BEPERKT TOEZICHT

TOEZICHTRAPPORT EN VISITATIE BIJ EEN POLITIEZONE IN OOST-VLAANDEREN DOOR HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE IN HET RAAM VAN ZIJN CONTROLE- EN TOEZICHTSBEVOEGDHEDEN

Referte: DIO21001

Inhoudsopgave

1 INLEIDING

1. Gelet op zijn bevoegdheden als externe controledienst en bevoegde toezichthoudende autoriteit ten aanzien van de gegevensverwerkingen door de geïntegreerde politie georganiseerd op twee niveaus (GPI) heeft het Controleorgaan op de politionele informatie (Controleorgaan of COC) beslist een visitatie te verrichten bij een politiezone in Oost-Vlaanderen in het raam van een 'Beperkt Toezicht'[1], en dit naar aanleiding van een klacht (COC referentie DKL21002) inzake het opnemen van beelden en geluiden tijdens een vertrouwelijk overleg met een advocaat. Klager stelt dat, na een vertrouwelijk overleg dat hij in het nieuwe politiegebouw van een politiezone in Oost-Vlaanderen had met zijn advocaat, de betrokken politieambtenaren blijkbaar op de hoogte waren van de inhoud van dit gesprek. Er was geen voorafgaande kennisgeving van het feit dat beeld- of geluidsopnames mogelijk waren in het politiegebouw of in de ruimte waar het vertrouwelijk overleg plaatsvond. Inzage in de beelden achteraf werd niet toegestaan. Onderhavig verslag heeft betrekking op de onderzoeksbevindingen van de visitatie.

1.1 De bevoegdheden van het Controleorgaan op de politionele informatie

2. De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WGB)[2] 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.

[1] 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] *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*)).

Het Controleorgaan is bevoegd voor de politiediensten[3], de Algemene inspectie van de federale en lokale politie (AIG)[4] en de Passagiersinformatie-eenheid (PIE)[5]. De toezichtbevoegdheid van het Controleorgaan, wat betreft de politiediensten, omvat zoals gezegd zowel de operationele als niet-operationele verwerkingsactiviteiten[6].

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 overtredingen vaststelt op wetten en reglementen.

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[7]. 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.

Daarnaast neemt het Controleorgaan kennis van klachten en beslist het over de gegrondheid ervan[8]. In dat verband beschikken de leden en de leden van de dienst Onderzoeken (DOSE)[9] van het Controleorgaan over onderzoeksbevoegdheden en kunnen corrigerende maatregelen worden genomen[10].

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[11].

2 OPZET VAN DE VISITATIE

3. Op 11 februari 2021 heeft het Controleorgaan op eigen initiatief een onaangekondigde visitatie[12]uitgevoerd bij de betrokken politiezone met het oog op het controleren van de verwerkingen middels camera's in het nieuwe politiegebouw van de politiezone. De visitatie was het gevolg van bovengenoemde individuele klacht naar aanleiding van mogelijke onregelmatigheden bij het opnemen van beelden en geluiden tijdens een vertrouwelijk overleg met een advocaat.

[3] Zoals gedefinieerd in artikel 2, 2° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (art. 26, 7°, a WGB).
[4] 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 (art. 27, 7°, d WGB).
[5] Zoals bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (art. 26, 7°, f WGB). Ook wel aangeduid als *BELPIU'* (*Belgian Passenger Information Unit*).
[6] Art. 4 § 2 4e lid, wet van 3 december 2018 tot oprichting van de Gegevensbeschermingsautoriteit (WOG).
[7] BAM staat voor '**B**ijzondere **A**dministratieve **M**ethoden'.
[8] Art. 240, 4° WGB.
[9] **D**ienst **O**nderzoeken / **S**ervice d'**E**nquête.
[10] Art. 244 en 247 WGB.
[11] Art. 248 WGB.
[12] Een onaangekondigde visitatie in het raam van een Beperkt Toezicht is een onderzoek gericht naar een specifiek thema meer gericht op specifieke juridische aspecten of aspecten van gegevensbescherming of privacy. Gegeven de COVID crisis en de ermee gepaard gaande gezondheidsmaatregelen werd om opportuniteitsredenen beslist om de visitatie daags voordien kenbaar te maken aan de korpschef, evenwel zonder vermelding van het specifieke thema.

3 JURIDISCH KADER

3.1 Camerabewaking

3.1.1 Rechtsgrond

4. 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[13]. 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[14].

3.1.2 Verwerkingsverantwoordelijke

5. 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*"[15]. 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*"[16]. 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*"[17].

6. Hoewel 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 overeenstemming met het wettelijk kader worden verwerkt. Hij, zijn aangestelde of gemachtigde, is ook de persoon tegenover wie eventuele corrigerende maatregelen kunnen worden opgelegd of strafrechtelijk kan aangesproken worden[18]. De korpschef is de verwerkingsverantwoordelijke voor het bewaren van camerabeelden in een lokale technische gegevensbank[19].

De korpschef is ook de verwerkingsverantwoordelijke voor de bijzondere gegevensbanken[20]. 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[21] en (2) van

[13] 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.
[14] 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).
[15] Art. 4. 7) AVG.
[16] Art. 26, 8° WGB.
[17] Art. 26, 7° WGB.
[18] Zie de artikelen 221 en 222 WGB. Concreet kan het Controleorgaan onder meer de volgende maatregelen nemen (art. 25.2, 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.

[19] Art. 44/11/3*sexies* § 1, 2de lid WPA.
[20] Artikel 44/4 § 1, derde lid WPA.
[21] MERCURE.

klassieke camerabeelden. Het betreft gegevens die in verband staan met opdrachten van bestuurlijke en gerechtelijke politie, maar niet *ipso facto* in de ANG moeten geregistreerd/gevat worden[22]. 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[23]. 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 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 is, handelt de bevoegde politieambtenaar onder de verantwoordelijkheid van de korpschef. De korpschef is immers, op grond van artikel 44 Wet Geïntegreerde Politie, 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[24].

De korpschef is dus de verwerkingsverantwoordelijke voor wat betreft alle vormen van cameragebruik binnen zijn of haar politiezone.

3.1.3 Procedurele vereisten

7. Vooraleer een politiedienst camerabewaking op het grondgebied van een gemeente wenst in te voeren, heeft zij daartoe de principiële toestemming van de gemeenteraad nodig[25]. 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[26]. Het is van belang er op te wijzen dat wanneer de toestemming van de gemeenteraad reeds vóór de wetswijzing van 21 maart 2018 werd verkregen onder de toepassing van de camerawet van 2007 de toestemming niet opnieuw van de gemeenteraad verkregen moet worden[27]. Deze initieel bekomen 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[28]. In dat geval moet er dus een nieuwe, of aanvullende, toestemming van de gemeenteraad verkregen worden.

3.1.4 Bewaartermijn van de beelden

8. De camerabeelden kunnen maximaal 1 jaar worden bewaard[29]. 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 (zie randnummer 3.3.8), aangeeft op welke gegevensdrager de beelden worden opgeslagen. Deze gegevensdrager moet toegankelijk zijn voor het Controleorgaan.

3.1.5 Technische gegevensbanken

[22] Art. 44/11/3 WPA.
[23] 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.
[24] 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
[25] Art. 25/4 § 1, 1° WPA.
[26] Memorie van Toelichting bij deze wet, p. 21 (Parl. St. *Kamer* 2017-2018, nr. 54-2855/001).
[27] 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).
[28] Art. 25/4 § 2, 2de lid WPA.
[29] Art. 25/6, 44/11/3*decies* § 2, eerste lid, en 46/12, eerste lid WPA.

9. Hoewel buiten de context van het voorwerp van de klacht is het 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*"[30]. Wanneer *ANPR* camerabewaking wordt toegepast, moeten de beelden in een "*technische gegevensbank*" worden opgeslagen,[31]waarbij de persoonsgegevens en informatie tevens worden doorgezonden naar de nationale technische gegevensbank[32]. De beelden kunnen maximum een jaar worden bewaard en ook hier is geen minimumtermijn bepaald[33].

De technische gegevensbank bevat, indien ze verschijnen op de beelden, de volgende gegevens[34]:
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[35],, aan de achterkant;
4) een foto van het voertuig;
5) in voorkomend geval[36],, 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.

10. 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[37]. 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;
- 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

11. 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[38]. De toegang moet gemotiveerd en operationeel noodzakelijk zijn voor het uitvoeren van een specifieke opdracht[39]. Dit komt erop neer dat de toegang tot

[30] Art. 25/2 § 1, 3°, *juncto* 44/2 § 3, derde lid WPA.
[31] Art. 44/2 § 3, eerste lid, WPA.
[32] Art. 44/11/3*sexies* WPA.
[33] Art. 44/11/3*decies* § 2, eerste lid WPA.
[34] Art. 44/11/3*decies* § 1 WPA.
[35] « In voorkomend geval » verwijst naar de technische mogelijkheid van de camera zulks al dan niet te doen.
[36] Ibid.
[37] 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.
[38] Art. 25/7 § 1, 1ste en 2de lid en 44/11/3*decies* § 3, tweede lid WPA.
[39] Art. 44/11/3*decies* § 3, 1ste lid WPA.

de beelden alleen toegelaten is voor personen die deze persoonsgegevens en informatie nodig hebben en wanneer daartoe dus een concreet operationeel belang aanwezig is[40].

12. 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 GBW 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[41]. Daarbij kan het systeem van toegang naar analogie van 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

13. Zichtbare camera's zijn camera's waarbij het gebruik ervan wordt aangekondigd door pictogrammen, de camera's gemonteerd zijn in als zodanig herkenbare politievoertuigen, -vaartuigen, -luchtvaartuigen of elk ander vervoermiddel van de politie of gedragen worden door politieambtenaren die als zodanig herkenbaar zijn[42]. 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[43]. 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) en
4) tijdens de overbrenging van aangehouden of opgesloten personen (art. 46/11 WPA).

Behalve wanneer het niet-zichtbaar gebruik van camera's onder het gezag van een magistraat wordt uitgevoerd, moet deze vorm cameragebruik evenwel **voorafgaand** aan het Controleorgaan worden aangeven. Deze voorafgaande mededeling moet het Controleorgaan toelaten om de wettelijkheid van de beslissing te beoordelen[44].

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

14. 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 tegenover het operationele niveau van het cameragebruik[45]. Deze oefening moet ook worden gemaakt vóór het oprichten van een (lokale) technische gegevensbank[46]. Hiervoor wordt de bijstand van de *DPO* gevraagd[47].

Mits 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

[40] Memorie van Toelichting bij deze wet, p. 29 (Parl. St. *Kamer* 2017-2018, nr. 54-2855/001).
[41] Zoals principieel vastgelegd in artikel 14 (recht van inzage) Richtlijn Politie-Justitie.
[42] Art. 25/2 § 2 WPA.
[43] Art. 46/4 e.v. WPA.
[44] Art. 46/6 en 46/10 WPA.
[45] Art. 25/4 § 2 WPA.
[46] Art. 44/11/3*octies* WPA.
[47] Art. 65, 3° *juncto* 58 WGB.

analyse conform de WGB alle relevante systemen en procedures van verwerkingsactiviteiten moet bestrijken. 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 Register

15. Het gebruik van camerabewaking moet in een (lokaal) register worden bijgehouden[48]. 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 aanlegt 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 zelf ook en wel in de eerste plaats) (in)zicht (op) over het gebruik van camerabewaking op het grondgebied van de gemeente dat onder de diens bevoegdheid valt. 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 ook in het register van verwerkingen opgenomen worden[49]. Beide registers zijn of moeten beschikbaar zijn voor het Controleorgaan.

3.1.10 Camerabewaking van de gebouwen en politiekantoren en politiecellen

16. De camerabewaking van de gebouwen en politiekantoren en politiecellen valt onder de WPA[50]. Dat is tevens het geval voor camerabewaking van de inkomhal of het onthaal van het politiecommissariaat. Videobewaking[51]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[52]. Deze videobewaking 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, 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[53]. Het politiegebouw – of de politiepost moet uitgerust zijn met een duidelijke signalisatie van de videobewaking 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 tijdens 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.

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.

3.2 Audiovisuele opname in het raam van een strafrechtelijk onderzoek

[48] Art. 25/8 WPA.
[49] Art. 55 WGB.
[50] 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.
[51] 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
[52] Europees Verdrag voor de Rechten van de Mens
[53] 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

17. Naar verluidt van artikel 112*ter* Wetboek van Strafvordering (Sv) "*kan de procureur des Konings of de onderzoeksrechter de audiovisuele of de auditieve opname van het verhoor bevelen. De te horen persoon wordt op voorhand van dit bevel op de hoogte gebracht*" (§ 1). De audiovisuele of de auditieve opname van het verhoor kan door een politieambtenaar worden uitgevoerd (§ 2) en moet daarbij deze wijze van verhoor in het proces-verbaal opnemen (§ 3). Het betreft hier dus geen vorm van cameratoezicht (met audio) zoals bedoeld en geregeld in de WPA. Bovendien kan de beslissing om een audiovisuele of een auditieve opname op te zetten niet autonoom door de korpschef worden genomen. De te horen persoon (en de advocaat) mag evenmin onwetend zijn van de audiovisuele of de auditieve opname. Een heimelijk audiovisuele opname of het heimelijk gebruik van de audiovisuele beelden zoals bedoeld in artikel 112*ter* Sv is dus onwettig.

3.3 Vertrouwelijk overleg met advocaat

18. Uit de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM)[54]blijkt al één en ander inzake de vertrouwelijkheid van de relatie tussen de cliënt en de advocaat. De vertrouwelijkheid van deze relatie[55]is fundamenteel en wordt beschermd door artikel 6 en 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM)[56]. Deze relatie raakt aldus zowel aan het recht tot privacy in brede zin van de betrokkene (artikel 8) als aan zijn recht op een eerlijk proces (artikel 6).

Een schetsend voorbeeld van een zaak in een politiecommissariaat vinden we terug in de volgende casus R.E. versus Verenigd Koninkrijk[57] waarin eveneens wordt verwezen naar eerdere rechtspraak: *"131. The present case concerns the surveillance of legal consultations taking place in a police station, which the Court considers to be analogous to the interception of a telephone call between a lawyer and client. The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford* ***"strengthened protection"*** *to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential (Michaud v. France, no. 12323/11, § 118, ECHR 2012)."*

Zelfs de loutere aanwezigheid van een camera in een lokaal voor vertrouwelijke gesprekken tussen de advocaat en zijn cliënt kan indruisen tegen artikel 6 en 8 van het EVRM, los van het feit of die daadwerkelijk filmt/opneemt, meer specifiek omdat de vertrouwelijkheid die er tijdens zo een gesprek zou moeten kunnen plaatsvinden, niet wordt gewaarborgd. *A fortiori* indien er effectief wordt gefilmd en geluid wordt opgenomen/of de audio kan worden gehoord. Enkel indien de advocaat erom verzoekt, in het raam van zijn of haar veiligheid, is het gebruik van video en dus **niet** van audio, gerechtvaardigd.

4 ONDERZOEKSBEVINDINGEN

4.1 Cameragebruik door de politiezone in het algemeen

4.1.1 Gebruik pictogram art. 25/2 §2 WPA en het KB van 22 mei 2019

19. Het gebruik van vaste camera's binnen de politiezone is op diverse plaatsen van het grondgebied aanwezig.

Binnen het gebouw van de politiezone stellen we vast dat het pictogram duidelijk zichtbaar is aan de toegang van het cellencomplex. Aan de ingang voor bezoekers is er geen duidelijk zichtbaar pictogram aanwezig. De politiezone laat evenwel weten dat de pictogrammen besteld zijn en dat het een kwestie van tijd is om deze aan te brengen.

[54] Europees Hof voor de Rechten van de Mens
[55] We verwijzen onder meer naar EHRM 10 september 2013, Helander versus Finland, nr. 10410/10, en naar EHRM 21 februari 1975, Golder versus Verenigd Koninkrijk, nr. 4451/70.
[56] Europees Verdrag voor de Rechten van de Mens
[57] EHRM R.E. vs. Verenigd Koningrijk van 27 oktober 2015, nr. 62498/11.

4.1.2 Gemeenteraadsbesluiten inzake cameragebruik (voorafgaande principiële toestemming 25/4 WPA)

20. De politiezone wijst erop dat de toestemming voor de plaatsing van bewakingscamera's voor het grondgebied van de zone reeds dateert van 2010, dus van lang vóór 21 maart 2018 en houdt in voorkomend geval de besluiten beschikbaar voor inzage door het COC. Zoals supra reeds gesteld voor het cameragebruik binnen het gebouw van de politiezone geen voorafgaandelijke toestemming van de gemeenteraad vereist.

4.1.3 Impact- en risico analyse inzake cameragebruik (25/4 WPA)

21. De politiezone wijst erop dat de toestemming voor de plaatsing van bewakingscamera's dateert van rond 2010, dus van lang vóór 21 maart 2018. Er is dus geen impact- en risico analyse voorhanden voor het gebruik van camera's. Inzake het gebruik van de camera's binnen het politiegebouw stelt zich evenwel de vraag naar de toepassing van de artikelen 55 t.e.m. 62 WGB, inzonderheid artikel 58, met betrekking tot het opstellen van een beoordeling van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Vooruitlopend op de conclusies van dit rapport ontbreekt het de politiezone manifest aan een algemene beschrijving van de beoogde cameraverwerkingen, een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen, met inachtneming van de rechten en legitieme belangen van de betrokkenen en de andere belanghebbenden.

4.1.4 Gebruik en naleving van de proportionaliteits- en subsidiariteitsbeginselen (art 25/5 WPA)

22. Een duidelijke interne regelgeving omtrent het gebruik van de camera's in het politiegebouw is er niet. Eveneens is er verwarring binnen de politiezone omtrent het gebruik. Het korps beschikt wel over zogenaamde 'leefregels' waarin dergelijke richtlijnen kunnen worden opgenomen. Het behoort, aldus het korps, tot de intenties om een intern beleid hieromtrent uit te werken.

Voor alle duidelijkheid en volledigheid wil het COC wel opmerken dat de camera's in de cellen zijn opgesteld op een wijze die de privacy respecteert in de zin van het artikel 10 van het KB van 14 september 2007.

4.1.5 Opname en opslagtermijn van de beelden (art 25/6 WPA)

23. De camera's die aanwezig zijn in het gebouw filmen permanent. De opslag van de beelden gebeurt automatisch, met uitzondering van de beelden van de verhoorlokalen. **In de verhoorlokalen gebeurt de opslag door middel van een knop maar wordt er dus sowieso gefilmd. Bij het activeren van de knop tot opslag wordt evenwel zowel de opslag van video als van audio geactiveerd. Deze praktijk en deze verwerking (in de verhoorlokalen) is en zijn onwettig**.

Een loutere mededeling aan de verhoorde uit hoofde van transparantie is niet afdoende, noch kan de toestemming van de verhoorde persoon als rechtsgrondslag dienen[58]. Zoals hiervoor gesteld, wordt het audiovisueel verhoor strikt geregeld in hoofdstuk VII*quater* (in het bijzonder art. 112*ter* Sv.), naast de bepalingen inzake het audiovisueel verhoor voor minderjarigen, dat geregeld wordt in de artikelen 92 tot en met 103 Sv. Een audiovisueel verhoor kan slechts plaatsvinden indien bevolen door de procureur des Konings of de onderzoeksrechter, gevolgd door alle in voormelde artikelen voorziene modaliteiten en pleegvormen. **Het komt de politie dus <u>niet</u> toe om dit ambtshalve te doen. Daarmee bedoelen we noch het filmen op zich (zonder opslag) van een verhoor (behoudens om redenen van veiligheid en dus in het kader van de bestuurlijke politiefunctie), laat staan het opnemen, ergo het filmen (en opnemen) van een vertrouwelijk overleg in dergelijk verhoorlokaal.**

[58] De toestemming kan nooit een valabele rechtsgrond zijn voor een operationeel politionele verwerking; er moet steeds een uitdrukkelijke wettelijke (of eventueel reglementaire) basis zijn (cf. art. 33 §1, 1° en 2° WGB)

Er is een aparte infrastructuur aanwezig in de politiezone die het afnemen van een audiovisueel verhoor conform de genoemde bepalingen mogelijk maakt. Zelfs de loutere aanwezigheid van de mogelijkheid tot audio opname van de verhoren in de verhoorlokalen van de politiezone lijkt in de feiten overigens wel wat *overkill*. Het COC kan zich moeilijk inbeelden dat alle verhoorlokalen tegelijk worden gebruikt (of in het verleden werden gebruikt) om een audiovisueel verhoor in de zin van het Sv. te verrichten. Maar goed, theoretisch bestaat de mogelijkheid.

Tijdens de visitatie stelt het COC bovendien vast dat de configuratie van de audiomodule in verhoorlokaal 4 niet correct is, daar de aanwezige OGP permanent kan horen wat er in dit lokaal gezegd wordt, dus ook zonder de activatie van de opnameknop. Het verhoorlokaal 4 blijkt ook nog het verhoorlokaal te zijn waar een vertrouwelijk overleg tussen advocaat en cliënt kan plaatsvinden en doorgaans ook plaatsvindt. Hoewel de infrastructuur op zich niet onwettig is, wordt deze in alle geval niet correct gebruikt, en lijkt ook de technische kennis om dit gebruik correct te configureren in onvoldoende mate aanwezig. **Hoe dan ook is het auditief (kunnen) beluisteren van een vertrouwelijk overleg tussen advocaat en cliënt, laat staan de opname (en opslag) ervan, volstrekt onaanvaardbaar. Meer zelfs, het beluisteren op zich is een strafrechtelijke inbreuk op de artikelen 151 en 259*bis* Sw. en op artikel 222, 1°, 2° WGB.**

De keuze voor een bepaald verhoorlokaal als ruimte voor het vertrouwelijk overleg lijkt ingegeven te zijn door de specifieke locatie binnen het gebouw. Het is het enige verhoorlokaal waar middels een glazen wand die geluid doorlaat, de mogelijkheid bestaat om te praten met een persoon die zich aan de andere zijde bevindt. Deze andere zijde omvat een lokaal dat enkel bereikbaar is via het cellencomplex.

Omtrent de termijn van opslag van de beelden kan de politiezone geen uitsluitsel geven.

4.1.6 Toegang, reden raadpleging en logbestanden (art 25/7 WPA)

24. In de politiezone wordt momenteel gewerkt met een generieke toegang tot de beelden van het politiegebouw. Het is niet duidelijk of er voor deze toegang een reden dient te worden opgegeven of niet. Met de generieke login kan de generieke gebruiker retro bevragingen doen. Het is niet duidelijk of daarbij het onderscheid kan gemaakt worden tussen de eerste opslagperiode van een maand, en de bevraging na de eerste maand met inbegrip van de schriftelijke en met redenen omklede beslissing van de procureur des Konings.

Op minstens twee plaatsen is via een beeldscherm een real time toegang tot de camerabeelden mogelijk, met name in het lokaal van de OGP van wacht alsmede in het lokaal van het onthaal. Het gaat hier wel degelijk om een toegang tot alle in het gebouw aanwezige camera's. Er wordt geen onderscheid gemaakt tussen de beelden, dus ook vanuit het lokaal van het onthaal is er een zicht op wat zich afspeelt in de **cellen én de verhoorlokalen**. Het beeldscherm in het lokaal van het onthaal is opgehangen op een wijze die toelaat om via het raam, vanaf de publieksparking, het scherm te bekijken. **Ook dit is een niet aanvaardbare, manifest onwettige praktijk.**

De politiezone kon niet antwoorden op de vraag of er een zicht is op de aanwezigheid van logbestanden van de toegangen tot de camerabeelden. Hoe dan ook, de generieke login laat niet toe om een koppeling te maken met een specifieke gebruiker zodat eventuele logbestanden niet echt dienstig kunnen zijn waarvoor ze dienen, met name een eventuele controle van de toegangen tot beelden.

4.1.7 Registers (art 25/8 WPA)

25. Het cameragebruik is niet vermeld in het register van de categorieën van verwerkingsactiviteiten REGPOL[59]. Het COC stelt wel vast bij nazicht van dit register dat de politiezone over een Lokale Technische Gegevensbank (LTGB) beschikt, doch dat hiervoor een impact -en risico analyse ontbreekt.

De politiezone beschikt niet over een register inzake het gebruik van camera's binnen de zone zoals verplichtend gesteld door art. 25/8 WPA.

[59] 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.

Het COC stelt vast dat er vattingen zijn gebeurd in het nationale register voor Geolocalisatie "*Camelia*", doch stelt eveneens vast dat het cameragebruik binnen het politiegebouw niet werd aangeduid in dit register.

4.1.8 Recht van toegang tot de beelden (art 42 WGB en art 12 camerawet)

26. De politiezone is niet op de hoogte van het standpunt van het COC inzake het recht op toegang van de gefilmde persoon tot de beelden indien het niet gaat om beelden die een operationele behoefte hebben, waarbij de politiezone in dergelijk geval dit recht op toegang zelf kan organiseren.

4.2 Cameragebruik tijdens het vertrouwelijk overleg met een advocaat

27. Het COC kon tijdens de visitatie duidelijk vaststellen dat de politiezone over de mogelijkheid beschikt om in de verhoorlokalen 1 tot en met 4 naast video-opnames ook geluidsopnames te maken middels het indrukken van een opnameknop. Daarbij werd tevens vastgesteld dat door een configuratieprobleem in verhoorlokaal 4, zijnde het lokaal waar doorgaans (maar niet uitsluitend) het vertrouwelijk overleg tussen de advocaat en zijn cliënt plaatsvindt, het doorgeven van dit geluid naar het lokaal van de OGP permanent was en de gesprekken aldus **altijd** hoorbaar (afluisterbaar) waren. Zoals hoger vermeld vormt deze praktijk een inbreuk op de artikelen 151 en 259*bis* Sw, met name inzake het onderscheppen, kennisnemen en opnemen van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem of inzake het geheim van niet voor het publiek toegankelijke communicatie en gegevens van een informaticasysteem en is het tevens een onrechtmatige gegevensverwerking, wat evenzeer correctioneel bestraft wordt (art. 222, 1° en 2° WGB).

Het COC gaat ervan uit dat bovenvermelde onwettige praktijk niet 'wetens willens' is gebeurd. Dit belet niet dat er onafgebroken strafbare feiten gebeuren waar met onmiddellijke ingang een einde dient aan te worden gesteld. Alleszins is er sprake van ernstige nalatigheid, zowel uit hoofde van de opdrachtgever als van de opdrachtnemer, daar in de aanloop van de constructie van het politiegebouw meerdere andere locaties werden bezocht en de resultaten daarvan zichtbaar zijn in de gemaakte architectuurkeuzes. Het cameragebruik binnen het gebouw behoorde duidelijk tot het lastenboek. Of de DPO werd geconsulteerd, dan wel of de hoofd- of onderaannemer beschikken over een kennis inzake "*privacy by design*" is niet duidelijk.

Hoe dan ook is dit alles ondergeschikt aan de eigen verantwoordelijkheid van de korpschef als verwerkingsverantwoordelijke van het hele cameragebruik binnen de politiezone.

5 CONCLUSIES, VERZOEKEN EN CORRIGERENDE MAATREGELEN

28. Uit de klacht bleek dat de klager en de advocaat duidelijk merkten aan opmerkingen/reacties van de aanwezige politieambtenaren dat dezen het vertrouwelijk gesprek tussen klager en advocaat hadden gehoord.

29. Uit de vaststellingen van het COC tijdens de visitatie van 11 februari 2021 blijkt dat de klacht gegrond was. Tevens blijken diverse non-conformiteiten op het vlak van de vigerende regelgeving. Deze non-conformiteiten lijken, met veel goede wil in hoofde van het COC, eerder voort te vloeien uit onwetendheid dan wel een doelbewuste politiek. Maar deze veronderstelde onwetendheid is in hoofde van een politiedienst niet aanvaardbaar. Alleszins kan niet anders dan een verregaande en grove nalatigheid worden vastgesteld. Van een professionele organisatie en zijn leidinggevenden mag en moet verwacht worden dat zij ervan op de hoogte zijn dat het auditief horen (laat staan opnemen) van een vertrouwelijk gesprek tussen advocaat en cliënt niet door de beugel kan.

De kennis inzake het gebruik van deze systemen is *in globo* ondermaats binnen de politiezone en alleszins in onvoldoende mate en verspreid aanwezig, wat een ernstig gevaar oplevert voor de verantwoordelijkheid, de veiligheid en de persoonlijke levenssfeer van alle betrokken personen.

OM DEZE REDENEN,

Het Controleorgaan;

verzoekt de politiezone,

1. Verzoek

om voor het vertrouwelijk overleg tussen een advocaat en een cliënt een lokaal te gebruiken dat de vertrouwelijkheid van dit overleg waarborgt, doch de veiligheid van de advocaat kan verzekeren indien laatstgenoemde hierom zou verzoeken of zich daartegen minstens niet verzet. Dit betekent in concreto dat **enkel** een visueel (met of zonder camera) zicht op dat vertrouwelijk overleg toelaatbaar is na toestemming van de advocaat of op diens verzoek;

2. Verzoek

om een beoordeling te maken inzake het cameragebruik binnen het politiegebouw op het vlak van de beoogde verwerkingen, de risico's voor de rechten en vrijheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen, met inachtneming van de rechten en legitieme belangen van de betrokkenen en de andere belanghebbenden, en dit binnen de zes maanden na ontvangst van dit rapport;

3. Verzoek

om duidelijke richtlijnen uit te vaardigen inzake het cameragebruik binnen de politiezone in het algemeen, en binnen het politiegebouw in het bijzonder. Deze richtlijnen moeten minstens rekening houden met de profielen, het invullen van de reden raadpleging, de opslagtermijnen en de logbestanden, en dit binnen de zes maanden na ontvangst van dit rapport;

4. Verzoek

om de voorziene registers inzake verwerkingen, cameragebruik en geolokalisatie duidelijk op te maken of te vervolledigen, en dit binnen de drie maanden na ontvangst van dit rapport;

5. Verzoek

om te voorzien in een recht op toegang voor de gefilmde persoon indien het gaat om beelden die geen operationele behoefte hebben.

* * * * * * * * *

Gelet op artikel 221 § 1 en 247, 4°, 5° en 6° WGB,

Gelast de volgende corrigerende maatregelen ten aanzien van de politiezone,

a. Corrigerende maatregel

met onmiddellijke ingang een einde te stellen aan het maken van audio opname - en opslag in de verhoorlokalen buiten de omstandigheden voorzien in het Wetboek van Strafvordering en daarvan aan het Controleorgaan bevestiging te geven; zegt voor recht dat onder "*onmiddellijke ingang*" moet begrepen worden, de datum van het overmaken van het huidig rapport (per e-mail) door het Controleorgaan vermeerderd met twee werkdagen (zaterdag en zondag niet inbegrepen);

b. Corrigerende maatregel

de nodige technische en organisatorische maatregelen te nemen om de toegang tot de beelden in het onthaal lokaal te regelen conform de vigerende regelgeving (cf. randnummer 24), en dit binnen de drie maanden na ontvangst van dit rapport;

c. Corrigerende maatregel

ingevolge de artikelen 44/11/3*octies* WPA en art 59 WGB, de politiezone een ontwerp van oprichting van een lokale technische gegevensbank op te maken met vermelding van de doeleinden en de verwerkingsmodaliteiten, met inbegrip van een impact- en risicoanalyse op het vlak van de bescherming van de persoonlijke levenssfeer en op operationeel niveau, met name wat de categorieën van verwerkte persoonsgegevens betreft, de proportionaliteit van de aangewende middelen, de te bereiken operationele doelstellingen en de bewaartermijn van de gegevens die nodig is om deze doelstellingen te bereiken.

Gelet op de werklast die dergelijke inspanning vergt wordt een eerste stand van zaken verwacht binnen een termijn van zes maanden na ontvangst van dit rapport;

d. Corrigerende maatregel

de nodige pictogrammen aan te brengen aan de hoofdingang van het politiegebouw en dit binnen de maand na ontvangst van dit rapport;

* * * * * * * * *

Zegt voor recht dat de aanvangsdata, voor de bepaling van de termijnen bedoeld in de hogervermelde verzoeken 1 tot en met 5 en de corrigerende maatregelen b, c en d, moet begrepen worden als zijnde de datum van het overmaken van het huidig rapport (per e-mail) door het Controleorgaan vermeerderd met twee werkdagen (zaterdag en zondag niet inbegrepen).

Aldus beslist door het Controleorgaan op de Politionele Informatie op 26 maart 2021.

Voor het Controleorgaan,

Philippe Arnould (GET)
Voorzitter

Kopie:

- De voorzitter van het politiecollege
- De procureur des Konings te Oost-Vlaanderen

Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière