THEMATISCH TOEZICHT

TOEZICHTRAPPORT VAN HET CONTROLEORGAAN OP DE POLITIONELE INFORMATIE MET BETREKKING TOT HET GEBRUIK VAN *CLEARVIEW AI* DOOR DE GEÏNTEGREERDE POLITIE

Referte: DIO21006

RAPPORT

INHOUDSOPGAVE

De bevoegdheden van het Controleorgaan op de politionele informatie

De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (WGB)[1] 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 2 en 7 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[2].

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 inbreuken 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.

---

[1] *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*)).

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

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

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

[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 en art. 27, 7°, d WGB.

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

[6] Art. 4 § 2 4e lid, wet van 3 december 2018 tot oprichting van de Gegevensbeschermingsautoriteit (WOG).

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].

De leden en de personeelsleden van het Controleorgaan waaronder onder meer zijn 'dienst Onderzoeken (DOSE)'[9] beschikken over onderzoeksbevoegdheden waarna zo nodig door het Controleorgaan, en meer specifiek zijn directiecomité (DIRCOM) corrigerende maatregelen kunnen 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].

1. VOORWERP VAN HET TOEZICHT

1. Het onderzoek heeft betrekking op het mogelijk gebruik van de gezichtsherkenningsapplicatie *Clearview AI*[12] door de geïntegreerde politie (GPI[13]). Het betreft een naar het Amerikaans bedrijf genaamd commercieel beschikbaar gestelde applicatie waarbij de klant aan de hand van gezichtsherkenningssoftware foto's kan vergelijken met foto's die in de gegevensbank van *Clearview* worden bewaard. Het bedrijf *Clearview* kwam in België in februari 2020 in opspraak. Het bedrijf schraapt massaal foto's van digitaal publiek toegankelijk bronnen, zoals sociale media, om deze voor commerciële doeleinden ter beschikking te stellen aan rechtshandhavingsautoriteiten[14]. Volgens de media zouden ook Belgische politiediensten van de *Clearview* applicatie gebruik maken of gemaakt hebben. Op 25 augustus 2021 vermeldt de nieuwswebsite *Buzzfeed* dat de Belgische federale politie 100 tot 500 opzoekingen heeft of zou hebben uitgevoerd met de *Clearwiew* tool[15]. Het Controleorgaan stelt vast de federale politie niet heeft willen reageren op dit bericht.

2. VOORGAANDEN

2. Na het eerste persbericht op 28 februari 2020 werd door het Controleorgaan op **2 maart 2020** aan het nieuwe 'Strategisch Comité Informatie en ICT'[16]van de GPI een schrijven gericht waarbij wordt gemeld dat het Controleorgaan werd bevraagd met betrekking tot het gebruik van de *Clearview* applicatie door de GPI Het Controleorgaan stelde de volgende vraag:
"Wordt actueel gebruik gemaakt of geëxperimenteerd met FRT door de Belgische GPI of één van haar onderdelen (hetzij de federale politie, hetzij een lokale politie)? Zo ja, kan het COC meegedeeld worden door welke entiteit dat zou gebeuren? Ik zou u dank weten deze vraag te willen voorleggen aan de politiediensten en het COC een antwoord te formuleren."

3. Op **19 mei 2020** ontvangt het COC van het Strategische Comité ICT het kennelijk aan dit Comité door de federale politie en de Vaste Commissie van de Lokale Politie gestuurd hiernavolgend antwoord: "***Op basis van de thans beschikbare informatie is er binnen de Federale Politie op organisatieniveau geen kennis over het gebruik van gezichtsherkenningssoftware binnen de politiediensten***[17]*". Er zijn op dit moment ook geen intenties om dit soort software te gaan inzetten aangezien er een meer soliede wettelijke basis vereist is om deze technologie aan te kunnen wenden*". Op grond van dit bericht ging het Controleorgaan er dan ook van uit dat er door de Belgische politiediensten geen gebruik is of werd gemaakt van de *Clearview* gezichtsherkenningstechnologie. Vragen uitgaande van de pers naar het gebruik ervan door de Belgische politie werden door het COC dan ook steevast ontkennend beantwoord.

---

[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] *Artificial Intelligence.*
[13] GPI staat voor **G**eïntegreerde **P**olitie – **P**olice **I**ntégrée.
[14] VRT nieuwdienst 28 februari 2020, https://www.vrt.be/vrtnws/nl/2020/02/28/clearview (met verwijzing naar de nieuwswebsite *Buzzfeed* van 27 februari 2020).
[15] https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.
[16] Het zgn. 'Strategisch adviescomité voor informatie' bedoeld in artikel 8*sexies* van de Wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus (WGP)
[17] Onderlijning door het Controleorgaan.

Op **25 augustus 2021** verschijnt er evenwel opnieuw een artikel in het Amerikaanse *Buzzfeednews* met betrekking tot de *Facial Recognition Technologie* (*FRT*) van *Clearview* waarin deze keer uitdrukkelijk wordt gesteld dat ook de Belgische federale politie tussen 100 en 500 keer gebruik zou hebben gemaakt van de technologie. Er werd ook melding gemaakt van een vergadering in Europol in oktober 2019 waaraan België zou hebben deelgenomen en tijdens dewelke het gebruik ervan door Europol, Interpol en 21 lidstaat-vertegenwoordigers zou zijn besproken. De Europol woordvoerder zou één en ander hebben bevestigd. Van dit alles werd voor alle duidelijkheid geen melding gemaakt in de eerdere bevraging van de GPI door het COC in 2020.

Bij schrijven van **27 augustus 2021** bevraagt het COC de commissaris-generaal van de federale politie derhalve opnieuw naar het beweerdelijk gebruik van de *Clearview* gezichtsherkenningstechnologie door de GPI in het algemeen of door de federale politie in het bijzonder. Het COC wijst erop dat een en ander niet lijkt overeen te stemmen met het (hiervoor vermelde) antwoord van 19 mei 2020 dat het COC van de federale politie namens de hele GPI had ontvangen. Het COC verzoekt de commissaris-generaal het waarheidsgehalte van de berichtgeving te onderzoeken en daarover tegen 27 september 2021 duidelijkheid te verschaffen.

Op **22 september 2021** ontvangt het COC een antwoordschrijven van de commissaris-generaal waarin, na een intern onderzoek en een bevraging bij *Clearview* zelf, tekst en uitleg wordt gegeven nopens het al dan niet gebruik van de *FRT* technologie. Daaruit blijkt in essentie toch wel een heel ander verhaal dan de boodschap die vanuit de GPI in mei 2020 aan het COC werd overgemaakt en waarop het Controleorgaan zich tot dan toe had gesteund. Zo blijkt volgens het intern gevoerd onderzoek dat leden van DGJ/DJSOC[18], dient *Child Abuse*, twee maal per jaar deelnemen aan een operationele Europol *taskforce*, *Victim Identifcation Taskforce*. In 2019 ging de taskforce fysiek en in 2020 virtueel door (in aanwezigheid van de Amerikaanse FBI). Het is in dat kader dat testlicenties ter beschikking werden gesteld door Europol aan de deelnemers (waaronder dus twee leden van DJSOC). Die personeelsleden van DJSOC hebben volgens de commissaris-generaal de applicatie dan herhaaldelijk getest/gebruikt op niet Belgische dossiers tijdens de Europol taskforce en (bij terugkeer in België) ook op dossiers van het Amerikaanse *NCMEC* (*National Center for Missing and Exploited Children*) en verder testen gedaan met eigen foto's en foto's van collega's/kennissen. Er werden blijken de brief van 22 september 2021 bij die testen nooit "*operationele resultaten*" gehaald (in de betekenis van opsporingsmatig relevante resultaten). Volgens *Clearview* zouden er in totaal 78 bevragingen gebeurd zijn met 10 februari 2020 als laatste datum van gebruik. De commissaris-generaal bevestigt in dit schrijven tot slot dat de applicatie door de federale politie niet zal worden gebruikt zolang het wettelijk kader dit niet toelaat en dat, teneinde elk gelijkaardig voorval in de toekomst te vermijden, aan alle personeelsleden in herinnering zal worden gebracht dat elk gebruik van applicaties of elke verwerking van persoonsgegevens voor professionele doeleinden slechts mogelijk is mits de strikte eerbiediging van de wettelijk voorzien voorwaarden.

Bij schrijven van **1 oktober 2021** wijst het COC op enige inconsistenties in het antwoord van de commissaris-generaal van 22 september 2021 waardoor en waarna het Controleorgaan beslist een meer actief ambtshalve onderzoek op te starten. Immers, waar in het antwoord van 19 mei 2020 van het Strategisch Comité Informatie en ICT werd gesteld dat de *Clearview* applicatie niet door de (federale) politie wordt gebruikt, werd in voormelde brief van de 22 september 2021 het volgende geantwoord: " *A leur retour, l'un des deux participants a utilisé l'outil à quelques jours qui restaient de la licence d'essai, mais toujours sans résultat*", terwijl anderzijds werd gesteld, "*Le Chef de service confirme donc bien que la solution n'a pas été utilisé dans des analyses par DGJ*». Om meer duidelijkheid te krijgen werden door het COC in dezelfde brief van 1 oktober 2021 aan de commissaris-generaal negen (9) vragen gesteld (zie hierna).
In die brief van het Controleorgaan wordt er tevens op gewezen dat deze informatie reeds had moeten opgenomen (geweest) zijn in de gegevensbeschermingseffectbeoordeling (GEB) of DPIA[19], die voorafgaand aan het gebruik van deze technologie had moeten opgemaakt zijn en die het Controleorgaan niet en nooit heeft ontvangen.

In het raam van parlementaire vragen over de software *Clearview* in de Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van **6 oktober 2021** antwoordt de minister van Binnenlandse Zaken dat er geen structureel gebruik wordt gemaakt van de *Clearview* tool binnen de federale politie, maar dat uit intern onderzoek door de federale politie blijk dat 2 rechercheurs tijdens een vergadering van de *taskforce* Slachtofferidentificatie bij Europol in oktober 2019 toegang hadden tot een proeflicentie die voor een beperkte periode geldig was. De minister voegt eraan toe "*Aangezien het Belgisch wettelijk kader de exploitatie van deze software niet toelaat, zal ze niet door de federale politie worden gebruikt*"[20]. De minister vermeldt erbij dat de nodige informatie aan het COC wordt verstrekt.

Tot slot verstrekt de commissaris-generaal bij brief van **18 oktober 2021** een antwoord op de brief van het COC van 6 oktober 2021 waarin het ambtshalve onderzoek wordt aangekondigd. Daarbij wordt aan het COC een bundel bezorgd dat betrekking heeft op het intern onderzoek dat door de commissaris-generaal werd uitgevoerd naar aanleiding van de brieven van 22 september 2021 en 1 oktober 2021. Uit het antwoord van de commissaris-generaal blijkt verder nog

[18] Algemeen Directie Gerechtelijke Politie, Directie van de bestrijding van de zware en georganiseerde criminaliteit.
[19] Data Protection Impact Assessment.
[20] Parl. St. Kamer 2020-2021, CRIV 55 COM 597, 3-4.

dat in totaal door 3 leden van de federale gerechtelijk politie een tijdelijk account bij het bedrijf *Clearview* werden aangemaakt met het oog op het gebruik van de gezichtsherkenningstechnologie van het bedrijf.

Naar aanleiding van een bilateraal overleg op 3 november 2021 tussen het Controleorgaan en de toezichthouder op Europol, de *European Data Protection Supervisor* (EDPS)[21]werd door deze laatste aangekondigd dat het in opvolging van het door hen gevoerde onderzoek naar het gebruik van *Clearview* door Europol, een advies over het gebruik van de *Clearview*-applicatie door Europol werd uitgebracht. Dit advies van 29 maart 2021 werd inmiddels gepubliceerd weliswaar met weglating van enkele elementen. Niettemin leert de lezing van dit advies dat de vaststellingen door de EDPS grotendeels gelijklopen met deze gemaakt in huidig rapport[22].

3. METHODOLOGIE

4. Het onderzoek kan globaal worden opgesplitst in drie onderdelen. Het eerste onderdeel betrof het verkrijgen van duidelijke antwoorden op de door het COC in de brief van 1 oktober 2021 gestelde 9 vragen, met name:

Onderdeel 1

1) een kopie van het door de politiedienst intern gevoerd onderzoek naar het gebruik van deze technologie wat heeft geleid tot het schrijven van 22 september 2021;
2) eventuele afspraken met het bedrijf *Clearview* met betrekking tot het gebruik van de technologie;
3) de datum waarop de technologie daadwerkelijk in gebruik werd genomen;
4) in geval het gebruik van de technologie ondertussen werd stopgezet, de einddatum daarvan;
5) het volledig verwerkingsproces van het gebruik van de technologie (de wijze van gebruik van de technologie, lokale opslag van software en/of verwerking op het platform van *Clearview*, enz.);
6) het aantal, de aard en de PV-nummers van de dossiers waarvoor de technologie werd toegepast;
7) een presentatie (uitprint) van "een resultaat" bij het gebruik van de technologie (ook al is het resultaat opsporingsmatig negatief);
8) waar het resultaat van de toepassing van deze technologie bij de politie wordt bewaard;
9) hoeveel personen en van welke politie-entiteit geautoriseerd zijn/waren om deze technologie te gebruiken en wie dat heeft geautoriseerd;

Onderdeel 2

Op basis van de antwoorden en bevindingen werden twee leden van de centrale directie van de bestrijding van de zware en georganiseerde criminaliteit (DJSOC) gehoord in verband met het daadwerkelijk gebruik van de *Clearview* applicatie.

Onderdeel 3

Dit onderdeel betreft de juridische aftoetsing van het gebruik van de *Clearview* gezichtsherkenningstechnologie.

Voor een goed begrip volgt hierna eerst een algemene en korte toelichting over de toepassing van gezichtsherkenningstechnologie (hoofdstuk 4). Daarna komen de onderzoeksbevindingen aan bod waarbij eerst toelichting wordt gegeven bij de werking van de *Clearview* applicatie, gevolgd door het gebruik ervan door de federale gerechtelijke politie (hoofdstuk 5). Daarna volgt een toetsing van het gebruik van deze applicatie aan het huidig wettelijke kader (hoofdstuk 6). We eindigen dit rapport met enkele beschouwingen, de conclusie en de aanbevelingen en de corrigerende maatregelen (hoofdstukken 7 en 8).

Op 10-01-2022 werd het ontwerprapport voor overmaking in prelectuur goedgekeurd door het DIRCOM van het COC.
Op 10-01-2022 werd het ontwerprapport in prelectuur overgemaakt aan de commissaris-generaal in het raam van de tegenspraak.
Op 28-01-2022 ontving het COC de bemerkingen en verzoeken tot wijziging van de commissaris-generaal op het ontwerprapport en werden deze verwerkt en waar nodig toegelicht. Hierbij werd eveneens door de commissaris-generaal een nieuwe tijdelijke nota van 28.01.2022 CG/2022-16, getiteld "*Herinnering aan de richtlijnen inzake de verwerking van persoonsgegevens*", gericht aan alle eenheden van de federale politie, meegedeeld.

Op 4 februari 2022 werd het definitief rapport goedgekeurd door het DIRCOM van het COC.

[21] De EDPS is de gegevensbeschermingsautoriteit voor Europol; zie ook www.edps.europa.eu
[22] https://edps.europa.eu/system/files/2022-01/21-03-29_edps_opinion_2020-0372.pdf

4. DE TOEPASSING VAN GEZICHTHERKENNING

5. Het gebruik van gezichtsherkenningstechnologie of *FRT* staat in verband met de verwerking van biometrische persoonsgegevens. Deze persoonsgegevens behoren tot de 'bijzondere categorieën' van persoonsgegevens omdat ze onmiskenbare aspecten bevatten die tot (de kern van) het privéleven behoren doordat ze unieke persoonskenmerken bevatten. Behalve gezichtsafbeeldingen behoren onder meer ook vingerafdrukken[23] en de stem van de natuurlijke persoon tot deze bijzondere categorie van persoonsgegevens. De gezichtsherkenning vereist evenwel een aanvullende technische verwerking van de gezichtsafbeelding (de foto of het beeld)[24].

6. Kort gezegd kan het verwerkingsproces *in casu* in drie fasen worden opgedeeld. Nadat de foto of het beeld werd vastgelegd of beschikbaar gesteld (eerste fase), wordt vervolgens gebruik gemaakt van *software* die specifiek ontwikkeld is om unieke persoonskenmerken op de foto (beeld) te herkennen (tweede fase). Deze bewerking kan beschouwd worden als het vastleggen, en dus het verwerken, van biometrische gegevens waarbij de 'ruwe' gegevens (het vastleggen van de gezichtskenmerken) in een unieke cijfercode worden omgezet en op een drager worden bijgehouden (een zgn. *template*). Aan de hand van deze gegevens (biometrische *template*: de unieke cijfercode) kan de persoon uniek geïdentificeerd worden uit een (on)bepaalde groep personen. Hoewel in deze fase dus reeds biometrische gegevens worden verwerkt, zal het resultaat pas daadwerkelijk bereikt kunnen worden door deze *template* te vergelijken (bewerking van persoonsgegevens) met andere beschikbare foto's of beelden (derde fase)[25]. Bij een positief resultaat (*hit*: overeenstemming tussen de gezichtskenmerken) dient deze vervolgens gevalideerd te worden (*match*)[26]. De daadwerkelijke gezichtsherkenning gebeurt dus op basis van een specifieke technologische toepassing met het oog op de unieke identificatie van de persoon als gevolg van een koppeling (vergelijking) tussen minstens twee foto's of beelden.

7. In de politionele context beoogt het gebruikt van gezichtsherkenningstechnologie *grosso modo* twee algemene doelstellingen: **identificatie** op basis van ongerichte dan wel gericht opzoeking van personen[27].

8. Bij ongerichte (*real time - remote*) publieke gezichtsherkenning wordt een zeer omvangrijke hoeveel foto's of beelden (persoonsgegevens) vergeleken met een lijst van gezochte of vermiste personen. De toepassing van de gezichtsherkenning werkt vanop afstand (*remote*), zoals het cameranetwerk van de politie op publieke plaatsen die in en vanuit het politiegebouw wordt opgevolgd en beheerd. De gezichtsherkenning is in beginsel 'ongericht' omdat de beelden of foto's van een onbepaald aantal (toevallige) passanten, en dus van een ongedifferentieerd groep personen, worden gecapteerd. Het betreft in wezen een 'niet-verdachte versus verdachte/vermiste persoon' situatie (N:1). De gezichtsherkenning kan toegepast worden op de verwerking van beelden waarvoor de politiedienst de verwerkingsverantwoordelijke is dan wel op de beelden die bij een derde voor de politie (in *real time*) toegankelijk zijn, zoals de beelden van de openbare vervoersmaatschappijen of beelden bij een groot (door een private of publieke speler georganiseerd) evenement, die tijdens de duur van het evenement voor de politie toegankelijk (kunnen) zijn[28].

9. Bij publiek gerichte (*remote*) gezichtsherkenning worden de foto's of de beelden van verdachten of vermiste personen (slachtoffers) vergeleken met foto's of beelden die door camera's op publiek toegankelijk plaatsen worden verzameld en bewaard. Het betreft hier dus een omgekeerde beweging. In plaats van dat de foto's of beelden van een onbepaald en ongedifferentieerde groep personen worden vergeleken met een welbepaalde lijst, wordt aan de hand van door politie geselecteerde foto's of beelden gericht (en reactief) gezocht naar overeenstemmende foto's of beelden die door derden[29] of de politie worden beheerd (op een digitaal platform). Het betreft hier dus een gerichte onderzoeks- of

---

[23] Art. 26, 13° WGB en overweging 51 *LED*. Daarnaast gaat het ook om gedragsherkenning (gedragskenmerken) van de persoon.

[24] Art. 34 § 1, aanhef WGB.

[25] Op basis van de detectie van overeenstemmende unieke kenmerken op de foto's waarop de vergelijking wordt toegepast.

[26] Zie artikel 35, 1ste lid WGB. Het positief resultaat (de *match*) mag niet louter gebaseerd zijn op een geautomatiseerd besluit (verwerking), tenzij de wet die uitdrukkelijk regelt en met de nodige waarborgen omringd. In de huidige stand van de wet (WGB) moet de beslissing gebaseerd zijn op basis van een menselijke beoordeling.

[27] We laten hier 'authenticatie' buiten beschouwing. Waarbij het verwerkingsproces in vier fasen kan worden opgedeeld omdat de biometrische gegevens twee maal worden verwerkt: de eerste keer bij het inzamelen en opnieuw wanneer de betrokkene zich authentiseert. 'Authenticatie' betreft een verificatie aan de hand van één-op-één vergelijking (1:1): stemt de afbeelding van de persoon overeen met de persoon van wie de persoonsgegevens die in gegevensbank zijn opgeslagen (en zich daarmee identificeert)? Identificatie betreft daarentegen een één-tegenovermenig/veel (1:N) vergelijking zonder dat de persoon een bepaalde identiteit (verificatie) opeist. Anders gesteld, identificatie beantwoordt de vraag 'wie is deze persoon?' De persoon wordt uniek geïndividualiseerd. Bij authenticatie, daarentegen, wordt antwoord gegeven op de vraag 'is de persoon degene die hij is of beweert te zijn?'. In dat geval wordt de persoon dus niet uit een onbepaalde groep personen uniek geïndividualiseerd. Vgl. WENDEHORST, Y. DULLER, *Biometric Recognition and Behavioral Detection. Assessing the ethical aspects of biometric recognition en behavioural techniques with a focus on their current and future use in public spaces*. European Union 2021, 20, http://www.europarl.europa.eu/supporting-analyses.

[28] Zie in dat verband artikel 9, 3de lid, 3°, a) en b) Wet van 21 maart 2007 .

[29] Zoals trein- en busstations en andere publieke toegankelijke plaatsen waarvoor de politiedienst niet de beheerder is, zoals geregeld in artikel 9, 3de lid, 3° Wet van 21 maart 2007 "*tot regeling van de plaatsing en het gebruik van bewakingscamera's*" en artikel 25/1 § 2 WPA.

opsporingshandeling: de afbeelding van (verschillende) verdachten of slachtoffers wordt vergeleken met (ter beschikking gestelde) foto's of beelden met het oog op de identificatie van de verdachte of het slachtoffer (1:N)[30].

In de hiervoor besproken toepassingen wordt iedere *hit* door een bevoegde politieambtenaar gevalideerd (om al dan niet te komen tot een *match*).

10. Uit wat hierna volgt, blijkt dat bij voorliggend onderzoek de focus op het gebruik van gerichte gezichtsherkenning met het oog op de (reactieve) identificatie van slachtoffers en daders ligt. Er wordt gezocht naar een specifieke persoon of personen (dader of slachtoffer) in een (on)bepaalde aantal personen (1:N).

5. ONDERZOEKSBEVINDINGEN

5.1. De *Clearview* applicatie

11. Het bedrijf *Clearview* is naar eigen zeggen alleen toegankelijk voor *Law enforcement agencies*. Het bedrijf stelt haar product voor als *"a revolutionary, web-based intelligence platform for law enforcement to use as a tool to help generate high-quality investigative leads. Our platform, powered by facial recognition technology, includes the largest known database of 10+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources"*[31]. *Clearview* beheert, optimaliseert en exploiteert dus een gigantische gegevensbank met gezichtsafbeeldingen (foto's en beelden) van personen die op het internet, sociale media en persmedia in het bijzonder, publiek toegankelijk zijn en stelt deze commercieel ter beschikking van politiediensten.

12. Het bedrijf biedt een zogenaamde *trial* versie (gratis proefperiode) aan voor 30 dagen, zodat de gebruiker vertrouwd geraakt met de verwerking van de *Clearview* toepassing. Na deze *trial* is het gebruik van de *Clearview* toepassing betalend. De website van *Clearview* bevat een link met als benaming '*request trial*'. Wanneer de potentiële gebruiker die link aanklikt, verschijnt een scherm waarop duidelijk wordt vermeld dat deze toepassing alleen toegankelijk is voor politiediensten (*Law enforcement personnel*[32]) en dat de waarachtigheid ervan moet blijken op basis van een validatie door de verantwoordelijke leidinggevende van de gebruiker van het *Clearview* account. Nadat het registratieproces is voltooid, krijgt de gebruiker een link toegestuurd om zijn of haar *Cleaview*-account te activeren. Wanneer de gebruiker met zijn *Clearview* account inlogt, krijgt hij een link (URL[33]) toegestuurd waarop de gebruiker een foto kan opladen. Eén foto mag meerdere afbeeldingen van personen bevatten. In dat laatste geval zal de applicatie automatisch iedere foto afzonderlijk selecteren en vervolgens vergelijken met de gegevensbank van *Clearview*. Wanneer de vergelijking een positief resultaat oplevert, krijgt de gebruiker een link (URL) van de bron waar *Clearview* de foto's heeft verzameld (een website, Facebook, enz.) of '*gescrapted*'.

Stapsgewijs kan het gebruik van de *Clearview* applicatie derhalve als volgt worden geduid:

1) de gebruiker laadt een foto of een beeld (met één of meerdere personen) op;
2) het systeem zoekt, zonder tussenkomst van de gebruiker, in de *Clearview* gegevensbank naar overeenstemmende afbeeldingen (gezichten);
3) als het systeem een zogenaamde *match* en/of gelijkaardig gezicht (*similar*) vindt, krijgt de betrokkene daarvan het resultaat te zien;
4) in geval van een *match* en *similar* wordt tevens de link zichtbaar waar de foto beschikbaar is (bijvoorbeeld op Facebook of Instagram, digitale pers, enz. …);
5) tot slot kan de link waar de foto (of foto's) zich bevindt (bevinden) worden geopend, die op zijn beurt naar een andere digitale bron of bronnen kan (kunnen) verwijzen (waar mogelijk opnieuw (andere) foto's beschikbaar zijn).

---

[30] Nog een andere mogelijkheid betreft de interne gezichtsherkenning. Bij interne (besloten) gezichtsherkenning werkt het systeem niet vanop afstand en niet *real time*. De gezichtsherkenningstechnologie wordt door de politie toegepast op foto's en beelden die reeds in gegevensbanken zijn opgeslagen en met elkaar worden vergeleken. Te denken valt aan de politionele camerabeelden die worden opgeslagen onder de toepassing van het algemeen cameragebruik en/of de foto's in een operationele gegevensbank. Het betreft ook hier een gerichte onderzoekshandeling, maar waarbij de gezichtsherkenning op bestaande interne politiegegevens worden toegepast. Het betreft de geautomatiseerde onderlinge vergelijking van foto's en beelden die in politionele gegevensbanken zijn opgeslagen met het oog op een correcte identificatie of verificatie van de verdachte en/of veroordeelde persoon. Dit gebeurt vooral vanuit praktisch en organisatorisch oogpunt: een manuele vergelijking ('hit') een onredelijke inzet van mankracht en tegelijkertijd veel tijd zou in beslag nemen. In dat scenario kan de vergelijking worden opgezet met het oog op identificatie (dader van een ander misdrijf) of de verificatie (het gaat om dezelfde persoon?).

[31] https://www.clearview.ai.

[32] Wat overigens in de Amerikaanse context ruimer is dan politiediensten in de zin van de Belgische wetgeving.

[33] *Uniform Resource Locator*. Dit is het adres van, *in casu*, de gegevensbank van *Clearview.*

De *Clearview* applicatie is zeer gebruiksvriendelijk. Het vraagt weinig moeite om de *Clearview* toepassing op gelijk welke computer of *device* te gebruiken.

Ondertussen weten we dat *Clearview* onder vuur ligt van meerdere nationale toezichthoudende autoriteiten[34] over de hele wereld, waarbij de Franse collega van de *CNIL*[35] op 21 december 2021 bijvoorbeeld een bevel hebben gegeven aan *Clearview* om alle *scraping* activiteiten op het Franse grondgebied stop zetten[36] wegens meerdere inbreuken op de AVG. De CNIL beslissing bevat overigens een goede beschrijving van de door Clearview gebruikte techniek en technologie.

5.2. Het gebruik van de *Clearview* applicatie door de federale gerechtelijke politie

13. Uit het door het COC gevoerde onderzoek blijkt dat de *Clearview* gezichtsherkenningstechnologie door de federale gerechtelijke politie werd gebruikt, en dit voor het eerst tijdens de *taskforce* bij Europol te Den Haag, die plaatsvond van 14 tot en met 25 oktober 2019[37]. Deze *taskforce* vond plaats in het raam van een internationaal gecoördineerd dossier, met name het *Nationaal Center of Missing and Exploited Children* (NCMEC)"[38]. Het NCMEC betreft in wezen een Amerikaanse rechtshandhavingsdienst waarin de *Federal Bureau of Investigation* (FBI) participeert[39]. Ook de Belgische federale gerechtelijke politie participeert in NCMEC-dossiers[40]. NCMEC verzamelt (en ontvangt ook van internetdiensten, zoals sociale media) foto's en beelden van potentiële daders en slachtoffers van seksueel geweld op minderjarigen (kinderporno). Het betreft potentiële daders en slachtoffers die nog niet gelokaliseerd zijn (identiteit en verblijfplaats of tijd/ruimte).

14. Tijdens deze *taskforce* werden de mogelijkheden van de *Clearview* gezichtsherkenning voor de deelnemende politiediensten van 24 landen gedemonstreerd en toegepast op NCMEC-gegevens. Blijkens de bevindingen was het in dat verband dat een aanwezig lid van de federale gerechtelijke politie in oktober 2019 tijdens de *taskforce* de gezichtsherkenningstechnologie voor het eerst heeft gebruikt. Het blijkt tevens dat door de federale gerechtelijke politie de *Clearview* gezichtsherkenningstechnologie ook na afloop van de *taskforce* bij Europol op foto's en beelden in het raam van onderzoeken naar potentieel seksueel misbruik van minderjarigen heeft gebruikt[41]. De laatste activiteit met de gezichtsherkenningstechnologie zou volgens *Clearview*, zoals gezegd, op 10 februari 2020 hebben plaatsgevonden. Daarna werden de accounts op initiatief van *Clearview* afgesloten[42].

15. De *Clearview* gezichtsherkenning werd gebruikt met het oog op het vaststellen van de identiteit (en mogelijk de verblijfplaats) van daders van seksueel misbruik van minderjarigen (kinderporno) in het raam van NCMEC-dossiers om vervolgens een opsporingsdossier te kunnen opstarten[43]. Uit het onderzoek blijkt dat de federale gerechtelijke politie in totaal 78 opzoekingen in de gegevensbank van *Clearview* zou hebben uitgevoerd[44], en dus effectief de *Clearview* gezichtsherkenning heeft gebruikt. Het gebruik van de *Clearview* applicatie door de federale gerechtelijke politie zou tijdens zowel de *taskforce* bij Europol als, na afloop van de *tasforce*, bij onderzoeken in België geen opsporingsmatig positief resultaat hebben opgeleverd[45]. Hoewel de foto's en de beelden in dit stadium niet noodzakelijk deel uit maakten van een 'Belgische' strafonderzoek, zijn deze foto's en beelden wel te beschouwen als politionele persoonsgegevens in de zin van titel 2 WGB en de WPA[46].

Uit het voorgaande rijzen bijgevolg twee onderzoeksvragen:

---

[34] Zie o.a. Audibert, L, « Les technologies de reconnaissance faciale menacent la notion de vie privée en ligne et hors ligne », Le monde, 6 januari 2022, https://journal.lemonde.fr/data/1838/reader/reader.html?xtor=EPR-32..

[35] Commission Nationale de l'Informatique et des Libertés, www.cnil.fr

[36] www.cnil.fr, *Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI (cnil.fr)*

[37] Brief van de commissaris-generaal van de federale politie van 18 oktober 2021 en bevestigd op basis van een interview met een lid van de federale gerechtelijke politie.

[38] Brief van de commissaris-generaal van de federale politie van 18 oktober 2021, p. 1.

[39] Ibid, p. 3.

[40] Brief van de commissaris-generaal van de federale politie van 18 oktober 2021, p. 1.

[41] Dat blijkt uit het antwoord van *Clearview* waarin wordt gesteld dat de toepassing nog op 10 februari 2020 werd gebruikt. Dit wordt bevestigd door DGJ (e-mail van 19 september 2021). Het is hierbij van belang om voor ogen te houden dat het COC de waarachtigheid van de informatieverstrekking door *Clearview* niet heeft onderzocht en dat in wezen ook niet kan doen omdat dit bedrijf niet onder de bevoegdheid van het COC valt.

[42] Ibid. Omdat de proeftijd was verlopen.

[43] Het gaat voor alle duidelijkheid om het vaststellen van de identiteit van personen van wie de identiteit nog niet door federale gerechtelijke politie gekend was. Indien dat wel het geval was geweest, dan zou de gezichtsherkenning eerder gebruikt geweest zijn met het oog op verificatie van de identiteit ('is dit dezelfde persoon als deze die bij de politie – voor dergelijk misdrijf - gekend is?').

[44] E-mail *Clearview AI* van 16 september 2021. De *Cleraview* applicatie werd door de gebruikers eerst getest op hun persoonlijke foto's en die van kennissen/collega's om de doeltreffendheid van de gezichtsherkenningstechnologie te testen.

[45] Brief van de commissaris-generaal van de federale politie van 18 oktober 2021, p 3 en bevestigd door DGJ (e-mail 19 september 2021). Het COC kon de waarachtigheid van deze bewering niet nagaan. Zoals in de vorige voetnoot wordt vermeld, is daarvoor de medewerking van *Clearview* essentieel.

[46] Art. 26, 1° en 2° WGB en 44/1 § 1 WPA.

1) was het commissariaat-generaal van de federale politie in het algemeen en de algemene directie van de federale gerechtelijke politie (DGJ) in het bijzonder, op de hoogte of hadden zij dat moeten zijn van het gebruik van de *Clearview* gezichtsherkenningstechnologie door leden van de federale (gerechtelijke) politie, met nam de directie DJSOC?
2) is (en was) het gebruik van de *Clearview* gezichtsherkenning in overeenstemming met het wettelijk kader? Op deze vraag wordt in punt 5.4 een antwoord verstrekt.

5.3. Toestemming voor en kennis van het gebruik van de gezichtsherkenningstechnologie

16. Uit het onderzoek en het syntheserapport van het lid van de federale gerechtelijke politie die deelnam aan de *taskforce* bij Europol (van 14 oktober 2019 tot 25 oktober 2019) blijkt dat de centrale directie van de bestrijding van de zware en georganiseerde criminaliteit (DJSOC) onmiddellijk na afloop van de *taskforce* mondeling en **minstens op 7 november 2019** formeel schriftelijk op de hoogte was van het gebruik van de *Clearview* applicatie[47]. Dit betekent dat de hiërarchie van de federale gerechtelijke politie onmiddellijk na de taskforce bij Europol en dus voor dossiers waarin door leden van de federale gerechtelijke politie werd gewerkt op de hoogte was van het gebruik van de *Clearview* gezichtsherkenningstechnologie en dit ook heeft toegestaan. Dit laatste blijkt ook uit de vaststelling dat het betalend gebruik van de *Clearview* applicatie door de federale gerechtelijke politie nadien werd onderzocht maar uiteindelijk niet werd uitgevoerd.

17. Het is dan ook opmerkelijk dat de commissaris-generaal in zijn brief van 19 mei 2020 aan het COC antwoordt, dat "*Op basis van de thans beschikbare informatie er binnen de Federale Politie op organisatieniveau geen kennis (is) over het gebruik van gezichtsherkenningssoftware binnen de politiediensten. Er zijn op dit moment ook geen intenties om dit soort software te gaan inzetten aangezien er een meer soliede wettelijke basis vereist is om deze technologie aan te kunnen wenden*"[48]. Pas na aandringen van het kabinet van de commissaris-generaal bij een tweede interne bevraging (als gevolg van de hernieuwde vraag van het COC van 27 augustus 2021 op zijn beurt het gevolg van persberichten) - gebaseerd op de bevestiging van *Clearview* op 16 september 2021 van het gebruik van de gezichtsherkenning door leden van de federale politie - aan de algemene directie van de federale gerechtelijke politie (DGJ) volgt op 19 september 2021 de formele bevestiging door DGJ dat de *Clearview* applicatie inderdaad werd ingezet door leden van de federale gerechtelijke politie in (enkele) NCMEC-dossiers.

18. Uit de elementen van het voorliggend onderzoek blijkt dus duidelijk dat het antwoord van de commissaris-generaal aan het Controleorgaan van 19 mei 2020 **niet** met de werkelijkheid overeenstemde aangezien de federale gerechtelijke politie minstens reeds op 7 november 2019 wel degelijk op de hoogte was van het gebruik van de *Clearwiew* applicatie door leden van DJSOC, het gebruik ervan toestond en er naderhand een met kennis van zaken genomen beslissing is gevallen om geen licenties van de applicatie aan te kopen.

Onafgezien van het wettelijk onrechtmatig gebruik van de *Clearview FRT* (cf. punt 5.4 infra) door één of meer (overigens zeer gedreven) individuele onderzoekers van DJSOC, tilt het Controleorgaan nog het zwaarst aan de niet mededeling door (de hiërarchie van) de algemene directie gerechtelijke politie van het gebruik van *Clearview*, kennelijk niet enkel ten aanzien van het COC, maar ook ten aanzien van de commissaris-generaal. Het hoeft weinig betoog dat deze vaststelling op gespannen voet staat met de medewerkingsplicht die wettelijk wordt opgelegd aan de onder toezicht staande politiediensten[49] en in het algemeen nefast is voor het toezicht dat er moet kunnen op vertrouwen dat de antwoorden van de GPI conform de realiteit zijn. De commissaris-generaal stelt in het kader van de tegenspraak geen moedwillige verzwijging te zien vanuit DGJ maar eerder een samenloop van omstandigheden die hebben gemaakt dat de informatie-uitwisseling niet verlopen is zoals gewenst. Het COC neemt hiervan akte.

Gelet op de gevoeligheid van de materie, de (terechte) vaststelling van de commissaris-generaal dat het publiek en de beleidsmakers én uiteraard de toezichthouder meer en meer belang hechten aan de wettelijkheid en de proportionaliteit van politionele gegevensverwerkingen[50]moet ervan uitgegaan worden dat de *awareness* bij de GPI thans van die aard is dat dit soort van miscommunicatie tot het verleden behoort.

Het behoort verder niet tot de taakstelling van het COC om de interne communicatiekanalen van de federale politie nader en in detail te onderzoeken, laat staan op zoek te gaan naar individuele verantwoordelijken voor één en ander.

5.4. Het ontbreken van een wettelijke basis

[47] Syntheserapport van de buitenlandse zending met betrekking tot *taskforce Victim Identification seksueel misbruik van minderjarigen* (gedateerd via verzendingsmail op 7 november 2019 van het deelnemend lid van de DJSOC).
[48] Zoals hiervoor in rubriek 2 wordt vermeld.
[49] Cf. art. 57 WGB: "*De verwerkingsverantwoordelijke en de verwerker werken op verzoek van de bevoegde toezichthoudende autoriteit met deze laatste samen bij het vervullen van haar opdrachten*". Een en ander is overigens strafbaar als belemmering van toezicht conform art. 222, 7° WGB.
[50] Zie ook de tijdelijke nota van 28.01.2022 CG/2022-16 "*Herinnering aan de richtlijnen inzake de verwerking van persoonsgegevens*" gericht aan alle eenheden van de federale politie.

19. Uit het voorgaande blijkt ontegensprekelijk dat de federale gerechtelijke politie de *Clearview* gezichtsherkenningstechnologie daadwerkelijk op politionele persoonsgegevens (foto's en beelden) heeft toegepast. Dat de foto's die daarbij werden gebruikt geen betrekking zouden[51] hebben gehad op 'Belgische dossiers' doet daar niets aan af. Daarbij is de nationaliteit van de betrokkenen noch de vraag of het gaat om personen die al dan niet deel uitmaken van een 'Belgisch' opsporingsdossier relevant. Het COC benadrukt dat deze verwerking van persoonsgegevens onder de verantwoordelijkheid van een Belgische politiedienst valt. Op de persoonsgegevens die door de Belgische politiediensten worden verwerkt, is het juridisch kader van de Europese Unie betreffende de bescherming van de persoonsgegevens (omgezet in titel 2 WGB) en de bepalingen van het informatiebeheer van de WPA onverkort van toepassing.

20. Dit betekent dat de federale gerechtelijke politie daarenboven politonele gegevens aan een (buitenlandse) derde private onderneming (dus geen politiedienst of overheid) heeft medegedeeld. Zoals hierna zal worden toegelicht, vindt deze mededeling van politionele gegevens geen enkele steun in de WPA en is ze derhalve onwettig. Het COC stelt vast dat de federale politie in het raam van de tegenspraak hierover geen opmerkingen noch voorbehoud heeft gemaakt en zich derhalve aansluit bij de beoordeling van het COC.

21. Samen met de minister van Binnenlandse Zaken[52]moet vastgesteld worden dat het gebruik van de gezichtsherkenningstechnologie niet (concreet) in de wet op het Politieambt (WPA) wordt geregeld. Dat is evenmin het geval voor de doorgifte van politionele gegevens aan een derde private actor als *Clearview*.

Artikel 44/1, § 2, 1° WPA bevat op zeer algemene wijze een wettelijke basis voor de verwerking van 'biometrische gegevens' met het oog op de ondubbelzinnige identificatie van onder meer verdachten van een strafbaar feit en vermiste personen. Merk, bijvoorbeeld, op dat in het raam van de NCMEC-dossiers kinderen het slachtoffer zijn. Welnu, om hun biometrische gegevens te gebruiken vereist de wet – zolang er geen Belgisch strafdossier (of eventueel een buitenlands onderzoek waarop de regels inzake rechtshulp van toepassing zijn) is geopend, wat *in casu* steeds het geval bleek - strikt genomen dat daarvoor de toestemming, *in casu* van de ouders of voogd, moet worden verkregen. Het is dan ook zeer twijfelachtig, om niet te zeggen onbestaande, dat de wetgever bij het invoegen van de verwerkingsbevoegdheid voor biometrische gegevens in 2019 ook heeft rekening gehouden met de verwerking ervan in het raam van seksueel misbruik van kinderen zoals zich dat *in casu* in het kader van de Europol taskforce voordoet.

Bovendien is het begrip biometrische gegevens ruimer dan gezichtsherkenning waarbij de verwerking ervan, naar gelang de omstandigheden van de verwerking en de technologie die wordt gebruikt, een bijzonder (hoog) risico vormt voor de bescherming van de fundamentele rechten en vrijheden. In het licht van de kwaliteit van de wettelijke basis die door de (Europese) rechtspraak aan de verwerking van biometrische gegevens door rechtshandhavingsautoriteiten wordt gesteld, wordt een specifieke en duidelijke wettelijke basis vereist waarbij de omstandigheden en voorwaarden voor het gebruik ervan in een rechtsnorm worden vastgelegd en met specifieke en adequate (veiligheids)waarborgen worden omringd[53]. In dat verband werd door het COC al eerder gewezen op het ontbreken van een specifieke wettelijke basis voor het gebruik van gezichtsherkenningstechnologie door de luchthavenpolitie van Zaventem[54]waarbij het COC corrigerend heeft moeten optreden.

In het raam van de tegenspraak wordt het COC door de commissaris-generaal van de federale politie gevraagd een standpunt in te nemen aangaande de conformiteit met de huidige WPA voor het gebruik van gezichtsherkenning op bestaande interne politiegegevens. Het COC benadrukt dat de federale politie daarbij verwijst naar de voetnoten 27 en 30 uit het ontwerprapport op tegenspraak, die in het onderhavig definitief rapport ongewijzigd zijn gebleven. Het verzoek tot standpuntinname betreft dus, voor alle duidelijkheid, **niet** de gerichte opzoeking zoals dat wel het geval was met het gebruik van de *Clearview* applicatie door de DJSOC, maar wel het toepassen van gezichtsherkenningstechnologie op interne bestaande politiegegevens (vergelijking van foto's die in politiegegevensbanken zijn opgenomen). Er moet worden benadrukt dat deze vraag *hic et nunc* en in dit rapport buiten beschouwing moet worden gelaten nu het gebruik van gezichtsherkenning die door de federale politie in haar reactie van 28 januari 2022 wordt bedoeld totaal verschillend is van het gebruik van *Clearview* en alleen deze laatste het voorwerp uitmaakt van het toezichtonderzoek en het onderhavig definitief rapport. Bovendien, en louter

[51] "*zouden*" omdat het niet meer te achterhalen is op welke foto's of beelden (laat staan op welke "dossiers") de applicatie werd gebruikt door de leden DJSOC.

[52] Parl. St. Kamer 2020-2021, Commissie voor de binnenlandse zaken, veiligheid, migratie en bestuurszaken, 6 oktober 2021, CRIV 55 COM 597, p. 4.

[53] Niet alleen op juridisch vlak, maar ook op het vlak van betrouwbaarheid (objectiviteit, homologatie, …) en transparantie van de technische aspecten van deze technologie. Het gebruik van deze technologie (verwerkings- en beslissingsprocessen) is immers *in se* op zichzelf niet performant.

[54] Tussentijds rapport met corrigerende maatregel betreffende de visitatie bij de federale politie van de luchthaven Zaventem door het Controleorgaan op de politionele informatie met betrekking tot het gebruik van gezichtsherkenning op de nationale luchthaven van Zaventem (DIO19005), https://www.controleorgaan.be/publicaties/rapporten.

volledigheidshalve, zijn de door het COC in het rapport gestelde situaties waarvoor de politie gezichtsherkenning zou kunnen gebruiken louter hypothetisch gesteld en, ten overvloede, in zoverre dit gebruik duidelijk en nauwkeurig in de WPA zou worden geregeld, wat actueel niet het geval is. Zoals hiervoor opgemerkt, wordt het begrip 'biometrische gegevens' zeer ruim opgevat (zoals vingerafdrukken, gezichts- gedragskenmerken, de iris van het oog, oorafdruk, de stem, emoties …) waarbij de zeer specifieke aard van de gegevens en de (achterliggende) verwerkingsprossen erg verschillend zijn mede in functie van de specifieke artificiële intelligentie die daarbij wordt gebruikt én (de mate van) het risico voor de fundamentele rechten en vrijheden van de persoon waardoor een specifiek en nauwkeurig, met waarborgen omringd, wettelijk kader noodzakelijk is. Dat is er actueel niet.

Voor het overige verwijst het COC naar het advies DA210029 van 24 januari 2022 betreffende een voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en – algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen (DOC 55 1349/001 van 16 juni 2020)[55] waarin het uitgebreid ingaat op de wetgevend kader de *lege lata* en de *lege ferenda*.

22. Er moet, voor de volledigheid, ook voor ogen worden gehouden dat het gebruik van de *Clearview* applicatie op bepaalde (essentiële) punten afwijkt van het gebruik van gezichtsherkenningstechnologie door de luchthavenpolitie van Zaventem.

In de eerste plaats wordt de *Clearview* gezichtsherkenning *in casu* niet toegepast op camerabeelden van publieke plaatsen. Er worden foto's of beeldmateriaal gebruikt waarover de politie reeds beschikt in het kader van de NCMEC-dossiers. Er is sprake van een gericht gebruik van de gezichtsherkenning. In de tweede plaats werd door de federale gerechtelijke politie voor het gebruik van gezichtsherkenningstechnologie een beroep gedaan op een derde, *in casu*, een privaat en commercieel (Amerikaans) bedrijf. De politie zendt de politionele foto's (persoonsgegevens), via een URL van *Clearview*, immers door aan of stelt deze minstens beschikbaar voor *Clearview*, die als een 'derde' te beschouwen is in het licht van de titel 2 WGB, waardoor in wezen een overdracht (*transfer*) plaatsvindt van, of minstens toegang wordt verleend tot, politionele informatie en persoonsgegevens (foto's van personen)[56]. Daardoor worden **politionele persoonsgegevens doorgegeven aan een ontvanger in een derde land zonder dat duidelijk is of deze een passend beschermingsniveau waarborgt dan wel passende waarborgen heeft**[57]. Ook de Finse Ombudsman Gegevensbescherming komt tot dezelfde vaststelling wat betreft het experimenteel gebruik van de *Clearview* applicatie door de Finse politie[58]. Ten derde **worden in deze context door Belgische politiediensten politionele informatie en persoonsgegevens doorgegeven of minstens beschikbaar gesteld aan een derde private bestemmeling (onderneming die ook geen verwerker is)**, **wat niet in de WPA wordt geregeld, en dus niet is toegestaan (noch aan een Belgische of EU instelling of onderneming, laat staat aan een Amerikaanse onderneming)**. De niet-politionele bestemmelingen worden in de WPA immers strikt afgebakend[59]. Het COC stelt vast dat deze drie punten in het raam van de tegenspraak niet door de federale politie worden betwist noch wordt ter zake enig voorbehoud gemaakt.

23. Volledigheidshalve wordt herhaald en benadrukt dat het gebruik van de *Clearview* applicatie op personen (daders of slachtoffers) met een niet-Belgische nationaliteit **niets** afdoet aan het ontbreken van een afdoende wettelijke basis in de WPA. Wanneer de verwerking binnen de werkingssfeer van de Europese Unie valt, is de bescherming die door de *LED* (omgezet in titel 2 WGB en de WPA) wordt geboden van toepassing op natuurlijke personen, ongeacht hun nationaliteit of verblijfplaats[60]. Hieruit volgt dat, zelfs indien de *Clearview* gezichtsherkenning door de federale gerechtelijke politie werd toegepast op niet-Belgische burgers (wat niet geweten is) of burger met een nationaliteit van een andere lidstaat of een derde land, een wettelijke basis voor de toepassing van gezichtsherkenningstechnologie wordt vereist[61].

---

[55] Zie www.controleorgaan.be onder de rubriek publicaties/adviezen regelgeving.

[56] Vgl. *European Data Protection Board*, "*Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on the international transfers as per Chapter V on the GDPR*", Adopted on 18 November 2021, raadpleegbaar: edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-pratices_en.

[57] Artt. 66-70 WGB.

[58] Raadpleegbaar op: edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

[59] Art. 44/11/9 § 1 WPA. Op grond van de 2de paragraaf van hetzelfde artikel kunnen politiegegevens en informatie onder specifieke voorwaarden eveneens meegedeeld worden aan de **Belgische** openbare overheden, publieke organen of instellingen of instellingen van openbaar nut die door de wet belast zijn met de toepassing van de strafwet of die wettelijke verplichtingen inzake de openbare veiligheid hebben, wanneer deze ze nodig hebben voor de uitoefening van hun wettelijke opdrachten. Deze mogelijkheid wordt hier slechts ten overvloede vermeld aangezien *Clearview* niet alleen geen Belgische instelling is, maar ook geen overheid, publieke instelling of orgaan is, laat staan dat het bedrijf door de wet belast zou zijn met de toepassing van de strafwet.

[60] Art. 2 *LED* samen gelezen met Overwegingen 2 en 17 . Art. 2 AVG samen gelezen met overweging 2 AVG.

[61] In het antwoord van DGJ van 19 september 2021 wordt er op gewezen dat het gebruik van gezichtsherkenningstechnologie geen betrekking had op geen Belgische dossiers. Dat staat in contrast met de brief van de commissaris-generaal van 18 oktober 2021 waarin wordt gesteld dat "(…) *nous avons bien mentionné que des uitilations avaient eu lieu "a quelques reprises dan les dossiers du National Center for Missing and Exploited Shildren en Belgique*"" (onderlijning COC).

24. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke, *in casu* de federale gerechtelijke politie, om te onderzoeken of het experimenteel gebruik van deze gezichtsherkenningstechnologie wettelijk mogelijk was (is).

Het komt er dus *in concreto* op neer dat federale gerechtelijke politie zich *in globo* de volgende vragen had moeten stellen en ook beantwoorden:

1) Welke persoonsgegevens worden verwerkt?
2) Is de politie verwerkingsbevoegd?
3) Welke bewerking wordt er uitgevoerd (biometrische bewerking, doorgifte naar een derde land, …)?
4) Is deze verwerking juridisch toegelaten?
5) Waar worden de persoonsgegevens bewaard en voor welke termijn?
6) Worden de biometrische gegevens met passende waarborgen omringd?

Deze vragen en risico's hadden in een gegevensbeschermingseffectbeoordeling (*DPIA*[62]) geïdentificeerd en geremedieerd moeten worden.

Er werd aan het COC geen informatie verstrekt waaruit blijkt dat DJSOC dit onderzoek heeft uitgevoerd.

Er mag dus redelijkerwijze van uitgegaan worden dat ook deze verplichting opgelegd door de WGB door de federale gerechtelijke politie niet werd nageleefd, wat eveneens wordt bevestigd door de niet betwisting van deze vaststelling in het kader van de tegenspraak procedure.

6. BESCHOUWINGEN

25. Het gebruik van de *Clearview* gezichtsherkenningstechnologie door de Algemene directie gerechtelijke politie (*in concreto* door DJSOC) en de gezichtsherkenningstechnologie door de Algemene Directie Bestuurlijke Politie (in concreto door LPA Brussel-Nationaal) hebben gemeen dat beiden zich mede in een zogenaamde 'testfase' hebben afgespeeld. Maar ook in deze 'testfase' of m.a.w. wanneer de doelstelling van de persoonsgegevensverwerking louter of mede op het testen is gericht, moeten de WGB en de WPA worden nageleefd. De *lege ferenda* zijn er geen afwijkingen op het wettelijk kader voorzien zelfs wanneer het om een loutere testfase of proefproject zou gaan.

26. Het wezenlijk onderscheid tussen beide gevallen is wel gelegen in het achterliggend verwerkingsproces van de *Clearview* toepassing. In tegenstelling tot het gebruik van gezichtsherkenning door de Luchthavenpolitie te Zaventem, heeft de gebruiker van de *Clearview* toepassing geen enkele controle over de verwerking van de biometrische gegevens. De foto's en beelden worden immers via een URL opgeladen waardoor de beschikbaarheid over de foto's en beelden volledig wordt overgedragen aan het Amerikaanse *Clearview*. De foto's en de beelden, inclusief de biometrische verwerking (template die de unieke persoonsgegevens bevat) worden buiten de politionele omgeving (en buiten de EU rechtsorde) gestuurd en vervolgens verwerkt. **De politie-entiteit die de foto's en beelden verstrekt, heeft dus geen enkele vat (meer) op de verwerking van de biometrische gegevens, noch op het verder verwerkingsproces van en door de ontvanger.** Het is dus duidelijk, en daarmee hoogst problematisch, dat de politiedienst die de foto's en beelden verstrekt geen invloed heeft op, onder meer, de bewaartermijn van de foto's en beelden en het potentieel verder commercieel gebruik van deze politiegegevens door *Clearview*. Het is daarnaast onduidelijk of *Clearview*, naast de template (die unieke code van de biometrische kenmerken) ook de ruwe biometrische gegevens (de unieke gezichtskenmerken op basis waarvan de unieke code wordt gemaakt) heeft bewaard, laat staan of ze die verder commercieel (heeft) (ge)exploiteert(d). Tot slot staat vast dat het zo goed als onmogelijk is te weten voor de betrokkenen dat hun foto werd opgeladen in de *Clearview* applicatie en blijkt het bovendien evenzeer bijzonder moeilijk tot onmogelijk voor een betrokkene om zijn rechten t.a.v. *Clearview* uit te oefenen (zie o.a. onderzoek CNIL waarvan hoger sprake, cf. randnummer 12).

27. Uit het door het COC gevoerde onderzoek kan tevens afgeleid worden dat de federale gerechtelijke politie het gebruik van de *Clearview* gezichtsherkenning niet (noodzakelijk) als een onderzoeks- of opsporingshandeling beschouwt, waardoor aan de legitieme verwachting dat ook aan de registratieverplichtingen voor verwerking van politionele informatie en persoonsgegevens uit hoofde van de WPA en de MFO3[63] moet worden voldaan, niet kan worden tegemoet gekomen. De verwerkingen spelen zich kennelijk af in de fase vóórafgaand aan de opstart van een (Belgisch) opsporingsonderzoek of gerechtelijk onderzoek en blijven (eventueel zelfs uitsluitend) 'hangen' op politioneel niveau. Daardoor kon het COC ook niet objectief en/of materieel nagaan of het gebruik van de gezichtsherkenning effectief een negatief dan wel positief opsporingsresultaat heeft opgeleverd (het Controleorgaan kan hier enkel maar

[62] *Data Protection Impact Assessment*.
[63] Gemeenschappelijke richtlijn MFO-3 van 14 juni 2002 van de Ministers van Justitie en van Binnenlandse Zaken "*betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie*".

steunen op de beweringen van de twee verhoorde onderzoekers). Nergens blijken er vattingen (en/of loggingen) te gebeuren in de bestaande politionele gegevensbanken van deze verwerkingen van persoonsgegevens.

De applicatie wordt dus eerder als een vorm van 'internet zoekmotor' aanzien. Door de betrokken rechercheurs werd er *in casu* vanuit gegaan dat wie zich in de publiek toegankelijk digitale wereld begeeft zich wetens en willens 'blootstelt' aan controle van en door de politie naar analogie met personen die zich in de reële wereld op publieke plaatsen bevinden. Deze perceptie van (sommige) leden van de federale gerechtelijke politie is mede gebaseerd op de veronderstelling dat wat in de digitale wereld publiek toegankelijk is, ook daadwerkelijk voor de politie beschikbaar is en door deze kan gebruikt worden (*open source intelligence*). Daarbij is *Clearview* in die visie slechts een middel dat de toegang tot deze publiek toegankelijke foto's makkelijker maakt. Deze zienswijze is allerminst evident en staat alleszins op gespannen voet met het vigerende gegevensbeschermingskader.

Het gebruik van de *Clearview* gezichtsherkenning door de federale gerechtelijke politie is onmiskenbaar als een politionele onderzoeks- of opsporingshandeling te beschouwen (en dat is trouwens ook de enige doelstelling) waardoor, zoals hiervoor opgemerkt, de verplichtingen voortvloeiende uit de bepalingen van de WPA en de MFO3 onverminderd van toepassing blijven waardoor deze verwerkingen ook traceerbaar worden of moeten zijn, hetgeen *in casu* niet het geval is.

28. Vóór dat deze gezichtsherkenningstechnologie door de federale gerechtelijke politie werd gebruikt, werd vrij 'geëxperimenteerd' met persoonlijke foto's van deelnemende politieambtenaren. Dat was ook het geval bij het gebruik van foto's van slachtoffers en daders uit NCMEC-dossiers. Daarbij waren de leden van de DJSOC zich kennelijk van geen kwaad of probleem bewust, temeer daar de hiërarchie geen bezwaar heeft gemaakt tegen het gebruik van de gezichtsherkenningstechnologie. Opmerkelijk en tegelijk interpellerend is dat DJSOC of DGJ, en de hiërarchie in het bijzonder, daarbij geen oog lijkt te hebben gehad voor de impact en de gevolgen van het verwerkingsproces van de *Clearview* applicatie. Minstens lijken ze de draagwijdte van de *Clearview* applicatie niet of onvoldoende procesmatig en juridisch te begrijpen dan wel met kennis van zaken te kunnen inschatten.

De federale gerechtelijke politie lijkt niet te beseffen dat daardoor niet alleen politionele foto's aan een commercieel bedrijf worden doorgestuurd (en dan nog buiten de Europese Unie) noch dat de biometrische gegevens, *in casu* gezichtskenmerken, sindsdien door het bedrijf *Clearview* bijgehouden worden[64].

Er werd en wordt kennelijk niet stilgestaan bij het gegeven dat de verwerking van deze foto's en beelden (en biometrische gegevens) het *business model* van dit bedrijf vormt. Het optimaliseren van de *Clearview* gegevensbank is de kernactiviteit waarop hun winstmodel, en dus voortbestaan, steunt. Het is natuurlijk niet zonder reden dat *Clearview* in het mailverkeer met de gebruikers van de *Clearview* account deze oproept om zoveel mogelijk opzoekingen te verrichten (en dus foto's en beelden met *Clearview* te delen).

29. Het is een misvatting te denken dat alleen foto's van daders en/of verdachten worden bijgehouden. Het betreft logischerwijze foto's die deel uitmaken van politionele dossiers. Niet alleen foto's van daders, maar ook van slachtoffers (en zelfs getuigen of omstaanders) komen zo in handen van een bedrijf die zijn bestaan en winst genereert en optimaliseert op basis van zeer gevoelige informatie en persoonsgegevens, waaronder zeer kwetsbare personen. De gebruiker van de *Clearview* applicatie heeft geen enkele controle over deze verwerking.

In het raam van de tegenspraak worden door federale politie omstandigheden ingeroepen[65]die betrekking hebben op het zeer beperkt en tijdelijk gebruik van Cleaview door DGJ, enerzijds, en de zware werklast van deze algemene directie, anderzijds. Hoewel het COC begrijpt dat de politiedienst de *Clearview* applicatie louter resultaatgericht heeft gebruikt, doet dit evenwel niets af aan de vaststelling van het COC dat politiegegevens (foto's van daders, slachtoffers en derden) in handen van een privaat Amerikaans bedrijf zijn gekomen. Dat dit kennelijk niet is doorgedrongen bij DGJ is een belangrijk aandachts – en werkpunt en daarmee heeft de ingeroepen zware werklast op zich weinig van doen.

[64] Er moet worden opgemerkt dat aan het Controleorgaan niet het bewijs werd overlegd waaruit de validatie voor het aanmaken van een account bij *Clearview* door de politieambtenaren (laat staan door de leidinggevende van de politie) blijkt. Het is niet uitgesloten dat in de praktijk bij *Clearview* geen sprake is van een daadwerkelijk validatieproces bij het aanmaken van een account. Het hebben van een e-mailadres met de domeinnaam '@police.belgium.eu' lijkt op zich immers reeds afdoende te zijn opdat *Clearview* de gebruiker als een personeelslid van een Belgische politiedienst beschouwt en bijgevolg toegang verleent tot hun gegevensbank. Deze werkwijze is natuurlijk zeer problematisch aangezien ook niet-operationeel politiepersoneel en zelfs personen die helemaal geen deel uit maken van een politiedienst over een account @police.belgium.eu kunnen beschikken (vb. bepaalde externe consultants).

[65] De federale politie verwijst onder meer naar het randnummer 27 van het ontwerprapport op tegenspraak dat op het vlak van nummering ongewijzigd is gebleven in het onderhavig definitief rapport. Bijgevolg gaat het COC er vanuit dat de door de commissaris-generaal aangevoerde omstandigheden ook voor dit randnummer wordt ingeroepen.

7. CONCLUSIE

29. Uit het onderzoek van het Controleorgaan blijkt dat leden van de federale gerechtelijke politie geëxperimenteerd hebben met de gezichtsherkenningstechnologie van het Amerikaans bedrijf *Clearview*. Daarbij werden foto's van slachtoffers en daders in het raam van een onderzoek naar kinderporno gebruikt.

Ook het experimenteren met gezichtsherkenningstechnologie waarbij foto's van slachtoffers en verdachten worden gebruikt betreft een verwerking van persoonsgegevens waarop de WGB en de WPA van toepassing is.

De toepassing van gezichtsherkenningstechnologie betreft een specifieke verwerking van biometrische persoonsgegevens van het gezicht van de persoon waarbij unieke gezichtskenmerken van de persoon worden vastgelegd. De toepassing van gezichtsherkenningstechnologie betreft een zeer ernstige inmenging op de eerbiediging van de persoonlijke levenssfeer en de bescherming van de persoonsgegevens.

Hoewel de Wet op het Politieambt de verwerking van biometrische gegevens in het algemeen voorziet[66], bevat deze geen afdoende wettelijke basis om deze vorm van gezichtsherkenningstechnologie toe te passen. Dat wordt ten overvloede tevens bevestigd door de minister van Binnenlandse Zaken en door de federale politie zelf.

De hiërarchie van de federale (gerechtelijke) politie was op de hoogte van het experimenteel gebruik van de *Clearvieuw* gezichtsherkenningstechnologie terwijl binnen DGJ het gebruik ervan niet of onvoldoende tijdig aan banden werd gelegd.

De federale gerechtelijke politie heeft deze gezichtsherkenningstechnologie voor een korte periode gebruikt, maar zonder de kennis te verwerven over de impact en gevolgen van het verwerkingsproces op de politionele persoonsgegevens.

Door het gebruik van de *Clearview* applicatie vond een doorgifte (overdracht) van politionele informatie en persoonsgegevens (foto's) naar een niet politionele overheid in de zin van de WGB plaats. Bovendien betreft het een overdracht van politionele gegevens naar een ontvanger in een derde land, zonder dat door de federale gerechtelijke politie werd onderzocht of de ontvanger over een passend beschermingsniveau beschikt en handhaaft zoals vereist in de WGB[67]. Deze vaststelling wordt in het raam van de tegenspraak door de federale politie niet betwist.

De doorgifte van politionele informatie en persoonsgegevens (foto's uit NCMEC) naar een privaat bedrijf, laat staan een onderneming buiten de Europese Unie, is niet geregeld in de WPA, bijgevolg onwettig en een onrechtmatige gegevensverwerking. Deze vaststelling wordt evenmin in het raam van de tegenspraak door de federale politie betwist.

8. AANBEVELINGEN EN CORRIGERENDE MAATREGELEN

29. In het licht van het voorgaande brengt het COC drie (3) aanbevelingen uit en neemt het twee (2) corrigerende maatregelen.

30. Het komt voor het overige aan de federale politie zelf of haar voogdijoverheid toe de nodige lessen te trekken uit zowel dit onderzoek, als het in 2019 gevoerde onderzoek naar het gebruik van gezichtsherkenningstechnologie door LPA Brussel-Nationaal.

OM DEZE REDENEN,

Het Controleorgaan;

<u>Aanbeveling 1</u>

1) beveelt aan dat wordt ingezet op het organiseren van opleidingen en het stimuleren van *awareness* bij de personeelsleden (en leidinggevenden) bij het gebruik van *open source intelligence* in functie van de toepassing het vigerende juridisch kader in het algemeen en het gegevensbeschermingsrecht in het bijzonder;

[66] De commissaris-generaal verwijst ter zake terecht naar de artikelen 34 WGB juncto de artikelen 44/1 §2, 2e lid, 1° en §2, 3e lid WPA.

[67] Waarbij voor de volledigheid wordt opgemerkt dat de doorgifte ook geen uitzonderlijke omstandigheid betreft zoals voorzien in artikelen 69 of 70 WGB. Bovendien had DJSOC, in de hypothese dat de doorgifte wel gebaseerd zou kunnen worden op de bepalingen van 69-70 (doorgifte naar derde landen in uitzonderlijke gevallen naar een niet-bevoegde overheid) WGB – quod non, het in artikel 70 geregeld onderzoek moeten uitvoeren, documenteren en aan het COC ter beschikking stellen, wat helemaal niet is gebeurd.

Aanbeveling 2

2) beveelt aan dat de verwerking van politionele informatie en persoonsgegevens met het oog op het (uit)testen, in een experimentele fase, in de WGB of de WPA wordt geregeld en een helder juridisch kader krijgt;

Aanbeveling 3

3) dringt er op aan dat, wanneer het gebruik van gezichtsherkenningstechnologie in de WGB/WPA zou worden vastgelegd – al dan niet na een periode van moratorium[68]en al dan niet enkel in een testkader -, minstens de volgende aspecten worden behandeld:
- de bijzondere omstandigheden waarin de gezichtsherkenning kan gebruikt worden;
- naar gelang van het doeleinde van bestuurlijke of gerechtelijke politie, de tussenkomst van respectievelijk het Controleorgaan dan wel de bevoegde magistraat wordt voorzien waarbij de noodzakelijkheid, proportionaliteit en duur van het gebruik wordt gemotiveerd (cf. regels betreffende niet zichtbaar cameragebruik) en gecontroleerd;
- de bewaartermijn van de verwerking van de onderscheiden biometrische gegevens, met name de unieke code en de ruwe biometrische gegevens;
- de homologatie van het technisch verwerkingsproces (waaronder de minimum drempelwaarde);
- de periodieke controle op de betrouwbaarheid van het technisch verwerkingsproces;
- de transparantie van het verwerkingsproces;

stelt vast dat het gebruik van de *Clearview* gezichtsherkenningstechnologie niet wettelijk is en bijgevolg niet was noch is toegestaan;

stelt vast dat het gebruik van de *Clearview* gezichtsherkenning een doorgifte van politionele gegevens naar een derde land in de zin van de WGB betrof, zonder dat een adequaatheidsbesluit van de Europese Commissie in de zin van artikel 67 WGB voorhanden is, en dat er geen beroep kan worden gedaan of werd gedaan op de specifieke uitzonderingen zoals bepaald in artikelen 68 tot en met 70 WGB;

stelt derhalve vast dat de doorgifte naar *Clearview* aanzien moet worden als een *databreach* in de zin van de WGB en beveelt de federale politie de toepasselijke regels bij een inbreuk op de gegevensbeveiliging integraal na te komen; daarbij kan nuttig gebruik gemaakt worden van het model van aangifte op de website van het Controleorgaan (www.controleorgaan.be).

legt, in toepassing van artikel 247, 2° en 4° WGB de volgende twee corrigerende maatregelen op:

Corrigerende maatregel 1

gelast de federale politie om de nodige maatregelen en initiatieven te nemen teneinde de verplichtingen als verwerkingsverantwoordelijke bij een inbreuk op de gegevensbeveiliging na te komen conform de artikelen 61 en 62 WGB

Daartoe behoren minstens het initiatief te nemen om de onderneming *Clearview* er toe aan te zetten om:

a) de door de DJSOC verstrekte foto's uit hun gegevensbank te verwijderen;
b) de biometrische verwerking, met name de template en de ruwe biometrische gegevens, bij *Clearview* te verwijderen;

Het bewijs van de naleving van deze corrigerende maatregelen wordt binnen de twee maanden na datum van kennisname van deze maatregel aan het Controleorgaan overlegd;

Corrigerende maatregel 2

[68] Zie Voorstel van resolutie over een driejarig moratorium op het gebruik van gezichtsherkenningssoftware en -algoritmen in vaste of mobiele beveiligingscamera's in openbare en privéplaatsen van 16 juni 2020, Parl.St. *Kamer*, 2019-2020, DOC 1349/001, 22 blz. Het Controleorgaan verleende op die voorstel zijn advies DA210029 van 24 januari 2022, cf. randnummer 19, in fine.

<u>waarschuwt</u> de federale politie dat elk toekomstig (potentieel) gebruik van de *Clearview* gezichtsherkenningstechnologie of een gelijkaardige applicatie dan wel het gebruik van een gelijkaardige gegevensbank onwettig is en derhalve een eventuele voorgenomen verwerking van persoonsgegevens *de lege lata* de reglementering inzake de verwerking van persoonsgegevens kan (zal) schenden;

Zegt voor recht dat de aanvangsdatum van de corrigerende maatregelen en de datum van kennisname ervan bedoeld onder de littera 1. a) en 1. b) moet begrepen worden als zijnde de datum van het overmaken van het huidig definitief rapport van het Controleorgaan vermeerderd met twee dagen.

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

Goedgekeurd door het Controleorgaan op de politionele informatie op 4 februari 2022.

Voor het Controleorgaan,

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

Elektronisch afschrift aan:

- De Voorzitster van de Kamer van Volksvertegenwoordigers
- De Voorzitter van de Commissie voor de binnenlandse zaken, veiligheid, migratie en bestuurszaken van de Kamer van Volksvertegenwoordigers
- De Minister van Justitie
- De Minister van Binnenlandse Zaken
- De Voorzitter van het College van procureurs-generaal
- De Voorzitter van de Vaste Commissie van de Lokale Politie


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