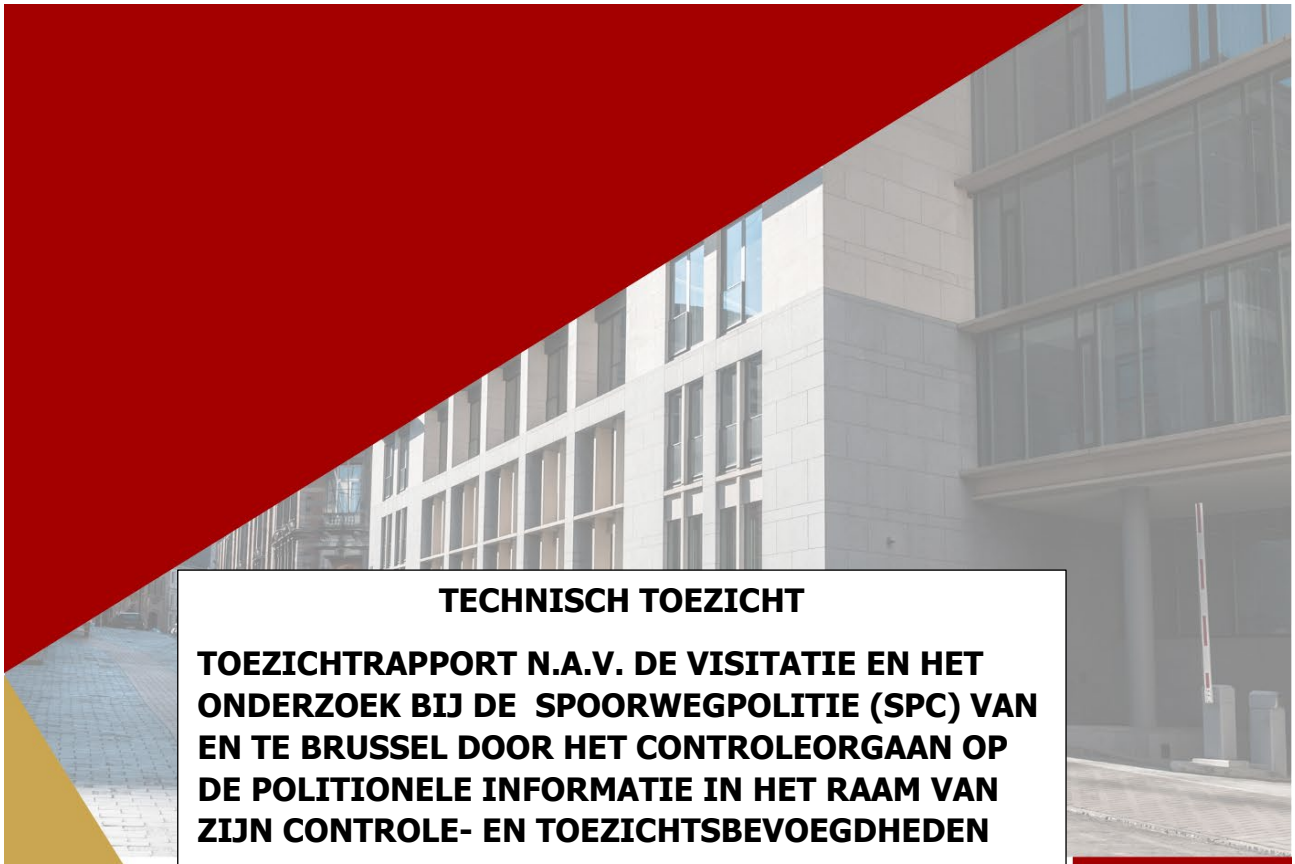


TECHNISCH TOEZICHT

TOEZICHTRAPPORT N.A.V. DE VISITATIE EN HET ONDERZOEK BIJ DE SPOORWEGPOLITIE (SPC) VAN EN TE BRUSSEL DOOR HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE IN HET RAAM VAN ZIJN CONTROLE- EN TOEZICHTSBEVOEGDHEDEN

RAPPORT

Referte: CON20004

0 Inhoud

1 INLEIDING

1. Gelet op zijn bevoegdheden als externe controledienst en bevoegde toezichthoudende autoriteit ten aanzien van de gegevensverwerkingen door de geïntegreerde politie (GPI) heeft het Controleorgaan op de politionele informatie ('Controleorgaan' of 'COC') beslist een visitatie te verrichten bij SPC[1] Brussel in het raam van een zgn. 'technisch toezicht'[2]. Onderhavig verslag heeft betrekking op de onderzoeksbevindingen van dit toezicht. Dit rapport is het gevolg van de vaststellingen tijdens de visitatie bij SPC als verwerkingsverantwoordelijke. De conclusies onder de vorm van verzoeken, aanbevelingen en corrigerende maatregelen zijn de gevolgen van deze vaststellingen en zijn dientengevolge gericht aan de SPC in de hoedanigheid van verwerkingsverantwoordelijke enerzijds, maar ook aan de verantwoordelijken op beleidsmatig niveau anderzijds.

1.1 De bevoegdheden van het Controleorgaan op de politionele informatie

[1] **S**poorweg**P**olitie / **P**olice des **C**hemins de fer.

[2] Het COC maakt een onderscheid tussen meerdere vormen van controles of toezicht. Het COC doet ofwel een:

- **Globaal Toezicht**: dit is een controleonderzoek dat gepaard gaat met één of meerdere doorgedreven plaats bezoeken of visitaties waarbij de scope van de controle zeer ruim is.
- **Thematisch Toezicht**: zoals de benaming aangeeft wordt een onderzoek gedaan naar één bepaald thema, waarbij zowel deskresearch als bezoeken ter plaatse mogelijk zijn.
- **Technisch Toezicht**: deze controles beperken zich in hoofdzaak tot nazicht van de wettigheid, volledigheid en correctheid van de vattingen en verwerkingen in de politionele gegevensbanken.
- **Beperkt Toezicht**: deze controles behandelen één of slechts enkele (deel)aspecten van een politionele of niet politionele gegevensverwerking.
- **Internationaal Toezicht**: dit zijn de eventuele Internationale onderzoeken waaraan het COC zijn medewerking verleent.
- **Bijzonder Toezicht**: dit betreft onderzoeken en controles in bijzondere materies, zoals de jaarlijkse controles op de gemeenschappelijke gegevensbanken terrorisme en extremisme.

2. De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WGB)[3] heeft het Controleorgaan hervormd tot onder meer een volwaardige toezichthoudende autoriteit, bovenop de bestaande controlerende bevoegdheden inzake politionele informatiehuishouding zoals voorzien in de Wet van 5 augustus 1992 op het Politieambt (WPA). In artikel 71 § 1 en de titels II en VII WGB worden de opdrachten en de bevoegdheden van het COC omschreven. Daarin wordt tevens verwezen naar de controleopdrachten vervat in de artikelen 44/1 tot en met 44/11/14 WPA inzake de informatiehuishouding van de politiediensten. Op die manier heeft het Controleorgaan een toezichthoudende en een controlerende opdracht. Dit betekent dat, naast privacy en gegevensbescherming, het COC ook aandacht heeft voor elementen als efficiëntie en effectiviteit van de informatiehuishouding en het politieoptreden. Het COC heeft op grond van bovenstaande regelgeving derhalve een algemene toezichtsbevoegdheid op alle operationele en niet operationele (persoons)gegevensverwerkingen door de GPI.

Het Controleorgaan is bevoegd voor de politiediensten[4], de Algemene inspectie van de federale en lokale politie (AIG)[5] en de Passagiersinformatie-eenheid (PIE)[6]. De toezichtbevoegdheid van het Controleorgaan, wat betreft de politiediensten, omvat zoals gezegd zowel de operationele als niet-operationele verwerkingsactiviteiten[7].

Wat de controleopdracht betreft, is het Controleorgaan belast met de controle van de verwerking van de informatie en de gegevens bedoeld in artikel 44/1 WPA, met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2 en elke andere opdracht die haar door of krachtens andere wetten wordt verleend.

In dit raam gaat het COC over tot vaststellingen, en kan het overgaan tot vragen, aanbevelingen, waarschuwingen en/of corrigerende maatregelen (met dwingend karakter) als «*ultimum remedium* » indien het COC inbreuken vaststelt op de toepasselijke regelgeving.

Het Controleorgaan is in het bijzonder belast met de controle van de naleving van de regels inzake de rechtstreekse toegang tot de Algemene Nationale Gegevensbank (ANG) en de rechtstreekse bevraging ervan, alsook van de naleving van de in artikel 44/7, 3e lid WPA bedoelde verplichting, voor alle leden van de politiediensten, tot voeding van deze gegevensbank.

Het Controleorgaan gaat door middel van onderzoek naar de werking na of de inhoud van de ANG en de procedure voor de verwerking van de daarin bewaarde gegevens en informatie overeenkomen met het bepaalde in de artikelen 44/1 tot 44/11/14 WPA en met hun uitvoeringsmaatregelen.

In het raam van het gebruik van niet-zichtbare camera's fungeert het Controleorgaan als een soort "BAM"-commissie[8]. Overeenkomstig 46/6 van de WPA moet elke toestemming en verlenging voor niet-zichtbaar gebruik van camera's in de gevallen bedoeld in artikel 46/4 worden meegedeeld aan het Controleorgaan, behalve wanneer het gebruik van camera's wordt uitgevoerd onder het gezag van een magistraat. Daarbij moet het Controleorgaan onderzoeken of voldaan is aan de voorwaarden voor de beslissing, de verlenging of de uitvoering van de maatregel.

[3] *BS*, 5 september 2018. Deze wet bevat tevens bepalingen die uitvoering geven aan 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 het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming), hierna de AVG, en de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (hierna de Richtlijn politie-justitie of *LED* (***L**aw **E**nforcement **D**irective*)).

[4] Zoals gedefinieerd in artikel 2, 2° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (Wet Geïntegreerde Politie) en art. 26, 7°, a WGB.

[5] Zoals gedefinieerd in artikel 2 van de wet van 15 mei 2007 op de Algemene Inspectie houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten en art. 27, 7°, d WGB.

[6] Zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens en art. 26, 7°, f WGB. Ook wel aangeduid als *BELPIU'* (*Belgian Passenger Information Unit*).

[7] Art. 4 § 2 4e lid, wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (WOG).

[8] BAM staat voor '**B**ijzondere **A**dministratieve **M**ethoden'.

Daarnaast neemt het Controleorgaan kennis van klachten en beslist het over de gegrondheid ervan[9]. In dat verband beschikken de leden en de leden van de dienst Onderzoeken (DOSE)[10]van het Controleorgaan over onderzoeksbevoegdheden en kunnen corrigerende maatregelen worden genomen[11].

Tegen bepaalde beslissingen van het Controleorgaan staat binnen de dertig dagen een jurisdictioneel beroep open bij het Hof van Beroep van de woonplaats of de zetel van de eiser, die de zaak behandelt zoals in kort geding overeenkomstig de artikelen 1038, 1040 en 1041 van het Gerechtelijk Wetboek[12].

2 OPZET VAN HET TOEZICHT EN METHODOLOGIE

3. Op 18 mei 2021 heeft het Controleorgaan op eigen initiatief een technisch toezicht[13]uitgevoerd bij de SPC Brussel. Dit toezicht is derhalve niet het gevolg van een (individuele) klacht of het bestaan van (concrete) aanwijzingen over het niet naleven van de wet- en regelgeving door de gevisiteerde politiedienst. Gezien de vaststellingen ter plaatse werd voor bepaalde verwerkingen, hoofdzakelijk in het raam van de beeldverwerking, buiten de initiële scope van het louter technisch toezicht gegaan en hebben de vaststellingen dienaangaande aanleiding gegeven tot een diepere analyse met daaruit voortvloeiende aanbevelingen, verzoeken en corrigerende maatregelen ten aanzien van de verwerkingsverantwoordelijke SPC enerzijds en de verantwoordelijken op beleidsmatig niveau anderzijds.

4. Gelet op de omvang, de aard van de gegevens en de vorm van de verwerkingen in het raam van het gebruik van camera's, het gebruik van de ANG, het oprichten van bijzondere gegevensbanken, de toegang tot specifieke gegevensbanken van externe partners en de gerechtelijke aanhoudingen binnen de politie en de daarbij horende zgn. 'triptiek'[14], gaat het bij dergelijke gegevensverwerkingen om een verregaande inmenging in de persoonlijke levenssfeer. Met het oog op een correcte informatie-inwinning zijn deze verwerkingen gekoppeld aan uitvoeringsvoorwaarden die beschreven worden in de wetgeving (voornamelijk de WPA en de WGB), uitvoeringsbesluiten en richtlijnen (waaronder voornamelijk de zgn. MFO3 en het bijhorende Vademecum). Er wordt door het COC nagegaan of het politionele cameragebruik conform de toepasselijke regelgeving verloopt, of de bijzondere gegevensbanken volgens de toepasselijke regels in het leven geroepen werden, of er al dan niet toegang is tot gegevensbanken van externe partners en of de uitvoering van de gerechtelijke aanhoudingen en triptiek in overeenstemming is met de toepasselijke regelgeving en op een kwalitatieve manier gebeurt.

5. Met een technisch toezicht beoogt het COC een inzicht te verwerven in bepaalde werkingsprocessen van de SPC Brussel met betrekking tot de politionele informatiehuishouding. Dit toezicht met visitatie werd *in casu* afgebakend tot volgende specifieke thema's:

- Het politioneel cameragebruik:
  - toepassing van het wetgevend kader;
  - operationeel gebruik.
- Databanken:
  - registratie van verwerkingen in REGPOL[15];
  - gebruik ANG;
    - toekenning profielen;
    - beleid inzake raadpleging en onrechtmatige toegang;
  - gebruik basisgegevensbanken;

[9] Art. 240, 4° WGB.
[10] **D**ienst **O**nderzoeken / **S**ervice d'**E**nquête.
[11] Art. 244 en 247 WGB.
[12] Art. 248 WGB.
[13] Een technisch toezicht is een hoofdzakelijk operationeel-politioneel technisch onderzoek met telkens één of meerdere specifieke onderwerpen, zoals de 'controle van de triptiek', 'de ANG-voeding', de 'onrechtmatige toegang/logging' (zie ook artikel 236 §3 en artikel 239 WGB). Dit soort toezicht is minder gericht op juridische aspecten of aspecten van gegevensbescherming of privacy zonder dat deze evident uit het oog worden verloren (zie ook voetnoot 1).
[14] De triptiek betreft het afnemen van vinger- en handpalmafdrukken, het nemen van foto's en het opstellen van de individuele beschrijving om tot een identificatie van een persoon te komen.
[15] REGPOL is het unieke register van de verwerkingen van de persoonsgegevens opgericht op niveau van de geïntegreerde politie, zoals bedoeld in artikel 145 van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

  - gebruik bijzondere gegevensbanken;
  - gebruik internationale gegevensbanken;
  - gebruik gegevensbanken NMBS[16] en/of INFRABEL[17];
  - het verloop van het functioneel beheer bij SPC:
    - relatie met SICAD-AIK[18];
    - afhandeling dossiers onrechtstreekse toegang.
- Vingerafdrukken:
  - afname vingerafdrukken van asielzoekers;
  - communicatie met DVZ[19]in het raam van EURODAC[20].

6. Het toezicht viel uiteen in twee fasen.

2.1 De eerste fase

In de eerste fase werd het technisch toezicht kenbaar gemaakt aan de betrokken politiedienst, werden vragenlijsten overgemaakt en stukken opgevraagd. Afhankelijk van de inhoud van de antwoorden en stukken werden specifieke bijvragen gesteld met het oog op nader onderzoek tijdens de visitatie.

In casu verstuurde het COC de aankondiging van het onderzoek met visitatie alsmede de vragenlijst op 30-03-2021.

Voorafgaand aan deze aankondiging verstuurde het COC een vraag aan CG/ISPO[21] inzake het ontbreken van registraties aangaande SPC verwerkingen in het register REGPOL.

Het COC ontving van de genoemde diensten, zoals gevraagd, onderstaande antwoorden en documenten:

- op 14-04-2021: van SPC Brussel, de melding dat het dossier zou beheerd worden door de centrale directie van SPC met SPC Brussel in steun;
- op 14-04-2021: van CG/ISPO, de melding dat er in het register voorafgaand aan de oprichting van het REGPOL register in 2018 nog een aantal vattingen van bijzondere gegevensbanken (GBO) uit hoofde van SPC aanwezig waren, doch dat de conversie ervan nog diende te gebeuren. Gezien er nog eenheden in deze situatie verkeerden engageerde CG/ISPO zich de betrokken DPO hierom te verzoeken;
- op 12-05-2021 van SPC: een uitgebreide documentatie over interne richtlijnen in wording, doch evenwel geen antwoorden op de gestelde vragen;
- op 15-05-2021 van SPC: een aantal antwoorden op de gestelde vragen. Deze waren door een administratieve vergissing niet op 12-05-2021 verstuurd.

2.2 De tweede fase

De tweede fase had betrekking op het onderzoek ter plaatse (de visitatie).

In casu verliep dit bezoek aan de SPC Brussel als volgt:

1. een introductie van het COC en de aanwezige leden van zowel de Algemene Directie DGA waaronder de SPC ressorteert, de (centrale) directie SPC en SPC Brussel;
2. een algemene inleiding door SPC:
   a. actieplan SPC;
   b. organogram Directie SPC;

[16] **N**ationale **M**aatschappij der **B**elgische **S**poorwegen.
[17] Infrastructuurbeheerder van de Belgische spoorwegen.
[18] Het AIK is de tweede pijler van de SICAD werking; deze staat in voor de verwerking van de informatie in tweede lijn.
[19] **D**ienst **V**reemdelingen **Z**aken
[20] Eurodac is een databank met vingerafdrukken van asielzoekers die wordt gebruikt ter ondersteuning van het gemeenschappelijk asielbeleid van de Europese Unie (EU). De Eurodac-database is opgericht in 2003. Wanneer een persoon asiel aanvraagt in een lidstaat van de Europese Unie of op een niet-regulier wijze vanuit een niet-EU land de grens van de Europese Unie passeert, worden de vingerafdrukken afgenomen en opgeslagen in Eurodac.
[21] ***I**nformation **S**ecurity and **P**rivacy **O**ffice van het commissariaat generaal.*

c. organogram SPC Brussel;
3. bespreking cameragebruik door SPC Brussel
4. bespreking gebruik databanken;
5. bespreking afname vingerafdrukken/EURODAC;

Op 09-06-2021 verstuurde het COC bijkomende vragen inzake de tijdens de visitatie getoonde documentatie. SPC verstuurde de antwoorden op deze vragen op 14-06-2021.
Op 17-06-2021 nam het COC kennis van een persbericht van Infrabel inzake het gebruik van *ANPR*[22] camera's op spoorwegovergangen.
Op 27-08-2021 werd het ontwerp-verslag voor overmaking in prelectuur goedgekeurd door het DIRCOM van het COC.
Op 01-09-2021 werd het ontwerp-verslag in prelectuur overgemaakt aan de directie SPC in het raam van de tegenspraak.
Op 22-09-2021 ontving het COC de bemerkingen van de directie SPC op het ontwerp-verslag en werden deze verwerkt en waar nodig toegelicht.
Op 09-11-2021 werd het definitief verslag goedgekeurd door het DIRCOM COC.

3 JURIDISCH KADER

3.1 Camerabewaking door de politie

3.1.1 Rechtsgrond

7. Sinds de aanpassingswet van de WPA van 21 maart 2018 kan de beslissing om in de openbare ruimtes camera's te plaatsen nog enkel door een openbare overheid worden genomen, zoals de gemeente[23]. Wanneer de politie gebruik maakt van camerabewaking zijn de bepalingen van de WPA van toepassing, behalve wanneer het gebruik van camera's in andere wetgeving wordt geregeld[24].

3.1.2 Verwerkingsverantwoordelijke

8. In het gegevensbeschermingsrecht is een belangrijke rol weggelegd voor de 'verwerkingsverantwoordelijke'. Het is "*de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*"[25]. Wat betreft de verwerkingsactiviteiten in het raam van de opdrachten van bestuurlijke en gerechtelijke politie wordt de verwerkingsverantwoordelijke in de WGB afgebakend tot de "*de 'bevoegde overheid' die, alleen of samen met andere, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doeleinden van en de middelen voor die verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, is de verwerkingsverantwoordelijke de entiteit die door of krachtens de wet, het decreet of de ordonnantie als de verwerkingsverantwoordelijke wordt aangewezen*"[26]. Onder de "*bevoegde overheden*" wordt begrepen "*a) de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus*"[27].

9. Hoewel aan de verwerkingsverantwoordelijke in de WPA op bepaalde plaatsen een (specifieke) rol wordt toebedeeld, is dat niet het geval wat betreft het cameragebruik. Zoals hiervoor gesteld is de verwerkingsverantwoordelijke een essentiële actor bij de verwerking van persoonsgegevens. Hij moet namelijk aantonen dat de persoonsgegevens in

[22] ***A**utomatic **N**umber **P**late **R**ecognition.*
[23] Wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiedienst te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling en van de plaatsing en het gebruik van bewakingscamera's, de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *BS*. 16 april 2018.
[24] Zoals trajectcontrole, die onder de toepassing van de wet van 16 maart 1968 betreffende de politie op het wegverkeer valt (Parl. St. *Kamer* 2017-2018, nr. 54-2855/001, 9). Ook de *real time* toegang tot beelden van bewakingscamera's van het net van openbare vervoersmaatschappijen wordt geregeld conform art 9 van de Camerawet van 21 maart 2007.
[25] Art. 4. 7) AVG.
[26] Art. 26, 8° WGB.
[27] Art. 26, 7° WGB.

overeenstemming met het wettelijk kader worden verwerkt[28]. Hij, zijn aangestelde of gemachtigde, is ook de persoon tegenover wie eventuele corrigerende maatregelen kunnen worden opgelegd of tuchtrechtelijke dan wel strafrechtelijk kan aangesproken worden[29]. De korpschef is de verwerkingsverantwoordelijke voor het bewaren van camerabeelden in een lokale technische gegevensbank[30].

De korpschef of directeur is ook de verwerkingsverantwoordelijke voor de bijzondere gegevensbanken[31]. In bijzondere gegevensbanken worden gegevens opgeslagen die niet in aanmerking komen om in de ANG opgenomen te worden, hoewel de gegevens een operationele behoefte hebben. Voorbeelden van een bijzondere gegevensbank zijn (1) de opslag van telefoonnummers of *ANPR* gegevens die verzameld zijn in het kader van een strafonderzoek[32] en (2) van klassieke camerabeelden. Het betreft gegevens die in verband staan met de opdrachten van bestuurlijke en gerechtelijke politie, maar niet *ipso facto* in de ANG moeten geregistreerd/gevat worden[33]. Wat deze laatste betreft dient verwezen te worden naar artikel 25/6 WPA dat alleen bepaalt dat de informatie en persoonsgegevens voor maximum twaalf maanden kunnen worden bewaard[34]. Er wordt voor de opslag van de gegevens echter geen verwerkingsverantwoordelijke aangeduid.

Het Controleorgaan is van oordeel dat het hier (tevens) een bijzondere gegevensbank betreft waardoor de korpschef of directeur als verwerkingsverantwoordelijke beschouwd moet worden. Artikel 44/4 § 1, 3e lid WPA bepaalt immers dat de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs de verwerkingsverantwoordelijke zijn voor de bijzondere gegevensbanken die zij oprichten doordat zij de doeleinden en middelen bepalen. De aanduiding van de korpschef als verwerkingsverantwoordelijke sluit overigens aan bij de geest van de bepalingen van de WPA inzake de oprichting van lokale gegevensbanken. Volgens artikel 25/5 WPA wordt de beslissing om camerabewaking in te zetten genomen door de bevoegde politieambtenaar en onder zijn verantwoordelijkheid. Indien dit niet de korpschef of de directeur is, handelt de bevoegde politieambtenaar onder de verantwoordelijkheid van de korpschef of directeur. De korpschef is immers, op grond van artikel 44 Wet Geïntegreerde Politie[35], verantwoordelijk voor de uitvoering van het lokaal politiebeleid, en meer bepaald, voor de uitvoering van het zonaal veiligheidsplan en verantwoordelijkheid voor de leiding, de organisatie en de verdeling van de taken binnen het lokaal politiekorps en de uitvoering van het beheer van dit korps[36].

De korpschef, directeur of diensthoofd is dus de verwerkingsverantwoordelijke voor wat betreft alle vormen van cameragebruik binnen zijn of haar politiezone of -dienst.

3.1.3 Procedurele vereisten

10. Vooraleer een politiedienst camerabewaking op het grondgebied van een gemeente wenst in te voeren, heeft zij daartoe de principiële toestemming van de gemeenteraad nodig[37]. Voor de diensten van de federale politie is dit de minister van Binnenlandse zaken of zijn gemachtigde[38]. Er is evenwel geen toestemming vereist voor het gebruik van camera's op besloten plaatsen waarvan de politie zelf de beheerder is, zoals een politiecommissariaat[39]. Het is van belang er op te wijzen dat, wanneer de toestemming van de gemeenteraad reeds vóór de wetswijzing van 21 maart

[28] Art. 50, 2e lid WGB.
[29] Zie de artikelen 221 juncto 247 WGB. Concreet kan het Controleorgaan onder meer de volgende corrigerende maatregelen nemen (art. 58.2, AVG):
- een waarschuwing geven;
- een berisping geven;
- gelasten om binnen een bepaalde termijn de verwerking in overeenstemming te brengen met wet het wettelijk kader;
- tijdelijke of definitieve verwerkingsbeperking of verwerkingsverbod opleggen.
[30] Art. 44/11/3*sexies* § 1, 2de lid WPA.
[31] Artikel 44/4 § 1, 3e lid WPA.
[32] MERCURE.
[33] Art. 44/11/3 WPA.
[34] Er wordt volledigheidshalve opgemerkt dat de WPA geen vaste bewaartermijn oplegt voor de gegevens die in bijzondere gegevensbanken worden opgeslagen (art. 44/11/3, § 4 WPA). Doordat artikel 25/6 WPA een maximum van 12 maanden oplegt, wordt daarmee ook de maximumtermijn gesteld aan deze bijzondere gegevensbank.
[35] Voor de federale politie kan verwezen worden naar de artikelen 99 tot en met 105 WGP.
[36] Zie ook en meer in detail, Advies uit eigen beweging van het COC DD200026 dd. 11.02.2021 met betrekking tot de vraag wie de verwerkingsverantwoordelijke is voor gegevensverwerkingen door de politiediensten in het kader van de uitvoering van politionele opdrachten enerzijds en voor gegevensverwerkingen onder de AVG anderzijds, https://www.controleorgaan.be/files/DD200026_Verwerkingsverantwoordelijke_GPI_N.PDF.
[37] Art. 25/4 § 1, 1° WPA.
[38] Art 25/4 § 1, 2° WPA
[39] Memorie van Toelichting bij deze wet, p. 21 (Parl. St. *Kamer* 2017-2018, nr. 54-2855/001).

2018 werd verkregen onder de toepassing van de camerawet van 2007, de toestemming niet opnieuw van de gemeenteraad verkregen moet worden[40]. Deze initieel verkregen toestemming blijft dus geldig. Dezelfde toestemming kan evenwel niet gebruikt worden voor het gebruik van nieuwe types van camera's die door de wet van 21 maart 2018 werden ingevoerd. Zo legt de WPA specifieke voorwaarden op voor het gebruik van tijdelijk vaste camera's waarover de gemeenteraad zich moet uitspreken[41]. In dat geval moet er dus een nieuwe, of aanvullende, toestemming van de gemeenteraad verkregen worden.

3.1.4 Bewaartermijn van de beelden

11. De camerabeelden kunnen maximaal 1 jaar worden bewaard[42]. De wet bepaalt geen minimumtermijn. Wat de klassieke camerabeelden betreft, bepaalt de WPA niet op welke gegevensdrager de beelden moeten opgeslagen worden. Daarom is het aangewezen dat de korpschef in het register met betrekking tot de verwerking van persoonsgegevens, zoals geregeld in artikel 55 WGB, aangeeft op welke gegevensdrager de beelden worden opgeslagen. Deze gegevensdrager moet toegankelijk zijn voor het Controleorgaan.

3.1.5 Technische gegevensbanken

12. Het is ter zake van belang te vermelden dat voor het gebruik van *ANPR* camera's een specifieke regeling geldt. Het gaat om "*intelligente camera's*", met name "*camera's die ook software bevat die al dan niet gekoppeld wordt aan registers of bestanden, de verzamelde beelden al dan niet autonoom kunnen verwerken*"[43]. Wanneer *ANPR* camerabewaking wordt toegepast, moeten de beelden in een "*technische gegevensbank*" worden opgeslagen,[44] waarbij de persoonsgegevens en informatie tevens worden doorgezonden naar de nationale technische gegevensbank[45]. De beelden kunnen maximum een jaar worden bewaard en ook hier is geen minimumtermijn bepaald[46].

De technische gegevensbank bevat, indien ze verschijnen op de beelden, de volgende gegevens[47]:
1) de datum, het tijdstip en de precieze plaats van langsrijden van de nummerplaat;
2) de kenmerken van het voertuig dat verbonden is aan deze nummerplaat;
3) een foto van de nummerplaat aan de voorkant van het voertuig en in voorkomend geval[48], aan de achterkant;
4) een foto van het voertuig;
5) in voorkomend geval[49], een foto van de bestuurder en van de passagiers;
6) de loggingsgegevens van de verwerkingen.

Deze gegevens moeten dus in de technische gegevensbank worden opgenomen voor zover *ANPR* beelden deze gegevens bevatten.

13. De principes met betrekking tot de koppelingen en de correlaties van de technische gegevensbanken met gegevensbanken bedoeld in artikel 44/2 §§ 1 en 2 WPA of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen conform artikel 44/4 §6 WPA worden geregeld door de richtlijn koppelingen en correlaties *ANPR*[50]. Koppelingen en correlaties dienen met name rekening te houden met:

- de criteria tijd, ruimte en frequentie zoals bepaald in artikel 44/4 §6 WPA;
- de registratie van de noodzakelijke toestemmingen in het register van de verwerkingen REGPOL;

[40] Art. 88 wet van 21 maart 2018 en Memorie van Toelichting bij deze wet, p. 113-114 (Parl. St. *Kamer* 2017-2018, nr. 54-2855/001).
[41] Art. 25/4 § 2, 2de lid WPA.
[42] Art. 25/6, 44/11/3*decies* § 2, 1e lid, en 46/12, 1e lid WPA.
[43] Art. 25/2 § 1, 3°, *juncto* 44/2 § 3, 3e lid WPA.
[44] Art. 44/2 § 3, 1e lid, WPA.
[45] Art. 44/11/3*sexies* WPA.
[46] Art. 44/11/3*decies* § 2, 1e lid WPA.
[47] Art. 44/11/3*decies* § 1 WPA.
[48] « *In voorkomend geval* » verwijst naar de technische mogelijkheid van de camera zulks al dan niet te doen.
[49] *Ibid*.
[50] Gemeenschappelijke bindende richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de bepaling van de nadere regels voor de toereikende, terzake dienende en niet overmatige maatregelen met betrekking tot de koppeling of correlatie van de technische gegevensbanken ingevolge het gebruik van intelligente camera's en systemen voor de automatische nummerplaatherkenning, bedoeld in artikel 44/2, § 3 van de wet op het Politieambt, met de gegevensbanken bedoeld in artikel 44/2, §§ 1 en 2 WPA, of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden, *BS,* 28 januari 2021.

- de noodzaak een transparante procedure aan te nemen die kan worden geaudit wanneer de politie-eenheden gebruik maken van lijsten of uittreksels buiten de nationale standaarden die zij koppelen met de lokale *ANPR's* en de nationale *ANPR* teneinde vergelijkingen te maken;
- de noodzaak om in geval van een *hit* (positieve correlatie) het nationale actiebeleid en een gericht interventiebeleid te volgen;
- de noodzaak terug te keren naar de authentieke bron in geval van een *hit* op een nummerplaat gedetecteerd met behulp van een lijst of uittreksel ingevoerd in een lokale of nationale technische gegevensbank, tenzij de correlatie *in real time* met de authentieke bron gebeurt.

3.1.6 Toegang tot de beelden

14. De toegang tot de beelden is afhankelijk van de finaliteit en gelijk geregeld voor zowel de gewone camerabewaking als voor het gebruik van *ANPR*-camera's. In beide gevallen kunnen de beelden maximum 12 maanden worden bewaard. Wat betreft de opdrachten van bestuurlijke politie is de toegang beperkt tot de eerste maand na de registratie van de beelden. Voor opdrachten van gerechtelijke politie zijn de beelden over de volledige bewaartermijn toegankelijk, waarbij na de eerste maand de tussenkomst van de procureur des Konings is vereist[51]. De toegang moet gemotiveerd en operationeel noodzakelijk zijn voor het uitvoeren van een specifieke opdracht[52]. Dit komt erop neer dat de toegang tot de beelden alleen toegelaten is voor personen die deze persoonsgegevens en informatie nodig hebben en wanneer daartoe dus een concreet operationeel belang aanwezig is[53].

15. Met betrekking tot het recht tot toegang tot de beelden van iedere gefilmde persoon is het recht op onrechtstreekse toegang zoals voorzien in art 42 WGB van toepassing indien het gaat om beelden die voor operationele doeleinden worden verwerkt. De WPA bevat evenwel geen regeling met betrekking tot de rechten van de politieambtenaar of de burger in verband met de toegang tot de beelden in de hypothese dat de beelden en de audio niet voor operationele doeleinden worden gebruikt (dus bijvoorbeeld niet als basis dienen voor de opmaak van een proces-verbaal). Wanneer de beelden niet relevant zijn voor de opdrachten van bestuurlijke of gerechtelijke politie, en dus geen operationeel belang hebben, verzet de WPA er zich evenmin tegen dat de verantwoordelijke politiezone zelf een recht van toegang tot de beelden organiseert[54]. Daarbij kan het systeem van toegang naar analogie met de Camerawet van 21 maart 2007 als voorbeeld dienen waarbij niet alleen de politieambtenaar maar ook de burger zich in eerste orde rechtstreeks tot de betrokken politiedienst wendt.

3.1.7 Zichtbaar en niet-zichtbaar gebruik van camera's

16. Zichtbare camera's zijn camera's waarvan het gebruik wordt aangekondigd door pictogrammen; de camera's zijn gemonteerd in als zodanig herkenbare politievoertuigen, -vaartuigen, -luchtvaartuigen of elk ander vervoermiddel van de politie of worden gedragen door politieambtenaren die als zodanig herkenbaar zijn[55]. In uitzonderlijke situaties kan de politie heimelijk gebruik maken van camera's (niet-zichtbaar gebruik). Daarbij kan de camera gedragen worden door de politieambtenaar of in een anoniem politievoertuig geplaatst zijn. Er is sprake van een anoniem politievoertuig wanneer het politievoertuig niet als zodanig herkenbaar is. In dat geval is er dus sprake van "*niet-zichtbaar*" cameragebruik[56]. De toepassing van niet-zichtbare camera's is strikt geregeld en beperkt tot vier situaties. Met name:
1) omwille van bijzondere omstandigheden, met name bij grote volkstoelopen met het oog op het inwinnen van informatie van bestuurlijke politie over geradicaliseerde personen of *terrorist fighters* en op anonieme politievoertuigen voor het automatisch inlezen van nummerplaten, teneinde geseinde voertuigen op te sporen (art. 46/4 WPA);
2) bij de voorbereiding van acties van gerechtelijke politie of bij de handhaving van de openbare orde tijdens deze acties (artikelen 46/7 en 46/8 WPA);
3) in het raam van de gespecialiseerde opdrachten van bescherming van personen (art. 44/9 WPA);
4) tijdens de overbrenging van aangehouden of opgesloten personen (art. 46/11 WPA).

[51] Art. 25/7 § 1, 1ste en 2de lid en 44/11/3*decies* § 3, 2e lid WPA.
[52] Art. 44/11/3*decies* § 3, 1ste lid WPA.
[53] Memorie van Toelichting bij deze wet, p. 29 (Parl. St. *Kamer* 2017-2018, nr. 54-2855/001).
[54] Zoals principieel vastgelegd in artikel 14 (recht van inzage) Richtlijn Politie-Justitie.
[55] Art. 25/2 § 2 WPA.
[56] Art. 46/4 e.v. WPA.

Behalve wanneer het niet-zichtbaar gebruik van camera's onder het gezag van een magistraat wordt uitgevoerd, moet deze vorm cameragebruik **voorafgaand** aan het Controleorgaan worden aangeven. Deze voorafgaande mededeling moet het Controleorgaan toelaten om de wettelijkheid van de beslissing te beoordelen[57].

3.1.8 Impact- en risicoanalyse en gegevensbeschermingseffectbeoordeling (GEB of *DPIA*, *Data Protection Impact Assessment*)

17. Sedert de wet van 21 maart 2018 is het verplicht om, voorafgaand aan het gebruik van camerabewaking, een impact- en risicoanalyse op te maken waarbij de bescherming van de persoonlijke levenssfeer wordt afgetoetst aan en geplaatst wordt tegenover het operationele niveau van het cameragebruik[58]. Deze oefening moet ook worden gemaakt vóór het oprichten van een (lokale) technische gegevensbank[59]. Hiervoor wordt de bijstand van de *DPO* gevraagd[60].

Mits aan de voorwaarden van de WGB voor een *DPIA* en de voorwaarden voor een risico- en impactanalyse betreffende het zichtbaar gebruik van camera's en/of betreffende de oprichting van technische gegevensbanken onder de WPA voldaan zijn, kunnen beide analyses in één document vervat zijn. Aangezien een *DPIA* onder de WGB een bredere analyse vergt dan hetgeen in de WPA is voorgeschreven, wordt er op gewezen dat, ingeval beiden samen worden behandeld, die analyse conform de WGB alle relevante systemen en procedures van verwerkingsactiviteiten moet behandelen. Behalve de naleving van de WGB en de WPA moeten tevens de operationele voorzorgsmaatregelen en beveiligingsmaatregelen worden omschreven (die worden genomen om de risico's voor de te beschermen persoonsgegevens te beperken).

3.1.9 Registers

18. Conform de bepalingen van art 25/8 WPA moet het gebruik van camerabewaking in een (lokaal) register worden bijgehouden[61]. In het register wordt het type camera's en de locatie opgenomen. Er is evenwel nog geen Koninklijk besluit uitgevaardigd waarbij de inhoud van het register nader wordt uitgewerkt. Niettemin is het Controleorgaan van oordeel dat in het licht van de effectiviteit van haar toezichtsbevoegdheden, de politie, in afwachting van het uitvoeringsbesluit, uit eigen beweging een register moet bijhouden waarop elk gebruik van (type) camera's wordt vermeld, inbegrepen het niet-zichtbaar gebruik van camera's. Op die manier verkrijgt het Controleorgaan en trouwens de politiezone of -dienst zelf (in)zicht op (over) het gebruik van camerabewaking op het grondgebied van de gemeente(n) dat (die) onder diens bevoegdheid val(llen)t. Tegelijk kan het gebruik van camerabewaking afgetoetst worden aan het register van de verwerkingsactiviteiten. Aangezien er door het filmen persoonsgegevens worden verwerkt, moet deze verwerking immers ook in het register van verwerkingen opgenomen worden[62]. Beide registers zijn of moeten beschikbaar zijn voor het Controleorgaan. Het COC verzet zich niet tegen het samenbrengen van beide finaliteiten in het REGPOL register, in afwachting van de genoemde uitvoeringsbesluiten. Tenslotte is er in art 25/8 WPA ook nog sprake van het nationaal register geolocalisatie, zijnde een nationaal register met de geolocalisatie van alle door de politiediensten gebruikte vaste camera's dat door de federale politie wordt bijgehouden en op digitale wijze bewaard, onder de benaming "*CamELIA*"[63]. Dit register "*CamELIA*" bevat tevens de geolocalisatiegegevens van de bewakingscamera's die door de verantwoordelijke(n) moet(en) worden aangemeld aan de politie in het raam van de wettelijke bepalingen van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's.

3.1.10 Camerabewaking van de gebouwen en politiekantoren en politiecellen

[57] Art. 46/6 en 46/10 WPA.
[58] Art. 25/4 § 2 WPA.
[59] Art. 44/11/3*octies* WPA.
[60] Art. 65, 3° *juncto* 58 WGB.
[61] Art. 25/8 WPA.
[62] Art. 55 WGB.
[63] *CamELIA* is een visuele toepassing waarmee camera's op een kaart worden getoond. De naam *CamELIA* staat voor *Camera **E**nhanced **L**ocation **I**nformation **A**pplication*. In deze zin is het de materialisering van het nationaal register geolocalisatie zoals bepaald in art 25/8 WPA. Via *CamELIA* zijn alle camera locaties en details - komende van verschillende bronnen - visueel te benaderen*: ANPR* camera's (*AMS*), bewakingscamera's van privé personen, ondernemingen of lokale overheden (IBZ/Camine) en camera's gevat door de GPI zelf.

19. De camerabewaking van de gebouwen en politiekantoren en politiecellen valt onder de WPA[64]. Dat is tevens het geval voor camerabewaking van de inkomhal of het onthaal van het politiecommissariaat. Camerabewaking[65]in opsluitingsplaatsen draagt bij tot het beschermen en waarborgen van het welzijn van de personen die van hun vrijheid beroofd zijn en draagt bovendien bij tot een verbeterde eerbiediging van de rechten van de verdediging, bedoeld in artikel 6 EVRM[66]. Deze camerabewaking is echter alleen denkbaar als een element dat toegevoegd wordt aan een geheel van maatregelen, zoals regelmatige fysieke controle van de opgesloten personen, een beleid ter voorkoming van zelfmoord of zelfverminking, een efficiënt aangiftesysteem voor slachtoffers van ongeoorloofde handelingen in cellen, scheiding, afzondering, toepassing van tuchtsancties of nog de aanwezigheid van een advocaat tijdens het politieverhoor[67]. Het politiegebouw – of de politiepost - moet uitgerust zijn met een duidelijke signalisatie van de camerabewaking zodat de persoon die in een van de cellen zit opgesloten daarvan uitdrukkelijk is ingelicht. De opnames van de opsluiting moeten volledig blijven (geen enkele gedeeltelijke uitwissing) en bewaard worden gedurende een redelijke periode gedurende welke men een klacht kan indienen.

Aangezien deze beelden niet noodzakelijk en zelfs meestal geen operationeel belang hebben is de procedure voor onrechtstreekse toegang tot deze beelden via het COC niet van toepassing en kan de betrokkene overeenkomstig de WGB en de AVG rechtstreeks toegang verkrijgen tot de geregistreerde beelden van zijn opsluiting (zie hoger).

Bij het vertonen van de beelden van de verschillende cellen op monitors in het commissariaat, moet de politie een aantal strikte veiligheids- en toegangsmaatregelen nemen: de toegang moet beperkt zijn conform het *need to know* beginsel. Een algemene toegang tot de beelden (bijvoorbeeld: monitors in een lokaal waar de personeelsleden in en uit lopen of aan het onthaal) moet worden vermeden.

3.1.11 Beelden van camera's die geïnstalleerd zijn op het net van openbare vervoersmaatschappijen

20. De federale en lokale politiediensten hebben, binnen het raam van hun opdrachten van gerechtelijke of bestuurlijke politie, vrije en kosteloze toegang in *real time* tot de beelden van de camera's die geïnstalleerd zijn op het net van de openbare vervoersmaatschappijen. De nadere regels van deze vrije toegang tot de beelden, de overdracht en de beveiliging ervan worden bepaald in protocolakkoorden tussen de betrokken politiediensten en openbare vervoersmaatschappij en ter advies voorgelegd aan de Gegevensbeschermingsautoriteit, voorafgaandelijk aan de ondertekening ervan[68]. Wij[69]wijzen er hier op dat het dus wel degelijk gaat over bewakingscamera's geplaatst door de beheerder van de plaats waarvan sprake, en niet over camera's geplaatst en volledig beheerd door de politiediensten. Als het gaat over vaste camera's geplaatst door de politiediensten zelf op een voor het publiek toegankelijke besloten plaats waarvan zij niet de beheerder zijn, kan dit slechts gebeuren in de gevallen bedoeld in artikel 25/3, §1, 2°, b) tot d) WPA. Men beoogt hier dus alleen de gevallen waarin in eerste instantie de bewakingscamera's worden geplaatst door de beheerder van de plaats, met inachtneming van de Camerawet van 2007, en waarvan de toegang tot de beelden in *real time* wordt gegeven aan de politiediensten, op basis van artikel 9, derde lid, 3°, a), van voormelde Camerawet. Als de partijen in de overeenkomst betreffende deze toegang het eens worden over het feit dat deze toegang in *real time* eveneens een opname van de beelden bij de politiediensten als gevolg zal hebben, zullen deze laatste er eveneens op moeten toezien dat alle regels zoals voorzien door de wet op het politieambt, in haar afdeling op het zichtbaar gebruik van camera's, worden nageleefd. Dit vloeit voort uit de gecombineerde toepassing van artikel 9 van de camerawet en de artikelen 25/1 §2 en 25/4 §1 WPA. Het betreft dus een andere hypothese dan die bedoeld in artikel 25/3, §1, 2°, b), die het voorwerp uitmaakt van een ander specifiek koninklijk besluit[70] en slechts de gevallen

[64] Zie ook het KB van 14 september 2007 betreffende de minimumnormen, de inplanting en de aanwending van de door de politiediensten gebruikte opsluitingsplaatsen, inzonderheid art. 10.
[65] Aanbeveling 06/11 uitgaande van de voormalige Privacycommissie of CBPL – nu Gegevensbeschermingsautoriteit of GBA - betreffende installatie en gebruik van bewakingscamera's in opsluitingsplaatsen (cellen en arrestantenlokalen) en andere plaatsen van het commissariaat.
[66] Europees Verdrag voor de Rechten van de Mens.
[67] Zie in dit verband : «*Les normes du CPT – Chapitres des rapports généraux du CPT consacrés à des questions de fond*» (document CPT/Inf/E (2002) 1 – Rev. 2009), beschikbaar op www.cpt.coe.int/en/docsstandards.htm.
[68] Art 9 van de Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's.
[69] Zie ook Verslag aan de Koning bij het Koninklijk besluit van 6 december 2018 tot vaststelling van de plaatsen waar de verwerkingsverantwoordelijke zijn bewakingscamera's kan richten op de perimeter rechtstreeks rond de plaats, de beelden van de bewakingscamera's gedurende drie maanden kan bewaren en toegang in real time tot de beelden kan geven aan de politiediensten (*BS*, 18 december 2018, 99553 , bespreking artikelen 3 en 4.
[70] Met name Koninklijk besluit van 6 december 2018 tot uitvoering van artikel 25/3, § 1, 2°, b) van de wet op het politieambt, *BS*, 24 december 2018, 102186 .

beoogt waarin de politiediensten exclusief plaatser en gebruiker zijn van camera's op een plaats die een bijzonder risico inhoudt voor de veiligheid, die voorkomt in de lijst, na akkoord van de beheerder van de plaats. Samengevat zijn dus de hypotheses de volgende:

- de politie maakt gebruik van bewakingscamera's geplaatst en gebruikt door een openbare vervoersmaatschappij in een voor het publiek toegankelijke besloten plaats middels een toegang in *real time*, zonder de beelden op te nemen: art 9 Camerawet is van toepassing;

- de politie maakt gebruik van bewakingscamera's geplaatst en gebruikt door een openbare vervoersmaatschappij in de zin van het voorgaande streepje en neemt de beelden ook op: art 25/1 §2 e.v. WPA zijn van toepassing;

- de politie is exclusief plaatser en gebruiker van bewakingscamera's binnen de voor het publiek toegankelijke, besloten plaatsen van de openbare vervoersmaatschappij met toestemming van deze laatste: toepassing van art 25/3 §1, 2° b WPA.

De maximale bewaartermijn voor de verantwoordelijke van de verwerking, wanneer dit voor alle duidelijkheid *niet* de politie is, bedraagt in dit geval drie maanden, overeenkomstig de artikelen 5 §4, 5e lid, 6 §3, 3e lid, 7 §3, 3e lid en 7/3 §4, 2e lid van de Camerawet van 21 maart 2007. Het gaat hier om een maximale bewaartermijn en dus geen verplichting.

3.2 Bijzondere gegevensbanken

21. Art. 44/11/3 WPA bepaalt dat de oprichting van een bijzondere gegevensbank (GBO) enkel mogelijk is wanneer de uitoefening van de opdrachten van bestuurlijke politie en van gerechtelijke politie vereisen dat de politiediensten de persoonsgegevens en de informatie bedoeld in artikel 44/1 WPA structureren, zodat ze rechtstreeks kunnen worden teruggevonden (het gaat dus om een 'operationele' gegevensbank).

22. Verder voorziet voormeld artikel 44/11/3 §1 WPA de volgende cumulatieve voorwaarden voor de oprichting van een GBO:

- in specifieke omstandigheden;
- voor de uitoefening van de opdrachten van bestuurlijke of gerechtelijke politie;
- voor bijzondere behoeften.

Artikel 44/11/3 §2 WPA voorziet verder dat de oprichting van een GBO (bijkomend) door minstens één van de volgende bijzondere behoeften moet worden verantwoord:

a) de noodzaak om persoonsgegevens en informatie te classificeren in de zin de van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

b) de technische of functionele onmogelijkheid om de ANG te voeden met alle of een gedeelte van de in deze gegevensbanken verwerkte persoonsgegevens en informatie;

c) het niet ter zake dienend of overmatige karakter van de centralisering van alle of een gedeelte van de persoonsgegevens of de informatie in de ANG in het raam van de uitoefening van de opdrachten van bestuurlijke politie en van gerechtelijke politie.

23. De doeleinden en voorwaarden voor de oprichting van een bijzondere gegevensbank liggen dus duidelijk wettelijk vast. Deze wettelijke bepalingen vormen dan ook het uitgangspunt voor het COC om een bepaalde databank te aanzien als een GBO. De verwerkingsverantwoordelijke moet, vooraleer deze gegevensbank op te nemen in het nationaal register der verwerkingen (REGPOL) of in een lokaal register, deze criteria overlopen, aanvinken en van de nodige uitleg of commentaar voorzien.

24. Conform art. 58 en 59 WGB moeten de politiediensten vooraf het advies van het COC vragen wanneer:

- bij uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB of *DPIA*)[71] blijkt dat de verwerking, in het bijzonder bij gebruik van nieuwe technologieën, een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen (art. 58);
- uit de *DPIA* een hoog risico blijkt en de verwerkingsverantwoordelijke niet de nodige maatregelen neemt om het risico te beperken; of indien de aard van de verwerking, in bijzonder bij gebruik van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van de betrokkenen met zich brengt (art. 59 §1 1° en 2°).

25. De GPI kan dus bijvoorbeeld niet de volgende argumenten weerhouden om een bijzondere gegevensbank op te richten:

- werklast vereist voor de vatting, de voeding en de overdracht van de gegevens naar de ANG;
- gebrek aan kennis van het gebruik van een ANG of een basisgegevensbank;
- gebrek aan (beweerdelijke) gebruiksvriendelijkheid van de ANG of een basisgegevensbank.

3.3 Logging ANG

26. De politie is verplicht om logbestanden bij te houden[72]. Een logbestand is bij uitstek een instrument om het bewijs van de (on)rechtmatigheid van de verwerking te controleren en de integriteit en de beveiliging van de gegevens te garanderen[73]. In dat verband zijn logbestanden tevens van belang bij interne tuchtprocedures of administratieve onderzoeken. Cijfers van de tuchtraad van de GPI tonen aan dat een onrechtmatige raadpleging het meest frequent gepleegde tuchtmisdrijf is. Logbestanden zijn bijgevolg van belang met het oog op zowel proactieve als reactieve controle en zowel op intern als op extern niveau. Het belang wordt ook aangetoond door de recente beslissing van het directiecomité van de federale politie om de reden van raadpleging ICT-matig verplicht te maken[74] en nog eens herhaald in de permanente nota van het coördinatiecomité van de GPI n° CG-2021/4833_N van 8 september 2021[75]

3.4 ANG werking /

27. De politionele en gerechtelijke gegevens zijn een bijzondere categorie persoonsgegevens en uit hun aard zeer gevoelig. Zij mogen enkel in het raam van opdrachten van gerechtelijke of bestuurlijke politie worden verwerkt en in overeenstemming met de wettelijke voorschriften (WPA, WGB, MFO3[76], het wetboek van strafvordering en beginselen zoals het beroepsgeheim, het geheim van het onderzoek, de discretieplicht opgelegd aan leden van de GPI, enz. …). Een nauwkeurige toepassing van de vattings- en ventilatieregels conform de wettelijke bepalingen van de WGB[77] en de WPA[78]enerzijds, en de reglementaire bepalingen van de genoemde MFO3 en het bijhorende Vademecum[79]is van primordiaal belang.

3.5 Triptiek

3.5.1 Algemeen

28. De regelgeving rond het uitvoeren van de triptiek vindt zijn oorsprong in de dwingende 'Gemeenschappelijke Richtlijn MFO3' van de Ministers van Justitie en van Binnenlandse Zaken betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie.

---

[71] *DPIA* staat voor ***D**ata **P**rotection **I**mpact **A**ssessment.*
[72] Art. 56, § 1, WGB, ter uitvoering van artikel 25 Richtlijn Politie & Justitie.
[73] Art. 56, § 2, WGB.
[74] Directiecomité van 21 september 2020, punt 3, uitgiftenummer CG/2020/4855.
[75] Permanente nota "*Richtlijn betreffende de motivering van de raadplegingen van de politionele gegevensbanken en de gegevensbanken waartoe de politiediensten toegang hebben in het raam van de uitvoering van de opdrachten van bestuurlijke en gerechtelijke politie*", 5 blz.
[76] De gemeenschappelijke richtlijn MFO 3 van de Ministers van Justitie en van Binnenlandse Zaken "*betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie*".
[77] Inzonderheid de titel 2.
[78] Inzonderheid de artikelen 44/1 tem 44/11/13.
[79] Het Vademecum Gerechtelijke Politie beschrijft in detail de toe te passen vattingsregels bij ANG registraties.

29. Het uitvoeren van de triptiek is essentieel in de doelstelling om de juiste informatie op het juiste ogenblik op de juiste plaats te brengen met het oog op een efficiëntere en effectievere uitvoering van de opdrachten van gerechtelijke en bestuurlijke politie.

De gerechtelijke triptiek wordt uitgevoerd om bij te dragen tot de identificatie van personen en bestaat uit 3 luiken:

a: vinger- en handpalmafdrukken;
b: foto's;
c: individuele persoonsbeschrijving.

30. De triptiek wordt opgemaakt in het raam van de opdrachten van gerechtelijke politie en, in voorkomend geval, in het raam van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen (Vreemdelingenwet).

31. Onder 'persoon' wordt hier verstaan hetzij:

- de dader, de mededader, de medeplichtige of de verdachte (categorie "VERDACHT");
- de persoon die niet over een wettelijke verblijfstitel beschikt of die geen identificatiestukken heeft, met uitzondering van de niet-begeleide minderjarige vreemdeling (NBMV) of de asielzoeker (categorie "VERDACHT");
- het slachtoffer, de benadeelde, de getuige of het (de) lid (leden) van de politie- of hulpdiensten aanwezig op de plaats van de feiten (categorie "NIET VERDACHT"). Elk lijk wordt beschouwd als behorend tot de categorie "niet verdacht" (bij afname vinger- en handpalmafdrukken);
- de vermiste persoon (nemen foto's);
- de vermiste persoon of de persoon die het voorwerp van een te nemen maatregel uitmaakt (opmaken individuele beschrijving).

32. Er moeten **verplicht** vingerafdrukken van een verdachte genomen worden wanneer de betrokken persoon ouder is dan 14 jaar en indien de persoon hetzij:

- verhoord wordt en er voor hem een verband met een concreet feit werd bevestigd (bewezen) of hij het voorwerp uitmaakt van ernstige verdenkingen door de politiediensten (voor zover het niet gaat om een KOF4[80]);
- van zijn vrijheid beroofd wordt (vanaf het moment waarop, ten behoeve van het onderzoek, de betrokken persoon niet meer de vrijheid heeft om te gaan en te komen waar hij wil);
- ter beschikking gesteld wordt van de gerechtelijke overheid of van de Dienst Vreemdelingenzaken;
- opgesloten dient te worden in een strafinrichting als gevolg van een gerechtelijk bevel of een gerechtelijke beslissing.

33. Voor minderjarigen die jonger zijn dan 14 jaar moet de met het dossier belaste magistraat bovendien zijn toestemming gegeven hebben om de drieledige gerechtelijke identificatie uit te voeren. Deze toestemming moet vermeld worden in het proces-verbaal.

34. Bij illegaal verblijf **MOET** de gerechtelijke triptiek altijd toegepast worden. De strikt noodzakelijke dwang kan uitgevoerd worden voor het afnemen van vingerafdrukken (cf. art. 37 WPA). Voor de triptiek werd de praktische werkwijze uitgewerkt in de fiches B03, B04 en B05 van de MFO3.

[80] Een concreet feit van type 4 (KOF 4) is een concreet feit dat omwille van het samenstellen van een volledig beeld betreffende de verbonden entiteiten en omwille van beleidsdoeleinden, steeds wordt geregistreerd in de ANG.

3.5.2 EURODAC

3.5.2.1 Inleiding

35. Eurodac is een centrale gegevensbank[81]die is opgericht in het raam van de toepassing en uitvoering van het gemeenschappelijk asielbeleid met betrekking tot personen die om internationale bescherming verzoeken[82]. Eurodac biedt de mogelijkheid om na te gaan of een onderdaan van een derde land of een staatloze persoon de buitengrens overschrijdt of illegaal op het grondgebied van een lidstaat verblijft en/of reeds in andere lidstaat om internationale bescherming heeft verzocht. Daarnaast is Eurodac ook een belangrijke instrument in het raam van de bestrijding van terrorisme en andere ernstige misdrijven. Daarom zijn de gegevens in Eurodac onder voorwaarden beschikbaar voor verzoeken tot vergelijking van vingerafdrukken door de aangewezen autoriteiten (*in casu* de politiediensten) van de lidstaten en Europol.

Het operationele beheer, het toezicht, beveiliging en de coördinatie van Eurodac is handen van het Europees Agentschap (EU-LISA[83]) dat daarmee is belast. De communicatie tussen het centraal systeem en het nationaal toegangspunt van de lidstaat verloopt via een versleuteld virtueel netwerk[84].

De regels van Eurodac zijn van toepassing vanaf het ogenblik dat de gegevens door de lidstaat naar het centraal systeem worden toegezonden. Op het nemen van de vingerafdrukken en de verwerking van de gegevens voorafgaand aan de verzending zijn bijgevolg de nationale regels van toepassing[85].

3.5.2.2 Het verwerken en vergelijken van vingerafdrukken

36. Er kunnen globaal drie categorieën worden onderscheiden waarbij de vingerafdrukken in het kader van het asielrecht van de betrokkene worden genomen. Als algemene regel geldt dat van elke persoon vanaf 14 jaar de vingerafdrukken worden genomen, behalve wanneer de persoon onmiddellijk wordt teruggestuurd en aldus niet tot het grondgebied van de EU wordt toegelaten.

De eerste categorie betreft de personen (minderjarigen) die om internationale bescherming verzoeken. Behalve de vingerafdrukken worden andere (samenhangende) gegevens[86]naar Eurodac toegezonden, identiteitsgegevens uitgezonderd. Van deze personen worden de gegevens opgeslagen met het oog op vergelijking met de gegevens over vingerafdrukken die door andere lidstaten in Eurodac zijn opgenomen[87]. De gegevens (vingerafdrukken) worden voor een periode van 10 jaar bewaard. Na deze termijn worden de gegevens automatisch verwijderd[88]. De gegevens moeten evenwel eerder worden verwijderd van zodra de persoon het burgerschap van een lidstaat heeft verkregen[89].

De tweede categorie betreft de personen die illegaal de buitengrenzen (van de Europese Unie) overschrijden. Indien de vingerafdrukgegevens van de persoon niet in Eurodac wordt teruggevonden, worden de vingerafdrukken en de samenhangende gegevens[90]in Eurodac opgeslagen. De gegevens worden 18 maanden bewaard. Na deze termijn worden de gegevens automatisch verwijderd[91]. De gegevens worden eerder verwijderd wanneer de betrokkene een

---

[81] Verordening (EU) nr. 603/2013 van het Europees Parlement en van de Raad van 26 juni 2013 betreffende de instelling van „Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving, en tot wijziging van Verordening (EU) nr. 1077/2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (Verordening Eurodac).

[82] Verordening (EU) nr. 604/2013 van het Europees Parlement en de Raad van 26 juni 2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend.

[83] Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.

[84] Artikelen 2, 1 e), art. 3.1, b), 3.5. en 4.1. Verordening Eurodac.

[85] Art. 3, 4de lid Verordening Eurodac. Met name afdeling 12 inzake het informatiebeheer (artikelen 44/1 e.v.) WPA) .

[86] Met name de lidstaat van oorsprong, plaats en datum van het verzoek om internationale bescherming, het geslacht, het referentienummer van de lidstaat van oorsprong, de datum waarop de vingerafdrukken zijn genomen, de datum van toezending van de gegevens naar Eurodac en de gebruikersidentificator van de operator (art. 9 en 11 b-g Verordening Eurodac).

[87] Art. 9 en 14 Verordening Eurodac.

[88] Art. 12 Verordening Eurodac.

[89] Art. 13 Verordening Eurodac.

[90] Behalve de vingerafdrukken, lidstaat van oorsprong de plaats en datum van aanhouding, het geslacht, het referantienummer dat door de lidstaat van oorsprong wordt gebruikt, de datum waarop de vingerafdrukken zijn genomen, de datum van toezending naar Eurodac en de gebruikersidentificatie van de operator (art. 14, 2de lid Verordening Eurodac).

[91] Art. 16, 1ste lid Verordening Eurodac.

verblijfstitel heeft gekregen, het grondgebied van de lidstaten heeft verlaten dan wel het burgerschap van een lidstaat heeft verkregen[92].

De derde categorie betreft de personen die illegaal in het land verblijven. Van deze personen worden de vingerafdrukgegevens met het gebruikte referentienummer in de regel naar Eurodac toegezonden met het oog om na te gaan (te vergelijken) of de betrokkene reeds in een andere lidstaat om internationale bescherming heeft verzocht wanneer hij verklaart reeds om bescherming in een ander land te hebben verzocht zonder de lidstaat te vermelden, geen bescherming verzoekt en zich tevens verzet tegen terugzending of weigert zijn identiteit mee te delen[93]. De vingerafdrukgegevens worden echter niet in het centraal systeem bewaard[94].

De gegevens van personen die internationale bescherming genieten worden in Eurodac als zodanig gemarkeerd en zijn onder strikte voorwaarden voor de politie beschikbaar in het raam van de politionele doeleinden voor een periode van drie jaar na de datum waarop de betrokkene internationale bescherming heeft verkregen. Na deze termijn dienen de gegevens voor de politie afgeschermd te zijn[95]. In de praktijk wordt de toegang tot Eurodac door de GPI met het oog op rechtshandhavingsdoeleinden[96] ook als een 'vierde categorie' aangeduid.

3.5.2.3 De organen of diensten die vingerafdrukken verwerken

37. Bij het verwerken van de vingerafdrukken in het raam van de toepassing van Eurodac komen drie actoren in beeld: het nationaal toegangspunt, de aangewezen autoriteiten en de controlerende autoriteit[97]. Voor België werd de Dienst Vreemdelingenzaken (DVZ) als nationaal toegangspunt aangeduid, in de praktijk uitgevoerd door de dienst 'Printrak' van DVZ. Dat is de enige dienst die bevoegd is om de vingerafdrukken en de samenhangende gegevens naar Eurodac toe te zenden en te verzoeken om een vergelijking van de vingerafdrukken met Eurodac te behandelen. Op basis van de vingerafdrukken kan DVZ nagaan of de betrokkene via een andere lidstaat België is binnengekomen of reeds in een andere lidstaat asiel heeft aangevraagd. De Gerechtelijke Identificatiedienst (GID) van de federale politie[98]is de controlerende autoriteit wat betreft de toegang tot Eurodac voor politionele doeleinden. Deze entiteit van de federale politie behandelt en controleert de verzoeken om vergelijking van vingerafdrukken die door de federale en lokale politiediensten of -entiteiten aan de GID worden doorgestuurd[99] en stuurt deze vervolgens naar DVZ voor vergelijking in Eurodac.

4 ONDERZOEKSBEVINDINGEN

4.1 Algemeen

38. Na het versturen van de vragenlijst met aankondiging van de visitatie door het COC op 30-03-2021 volgt op 14-04-2021 een overleg met het diensthoofd van SPC Brussel. Deze stelt dat, ingevolge de specificiteit van de vragen en de interne bevoegdheden, de directie SPC het dossier zal piloteren en ook aanwezig zal zijn op de visitatie, samen met een vertegenwoordiger van de Algemene Directie Bestuurlijke Politie (DGA).

Tevens blijkt dat de directie SPC totaal verrast was met de aankondiging van het bezoek en de specifieke vragenlijst. Het was voor de directie in elk geval een *incentive* om een en ander van de eigen werking meer en beter in kaart te brengen. Om die reden wordt ook een veel ruimere documentatie dan eigenlijk gevraagd overgemaakt, al blijkt die documentatie vooral een structureel gegeven te zijn met identificatie van processtappen die nog verder dienen uitgewerkt te worden in nota's en richtlijnen enerzijds en blijken de antwoorden op de specifieke COC vragenlijst eerder beperkt. De onderzoeksbevindingen in dit rapport beperken zich in alle geval hoofdzakelijk tot de vragenlijst.

[92] Art. 16, 2de lid Verordening Eurodac.
[93] Art. 17, 1ste lid Verordening Eurodac.
[94] Art. 17, 3de lid Verordening Eurodac.
[95] Art. 18, 2de lid Verordening Eurodac.
[96] Art. 19 Verordening Eurodac.
[97] Art. 5, 6 Verordening Eurodac.
[98] De GID maakt deel uit van de Centrale directie van technische en wetenschappelijke politie.
[99] Merk op dat de in het kader van Eurodac aangewezen autoriteiten geen agentschappen of diensten mogen zijn die uitsluitend bevoegd zijn op het vlak van de nationale veiligheid, zoals de Veiligheid van de Staat en de Algemene Dienst Inlichtingen en Veiligheid (ADIV, de militaire inlichtingendienst).

Zoals supra reeds vermeld bij de inleiding kunnen bepaalde van de aanbevelingen die volgen uit de onderzoeksbevindingen aanleiding geven tot initiatieven op beleidsmatig of wetgevend vlak. Deze zijn dan ook in het bijzonder bedoeld voor de beleidsverantwoordelijken en de verantwoordelijke ministers (die een afschrift van dit rapport zullen ontvangen) en niet in eerste instantie gericht aan de SPC.

4.2 Camerabewaking

4.2.1 Camerabewaking onder de Camerawet

4.2.1.1 Real Time toegang tot beelden van vervoersmaatschappijen

39. Het voornaamste cameragebruik door de SPC situeert zich binnen de bepalingen van art. 9 van de wet op de bewakingscamera's en het daarbij horende uitvoeringsbesluit[100], met name de *real time* toegang tot de beelden van een aantal camera's waarvan de vervoersmaatschappijen de verantwoordelijke van de verwerking zijn, evenwel zonder de opname ervan bij de SPC zelf. De dienst NARAIL[101]heeft daartoe zicht op de camera's van de MIVB in metrostations, en camera's in 109 stations van de NMBS. Deze dienst beschikt over twee posten die toegang geven tot beelden van de MIVB, en een post die toegang geeft tot de beelden van de NMBS. De toegangen tot de beelden zijn nominatief geregeld met een login en een paswoord. Noch de camera's, noch de beelden kunnen gemanipuleerd worden. SPC heeft geen zicht op de camera's op de overwegen, langs spoorlijnen of voorlopige camera's van de NMBS. De overdracht van de beelden waartoe de politiediensten niet in *real time* toegang hebben is mogelijk op vraag van de SPC of andere politiediensten, met name via de dienst SOC[102]en dit op voorlegging van een verzoek. Er blijken evenwel geen protocolakkoorden beschikbaar en logischerwijze ook geen voorafgaand advies van de Gegevensbeschermingsautoriteit[103]. Nochtans zijn dergelijke protocolakkoorden wettelijk vereist[104]en moeten deze naast de principes over de kostprijs van de investeringen om de toegang mogelijk te maken, ook de technische en praktische modaliteiten van de toegang bepalen (welke camera's, het bekijken in *real time* op initiatief of op verzoek, terugspoelen of niet, mogelijkheid om de camera's te richten, verantwoordelijkheid, beveiliging, opname van de beelden, wederzijdse informatie-uitwisseling, samenwerkingsakkoorden, enz. …). De SPC heeft daartoe in 2014 reeds een vraag gesteld aan de verantwoordelijke van de verwerking doch sindsdien lijkt het dossier stil te liggen; de vragenlijst van het COC alsmede de visitatie was een aanleiding voor de SPC om de problematiek van deze protocolakkoorden opnieuw te bespreken met de verantwoordelijke van de verwerking. Hoewel de Gegevensbeschermingsautoriteit bevoegd is om over het protocolakkoord advies te verlenen moet het protocolakkoord beschikbaar zijn voor het COC om inzicht te krijgen in het verloop van de gegevensstromen en de verwerkingen.

40. Zoals hierboven vermeld, stelt het COC vast dat voor wat de SPC betreft het merendeel van het cameragebruik verloopt onder toepassing van de bepalingen van art 9 van de Camerawet. *Prima facie* lijkt dit aan de kant van SPC conform de vigerende wetgeving te zijn, met evenwel een aantal aanbevelingen die dienen besproken te worden met de verantwoordelijken van de verwerking aan de kant van de NMBS. Gelet evenwel op het feit dat de beelden rechtstreeks en bovendien systematisch toegankelijk zijn in de politie-omgeving, met name via het commandocentrum NARAIL van de SPC, doch weliswaar zonder de mogelijkheid tot opslag of manipulatie, stelt zich de vraag of het niet beter zou zijn om de verwerking volledig te enten op de bepalingen van de WPA. Het systematisch en permanent meekijken door de politie is immers op zich ook een verwerking, ook wanneer er geen sprake is van opslag, en gegeven de specificiteit van het terrein en de opdrachten is een *real time* aansturing van politieploegen door het commandocentrum NARAIL een reële mogelijkheid. Dit blijkt overigens ook uit de evolutie van de technologische mogelijkheden en de daaruit voortvloeiende operationele mogelijkheden beschreven onder punt 4.2.3. Door het

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

[101] NARAIL: dienst bij SPC die beelden bekijkt om de SPC ploegen van niveau 3 en 4 te kunnen aansturen. Het voordeel is dat NARAIL alle SPC ploegen op het nationale grondgebied *in real time* volgt (belangrijk voor de operaties van niveau 3 en 4 die verschillende provincies doorkruisen).
Er werden voor SPC namelijk vier niveaus van gespecialiseerde opdrachten vastgelegd:
-Niveau 1: interventie/permanentie, dispatching door het provinciale CIC (i.e. Communicatie- en InformatieCentrum of de provinciale meldkamer of dispatching).
-Niveau 2: overlast/storend gedrag die kunnen leiden tot administratieve sancties, dispatching door het provinciale CIC.
-Niveau 3: regionale acties ('rollercoaster'): op basis van de info verstrekt door de gebiedsagenten, lokale acties in de stations.
-Niveau 4: nationale en internationale acties om een fenomeen (koperdiefstal, drugs, migranten ...) te bestrijden.

[102] ***S**ecurity **O**peration **C**enter.*

[103] Art. 80 van de Wet van 21 maart 2018.

[104] Art. 9 van de Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's.

cameragebruik te enten op de WPA ontstaat immers transparantie ten aanzien van de burger,[105]alsmede ten aanzien van de bestuurlijke en gerechtelijke overheden omtrent welke camera's systematisch mee opgevolgd worden door de politiediensten. In het licht van deze visie zou dit onder meer kunnen betekenen dat:

- middels het pictogram wordt aangegeven met welke camera's de politie systematisch meekijkt;

- impact- en risicoanalyses worden opgesteld;

- meldingen worden gedaan in het register van de verwerkingen;

- meldingen worden gedaan in het register voor cameragebruik;

-…

Terugkerende naar de vigerende regelgeving en abstractie makende van elke toekomstvisie zoals hierboven terzijde vermeld, blijkt de SPC geen verwerkingen te hebben geregistreerd in REGPOL, laat staan dat er al een register van camera gebruiken in de zin van art 25/8 WPA zou zijn aangelegd. Wat dit laatste betreft is de wet hier onduidelijk: art 25/8 heeft het over "*een register met alle gebruiken van camera's*", waardoor de vraag zich uiteraard stelt of het systematisch bekijken van beelden van vervoersmaatschappijen in *real time* binnen de lokalen van de politie in de zin van de Camerawet hieronder valt of niet. In alle geval, het geautomatiseerd meekijken is sowieso een verwerking waardoor de verwerking op zich alvast dient vermeld te worden in het register van de verwerkingen[106], waarbij het COC niet uitsluit dat beide finaliteiten (registratie van cameragebruik en registratie van de verwerking op zich) in een enkel register kunnen opgenomen worden.

In alle geval geeft het ontbreken van de nu reeds wettelijke voorziene registraties aanleiding tot het nemen van corrigerende maatregel 1.

41. Op het vlak van de voorafgaande principiële toestemmingen zoals bepaald in art 25/4 WPA, werd deze bevoegdheid voor de diensten van de federale politie gedelegeerd aan DGA[107]. Hier stelt het COC zich de vraag of het wel opportuun is dat de toestemming zou worden verleend door de directie die ook de uiteindelijke gebruiker van de camera's is. In het licht van de bepalingen die, voor wat de lokale politie betreft, deze bevoegdheid toekent aan de gemeenteraad lijkt hier de noodzakelijke 'onpartijdigheid' te ontbreken. Bovendien is het onduidelijk in hoeverre ook de lokale politie een bepaalde betrokkenheid heeft bij het beheren van gebeurtenissen in stations en langs de spoorlijnen, zeker wanneer blijkt dat de SPC niet onmiddellijk ter plaatse kan komen. De vraag stelt zich dus, of in deze niet eerder (ook) de gemeenteraad zich dient uit te spreken of minstens de Minister zelf of een gedelegeerde die niet tot de federale politie behoort (bv. de directeur-generaal van de Algemene Directie Veiligheid en Preventie van de FOD Binnenlandse Zaken) de principiële toestemming zou moeten geven.

4.2.1.2 Aangifteverplichtingen door de verwerkingsverantwoordelijke

42. Tot 25 mei 2018 moesten de bewakingscamera's aangegeven worden via het elektronisch loket van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL). Sinds de inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming (de 'AVG') op 25 mei ontvangt de CBPL (ondertussen de Gegevensbeschermingsautoriteit) geen aangiftes meer. Daarom werd ook in de Camerawet de aangifteverplichting bij de CBPL opgeheven. Om operationele redenen blijft het echter nuttig voor de politiediensten om te weten waar er bewakingscamera's worden geplaatst. Daarom werd deze aangifte behouden in de camerawet. Het aangiftesysteem www.aangiftecamera.be werd dus ontwikkeld, waarbij alle verantwoordelijken voor de verwerking van camerabeelden de mogelijkheid hebben te voldoen aan deze verplichting. Dit aangiftesysteem wisselt zijn informatie uit met het register van geolocalisatie CamELIA van de federale politie. Daar een exhaustief overzicht van alle door de NMBS aangegeven en in CamELIA zichtbare camera's momenteel technisch niet mogelijk is, is het COC overgegaan tot een *prima facie* analyse van een aantal cameraposities op overwegen en in stations. Hieruit blijkt, dat de NMBS zeer veel camera's heeft aangegeven. Evenwel blijkt ook dat wanneer ter plaatse aan de overwegen wordt nagekeken, in vele gevallen een

[105] Met dien verstande dat de burger zich nog steeds zal moeten richten naar de NMBS als verwerkingsverantwoordelijke aangezien de beelden aldaar worden opgeslagen, en dat de bewaartermijnen van de Camerawet van toepassing blijven.
[106] Art 55 WGB.
[107] Nota SAT/Adm/2018/1959 dd 14-09-2018.

pictogram[108]ontbreekt. Dit is evenwel de verantwoordelijkheid van de verantwoordelijke van de verwerking zijnde de NMBS en de bevoegdheid van de Gegevensbeschermingsautoriteit. De voor de politie operationele meerwaarde van een correcte aangifte van een bewakingscamera door de verwerkingsverantwoordelijke staat buiten elke discussie. De hierboven vermelde uitwisseling met de politie in het geolocalisatieregister CamELIA maakt deze informatie toegankelijk voor elke politiegebruiker die gemachtigd is om hiervan kennis te nemen in het raam van een concreet dossier. Politiediensten op het terrein hebben er dan ook alle belang bij, mee toe te zien op een correcte aangifte.

4.2.1.3 Van louter opslag naar systematisch gebruik als criterium binnen de WPA

43. Met de technologische evoluties gekoppeld aan een uitgebreider operationeel gebruik (zie ook infra vermelde voorbeelden van mogelijk geïntegreerd operationeel gebruik) lijkt het voor het COC aannemelijk om bij de *real time* overdracht van camerabeelden, zoals bepaald in art 9 van de Camerawet en art 4 van het Uitvoeringsbesluit, een duidelijk onderscheid te maken tussen een eerder evenement gerelateerd en dus *ad hoc* of casuïstisch én in de tijd beperkt gebruik van deze *real time* overdracht enerzijds, en een systematisch gebruik anderzijds, waarbij dus niet louter de opslag maar vooral het systematisch gebruik van de beelden zou gelden als criterium om dit gebruik te regelen onder de bepalingen van de WPA. Dit valt uiteraard buiten de bevoegdheid van de SPC en is eerder materie voor beleidsverantwoordelijken en de verantwoordelijke Ministers. Het COC benadrukt evenwel dat er, behoudens de in de supra vermelde tekst en infra geformuleerde aanbevelingen, *an sich* geen anomalieën werden vastgesteld met betrekking tot het cameragebruik zoals bepaald onder art 9 van de Camerawet door SPC. Concluderend voor dit punt stelt het COC dus voor:

- om het artikel 25/1 §2 WPA te wijzigen door niet langer de opslag te nemen als criterium om de cameraverwerking door de politie van beelden afkomstig van een andere verwerkingsverantwoordelijke toe te laten, maar wel het systematische karakter van het gebruik van deze beelden in de politie-omgeving;

- om de *real time* overdracht naar de GPI van de beelden van bewakingscamera's van verantwoordelijken van de verwerking van bijzondere plaatsen zoals bepaald in de Camerawet en in het Uitvoeringsbesluit uiteraard nog steeds toe te laten;

- om deze overdracht enkel nog buiten de regeling van de WPA te houden in de omstandigheden zoals beschreven in art 4, 4° van het Uitvoeringsbesluit, te weten: de plaatsen waar evenementen van culturele, maatschappelijke, festieve, folkloristische, commerciële of sportieve aard worden georganiseerd, beschouwd als grote volkstoelopen in de zin van artikel 22 van de wet op het politieambt, onder de volgende voorwaarden:

a) de toegang in *real time* wordt slechts ingesteld voor de duur van deze evenementen;

b) het instellen van deze toegang in *real time* gebeurt na een risicoanalyse uitgevoerd door de organisator van het evenement, waarbij moet worden aangetoond dat een toegang in *real time* van de politiediensten gerechtvaardigd is ondanks de genomen voorzorgs- en veiligheidsmaatregelen om het evenement te omkaderen;

c) het instellen van deze toegang in *real time* gebeurt in het kader van de opdrachten van bestuurlijke politie, na het uitvoeren, door de politiediensten, van een impact- en risicoanalyse op het niveau van de bescherming van de persoonlijke levenssfeer en op operationeel niveau, goedgekeurd door de politieambtenaar bedoeld in de artikelen 7 tot 7/3 van de wet op het politieambt, waarbij wordt aangetoond dat deze plaatsen een bijzonder risico inhouden op het vlak van de veiligheid.

4.2.2 Camerabewaking onder de WPA

4.2.2.1 ANPR

44. Noch de directie SPC, noch SPC Brussel lijken in eerste instantie gebruiker te zijn van *ANPR* camera's. Toch verneemt het COC na de visitatie, dat in het raam van een test op een spoorwegoverweg in Oudegem bij Dendermonde een eerste van in totaal drie testsites met *ANPR* camera's op overwegen werd uitgerold en dit op 16-06-2021. Het doel is om via nummerplaatherkenning het niet respecteren van het rood licht aan een overweg vast te stellen. De sites bestaan uit een camera voor automatische nummerplaatherkenning en een overzichtscamera. Wanneer een autobestuurder aan deze overweg door een rood licht rijdt, wordt dit geregistreerd door deze roodlichtcamera's die de beelden versturen

[108] KB van 28 mei 2018 tot wijziging van het KB van 10 februari 2008 tot vaststelling van de wijze waarop wordt aangegeven dat er camerabewaking plaatsvindt.

naar de Nationale Technische Gegevensbank (NTGB)[109]AMS[110]. Dit nieuwe, gezamenlijke pilootproject zal de verkeers- en spoorveiligheid aan overwegen verder helpen verhogen en dient ook als test voor de mogelijke uitrol van camera's aan andere overwegen. De andere locaties zijn gelegen in Waver en in Kallo. Voor deze laatste twee sites bestaat er nog geen datum van uitrol. Het pilootproject lijkt tot stand gekomen in samenspraak tussen de lokale politie van Dendermonde, Infrabel, de federale wegpolitie met het GVC[111]en de directie DRI. Het GVC verwerkt in opdracht van de lokale politie de camerabeelden conform de bepalingen van artikel 62 van de Wegverkeerswet (WVW) en stelt een proces-verbaal op. Zij controleren en bepalen of het daadwerkelijk over het negeren van een rood licht gaat. Omwille van het feit dat de camera's ook conform de bepalingen van de artikelen 25/1 tem 25/8 werden 'vergund' kunnen zij ook voor de andere finaliteiten van de technische gegevensbanken zoals omschreven in de artikelen 44/11/3*sexies* tem 44/11/3*decies* WPA worden gebruikt.

Een *prima facie* analyse van dit opzet door het COC levert de volgende vaststellingen op:

- Infrabel heeft de camera's geplaatst en is dus eigenaar van de installatie. Evenwel gebruikt Infrabel op geen enkele manier de beelden. Infrabel is dus NIET de verantwoordelijke van de verwerking (en dit in tegenstelling tot de supra gemelde verwerkingen met andere bewakingscamera's geplaatst en gebruikt door de NMBS).
- Voor wat het aspect 'verkeer' betreft:
    - werd een protocolakkoord afgesloten conform de bepalingen van art 62 van de Wegverkeerswet (WPW)[112];
    - vond een ijking plaats op het vlak van de conformiteit inzake de vaststellingen van overtredingen op de rode lichten geplaatst op spoorwegovergangen en dit op 16-01-2020;
    - werd een akkoord afgesloten met het GVC Gent voor de verwerking van de vaststellingen.
- Voor wat het aspect 'zichtbaar gebruik van camera's door politiediensten' betreft:
    - treedt de korpschef van de lokale politiezone Dendermonde op als verwerkingsverantwoordelijke voor de camera's;
    - heeft de korpschef van de lokale politiezone Dendermonde de toestemming van de gemeenteraad verkregen op 21-04-2020;
    - worden de beelden rechtstreeks doorgestuurd naar de NTGB en aldaar verwerkt conform de bepalingen van de artikelen 44/11/3*sexies* tem 44/11/3*decies* WPA en de *DPIA*;
    - staan op het pictogram de Ministers van Binnenlandse Zaken en Justitie vermeld als de verwerkingsverantwoordelijken gezien de beelden rechtstreeks verwerkt worden in de NTGB.

Hoewel de SPC in eerste instantie geen rechtstreeks betrokken partner lijkt, roept het COC de SPC op, om dit project mee op te volgen gezien dit plaatsvindt op het actieterrein van de SPC, en rekening houdende met de supra vermelde vaststellingen.

4.2.2.2 Camerabewaking van de cellen

45. SPC Brussel is niet de beheerder van een eigen cellencomplex. Hiervoor wordt gebruik gemaakt van het cellencomplex van de federale politie in het Rijksadministratief Centrum (RAC). Andere eenheden van SPC beschikken wel over doorgangscellen, met camerabewaking geplaatst door de firma Fabricom, binnen een raamcontract van de federale politie beheerd door de dienst DRL[113]. Volgens de directie SPC kunnen deze camera's zowel geluid als beeld registreren. Deze camera's werden niet geregistreerd in REGPOL, noch werden ze opgenomen in een register van gebruiken van camera's. Het is niet duidelijk in kaart gebracht waar de beelden worden opgeslagen en voor hoelang. Het is de bedoeling van de directie SPC om deze problematiek aan te pakken voor einde 2021.

[109] Art 44/11/3 sexies WPA.
[110] ***A**NPR **M**anaged **S**ervices.*
[111] **G**ewestelijk **V**erwerkings **C**entrum, De gewestelijke verwerkingscentra werden opgericht in de tweede helft van 2009. Er zijn er momenteel vier (Namen, Gent, Antwerpen en Brussel). Ze verwerken de automatisch vastgestelde verkeersovertredingen (radars, trajectcontroles, door een rood licht rijden ...). Deze centra werken niet uitsluitend voor de Federale Wegpolitie: ze leveren ook steun aan de lokale politiezones op het vlak van verwerking.
[112] Wet Politie Wegverkeer. Het *gaat in casu* om het overleg omtrent de plaatsing en de gebruiksomstandigheden, georganiseerd door de bevoegde gerechtelijke, politionele en administratieve overheden, waaronder de wegbeheerders.
[113] De directie logistiek, onderdeel van de Algemene Directie van de Middelen (Resources) DGR.

Deze onduidelijkheden geven aanleiding tot het nemen van de corrigerende maatregel 2.

46. Het COC wenst hier expliciet te waarschuwen voor de artikelen 314*bis* en 259*bis* Sw. Deze beschermen de burger namelijk tegen het afluisteren, kennisnemen en opnemen van "*niet voor het publiek toegankelijke communicatie*"[114]. Dit houdt in dat heimelijk afluisteren (onderscheppen) of heimelijk opnemen van een gesprek waaraan men **niet** deelneemt onder de strafbaarstelling van de artikelen 314*bis* of 259*bis* Sw. valt. Het eerste artikel beschermt de communicatie in hoofde van particulieren, terwijl het tweede artikel bescherming biedt tegen inbreuken door (politie)ambtenaren[115]. Inbreuken op de bescherming van de communicatie zijn slechts mogelijk indien en in de mate dat de wet daarin voorziet, zoals in de omstandigheden en onder de voorwaarden geregeld in artikel 90*ter* van het wetboek van Strafvordering.

Zowel gewone gesprekken als telecommunicatie worden beschermd. Het gaat om communicatie dat zich in de privésfeer afspeelt[116]. De term 'privé' mag niet restrictief gelezen worden. Alle communicatie wordt beschermd, ook al wordt niet noodzakelijk geraakt aan het privéleven van de deelnemers aan het gesprek. Als het gesprek niet bedoeld is om door derden beluisterd te worden, gaat om op 'privécommunicatie' of 'niet voor het publiek toegankelijke communicatie' in de zin van artikel 259*bis* (en artikel 314*bis*) Sw. Met andere woorden, ook gesprekken in een professionele context worden beschermd[117]. De bescherming is bovendien niet plaatsgebonden maar hangt eerder af van de context en de intenties van de deelnemers aan het gesprek. Een gesprek valt bijgevolg onder de bescherming van het communicatiegeheim wanneer ze niet bestemd is om door iedereen gehoord te worden, waar deze zich ook plaatsvindt, in de huiskamer, op het werk of in de publieke ruimte[118].

Artikel 259*bis* Sw. bestraft ook het onwettig kennisnemen van communicatie waaraan men niet deelneemt. Niet alleen degene die gesprekken opneemt, zal er kennis van nemen. Behalve de politieambtenaar die het gesprek opneemt, is de communicatie (de beelden met audio) doorgaans ook toegankelijk voor de politionele hiërarchie (in het kader van een tuchtonderzoek bijvoorbeeld of gewoon voor interne kwaliteitscontrole).

---

[114] Art. 30 tot en met 32 van de wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en de oprichting van een gegevensbank stemafdrukken. Door deze wet werden de woorden "*privé-communicatie of -telecommunicatie*" in de artikelen 314bis en 259bis van het Strafwetboek vervangen door "*niet voor het publiek toegankelijke communicatie*". Het gaat om een loutere terminologische wijziging (Parl. St. *Kamer* 2015-2016, nr. 54-1966/001, 75). Bovendien is ook het bestanddeel "*tijdens de overbrenging*" uit beide strafbepalingen geschrapt.

[115] Artikel 259*bis* Sw. luidt als volgt:

"§ 1. Met gevangenisstraf van zes maanden tot drie jaar en met geldboete van vijfhonderd euro tot twintigduizend euro of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft :

1° ofwel, opzettelijk, met behulp van enig toestel niet voor publiek toegankelijke communicatie, waaraan hij niet deelneemt, onderschept of doet onderscheppen, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie;

2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen;

3° ofwel wetens de inhoud van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem die onwettig onderschept of opgenomen zijn of waarvan onwettig kennis genomen is, onder zich houdt, aan een andere persoon onthult of verspreidt, of wetens enig gebruik maakt van een op die manier verkregen inlichting.

§ 2. Met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van vijfhonderd euro tot dertigduizend euro of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk te schaden, gebruik maakt van een wettig gemaakte opname van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem.

§ 2bis. Met gevangenisstraf van zes maanden tot drie jaar en met geldboete van vijfhonderd euro tot twintigduizend euro of met één van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, onrechtmatig, een instrument, met inbegrip van informaticagegevens, dat hoofdzakelijk is ontworpen of aangepast om het in § 1 bedoelde misdrijf mogelijk te maken, bezit, produceert, verkoopt, verkrijgt met het oog op het gebruik ervan, invoert, verspreidt of op enige andere manier ter beschikking stelt.

§ 3. Poging tot het plegen van een der misdrijven bedoeld in §§ 1, 2 of 2bis wordt gestraft zoals het misdrijf zelf.

§ 4. De straffen gesteld in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten beoogd in artikel 314bis, §§ 1 tot 3, dat in kracht van gewijsde is gegaan."

[116] De wijziging van de terminologie doet geen afbreuk aan de draagwijdte van het begrip 'prive-communicatie' in het oude artikel (Parl. St. *Kamer* 2015-2016, nr. 54-1966/001, 53).

[117] Verslag bij het wetsontwerp, Parl. St. *Senaat* 1992-1993, nr. 843/2, 11 (verslag wetsontwerp).

[118] Verslag bij het wetsontwerp, Parl. St. *Senaat* 1992-1993, nr. 843/2, 10 (verslag wetsontwerp).

De bescherming geldt alleen indien het gesprek wordt onderschept, opgenomen of ervan kennis wordt genomen door gebruik te maken van een technisch hulpmiddel. Het louter zintuigelijk meeluisteren is dus niet strafbaar en stelt geen probleem. Wanneer derhalve diverse politieambtenaren actief en/of passief (zintuigelijk) deelnemen aan het gesprek/interactie stelt zich voor hen dus geen probleem.

Het betekent wel dat de politieambtena(a)r(en) die het gesprek afluister(en)t, opne(e)m(en)t of ervan kennis neemt zonder dat de voorwaarden van art. 25/2 § 2, 2°, b) WPA én art. 259*bis* Sw. worden nageleefd zich aan strafbaarstelling blootstelt.

Het loutere feit dat de politie verantwoordelijk is voor het welzijn van de arrestant kan niet als een expliciete uitzondering op de bescherming van de communicatie worden beschouwd. De (Europese) rechtspraak heeft reeds herhaaldelijk gesteld dat een uitzondering op dit grondrecht expliciet en duidelijk (de eis van voorzienbaarheid) moet geregeld zijn (omstandigheden waarin en voorwaarden waaronder een inbreuk op de bescherming van de communicatie is toegestaan). Het loutere feit dat men in de politiecel beland en daardoor onder de verantwoordelijkheid van de politie valt, rechtvaardigt op zichzelf bijvoorbeeld dus niet de opname van een monoloog van de arrestant zonder zijn toestemming.

Zoals het COC in het *bodycam*[119] advies verdedigt, kan de politie in sommige situaties als 'deelnemer' aan de communicatie worden aanzien. Dit kan, naar het oordeel van het COC, *in casu* het geval zijn wanneer de politieambtenaar via de intercom peilt naar de toestand van de arrestant en daarbij de communicatie opneemt. Dat kan ook omgekeerd het geval zijn wanneer de arrestant via de intercom/noodknop contact opneemt met de politieambtenaar. Het is niet zonder belang dat de arrestant daarvan voorafgaandelijk op de hoogte wordt gebracht. Maar, de systematische opname van de communicatie van de arrestant zal hoogstwaarschijnlijk een inbreuk zijn op artikel 259*bis* Sw. precies omdat de politie niet automatisch als een deelnemer aan het gesprek kan worden beschouwd. Ook een algemene aankondiging in het cellencomplex staat niet gelijk met de (impliciete) toestemming van de arrestant[120].

4.2.2.3 Toegangscontrole

47. De camerabewaking voor de toegangscontrole tot de gebouwen waarin de lokalen van SPC zijn gesitueerd gebeurt in elk gebouw waar SPC gevestigd is. Het gebruik ervan wordt volgens de directie SPC duidelijk aangegeven door een pictogram. Het COC kon ter plaatse, voor wat SPC Brussel betreft, de aanwezigheid van het pictogram vaststellen, doch stelt tevens vast dat de SPC Brussel niet vermeld staat als verantwoordelijke van de verwerking, en stelt tevens vast dat het politielogo afwezig is. Het is onduidelijk hoe de bewaartermijnen geregeld zijn; volgens de directie SPC hangt dit af van elke locatie. Voor de gebouwen van SPC Brussel wordt gesteld, dat de toegangscontrole middels camerabewaking gebeurt door de diensten van de Regie der Gebouwen.

Ook deze onduidelijkheden maken het voorwerp uit van de corrigerende maatregel 2.

---

[119] Advies uit eigen beweging van het Controleorgaan naar aanleiding van de bevindingen in het kader van een onderzoek naar het gebruik van *bodycams*, 8 mei 2020, CON19008.

[120] Repliek van SPC in het raam van tegenspraak: *Hoewel we deze bedenking begrijpen, menen wij dat de opname van geluid in de cel alsnog noodzakelijk is aangezien de geluidsopname van personen die van hun vrijheid beroofd zijn, het mogelijk maakt om in gevallen waarin camerabeelden een situatie niet adequaat kunnen weergeven, de aandacht van de politie te vestigen op een gebeurtenis die hun optreden vereist. Bijvoorbeeld wanneer een gearresteerde die niet langer in staat is zijn ongemak fysiek uit te drukken. Het is duidelijk dat eventuele gesprekken tussen twee gedetineerden niet kunnen worden gebruikt voor bewijselementen in het kader van de procedure tegen hen, maar in het kader van hun bewaking betreft dit een noodzakelijkheid. De Commissie voor de bescherming van de persoonlijke levenssfeer heeft dit standpunt trouwens ook onderschreven in haar aanbeveling nr. 06/2011 van 6 juli 2011 betreffende installatie en* gebruik *van bewakingscamera's in opsluitingsplaatsen (cellen en arrestantenlokalen) en andere plaatsen van het commissariaat (CO-AR-2010-04).* Als antwoord op deze repliek stelt het COC evenwel dat er in het randnummer 37 van de aanbeveling van 06 juli 2011 van de GBA inderdaad sprake is van 'geluidsopname', die de GBA "gunstig gezind" is. Er moet evenwel voor ogen worden gehouden dat het niet duidelijk is of de GBA daaronder ook de daadwerkelijke en automatische opname van gesprekken (communicatie) begrijpt. In de memorie van toelichting bij de wet van 21 maart 2018, die het gebruik van camerabewaking door politiediensten regelt, is ook sprake van 'geluidsopname'. De wetgever heeft evenwel nagelaten dit in de WPA te regelen. Door het gebrek aan uitdrukkelijke regeling in de WPA, pleegt de politieambtenaar desgevallend een inbreuk op artikel 259bis Sw. doordat (1) de WPA geen uitzondering maakt op artikel 259bis Sw. en (2) dit terwijl de wetgever in de memorie van toelichting uitdrukkelijk stelt dat de politie de toepassing van deze bepaling (zij het artikel 314bis Sw., dat betrekking heeft op particulieren en analoog is aan artikel 259bis Sw.) moet respecteren. Zo beschouwd moet randnummer 37 van het GBA-advies (onvermijdelijk) ook in die zin worden gelezen.

4.2.3 Visie op een cameranetwerk GPI

48. Het opbouwen van het nationaal *ANPR* netwerk[121]heeft gezorgd voor een glasvezelconnectiviteit tussen een aantal nationaal of gewestelijk verspreide glasvezelnetwerken en het Datacenter van de GPI in Brussel. Tevens beschikken het NIP[122]als nationale component van de GPI, de 10 meldkamers van de provinciale CIC[123]als gedeconcentreerde component van de GPI alsmede de dienst Luchtsteun (DAFA) van de federale politie en vele dispatchings van lokale politiezones over een VMS[124], die dus het *real time* volgen van beelden alsmede de opslag en verdere verwerking toelaat.

De federale VMS systemen, zijnde deze van het NIP, van de meldkamers van de CIC en van de dienst Luchtsteun zijn al onderling met elkaar verbonden om de beelden van de helicopters en/of de *drones*, die middels 8 masten gecapteerd en doorgestuurd worden naar de VMS van DAFA, te kunnen ontvangen. Aldus vormt dit systeem alsmede de deelnemende VMS systemen de facto een *backbone* voor wat verder nationaal zou kunnen uitgerold worden. Deze backbone, gekoppeld aan de reeds genoemde glasvezelnetwerken, kunnen aldus gebruikt worden om zowel politionele (WPA) als camera's van derde partijen (Camerawet) te ontvangen en verder te ontsluiten.

Een videomanagementsysteem, ook bekend als videomanagementsoftware of een videomanagementserver, is een onderdeel van een beveiligingscamerasysteem dat in het algemeen:

- beelden van camera's en andere bronnen verzamelt;
- beelden opslaat;
- een interface biedt om zowel de live video te bekijken als toegang te krijgen tot opgeslagen beelden.

Door de verbeteringen in de technologie is het noodzakelijk een onderscheid te maken tussen een VMS en de ingebouwde functies van moderne, netwerkgebaseerde beveiligingscamera's. Veel moderne netwerkcamera's bieden interne mogelijkheden om zelf rechtstreeks videobeelden op te nemen en te bekijken via een webbrowser en zonder gebruik te maken van een VMS. De ingebouwde webinterface van een camera is echter meestal exclusief voor de camera zelf en biedt normaal gesproken geen gedeelde toegangsmogelijkheid voor andere netwerkcamera's. Voor een geïntegreerde aanpak is een VMS dus noodzakelijk. Het juridisch statuut van een dergelijk VMS systeem is nog onduidelijk en alleszins niet expliciet geregeld. Wettelijk gezien kunnen deze niet het statuut krijgen van technische gegevensbank daar dit type van gegevensbank[125]momenteel enkel voorzien is voor intelligente camera's of systemen van nummerplaatherkenning. Deze zullen dan afzonderlijk dienen aangegeven te worden als bijzondere gegevensbank[126], waarbij de richtlijnen inzake toegangen en koppelingen uitsluitsel zullen dienen te geven over een aantal gebruiksmogelijkheden binnen de GPI.

Als de verschillende bestaande VMS binnen de GPI zich in één videobewakingssysteem federeren, met een geconsolideerde juridische status alsmede zijn eigen functioneel videomodel, wordt de videosynergie tussen de GPI en haar externe partners aanzienlijk vergemakkelijkt: standaardovereenkomsten en protocolakkoorden, model *DPIA*'s en één technische aansluiting zouden dan volstaan om de uitwisseling van camerabeelden te verwezenlijken. Aldus zouden zij een toegangspoort vormen voor camerabeelden die politioneel kunnen gebruikt worden, wat enerzijds een risico zou kunnen vormen indien niet de gepaste mitigerende maatregelen worden genomen, maar anderzijds aanzienlijke voordelen biedt voor een kwalitatiever gegevensbeheer en een verminderd potentieel voor misbruik van gegevens; een uniform veiligheidsbeleid zou kunnen toegepast worden waarbij sterke garanties naar traceerbaarheid en vertrouwelijkheid van gegevens geboden kunnen worden, wat het operationele politionele cameragebruik alleen maar ten goede kan komen.

49. De NMBS camera's zijn middels het glasvezelnetwerk van Infrabel geconnecteerd. Dit glasvezelnetwerk is eveneens geconnecteerd met het Datacenter van de GPI. Indien dus ook de betrokken meldkamers van de CIC en eventueel zelfs de lokale politiezones aangesloten zijn op een van de deelnemende netwerken, kunnen de camerabeelden aldus

[121] Regeringsbeslissing dd 19-11-2015 inzake de 18 maatregelen in de strijd tegen het terrorisme.
[122] **N**ationaal **I**nvals**P**unt.
[123] CIC staat voor **C**ommunicatie en **I**nformatie **C**entrum. Het is de eerste pijler van de provinciale SICAD werking, die instaat voor het *real time* gebeuren via de calltaking en de dispatching van de ploegen op het terrein. Het AIK is de tweede pijler van de SICAD werking; deze staat in voor de verwerking van de informatie in tweede lijn.
[124] ***V**ideo **M**anagement **S**ysteem.*
[125] Art 44/2 §3 WPA.
[126] Art Art 44/11/3 WPA.

technisch beschikbaar worden gesteld indien ook aan alle juridische voorwaarden werd voldaan. Zo wordt het bijvoorbeeld operationeel denkbaar om geplande operaties of incidenten inzake fenomenen zoals koperdiefstallen langs spoorlijnen via beeldverwerking op te volgen door beelden van bewakingscamera's van de NMBS langs de spoorlijnen samen met beelden van mobiele luchtvaartuigen zoals *drones* of helicopters door te sturen naar het VMS van het al dan niet mobiele commandocentrum of meldkamer van waaruit de operatie of het incident wordt geleid. Eventueel betrokken voertuigen kunnen via het nationaal *ANPR* netwerk vanuit hetzelfde commandocentrum of meldkamer worden opgespoord, waardoor de betrokken ploegen tactisch kunnen worden aangestuurd. Zeker in dergelijke gevallen is de WPA onverminderd van toepassing, ook al worden de beelden niet meteen opgeslagen. Het gaat immers om een politionele operatie. Door een eventuele opname achteraf te herbekijken of een zoekopdracht te voeren naar personen met bepaalde kenmerken zoals bijvoorbeeld het 'dragen van een gele rugzak', kan ook recherchematig met de problematiek worden omgegaan. Bij uitbreiding geldt hetzelfde voor camera's van andere verwerkingsverantwoordelijken zoals de Gewesten, die geïnstalleerd werden op gewest- of autosnelwegen met als primaire finaliteit opvolging van verkeersstromen. Ook de netwerken waarvan deze gebruik maken zijn namelijk geconnecteerd op het Datacenter van de GPI.

De geconsolideerde juridische status lijkt in het huidig wetgevend kader enkel maar mogelijk te zijn door een VMS het statuut te geven van een bijzondere gegevensbank (GBO). Op middellange tot lange termijn lijkt hier een wetgevend initiatief sterk aan te bevelen, door de verwerking van beelden van bewakingscamera's onder te brengen in een bijkomend type van technische gegevensbanken in de zin van art 44/2 §3 WPA, en de artikelen 44/11/3*sexies* tem 44/11/3*decies* WPA. Beeldverwerking onder de WPA gebeurt immers in het kader van de uitvoering van de opdrachten van bestuurlijke en gerechtelijke politie, en de in de VMS geregistreerde informatie is op een dergelijke wijze gestructureerd dat zij rechtstreeks kan teruggevonden worden. Afhankelijk van de technische mogelijkheden zal bekeken moeten worden of er naar een nationale gegevensbank dient gestreefd te worden, eerder dan naar verschillende, geïnterconnecteerde lokale technische gegevensbanken van het type beeldverwerking. In elk geval biedt een dergelijke benadering, ondanks de ruimere opslag, verwerkings- en toegangsmogelijkheden op termijn meer en betere garanties op bescherming van de (persoons)gegevens enerzijds en een duidelijke operationele meerwaarde anderzijds.

4.2.4 Conclusies voor Camerabewaking

4.2.4.1 Ter attentie van de beleidsverantwoordelijken en de verantwoordelijke Ministers

Aanbeveling 1

Het COC beveelt de beleidsverantwoordelijken en de verantwoordelijke Ministers aan, na te denken over wetgevende initiatieven die een onderscheid maken tussen de systematische en casuïstische real time overdracht van camerabeelden onder gelding van artikel 9 van de Camerawet en artikel 4 van het Uitvoeringsbesluit, en de systematische real time overdracht voor politioneel gebruik te regelen onder de bepalingen van de WPA eerder dan onder de bepalingen van de Camerawet.

Aanbeveling 2

Het COC beveelt de beleidsverantwoordelijken en de verantwoordelijke Ministers aan om gestalte te geven aan een globale en geïntegreerde visie op cameragebruik binnen de GPI middels het concept van een Video Management Systeem en een geconsolideerde juridische status te geven aan beeldverwerkingen binnen de GPI door het creëren van een bijkomend type van technische gegevensbank onder de bepalingen van de WPA.

4.2.4.2 Ter attentie van de SPC

Aanbeveling 3

Met het oog op de operationele meerwaarde voor de GPI, beveelt het COC de SPC aan om met de verantwoordelijke van de verwerking van de vervoersmaatschappijen na te gaan of aan de verplichtingen inzake aangifte en pictogram werd voldaan. Hetzelfde geldt voor de handelaars die aanwezig zijn in de stations en eveneens beschikken over systemen van camerabewaking.

Aanbeveling 4

Met het oog op de operationele meerwaarde voor de GPI beveelt het COC de SPC aan om aan de ontwikkelaars van CamELIA te verzoeken om de rapportage mogelijkheden uit te breiden. Het lijkt bovendien opportuun om in de toepassing ook het onderscheid te maken tussen camera's gebruikt door de politie onder de bepalingen van de WPA en de camera's waartoe de politie in real time toegang heeft middels toepassing van artikel 9 van de Camerawet.

Verzoek 1

Het COC verzoekt de Directie SPC om met DGA de opportuniteit te bekijken inzake het verlenen van toestemmingen door DGA tot gebruik van camera's binnen dezelfde directie en dit aspect dus op te nemen met de voogdijoverheid.

Verzoek 2

Het COC verzoekt de SPC de nodige stappen te ondernemen ten aanzien van de verwerkingsverantwoordelijken om de noodzakelijke protocolakkoorden af te sluiten conform de bepalingen van de Camerawet van 21 maart 2007.

Verzoek 3

Het COC verzoekt de SPC om het testproject inzake installatie van ANPR camera's aan spoorwegovergangen mee op te volgen.

Corrigerende maatregel 1

Gelet op de vaststellingen zoals vermeld in randnummer 40, met name het ontbreken van registraties van beeldverwerkingen in het REGPOL register enerzijds, en het ontbreken van een register voor cameragebruiken anderzijds;

beveelt het COC de SPC Brussel om de verwerkingen aan de hand van het bekijken van de beelden van de vervoersmaatschappijen te vermelden in het register REGPOL en dit binnen de drie maanden na ontvangst van het rapport.

Corrigerende maatregel 2

Gelet op de vaststellingen zoals vermeld in randnummers 45, 46 en 47, met name de afwezigheid van de registraties van het cameragebruik in de cellen van de 4 regio's buiten Brussel, het mogelijk onderscheppen of heimelijk afluisteren van de gesprekken in de cellen van de 4 regio's, en de onduidelijkheden met betrekking tot de toegangscontroles;

beveelt het COC de directie SPC om de camera- en geluidsverwerkingen in de gebouwen van de 4 regio's van de SPC buiten Brussel in overeenstemming te brengen met het vigerend wettelijk kader op het vlak van verzameling, bewaring, toegang en logging en dit binnen de zes maanden na ontvangst van dit rapport.

4.3 Databanken

4.3.1 Registraties in REGPOL

50. Zoals eerder gesteld, blijkt SPC tot op het moment van de visitatie geen registraties van verwerkingen gedaan te hebben in REGPOL. Volgens een schrijven van CG/ISPO van 14-04-2021, na een vraagstelling van het COC dienaangaande, blijkt SPC evenwel wel degelijk registraties gemaakt te hebben in het systeem vóórafgaand aan REGPOL, met name het 'registratiesysteem GBO' daterend van voor de wetswijziging in 2018. CG/ISPO stelt daarbij, dat de nodige instructies werden gegeven aan de DPO om vattingen gedaan in dit oude register om te zetten naar REGPOL. SPC stelt hieromtrent, dat ze het nodige zullen doen om de registraties in REGPOL in orde te brengen[127].

Het ontbreken van deze registraties is evenwel de reden om over te gaan tot het nemen van de corrigerende maatregel 3.

[127] Repliek van SPC in het raam van tegenspraak: *Dienaangaande kunnen we melden dat deze conversie ondertussen progressief is aangevangen.* Als antwoord op deze repliek stelt het COC evenwel dat bij een *prima facie* nazicht van de registraties van SPC in REGPOl op 24-09-2021 zijnde twee dagen na ontvangst van de repliek, er welgeteld één registratie is bijgekomen, die bovendien een bezoekersregister is en dus geen GBO (record ID 4976). Ook op 05-11-2021 blijkt dit nog steeds het geval.

Het gebrek aan registraties specifiek met betrekking tot de bijzondere gegevensbanken wijst tevens op een gebrek aan een beleid hieromtrent wat aanleiding geeft tot het nemen van de corrigerende maatregel 4.

4.3.2 ANG werking en basisgegevensbanken

51. Op het vlak van de ANG werking stelt SPC dat de fiche D41[128]van de MFO3 wordt toegepast, en dat slechts een beperkt aantal leden van de SPC toegang hebben tot het 'recherche' profiel, zoals de functioneel beheerders en de leden van de cel radicalisme. Het feit dat een beperkt aantal leden van de SPC toegang heeft tot dit profiel wil evenwel niet zeggen dat er ook onderzoeken worden gevoerd. SPC stelt dat geen enkele van de door hen gevoerde onderzoeksdaden verloopt op een wijze die een coördinatie inhoudt in de zin van de fiche C13[129]van de MFO3. Ze maken dan ook geen gebruik van een specifieke basisgegevensbank onderzoeken zoals bijvoorbeeld de GES[130]applicatie en stellen ook geen DOS formulieren op. Voortbouwend op deze discussie stelt SPC tevens, dat zij als eerstelijnseenheid van DGA niet instaat voor de basispolitiezorg[131]binnen hun verantwoordelijkheidsdomein zijnde de spoorwegen, doch zich enkel beperken tot taken van bestuurlijke politie. Slechts in zeer beperkte mate houdt SPC zich bezig met taken van gerechtelijke politie. Het COC deelt deze visie niet, daar voor elk van de zeven componenten voorbeelden kunnen gevonden worden van een concrete, mogelijk specifieke, toepassing binnen de SPC werking (denken we maar aan de APO dossier, cf. randnummer 54). De loutere beperking tot bestuurlijke opdrachten vertaalt zich evenwel niet in een toegang tot BEPAD[132]. De vraag is dan ook, hoe de SPC haar bestuurlijke opdrachten registreert.

52. Er vinden grondige controles plaats op de toegangen verstrekt op basis van de fiche D41. Dit is niet eenvoudig, omdat de SPC als geheel een tiental eenheidscodes omvat, en elke beweging van personeelsleden tussen een van deze eenheidscodes of bewegingen van personeelsleden die de SPC vervoegen of deze verlaten, nauwgezet dienen opgevolgd te worden. Dit wordt ook toegepast ingevolge langdurige afwezigheden, als gevolg van dewelke de toegangen ook worden afgesloten voor de duur ervan. Dit is met name van belang voor mobiele toepassingen zoals *BeSecure*[133], een toepassing waarvan SPC een zestigtal pool-licenties heeft. In elk geval, in tegenstelling tot de heersende politiecultuur waarbij geen enkele of veel te weinig aanpassing plaatsvindt aan het profiel van de gebruiker in geval van mobiliteit, voert de SPC bewust een beleid waarbij bij elke mutatie-*out* het profiel systematisch op "*geen toegang*" wordt gezet voor de operationele, politionele toepassingen. Dit geldt evenwel niet voor de toepassingen via de Office 365 GPI.

De specifieke organisatie van de eenheidscodes en de talrijke hoeveelheid gedetacheerde medewerkers maakt tevens, dat controles op de loggings van ANG consultaties door medewerkers van SPC niet evident zijn.

53. De SPC staat zelf in voor haar eigen functioneel beheer. Daartoe worden contacten onderhouden met de SICAD-AIK. Specifiek voor SPC Brussel worden tevens nauwe contacten onderhouden met de functioneel beheerders van de zes Brusselse politiezones.

54. SPC Brussel stelt dat, ingevolge lokale parketrichtlijnen, de APO[134]dossiers in de eigen eenheid bewaard dienen te worden. Deze opslag bij de SPC Brussel heeft wel zijn limieten inzake bewaring. Het parket is daarom akkoord met een ventilatie van deze dossiers na 5 jaar.

---

[128] De fiche D41 regelt het beheer van de toegangen en de veiligheid van de gegevens in de ANG.
[129] De fiche C13 van de MFO3 heeft betrekking op de coördinatie van de onderzoeken via de ANG en wordt gematerialiseerd via het opstellen van een DOS formulier.
[130] GES, *Police Search* GES, BNBB, *Datamapper* en ITINERA zijn de verschillende toepassingen die het geïntegreerd beheer van de onderzoeken voor alle politiezones en eenheden van de Geïntegreerde Politie mogelijk maken. De toepasisng GES kan in deze beschouwd worden als de basisgegevensbank voor onderzoeken zoals gedefinieerd in art 44/11/2 §6 WPA.
[131] Om te voldoen aan de basispolitiezorg zijn er 7 basisfunctionaliteiten voorzien.
Deze zijn: onthaal, wijk, interventie, verkeer, recherche, slachtofferbejegening en handhaving openbare orde.
[132] BePad (Bestuurlijke Politie-Police Administrative) is een toepassing/gegevensbank die een geïntegreerde oplossing aanbiedt voor de uitwisseling en het operationele beheer van de informatie bestuurlijke politie. Meer dan een 'eenvoudige' toepassing, biedt BePad naast een geïntegreerde opvolging voor evenementen, groeperingen en personen ook een communicatiesysteem tussen de eenheden en de partners van de GPI.
[133] *BeSecure* is een toepassing die via het internet en een standaardbrowser toegang biedt tot de politionele intranetomgeving met inbegrip van de specifieke politietoepassingen, dus gegevensverwerkingen die vallen onder de titel 2 WGB.
[134] **A**mbtshalve **p**olitioneel **o**nderzoek.

55. SPC maakt nog geen gebruik van FOCUS[135]. De implementatie ervan is eerder voor de lange termijn, daar alle finaliteiten momenteel bereikt kunnen worden via de huidige manier van werken. Ook is het niet de bedoeling om andere dan gevalideerde ANG gegevens te delen met politiezones op wiens grondgebied wordt gewerkt.

4.3.3 Bijzondere gegevensbanken

56. Daar waar SPC initieel stelde geen bijzondere gegevensbanken te beheren, bleek uit het gesprek dat SPC Brussel verantwoordelijke is van de verwerking van minstens één bijzondere gegevensbank met name "*Apollo*". Deze GBO bleek reeds aangegeven te zijn volgens het oude systeem zoals supra gemeld, maar is gezien de afwezigheid van welke registratie dan ook in REGPOL niet aangegeven in dit register. Gelet op de eerdere registraties van bijzondere gegevensbanken in de module 'registratiesysteem GBO', gelet op de afwezigheid van registraties van bijzondere gegevensbanken in REGPOL en gelet op het feit dat SPC stelde geen bijzondere gegevensbanken te beheren en er uiteindelijk toch minstens een lijkt te beheren, lijkt er geen duidelijk beleid te zijn inzake bijzondere gegevensbanken.

Het gegeven van het afwezigheid van beleid omtrent bijzondere gegevensbanken maakt zoals vermeld onder randnummer 50 het voorwerp uit van de corrigerende maatregel 4.

De specifieke aangifte van de gegevensbank *"Apollo"* maakt het voorwerp uit van de corrigerende maatregel 5.

4.3.4 Internationale politiesamenwerking

57. Op het vlak van de internationale politiesamenwerking past de SPC de principes van de MFO3 toe[136], en maakt daarbij gebruik van de daartoe bestemde formulieren[137]INI en INO. Er is geen internationale uitwisseling van persoonsgegevens buiten de voorziene processen via CGI[138], ook niet via het internationale samenwerkingsverband tussen spoorwegpolitiediensten RAILPOL[139], dat voornamelijk geldt als strategisch overlegforum.

4.3.5 Gegevensbanken van vervoersmaatschappijen

58. SPC stelt dat het geen toegang heeft tot databanken van de vervoersmaatschappijen.

4.3.6 Data breaches

59. SPC stelt, dat er tot op heden nog geen *databreaches* zijn geweest.

4.3.7 Ontwikkelingen van informaticatoepassingen

60. SPC dient de behoeften voor het ontwikkelen van informaticatoepassingen over te maken aan DGA die de relevantie ervan bekijkt en prioriteiten stelt alvorens de behoefte over te maken aan DRI.

4.3.8 Conclusies voor databanken

Aanbeveling 5

Inzake de functionele behoeften van informaticatoepassingen roept het COC de SPC op om zoveel als mogelijk aansluiting te zoeken bij bestaande applicaties en in voorkomend geval bijkomende behoeften vooral te enten op functionaliteiten binnen reeds bestaande toepassingen. Het verdient de voorkeur om behoeften inzake personeelsbeheer te bekijken in het licht van de mogelijkheden van de toepassing GALOP, eerder dan in een door DGA eigen ontwikkelde tool.

Verzoek 4

Het COC verzoekt de SPC op stelselmatige en proactieve wijze controles uit te voeren betreffende het gebruik en/of de consultatie van de politionele gegevensbanken, meer bepaald door elke maand of elk kwartaal controles te verrichten op basis van steekproeven met behulp van loggings. Het COC zal aandringen bij de verantwoordelijken GPI om deze

[135] FOCUS biedt in één platform een bundeling van vele politietoepassingen. Gebruikers vinden er eerst en vooral een integraal aanbod aan politionele informatiebronnen. Het platform biedt daarnaast alle mogelijkheden om *live* te communiceren en informatie te delen tijdens operaties en dagelijks werk. Tenslotte kan de politiemedewerker in FOCUS op de meest eenvoudige wijze vaststellingen (PV's, RIR, ...) invoeren of dossiers aanvullen.

[136] Deze principes worden toegelicht in de fiches C21 (Internationale politionele samenwerking) en C22 (Internationale signaleringen).

[137] De formulieren INO en INI laten een beheer toe van de uitgaande (INO) en inkomende (INI) internationale informatie via de dienst CGI.

[138] Directive van de internationale politiesamenwerking.

[139] Railpol is een internationaal netwerk van samenwerkende spoorwegpolitieorganisaties voor lidstaten van de Europese Unie. De organisatie heeft als doel de samenwerking en kennis- en informatie-uitwisseling tussen de verschillende nationale spoorwegpolitieorganisaties te versterken en de veiligheid van het Europese spoorwegnet te verbeteren. Railpol wordt gesubsidieerd door de EU. Deelnemende landen zijn Oostenrijk, Bulgarije, Nederland (voorzitter), België, Duitsland, Tsjechië, Frankrijk, Hongarije, Italië, Letland, Roemenië, Slowakije, Spanje en Zwitserland en Engeland. Niet-Europese organisaties, zoals de *Amtrak Police* en de TSA uit de Verenigde Staten, nemen periodiek ook deel aan overlegmomenten.

controles te faciliteren door het aanleveren van aangepaste tools. De resultaten van de controles dienen beschikbaar te worden gehouden voor het COC. Specifiek met betrekken tot de problematiek van de gedetacheerden en de verschillende eenheidscodes verzoekt het COC de SPC, de loggings tevens op te vragen op de specifieke terminalnummers die toegekend zijn aan SPC, en na te kijken of de terminals toegekend aan SPC nog steeds overeenstemmen met de realiteit van het terrein.

Corrigerende maatregel 3

Gelet op de vaststellingen zoals vermeld in randnummer 50, met name dat er geen registraties van verwerkingen werden aangetroffen in het REGPOL register;

beveelt het COC SPC om de bepalingen van art 55 WGB correct toe te passen op het vlak van registratie van verwerkingsactiviteiten die onder de verantwoordelijkheid van SPC vallen en zich daartoe te enten op de interne bepalingen van de federale politie, en dit binnen de zes maanden na ontvangst van dit rapport.

Corrigerende maatregel 4

Gelet op de vaststellingen zoals vermeld in randnummer 50 en randnummer 56 met name de vaststelling dat het aan een duidelijk beleid omtrent bijzondere gegevensbanken binnen SPC ontbreekt en dit omwille van het ontbreken van registraties van bijzondere gegevensbanken in het REGPOL register en het onduidelijke overzicht of er al dan niet bijzondere gegevensbanken in gebruik zijn bij SPC;

beveelt het COC de SPC, om, al dan niet in samenspraak met DGA, een duidelijk beleid op te stellen inzake de bijzondere gegevensbanken en dit ook consequent toe te passen en dit binnen de zes maanden na ontvangst van dit rapport.

Corrigerende maatregel 5

Gelet op de vaststelling zoals vermeld in randnummer 56, met name dat er bijzondere gegevensbank genaamd "Apollo" in gebruik is bij de SPC Brussel;

beveelt het COC de SPC Brussel om de GBO "Apollo" correct te registreren als GBO in het register van de verwerkingsactiviteiten en dit binnen de maand na ontvangst van dit rapport.

4.4 Triptiek en EURODAC

4.4.1 Algemeen

61. In het algemeen verloopt de afname van de gerechtelijke triptiek conform de bepalingen van de MFO3. Deze vindt plaats in de lokalen van het RAC te Brussel.

62. De SPC stelt enkel dossiers vreemdelingen op te stellen wanneer er een inbreuk is op de vreemdelingenwetgeving. Er zijn minder dan 100 van dergelijke gevallen per jaar.

In deze gevallen wordt de afname van de triptiek overgemaakt aan de DVZ[140]voor verdere verwerking aldaar middels het daartoe bestemde vakje in de toepassing.

Asielzoekers die zich als dusdanig aanbieden, worden niet *a priori* aanzien als overtreders op de vreemdelingenwetgeving.

De SPC stelt zelf geen vragen op basis van het art 32 van de EURODAC Verordening.

4.4.2 Conclusies voor Triptiek en Eurodac

Aanbeveling 6

Het COC beveelt de SPC aan, om de afname van de gerechtelijke triptiek aan te wenden als mogelijkheid voor een verificatie van de kwaliteit van de vatting in de ANG van de persoon die het voorwerp uitmaakt van de afname, en dit op het vlak van de individuele beschrijving, de foto en de vingerafdrukken en in voorkomend geval over te gaan tot de fusie van de entiteit indien blijkt dat deze meerdere malen werd gevat in de ANG.

[140] **D**ienst **V**reemdelingen **Z**aken.

5 CONCLUSIE – AANBEVELINGEN, VERZOEKEN EN CORRIGERENDE MAATREGELEN

OM DEZE REDENEN,

Het Controleorgaan;

brengt de volgende aanbevelingen uit,

5.1 Ten aanzien van de beleidsverantwoordelijken en de verantwoordelijke Ministers

Aanbeveling 1

Het COC beveelt de beleidsverantwoordelijken en de verantwoordelijke Ministers aan, na te denken over wetgevende initiatieven die een onderscheid maken tussen de systematische en casuïstische *real time* overdracht van camerabeelden binnen artikel 9 van de Camerawet, en de systematische *real time* overdracht voor politioneel gebruik te regelen onder de bepalingen van de WPA eerder dan onder de bepalingen van de Camerawet.

Aanbeveling 2

Het COC beveelt de beleidsverantwoordelijken en de verantwoordelijke Ministers aan, om gestalte te geven aan een globale en geïntegreerde visie op cameragebruik binnen de GPI middels het concept van een Video Management Systeem en een geconsolideerde juridische status te geven aan beeldverwerkingen binnen de GPI door het creëren van een bijkomend type van technische gegevensbank onder de bepalingen van de WPA. .

5.2 Ten aanzien van de SPC

Aanbeveling 3

Met het oog op de operationele meerwaarde voor de GPI, beveelt het COC de SPC aan, om met de verantwoordelijke van de verwerking van de vervoersmaatschappijen na te gaan of aan de verplichtingen inzake aangifte en pictogram werd voldaan. Hetzelfde geldt voor de handelaars die aanwezig zijn in de stations en eveneens beschikken over systemen van camerabewaking.

Aanbeveling 4

Met het oog op de operationele meerwaarde voor de GPI, beveelt het COC de SPC aan om aan de ontwikkelaars van *CamELIA* te verzoeken om de rapportagemogelijkheiden uit te breiden. Het lijkt bovendien opportuun om in de toepassing ook het onderscheid te maken tussen camera's gebruikt door de politie onder de bepalingen van de WPA, en de camera's waartoe de politie in *real time* toegang heeft middels toepassing van artikel 9 van de Camerawet.

Aanbeveling 5

Inzake de functionele behoeften van informaticatoepassingen roept het COC de SPC op om zoveel als mogelijk aansluiting te zoeken bij bestaande applicaties en in voorkomend geval bijkomende behoeften vooral te enten op functionaliteiten binnen reeds bestaande toepassingen. Het verdient de voorkeur om behoeften inzake personeelsbeheer te bekijken in het licht van de mogelijkheden van de toepassing GALOP, eerder dan in een door DGA eigen ontwikkelde tool.

Aanbeveling 6

Het COC beveelt de SPC aan, om de afname van de gerechtelijke triptiek aan te wenden als mogelijkheid voor een verificatie van de kwaliteit van de vatting in de ANG van de persoon die het voorwerp uitmaakt van de afname, en dit op het vlak van de individuele beschrijving, de foto en de vingerafdrukken en in voorkomend geval over te gaan tot de fusie van de entiteit indien blijkt dat deze meerdere malen werd gevat in de ANG.

verzoekt de SPC,

Verzoek 1

Het COC verzoekt de Directie SPC, om met DGA de opportuniteit te bekijken inzake het verlenen van toestemmingen door DGA tot gebruik van camera's binnen dezelfde directie.

Verzoek 2

Het COC verzoekt de SPC, de nodige stappen te ondernemen ten aanzien van de verwerkingsverantwoordelijken, om de noodzakelijke protocolakkoorden af te sluiten conform de bepalingen van de Camerawet van 21 maart 2007.

Verzoek 3

Het COC verzoekt de SPC om het testproject inzake installatie van ANPR camera's aan spoorwegovergangen mee op te volgen.

Verzoek 4

Het COC verzoekt de SPC op stelselmatige en proactieve wijze controles uit te voeren betreffende het gebruik en/of de consultatie van de politionele gegevensbanken, meer bepaald door elke maand of elk kwartaal controles te verrichten op basis van steekproeven met behulp van loggings. Het COC zal aandringen bij de verantwoordelijken GPI om deze controles te faciliteren door het aanleveren van aangepaste tools. Het COC vraagt de resultaten van de controles beschikbaar te houden voor het COC. Specifiek met betrekken tot de problematiek van de gedetacheerden en de verschillende eenheidscodes verzoekt het COC de SPC, de loggings tevens op te vragen op de specifieke terminalnummers die toegekend zijn aan SPC, en na te kijken of de terminals toegekend aan SPC nog steeds overeenstemmen met de realiteit van het terrein.

verzoekt de SPC Brussel en/of de directie SPC een stand van zaken van deze aanbevelingen en verzoeken binnen de 12 maanden na ontvangst van dit rapport;

gelast de volgende corrigerende maatregelen ten aanzien van de SPC Brussel en de directie SPC,

Gelet op artikel 71, 221 § 1 en 247, 4° WGB,

Corrigerende maatregel 1

Gelet op de vaststellingen zoals vermeld in randnummer 40, met name het ontbreken van registraties van beeldverwerkingen in het REGPOL register enerzijds, en het ontbreken van een register voor cameragebruiken anderzijds ;

beveelt de SPC Brussel en de Directie SPC om de verwerkingen aan de hand van het bekijken van de beelden van de vervoersmaatschappijen te vermelden in het register REGPOL en dit binnen de drie maanden na ontvangst van het rapport.

Corrigerende maatregel 2

Gelet op de vaststellingen zoals vermeld in randnummers 45, 46 en 47, met name de afwezigheid van de registraties van het cameragebruik in de cellen van de 4 regio's buiten Brussel, het mogelijk onderscheppen of heimelijk afluisteren van de gesprekken in de cellen van de 4 regio's buiten Brussel, en de onduidelijkheden met betrekking tot de toegangscontroles in alle regio's;

beveelt de directie SPC om de camera- en geluidsverwerkingen in de gebouwen van alle regio's van de SPC in overeenstemming te brengen met het vigerend wettelijk kader op het vlak van verzameling, bewaring, toegang en logging en dit binnen de zes maanden na ontvangst van dit rapport.

Corrigerende maatregel 3

Gelet op de vaststellingen zoals vermeld in randnummer 50, met name dat er geen registraties van verwerkingen werden aangetroffen in het REGPOL register;

Beveelt de directie SPC, om de bepalingen van art 55 WGB correct toe te passen op het vlak van registratie van verwerkingsactiviteiten die onder de verantwoordelijkheid van SPC vallen en zich daartoe te enten op de interne bepalingen van de federale politie, en dit binnen de zes maanden na ontvangst van dit rapport.

Corrigerende maatregel 4

Gelet op de vaststellingen zoals vermeld in randnummer 50 en randnummer 56, met name de vaststelling dat het aan een duidelijk beleid omtrent bijzondere gegevensbanken binnen SPC ontbreekt en dit omwille van het ontbreken van registraties van bijzondere gegevensbanken in het REGPOL register en het onduidelijke overzicht of er al dan niet bijzondere gegevensbanken in gebruik zijn bij SPC;

beveelt de SPC Brussel, om, al dan niet in samenspraak met DGA, een duidelijk beleid op te stellen inzake de bijzondere gegevensbanken en dit ook consequent toe te passen en dit binnen de zes maanden na ontvangst van dit rapport.

Corrigerende maatregel 5

Gelet op de vaststelling zoals vermeld in randnummer 56, met name dat er bijzondere gegevensbank genaamd "*Apollo*" in gebruik is bij de SPC Brussel;

beveelt de SPC Brussel om de GBO "Apollo" correct te registreren als GBO in het register van de verwerkingsactiviteiten en dit binnen de maand na ontvangst van dit rapport

Zegt voor recht dat voor de berekening van de termijnen voor de naleving van de aanbevelen, verzoeken en de corrigerende maatregelen 1 tot en met 5, als datum van het overmaken van het huidig definitief rapport van het Controleorgaan, de datum van overmaken ervan, vermeerderd met twee werkdagen, moet genomen worden.

Het Controleorgaan wijst op de mogelijkheid voor de politiedienst om binnen de 30 dagen na de definitieve beslissing van het Controleorgaan beroep aan te tekenen bij het hof van beroep van de woonplaats of zetel van eiser (artikel 248 § 1, eerste lid, en § 2 WGB).

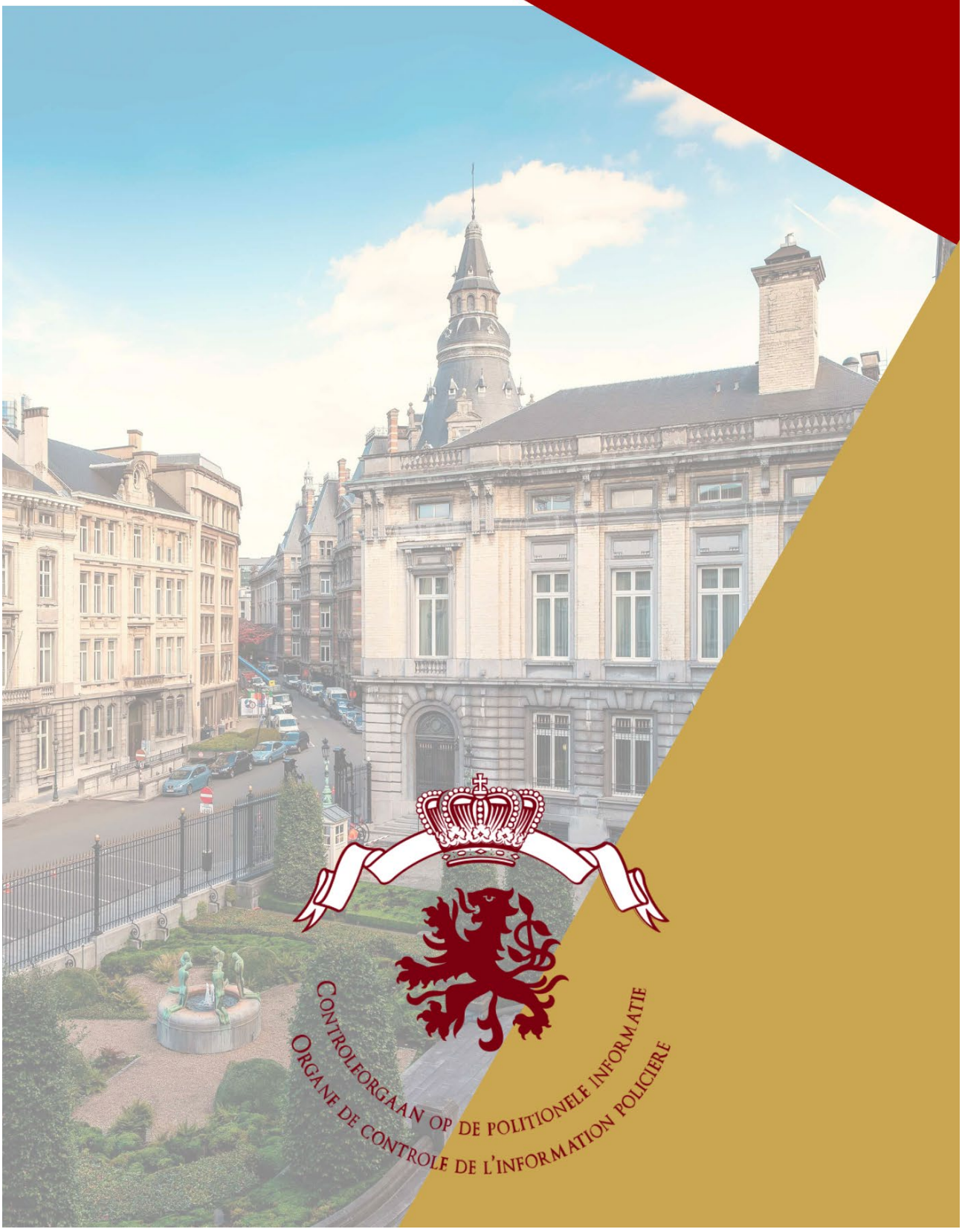
Aldus beslist door het Controleorgaan op de Politionele Informatie op 9 november 2021.

Afschrift aan:

- Procureur-generaal te Brussel
- Procureur des Konings te Brussel
- Directeur-generaal Algemene Directie Bestuurlijke Politie

Voor het Controleorgaan,

Koen Gorissen	Frank Schuermans	Philippe Arnould
Lid-raadsheer	Lid-raadsheer	Voorzitter



CONTROLEORGAAN OP DE POLITIONELE INFORMATIE
ORGANE DE CONTROLE DE L'INFORMATION POLICIERE