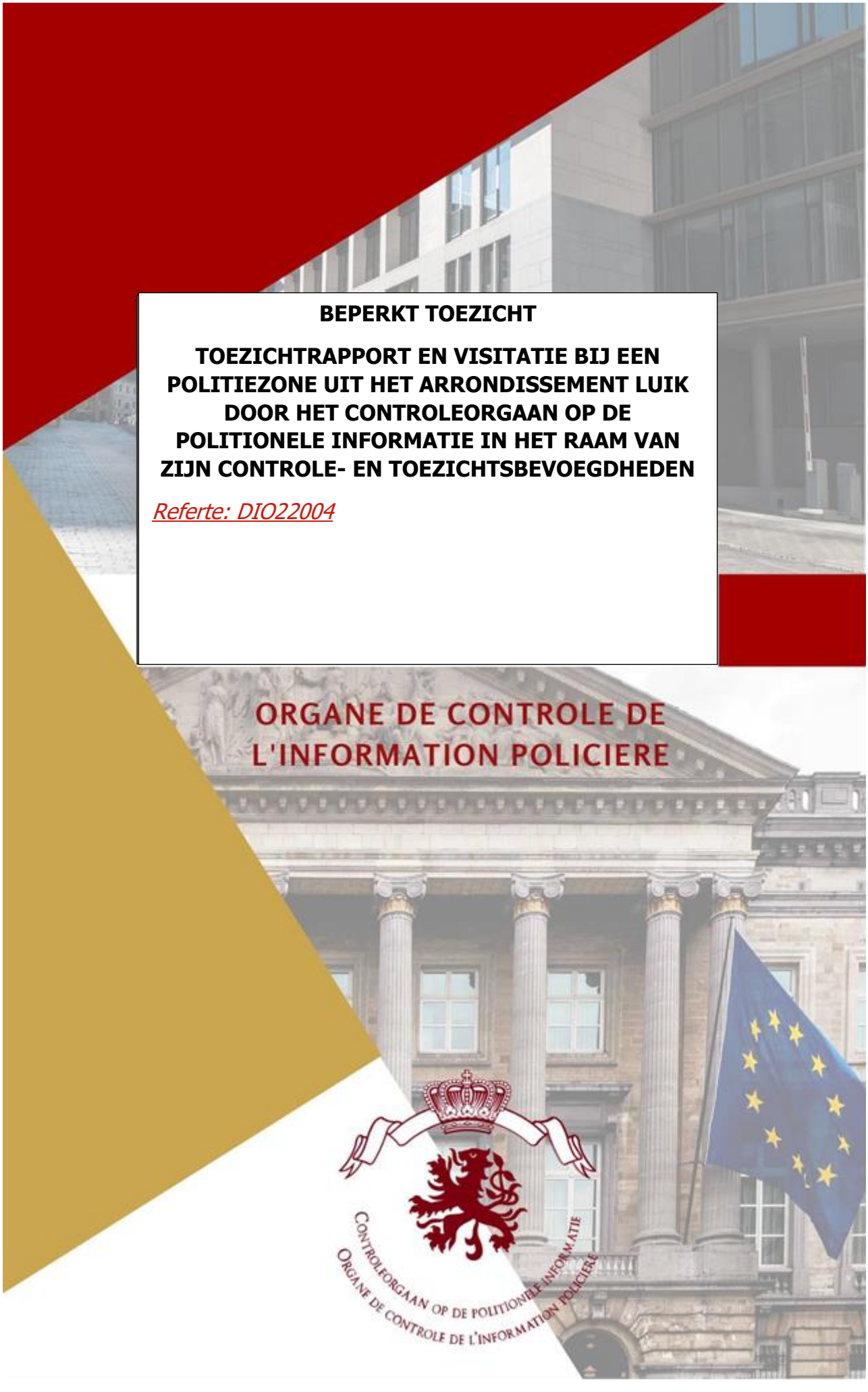


BEPERKT TOEZICHT

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

Referte: DIO22004

Inhoudsopgave

1 INLEIDING

1. Op verzoek van de ministers van Justitie en Binnenlandse Zaken heeft het Controleorgaan op de politionele informatie (hierna 'COC' genoemd) een thematisch onderzoek[1] (steekproef) gevoerd naar de toepassing van een deel van de 'Salduz-regeling' binnen de geïntegreerde politie. Het onderzoek heeft meer bepaald betrekking op het gebruik van bewakingscamera's en/of een systeem voor geluidsopnames tijdens of na afloop van het vertrouwelijk overleg tussen een cliënt (verdachte / beschuldigde persoon) en zijn advocaat.

In haar antwoorden op de algemene vragenlijst die het voorwerp is van dit thematisch toezicht, verklaart de politiezone Arrondissement Luik (PZ Arrondissement Luik): "*In onze verhoorlokalen worden continu beelden en geluiden opgenomen, maar de inhoud van deze opnames is enkel toegankelijk voor de interne controledienst*. *De politieambtenaar die het verhoor afneemt, neemt dus geen enkele beslissing*."
Bovendien antwoordde de PZ Arrondissement Luik '*ja*' op vraag 4 van de vragenlijst, die luidde:
"Wordt dit lokaal waarin het vertrouwelijk overleg plaatsvindt gewoonlijk als verhoorlokaal gebruikt?"

Uit de informatie die werd verkregen[2] bij de politiezone Arrondissement Luik blijkt wat volgt:
- Er bestaat geen richtlijn betreffende deze opnames. Er werd enkel aangifte gedaan van het videobewakingsysteem in het register van gegevensbanken (RegPol);
- De advocaat werd/wordt niet stelselmatig op de hoogte gebracht van de opnames.

Rekening gehouden met zijn bevoegdheden als externe controledienst en toezichtautoriteit die bevoegd is inzake gegevensverwerking door de geïntegreerde politie, gestructureerd op twee niveaus (GPI), en in weerwil van het feit dat het thematisch toezicht *a priori* geen betrekking had op individuele politie-entiteiten, heeft het Controleorgaan op de politionele informatie (Controleorgaan of COC) beslist om over te gaan tot een plaatsbezoek bij de politiezone Arrondissement Luik in het raam van een beperkt toezicht.

1.1 Bevoegdheden van het Controleorgaan op de politionele informatie

2. In het kader van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WGB)[3] werd het COC hervormd en is het een volwaardige toezichthoudende autoriteit geworden, naast de al bestaande controlerende bevoegdheden inzake operationele informatieverwerking zoals bedoeld in de wet van 5 augustus 1992 op het politieambt (WPA). In artikel 71 § 1 en de titels 2 en 7 van de 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 van de WPA inzake de informatieverwerking door de politiediensten. Op die manier heeft het Controleorgaan een toezichthoudende en een controlerende opdracht. Dit

[1] Het COC maakt een onderscheid tussen meerdere vormen van toezicht of supervisie:
- **Globaal toezicht**: dit is een controleonderzoek dat gepaard gaat met een of meerdere doorgedreven plaatsbezoeken 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 of die passen in het kader van zijn internationale verplichtingen.

- **Bijzonder toezicht**: dit betreft onderzoeken en controles in bijzondere materies, zoals de jaarlijkse controles op de gemeenschappelijke gegevensbanken terrorisme en extremisme.

2 Mailverkeer tussen het COC en de PZ Arrondissement Luik van 24-01-2022, 09-02-2022 en 15-02-2022.

[3] B.S. 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 WGB, 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.

betekent dat, naast de bescherming van de persoonlijke levenssfeer en gegevensbescherming, het COC ook aandacht heeft voor elementen als efficiëntie en effectiviteit van de informatieverwerking 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 COC is inzonderheid bevoegd voor de politiediensten[4], voor de Algemene Inspectie van de federale en de lokale politie (AIG)[5] en voor de Passagiersinformatie-eenheid (PIU)[6]. De bevoegdheid van het COC ten aanzien van de politiediensten heeft betrekking op zowel de operationele (Titel 2 WGB) als de niet-operationele activiteiten (AVG)[7].
Wat betreft de controleopdracht is het COC belast met het toezicht op de verwerking van de informatie en gegevens zoals bedoeld in artikel 44/1 WPA, met inbegrip van die welke worden ingevoerd in de gegevensbanken zoals bedoeld in artikel 44/2 van dezelfde wet. Het COC is ook belast met alle andere opdrachten waarmee het door of krachtens andere wetten wordt belast.

In dit raam verricht het COC vaststellingen en kan het gebruik maken van verzoeken, aanbevelingen, waarschuwingen en/of corrigerende maatregelen (dwingende bevelen) als '*ultimum remedium*' en/of wanneer het COC inbreuken op de wet- en regelgeving vaststelt.

Het COC is ook belast met de controle op de inachtneming van de regels betreffende de toegang tot de Algemene Nationale Gegevensbank (ANG) en de directe raadpleging ervan, alsook met de inachtneming van de verplichting, bedoeld in artikel 44/7, paragraaf 3 WPA, voor alle leden van de politiediensten om deze gegevensbank van input te voorzien.

Het COC verifieert ook de goede werking van de ANG en de procedure voor verwerking van de gegevens en informatie die ze bevat om te bepalen of die verwerking beantwoordt aan de bepalingen van de artikelen 44/1 tot 44/11/13 WPA en de toepassingsmaatregelen daarvan.

In verband met het gebruik van onzichtbare camera's handelt het COC als een soort 'BAM'-commissie[8]. Volgens artikel 46/6 WPA moeten elke toestemming en elke wijziging van het niet-zichtbaar gebruik van camera's in de gevallen bedoeld in artikel 46/4 worden meegedeeld aan het COC, behalve wanneer het gebruik van camera's wordt uitgevoerd onder het gezag van een magistraat. In dit raam onderzoekt het COC of er is voldaan aan de voorwaarden voor de beslissing tot uitvoering of verlenging van de maatregel.

Bovendien behandelt het COC de klachten betreffende de toepassing van de wetgeving die betrekking heeft op de verwerking van persoonsgegevens door de politiediensten[9]. Daartoe beschikken de leden van het COC en de leden van de dienst Onderzoeken (DOSE)[10] over onderzoeksbevoegdheden en kunnen er corrigerende maatregelen worden getroffen[11].

Tegen sommige beslissingen van het COC kan er binnen een termijn van 30 dagen beroep worden ingesteld voor het hof van beroep van de plaats waar de klager zijn verblijfplaats of maatschappelijke zetel heeft; dit hof behandelt de zaak als een tussenprocedure overeenkomstig de artikelen 1038, 1040 en 1041 van het Gerechtelijk Wetboek[12].

2 OPZET EN METHODOLOGIE VAN HET BEPERKT TOEZICHT

[4] Zoals bepaald in artikel 2, 2° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus (artikel 26, 7°, a) WGB).
[5] Zoals bepaald in artikel 2 van de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten (artikel 26, 7°, d) WGB).
[6] Overeenkomstig hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (art. 26, 7°, f) WGB).
[7] Art. 4 § 2, lid vier, van de wet van 3 december 2017 houdende oprichting van de Gegevensbeschermingsautoriteit.
[8] **B**ijzondere **M**ethoden inzake **B**estuurlijke politie.
[9] Art. 240, 4° en 247 WGB.
[10] **D**ienst **O**nderzoeken / **S**ervice d'**E**nquête.
[11] Art. 244 en 247 WGB.
[12] Art. 248 WGB.

2.1 Algemene context

3. Op 18-05-2021 hebben de ministers van Justitie en Binnenlandse Zaken aan het COC gevraagd een thematisch onderzoek te voeren naar de toepassing van een deel van de Salduz-regeling binnen de geïntegreerde politie. Dit onderzoek had meer bepaald betrekking op het gebruik van bewakingscamera's en/of een systeem voor geluidsopnames tijdens of na afloop van het vertrouwelijk overleg tussen de cliënt (verdachte / beschuldigde persoon) en zijn advocaat.

De methodologie van het onderzoek bestond in het toesturen van een algemene vragenlijst naar de GPI (1) en in het afleggen van plaatsbezoeken (2).

Op 21-06-2021 werd de vragenlijst verzonden naar de 235 entiteiten van de GPI. Op 12-08-2021 werd een herinnering verstuurd naar 50 entiteiten die nog niet hadden geantwoord. De politiezone Arrondissement Luik heeft geantwoord op 19-08-2021, en verklaarde: "*In onze verhoorlokalen worden continu beelden en geluiden opgenomen, maar de inhoud van deze opnames is enkel toegankelijk voor de interne controledienst. De politieambtenaar die het verhoor afneemt, neemt dus geen enkele beslissing.*"

2.2 Bijzondere context en methodologie

4. Op 24-01-2022, na uitvoering van de analysetaken en van meerdere plaatsbezoeken in het globale kader van het toezicht zoals gevraagd door de ministers van Binnenlandse Zaken en Justitie, is het COC overgegaan tot de verwerking van het antwoord van de politiezone Arrondissement Luik met als doel nadere informatie te verkrijgen.

Nog op 24-01-2021 werd een vraag gesteld aan de politiezone Arrondissement Luik. Rekening gehouden met de bijzondere situatie en de gevolgen van de overstromingen in juli 2021 waarmee de politiezone Arrondissement Luik werd geconfronteerd, kon het COC aanvaarden dat een reactie enige tijd op zich liet wachten. Daar het op 09-02-2022 nog geen antwoord had gekregen, heeft het COC contact opgenomen met de politiezone Arrondissement Luik om te polsen naar de stand van zaken. Op 15-02-2022 antwoordde de politiezone Arrondissement Luik wat volgt:

- "*Er zijn geen richtlijnen met betrekking tot deze opnames. Er werd enkel aangifte gedaan van het systeem van videobewaking in het register van de gegevensbanken (RegPol);*
- *de advocaat werd niet stelselmatig op de hoogte gebracht van de opnames.*"

Op 16-02-2022 bevestigde het COC de ontvangst van de antwoorden van de politiezone Arrondissement Luik.

Op 28-02-2022 besliste het COC om over te gaan tot een plaatsbezoek bij de politiezone Arrondissement Luik in het kader van een beperkt toezicht.

Op 02-03-2022 stuurde het COC, per e-mail, een brief ter aankondiging van een kort plaatsbezoek op 09-03-2022 om 10.30 uur in het kader van het gebruik door de politie van camera's in het politiegebouw. Er werd gevraagd dat een gemachtigde persoon alsook een deskundige ter zake daarbij aanwezig zouden zijn.

Op 02-03-2022 bevestigde de politiezone Arrondissement Luik de ontvangst van de e-mail en van de brief waarin het plaatsbezoek werd aangekondigd.

Op 09-03-2022 heeft het COC het bezoek afgelegd tussen 10.30 en 12.00 uur. Het bezoek omvatte drie delen:

1. een inleiding van het algemeen kader;
2. een kort plaatsbezoek in het kader van de doelstellingen;
3. een interview betreffende het gebruik van de camera's voor politionele doeleinden in het politiegebouw;
4. de selectie van een steekproef, in aanwezigheid van het COC, van verwerkte beelden afkomstig van de in het politiegebouw gebruikte camera's.

3 RECHTSGROND

3.1 Camerabewaking

3.1.1 Rechtsgrond

5. Sinds de wet tot aanpassing van de WPA van 21 maart 2018 mag de beslissing om camera's in openbare ruimten te plaatsen alleen nog maar worden genomen door een overheid, zoals de gemeente[13]. Wanneer de politie gebruik maakt van cameratoezicht, zijn de bepalingen van de WPA van toepassing, tenzij het gebruik van camera's wordt beheerst door andere wetgeving[14].

3.1.2 Verwerkingsverantwoordelijke

6. In het recht betreffende de gegevensbescherming is een belangrijke rol weggelegd voor de '*verwerkingsverantwoordelijke*'. Het gaat om de "*natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*"[15]. Wat betreft de verwerkingsactiviteiten in het raam van de opdrachten van bestuurlijke en gerechtelijke politie wordt de verwerkingsverantwoordelijke in de WGB gedefinieerd als "*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]. Met '*bevoegde overheid*' wordt bedoeld: "*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].

7. Hoewel de verwerkingsverantwoordelijke in de WPA in bepaalde opzichten een (specifieke) rol krijgt toebedeeld, is dit niet het geval wat betreft het gebruik van camera's. Zoals hierboven gezegd, is de verwerkingsverantwoordelijke een belangrijke speler op het vlak van de verwerking van persoonsgegevens. Hij moet immers het bewijs leveren van het feit dat de persoonsgegevens worden verwerkt in overeenstemming met het wettelijk kader. Hijzelf, zijn aangestelde of lasthebber is ook de persoon aan wie eventuele corrigerende maatregelen kunnen worden opgelegd of die strafrechtelijk kan worden vervolgd[18]. De korpschef is de verwerkingsverantwoordelijke voor de registratie van camerabeelden in een lokale technische gegevensbank[19].

De korpschef is ook de verwerkingsverantwoordelijke voor de bijzondere gegevensbanken[20]. In de bijzondere gegevensbanken worden gegevens geregistreerd die niet in aanmerking komen voor registratie in de ANG, ook al bezitten ze een operationele noodzaak. Voorbeelden van een bijzondere gegevensbank zijn (1) de registratie van telefoonnummers of ANPR-gegevens die worden verzameld in het kader van een strafrechtelijk onderzoek[21] en (2) klassieke camerabeelden. Het zijn gegevens in verband met opdrachten van bestuurlijke en gerechtelijke politie, die echter niet *ipso facto* moeten worden geregistreerd/samengevat in de ANG[22]. Met betrekking tot deze laatste verwijzen we naar artikel 25/6 van de WPA dat enkel bepaalt dat informatie en persoonsgegevens gedurende maximaal 12

[13] Wet van 21 maart 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, B.S. 16 april 2018.
[14] Zoals de trajectcontrole, die valt onder de toepassing van de wet van 16 maart 1968 betreffende de politie over het wegverkeer (Parl. St., Kamer 2017-2018, nr. 54-2855/001, 9).
[15] Art. 4. 7) van de AVG.
[16] Art. 26, 8° van de WGB.
[17] Art. 26, 7° van de WGB.
[18] Zie de artikelen 221 en 222 van de WGB. Concreet kan het Controleorgaan inzonderheid de volgende maatregelen nemen (art. 25.2, AVG): - een waarschuwing geven; - een berisping geven; - bevelen om de verwerkingsverrichtingen binnen een welbepaalde termijn in overeenstemming te brengen met het rechtskader; een tijdelijke of definitieve beperking opleggen, met inbegrip van een verbod, aan de verwerking.

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

maanden moeten kunnen worden bewaard[23]. Er wordt echter geen verwerkingsverantwoordelijke aangewezen voor de bewaring van de gegevens.

Het Controleorgaan meent dat het (ook) gaat om een bijzondere gegevensbank, zodat de korpschef moet worden beschouwd als de verwerkingsverantwoordelijke. Artikel 44/4 § 1, 3de lid van de WPA bepaalt immers dat de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs die de doelstellingen en de middelen met betrekking tot deze bijzondere gegevensbanken hebben bepaald, de verwerkingsverantwoordelijken zijn voor de bijzondere gegevensbanken die zij aanleggen. Overigens sluit de aanwijzing van de korpschef als verwerkingsverantwoordelijke aan bij de geest van de bepalingen van de WPA betreffende het aanleggen van plaatselijke gegevensbanken. Volgens artikel 25/5 van de WPA worden camera's gebruikt op beslissing en onder de verantwoordelijkheid van de bevoegde politieambtenaar. Zo deze laatste niet de korpschef is, handelt de bevoegde politieambtenaar onder de verantwoordelijkheid van de korpschef. Krachtens artikel 44 van de wet op de geïntegreerde politie is de korpschef immers verantwoordelijk voor de uitvoering van het plaatselijk politioneel beleid en inzonderheid voor de uitvoering van het veiligheidsplan van de politiezone; hij verzekert ook de leiding, de organisatie en de taakverdeling binnen het lokale politiekorps en is belast met de uitvoering van het beheer over dit korps[24].

De korpschef is dus de verwerkingsverantwoordelijke wat betreft alle vormen van gebruik van camera's in zijn politiezone.

3.1.3 Procedurele vereisten

8. Alvorens een politiedienst mag overgaan tot de plaatsing van bewakingscamera's op het grondgebied van een gemeente, heeft hij daartoe de voorafgaande principiële toestemming van de gemeenteraad nodig[25]. Een toestemming is echter niet vereist voor het gebruik van camera's in gesloten plaatsen waarvan de politie zelf de beheerder is, zoals een politiecommissariaat[26]. Het is belangrijk de aandacht te vestigen op het feit dat, wanneer de toestemming van de gemeenteraad al is verkregen vóór de wijziging van de wet van 21 maart 2018 bij toepassing van de wet op de camera's van 2007, er geen nieuwe toestemming van de gemeenteraad dient te worden verkregen[27]. Deze initieel verkregen toestemming blijft dus geldig. Dezelfde toestemming mag echter niet worden gebruikt voor het gebruik van nieuwe types camera's die zijn ingevoerd door de wet van 21 maart 2018. Aldus legt de WPA specifieke voorwaarden op voor het gebruik van tijdelijke vaste camera's waarover de gemeenteraad zich dient uit te spreken[28]. In dit geval moet er dus een nieuwe, of bijkomende, toestemming van de gemeenteraad worden verkregen.

3.1.4 Bewaringsduur van de beelden

9. De camerabeelden mogen worden bewaard gedurende een termijn van maximaal twaalf maanden[29]. De wet stelt geen minimale termijn vast. Wat betreft de klassieke camerabeelden bepaalt de WPA niet op welke gegevensdrager de beelden moeten worden geregistreerd. Het is bijgevolg aangewezen dat de korpschef in het register betreffende de verwerking van persoonsgegevens, zoals bedoeld in artikel 55 van de WGB (zie nummer 3.3.8), aangeeft op welke gegevensdrager de beelden worden opgeslagen. Deze gegevensdrager moet toegankelijk zijn voor het Controleorgaan.

3.1.5 Toegang tot de beelden

10. De toegang tot de beelden is afhankelijk van het doel en wordt op dezelfde wijze geregeld voor zowel de bewaking met gewone camera's als het gebruik van *ANPR*-camera's. In beide gevallen mogen de beelden gedurende maximaal 12 maanden worden bewaard. Wat betreft de opdrachten van bestuurlijke politie is de toegang beperkt tot de eerste maand die volgt op de registratie van de beelden. Voor de opdrachten van gerechtelijke politie zijn de beelden

[23] Volledigheidshalve merken we op dat de WPA geen vaste bewaringstermijn oplegt voor de gegevens die worden opgeslagen in de bijzondere gegevensbanken (art. 44/11/3, §4 van de WPA). Daar artikel 25/6 van de WPA een maximum van 12 maanden oplegt, is de maximale termijn aldus ook bepaald voor deze bijzondere gegevensbank.
[24] Zie ook en meer in detail, Advies op eigen initiatief van het COC DD200026 van 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° van de WPA.
[26] Memorie van toelichting van deze wet, p. 21 (Parl. St., *Kamer* 2017-2018, nr. 54-2855/001).
[27] Art. 88 van de wet van 21 maart 2018 en Memorie van toelichting van deze wet, p. 113-114 (Parl. St., *Kamer* 2017-2018, nr. 54-2855/001).
[28] Art. 25/4 § 2, lid 2 van de WPA.
[29] Art. 25/6, 44/11/3*decies* § 2, eerste lid, en 46/12, eerste lid van de WPA.

toegankelijk voor de volledige duur van hun bewaring, maar is de tussenkomst van de procureur des Konings noodzakelijk eens de eerste maand is verstreken[30]. De toegang moet worden gemotiveerd op operationeel vlak en is noodzakelijk voor de uitoefening van een welbepaalde opdracht[31]. Met andere woorden, de toegang tot de beelden is enkel toegestaan voor personen die deze persoonsgegevens en informatie nodig hebben en wanneer daartoe dus een concreet operationeel belang aanwezig is[32].

11. Wat betreft het recht op toegang tot de beelden van eender welke gefilmde persoon is het recht op indirecte toegang zoals bedoeld in artikel 42 WGB toepasselijk indien het gaat om beelden die voor operationele doeleinden worden verwerkt. De WPA bevat echter geen regelgeving betreffende de rechten van de politieambtenaar of de burger in het kader van de toegang tot de beelden in de hypothese waarin de beelden en de klank niet voor operationele doeleinden worden gebruikt (i.e., bijvoorbeeld, wanneer ze niet als basis voor de opmaak van een proces-verbaal dienen). Zo de beelden niet relevant zijn voor de opdrachten van bestuurlijke of gerechtelijke politie en bijgevolg geen operationeel belang hebben, verzet de WPA zich er evenmin tegen dat de verantwoordelijke politiezone zelf een recht van toegang tot de beelden organiseert[33]. In casu kan het toegangssysteem, naar analogie met de wet betreffende de camera's van 21 maart 2007, als voorbeeld dienen, zodat niet alleen de politieambtenaar maar ook de burger zich rechtstreeks kan wenden tot de betrokken politiedienst.

3.1.6 Zichtbaar en niet-zichtbaar gebruik van camera's

12. Zichtbare camera's zijn camera's waarvan het gebruik wordt aangegeven door middel van pictogrammen, camera's gemonteerd aan boord van politievoertuigen, -vaartuigen, -luchtvaartuigen of elk ander vervoermiddel van de politie, dat als dusdanig geïdentificeerd kan worden of gedragen door politieambtenaren die als dusdanig identificeerbaar zijn[34]. In buitengewone situaties mag de politie gebruik maken van een verborgen gebruik van camera's (niet-zichtbaar gebruik). In dit geval wordt de camera gedragen door de politieambtenaar of in een anoniem politievoertuig geïnstalleerd. Er is sprake van een anoniem politievoertuig wanneer het politievoertuig niet als dusdanig herkenbaar is. In dit geval is er dus sprake van '*niet-zichtbaar*' gebruik van de camera[35]. Het gebruik van niet-zichtbare camera's wordt strikt gereglementeerd en beperkt zich tot vier situaties, i.e.:
1) wegens bijzondere omstandigheden, inzonderheid in geval van samenscholingen, om informatie van bestuurlijke politie in te winnen in verband met geradicaliseerde personen of *terrorist fighters,* en politievoertuigen die niet als dusdanig herkenbaar zijn, voor de automatische inlezing van nummerplaten, met als doel geseinde voertuigen op te sporen (art. 46/4 WPA);
2) om acties van gerechtelijke politie voor te bereiden en om de openbare orde te doen handhaven tijdens deze acties (artikelen 46/7 en 46/8 WPA);
3) in het raam van gespecialiseerde opdrachten van bescherming van personen (art. 44/9 WPA); en
4) bij de overbrenging van aangehouden of opgesloten personen (art. 46/11 WPA).

Tenzij het niet-zichtbare gebruik van camera's plaatsvindt onder het gezag van een magistraat, moet deze vorm van gebruik van camera's echter **voorafgaandelijk** ter kennis worden gebracht van het Controleorgaan. Deze voorafgaande kennisgeving moet het voor het Controleorgaan mogelijk maken de wettelijkheid van de beslissing te beoordelen[36].

3.1.7 Impact- en risicoanalyse en gegevensbeschermingseffectbeoordeling (GBEB of *DPIA*, *Data Protection Impact Assessment*)

13. Sinds de wet van 21 maart 2018 bestaat de verplichting om een impact- en risicoanalyse te maken voorafgaand aan het gebruik van bewakingscamera's, daar de bescherming van de persoonlijke levenssfeer wordt afgewogen ten aanzien van het operationeel niveau van het gebruik van de camera's[37]. Deze oefening moet ook worden gemaakt

[30] Art. 25/7 § 1, lid 1 en lid 2, en 44/11/3*decies* § 3, tweede lid van de WPA.
[31] Art. 44/11/3*decies* § 3, lid 1 van de WPA.
[32] Memorie van toelichting van deze wet, p. 29 (Parl. St., *Kamer* 2017-2018, nr. 54-2855/001).
[33] Zoals in principe bepaald in artikel 14 (recht van inzage) van de Richtlijn Politie-Justitie.
[34] Art. 25/2 § 2 van de WPA.
[35] Art. 46/4 e.v. van de WPA.
[36] Art. 46/6 en 46/10 van de WPA.
[37] Art. 25/4 § 2 van de WPA.

voorafgaand aan het aanleggen van een (lokale) technische gegevensbank[38]. Daartoe wordt de bijstand van de *DPO* gevraagd[39].

Voor zover er is voldaan aan de voorwaarden van de WGB voor een *DPIA* en aan de voorwaarden voor een impact- en risicoanalyse met betrekking tot het zichtbare gebruik van de camera's en/of betreffende het aanleggen van de technische gegevensbanken krachtens de WPA, mogen beide analyses worden samengebracht in een en hetzelfde document. Daar een *DPIA* krachtens de WGB een grondiger analyse vereist dan dit het geval is krachtens de WPA, wordt erop gewezen dat, indien beide samen worden behandeld, deze analyse – overeenkomstig de bepalingen van de WGB – betrekking moet hebben op alle relevante systemen en procedures van verwerkingsverrichtingen. Naast de inachtneming van de WGB en de WPA moeten ook de operationele voorzorgsmaatregelen en de beschermingsmaatregelen (die worden genomen om de risico's voor de te beschermen persoonsgegevens te beperken) worden beschreven.

3.1.8 Register

14. De gebruiken van camera's moeten worden vastgelegd in een (lokaal) register[40]. Het register vermeldt het type camera's en hun plaats. Er is echter nog geen enkel koninklijk besluit afgekondigd om de inhoud van dit register nader te bepalen. Dit belet niet dat het Controleorgaan van mening is dat de politie, in het licht van de doeltreffendheid van haar toezichtsbevoegdheden en in afwachting van het uitvoeringsbesluit, zelf het initiatief moet nemen om een register aan te leggen waarin alle gebruiken van (types) camera's worden opgenomen, met inbegrip van het niet-zichtbare gebruik van camera's. Op die manier heeft het Controleorgaan (en overigens ook de politiezone zelf, in eerste instantie) een overzicht alsook een idee van het gebruik van bewakingscamera's op het grondgebied van de gemeente waarvoor ze bevoegd is. Tegelijk kan het gebruik van bewakingscamera's worden gecontroleerd in functie van het register van de verwerkingsactiviteiten. Daar de camera persoonsgegevens verwerkt, moet deze verwerking ook worden opgenomen in het register van de verwerkingsactiviteiten[41]. Beide registers zijn beschikbaar, of moeten dat zijn, voor het Controleorgaan.

3.1.9 Camerabewaking in de gebouwen, politiekantoren en politiecellen

15. De camerabewaking in de gebouwen, kantoren en cellen van de politie behoort tot het toepassingsgebied van de WPA[42][43]. Dit geldt ook voor de camerabewaking in de inkomhal of aan het onthaal van het politiecommissariaat. De videobewaking[44] in de opsluitingsplaatsen draagt bij tot de bescherming en de garantie van het welzijn van de personen die van hun vrijheid worden beroofd en draagt ook bij tot een betere inachtneming van de rechten van de verdediging, zoals bedoeld in artikel 6 van het Europees Verdrag voor de Rechten van de Mens[45]. Dergelijke videobewaking is echter enkel mogelijk als element dat wordt toegevoegd aan een reeks maatregelen zoals een regelmatige fysieke controle van de opgesloten personen, een beleid tot voorkoming van zelfmoord, een doeltreffend aangiftesysteem voor de slachtoffers van onwettige handelingen in de cellen, afzondering, isoleren, het opleggen van tuchtsancties of ook de aanwezigheid van een advocaat bij het verhoor door de politie[46]. Het politiegebouw – of de politiepost – moet uitgerust zijn met duidelijke signalisatie van de videobewaking zodat de persoon die in een van de cellen wordt opgesloten daar

[38] Art. 44/11/3*octies* van de WPA.
[39] Art. 65, 3° *juncto* 58 van de WGB.
[40] Art. 25/8 van de WPA.
[41] Art. 55 van de WGB en 145 WGP.
[42] Zie ook het KB van 14 september 2007 betreffende de minimumnormen, de inplanting en de aanwending van de door de politiediensten gebruikte opsluitingsplaatsen, inzonderheid artikel 10.
[43] Met uitzondering van de camerabewaking met het oog op de controle op de uitvoering van de arbeidsvoorwaarden (zie Advies uit eigen beweging van het Controleorgaan op de politionele informatie met betrekking tot het invoeren van camerabewaking door de geïntegreerde politie met het oog op de controle van de naleving van de arbeidsvoorwaarden, BD200007, 17 augustus 2020, te vinden op www.controleorgaan.be).
[44] Aanbeveling 06/11 van de gewezen Commissie voor de bescherming van de persoonlijke levenssfeer of CPL – vandaag de Gegevensbeschermingsautoriteit of GBA – betreffende de installatie en het gebruik van bewakingscamera's in de opsluitingsplaatsen (cellen en verhoorlokalen) en in andere plaatsen van het commissariaat.
[45] Europees Verdrag voor de Rechten van de Mens.
[46] Zie in verband hiermee: "Les normes du CPT – Chapitres des rapports généraux du CPT consacrés à des questions de fond" (document CPT/Inf/E (2002) 1 – Rev. 2009), te vinden op www.cpt.coe.int/en/docsstandards.htm.

uitdrukkelijk kennis van zou krijgen. De registraties van de opsluiting moeten volledig blijven (gedeeltelijk wissen of wijzigen is niet mogelijk) en moeten worden bewaard tijdens een redelijke periode waarbinnen een klacht kan worden ingediend.

Daar deze beelden niet noodzakelijk of over het algemeen zelfs geen operationeel belang hebben, is de procedure inzake de indirecte toegang tot deze beelden via het COC niet van toepassing en kan de betrokkene, overeenkomstig de WGB en de AVG, rechtstreeks toegang krijgen tot de geregistreerde beelden van zijn opsluiting.

Bij het bekijken van de beelden van de verschillende cellen op de beeldschermen in het commissariaat, moet de politie meerdere strikte veiligheids- en toegangsmaatregelen nemen: de toegang moet worden beperkt overeenkomstig het principe *need to know*. Algemene toegang tot de beelden (bv. beeldschermen in een doorgangslokaal voor personeelsleden of bij het onthaal) moet worden vermeden.

3.2 Audiovisuele opname in het kader van een strafrechtelijk onderzoek

16. Krachtens artikel 112*ter* van het Wetboek van Strafvordering (Wb. 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 auditieve opname van het verhoor kan worden verricht door een politieambtenaar (§ 2) die in dit geval deze wijze van verhoor moet vermelden in het proces-verbaal (§ 3). Het gaat dus niet om een vorm van camerabewaking (met audio), zoals bedoeld in en geregeld door de WPA. Bovendien wordt de beslissing inzake audiovisuele of auditieve opname niet genomen op initiatief van de korpschef. De te verhoren persoon (en de advocaat) mogen ook niet onwetend zijn van het feit dat er een audiovisuele of auditieve opname wordt gemaakt. Een verborgen audiovisuele opname of het verborgen gebruik van de audiovisuele opname zoals bedoeld in artikel 112*ter* Wb. Sv. is dus onwettig.

3.3 Vertrouwelijk overleg met een advocaat

17. Dit alles blijkt uit de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM)[47] met betrekking tot de vertrouwelijkheid van de relatie tussen de cliënt en de advocaat. De vertrouwelijkheid van deze relatie[48] is fundamenteel en wordt beschermd door de artikelen 6 en 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM)[49]. Deze relatie betreft dus zowel het recht op privacy, in de ruime betekenis, van de betrokkene (artikel 8) als zijn recht op een eerlijk proces (artikel 6).

Een veelzeggend voorbeeld van een zaak in een politiecommissariaat vinden we in het geval R.E. t/ Verenigd Koninkrijk[50] dat ook verwijst 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)."*

Alleen al de aanwezigheid van een camera in een lokaal bestemd voor vertrouwelijke gesprekken tussen de advocaat en zijn cliënt kan in strijd zijn met de artikelen 6 en 8 van het EVRM, los van het feit of de camera al dan niet effectief filmt / opneemt, inzonderheid omdat de vertrouwelijkheid die tijdens een dergelijk gesprek zou moeten kunnen ontstaan niet is gewaarborgd. *A fortiori* indien de beelden en/of de klank effectief worden geregistreerd of indien de audio kan worden gehoord. Alleen wanneer de advocaat dat vraagt, in het raam van de eigen veiligheid, kan het gebruik van video, maar dus **niet** van audio, gerechtvaardigd zijn.

[47] Europees Hof voor de Rechten van de Mens.
[48] We verwijzen meer bepaald naar EHRM 10 september 2013, Helander t/ Finland, nr. 10410/10, en naar EHRM 21 februari 1975, Golder t/ Verenigd Koninkrijk, nr. 4451/70.
[49] Europees Verdrag voor de Rechten van de Mens.
[50] EHRM R.E. t/ Verenigd Koninkrijk van 27 oktober 2015, nr. 62498/11.

4 RESULTATEN VAN HET TOEZICHT

4.1 Audiovisuele registratie van het vertrouwelijk overleg

18. Tijdens het bezoek kon het COC vaststellen wat volgt:

1. Het cameratoezicht wordt effectief gebruikt in het politiecommissariaat;
2. Het cameratoezicht wordt in reële tijd visueel gevolgd voor de volgende camera's:
    a. In het onthaallokaal: de camera's aan de buitenkant van het gebouw;
    b. In het dispatchinglokaal: de camera's van de cellen;
    c. Wat betreft de camera's van het wapenlokaal, het lokaal met de overtuigingsstukken, het lokaal voor fouilleren en de verhoorlokalen / lokalen voor vertrouwelijk overleg: de beelden kunnen enkel worden geraadpleegd door de interne controledienst en de ICT-verantwoordelijke;
3. De camerabeelden worden bewaard gedurende een termijn van maximaal 30 dagen;
4. De camera's draaien de klok rond (24/7), zonder enige uitzondering. Bijgevolg registreren de camera's in de verhoorlokalen ook het vertrouwelijk overleg;
5. De PZ Arrondissement Luik gebruikt camera's in de verhoorlokalen / lokalen voor vertrouwelijk overleg op eigen initiatief voor doeleinden van algemene veiligheid alsook voor de veiligheid van de advocaat;
6. Er is echter geen effectief gebruik van de camera tijdens het vertrouwelijk overleg in de vorm van visuele bewaking in reële tijd;
7. Het audioregistratiesysteem draait de klok rond (24/7), zonder enige uitzondering, in de verhoorlokalen / lokalen voor vertrouwelijk overleg. **Bijgevolg worden de gesprekken tijdens het vertrouwelijk overleg eveneens geregistreerd**;
8. De gesprekken van het vertrouwelijk overleg worden echter niet in reële tijd beluisterd;
9. De PZ Arrondissement Luik registreert de gesprekken in de verhoorlokalen / lokalen voor vertrouwelijk overleg op eigen initiatief voor doeleinden van algemene veiligheid alsook voor de veiligheid van de advocaat;
10. Een pictogram en een tekst waarschuwen de personen die zich in de verhoorlokalen / lokalen voor vertrouwelijk overleg bevinden met betrekking tot het feit dat er permanent audio- en video-opnames worden gemaakt;
11. Tijdens de voorbije 5 maanden waren er in de politiezone Arrondissement Luik geen gevallen waarbij audiovisuele verhoren dienden te worden geregistreerd op verzoek van de procureur des Konings / de onderzoeksrechter (art. 112ter Wb. Sv.);
12. Wanneer dergelijke verhoren echter plaatsvinden, zal er gebruik worden gemaakt van hetzelfde systeem voor audiovisuele registratie;
13. Daar er permanent (24/7) opnames worden gemaakt in de verhoorlokalen / lokalen voor vertrouwelijk overleg, wordt het verloop van het verhoor op audiovisuele wijze opgenomen nadat er is verzaakt aan de bijstand van een advocaat (zie artikel 2bis, §3 van de wet betreffende de voorlopige hechtenis);
14. Met uitzondering van een (verouderde) richtlijn die van 2010 dateert, beschikt de politiezone Arrondissement Luik niet over richtlijnen die het gebruik van camera's voor politionele doeleinden regelen. Echter:
    a. Met betrekking tot de fouilleringen: deze worden uitgevoerd in het lokaal voor de cellen met een camera die de klok rond (24/7) opnames maakt. In het geval van een naaktfouillering bestaat de praktijk erin om de celdeur te openen op zodanige wijze dat de bewakingscamera de gefouilleerde persoon niet rechtstreeks kan filmen;
    b. Slechts één profiel krijgt toegang tot de opnames van de bewakingscamera's en van het geluid, i.e. de beheerder (administrator); in de feiten wordt dit profiel enkel toegewezen aan 2 natuurlijke personen van de dienst ICT, op verzoek van de interne controledienst;
    c. Daar de software voor beheer van de beeld- en klankopnames geen reden van raadpleging of loggen mogelijk maakt, worden de redenen voor raadpleging alsook de identiteit van de persoon die heeft geraadpleegd, geregistreerd in een wachtlogboek;
    d. Er is niet voorzien in een back-upsysteem;
    e. Indien de interne controledienst bepaalde opnames nodig zou hebben, worden die geëxporteerd op een externe harde schijf. Voor het COC is het niet duidelijk in welke mate noch op welke wijze de controle van de levensduur van de opnames op deze schijf wordt georganiseerd.

15. Het COC kon de aanwezigheid van de opnames van de verhoren vaststellen in de software voor beheer van de beelden van de camera's in de verhoorlokalen / lokalen voor vertrouwelijk overleg. Een opname van een vertrouwelijk overleg was echter niet beschikbaar bij de geregistreerde beelden. Het COC kon eveneens vaststellen dat de kwaliteit van het opgenomen geluid beperkt was.

4.2 Audiovisuele registratie in de cellen

19. Het COC kon ook vaststellen dat er permanent audio-opnames worden gemaakt in de cellen van de politiezone Arrondissement Luik. Het pictogram in het cellencomplex informeert de aangehouden personen daar echter niet over, daar enkel het pictogram betreffende het gebruik van camera's aanwezig is. Ondanks het feit dat de kwaliteit van de geluidsopnames beperkt is, wenst het COC hier toch een expliciete waarschuwing te formuleren ten aanzien van de artikelen 314*bis* en 259*bis* van het Strafwetboek, die de burger beschermen tegen het afluisteren, de kennisname en de registratie van "*niet voor publiek toegankelijke communicatie*"[51]. Dit betekent dat in het geheim afluisteren (interceptie) of de geheime registratie van een gesprek waaraan men **niet** deelneemt, wordt bestraft door artikel 314*bis* of artikel 259*bis* van het Strafwetboek. Het eerste artikel beschermt de communicatie ten aanzien van particulieren, terwijl het tweede artikel bescherming biedt tegen inbreuken die worden begaan door (politie)ambtenaren[52]. Inbreuken op de bescherming van de communicatie zijn enkel mogelijk indien – en voor zover dat – de wet daarin voorziet, zoals in de omstandigheden en onder de voorwaarden bedoeld in artikel 90*ter* van het Wetboek van Strafvordering.

Zowel normale gesprekken als telecommunicatie worden beschermd. Het gaat om communicatie die zich afspeelt in de privésfeer[53], met dien verstande dat de term 'privé' niet op restrictieve wijze mag worden geïnterpreteerd. Alle communicatie wordt beschermd, ook al heeft ze niet noodzakelijk betrekking op de persoonlijke levenssfeer van de deelnemers aan het gesprek. Vanaf het ogenblik waarop het gesprek niet bestemd is om te worden beluisterd door derden, gaat het om 'privécommunicatie' of 'niet voor publiek toegankelijke communicatie' in de betekenis van artikel 259*bis* (en artikel 314*bis*) van het Strafwetboek. Met andere woorden, gesprekken die in een professionele context worden gevoerd, worden eveneens beschermd[54]. Bovendien is de bescherming niet afhankelijk van de plaats maar veeleer van de context en van de bedoelingen van de deelnemers aan het gesprek. Bijgevolg valt een gesprek onder

[51] Artikelen 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 tot oprichting van een gegevensbank stemafdrukken. Deze wet vervangt in de artikelen 314bis en 259bis van het Strafwetboek de term '*privécommunicatie of -telecommunicatie*' door de term '*niet voor publiek toegankelijke communicatie*'. Het gaat om een louter terminologische wijziging (Parl. St. *Kamer* 2015-2016, nr. 54-1966/001, 75). Bovendien werd het element "*tijdens de overbrenging*" geschrapt in beide strafrechtelijke bepalingen.

[52] Artikel 259*bis* van het Strafwetboek 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."

[53] De wijziging van terminologie verandert niets aan de draagwijdte van het begrip 'privécommunicatie' in het oude artikel (Parl. St. *Kamer* 2015-2016, nr. 54-1966/001, 53).

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

de bescherming van het geheim van de communicatie wanneer het niet bestemd is om te worden gehoord door eender wie, ongeacht waar het plaatsvindt – in de woonkamer, op de werkvloer of in een openbare ruimte[55].

Artikel 259*bis* van het Strafwetboek bestraft ook de illegale kennisname van communicatie waaraan een persoon zelf niet deelneemt. De persoon die de gesprekken opneemt, is niet de enige die er kennis van zal nemen. Naast de politieambtenaar die het gesprek opneemt, heeft ook de hiërarchie van de politie meestal toegang tot de communicatie (de beelden en de klank) (bv. in het kader van een tuchtonderzoek of eenvoudigweg voor interne doeleinden van kwaliteitscontrole).

De bescherming is enkel van toepassing wanneer het gesprek wordt onderschept, wordt opgenomen of zo er kennis van wordt genomen met behulp van welk toestel ook. Luisteren met enkel de zintuigen is dus niet strafbaar en stelt dus geen probleem, wat betekent dat er dus geen probleem is wanneer politieambtenaren op actieve en/of passieve wijze (met de zintuigen) deelnemen aan het gesprek / de interactie.

Dit betekent echter dat de politieambtena(a)r(en) die het gesprek beluistert (beluisteren) of opneemt (opnemen) of er kennis van neemt (nemen) zonder dat de voorwaarden van artikel 25/2 §2, 2°, b) van de WPA en van artikel 259*bis* van het Strafwetboek in acht worden genomen, kan (kunnen) worden bestraft.

Het loutere feit dat de politie verantwoordelijk is voor het welzijn van de beklaagde kan niet worden beschouwd als een expliciete uitzondering op de bescherming van de communicatie. De (Europese) rechtspraak heeft al meermaals gesteld dat een uitzondering op dit fundamentele recht op duidelijke en expliciete wijze moet worden omschreven (vereiste inzake voorzienbaarheid; omstandigheden en voorwaarden waaronder een inbreuk op de bescherming van de communicatie is toegestaan). Het enkele feit dat de betrokkene zich in een politiecel bevindt en aldus onder de verantwoordelijkheid van de politie valt, rechtvaardigt bijvoorbeeld niet dat een monoloog van de beklaagde mag worden opgenomen zonder diens toestemming.

In zijn advies met betrekking tot *bodycams*[56] verdedigt het COC de zienswijze dat de politie in bepaalde situaties kan worden beschouwd als een 'deelnemer' aan de communicatie. Volgens het COC kan zulks *in casu* het geval zijn wanneer de politieambtenaar de intercom gebruikt om te weten hoe de beklaagde het stelt en daarbij de communicatie opneemt. Omgekeerd kan dat ook het geval zijn wanneer de beklaagde contact opneemt met de politieambtenaar met behulp van de intercom / de noodknop. Het is niet onbelangrijk om de beklaagde daarvan op voorhand kennis te geven. Anderzijds zal de stelselmatige registratie van de communicatie van de beklaagde naar alle waarschijnlijkheid een inbreuk vormen op artikel 259*bis* van het Strafwetboek, net omdat de politie niet automatisch kan worden beschouwd als een deelnemer aan het gesprek. Een algemene waarschuwing die in het cellencomplex wordt uitgehangen, zal ook niet worden gelijkgesteld met een (impliciete) toestemming van de beklaagde.

5 CONCLUSIES, VERZOEKEN EN CORRIGERENDE MAATREGELEN

20. Aan de hand van de verkregen antwoorden kon het COC duidelijk vaststellen dat de politiezone Arrondissement Luik permanent de beelden en de klank opneemt in verband met het vertrouwelijk overleg, zonder de advocaat en zijn cliënt daarvan noodzakelijkerwijze uitdrukkelijk kennis te geven. Een pictogram en een tekst informeren de advocaat en zijn cliënt over deze permanente registratie.

21. Het COC kon ook vaststellen dat er permanent audiovisuele opnames worden gemaakt in de cellen. Aangehouden personen worden echter niet geïnformeerd over het feit dat de klank permanent wordt opgenomen.

22. Er zijn geen richtlijnen beschikbaar met betrekking tot deze verwerking.

23. De geregistreerde beelden en klank zijn enkel toegankelijk voor twee personen die dezelfde account delen.

[55] Verslag bij het wetsontwerp, Parl. St. *Senaat* 1992-1993, nr. 843/2, 10 (verslag bij het wetsontwerp).
[56] Advies op eigen initiatief van het Controleorgaan op de politionele informatie naar aanleiding van de bevindingen in het kader van een onderzoek naar het gebruik van *bodycams*, 8 mei 2020, CON19008.

24. De software voor beheer van de beelden en de klank maakt het niet mogelijk om een reden voor de raadpleging te registreren en ook loggen is niet mogelijk. Dit technisch defect wordt gematigd in de vorm van een organisatorische maatregel, i.e. de registratie van de redenen voor raadpleging in een monitoringschrift.

25. Er is geen *back-up*. Het is niet duidelijk hoe de latere verwerking via harde schijf wordt georganiseerd.

OM DEZE REDENEN,

Het Controleorgaan;

verzoekt de politiezone Arrondissement Luik,

1. Verzoek

Duidelijke richtlijnen aannemen inzake het gebruik van camera's in de politiezone in het algemeen en in het politiegebouw in het bijzonder. Deze richtlijnen moeten ten minste rekening houden met de profielen, de reden voor de raadpleging invullen, de registratietermijnen, de logbestanden en de latere verwerking, desgevallend, van de opnames;

2. Verzoek

De mogelijkheid bestuderen om te voorzien in een afgescheiden lokaal waar het vertrouwelijk overleg tussen de advocaat en zijn cliënt zou kunnen plaatsvinden;

3. Verzoek

De mogelijkheid bestuderen om het systeem voor beeld- en klankopname in de verhoorlokalen te voorzien van een duidelijk zichtbare aan- en uitknop die toelaat het camerasysteem in en uit te schakelen;

4. Verzoek

Voorafgaand aan het verhoor de redenen en de nadere regels voor gebruik van de camera's duidelijk uitleggen aan de advocaat en zijn cliënt, en daarvan akte doen nemen in het proces-verbaal.

* * * * * * * * *

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

Beveelt aan de politiezone Arrondissement Luik aan om de volgende corrigerende maatregelen te nemen,

a. Corrigerende maatregel

Gelet op de vaststellingen in punt 18, i.e. de permanente registratie van het vertrouwelijk overleg tussen de advocaat en zijn cliënt, **met onmiddellijke ingang** een einde maken aan het permanent opnemen van beelden en klank van het vertrouwelijk overleg tussen de advocaat en zijn cliënt en dit bevestigen aan het Controleorgaan; zegt voor recht dat "*onmiddellijke ingang*" moet worden begrepen als de datum van toezending van het huidige verslag (per e-mail) door het Controleorgaan plus twee werkdagen (excl. zaterdag en zondag);

b. Corrigerende maatregel

Gelet op de vaststellingen in punt 19, i.e. de permanente geluidsopname in de cellen die de mogelijkheid biedt om de gesprekken te onderscheppen of in het geheim te beluisteren;

beveelt het COC aan de politiezone Arrondissement Luik aan om de geluidsopnames in de cellen in overeenstemming te brengen met het geldende wettelijk kader wat betreft het verzamelen, de bewaren, de toegang en het loggen, en **dit binnen de zes maanden** vanaf de ontvangst van dit verslag; zegt voor rechten dat "*binnen de zes maanden*" moet worden begrepen als de datum van toezending van het huidige verslag (per e-mail) door het Controleorgaan plus twee werkdagen (excl. zaterdag en zondag).

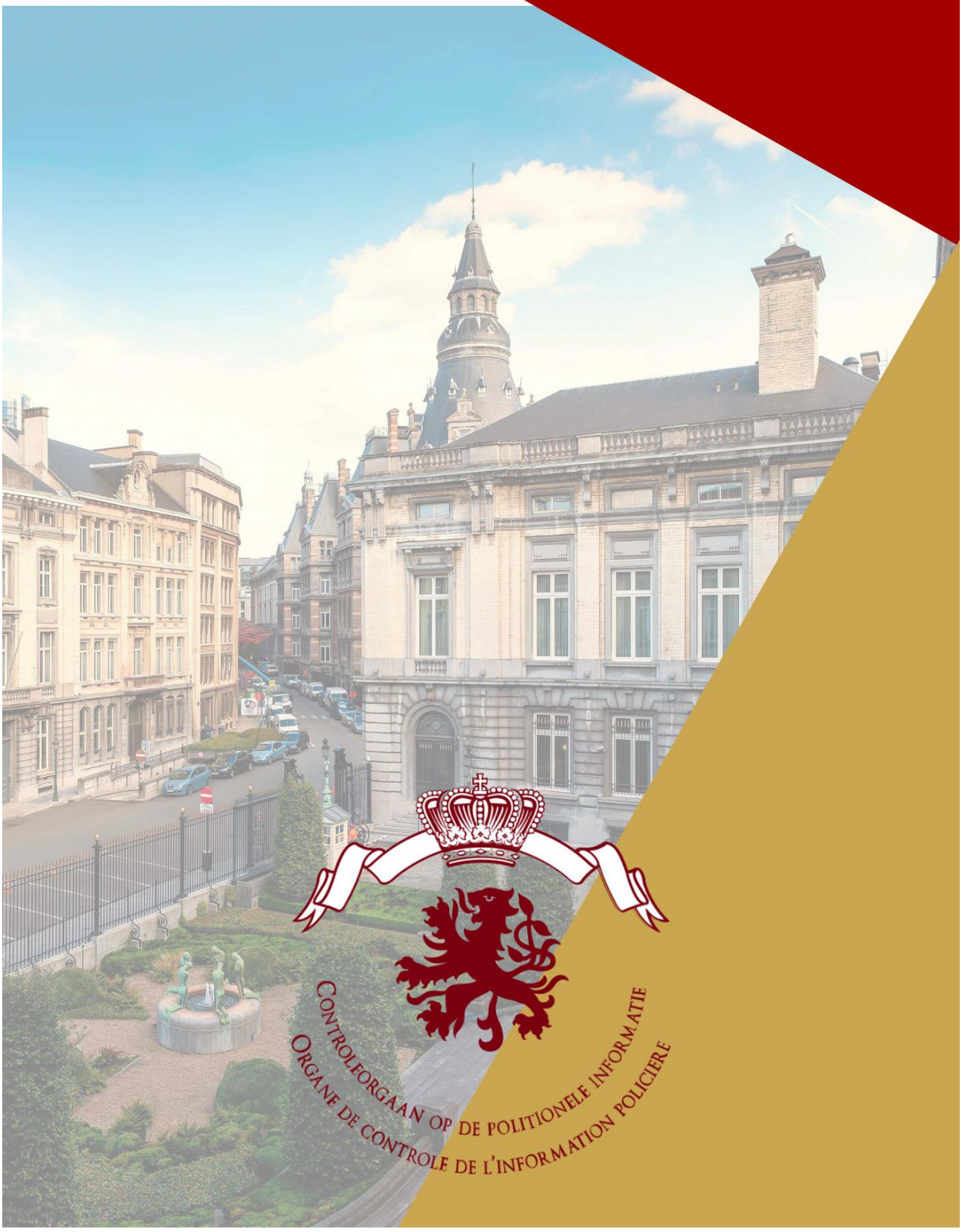
Aldus beslist door het Controleorgaan op de politionele informatie op 29 maart 2022.

Voor het Controleorgaan,

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

Kopie:

- De voorzitter van het politiecollege
- De procureur des Konings van Luik



Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière