cruciaal voor de politie: als er een nummerplaat wordt geregistreerd dient deze immers met de eigenaar te worden geïdentificeerd.

Viapass[5] is een interregionale entiteit die gecreëerd werd door, voor en in naam van de drie gewesten. De juridische basis van Viapass staat beschreven in het samenwerkingsakkoord van 31/01/2014. Dit samenwerkingsakkoord beschrijft ook de uitwisseling van gegevens. Viapass staat in voor het regelen van de kilometerheffing voor vrachtwagens in België. Zij heffen tol op het vrachtvervoer boven 3,5t en staan in voor de coördinatie en controle hierop. De controle wordt mede mogelijk gemaakt door ANPR-camera's.

Ook de Vereniging voor Vlaamse Steden en Gemeenten[6] speelt een rol door haar verbindende functie. VVSG betreft een ledenvereniging waar zowel Vlaamse Steden en Gemeenten, politiezones, intercommunales, hulpverleningszones, brandweer… lid van kunnen zijn. Zij zetten thema's zoals financiering, logistiek en personeelsbeleid op de agenda. De laatste jaren is het thema data-uitwisseling en het gebruik van ANPR-camera's brandend actueel.

VVSG heeft een verbindende rol op Vlaams niveau waarbij zij binnen specifieke thema's overlegplatforms organiseren tussen de federale en lokale politie, lokale overheden en toezichthouders. De verzamelde informatie wordt voorgelegd aan hun Raad van Bestuur en op basis hiervan wordt

[4] Zie: https://mobilit.belgium.be/nl/wegverkeer/inschrijving_van_voertuigen, geraadpleegd op 3 april 2020.
[5] Zie: https://www.viapass.be, geraadpleegd op 3 april 2020.
[6] Zie: https://www.vvsg.be/, geraadpleegd op 3 april 2020.

gekeken welke rol VVSG kan betekenen. Zo kan een thema worden aangekaart op het politieke niveau of kan er een vorming worden georganiseerd omtrent specifieke issues.

Naast DIV, Viapass en het VVSG zijn de leveranciers van camera's en software evenzeer een belangrijke speler in het ANPR-verhaal. Als een entiteit beslist om een ANPR-portaal op te zetten, moeten zowel camera's aangekocht worden als een specifieke software die nummerplaten kan uitlezen. Zoals reeds aangehaald worden door middel van het raamcontract garanties ingebouwd dat de leveranciers camera's en software installeren die compatibel zijn met het federale AMS.

De rol van de netwerkprovider wordt evenzeer vastgelegd door middel van het raamcontract. Als een netwerkprovider deel uitmaakt van het raamcontract genereert dit een zeer grote toegankelijkheid naar de geïnteresseerden terwijl diegene die er geen deel van uitmaakt met een meer gevarieerd aanbod naar de markt kan stappen.

De automatische nummerplaatherkenning wordt echter niet alleen gebruikt door politionele instanties of lokale overheden. Er is grote interesse in deze technologie bij private instanties, een laatste speler. Zo gebruiken private bedrijven dit als een vorm van toegangscontrole tot hun private parkings, bij industriële toepassingen zoals weegbruggen en als logistieke voorziening waarbij ANPR gebruikt wordt als verkeersgeleiding om het laden en lossen van vrachtwagens efficiënter te maken.

2.5.9 Toezichtsorganen

De organen die toezicht uitoefenen op de ANPR-data spelen een cruciale rol in de verwerking van deze data. Er zijn verschillende toezichtsorganen betrokken in het ANPR-verhaal, zoals de GBA, VTC en het COC.

De Gegevensbeschermingsautoriteit (GBA) is een onafhankelijk orgaan dat erop toeziet dat de grondbeginselen van de bescherming van de persoonsgegevens correct worden nageleefd.[7] De leden van het directiecomité, het kenniscentrum en de geschillenkamer van de GBA worden door de Kamer van Volksvertegenwoordigers benoemd. Samen bieden ze het hoofd aan de juridische, economische, ethische en technologische uitdagingen van de evolutie van de digitale samenleving. De GBA informeert op haar website over het gebruik van bewakingscamera's, mobiele camera's en ANPR-camera's.[8] Het concrete onderwerp van deze studie, het ontsluiten van ANPR-gegevens aan lokale besturen, maakt niet het voorwerp uit van een advies, een aanbeveling, een FAQ, of dergelijke.

De Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens (VTC) is als onafhankelijke autoriteit verantwoordelijk voor het toezicht op de toepassing van de Algemene Verordening Gegevensbescherming (GDPR) door de Vlaamse bestuursinstanties.[9] De VTC oefent toezicht uit op de Vlaamse steden en gemeenten in het kader van de verwerking van persoonsgegevens. De bevoegdheden van de VTC zijn bepaald in het "e-gov Decreet" van 18 juli 2008[10] en een concrete lijst met de taken en bevoegdheden is beschikbaar op de website van de VTC.[11]

Het Controleorgaan voor politioneel informatiebeheer (COC) heeft als wettelijke opdracht de controle en het toezicht in het brede domein van de informatiehuishouding en -technologie van de politie.[12] Het COC houdt toezicht op de verwerking van persoonsgegevens door de politiediensten. Het politioneel cameragebruik, met name alle camera's die door de politiediensten worden gebruikt, zijn uit het toepassingsgebied van de Camerawet gehaald en de regels omtrent de plaatsing en het gebruik ervan

---

[7] Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Zie: https://www.gegevensbeschermingsautoriteit.be/beslissingen (consultatie op 13 april 2020).

[8] https://www.gegevensbeschermingsautoriteit.be/welke-gevallen-mag-ik-gebruik-maken-van-mobiele-bewakingscamera%E2%80%99s (FAQ) en https://www.gegevensbeschermingsautoriteit.be/mobiele-bewakingscameras (consultatie op 13 april 2020).

[9] Decreet van 8 juni 2018 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).

[10] Gewijzigd door het Decreet van 8 juni 2018.

[11] https://overheid.vlaanderen.be/taken-vlaamse-toezichtcommissie.

[12] Meer concreet van (i) de federale politie en de korpsen van de lokale politie, (ii) de AIG (Algemene Inspectie van de Federale en de Lokale Politie) en (iii) de BEL_PIU (Passagiersinformatieeenheid).

worden uitdrukkelijk geregeld door de Wet op het Politieambt. Niet de GBA maar het COC is bevoegd voor controle op politioneel cameragebruik.

2.6 Gebruik en aantal ANPR-camera's

Een eerste doelstelling is het verkrijgen van een zo accuraat mogelijk overzicht over de aanwezigheid van ANPR-camera's, hoeveel er zijn, waar deze zich bevinden en wie eigenaar of beheerder is van deze camera's. Dit werd zowel bevraagd in de kwalitatieve interviews als in de kwantitatieve bevraging.

2.6.1 Meer dan drie op vier gebruikt ANPR-camera's

Meer dan drie op vier respondenten van de online-survey (78,4%) maakt gebruik van ANPR-camera's. De meeste respondenten van een politiezone maken gebruik van deze camera's (87,7%), gevolgd door een stad of gemeente (72,7%) en een haven (42,9%). De vragenlijst werd ook ingevuld door een medewerker uit één treinstation die gebruik maakt van ANPR-camera's.

De respondenten die geen ANPR-camera's op hun grondgebied hebben, werden gevraagd naar de redenen hiervoor. Een gebrek aan middelen speelt een rol voor sommige lokale besturen en havens. "*Andere redenen*" spelen ook een belangrijke rol voor alle type respondenten. Uit de vrije antwoorden voor deze redenen, valt op te maken dat bij politiediensten de camera's op termijn zullen komen. Ze zijn in een voorbereidende fase of al besteld. Bij de lokale zones komen twee argumenten vooral naar voren: ze zijn deze piste aan het onderzoeken; of een verkenning heeft uitgewezen dat de kosten niet opwegen tegen de voordelen. Dit eerste argument vinden we ook terug in de antwoorden van de havens.

2.6.2 Onduidelijkheid over het aantal ANPR-camera's

Op dit moment ontbreekt het in België aan een organisatie die op een centraal niveau over cijfers beschikt met betrekking tot het totale aantal ANPR-camera's in België. Het overzicht is verre van volledig en ook onze onderzoeksresultaten bekrachtigen deze stelling.

De vraag naar het aantal camera's levert binnen de online survey een diversiteit aan antwoorden op. Van de 92 respondenten die een specifiek aantal aanduiden heerst een enorme variëteit: gaande van minimaal één camera tot maximaal 172 camera's. De mediaan bedraagt 8 camera's. Dat wil zeggen, dat 50% van de antwoorden kleiner zijn dan acht en 50% van de antwoorden groter zijn dan acht. Er zijn wat verschillen met betrekking tot het aantal camera's naargelang het type respondent daarom worden de medianen vergeleken. Voor de politiezones ligt de mediaan op 12, voor de steden of gemeentes ligt de mediaan op vier en voor de havens op 23.

In de kwalitatieve interviews wordt gesproken over verschillende aantallen. Het meest volledige getal betreft 3.465 ANPR-camera's die de politie gebruikt of voor politie bruikbare data opleveren. Deze berekening gebeurde op het centrale niveau en betreft alle camera's die op het AMS kunnen aangesloten worden. Deze gegevens zijn niet publiek beschikbaar.

Zowel op basis van het kwantitatieve als kwalitatieve luik worden geen eenduidige cijfers gevonden. Dit betekent dat er tot dusver geen transparant zicht is op waar alle ANPR-camera's zich bevinden. Deze informatie is vaak versnipperd aanwezig, namelijk op lokaal niveau, maar zelfs op dit niveau worden soms geen exacte cijfers ontvangen. Het versnipperde landschap aan ANPR-camera's én het gebrek aan één centrale instantie die de aanwezigheid van alle ANPR-camera's centraliseert is een knelpunt zowel voor politionele en niet-politionele informatiedeling als naar transparantie naar de burger toe. Wanneer een datadeling mogelijk wordt gemaakt ten behoeve van zowel politionele als niet-politionele doeleinden, is het cruciaal om te weten hoeveel ANPR-camera's er worden ingezet en waar deze zich bevinden.

2.6.3 Locaties van de camera's

In de online survey werd een vraag gesteld naar de locatie van de ANPR-camera's. Er werd een limitatief overzicht van de genoemde en gekende locaties van de ANPR-camera's opgemaakt. Regelmatig staan er minimaal twee camera's op één locatie (bv. één camera gericht in de twee richtingen).

Agentschap Wegen en Verkeer beschikt over een 600-tal ANPR-camera's verspreid op 174 trajectcontrolelocaties. Een installatie voor trajectcontrole bestaat uit meerdere camera's. Het is belangrijk om een onderscheid te maken tussen het aantal ANPR-installaties (kunnen meerdere ANPR-camera's omvatten), het aantal locaties met trajectcontrole (op 1 locatie kunnen 2 trajectcontroles zijn, nl 1 in elke rijrichting), het aantal trajectcontroles (bestaan uit meerdere ANPR-installaties)...

De respondenten werd ook gevraagd op welk type weg de meeste camera's zich op bevinden. Niet onbegrijpelijk zijn de meeste camera's eigendom van de politiezone op gewestwegen (61,2%) en op gemeentewegen eigendom van de politiezone (36,4%), het lokale bestuur (27,3%) of van hen beide (13,6%). Voorbeelden van andere locaties zijn bijvoorbeeld: "*private wegen met openbaar karakter*" of "*op voertuig*". Hoewel autosnelwegen kon aangeduid worden als antwoordmogelijkheid, duidde men dit niet aan. Een bijkomende vraag werd gesteld of men beschikt over mobiele ANPR-camera's. Ongeveer één op drie (34,5%) respondenten beschikt over zulke ANPR-camera's. De lokale entiteiten die een mobiele ANPR-camera hebben, hebben steevast ook vaste camera's op hun grondgebied. Uit de antwoorden blijkt dat zelden het aantal camera's wordt genoemd maar wel het aantal voertuigen uitgerust met ANPR. Zo blijkt dat de voertuigen zijn uitgerust met minimaal één camera en maximaal met drie camera's.

2.7 Meerdere eigenaars, meerdere beheerders

2.7.1 Politie coördineert het vaakst

Een eerste belangrijk onderzoeksresultaat gaat in op wie eigenaar van de ANPR-camera's is. Dit gegeven komt zowel aan bod in het kwantitatieve als kwalitatieve luik.

In de kwantitatieve survey werd de vraag gesteld wie de eigenaar is van de ANPR-camera's. De frequentst aangeduide eigenaars betreffen de politiezone (56,3%), het lokaal bestuur (20,7%) en het Vlaams Gewest (16,3%). Sommige respondenten duidden meerdere eigenaars aan.

Er is soms sprake van meerdere eigenaars: Zo blijken zowel sommige steden of gemeenten eigenaar te zijn alsook de politiezones. Eén van de verklaringen hiervoor heeft betrekking op de financiering van de lokale politie, namelijk door de steden en gemeenten waardoor men zich beide het eigenaarschap toe-eigent. In andere gevallen, heeft dit verschil te maken met de finaliteit van het aanwenden van de ANPR-camera: bijvoorbeeld lage emissiezone (LEZ) in combinatie met trajectcontrolecamera's van het AWV. Een derde verklaring is geschiedkundig waarbij de camera's van het AWV opgenomen worden in het raamcontract van de federale politie, waardoor het soms zo is dat een lokale zone zowel de AWV-camera's heeft (bijvoorbeeld voor trajectcontroles) (met eigenaars Vlaams Gewest, federale politie) als eigen lokale camera's voor criminaliteitsdoeleinden (met eigenaar lokale politie, stad/gemeente).

Het beheer van ANPR-camera's kan, zoals eigendom, uit één of meerdere entiteiten bestaan. In totaal worden 132 beheerders gerapporteerd in de vragenlijst. Het vaakst wordt de politiezone als beheerder aangeduid (63,6%) gevolgd door de federale politie (15,9%). Meestal wordt één beheerder aangeduid, de overige beheerders bestaan uit combinaties tussen twee en vier anderen. Voorbeelden van andere beheerders zijn: het Agentschap Wegen en Verkeer (AWV); naburige politiezone of ander gemeentebestuur.

De antwoorden uit de interviews bevestigen dat openbare overheden vaak eigenaar zijn van ANPR-camera's en data. De politie of de stad/gemeente zijn de meest voorkomende eigenaars, evenals beheerders. De politie is vaak eigenaar en beheerder maar de gemeentes/steden zullen frequent de lokale politiezones financieren om een ANPR-portaal aan te kopen. Er werden in het verleden enkele

subsidies gegeven vanuit de federale en Vlaamse overheid maar de hoofdmoot van de lokale ANPR-camera's zou bekostigd worden door de steden en gemeenten.

Op de rol van het AWV wordt in de interviews ingegaan waarbij lokale autoriteiten soms het gevoel kregen weinig inspraak te hebben als zij camera's wensten aan te kopen. Lokale politiezones voelden zich genoodzaakt om zelf in te staan voor de financiering van de ANPR-camera's, wat een versnippering in de hand werkte. In navolging van het Vlaamse raamcontract (AWV), kregen lokale zones de mogelijkheid om ANPR-camera's binnen het federale raamcontract aan te kopen. Een bijkomende reden waarom lokale zones zich op het federale netwerk kunnen aansluiten heeft te maken met wettelijke verplichting om ANPR-data van een lokale naar een federale backoffice door te sturen. Echter zijn er technische redenen waarom tot op vandaag deze lokale backoffices niet aangesloten geraken op de federale backoffice. Bovendien ontbreken ministeriële richtlijnen over hoe de politie met deze data kan en mag werken.

2.7.2 Infrastructuur = data?

Eigenaar zijn van een ANPR-camera impliceert eigenaar zijn van ANPR-data, wat betekent dat wie in het bezit is van een camera ook over de data beschikt. Dit principe komt meer en meer onder druk te staan waarbij de eigenaar van de camera niet meer automatisch alleen over de data beschikt. Meer en meer duikt de tendens op dat de infrastructuur dus los staat van de data. Te meer gezien de wettelijke verplichting om de lokale data door te sturen naar de federale politie. "*Als alle lokale data worden doorgegeven aan het ANPR Managed Services of AMS, wat wettelijk bepaald staat, impliceert dit dat er twee eigenaars en twee beheerders zullen zijn: de lokale én de federale politie".* Als lokale entiteit kan men beslissen om zowel de infrastructuur als het databeheer in handen te houden op het lokale niveau, wat betekent dat lokale backoffices worden aangekocht of men kan beslissen om aan te sluiten op de federale backoffice en data naar deze backoffice doorsturen (dit betekent dat zij niet over een lokale backoffice beschikken).

Inzake het beheer wordt er frequent een onderscheid gemaakt tussen de technische beheerders en het datamanagement. De politie is eigenaar en operationeel beheerder van de data maar het technische beheer is een frequente taak van de netwerkprovider; deze staat in voor het netwerk (zowel voor het draadloos netwerk als voor de backbone om de datastromen op het netwerk van de politie te krijgen), service en onderhoud van de camera's. Ook specifieke instanties die ANPR-camera's hebben, zoals de haven van Antwerpen worden in deze context vermeld. Zo is de haven de technische beheerder van de door hen aangekochte ANPR-camera's en zijn de Ministers van Veiligheid en Binnenlandse Zaken en Justitie – de federale politie - verantwoordelijk voor de verwerking van de data.

2.8 Gebruik van ANPR-data

2.8.1 Hoe wordt ANPR-data gebruikt?

Er werden ook enkele vragen gesteld over het gebruik van ANPR-data. Zo werd gepeild naar: sporadisch, structureel gebruik, anonieme en niet-anonieme gegevens, gebruik van beeldmateriaal en afgeleide data. Zes op tien respondenten maakt gebruikt van ANPR-data op een structurele manier en vijf op tien respondenten maakt er eerder sporadisch gebruik van. Er zijn respondenten (doorgaans politiediensten) die zowel structureel als sporadisch gebruik maken van de ANPR-data. Diegenen die structureel gebruik maken van deze data betreffen in hoofdzaak politiediensten.

Niet-anonieme ANPR-data worden frequenter gebruikt (44,7%) in vergelijking met anonieme ANPR-data (19,7%). Vooral binnen de politiediensten wordt van niet-anonieme data (64,0%) vaker gebruik gemaakt dan binnen het lokaal bestuur (8,0%). Er werd tot slot een vraag gesteld of er beeldmateriaal gebruikt wordt of eerder afgeleide data. Bijna twee op de drie (63,2%) respondenten maakt gebruik van beeldmateriaal en minder dan één op vier (23,7%) van de respondenten maakt gebruik van afgeleide data. Wederom maken politiediensten het vaakst gebruik van deze data in vergelijking met andere type respondenten.

2.8.2 Waarvoor worden ANPR-data gebruikt?

Waartoe wordt deze ANPR-data aangewend, was een volgende vraag in de vragenlijst. Het vaakst wordt criminaliteitsbestrijding (50,0%) en verkeershandhaving (33,3%) als finaliteit genoemd. Minder dan één op drie respondenten (30,7%) noemt één finaliteit voor het gebruik van deze data. Dat betekent dat meer dan twee op drie respondenten (69,3%) de camera's voor meerdere doeleinden gebruikt. Kenmerkend bij deze meerdere doeleinden is dat hierbij steeds het gebruik voor criminaliteitsbestrijding wordt genoemd.

Indien ingegaan wordt op de actor die deze data aanwendt, dan zien we dat het zowel politiediensten als lokale besturen zijn die vooral gebruik maken van deze data voor criminaliteitsbestrijding en verkeershandhaving (52,0% en 41,7%) en criminaliteitsbestrijding (22,0% en 37,5%).

2.9 Delen van data

2.9.1 Deelt men data? Met wie deelt men data? En hoe gebeurt dit?

Het delen van informatie werd evenzeer bevraagd in de vragenlijst. Allereerst werd er gepeild of data wordt gedeeld, met wie de data wordt gedeeld en hoe deze uitwisseling is geregeld (bv. middels een protocol).

Van de 109 respondenten die ANPR-camera's op hun grondgebied hebben, vulden 80 respondenten (78,4%) de vraag in of zij ANPR-data delen waarvan 52 respondenten informatie delen. Wanneer we deze antwoorden bekijken per type respondent valt op dat de politie in 74,0% van de gevallen informatie met andere partijen deelt en het lokaal bestuur in 46,4%.

Van de respondenten die informatie delen, duidt 92,2% aan met wie zij informatie delen. Er worden in totaal 120 actoren opgesomd met wie data worden gedeeld. Het vaakst worden data gedeeld met de federale politie (28,3%), andere politiezone (25,8%), eigen politiezone (21,7%) of eigen organisatie (11,7%). Ongeveer 1 op 4 respondenten (28%) noemt maar één andere partij waarmee de data worden gedeeld. De overige respondenten delen de data met minimaal twee en maximaal vijf andere partijen.

Als we inzoomen op de specifieke diensten, merken we op dat de politiediensten het vaakst ANPR-data delen met een andere politiezone (10,8%); federale politie (10,8%); een eigen organisatie, eigen politiezone, andere politiezone en federale politie (10,8%). Het lokale bestuur deelt het vaakst ANPR-data met: andere politiezone (16,7%) en eigen politiezone, andere politiezone en federale politie (16,7%).

Voorts wordt bekeken welke modaliteiten (bijvoorbeeld een protocol) worden gebruikt om data te delen met anderen. We gaan in op de 52 respondenten die ANPR-camera's op het grondgebied hebben en ook data delen. Van deze 52 respondenten, gebruikt 34,7% een protocol, 65,3% gebruikt dit niet. Negentien respondenten delen wèl informatie maar volgens een andere modaliteit dan een protocol. De respondenten verwijzen onder meer naar het AMS, vergaderingen en afspraken met overheden, samenwerkingen met de DPO, de douane, etc. Bij de vraag naar de juridische basis verwijst het merendeel van de respondenten naar de WPA en de GDPR.

2.9.2 Politionele datadeling

2.9.2.1 Centralisering of decentralisering?

Het Vlaamse ANPR-netwerk wordt geconfronteerd met een ware versnippering waarbij zowel lokale als federale backoffices ANPR-data genereren. Deze versnippering wordt door sommige geïnterviewden geproblematiseerd en anderen beschouwen dit als niet-problematisch. Zo wensen veel zones een eigen lokale backoffice te behouden, wat hierboven werd beargumenteerd.

Het huidige versnipperde landschap is één van de grootste redenen waarom een centralisering zich opdringt. De politionele datadeling wordt geoptimaliseerd, wat politioneel onderzoek ten goede komt.

De criminaliteit stopt immers niet aan de grenzen. Het vermijdt bovendien dat lokale actoren talrijke vragen gesteld worden over een specifieke nummerplaat. Zo vragen lokale politiezones data aan het Arrondissementeel Informatie Kruispunt (AIK) of het Lokaal Informatie Kruispunt (LIK) en zij analyseren data voor en rond de politiezones of het arrondissement. Het zou een meerwaarde betekenen mocht een nationale datadeling opgezet worden in een nationaal systeem. Het feit dat er op het centrale niveau een link kan gelegd worden met DIV is bovendien voordelig. Deze datadeling is niet enkel belangrijk lokale versus federale politie en vice versa maar evenzeer voor nationale veiligheidsdiensten en voor politionele datadeling op het internationaal niveau.

De centralisering stelt allerhande instanties voor een diversiteit aan technische en juridische uitdagingen. We komen hier dadelijk uitvoerig op terug.

Aanhangers van een decentraal model halen vaak dezelfde argumenten aan als de aanhangers van het centraal model. Zo wordt vaak gewezen op de grootte van de databank en de privacy van de burger. Hoe groter de databank, hoe meer risico's men loopt als er dataverlies is. Tegenstanders stellen net dat er bij een centralisering een veel grotere professionele aanpak mogelijk is inzake privacy en beveiliging. Zowel de controle op de datadeling als het respecteren van de grondrechten van de burger worden op deze wijze vereenvoudigd.

De vraag wordt hier gesteld in hoeverre iedere lokale entiteit competent genoeg is om haar eigen databank te beveiligen. Dit vergt wellicht expertise van een derde partij, wat uiteindelijk leidt tot een lappendeken. Ook efficiëntie- en budgettaire redenen worden aangehaald als een pluspunt om te centraliseren.

Tot slot wensen enkele respondenten geen standpunt in te nemen en beklemtonen het feit dat beide databronnen veel informatie opleveren en dat lokale en federale politie dienen samen te werken.

2.9.2.2 Wie neemt het stuur in handen?

Het gebrek aan een centrale coördinerende beleidsinstantie wordt bekritiseerd. Er is volgens verschillende bevraagden geen centrale beleidsactor die het stuur in handen neemt. Niemand houdt op een bovenlokaal niveau in het oog wat er gebeurt op het federale, Vlaamse en lokale niveau; Waar staan de camera's? Wat er mag en wat mag niet? Wat steden en gemeenten met ANPR-data doen of kunnen doen? Een coördinerende beleidsinstantie zou een meerwaarde zijn, voor dergelijke materie met een groot maatschappelijk belang. Deze instantie kan instaan voor het delen van expertise en meezoeken naar gezamenlijke oplossingen voor aangehaalde problemen. Een uniforme aanpak impliceert dat er lessen getrokken worden over *good & bad practices* en gedeeld/gecommuniceerd worden naar lokale autoriteiten. Het risico op individuele fouten wordt gereduceerd evenals het risico op incidenten/inbreuken op de privacy van de burgers. Deze manier van werken komt ten goede van de burger waarbij op een transparante manier een centrale actor weet wat er kan en wat er met de gegevens gebeurt.

2.9.3 Niet-politionele datadeling met lokale overheden of andere partijen

2.9.3.1 Voorstander om te delen met lokale overheden

Alvorens ANPR-data worden gedeeld, is het belangrijk om te weten welke entiteiten, overheden, instellingen … ANPR-data mogen krijgen en aanwenden. Inzake het gebruik en de aanwending van ANPR-data worden drie niveaus onderscheiden. Het eerste niveau betreft het politionele luik of het strafrechtelijke luik. Op dit niveau zijn ANPR-data enkel ter beschikking van de politie en justitie. Een tweede niveau betreft de handhaving, bijvoorbeeld in het kader van controles op verkeerd parkeren, naleving lage emissiezone… Dit betreffen controles die uitgevoerd worden door de lokale politiezones of het lokaal bestuur. Dit niveau van dataverzameling vereist een link met DIV-gegevens waarbij de persoon van het voertuig wordt geïdentificeerd. Het derde niveau betreft datgene waarop geanonimiseerde of gepseudonimiseerde ANPR-data worden verzameld. Verschillende actoren zijn vragende partij om dergelijke data te ontvangen zoals Vlaamse administraties in de domeinen van verkeer, mobiliteit, openbare werken…; steden en gemeentes; havenbedrijven;… Deze actoren wensen geen individuele persoonsgegevens maar bijvoorbeeld verkeersstromen en – volumes. Dergelijke data zijn bovendien zeer waardevol voor diensten uit het domein ruimtelijke ordening en milieu. ANPR-data

kennen een grote toegevoegde waarde; zij geven een beeld van het aantal voertuigen, types voertuigen, CO2 uitstoot, gebruik van een elektrische wagen, merk…

De praktijk of de mogelijkheid tot het ontsluiten van ANPR-data met lokale overheden of andere partijen wordt uitvoerig geëxploreerd. Zo geven meerdere bevraagde actoren aan dat er reeds gedepersonaliseerde data worden gedeeld met lokale overheden. De politie is doorgaans op de hoogte van de finaliteit waarvoor deze data worden aangewend. Het is de politie die de data anonimiseert en doorstuurt; het gaat met andere woorden niet over beelden, foto's of nummerplaten maar over afgeleide data zoals cijfers en statistieken. Dit materiaal wordt ter beschikking gesteld aan mobiliteitsdiensten, diensten leefmilieu, openbare werken…

Het openstellen en delen van data met anderen in het kader van *smart city* toepassingen dient volgens meerderen mogelijk gemaakt te worden, op voorwaarde dat het GDPR-conform is en alle belanghebbenden hier een voordeel uit halen. Sommigen vinden het zelfs jammer dat er zoveel wordt in geïnvesteerd in ANPR, er zoveel data ter beschikking is en er weinig tot niets mee gebeurt. Belangrijk is dat de burger wordt gerespecteerd en hierin wordt betrokken. "*Geef die data terug aan de burger*", zodat hij weet dat ANPR-camera's niet enkel aangewend worden ter controle maar er veel meer mee kan.

Het delen van data met niet-gouvernementele actoren stuit op enige terughoudendheid, waarbij bijvoorbeeld het aanwenden van data voor commerciële doeleinden in twijfel wordt getrokken. Ongeacht het gegeven dat er reeds veel ANPR-data ter beschikking zijn, stelt iemand dat er hoge verwachtingen zijn over deze data.

Eén van de grootste knelpunten binnen het ter beschikking stellen van ANPR-data is dat nauwelijks iemand de bomen door het bos ziet. In de interviews wordt veelvuldig aangegeven dat ANPR-data op een anonieme manier zouden kunnen gedeeld worden met lokale autoriteiten. Er is echter bijzonder veel onduidelijkheid over wat er kan en wat er mag, met andere woorden onduidelijkheid troef op allerhande vlakken, zeker op juridisch en technisch vlak.

Vanuit toezichtperspectief geeft een bevraagde aan geen voorstander te zijn om derde diensten toegang te geven tot politionele databanken. Er wordt enerzijds gewezen op het feit dat dit niet wettelijk voorzien is maar evenzeer op het feit dat niemand een zicht zal hebben op het secundair gebruik van deze gegevens door derde actoren. Bovendien wordt er een verschil gemaakt tussen anonieme gegevens – wat op zich minder problematisch is om datadeling mogelijk te maken – en gepseudonimiseerde gegevens. Als lokale overheden gebruik wensen te maken van gepseudonimiseerde gegevens kan er met een *trusted third party* gewerkt worden. Deze partij kan de gegevensstromen 'avaliseren', wat een actie om een derde partij op te richten betekent. Deze trusted third party kan een voortdurende opdracht toegewezen krijgen, vergelijkbaar met het vroeger sectortaal comité. Een machtiging kan dan gegeven worden per gegevensstroom en per finaliteit.

In een interview stelt iemand dat er voldoende controle nodig is op de persoon binnen het lokaal bestuur die gegevens opvraagt. Zo kan er een ANPR-gegevensbeheerder worden aangeduid die door middel van gestandaardiseerde formulieren een aanvraag kan versturen. Eens data ter beschikking worden gesteld, dienen de afnemers hier zorgvuldig mee om te gaan. Het is zaak om dezelfde systemen aan te wenden zodat ook dezelfde soort van statistieken berekend worden.

2.9.3.2 Welke actor deelt data?

De lokale politie die data deelt met het lokaal bestuur garandeert een bepaalde mate van controle omdat zij weet wat de finaliteit is van het aanwenden van deze data. Doorgaans worden formele afspraken gemaakt over deze ter beschikking stelling van data, binnen het gehanteerde juridische kader.

Om een nationale ANPR-datadeling mogelijk te maken met lokale autoriteiten halen meerdere respondenten aan dat deze datadeling op centraal niveau moet georganiseerd worden. Er dient vooreerst een duidelijke nationale visie te worden uitgewerkt die gedragen wordt waarin zowel juridische als technische afspraken worden vastgelegd.

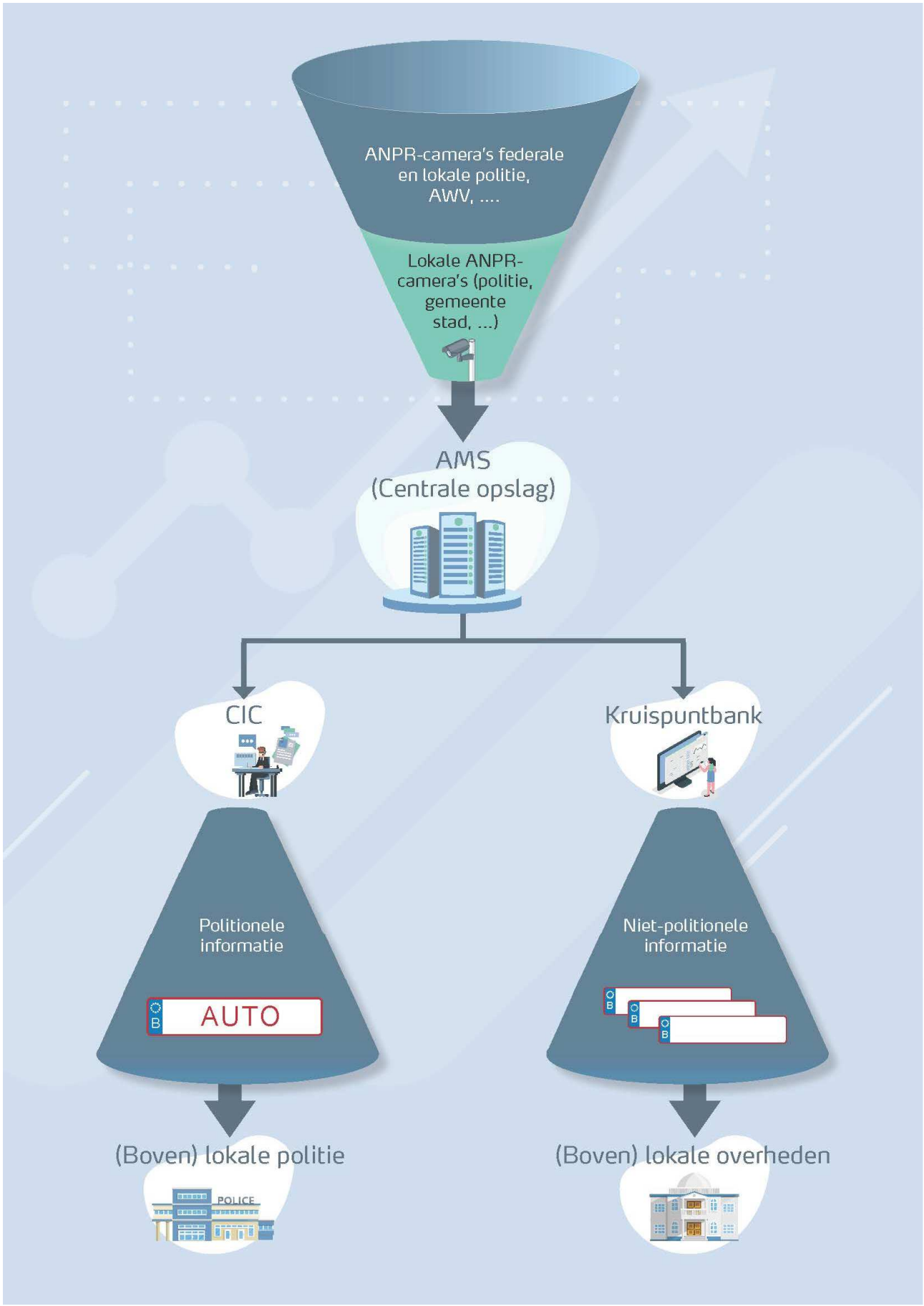
De redenen waarom dit op een nationaal niveau moet georganiseerd worden zijn velerlei. Zo is er vooreerst de wetgevende bepaling dat alle ANPR-data doorgestuurd moeten worden naar het nationale

AMS. Dit betekent dat de data van de door de politie gebruikte of voor politie bruikbare ANPR-camera's worden doorgestuurd naar de federale politie. Net omwille van deze centralisering van ANPR-data is het volgens meerdere respondenten interessant om deze datadeling met lokale overheden vanuit dit niveau te organiseren.

Het anonimiseren of pseudonimiseren van de ANPR-data is voor de meerderheid van de respondenten overduidelijk politiewerk. Het effectief uitdelen van deze data kan ofwel door de federale politie gebeuren ofwel door een derde instantie. Als de federale politie instaat voor de datadeling kan zij op een gecontroleerde manier data geven aan steden en gemeenten. Dit kan juridisch bekrachtigd worden door dat lokale overheden een verbintenis aangaan, zich compliant verklaren of een protocol ondertekenen. Als de federale politie data deelt dan biedt dit ook garanties dat dit binnen de bestaande wettelijke kaders gebeurt en dit GDPR-conform is. De CIC's kunnen instaan voor deze datadeling; zij krijgen deze rol toegewezen omdat ze ervaring hebben in het rapporteren op basis van massadata. Er kunnen bijvoorbeeld query's worden vastgelegd die op een uniforme wijze informatie ter beschikking stelt aan lokale besturen.

Het federale netwerk onderhoudt op haar beurt directe relaties met de gewesten, waardoor zij de stroom aan geanonimiseerde data ter beschikking kan stellen aan deze overheden. Voor het Vlaams gewest is dit Informatie Vlaanderen van de Vlaamse overheid. Meerdere bevraagden houden een pleidooi om de taak van dataverdeling aan een centrale dienstenintegrator zoals Informatie Vlaanderen toe te wijzen. Er wordt gewezen op de decretale machtiging, het feit dat zij reeds data ter beschikking stellen voor de lage emissiezone, er een *proof of concept* is rond datadeling met specifieke instanties en zij (boven)lokale overheden bevroegen over welke data zij willen, hoe deze data ter beschikking moeten gesteld worden, wat zij doen met deze data… Dit resulteerde in *use cases*. Zij stimuleren e-governancebeleid en stellen via platformen reeds heel wat data ter beschikking aan overheden. Er wordt veelvuldig verwezen naar de kruispuntdatabank. Informatie Vlaanderen wordt door meerdere geïnterviewden aangeduid omdat zij ervaring hebben in het delen van data. Bovendien heerst ook de idee dat een centralisering een minimalisering van risico's inhoudt op het vlak van privacybescherming.

Het scenario waarbij alle ANPR-camera's data doorsturen naar het AMS wordt visueel in onderstaande figuur weergegeven. De politionele informatiedeling wordt vanuit de CIC's gewaarborgd terwijl de niet-politionele datadeling door een kruispuntbank wordt gerealiseerd.


ANPR-camera's federale en lokale politie, AWV, ...
Lokale ANPR-camera's (politie, gemeente stad, ...)
AMS (Centrale opslag)
CIC
Kruispuntbank
Politionele informatie
AUTO
Niet-politionele informatie
(Boven) lokale politie
POLICE
(Boven) lokale overheden

2.9.3.3 Voorbeelden van datadeling met niet-politionele instanties

Gedurende de interviews wordt er op verschillende voorbeelden ingegaan inzake datadeling met niet-politionele instanties. Dit kan zowel binnen de reguliere werking als op projectmatige basis. In eerste instantie zijn er lokale politiezones die ANPR-data delen met lokale overheden. De meest voorkomende voorbeelden die worden gegeven betreffen het delen van data met stedelijke diensten zoals mobiliteit, leefmilieu/milieu en klimaat, openbare werken, stadsontwikkeling… Zo gebeurde dit in meerdere bevraagde entiteiten voor de controle op een C3 verbod. Ingrijpende riolerings- en grondwerken waren evenzeer aanleiding om ANPR-camera's in te zetten om sluipverkeer te controleren. ANPR-gegevens werden binnen het juridisch kader gedeeld met het lokaal bestuur. Het is echter niet altijd duidelijk hoe dit kader er uit ziet (zie ook de juridische analyse).

Het uitwisselen van verkeersdata tussen de federale politie en de Vlaamse overheid is een tweede toepassing die in de interviews wordt aangehaald. Een derde toepassing die wordt aangehaald betreft de ANPR-data uitwisseling voor de controle op de lage emissiezone (LEZ). Dit gebeurt binnen de context van het Vlaamse decreet.[13] Een vierde voorbeeld dat wordt aangehaald door enkele respondenten betreft de samenwerking tussen de federale politie en het havenbedrijf van Antwerpen. De federale politie krijgt ANPR-data van de Antwerpse haven en deze zou in ruil een geanonimiseerde dataset krijgen zodat zij inzicht krijgen in de stromen op hun grondgebied.

De gewestelijke mobiliteitscentrale in Brussel komt evenzeer ter sprake waarbij het Brussels hoofdstedelijk gewest data verzamelt voor verkeersdoeleinden alvorens deze door te sturen naar de federale politie volgens het zogenaamde forking-principe. Dit principe, dat ingaat op hoe ANPR-data mogelijk afgeleid kunnen worden naar een alternatieve server, wordt later toegelicht.

Een volgend voorbeeld betreft de aanwending van ANPR-camera's voor de controles op het autovrije toegangsgebied in Gent. Verschillende stedelijke diensten bezitten en beheren camera's en bepalen de functionaliteit ervan. De gegenereerde data worden doorgestuurd naar een lokale backoffice van de stad en daar verwerkt. Deze data van de lokale overheid worden vrij recent ter beschikking gesteld aan het AMS van de federale politie. Dit voorbeeld betreft dus een datadeling van een lokale overheid met de federale politie, in de vorm van een pilootproject.

S-LIM, een andere praktijk waarnaar verwezen wordt, betreft een samenwerkingsverband tussen politie en gemeenten/steden in Limburg rond *smart cities*. In Limburg werd een provinciale server uitgebouwd waarbij er informatiedeling met de lokale overheden mogelijk wordt gemaakt.

Als laatste wordt het project Policy Visualisations (Polivisu[14]) aangehaald en toegelicht. Dit project situeert zich in een Europese context (Horizon 2020) en heeft als doel visualisaties te maken van de mobiliteitsdata voor beleidsmakers. Op basis van de camerageGegevens, locatie en tijdstip en geëncrypteerde nummerplaten werden profielen, snelheidsovertredingen, herkomst- en bestemmingsanalyse, reistijden, tellingen en zo berekend.

ANPR-data delen in het kader van trajectcontroles, LEZ, autoluwe zones… er zijn veel mogelijkheden om data te delen maar de diversiteit aan wetgevingen maakt deze deling complex en moeilijk. Het hanteren van een goed juridisch kader is des te belangrijker. Bovendien zijn er naast formele juridische afspraken ook vaak financiële afspraken hieromtrent.

2.10 Technische vereisten

Er worden tijdens de onderzoeksfase niet alleen juridische maar ook technische vereisten opgesomd om het delen van ANPR mogelijk te maken. Bij de technische vereisten wordt er een onderscheid gemaakt op twee niveaus. Het eerste niveau betreft de vereisten om de integratie van de lokale politionele backoffices te integreren op het federale AMS. Het tweede niveau gaat in op de technische

[13] De volgende wetgevende teksten zijn relevant voor wat betreft de LEZ (Vlaanderen):

(i) Decreet van 27 november 2015 betreffende lage-emissiezones

(ii) Besluit van 26 februari 2016 van de Vlaamse Regering betreffende lage-emissiezones.

[14] Zie: wwww.polivisu.eu, consulted on 08/05/2020.

vereisten om ANPR-data te delen met lokale autoriteiten. Als een centrale datadeling op politioneel en niet-politioneel niveau mogelijk gemaakt wordt gaan beide niveaus hand in hand: "*Als datadeling mogelijk gemaakt wordt op centraal niveau, dan worden idealiter alle lokale backoffices aangesloten op het federale netwerk*".

Sommige geïnterviewden geven aan dat er weinig technische vereisten zijn. De technische vereisten moeten samen gelezen worden met de juridische vereisten. Een eerste technisch gegeven dat zowel in het kwantitatieve als kwalitatieve deel van dit project bevraagd werd, betreft de soorten camera's, soorten software… en de betreffende technische vereisten om datadeling mogelijk te maken. Vervolgens gaan we in op de IT-security om daarna in te gaan op het eerste niveau waarbij de lokale backoffices geconnecteerd dienen te worden op het federale AMS. Dit mogelijk maken stelt ons voor heel wat uitdagingen zoals middelen, opslagcapaciteit, controle, tijd…

Er wordt daarna ingegaan op de technische vereisten om data te delen met de lokale overheden. Technische en juridische vereisten gaan ook hier hand in hand, bijvoorbeeld het proces van het depersonaliseren van de data. Er wordt verder ingezoomd op het real time inzamelen van data, wat de finaliteit is, wie deze data doorgeeft en of dit kan gekoppeld worden aan andere databanken…

Tot slot komt de datadeling tussen lokale overheden en politie en met lokale overheden aan bod om dit technisch hoofdstuk af te sluiten met het principe van forking en de cumulatie met andere data.

2.10.1 Soorten camera's, soorten software

De respondenten van de vragenlijst noemen 112 merken. Daarbij wordt "*andere*" het vaakst genoemd (38,4%), gevolgd door Macq (32,1%). Het merendeel van de respondenten (77,6%) noemt maar één merk van camera's, de overige 19 respondenten (22,4%) noemt meer dan één merk. Wat betreft het antwoord "*andere*", blijkt dat zes op tien respondenten het merk niet kennen. De respondenten die wel een merk noemen, halen merken aan zoals Siemens, Sharp, Sony, Genetec, Tein Tech. Soms wordt er een meer algemeen antwoord gegeven zoals " *komen uit de aanbesteding*" of "*zie Vlaams Gewest*".

Voorts werd gevraagd welke software zij gebruiken voor de camera's. In de 100 antwoorden wordt "*andere*" het vaakst genoemd (n = 39), gevolgd door Macq (n = 28). Gerelateerd aan Macq duiden vier respondenten Icar manager en 19 Mcube aan. Wanneer de respondenten ICAR-manager (n = 4) of Mcube (n = 19) als antwoord hebben gegeven, kan dit ook worden aanzien als Macq. ICAR is immers de oude Macq server, terwijl Mcube de nieuwe Macq server is. In dat geval, komt het totaal van Macq op 51 terecht.

Bij de categorie "*andere*" weten 23 respondenten (59,0%) niet welke software er wordt gebruikt. Overige antwoorden betreffen: Genetec, Inforead, Tein Tech, Sightvision of een meer algemeen antwoord (zoals bv: "*zie Vlaams Gewest*"). Wanneer we de software kruisen met het merk van de camera's, leert ons dit vooral dat Macq camera's vaak samengaan met Macq software (66,7%).

Het gegeven dat er een diversiteit is aan leveranciers, cameramerken, software… wordt door veel respondenten in de interviews als weinig problematisch ervaren. Dit impliceert wel vaak een integratiekost.

Het mogelijk gebrek aan integratie van verschillende camera's en software wordt door het federaal raamcontract aan banden gelegd. In het raamcontract worden eigenschappen beschreven waaraan camera's en software moeten voldoen, wat als een bijzonder grote meerwaarde wordt ervaren door menig respondent. Dit biedt garanties dat er op een vrij uniforme wijze ANPR-data worden ingezameld – zeker indien alle data doorgestuurd worden naar het AMS - evenals gedeeld kunnen worden. Het raamcontract raadplegen voor de aankoop van een ANPR-portaal wordt bovendien als efficiënt beschouwd door de bevraagden omdat het een expertise impliceert die niet altijd aanwezig is bij lokale politiezones. Het raamcontract biedt niet alleen technische maar ook juridische garanties.

Twee respondenten wijzen op verschillen tussen camera's en de software waarbij de ene camera niet exact hetzelfde meet als de andere camera. Het afstemmen van deze verschillende camera's, software is uiteraard een cruciale voorwaarde voor politionele en niet-politionele ANPR-datadeling.

2.10.2 IT-security

Een belangrijke technische vereiste om goede datadeling mogelijk te maken tussen allerhande politionele en niet-politionele actoren betreft een doordacht IT-securitybeleid. Kennis en inzicht over de technische specificaties is vereist: Wie is de fabrikant? Over welke IT-security beschikt het systeem op hard- en softwareniveau? Op wie is de camera ingeplugd? Via welke switch of router verloopt dit?... Aandacht moet worden besteed aan end-to-end security en er moet bescherming zijn tegen allerhande vormen van hacking- of bedreigingstechnieken. Naast fysische en IT-security moet er bovendien aandacht besteed worden aan logische security.

2.10.3 Naar een AMS

Op het centraal niveau wordt een nationale ANPR-backoffice systeem ontwikkeld, het zogenaamde AMS. De reden waarom dit ontwikkeld wordt, heeft deels te maken met het versnipperde landschap aan ANPR-camera's en data én aan het gebrek aan een federaal ANPR-netwerk. Alle door de politie gebruikte of voor politie bruikbare ANPR-camera's dienen data door te sturen naar het AMS. Dit betekent dat alle lokale backoffices geconnecteerd worden aan het AMS. De geïnterviewden halen voor wat betreft dit onderwerp behoorlijk wat technische vereisten aan:

- Het AMS dient flexibel te zijn;
- Het AMS moet bereid zijn om verschillende systemen hierop toe te laten;
- Het AMS dient voldoende voorbereid te zijn;
- Om alle door de politie bruikbare of politie gebruikte ANPR-camera's aan te sluiten, zijn er resources nodig;
- De meeste data komt real time binnen op het AMS, wat een performant systeem noodzaakt met veel opslagcapaciteit. Aangaande opslagcapaciteit wordt er een onderscheid gemaakt tussen:
    - Opslag van data;
    - Verwerking van data;
- De processorcapaciteit moet voldoende krachtig zijn;
- Er moet voldoende kennis en *know how* zijn voor het lezen, het bepalen van de foutenmarge…;
- Het AMS moet beschikken over goede gebruiks- en gebruikersregels (bijvoorbeeld hoeveel mensen kunnen tegelijkertijd opzoekingen doen in het systeem, hoeveel gegevens kan men maximaal opzoeken…);
- Data moet real time van de lokale politie naar de federale politie gaan en vice versa;
- Aangaande de controle:
    - Moet een surveillance- en controlefunctie uitgewerkt worden die bepaalt wie de toegang krijgt en wie niet;
    - De data over wie inlogt op welk moment op welk systeem moet de lokale politie ter beschikking worden gesteld voor beleids- als integriteitsdoeleinden.

Tot slot zijn er ook voorwaarden voor de lokale politiezones met een eigen backoffice als zij zich aansluiten op het AMS. Zo betekent dit een integratiekost voor meerdere lokale entiteiten. Een geïnterviewde geeft aan dat het interessant kan zijn om samen de krachten te bundelen zodat zij in één geïntegreerde beweging aangesloten worden op het nationale systeem.

2.10.4 Naar een datadeling met lokale overheden

Eén van de kernvragen van dit project is mocht er ontsluiting van ANPR-data zijn met lokale overheden, wat de technische vereisten hiertoe zijn. Op basis van sommige interviews blijkt dat reeds data worden gedeeld met de lokale overheden, in het kader van LEZ, autoluwe zones… De data worden van de politionele backoffice geanonimiseerd en doorgestuurd naar de lokale overheden. Een bevraagde stelt dat datadeling gebeurt door middel van twee streams die van de ANPR-camera's doorgestuurd worden naar verschillende backoffices. Het lokaal bestuur beschikt over een server en de politie beschikt over een server en deze entiteiten staan elk afzonderlijk in voor de verwerking van de gegevens. De

hardware – het instrument – wordt gedeeld maar de datastreams en de verwerking van deze streams gebeurt afzonderlijk: "*Als je een deling wil mogelijk maken dan heb je aparte verwerkingsplaatsen nodig, dus gescheiden plaatsen waar aparte streams op toekomen".*

Andere lokale entiteiten delen geen data maar stellen doorgaans dat er weinig belemmeringen zijn om te delen. Echter "*Het is niet omdat iets technisch kan, dat het juridisch ook kan en mag*", is een belangrijke rode draad doorheen dit project waarbij de technische en juridische vereisten hand in hand gaan en niet van elkaar gescheiden kunnen worden. De finaliteit waarvoor deze data aangewend worden en door wie ze worden gebruikt, is en blijft een belangrijke premisse.

Het depersonaliseren van ANPR-data is een belangrijke vereiste alvorens deze gedeeld kunnen worden met lokale overheden. ANPR-data zijn immers politionele data die niet ter beschikking kunnen gesteld worden voor andere doeleinden dan politionele. De WPA laat dergelijke deling van data niet toe (zie verder hieronder). De politie is dé instantie die volgens meerdere bevraagden instaat voor het depersonaliseren van de ANPR-data. Dit betreft ofwel de lokale politie of de federale politie die als eigenaar en beheerder bepalen wat er al dan niet kan gedeeld worden. De politie wordt beschouwd als dé authentieke bron. Het anoniem maken van deze data gebeurt doorgaans door ingebouwde software. Vanuit juridisch oogpunt wordt anonimisering boven pseudonimisering verkozen, omdat er bij anonieme data geen enkele link is naar de identificatiegegevens van het voertuig. Bij de pseudonimisering worden data geëncrypteerd/versleuteld door de politie en wordt deze sleutel bijgehouden. Enkele respondenten halen aan dat geëncrypteerde informatie meer oplevert in het kader van *smart city* toepassingen dan anonieme informatie. Inzake deze encryptie wordt verwezen naar de koppeling met de databank van DIV.

Echter om anonieme data te delen met lokale overheden moeten die uit het politioneel netwerk worden gehaald. Een piste die bij menig respondent op bijval rekent, is dat de gewesten een centrale rol krijgen toebedeeld in dit verhaal. De federale politie – die toch alle data verzamelen in het AMS – kan anonieme data doorsturen naar Informatie Vlaanderen dat op zijn beurt instaat voor de dispatching van anonieme gegevens naar de geïnteresseerde lokale overheden. Anonieme ANPR-data staan als het ware ter beschikking op een centraal platform, wat een uniforme datadeling mogelijk maakt. Dit proces zou zelfs geautomatiseerd kunnen verlopen waarbij een volledig geautomatiseerde flow aan data ter beschikking staat.

Volgens meerdere respondenten is Informatie Vlaanderen het best geplaatst voor deze dispatching. De meest cruciale technische vereiste is uiteraard dat alle lokale backoffices geconnecteerd staan met het AMS. Vervolgens worden enkele technische vereisten aangehaald, die vaak gelijk zijn aan deze van het AMS. Zo is het belangrijk voor de netwerkprovider of de informatie al dan niet real time doorgestuurd moet worden. Er kan ook iedere week een bulk van data worden doorgestuurd. Voor Informatie Vlaanderen is het op haar beurt belangrijk om te weten hoe zij de data dient aan te leveren aan de lokale overheden; is dit een geaggregeerde dataset? Vooraf bepaalde query's? Onder welke format? … De technische vereiste van opslagcapaciteit voor de centrale instantie Informatie Vlaanderen is minder aan de orde dan deze van de federale politie gezien AMS beelden opslaat terwijl de anonieme data eerder cijfer- en tekstdata betreffen. Niettemin: het massaal delen van data vergt technische capaciteit.

2.10.5 Datadeling lokale overheid – politie – lokale overheid

In een interview komt de datadeling van de lokale overheid met de politie ter sprake. Deze lokale entiteit gebruikt ANPR-camera's voor de controle op wagens die het autovrij toegangsgebied betreden zonder autorisatie. Zij stonden technisch voor een aantal keuzes over hoe zij hun backoffice verbinden met deze van de federale politie. De redenen waarom zij data delen met de federale politie is omdat op deze wijze een centrale datadeling mogelijk wordt gemaakt en lokale eenheden niet om de haverklap worden bevraagd. Een tweede reden betreft de garantie op een automatische data-uitwisseling. Net zoals veel lokale politiezones wensen zij ook zelf hun eigen lokale backoffice te behouden en te beheren. Als derde voordeel wordt aangehaald dat bovenlokale analyses interessant zijn voor stedelijk/gemeentelijk beleid.

2.10.6 Forking

De vraag hoe data kunnen afgeleid/verstuurd worden naar de federale/lokale politie en vervolgens gedeeld worden met lokale autoriteiten wordt frequent door middel van forking beantwoord. Hoewel niet iedereen thuis was in dit principe, leven er verschillende ideeën over wat forking is en hoe ANPR-data mogelijk afgeleid kunnen worden naar een alternatieve server. Verschillende interpretaties worden aan dit begrip gegeven: of men haalt data van de lokale backoffice of men haalt data van de nationale backoffice om deze vervolgens te sturen naar de lokale overheden. Het forking principe kan ook toegepast worden via een tweesporenbeleid waarbij de ANPR-data zowel naar de lokale als nationale backoffice gaat en anonieme data bezorgt aan de lokale overheden.

Data van de lokale politionele backoffice rechtstreeks versturen naar lokale overheden is volgens sommigen de optie, anderen stellen dat dit beter via de federale backoffice gaat omdat de data sowieso bij de federale politie terechtkomen. Een federale aansturing, dus een centrale actor die het voortouw neemt lijkt voor behoorlijk wat respondenten de beste optie.

Data afleiden van de backoffice is voordelig omdat het gestroomlijnd gebeurt: alle data worden gecentraliseerd en op eenzelfde manier geanonimiseerd. Echter kunnen data niet alleen afgeleid worden van de backoffice maar dit kan tevens gebeuren vanuit de camera. De camera's kunnen rechtstreeks data versturen via een dubbele flux: één stroom naar de politionele backoffice én één stroom naar de burgeromgeving. Het rechtstreeks afhalen van de beelden van de camera genereert echt volgens een geïnterviewde netwerkissues omdat de informatie naar één plaats moet gestuurd worden en er een grote variëteit is aan netwerken.

ANPR-data kunnen tot slot ook verzameld worden op een gewestelijke server alvorens ze naar de politie worden verstuurd, zoals in het Brussels Hoofdstedelijk Gewest gebeurt.

2.10.7 Cumulatie met andere data

Tot slot wordt in de interviews frequent aangegeven dat het zinvol is om ANPR-data te combineren of cumuleren met andere databronnen. Er worden voorbeelden gegevens van publieke bewakingscamera's, sociale media, meldingen of informatie van burgers, GPS-coördinaten, telefoniegegevens, informatie van apps zoals app 112, informatie en camerabeelden van private bedrijven… Deze diversiteit aan databronnen kunnen complementair zijn aan ANPR-data. Voor wat betreft de aanwending ervan dient dit steeds te gebeuren met respect voor de privacy: "*De aanwending van technologie en respect voor privacy gaan hand in hand*".

2.11 Het knelpunt: het ontbreken van een passend wettelijk kader

De relevante wetgeving, zijnde (i) de Algemene Verordening Gegevensbescherming (beter bekend onder de Engelse afkorting "GDPR") en de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens die verder uitvoering geeft aan de GDPR in België, (ii) de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's ("Camerawet"), en (iii) de wet van 5 augustus 1992 op het politieambt ("WPA"), vormt een strikt wettelijk kader omtrent het gebruik van ANPR-camera's en het gebruik en delen van ANPR-data.

Het vandaag bestaand wettelijk kader laat geen ontsluiting toe van politionele gegevens, met inbegrip van ANPR-gegevens, naar niet-politionele overheden/instanties voor niet-politionele/justitiële doeleinden. Er bestaat dus geen wettelijke grondslag voor het ontsluiten van ANPR-data aan lokale besturen voor algemene beleidsdoeleinden zoals mobiliteit, milieu, klimaat, leefbaarheid, etc.

Teneinde die wettelijke basis te voorzien, lijkt de meest aangewezen optie een wijziging van de WPA, en in het bijzonder aanvulling van het huidig artikel 44/11/9 WPA. De nadere regels van dergelijke informatiedeling worden wellicht best vastgelegd in een uitvoeringsbesluit.

Deze studie laat ons toe de volgende suggestie voor wetswijziging te doen.

2.11.1 Wijziging van de WPA

2.11.1.1 Artikel 25/7 WPA

Artikel 25/7 WPA laat het toe om informatie en persoonsgegevens verzameld door middel van camera's in de zin van de WPA te anonimiseren en te gebruiken voor didactische en pedagogische doeleinden in het kader van de opleiding van de leden van de politiediensten.

> Vanuit privacy-oogpunt lijkt dit artikel enigszins overbodig. Anonieme gegevens (niet meer te linken aan een identificeerbare persoon) zijn immers geen persoonsgegevens. Wat er ook van zij, artikel 25/7 kan zo gelezen worden dat ander gebruik van deze geanonimiseerde gegevens, net zou zijn toegelaten. Daarnaast is er de problematiek van de partij die bestaande persoonsgegevens van de ANPR-camera's zou anonimiseren, wat op zich wel een verwerkging van persoonsgegevens is.

In een politionele context moet dit daarenboven wellicht ruimer gezien worden. Niet alleen persoonsgegevens maar ook politionele "informatie" in het algemeen wordt opgenomen in artikel 25/7. De heer Frank Schuermans (COC) stelt (over artikel 44/11/9 WPA waarin ook sprake is van persoonsgegevens en informatie): "*Voormeld artikel heeft het immers over alle persoonsgegevens en informatie. Van zodra er sprake is van politionele informatie, zelfs van informatie die geen persoonsgegevens zijn (maar bv. nummers, voorwerpen, enz …) is dat artikel van toepassing*.".[15] In diverse interviews gaven de respondenten ook mee dat het COC meent dat ook anonieme gegevens politiegegevens zijn en dus onder toepassing van de WPA/het toezicht van het COC vallen.

De wetgever zou ervoor kunnen opteren om dit artikel 25/7 WPA aan te vullen door ook "lokale besturen" toe te laten gebruik te maken van de geanonimiseerde gegevens voor een aantal welbepaalde doeleinden (beleid inzake mobiliteit, klimaat, leefbaarheid, etc.). Naast de politie in het kader van opleiding zouden dus ook lokale besturen op relatief eenvoudige manier toegang kunnen krijgen tot ANPR-data (en eventuele andere gegevens) voor deze ruimere beleidsdoeleinden.

Daarbij kan ook overwogen worden om te bekijken of niet enkel geanonimiseerde, maar ook gepseudonimiseerde gegevens, zoals gedefinieerd door de GDPR, zouden kunnen worden doorgegeven voor welomschreven doeleinden.[16] Evenwel - in het licht van het algemeen principe van "minimale gegevensverwerking" onder de GDPR – zullen redenen moeten worden aangedragen waarom de lokale overheden effectief nood hebben aan niet-geanonimiseerde gegevens voor de betrokken ruimere beleidsdoeleinden. Eventueel kan worden voorzien dat lokale overheden die wensen te werken met niet-anonieme gegevens, daartoe een afzonderlijke analyse zullen moeten maken en een afzonderlijke procedure zullen moeten doorlopen voor een bepaald project.

Naar ons weten (op basis van hetgeen wij hebben vernomen tijdens de interviews), heeft een aanvulling van artikel 25/7 WPA nooit op tafel gelegen.

2.11.1.2 Artikel 44/11/9 WPA

Artikel 44/11/9 WPA zou zodanig kunnen uitgebreid worden dat de openbare overheden (waarvan reeds sprake in de huidige versie van artikel 44/11/9 en waaronder dus ook steden en gemeenten vallen) niet louter met betrekking tot hun opdrachten van toepassing van de strafwet of wettelijke verplichtingen inzake de openbare veiligheid, maar ook met betrekking tot mobiliteit-, milieu-, leefbaarheidsbeleid, etc. toegang kunnen krijgen tot de gegevens in de zin van de WPA.

Aandachts- en mogelijke discussiepunten daarbij zijn:

- de definiëring van het begrip "openbare overheden" of eventueel de specificering naar "lokale besturen" (om de toegang desgewenst te beperken tot steden en gemeenten). Moeten ook andere actoren toegang kunnen krijgen? Men kan denken aan de havens, maar bijvoorbeeld

[15] Cf. de bewoording van de heer Frank Schuermans (in de schriftelijke antwoorden in het kader van deze studie).
[16] De WPA bevat geen eigen definitie van "pseudonimisering".

ook aan 'particuliere' initiatieven zoals een buurtnetwerk. Moet die mogelijkheid voorzien worden, of net uitdrukkelijk uitgesloten worden?;

- de bepaling van de "algemene beleidsdoeleinden" (moet men in de wet reeds verwijzen naar het beleid inzake mobiliteit, milieu, openbare werken, leefmilieu, etc., of is dit iets voor het uitvoeringsbesluit?). Kan men werken met subdoelstellingen (in de wet of wellicht eerder in het uitvoeringsbesluit) waarbij lokale overheden moeten kunnen aantonen (op basis van wettelijk vastgelegde criteria) dat het beoogde project valt onder een van de subdoelstellingen?;

- de uitdrukkelijke wettelijke bevestiging dat zowel anonieme als gepseudonomiseerde gegevens gedeeld kunnen worden, desgevallend onder welke voorwaarden, of eventueel, zij het onder zeer strikte voorwaarden en voor welbepaalde doeleinden, niet-gepseudonimiseerde gegevens;

- hoe kan men rekening houden met toekomstige ontwikkelingen in het kader van *smart city*-toepassingen (vermijden dat opnieuw wetswijzigingen vereist zijn van zodra de technologie of dagelijkse realiteit van bestuur van steden en gemeenten de wetgeving inhaalt)?

- kan een lokaal bestuur de ontvangen gegevens verder doorgeven (bijvoorbeeld aan verenigingen, buurtnetwerken, ondernemingen) en desgevallend onder welke voorwaarden, of moet dit expliciet wettelijk uitgesloten worden?

- **last but not least**: er zullen – in het licht van het algemeen principe van "minimale gegevensverwerking" onder de GDPR - redenen moeten worden aangedragen waarom de lokale overheden effectief nood hebben aan niet-geanonimiseerde gegevens voor de betrokken ruimere beleidsdoeleinden (zie punt 2.11.1.1 hierboven).

2.11.2 Centralisering boven decentralisering

Als lokale besturen ANPR-data opvragen/consulteren, moet dit dan gebeuren via een centrale aanpak waarbij er één centrale (federale?) databank bestaat die alle gegevens verzamelt en (al dan niet na anonimisering of pseudonimisering) doorgeeft conform de (nieuwe) wettelijke bepalingen, of behoudt men toch de mogelijkheid (of verplichting) om via de (bestaande of op te richten) lokale backoffices data te verkrijgen?

Huidig rapport toont aan dat er grote voorstanders en grote tegenstanders zijn van een centraal systeem. Er zijn inderdaad zowel voor- als nadelen aan beide systemen. Vanuit juridisch oogpunt is het ons inziens meest werkbare kader voor het delen van ANPR-data met lokale besturen te werken met een **centraal systeem**. Wij zien daarvoor de volgende redenen:

- Uniformisering, consistentie en professionele aanpak – Het lijkt onmogelijk om een uniform systeem op te zetten dat op gelijke wijze geldt voor alle lokale besturen als men rechtstreeks toegang verleent tot gegevens uit lokale backoffices met elk hun eigen specificiteit en niveau van beveiliging (zie verder hieronder). Een federaal systeem (en geen regionaal of provinciaal systeem) lijkt ons het meest geschikt in de federale materie waarin we ons bevinden.
- Deelname van alle politiezones en steden en gemeenten – Centraal beheer is de enige manier om het volledige ANPR-landschap op te nemen in een databank die beschikbaar is voor de steden en gemeenten. Het is onmogelijk om van alle (kleine) lokale zones een dergelijke inspanning te vragen die niet altijd in verhouding zal staan met de return die een kleinere gemeente zal krijgen.
- Waarborgen inzake veiligheid en bescherming van gegevens conform GDPR/richtlijnen toezichtsorganen – Tegenstanders van een centraal systeem halen vaak aan dat verschillende kleinere backoffices minder risicovol zijn wat betreft veiligheid ("als een lokaal systeem gehackt wordt, zijn er minder gegevens in gevaar dan wanneer hetzelfde gebeurt met een groot

centraal systeem"). Dit risico is uiteraard reëel en kan nooit geheel uitgesloten worden. Niettemin wordt ons inziens best geïnvesteerd in één centraal systeem met inbouw van de meest verregaande veiligheidsmaatregelen (desgevallend mede via financiering van de lokale niveaus). Eén professioneel beveiligd systeem heeft de voorkeur boven vaak minder veilige (omwille van bijvoorbeeld financiële redenen) lokale systemen.[17]

- Ons inziens kan de huidige praktijk van delen van ANPR-data tussen lokale politiezones en openbare besturen voor hun opdrachten inzake toepassing van de strafwet of wettelijke verplichtingen inzake de openbare veiligheid blijven bestaan. Het feit dat het delen van ANPR-data met lokale besturen voor niet-politionele/justitiële data via een centraal systeem moet gebeuren, doet geen afbreuk aan de bestaande afspraken (de kosten/inspanningen op lokaal niveau zijn o.i. niet verloren).
- Met het AMS bestaat reeds een federale databank (inspanningen zijn gedaan, kosten zijn gemaakt, uitrol is aan de gang). Er bestaat reeds een wettelijke verplichting om ANPR-data verzameld in een lokale backoffice door te sturen naar het AMS (cf. artikel 44/11/3sexies §2 WPA). Eén aanspreekpunt, één contractspartij die (desgevallend anonieme of gespeudominiseerde) gegevens aanlevert aan de diverse lokale overheden lijkt de meest eenvoudige aanpak. Artikel 25/7 WPA laat reeds toe om informatie en persoonsgegevens verzameld door middel van camera's in de zin van de WPA te anonimiseren en te gebruiken voor didactische en pedagogische doeleinden in het kader van de opleiding van de leden van de politiediensten – een uitbreiding daarvan lijkt dan ook voor de hand te liggen.

2.11.3 Uitvoering in de praktijk

Als men ervan uitgaat dat één centraal systeem zou bestaan met ANPR-gegevens dat geconsulteerd kan worden door de lokale besturen, hoe kan een lokaal bestuur dan aan de gegevens die het nodig heeft om een bepaald project te realiseren?

Een suggestie is het oprichten (via een uitvoeringsbesluit van de WPA (gewijzigd artikel 44/11/9)) van een **kruispuntbank** die instaat voor (i) het anonimiseren/pseudonimiseren van de ANPR-data en (ii) het verdelen van de gegevens aan de lokale besturen conform de wettelijk bepaalde doeleinden.

Over "wie" die kruispuntbank moet zijn, is geen eensgezindheid. Verschillende actoren die in het kader van deze studie bevraagd werden, zien een rol voor Informatie Vlaanderen in hun functie van "dataverzamelaar" voor Vlaanderen. De politie zelf (huidige beheerder van het AMS) botst wellicht op het ontbreken van middelen (o.m. personeel) om dergelijke niet-strikt politionele taken op zich te nemen (wat dan natuurlijk leidt tot de vraag naar beleidskeuzes ter zake en het daaraan koppelen van de nodige middelen). Alleszins, in de praktijk zal de concrete uitwerking (het anonimiseren/pseudonimiseren van gegevens, het opzetten van toegangspoorten voor gegevens en alle technische aspecten) wellicht toevertrouwd worden aan een externe dienstverlener, al dan niet in samenwerking met bijvoorbeeld Informatie Vlaanderen.

Omtrent het juridisch luik van het opzetten van een kruispuntbank kunnen zich de volgende vragen stellen:

- Worden alle data in de centrale databank meteen geanonimiseerd/gepseudonimiseerd (en hoe dan precies) of gebeurt dit enkel van zodra een aanvrager (lokaal bestuur) een bepaalde dataset nodig heeft? Vermoedelijk eerder het laatste, omdat men pas bij de aanvraag weet welke datasets men nodig heeft (tenzij men gebruik zou maken (voor zover juridisch en technisch mogelijk) van systemen die op continue basis data aanleveren (bijvoorbeeld omtrent parkeerbegeleiding)).

[17] Hoewel één van de geïnterviewden bij de GBA zich tijdens het interview niet wenste uit te spreken over de voorkeur voor een centrale of decentrale aanpak, gaf hij wel aan dat "een argument om wel te centraliseren is, vanuit privacy oogpunt is, dat je dan ook een meer professionele aanpak kunt hebben en dus beter beveiligde, en dus een betere beveiliging van die gegevens. Want als elke gemeente dat letterlijk voor zichzelf moet doen, of op zichzelf moet uitvissen hoe ze die data moeten beveiligen, dan gaan we een denk ik niet altijd optimaal beveiligde databank hebben."

- Komt dit systeem van kruispuntbank in de plaats van (het minder flexibel systeem van) "lijsten" op te maken door de bevoegde ministers (cf. artikel 44/11/9 WPA) of bestaan de systemen naast elkaar?
- Hoe moeten lokale besturen een aanvraag voor een bepaalde dataset indienen? Hoe moet die aanvraag eruit zien? Spreken we over een eenmalige aanvraag per categorie van gegevens, of een periodieke aanvraag (bijvoorbeeld jaarlijks te hernieuwen), of een aanvraag per specifiek project op lokaal niveau?
- Hoelang kunnen de lokale besturen de verkregen gegevens bijhouden en onder welke vorm (in het bijzonder wanneer het zou gaan om niet-anonieme gegevens)?
- Kunnen de lokale besturen de verkregen gegevens eventueel zelf doorgeven, en aan welke actoren en onder welke voorwaarden?
- Als Informatie Vlaanderen de "*trusted third party*" kan zijn voor Vlaanderen, wie moet die rol opnemen voor de andere regio's?

2.11.4 Geen afbreuk aan bestaande regels inzake bescherming van persoonsgegevens en GDPR

Uiteraard blijft de GDPR en de Belgische wet van 30 juli 2018 van toepassing telkens wanneer persoonsgegevens verwerkt worden voor die aangelegenheden die niet door bijzondere wetgeving worden geregeld. Het opzetten van een kruispuntbank of enige ander initiatief wijzigt de verplichtingen van lokale besturen op dat vlak niet.

Dit betekent dat de verwerking van de gegevens (minstens de gepseudonomiseerde gegevens, aangezien de GDPR niet van toepassing is op louter anonieme gegevens) moet plaatsvinden conform de basisprincipes van de GDPR (zie hieronder). Elke verwerking moet proportioneel zijn, de verwerkingsverantwoordelijke (lokaal bestuur) moet transparant zijn, etc.

Bovendien moet een lokaal bestuur nog steeds, indien zij meent dat er een verwerking een hoog risico inhoudt voor de vrijheden van natuurlijke personen, een DPIA (Gegevensbeschermingseffectbeoordeling) uitvoeren voorafgaand aan de verwerking van de gegevens (conform artikel 35 GDPR), wat evenwel ook kan worden opgenomen in bijzondere wetgeving.

Het feit dat er na een eventuele wetswijziging een wettelijke grondslag zou bestaan voor een verwerking (bijvoorbeeld een aangepast artikel 44/11/9 WPA) is dan ook geen vrijgeleide om de basisprincipes en verplichtingen van de GDPR verder naast zich neer te leggen. De eventuele gewijzigde wetgeving zou dit principe, voor zover nodig, nog kunnen onderlijnen.

2.11.5 Haalbaarheid – draagvlak voorgestelde wijziging

Deze studie zal aantonen dat er (groot) draagvlak bestaat voor het ontsluiten van ANPR-data naar lokale besturen voor algemene beleidsdoeleinden bij de steden en gemeenten, gesteund door meerdere actoren, maar ook bij de wetgever zelf.

Reeds van bij de opstart van het AMS was het naar wij begrijpen de uitdrukkelijke bedoeling om het AMS open te stellen voor bestuurlijke overheden voor andere dan de politionele/justitiële doeleinden, zoals mobiliteitsmanagement (maar dit is tot nu toe nog niet gebeurd).

Bovendien zou een aanvulling van artikel 44/11/9 WPA 'ooit' eens op tafel hebben gelegen, en daarover zou binnen de politie een voorstel van tekst hebben gecirculeerd. Men zou destijds de doeleinden van artikel 44/11/9 hebben willen uitbreiden naar 'monitorings- en rapporteringsopdrachten'. Het zou toen uitsluitend gegaan zijn om anonieme data (wat dus eigenlijk aansluit bij ons voorstel om eerder te kijken naar een uitbreiding van artikel 25/7 WPA).

Referenties

Advies DA190019 van 16 december 2019, https://www.controleorgaan.be/files/DA190019-NL.PDF

Billiet, T., & Colenbie, B. (2017). *Wat is de perceptie van de Vlaamse burger over de antiterreurmaatregelen die de Belgische overheid heeft genomen na de aanslagen in Parijs?* Masterthesis, UGent, Faculteit Economie en Bedrijfskunde

Crispel, M. (2020). De impact van de vaststellingen en aanbevelingen van de Parlementaire onderzoekscommissie Terroristische aanslagen op de lokale politie. In: D. Van Daele & L. Mergaerts (Eds.), *Naar een herijking van de Belgische veiligheidsarchitectuur: de vaststellingen en aanbevelingen van de Parlementaire onderzoekscommissie Terroristische aanslagen* (pp. 99-112). Antwerpen: Intersentia.

Decreet van 27 november 2015 betreffende lage-emissiezones waarbij het de gemeenten wordt toegestaan geanonimiseerde data te gebruiken of ter beschikking te stellen van derden om verkeers- en mobiliteitsstromen te analyseren en te rapporteren.

Decreet van 8 juni 2018 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).

De Hert, P. & De Schepper, T. (2018). Cameratoezicht, *Postal Memorialis*, 296, 2018.

Dodge, M. & Kitchin, R. (2007). *The automatic management of drivers and driving spaces*. Geoforum 38, 264-275.

Easton, M. (2019). Digitalisering brengt politie dichter bij de essentie van een gemeenschapsgerichte politiezorg. In: E. Devroe, A. Schmidt, L. G. Moor & P. Ponsaers (Eds.). *Cahier Politiestudies. De essentie van politiewerk* Antwerpen: Gompel & Svacina, 59 – 66.

Gegevensbeschermingsautoriteit. Zie: https://www.gegevensbeschermingsautoriteit.be/welke-gevallen-mag-ik-gebruik-maken-van-mobiele-bewakingscamera%E2%80%99s (FAQ) en https://www.gegevensbeschermingsautoriteit.be/mobiele-bewakingscameras, geraadpleegd op 13 april 2020.

Havadi, S., Buldeo Rai, H., Verlinde, S., Huang, H., Macharis, C., Guns, T. (2018), *Analysing passenger and freight vehicle movement from Automatic-Number Plate Recognition camera data*, MOBI Research groups, VUB.

Informatie Vlaanderen (2020). Zie: https://overheid.vlaanderen.be/informatie-vlaanderen geraadpleegd op 3 april 2020.

Inschrijving van voertuigen. Zie: https://mobilit.belgium.be/nl/wegverkeer/inschrijving_van_voertuigen, geraadpleegd op 3 april 2020.

Lage emissiezones (LEZ). Zie: https://www.vlaanderen.be/lage-emissiezones-lez, geraadpleegd op 21 april 2020.

Ministeriële omzendbrief van 10 december 2009 betreffende de Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, zoals gewijzigd door de wet van 12 november 2009.

Parlementaire vraag Nr 1448 van de heer Denis Ducarme aan de Vice-eersteminister en minister van Veiligheid en Binnenlandse Zaken, belast met de Regie der Gebouwen Veiligheid en Binnenlandse Zaken inzake Bewakingscamera's, QRVA 54 083, 15 juni 2016.

Simons, M. (2014). Praktijkcases van ANPR-gebruik in België. Het vaste ANPR-gebruik in België. *Politiejournaal, special issue ANPR,* 15 – 17.

s-LIM. Zie : https://www.s-lim.be/, geraadpleegd op 3 april 2020.

Strijd tegen terrorisme (19 november 2015). Zie: https://www.premier.be/nl/strijd-tegen-terrorisme-%E2%80%93-maatregelen-van-de-federale-regering-toespraak, geraadpleegd op 21 april 2020.

Uiteenzetting van de heer Arne Dormaels, directeur van het Vias institute, verslag van de mogelijke uitbreiding van de camerawet, namens de Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt uitgebracht door de heer Eric Thiébaut en mevrouw Sandrine De Crom, 26 april 2019, DOC 54 3727/001.

Uiteenzetting van de heer Arne Dormaels, directeur van het Vias institute, verslag van de mogelijke uitbreiding van de camerawet, namens de Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt uitgebracht door de heer Eric Thiébaut en mevrouw Sandrine De Crom, 26 april 2019, DOC 54 3727/001.

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).

Viapass. Zie: https://www.viapass.be, geraadpleegd op 3 april 2020.

Vlaamse Toezichtscommissie. Zie https://overheid.vlaanderen.be/taken-vlaamse-toezichtcommissie, geraadpeegd op 13 april 2020.

VRT NWS, 2020, Politie Zennevallei na diefstallenplaag: "Wij mogen een 30-tal slimme camera's niet gebruiken door vacuüm in wetgeving". Zie: https://www.vrt.be/vrtnws/nl/2020/03/11/politiezone-zennevallei-na-diefstallenplaag-wij-mogen-een-30-t/, geraadpleegd op 11 maart 2020.

VVSG. Zie: https://www.vvsg.be/, geraadpleegd op 3 april 2020.

Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.

Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's.

Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit. Zie: https://www.gegevensbeschermingsautoriteit.be/beslissingen, geraadpleegd op 13 april 2020.

Wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid.

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Vias institute
Haachtsesteenweg 1405, 1130 Brussel · Chaussée de Haecht 1405, 1130 Bruxelles · +32 2 244 15 11 · info@vias.be · www.vias.be