CONTROLEORGAAN OP DE POLITIONELE INFORMATIE

Uw referentie	Onze referentie	Bijlage(n)	Datum
	DA210029		24/01/2022

<u>Betreft</u>: Advies 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)

Het Controleorgaan op de politionele informatie (hierna afgekort 'COC' of 'Controleorgaan');

Gelet op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (BS, 5 september 2018, hierna afgekort als 'WGB'), artikel 71 en Titel VII, inzonderheid artikel 236 § 2, 1de lid WGB.
Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG').
Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').
Gelet op de wet van 7 december 1998 tot organisatie van een geïntegreerde politie, gestructureerd op twee niveaus (hierna 'WGP').
Gelet op de '*Law Enforcement Directive'* 2016/680 van 27 april 2016 (hierna '*LED*').
Gelet op het verzoek per e-mail van 25 november 2021 van de Commissie voor Binnenlandse Zaken van de Kamer van Volksvertegenwoordiger, verstuurd door de voorzitter van voormelde Commissie;

Gelet op het verslag van de heer Frank Schuermans, lid-raadsheer in het Controleorgaan.

Brengt op 24 januari 2022 het volgend advies uit.

I. Voorafgaande opmerking nopens de bevoegdheid van het Controleorgaan

1. In het licht van, respectievelijk, de toepassing en omzetting van de Verordening 2016/679[1] en de Richtlijn 2016/680[2] heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid van de WOG bepaalt dat de competenties, taken en bevoegdheden als toezichthoudende autoriteit voorzien door de Verordening 2016/679 voor 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, worden uitgeoefend door het Controleorgaan.

2. Het Controleorgaan moet geraadpleegd worden bij de voorbereiding van wetgeving of een regelgevende maatregel die verband houdt met de verwerking van persoonsgegevens door de politiediensten van de geïntegreerde politie (zie artikel 59 §1, 2e lid en 236 §2 WGB, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie of *LED*). Daarbij heeft het Controleorgaan de opdracht om te onderzoeken of de voorgenomen verwerkingsactiviteit door de politiediensten in overeenstemming is met de bepalingen van Titel 1 (voor de niet-operationele verwerkingen)[3] en Titel 2 (voor de operationele verwerkingen) van de WGB[4]. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in het kader van de opdrachten van bestuurlijke en/of gerechtelijke politie brengt het Controleorgaan advies uit, hetzij uit eigen beweging, hetzij op verzoek van de Regering of van de Kamer van volksvertegenwoordigers, van een bestuurlijke of gerechtelijke overheid of van een politiedienst, inzake iedere aangelegenheid die betrekking heeft op het politionele informatiebeheer zoals geregeld in Afdeling 12 van Hoofdstuk 4 van de wet op het politieambt[5].

3. Het Controleorgaan is, ten aanzien van de politiediensten, de Algemene Inspectie van de federale politie en lokale politie (afgekort 'AIG') zoals bedoeld in de wet van 15 mei 2007 op de Algemene Inspectie en de Passagiersinformatie-eenheid (hierna afgekort 'BELPIU') bedoeld in Hoofdstuk 7 van de wet van 25 december 2016 tevens belast met het toezicht op de toepassing van Titel 2 van de GBW en/of de verwerking van persoonsgegevens zoals bedoeld in de artikelen 44/1 tot 44/11/13 van de wet op het politieambt en/of elke andere opdracht die haar krachtens of door andere wetten wordt verleend[6].

---

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming of 'AVG').
[2] 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 'Richtlijn politie-justitie' of *LED*).
[3] Artikel 4 §2, vierde lid WOG.
[4] Artikel 71 §1, derde lid WGB.
[5] Artikelen 59 §1, 2e lid en 236 § 2 WGB.
[6] Artikel 71 §1, derde lid juncto 236 § 3, WGB.

4. Het Controleorgaan is tot slot ingevolge artikel 281, § 4, van de algemene wet van 18 juli 1977 "*inzake douane en accijnzen*", zoals gewijzigd door de wet van 2 mei 2019 "*tot wijziging van diverse bepalingen met betrekking tot de verwerking van passagiersgegevens*" ten aanzien van de Dienst Geschillen van de Algemene Administratie van Douane en Accijnzen bevoegd in het kader van de vorderingen gericht aan de BELPIU in fiscale materies.

II. Voorwerp van de aanvraag

5. De aanvrager legt 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*" (hierna de 'Resolutie') voor, ingediend door de heren Vanden Burre en Smet en mevrouw Soors.

6. De bedoeling van de stellers van de voorgelegde tekst bestaat erin:

1) een moratorium van drie jaar in te stellen op het gebruik van software en van algoritmen voor gezichtsherkenning in vaste of mobiele veiligheidscamera's, in openbare en privéplaatsen;

2) ervoor te zorgen dat in de Kamer van volksvertegenwoordigers een debat over dit gevoelige onderwerp wordt gehouden, opdat van deze intrusieve technologie alleen gebruik kan worden gemaakt als ze gepaard gaat met strikte garanties inzake de inachtneming van de rechten van de mens.

In essentie wensen de stellers van de resolutie derhalve een bevriezing op elk **gebruik** van gezichtsherkenningstechnologie of de zgn. *Facial Recognition Technology* (hierna afgekort als *FRT*). De bedoeling van de stellers is kennelijk niet om het moratorium ook betrekking te laten hebben op enig wetgevend initiatief met betrekking tot *FRT*.

7. Het Controleorgaan is niet alleen een dataprotectie autoriteit, maar is tevens belast met de controle en het toezicht op de politionele gegevensbanken[7] en op alle politionele verwerkingen, ook in termen van legaliteit, efficiëntie en effectiviteit. Ook deze elementen (van bijvoorbeeld operationele haalbaarheid en capaciteit) wordt steeds mee in ogenschouw genomen bij elke adviesverlening.

III. Bespreking van de aanvraag

A. Algemene opmerkingen

8. Voor de algemene inhoud en strekking van de resolutie verwijst het COC naar de uitgebreide tekst ervan. Het voorstel van resolutie dateert wel reeds van 20 mei 2020. Ondertussen heeft zich toch al

[7] Zie ook Activiteitenverslag 2020 van het COC, https://www.controleorgaan.be/files/Activiteitenverslag_COC_2020_N.pdf, randnummer 7 en 8.

een hele evolutie afgetekend waarvan enkele hoofdlijnen hierna zullen worden geduid. Het is in het kader van dit advies uiteraard niet mogelijk exhaustief in te gaan op de veelvuldige ontwikkelingen, publicaties en initiatieven die zich de laatste jaren rond deze thematiek hebben voorgedaan. Vast staat alleszins dat het thema maatschappelijk erg leeft en in voortdurende beweging is, maar dat echte inzichten in de werking van zowel *Artificial Intelligence* (*AI)* als *FRT* (laat staan in een handhavings – of (in het Engels) een *law enforcement* context) nog in grote mate ontbreken, net zoals dat het geval is wanneer gezocht wordt naar onafhankelijke evaluaties in die landen waar *FRT* wel reeds toegepast wordt in een *law enforcement* context (in essentie Angelsaksische en Aziatische rechtstelsels).

9. Het voorstel van resolutie is zoals vermeld uitgebreid gemotiveerd. In *globo* heeft het Controleorgaan, onder voorbehoud van het hierna gestelde, daarop geen bijzondere opmerkingen.

De toelichting onderbouwt inderdaad op overtuigende wijze het voorstel van moratorium op elk gebruik van *FRT* en dit onder verwijzing naar meerdere (rechts)bronnen. Voor wat de politionele verwerkingen betreft en dus voor handhavingsdoeleinden (of meer algemeen doeleinden van bestuurlijke en gerechtelijke politie of voor zgn. *law enforcement* doeleinden) is het voorstel van resolutie evenwel juridisch gezien in zekere zin overbodig vermits het actuele wettelijk kader sowieso geen (afdoende) rechtsgrond biedt voor de geïntegreerde politie (hierna 'GPI') - en dus ook voor parket en onderzoeksrechter - om dergelijke gezichtsherkenningstechnologie in te zetten. Inderdaad, noch de Wet op het Politieambt, noch het Wetboek van Strafvordering of enig andere bijzondere (straf)wet biedt de *lege lata* een (afdoende) rechtsgrond voor de inzet van *FRT* voor opdrachten van bestuurlijke of gerechtelijke politie. Wat derhalve thans wettelijk niet mogelijk is behoeft in wezen – althans strikt juridisch bekeken - dus ook geen resolutie om die onmogelijkheid te bevestigen. De resolutie voorziet wel een bevriezingsperiode tot mei 2023 op elk gebruik van *FRT*.

De resolutie staat er wel niet aan in de weg dat de wetgever ondertussen werk zou maken van een wetgevend kader rond het gebruik van *FRT* in het algemeen of *FRT* voor *law enforcement* doeleinden in het bijzonder, zij het, dat het daadwerkelijke gebruik slechts in mei 2023 zou mogen aanvangen. De vraag is of de stellers van het ontwerp deze datum nog steeds voor ogen hebben nu dit in wezen nog slechts om minder dan anderhalf jaar gaat. De vraag is ook of de stellers zich verzetten tegen de ontwikkeling van een wetgevend kader door het parlement. Dit lijkt niet het geval wanneer er wordt voor gepleit een parlementair debat te houden met als doel te komen tot een regeling waarbij het gebruik van deze intrusieve technologie alleen gebruikt kan worden als ze gepaard gaat met strikte garanties inzake de inachtneming van de mensenrechten.

10. Dat er actueel voor *law enforcement* doeleinden geen afdoende rechtsbasis voorhanden is behoeft niet zo veel bijkomende duiding. Daar lijkt consensus over te bestaan. Zo kan verwezen worden naar de beleidsnota bij de begroting 2022 van de Minister van Binnenlandse Zaken waarin het volgende kan worden gelezen:

"*De inzet van camera's en de uitwisseling van data verhogen de doeltreffendheid en kwaliteit van operaties en dienstverlening van de politie, de administratie bevolking en alle andere diensten die over*

onze veiligheid waken. Evenwel stuiten technologische ontwikkelingen soms op bijvoorbeeld de zorg en regelgeving voor de privacy. We zullen daarom in 2022 een ethische adviescommissie "veiligheid" oprichten die het ethisch en doeltreffend gebruik van technologie en onderzoeks- en interventiemethoden moet beoordelen. Deze inzichten kunnen ook bijdragen tot een betere camerawet"[8]. En verder:

"Het belang van de doelmatige aanwending van deze technologieën is reeds wettelijk verankerd in de Wet op het Politieambt (WPA). Naast de richtlijnen die in 2021 werden uitgewerkt onder de koepel van de WPA, zullen er vanaf 2022 bijkomende aanpassingen gebeuren om de onder punt 11 vermelde uitdagingen te consolideren in de WPA. Artikel 44 van de WPA is immers gestoeld op de oude leest van gegevensverwerking en derhalve op oude technologieën uit de vorige eeuw. Deze aanpassingen zullen in nauw overleg met het Controleorgaan (COC) en onder auspiciën van de EU gebeuren zodat nieuwe technologieën slechts gebruikt kunnen worden onder strikte voorwaarden en toezicht terwijl de opslag maximaal wordt afgeschermd. … De Europese resoluties en wetgeving inzake het reguleren van Artificiële Intelligentie worden nauwgezet opgevolgd zodat we blijven ijveren voor doelmatig gebruik van nieuwe technologieën binnen een strikt wettelijk en regelgevend kader met de nodige inbouw van gelaagde beveiligingsmaatregelen inclusief toezichtsorganen.[9]"

In het kader van het onrechtmatig gebruik van de *Clearview* gezichtsherkenningstechnologie door de federale politie stelde de Minister op 6 oktober 2021 in de Commissie Binnenlandse Zaken van de Kamer terecht het volgende[10]: "*Aangezien het Belgisch wettelijk kader de exploitatie van deze software niet toelaat, zal ze niet door de federale politie worden gebruikt, conform mijn eerdere antwoorden met betrekking tot dit thema. … Gezichtsherkenning is zeker een interessante piste om op termijn te gebruiken ter ondersteuning van de werking van de politie in uitvoering van de opdrachten van de bestuurlijke en gerechtelijke politie. Dat kan uiteraard enkel met een correcte wettelijke basis zodat de verkregen informatie rechtsgeldig bestuurlijk en gerechtelijk aangewend kan worden*"[11].

11. Het gebruik van gezichtsherkenningstechnologie of *FRT* betekent ook een 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[12] en de stem van de natuurlijke persoon tot deze bijzondere categorie

[8] Parl.St. *Kamer*, 2021-2022, n° 2294/18, p. 6; eigen onderlijning door het Controleorgaan.

[9] Parl.St. *Kamer*, 2021-2022, n° 2294/18, p. 59-60; eigen onderlijning door het Controleorgaan.

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

[11] Onderlijning door het Controleorgaan.

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

van persoonsgegevens. De gezichtsherkenning vereist evenwel een aanvullende technische verwerking van de gezichtsafbeelding (de foto of het beeld)[13].

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*'[14]). 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). Bij een positief resultaat (*hit*: overeenstemming tussen de gezichtskenmerken) dient deze vervolgens gevalideerd te worden ('*match*')[15]. 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.

In de politionele context beoogt het gebruikt van gezichtsherkenningstechnologie *grosso modo* twee algemene doelstellingen: identificatie op basis van ongerichte dan wel gerichte opzoeking van personen[16].

Bij ongerichte (al dan niet in *real time*) publieke gezichtsherkenning wordt een zeer omvangrijke hoeveelheid 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

---

[13] Art. 34 § 1, aanhef WGB.

[14] Een *template* kana ls volgt gedefinieerd worden: "*A biometric template is a digital representation of the unique features that have been extracted from a biometric sample and is stored in a biometric database*", zie *Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, June 2021*.

[15] 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.

[16] 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-tegenover-menig/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.

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 (al dan niet 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[17].

Bij publiek gerichte gezichtsherkenning worden de foto's of de beelden van één of meer 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 de 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 voordien geselecteerde foto's of beelden 'gericht' gezocht naar overeenstemmende foto's of beelden die door derden[18] of de politie worden beheerd (op een digitaal platform). Het betreft hier dus een gerichte onderzoeks- of 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)[19].

12. Samen met de minister van Binnenlandse Zaken[20]moet vastgesteld worden dat het gebruik van de gezichtsherkenningstechnologie niet concreet in de wet op het Politieambt (WPA) wordt geregeld. 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. 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 en nationale) rechtspraak aan de verwerking van biometrische gegevens door rechtshandhavingsautoriteiten wordt gesteld, wordt een specifieke en heldere wettelijke basis vereist waarbij de omstandigheden en voorwaarden voor het gebruik ervan in een rechtsnorm worden

---

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

[18] 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.

[19] 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?).

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

vastgelegd en met specifieke en adequate (veiligheids)waarborgen worden omringd[21]. 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[22]waarbij het COC corrigerend is moeten optreden. Eenzelfde optreden door het COC laat zich aanzien in de *Clearview* zaak waar het COC een ambtshalve onderzoek is opgestart dat zich thans in de eindfase bevindt.

B. Bredere context en retroakten

13. Sedert mei 2020 zijn er nog heel wat vermeldenswaardige initiatieven geweest die allen in rekening kunnen en/of moeten worden gebracht bij het nadenken over en de ontwikkeling van een beleid en opmaak van eventuele interne wetgeving inzake *AI* in het algemeen en *FRT* in het bijzonder.

B.1. Op het Internationale en Europese niveau

14. Op 21 april 2021 heeft de Europese Commissie haar voorstel voor een verordening voor kunstmatige intelligentie gepubliceerd (ook wel *Artificial Intelligence Act* of *AIA*)[23]. Zeven maanden later presenteerde de Raad van de EU een compromistekst met enkele belangrijke wijzigingen die ongetwijfeld nog heel wat discussiepunten bevatten. Inmiddels werd ook een gezamenlijke opinie van de EDPB[24] en de EDPS[25] op het Commissievoorstel uitgebracht[26].

15. De hangende discussiepunten zijn onder meer, maar niet uitsluitend:

- de definitie van AI-systemen waarvan het EU commissievoorstel door de Raad als te ruim wordt bestempeld. De Raad stelt voor om alle 'meer traditionele softwaresystemen' van de definitie uit te sluiten. Bovendien sluit de tekstversie van de Raad alle "*AI-systemen voor algemene doeleinden*" uit van het toepassingsgebied van de *AIA*. Met andere woorden, als een algemeen AI-systeem (zoals vaak ontwikkeld door grote *big tech* bedrijven) alleen het

---

[21] 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.

[22] 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.

[23] Voorstel voor een Verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Uni, https://eur-Lex.Europa.eu/Legal-content/EN/TXT/?uri=:52021PC0206

[24] De EDPB (European Data Protection Board) of Europees Comité Voor Gegevensbescherming is het Comité dat als onafhankelijk orgaan van de Unie alle nationale dataprotectie autoriteiten en de EDPS (cf. infra volgende voetnoot) verzamelt (de opvolger van de vroegere werkgroep 29) en toeziet op de correcte en consistente toepassing van het gegevensbeschermingsrecht in de EU; zie ook www.edpb.europa.eu

[25] De EDPS is de gegevensbeschermingsautoriteit voor Europol; zie ook www.edps.europa.eu

[26] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 june 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu).

'potentieel' heeft om risicovolle praktijken uit te voeren, maar (nog) niet is ontwikkeld in die risicovolle contexten, zou het niet per se onderworpen worden aan de *AIA*;

- één van de meest besproken bepalingen is artikel 5 *AIA*, dat de 'zwarte lijst' (de zgn. 'verboden praktijken op het gebied van artificiële intelligentie') bevat, d.w.z. de toepassingen waarbij het risico als onaanvaardbaar wordt beschouwd, onverminderd enkele uitzonderingen. De Raad heeft op dit punt een aantal wijzigingen doorgevoerd die ook het vlak van *law enforcement* belangrijk zijn. Wat de *real-time* biometrische herkenning betreft, roept het voorstel van de Commissie op tot een algemeen verbod op het gebruik ervan door rechtshandhavingsinstanties in openbare ruimten, weliswaar met een aantal belangrijke uitzonderingen. De Europese Raad heeft op het Commissievoorstel op zijn beurt meerdere wijzigingen aangebracht waaronder:
    - Wijziging van het toepassingsgebied waardoor:
        - doelstelling van nationale veiligheid (en dus de activiteiten van inlichtingendiensten) niet onder de *AIA* zouden vallen;
        - *AI* systemen waarvan de doelstelling wetenschappelijk onderzoek of ontwikkeling is (dus ook wetenschappelijk onderzoek/ontwikkeling door de politiediensten?) er niet zouden onder vallen;
        - het niet enkel betrekking heeft op de handhavingsdiensten op zich die gebruik maken van *AI* systemen maar ook eventuele verwerkers ("*on their behalf*");
    - het kenmerk *"remote"* werd geschrapt, waardoor de reikwijdte van het principiële verbod verder gaat;
    - bedreigingen voor kritieke infrastructuur en gezondheid zijn als uitzonderingen op het verbod geïntroduceerd en de omstandigheid dat de dreiging 'dreigt' te ontstaan is weggenomen, waardoor de reikwijdte van het legitieme gebruik ervan is uitgebreid (Art. 5.1.d.ii).

Samengevat voorziet het Raadsvoorstel nu dus een principieel verbod op *real time* ('*live*') gebruik van biometrische identificatie systemen (dus o.a. *FRT*) voor *law enforcement* doeleinden behoudens indien de doelstelling is:

- het gericht zoeken naar (potentiële) slachtoffers (ar. 5.1.d.i);
- de preventie van een specifieke en substantiële bedreigingen voor kritieke infrastructuur, leven, gezondheid, fysieke veiligheid van natuurlijke personen of een terroristische aanval (de criteria "*kritieke infrastructuur*" en "*gezondheid*" zijn zoals gezegd als bijkomende uitzonderingen geïntroduceerd en de omstandigheid dat de bedreiging echt 'op handen' moet zijn (*imminent*) werd geschrapt (Art. 5.1.d.ii);
- de opsporing, lokalisatie, identificatie en vervolging van plegers, verdachten of veroordeelden van misdrijven zoals opgenomen in de lijst voorzien in het kaderbesluit 2202/584/JBZ m.b.t. het Europees aanhoudingsmandaat waarop minimaal een maximale gevangenisstraf van drie jaar staat in het interne lidstatelijk recht.

Daarbij voorziet het ontwerp *AIA* van de Commissie, zoals geamendeerd door de Raad, dat bij dergelijk *law enforement* gebruik de volgende elementen (art. 5.2) in rekening moeten worden gebracht:

- de aard van de situatie waarvan sprake, in het bijzonder de ernst, probabiliteit en omvang van de nadelen verbonden aan het niet gebruik ervan;
- de gevolgen van het gebruik ervan voor de rechten en vrijheden van alle betrokken personen, in het bijzonder de ernst, probabiliteit en omvang van die gevolgen.

Ook temporele, geografische en persoonsgebonden waarborgen moeten worden voorzien bij elk *law enforcement* gebruik (art. 5.2). Krachtens het ontworpen art. 5.3 moet dit gebruik van *real time* biometrische systemen in openbare plaatsen voorafgaandelijk gemachtigd worden door een rechterlijke of onafhankelijke administratieve autoriteit op grond van een gemotiveerd verzoek conform het nationale recht. In geval van spoedeisendheid kan men starten zonder die machtiging voor zover men zonder noodzakelijk uitstel de machtiging aanvraagt en het gebruik ervan onmiddellijk stopzet indien die machtiging er niet komt.

Tot slot voorziet art. 5.4. dat het lidstatelijk recht erin kan voorzien volledig of slechts gedeeltelijk voormelde toepassing van biometrische systemen toe te laten (België zou dus beperkender of strikter kunnen zijn in het eigen interne recht). Dat nationale recht zal alleszins gedetailleerde regels moeten vastleggen m.b.t. de aanvragen, de machtigingen, de uitvoering, het toezicht en de rapportering met betrekking tot de gegeven toelatingen. Deze regels zullen ook moeten specifiëren voor welke doelstellingen opgesomd in art. 5.1.d en voor welke misdrijven (uit de lijst van misdrijven m.b.t. het Europees aanhoudingsmandaat) het nationale recht de mogelijkheid zal voorzien tot het gebruik van *real time* biometrische identificatiesystemen in openbare plaatsen.

Het is duidelijk dat de nationale wetgever, ook bij aanname van de *AIA* nog heel wat werk voor de boeg heeft en keuzes zal moeten maken.

16. Conform de bijlage III van de *AIA* worden onder meer als "*high risk*" *AI* systemen beschouwd:

- elk biometrisch systeem voor *real time* of post biometrische identificatie van natuurlijke personen zonder hun medeweten. Dat betekent dus ook biometrische identificatiesystemen zoals *FRT* die uitsluitend op reactieve wijze in opsporings- of gerechtelijke onderzoeken zouden gebruikt worden.
- In het domein van l*aw enforcement*: alle systemen die te maken hebben met '*predictive policing* en '*predictive justice'*, leugendetectors of gelijkaardige systemen die emoties proberen te detecteren, systemen om *deep fake* te detecteren, systemen om de betrouwbaarheid van bewijsmateriaal te beoordelen en systemen om aan politionele of justitiële *profiling* te doen. De Raad schrapt wel het voorstel van de Commissie om ook systemen voor criminaliteitsanalyses, die toelaten grote datavolumes uit verschillende

bronnen en van verschillende formaten te doorzoeken en te analyseren met het oog op het vinden van patronen of relaties, als hoog risico houdend te beschouwen.

De *labeling* van systemen als hoog risico houdend is essentieel vermits daaraan aan schare voorwaarden en verplichtingen worden gekoppeld die anders niet van toepassing zijn.

17. Er moet ook worden gewezen op het door de *EDPB* en *EDPS* gezamenlijk gevraagd algemeen verbod in zijn geheel op elke vorm van gebruik van AI ten behoeve van automatisch herkenning van menselijke eigenschappen (dus niet enkel gezichtsherkenning) in publiek toegankelijke plaatsen: "*the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context"*[27]. Het COC is alvast meer genuanceerd wat dat aspect betreft wanneer het om doelstellingen van *law enforcement* gaat.

Hoe dan ook, vast staat dat het maatschappelijke debat in het algemeen en de trialoog in het bijzonder met betrekking tot de *AI* verordening nog een hele tijd zal duren. In de doctrine wordt het jaar 2025 naar voren geschoven vooraleer er sprake kan zijn van een daadwerkelijke inwerkingtreding van de *AIA*, wordt gesproken over "*de lange strijd tot een finale AI-Verordening*" en dat we nog maar aan het begin van een moeilijk proces staan[28]. De vraag is dan natuurlijk of het überhaupt zinvol is dit Europees wetgevend initiatief niet af te wachten en zelf als lidstaat hieromtrent te legifereren (cf. verder).

18. De Europese Commissie wil anderzijds kennelijk wel vaart zetten met het gebruik van *FRT* zoals moge blijken uit een zeer recent voorstel rond de creatie van een zgn. *hub* bij Europol waarbij de politionele databanken van de 27 lidstaten zouden verbonden worden en waarbij ook biometrische data en *FRT* informatie en persoonsgegevens zouden worden uitgewisseld. Zo konden we in de pers het volgende lezen:
« *Face à l'activité croissante des réseaux criminels internationaux, la Commission européenne a proposé, ce mercredi, un paquet législatif visant à accroître la coopération entre les forces de polices des 27 États membres de l'Union européenne (UE). L'initiative comporte une proposition de directive sur les échanges d'informations entre les services de police. … La Commission propose de revoir les règles du traité de Prüm sur la coopération policière dans l'espace Schengen, afin de créer d'ici à 2027 un hub central pour accélérer l'échange d'informations. Ce point de contact unique, géré par Europol, sera accessible de manière permanente par les services de police des États européens. L'information demandée devrait être mise à disposition dans les 8 heures pour les cas urgents jusqu'à un maximum*

[27] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 june 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), zie nr. 30 e.v.

[28] S. De Schrijver, Een kijk op het strijdtoneel van de Verordening inzake artificiële intelligentie, Computerrecht, 2021, 247. De auteur stelt verder: "het moge duidelijk zijn, er is nog veel werk aan de AI-Verordening p.

de 7 jours. L'exécutif européen propose aussi d'inclure dans les informations à partager les images de reconnaissance faciale de suspects et de criminels condamnés[29] ainsi que les casiers judiciaires[30]. »

Dit bericht heeft te maken met het voorstel van de Europese Commissie[31] van 8 december 2021 van een zgn. *EU Police Cooperation Code* bestaande uit (1) een voorstel van richtlijn betreffende informatie-uitwisseling tussen handhavingsdiensten en tot intrekking van het Kaderbesluit 2006/960/JHA[32], (2) een voorstel van Verordening betreffende geautomatiseerde uitwisseling van informatie voor doeleinden van politiesamenwerking (Prüm II)[33] en een aanbeveling inzake operationele politiële samenwerking[34]. De doelstelling van de Verordening is "*adding facial images of suspects and convicted criminals and police records to the available data under the automated data exchange framework*"[35] en derhalve beelden van gezichten op geautomatiseerde wijze te laten uitwisselen en opzoeken tussen lidstaten. Een en ander zal nader nog technisch dienen geregeld te worden door uitvoeringshandelingen van de Commissie en door het nationale recht (die onder meer de toegang en opzoekingsmodaliteiten zal moeten regelen tot de te creëren nationale databank *facial images*). Hoewel het voorstel van Verordening er niet op ingaat – wel worden de *facial images* gedefinieerd als een biometrisch gegeven[36] - is duidelijk dat dergelijke geautomatiseerde opzoeking en uitwisseling van foto's/beelden van gezichten van natuurlijke personen niet mogelijk is zonder echte biometrische verwerkingen en dus een voldragen systeem van *FRT.*

19. Op dit moment (en eigenlijk reeds het hele jaar 2021) werkt de *EDPB* (Europees Comité voor Gegevensbescherming) van zijn kant aan richtlijnen rond het gebruik van *FRT* voor handhavingsdoeleinden[37]. Het COC vertegenwoordigt voor dit thema België als dataprotectie autoriteit. Alleen al de duurtijd nodig voor de opmaak van een richtlijn en het aantal vergaderingen die tot op heden hieromtrent werd gehouden toont de complexiteit van de thematiek aan.

Deze richtlijnen zullen belangrijk zijn, ook al omdat deze goed de verschillende mogelijke toepassingen van *FRT* omschrijven die allen niet dezelfde mate van inbreuk op de privacy met zich brengen. Ook dat is immers belangrijk om weten: voor welke gevallen en in welke *use cases* wil men *FRT* inzetten?

---

[29] Eigen onderlijning.

[30] L'Écho, *Vers une coopération policière plus musclée entre les 27 états membres*, 9 december 2021, p.8

[31] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6645/smo

[32] *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM(2021) 782 final 2021/0411(COD).*

[33] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, COM(2021) 784 final 2021/0410(COD).*

[34] Voorstel voor een AANBEVELING VAN DE RAAD inzake operationele politiële samenwerking, COM(2021) 780 final 2021/0415(CNS).

[35] Reinforcing police cooperation across Europe, Factsheet_Police cooperation package_Reinforcing police cooperation across Europe, https://ec.europa.eu/commission/presscorner/detail/en/fs_21_6647; zie ook overweging 5, 7, 10, 11 en het ontworpen artikel 1, 3, 4, 10° en 11° en in het bijzonder hoofdstuk 4

[36] Ontwerpen artikel 4, 11°, 37, 39, 50 van het voorstel van Verordening Prüm II.

[37] Op dit moment heet het document dus nog: "*Draft guidelines x/202x on the use of facial recognition technology in the area of law enforcement*", niet gepubliceerd.

Terecht wordt in de ontwerp gewezen op de veelheid aan doelstellingen, toepassingen en contexten van *FRT*.

20. In de ontwerpfase van de richtlijn worden alvast de volgende voorbeelden gegeven wanneer we het hebben over gezichtsherkenning voor identificatiedoeleinden[38]:

- het zoeken in een bestand van foto's/beelden om de identiteit van een onbekend persoon te achterhalen (dader/verdachte of een slachtoffer bv.);
- het monitoren van iemands gedrag in een openbare plaats. Het gezicht van die persoon wordt vergeleken met de templates van alle personen op die plaats gedurende een bepaalde periode (vb. nadat een misdrijf werd gepleegd op die plaats);
- de reconstructie van iemands reisweg en ook de personen waarmee betrokkene gedurende die reisweg contact heeft gehad;
- biometrische identificatie op afstand (*remote*) in openbare plaatsen van door politie/justitie gezochte personen, wat een vergelijking inhoudt van de *template* van de gezochte personen met de *templates* van alle gezichten van alle personen gedurende een bepaalde tijd aanwezig op die openbare plaats;
- geautomatiseerde herkenning met als doelstelling relaties op te sporen op sociale media;
- enz. …

Er wordt terecht ook gewezen op de aspecten van betrouwbaarheid en juistheid van de techniek: "*Like every technology, facial recognition may also be subject to challenges when it comes to its implementation, in particular when it comes to its reliability and efficiency in terms of authentication or identification, as well as the overall issue of quality and accuracy of the "source" data and the result of facial recognition technology processing.*
Such technological challenges entail particular risks for data subjects concerned which are all the more significant or serious in the area of law enforcement considering the possible legal effects for data subjects or other effects similarly affecting them in a significant manner.
As pointed out by the EU Fundamental Rights Agency in its 2019 report[39], "determining the necessary level of accuracy of facial recognition software is challenging: there are many different ways to evaluate and assess accuracy, also depending on the task, purpose and context of its use. When applying the technology in places visited by millions of people – such as train stations or airports – a relatively small proportion of errors (e.g. 0.01 %) still means that hundreds of people are wrongly flagged. In addition, certain categories of people may be more likely to be wrongly matched than others, as described in Section 3. There are different ways to calculate and interpret error rates, so caution is required. In addition, when it comes to accuracy and errors, questions in relation to how

[38] We hebben het dus niet over de toepassingen voor authentificatie doeleinden.

[39] *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, EU Fundamental Right Agency, 21st November 2019.

easily a system can be tricked by, for example, fake face images (called 'spoofing') are important particularly for law enforcement purposes".

Daarnaast worden in het ontwerp van richtlijn verschillende mogelijke scenario's (hypothetische toepassingen) of *use cases* uitgewerkt, waaruit ook blijkt dat de risico's voor de bescherming van de persoonlijke levenssfeer erg verschillend kunnen zijn naar gelang van het betrokken scenario of *use case*, rekening houdende met een uit te voeren *DPIA* waarin de noodzakelijkheid, de proportionaliteit, de doeleinden en het toepasselijke nationale of EU juridisch kader aan bod moeten komen. Vereenvoudigd betreft het de volgende mogelijke voorbeelden:

- grenscontrole systemen in een één op één vergelijking; het betreft dus een 1 – 1 verificatie en identificatie;
- een systeem ter identificatie van slachtoffers van seksueel kindermisbruik wordt ontwikkeld; een gezichtsherkenningsvergelijking gebeurt tussen de foto van een bepaald mogelijk slachtoffer met een politionele databank van foto's van slachtoffers van kindermisbruik; dit zou dan gebeuren in specifieke onderzoeken op een *case by case* basis met nadien telkens een verificatie op basis van alle dossierelementen; het betreft een 1 – N identificatie;
- een systeem om geselecteerde daders van vandalisme en geweld tijdens een manifestatie te identificeren door hun afbeelding te vergelijken met de beelden of foto's van (private en publieke) vaste of mobiele camera's op de plaats en in de omgeving van het gebeuren, beelden van de media, van sociale media, enz. … (de beelden/foto's waartegen de vergelijking wordt gemaakt betreft dus a priori geen politionele databank; de politie maakt *ad hoc* een database aan met behulp van voormelde 'private' beelden/foto's van alle personen die aanwezig waren tijdens de feiten); het betreft een 1 – N identificatie;
- idem als voorgaand scenario maar de vergelijking wordt deze keer gemaakt met de nationale politionele fototeekdatabase van verdachten zoals die door het forensisch departement wordt *up to date* gehouden; het betreft een 1 – N identificatie;
- een systeem van *real time remote* biometrische identificatie in publieke plaatsen waarbij er een onafgebroken vergelijking gebeurt van alle personen aanwezig op die plaats met een lijst van gezochte personen zonder dat er enige (of eventueel enkel een zeer vage) voorkennis is omtrent de mogelijke aanwezigheid van deze gezochte personen op de onder *surveillance* staande publieke plaatsen; het betreft een N – 1 identificatie
- een privaat systeem en private databank (type *Clearview*) wordt door de politie gebruikt om aan gezichtsherkenning te doen; het betreft op 1 – N identificatie maar kan slaan op verdachten, slachtoffers of zelfs getuigen.

Deze voorbeelden van mogelijk gebruik van *FRT* toont alvast de enorme complexiteit aan, alleen al om adequate wetgeving op te stellen onafgezien van het daadwerkelijke gebruik van de technologie.

21. Een ander belangrijk document in deze is ook de *Recommendation CM/Rec(2021)8* van het Comité van Ministers van de Raad van Europa "*on the protection of individuals with regard to automatic processing of personal data in the context of profiling*", aangenomen op 3 november 2021 en waar onder meer wordt ingegaan op de problematiek van *profiling*, de noodzakelijke kwaliteit van de gebruikte algoritmen en specifieke voorzieningen en te nemen maatregelen wanneer de *profiling* gesteund is op *AI* systemen die *machine learning* processen bevatten.

B.2. Op Belgische niveau

22. Behoudens het ontwerp van resolutie, voorwerp van het huidig advies, kan er ook verwezen worden naar het Wetsvoorstel n° 55 1904/001 van 6 april 2021 tot wijziging van de wet openbaarheid van bestuur[40] waarop het FIRM[41] zijn advies 5/2021 van 5 oktober 2021 heeft uitgebracht. In voormeld advies worden ook door het FIRM gewezen op de gevaren en uitdagingen rond het werken met *AI*, zij het dat het voorstel niet van toepassing is op handhavingsdiensten zoals politie en gerechtelijke overheid. Het voorstel heeft alvast de verdienste om het eerste te zijn dat een kader wil vastleggen voor de aanwending van bepaalde algoritmische technologieën en artificiële intelligentie door de Belgische overheden.

C. Argumenten die pleiten voor een moratorium

C.1. Legitimiteit van de politie en toepassing van de gemeenschapsgerichte politiezorg

23. Het onderwerp is allesbehalve uitgekristalliseerd. Dat toont bovenstaande opsomming van (wetgevende) initiatieven allerhande afdoende aan.

Michael O'Flaherty, directeur van het EU Fundamental Rights Agency (FRA) stelde het op de *EDEN*[42] conferentie van 18 oktober 2018[43] als volgt wanneer hij terecht het belang, in de eerste plaats voor de legitimiteit van de politie zelf, van het noodzakelijke respect voor grondrechten door de politie bij onder meer het gebruik van *AI* benadrukt: " … "*when policing itself shows a deep respect for human rights, it delivers better outcomes. Such approaches do, and will, help build public trust in policing, which is so essential for secure societies. We need to invest in the strengthening, the building of that trust right now, for instance, in the context of the use of biometric data applications in public settings*". Zonder dat vertrouwen van de bevolking in de politie en in de technologieën die het aanwendt kan er geen sprake zijn van een kwaliteitsvol *community policing* model, toch nog steeds het Belgische

---

[40] Wetsvoorstel van 6 april 2021 tot wijziging van de wet van 11 april 1994 betreffende de openbaarheid van bestuur, om meer transparantie te verschaffen over het gebruik van algoritmen door de overheid, Parl.St. *Kamer*, 2020-2021, n° 55. 1904/001.

[41] Federaal Instituut voor de bescherming en bevordering van de rechten van de mens, https://federaalinstituutmensenrechten.be, publicaties/adviezen.

[42] *EDEN* is Europols dataprotectie experten werkgroep (***E**uropol **D**ata Protection **E**xperts **N**etwork*).

[43] https://fra.europa.eu/en/speech/2021/data-protection-policing

politiemodel bij uitstek. Dat laatste staat reeds zwaar onder druk door de COVID-pandemie waarin de GPI in een bij uitstek repressieve rol wordt gedwongen. Het gebruik van technologie waarin er bij bevolking, laat staan bij overheden, onzekerheid of twijfel bestaat nopens betrouwbaarheid, accuraatheid, juistheid en kwaliteit kan de politie missen als kiespijn en heeft ook nefaste consequenties voor het geheel van de handhavingsketen.

Een ander belangrijk aspect is de kennis en *knowhow* bij de GPI zelf. Op dat vlak is het COC actueel helemaal niet gerustgesteld. Er is bij de GPI in het algemeen een reëel expertiseprobleem (juridische basiskennis, IT expertise, digitale vaardigheden, enz. …). Het is hier niet de plaats om veel uit te wijden over de opleiding van de Belgische politie, zowel de basispolitiezorg als alle vormen van voortgezette opleiding, maar we kunnen gerust stellen dat ons Belgische opleiding minimaal is en de vergelijking met het buitenland vaak niet kan doorstaan (alleen al de beperkte lengte van de basisopleiding om politie-inspecteur te worden blijft een majeur pijnpunt, daar waar in wezen van elk basiskaderlid een bacheloropleiding zou mogen en moeten verwacht worden). Ook het EU *FRA* dringt daar terecht op aan: "*We need high degrees of digital literacy, not only in the security communities …*"[44]

24. Daarnaast zijn er nog de informatieveiligheidsaspecten die nog belangrijker worden wanneer bij de politie zou worden overgegaan tot massale bewaring en verwerking van biometrische gegevens. Het is een illusie te denken dat de politie of handhavingsdiensten in het algemeen vrij zouden blijven van cyberaanvallen, laat staan onbewuste IT misslagen (denken we maar aan zware cyberaanval op defensie van 16 december 2021[45]). Steeds meer overheden worden het slachtoffer van dit soort van aanvallen zoals recent ook nog eens in Frankrijk is gebleken. De vaststelling is ook daar dat "*Les administrations ne cessent d'être ciblées par les cybercriminels pour les informations personnelles qu'elles possèdent* ». Niet minder dan 1.964 Franse openbare overheden kregen in 2021 te maken met cyberaanvallen/datadiefstal. De Franse gegevensbeschermingsautoriteit, de *CNIL*, heeft het Ministerie van Binnenlandse Zaken moeten sanctioneren wegens een gebrekkig geautomatiseerd beheer van vingerafdrukken[46].

Komt daarbij dat de Belgische GPI meer en meer gebruik maakt van Microsoft producten waarbij er hoe dan ook nooit zekerheid is dat de Amerikaanse autoriteiten geen toegang tot voormelde gegevens hebben. Die reeds bestaande risico's worden alleen maar groter bij de massale opslag van *FRT* persoonsgegevens, die, moet het herhaald, onwijzigbare biometrische gegevens bevatten.

---

[44] Ibid, https://fra.europa.eu/en/speech/2021/data-protection-policing

[45] « *Na 26 dagen kan het leger weer mailen*, De Standaard, 13 januari 2022, p. 9; "*Cyberaanval op defensie erger dan gedacht, De Morgen*", 13 januari 2022, p. 7;

[46] Le Monde van 27.12.2021, *Les failles de la protection des données des français par les pouvoirs publics*, https://journal.lemonde.fr/data/reader.html?xtor=EPR-32

Jaarlijks worden bij het COC door de GPI rond de 30 *databreaches* aangemeld, waarvan sommige vrij substantieel. Recent nog één wegens het verlies van twee zgn. FOCUS smartphones in een politiezone. Dergelijke smartphone geeft toegang tot een omvangrijk geheel aan politionele en niet politionele databanken. Het spreekt dan ook voor zich dat de gevolgen van inbreuken tegen de beveiliging vele malen groter zijn wanneer biometrische gegevens zoals foto's en templates van natuurlijke personen zouden worden gestolen of verloren geraken. De risico's worden exponentieel groter. Identiteitsdiefstal is daarnaast thans reeds een bijzonder ernstig en moeilijk te bevechten fenomeen met zeer snel bijzonder nadelige gevolgen voor de slachtoffers (waarbij men plots verdacht kan worden van strafbare feiten begaan door identiteitscriminelen met alle gevolgen van dien); men mag er niet aan denken wat de gevolgen zullen zijn als ook biometrische gegevens (al dan niet in grote volumes) worden gestolen …

25. Die politielegitimiteit kan ook alleen maar bereikt worden als de GPI scrupuleus haar verplichtingen betreffende het opstellen van een gegevensbeschermingseffectenbeoordeling (*DPIA*) naleeft en goed nadenkt vóóraleer met risico houdende verwerkingen te beginnen; een *DPIA* die vooral ook context - en applicatie specifiek moet zijn, vóóraleer *in concreto* met een *FRT* toepassing te beginnen. Maar ook reeds in de fase van het opstellen van de regelgeving mag die verplichting niet over het hoofd gezien worden, zeker wanneer het om *FRT* gaat. Het opstellen van een *DPIA* vóór men aan een risico houdende verwerking begint is bij de GPI evenwel nog helemaal geen evidentie. Integendeel, daarop wordt herhaaldelijk en ook bij de ingebruikname van grote en belangrijke IT applicaties gezondigd. We citeren als sprekende voorbeelden de toepassingen/databanken INFOTHEEK en FOCUS. Ook bij de uitrol van *police search* (een soort van politionele *Google* zoekmachine) die actueel aan de gang is, bleek dat de directie van operationele informatie en de ICT middelen (DRI) van de federale politie aanvankelijk niet van plan was een *DPIA* op te maken.

C.2. Draagvlak bij de bevolking voor het gebruik van AI en FRT

26. Het *FRA* deed in 2019 een EU bevolkingsbevraging waarin gepeild werd naar de mate waarin de burger bereid is gezichtsherkenningsbeelden voor doeleinden van identificatie te aanvaarden. Slechts 17% van de bevraagden bleek zich comfortabel te voelen bij het idee.

De door de Minister aangekondigde ethische adviescommissie veiligheid kan hier ongetwijfeld een belangrijke rol spelen[47] vermits deze "… *het wettelijk en operationeel kader voor een verantwoordelijk, ethisch en doeltreffend gebruik van technologie en bepaalde onderzoeks- en interventiemethoden op het gebied van veiligheid* (zal bepalen)"[48]. Vooraleer de GPI ook maar zou overwegen te starten met een *FRT* systeem dient dan ook deze commissie te zijn geïnstalleerd en geoperationaliseerd.

[47] Parl.St. *Kamer*, 2021-2022, n° 2294/18, p. 6 en 9

[48] Ibid, p. 16.

C.3. De inherente kwaliteitsproblemen van *FRT*

27. Uit de literatuur, de adviezen van de *EDPS* en *EDPB* en de eigen bevindingen van het COC (in de zaak van het gebruik van *FRT* in Brussel-nationale luchthaven bijvoorbeeld) weten we dat er nog heel wat problemen zijn van juistheid en accuraatheid van *FRT*. Het gebrek aan bestaande onafhankelijke evaluaties is gekend. Het aantal vals positieven en vals negatieven blijkt groot en gekende problemen zijn er bij mensen met donkere huidskleur, baarden en brillen, enz. … Vooralsnog ziet het COC weinig geruststellende signalen op dat vlak.

C.4. De grondrechten die aan de orde zijn bij het gebruik van FRT

28. Vast staat dat zeker niet enkel het recht op privacy en gegevensbescherming aan de orde is bij het gebruik van *FRT* voor handhavingsdoeleinden. Het gaat eveneens op het verbod op discriminatie, de grondrechten als vrijheid van vergaderen, de vrijheid van meningsuiting, de vrijheid om informatie te ontvangen en te verspreiden, de godsdienstvrijheid, enz. …[49];het zgn. *chilling effect* is ondertussen ruimschoots beschreven en erkend.

D. Beginselen die het gebruik van *AI/ FRT* dienen te omkaderen

29. Binnen de context van en *in concreto* toegepast op gebruik van *AI/FRT* door de GPI dienen de volgende principes absoluut te worden nageleefd en concreet te worden gemaakt, zowel in regelgeving als in de praktijk:

Wettelijkheid

29. De bescherming van persoonsgegevens die voortvloeit uit de uitdrukkelijke verplichting die is vastgelegd in artikel 8, lid 1 van het EU Handvest van de grondrechten, is met name van belang voor het recht op eerbiediging van het privéleven (bij de verwerking van persoonsgegevens, waaronder biometrische gegevens) dat is vastgelegd in artikel 7 van het Handvest[50]. De wetgeving moet duidelijke en nauwkeurige regels stellen voor de reikwijdte en de toepassing van de maatregel in kwestie en waarborgen bieden, zodat de personen van wie de gegevens zijn verwerkt, voldoende waarborgen hebben om hun persoonsgegevens effectief te beschermen tegen het risico van misbruik en tegen

[49] Ibid, https://fra.europa.eu/en/speech/2021/data-protection-policing

[50] HvJ nr. C-594/12, § 53.

elke onrechtmatige toegang of gebruik van die gegevens[51]. De behoefte aan dergelijke waarborgen is des te groter wanneer persoonsgegevens automatisch worden verwerkt en er een aanzienlijk risico bestaat op onrechtmatige toegang tot de gegevens, laat staan wanneer het biometrische gegevens betreft[52]. Er mag geen inmenging zijn van een overheid in de uitoefening van dit recht, behalve wanneer dit in overeenstemming is met de wet en voor zover noodzakelijk is in een democratische samenleving in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, voor het voorkomen van wanorde of misdaad, voor de bescherming van de gezondheid of de goede zeden, of voor de bescherming van de rechten en vrijheden van anderen. Het EVRM stelt ook standaarden betreffende de wijze waarop beperkingen kunnen worden opgelegd. Een basisvereiste, naast de *rule of law*, is de **voorzienbaarheid**. Om aan de eis van voorzienbaarheid te voldoen, moet de wet voldoende duidelijk zijn om individuen een adequate indicatie te geven van de omstandigheden waarin en de voorwaarden waaronder de autoriteiten bevoegd zijn om dergelijke maatregelen te nemen[53]. Naarmate de inbreuk op de persoonlijke levenssfeer ernstiger wordt, stelt het EHRM hoger kwaliteitseisen aan de wettelijke basis[54].

Het Controleorgaan sluit zich aan bij de *EDPB* en *EDPS* in hun opinie van juni 2020 waarin ze stellen dat "*the use of AI in the area of police and law enforcement requires area-specific, precise, foreseeable and proportionate rules that need to consider the interests of the persons concerned and the effects on the functioning of a democratic society*"[55].

De wetgeving zal, wanneer gericht op het gebruik van *FRT* door de politiediensten, ook aandacht moeten hebben voor de verschillende doeleinden en toepassingen die men nastreeft:

- voor de GPI betekent dat, dat niet alleen moet gekeken worden naar operationele *LED* gegevensverwerkingen, maar dat bijvoorbeeld ook het gebruik van *FRT* voor interne GPI en AVG doeleinden (intern toezicht, tuchtdoeleinden, interne toegangscontrole voor medewerkers, enz. …) moet geregeld worden. De *lege lata* is het gebruik van biometrische gegevens zoals gezichtsherkenning of vingerafdrukken immers niet toegelaten in een AVG context.
- Een ander aandachtspunt betreft de problematiek van de zgn. 'categorisering' (gender, huidskleur, emoties, …) als gevolg van *FRT*. Hoewel bij de GPI 'identificatie' het primaire doel

[51] HvJ nr. C-594/12, §. 54; zie ook m.b.t. artikel 8 EVRM, EHRM, Liberty and Others t. Verenigd Koninkrijk, 1 Juli 2008, nr. 58243/00, § 62 en 63; Rotaru t. Roemenië, § 57 to 59 en S. and Marper t. Verenigd Koninkrijk, § 99.

[52] HvJ nr. C-594/12, § 55, zie ook m.b.t. artikel 8 EVRM, S. and Marper t. Verenigd Koninkrijk, § 103 en M. K. t. Frankrijk, 18 April 2013, no. 19522/09, § 35.

[53] EHRM, Copland t. Verenigd Koninkrijk, 3 april 2007, no. 62617/00, § 46.

[54] EHRM Gaughran t. Verenigd Koninkrijk, 13 februari 2020, nr. 45245/15; EHRM P.N t. Duitsland 11 juni 2020, nr. 74440/17; EHRM S. and Marper t. Verenigd Koninkrijk, 2 december 2008, nrs. 30562/04 en 30566/04.

[55] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 june 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), p. 10, n° 27.

> van FRT is, kan er ook sprake zijn van categorisering. Hoewel het doel bij categorisering *in se* niet gericht is op identificatie als zodanig, zal er echter doorgaans, minstens, wel sprake zijn van indirect identificeerbaar. Welnu, naar het aanvoelen van het COC kan *FRT* met het oog op (h)erkennen van unieke emoties niet oninteressant zijn bij, bijvoorbeeld, de opname van een verhoor (vgl. met de polygraaf). Een strikte lezing van artikel 44/1 § 2, 1 ° WPA lijkt dit type van categorisering *de lege lata* alvast uit te sluiten, aangezien de biometrische gegevens actueel in beginsel enkel kunnen verwerkt met het oog op 'ondubbelzinnige identificatie'. Zo beschouwd is het gebruik van *FRT* met het oog op categorisering (zoals het vastleggen van emoties) *de lege lata* actueel uitgesloten, minstens lijkt dat het geval te zijn (althans in de WPA). Er zal moeten beoordeeld worden of men dergelijke toepassing van *FRT* wil mogelijk maken en zo ja, zal het actuele wettelijke kader moeten wijzigen.
>
> Aan de andere kant lijkt artikel 44/1 § 2, 1° WPA het gebruik van *FRT* met het oog op unieke gedragskenmerken niet uit te sluiten indien dit concreter geregeld in de WPA. Hoewel dit type van biometrische verwerking als een vorm van categorisering zou kunnen worden beschouwd, gaat het echter wel om 'identificeren'. Een voorbeeld kan dit verduidelijken: er wordt een gewapende bankoverval of inbraak gepleegd, waarbij de slachtoffers het gezicht van de daders niet konden zien, laat staan herkennen. Zij hebben daartegen bij de daders wel enkele in het oog springende lichaams- en gedragskenmerken opgemerkt, zoals een bepaald gewicht en grootte van de persoon of diens wijze van bewegen. De politie zou er kunnen aan denken om de daders mede via *FRT* op te sporen … Dergelijke toepassingen moeten voor het COC wel degelijk kunnen in een opsporingscontext, mits, zoals hiervoor gesteld, voorzien in een duidelijke en specifieke wettelijke basis omringd met de nodige waarborgen. Of is het de bedoeling van de stellers van de resolutie om ook deze vorm van 'gerichte' opsporing aan een moratorium te onderwerpen, of zelfs aan een volledige verbod?

Dit zijn voorbeelden van *FRT* met een verwerking van specifieke (types van) biometrische persoonsgegevens waarbij 1) de omstandigheden waarin en de voorwaarden waaronder naar gelang de specifieke biometrische gegevens die worden verwerkt en 2) de specifiek technologische vereisen waaraan de *AI* moet voldoen, heel wat vragen oproepen en niet op basis van één algemene bepaling in de wet afdoende kunnen geregeld worden (zoals actueel het geval is in artikel 44/1 §2, 1° WPA, knelpunt waarvoor de stellers van het nieuwe artikel 44/1 § 2, 1° WPA in 2019[56] wellicht geen aandacht zullen hebben gehad).

Noodzakelijkheid en proportionaliteit

[56] De juridische grondslag voor de GPI om biometrische gegevens te verwerken werd ingevoerd door de Wet van 22 mei 2019. tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft.

30. Elk *FRT* en elk biometrisch herkenningssysteem zal de test van de noodzakelijkheid en proportionaliteit moeten doorstaan. Een verwerking kan alleen als 'strikt noodzakelijk' worden beschouwd als de inmenging in de bescherming van persoonsgegevens en de beperkingen ervan beperkt is tot wat absoluut noodzakelijk is[57]. De toevoeging van het begrip 'strikt' betekent dat de wetgever de verwerking van bijzondere categorieën gegevens (zoals biometrische gegevens) alleen toelaat onder voorwaarden die nog strenger zijn dan de voorwaarden voor de 'gewone' noodzakelijkheid. Dat geldt nog des te meer bij geautomatiseerde verwerkingen.

Om de beoordeling van de noodzakelijkheid en evenredigheid van wetgevende maatregelen met betrekking tot gezichtsherkenning op het gebied van rechtshandhaving te vergemakkelijken en te operationaliseren, kunnen de nationale en Uniewetgevers alvast gebruik maken van de beschikbare praktische instrumenten die speciaal hiertoe werden ontworpen, zoals de *toolkit* en de richtlijnen van de *EDPS*[58].

Technologische transparantie.

31. Het actuele gebrek aan technologische transparantie van *AI* systemen en de gebruikte algoritmen is ongetwijfeld één van de grootste te nemen hindernissen.

De directeur van het *FRA* verwoordt het als volgt: "*It means we need to know what is in the algorithms. We need to know the content of machine training data. And again, the point needs to be made repeatedly and loudly, because, there is a pushback from parts of the industry. We are hearing voices, for instance, saying it is too difficult, it is too complicated, it is too hard to understand and therefore we cannot deliver on transparency*." Het Controleorgaan sluit zich daarbij aan, net zoals het FIRM de

---

[57] Vaste rechtspraak betreffende het grondrecht van het recht op privacy; zie o.a. HvJ nr. C73/07, Satakunnan Markkinapörssi and Satamedia, §56; HvJ nrs. C92/09 en C93/09, Schecke and Eifert, §§ 74, 77 en 86; HvJ nr. C/293/12 en C/594/12, Digital Rights, §§ 46, 52, 56, 62, 64 en 65 ; HvJ, nr. C/362/14, Schrems, §§ 92 en 93; HvJ nr. C/311/18, Schrems, §§ 167 en 176. Zie bijvoorbeeld inzake dit laatste arrest C/311/18: "*Ten slotte moet de betrokken regeling die de inmenging bevat, om te voldoen aan het evenredigheidsbeginsel volgens hetwelk de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke moeten blijven, duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de maatregel bevatten die minimale eisen opleggen, zodat degenen van wie de gegevens zijn doorgegeven over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik. Zij moet in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt".*

[58] "*Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit*" (11.4.2017); zie ook "*EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*" (19.12.2019), www.edps.europa.eu

noodzaak tot transparantie onder meer rond autonome leercapaciteit van algoritmische verwerkingen benadrukt[59].

32. Al te vaak stelt ook het COC in de praktijk trouwens vast dat de mensen op het terrein binnen de GPI de werking van de technologische middelen die ze inzetten onvoldoende tot niet kunnen uitleggen of zien we dat men de werking zelf niet echt begrijpt. Dat geldt reeds voor de actuele 'gewone' cameraverwerkingen en het laat zich raden wanneer complexe, door algoritmen aangestuurde, *FRT* systemen hun intrede zouden doen. De onderzoeken die het COC in zijn driejarig bestaan reeds heeft gedaan (sinds het ook een gespecialiseerde dataprotectie autoriteit is) waarin – *contra legem* – gezichtsherkenningstechnologie werd gebruikt, met name het onderzoek bij de luchthavenpolitie van Brussel Nationale Luchthaven (DGA/LPA) van de federale politie en het gebruik van de *Clearview* technologie door de centrale directie van de bestrijding van de zware en georganiseerde criminaliteit (*DJSOC*) van de Algemene Directie Gerechtelijke Politie van de federale politie tonen dat glashelder aan.

In een *AI/FRT* context betekent die transparantie naar de rechtsonderhorige ook "*the dimension of making people aware that they have been subject to the application of technology that has impacted their life*"[60]. Ook dat aspect zal op één of andere wijze zijn regelgevende en praktische weerslag moeten krijgen.

D. Rol en belang van de toezichthouder

33. Het belang van efficiënt werkende dataprotectie autoriteiten zal alleen maar belangrijker worden bij de uitrol van allerhande biometrische (gezichts)herkenningssystemen van natuurlijke personen. Dat is des te meer het geval in een *law enforcement* context. Het COC verwijst ten overvloede naar de toekomstige rol van die dataprotectie autoriteiten, waaronder dus het Controleorgaan, met betrekking tot de controle op *AI* systemen zoals voorzien door de *AIA*. De *AIA* voorziet in artikel 59.1 dat "*nationale bevoegde autoriteiten door elke lidstaat moeten worden opgericht of aangewezen met het oog op het waarborgen van de toepassing en uitvoering van deze verordening*". In hun gezamenlijke opinie pleiten de *EDPB* en *EDPS* ervoor dat "*DPAs should be designated as the national supervisory authorities pursuant to Article 59 of the Proposal*"[61]. Ook de reeds vermelde *FRA* directeur Michael O'Flaherty citeert als 5e essentiële beginsel, vooraleer de uitrol van *AI/FRT* wordt overwogen, het

[59] Federaal Instituut voor de bescherming en bevordering van de rechten van de mens, https://federaalinstituutmensenrechten.be, publicaties/adviezen, p. 10

[60] Ibid, https://fra.europa.eu/en/speech/2021/data-protection-policing.

[61] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 june 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), zie p. 14 en 15, nrs. 47 en 48.

belang van de rol van de toezichthouder: "*Fifth, we need independent oversight of the use of high-risk technologies. ... Oversight bodies also need to be given adequate resources and training*.[62]"

34. Vooral dat laatste aspect van afdoende mensen en middelen is belangrijk en baart het COC wat zorgen. Het COC heeft sinds zijn doorstart en bijkomende opdracht als bijzondere (politionele) gegevensbeschermingsautoriteit, waarbij ze deze taken en dossiers heeft overgenomen van de GBA, in 2018 geen euro aan bijkomende middelen gevraagd en dit terwijl er op dat korte tijdspanne heel wat bijkomende taken aan het COC zijn toebedeeld en sowieso het volume aan dossiers jaar na jaar toeneemt. De burger is zich immers duidelijk steeds meer bewust van zijn rechten in het algemeen en zijn recht op privacy en gegevensbescherming – ook in de *law enforcement* sector – in het bijzonder, wat op zich evident een zeer goede evolutie is, maar waar anderzijds onvermijdelijk een *issue* van mensen en middelen tegenover staat. Het volstaat te verwijzen naar de twee reeds door het COC gepubliceerde jaarrapporten (2016-2019 en 2020) om die vaststelling te maken. Voor 2021 geven we slechts één cijfer mee: het aantal verzoeken onrechtstreekse toegang tot de politionele databanken – reactieve dossiers die een belangrijk deel van de capaciteit hypothekeert - bedroeg in 2021 niet minder dan 547. Dat is ten opzichte van 2020 quasi een verdubbeling en sowieso een bijzonder forse stijging ten opzichte van de drie voorgaande jaren zoals onderstaande tabel aantoont:

Jaar	**Aantal dossiers onrechtstreekse toegang**
2018	333
2019	392
2020	283
2021	547

Het kader van het COC is sedert zijn opstart op 5 september 2018 niet gewijzigd, noch werden meer kredieten bekomen. De voormelde substantiële volumestijgingen alleen al zijn derhalve steeds opgevangen binnen de huidige middelen door voortdurend efficiënter te gaan werken, meer prioriteiten te stellen en minder proactief te gaan, maar de limieten zijn thans bereikt. Denken we ook aan de nieuwe en bijzonder belangrijke bevoegdheid die het COC binnenkort bijkomend zal dienen op te nemen in het kader van de nieuwe dataretentie wetgeving (met name de controle van de statistieken op grond waarvan de gegevensbewaring van de telefoniedata territoriaal zal worden vastgelegd en het nazicht van de vorderingen van de operatoren door de Cel Verdwijningen van de federale politie)[63]. Naast het grote volume aan dossiers onrechtstreeks toezicht (dat ongetwijfeld bij

[62] Eigen onderlijning door het Controleorgaan.

[63] Persberichten Ministerraad, "*Bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie -Tweede lezing*", https://news.belgium.be/nl; zie ook advies DA210014 van 21 mei 2020 van het COC op het voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie -, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten en het ontwerp van Koninklijk besluit tot

implementatie van *FRT* nog omhoog zal gaan) moet nog melding gemaakt worden dat eenzelfde evolutie in meer of mindere mate zich voordoet bij de andere louter reactieve dossiers zoals:

- algemene adviezen inzake dataprotectie, camera, e.a;
- de adviezen *DPIA* als gevolg van aangemelde *DPIA*;
- de aangemelde *databreaches*;
- de notificaties niet zichtbaar cameragebruik;
- de adviezen op wet- en regelgeving;
- de te voeren rechterlijke procedures (actueel drie procedures waarin het COC zelf zeer substantieel moeten investeren, gezien de zeer gespecialiseerde materie);
- de klachten;
- …

35. Daarnaast zijn er de eigen, hetzij ambtshalve, hetzij op vraag van de bestuurlijke of gerechtelijke overheden gevoerde (proactieve) eigen globale toezichtonderzoeken die onder de reactieve dossiers meer en meer te lijden hebben (en wat toch de *core business* van het COC is of zou moeten zijn). Zo doet het COC op vraag van de procureur des Konings te West-Vlaanderen een omvangrijk toezichtonderzoek binnen een lokale politiezone enerzijds, wordt volop gewerkt aan het door de Ministers van Binnenlandse Zaken en Justitie gevraagde 'Salduz' onderzoek bij de hele GPI rond het camera- en audiogebruik tijdens of naar aanleiding van het vertrouwelijk overleg advocaat-cliënt en is er het reeds gemelde *Clearview* onderzoek. Dit soort onderzoeken vragen heel wat (technische) capaciteit. De één (1) ICT'er die het COC thans heeft is actueel ruimschoots ontoereikend ook al omdat hij te veel tijd moet spenderen aan de eigen COC ICT-omgeving. Het aantal politieambtenaren (twee) binnen het COC is dat evenzeer. Dat is dan nog buiten beschouwing gelaten, allerhande verzoeken om opleidingen te geven aan de GPI (bv. aspirant-commissarissen of kandidaat brevethouders hoofdcommissaris), studenten te woord te staan in het kader van bachelor of masteropleidingen, heel wat *awareness* en technische meetings met de GPI korpsen zelf, enz. … Over de laatste jaren zijn daar nog opdrachten bijgekomen die hetzij reeds in uitvoering zijn (vb. de controle op de *BELPIU* vorderingen van de douane, controle op de GGB terrorisme, algemeen toezicht op de werking van de *BELPIU*, …), die zullen komen als gevolg van beslist beleid (bv. het elektronisch PV[64]),

---

wijziging van het Koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, www.controleorgaan.be

[64] Koninklijk besluit van 18 juli 2021 betreffende de veiligheidsmaatregelen en de minimale technische normen voor de informaticasystemen van de politie die het geavanceerde elektronisch zegel produceren, en de vermeldingen die in het geavanceerde elektronisch zegel en de gekwalificeerde elektronische handtekening voorkomen, BS, 13.08.2021. Het auditverslag - betreffende de veiligheidsmaatregelen en de technische normen van de politie-informaticasystemen die het geavanceerd elektronisch zegel produceren en die het mogelijk moeten maken een niveau van vertrouwelijkheid, beschikbaarheid, integriteit, betrouwbaarheid, authenticiteit en onweerlegbaarheid van de elektronische handtekeningendienst van de politie te waarborgen - moet door de federale politie worden toegezonden aan het Controleorgaan op de politionele

die zullen komen als op handen zijnde beleid (cf. opdracht inzake dataretentie telefoniegegevens) of die mogelijks zullen komen (het hele *FRT* gebeuren voor politionele doeleinden).

36. De Gegevensbeschermingsautoriteit (GBA) is bijvoorbeeld op 3 jaar tijd van een dotatie van zo'n 5.500 KEUR naar een dikke 9.064 KEUR gegaan (bijna een verdubbeling) met bijhorende recruteringen. Het Controleorgaan zit nog steeds ongewijzigd sedert 9/2018 op 1.288 KEUR dotatie (met een reële uitgave van 1.696 KEUR). Alleen al de loonmassa van de actueel elf leden en personeelsleden (3 DIRCOM leden en 8 personeelsleden) is even groot als de door het parlement toegekende dotatie. De rest van de uitgaven (werking en investeringen) wordt gefinancierd met nog resterende opgebouwde reserves uit het verleden (opgebouwd als gevolg van vertrek van personeelsleden die niet of sterk vertraagd vervangen werden of gewoon niet aangeworven werden) die thans slinken en een snel aflopend verhaal zijn. Een "boosterprik" voor het COC is dan ook noodzakelijk.

37. Het is essentieel dat de burger die zich in zijn rechten of rechtspositie geïmpacteerd ziet door een *AI/FRT* toepassing, daartegen een doeltreffende voorziening of een zgn. "*remedy*" heeft. Ook om die reden dient de toezichthouder over afdoende mensen en middelen te beschikken, in deze ook IT middelen en digitale expertise. Als toezichthouder dient ook het COC de nodige technische expertise in huis te hebben. Om al deze redenen wil het COC de absolute aandacht van het parlement trekken op de noodzaak voor het COC om over voldoende experten en middelen (waaronder vooral meer technische ICT en digitale expertise) te beschikken.

E. Besluit

38. Het COC kan zich alvast volledig vinden in de resolutie waar die stelt dat "*al die elementen pleiten voor een grote omzichtigheid met betrekking tot het gebruik van dergelijke toezichtsystemen met gezichtsherkenningscamera's in België*"[65]. De vraag moet dus ook gesteld worden of het überhaupt zinvol of opportuun is dat op lidstatelijk (Belgisch) niveau reeds gelegifereerd zou worden – althans met als doelstelling tot een definitieve wetgeving rond *AI* of *FRT* te komen - vóóraleer de definitieve tekst van de Europese AI-verordening is komen vast te staan. Hoe dan ook moet een eventuele nationale wetgeving wijken voor en rekening houden met de hogere internationale rechtsnorm die een EU-verordening is. Hoe dan ook kan er juridisch door de nationale wetgever niet meer opgetreden worden voor die aspecten die reeds uitdrukkelijk geregeld zijn door de Verordening. Indien de *AIA* bv. een algemeen verbod zou voorzien op enige vorm van *real time FRT* in openbare plaatsen, dan kan de Belgische wet dat evident niet meer voorzien. Daarnaast is het risico niet denkbeeldig dat beide

informatie, dat zelf ook die maatregelen en technische normen kan evalueren (zie art. 10 KB en Verslag aan de Konings, onder punt I, "Algemene Inleiding").

[65] Resolutie, p. 13

teksten verschillen zouden opleveren die niet overbrugbaar zijn of dat investeringen worden gedaan op grond van nationale wetgeving die zinloos zijn geworden omdat het EU kader één en ander niet zou toelaten, of, omgekeerd, dat verzuimd wordt investeringen te doen omdat een nationaal kader, in tegenstelling tot de EU-regelgeving, bepaalde toepassingen niet mogelijk zou maken.

Het komt het COC derhalve voor dat een Belgisch wetgevend initiatief, onder voorbehoud van een te creëren kader rond testomgevingen of proefprojecten (zie verder), **niet** aangewezen is en derhalve **een moratorium op een voorbarig wettelijk ingrijpen, minstens op het daadwerkelijk gebruik ervan voor een te bepalen termijn opportuun is**. Dit standpunt sluit ook aan bij de oproep van de *EDPB* en de *EDPS*.

In die zin heeft het COC een toch wat andere insteek dan bv. het FIRM dat stelt dat "*het noodzakelijk is dat de federale wetgever zo snel mogelijk*[66] *een voorstel van wetgeving opstelt dat garanties biedt voor de transparantie wat betreft het gebruik van systemen van artificiële intelligentie door alle federale overheden, niet enkel de bestuurlijke overheden*"[67]. Voor wat de politie betreft is het COC eerder gewonnen voor het in de resolutie voorgesteld moratorium onder voorbehoud van het hierna vermelde wat test- en proefprojecten betreft, alsmede de te voorziene termijn. Daarnaast pleit het COC hoe dan ook voor een specifieke regeling of wetgeving voor *law enforcement* doeleinden in het algemeen en zeker voor politionele doeleinden in het bijzonder.

39. Een tweede vraag is of ook elk louter reactief gebruik van *FRT* voor opsporingsdoeleinden moet bevroren worden, uitgaande van de hypothese dat er een behoorlijk wettelijk kader voorhanden zou zijn. Het COC is hier meer genuanceerd. In het kader van een door het parket of onderzoeksrechter geleid vooronderzoek in strafzaken moet het voor het COC mogelijk zijn aan de hand van *FRT* daders of slachtoffers te identificeren en/of authentificeren. Het *Clearview* onderzoek heeft aangetoond, voor zoveel als nodig, *quod non*, welke gigantische (ook internationale) criminaliteitsproblematiek en uitdaging het opsporen en vervolgen van bijvoorbeeld kinderpornografie en kindermisbruik is. Maar ook andere fenomenen zoals mensenhandel en georganiseerde criminaliteit zouden ongetwijfeld belangrijke criminaliteitsdomeinen kunnen zijn (ook ter identificatie van slachtoffers). Dat daarbij dus *tools* worden gezocht om meer en betere (opsporings)resultaten te halen, beoordeelt het COC als absoluut legitiem. Mits de creatie van een heldere wetgeving en de nodige *checks en balances*, met een dataprotectie toezichthouder en met tussenkomst van de magistraat en rekening houdende met de grendels en drempels voorzien in het Belgisch strafprocesrecht (die eventueel moeten verstrekt worden) moet dit zeker kunnen overwogen worden.

---

[66] Onderlijning door het COC.

[67] Federaal Instituut voor de bescherming en bevordering van de rechten van de mens, https://federaalinstituutmensenrechten.be, publicaties/adviezen, p.9, aanbeveling 4.

40. Een derde vraag is daarbij of dit betekent dat elke vorm van testomgeving, testfase of proefproject met *FRT* moet bevroren worden. Ook hier is het Controleorgaan genuanceerd. Het COC is in beginsel zelfs gewonnen voor een dergelijk beperkt regelgevend kader. Het staat immers vast dat er nog zeer weinig objectief evaluatiemateriaal voorhanden is rond het gebruik van deze technologie. Enkel de proefondervindelijke toepassing in de praktijk kan dit majeure euvel, waarbij niemand echt zicht heeft op de meerwaarde en de prestaties van dergelijke systemen, verhelpen. Dat betekent echter dat de GPI, onder strikte voorwaarden en met transparantie, zou moet kunnen experimenteren met deze technologie op *live* gegevens zonder meteen in de illegaliteit te belanden. De mate van inbreuk op de persoonlijke levenssfeer bij toepassing van *FRT* op, bijvoorbeeld, foto's van verdachten en slachtoffers die conform de wettelijke voorwaarden van de WPA (en eventueel het Wetboek van Strafvordering) worden verwerkt, is van een andere orde dan de ongerichte toepassing van *FRT* op publieke plaatsen.

41. Het voorstel van *AIA* voorziet in de artikelen 53 e.v. in de ontwikkeling van *AI* testomgevingen voor regelgeving. Deze regelgeving moet voorzien in een gecontroleerde omgeving ter vergemakkelijking van het ontwikkelen, testen en valideren van innovatieve *AI*-systemen. Deze AI-testomgevingen voor regelgeving laten de toezichthoudende en corrigerende bevoegdheden van de bevoegde autoriteiten onverlet. Significante risico's voor de gezondheid en veiligheid en de grondrechten die tijdens het ontwikkelen en testen van dergelijke systemen worden vastgesteld, moeten onmiddellijk worden beperkt en leiden bij gebreke daarvan tot de opschorting van het ontwikkelings- en testproces totdat beperkende maatregelen worden getroffen (art. 53.3). De modaliteiten en de voorwaarden van de werking van de *AI*-testomgevingen voor regelgeving, waaronder de toelatingscriteria en de procedures voor de toepassing en selectie van, deelname aan en terugtrekking uit de testomgeving, en de rechten en plichten van de deelnemers worden in uitvoeringshandelingen van de Europese Commissie uiteengezet (art. 53.6). Artikel 54.1 (a) i) voorziet de toepassing van deze *AI* testomgeving voor regelgeving ook voor doeleinden van *law enforcement*, zij het dat ook verwezen wordt naar toepasselijke nationale wetgeving (dus door België nog te ontwikkelen). Art. 54.1 (c) voorziet dat "*er doeltreffende monitoringmechanismen* (zijn) *om vast te stellen of zich tijdens de experimenten in de testomgeving hoge risico's voor de grondrechten van de betrokkenen kunnen voordoen evenals responsmechanismen om die risico's onmiddellijk te beperken en indien nodig de verwerking stop te zetten*". De doorslaggevende rol en het belang van de toezichthouder treedt hier dus weer op de voorgrond.

42. Hoewel er dus ook voorzien zal worden in Europese regelgeving rond deze *sandboxes* of testomgevingen is het toch maar de vraag of de Belgische regelgever daarop moet wachten. Deze proeftuinen dienen hoe dan ook een interne wettelijke grondslag te krijgen. Het nut en zelfs de noodzaak van testen lijkt het COC niet voor veel discussie vatbaar. Pas na een afdoende aantal testfases en proeven te hebben doorlopen kan beter zicht gekregen worden op percentages vals positieven, vals negatieven, welke soort van *biass* zich voordoet, welk bijkomende grendels, drempels,

of andere waarborgen noodzakelijk zijn, enz. …. Deze *lessons learned* kunnen en moeten dan meegenomen worden in een definitieve nationale (of Europese) wetgeving. Deze nationale wetgeving zal, bij het gebruiken van *LED* verwerkingen en persoonsgegevens in de testomgeving, weliswaar volledig onder de AVG vallen zoals de *EDPB* en *EDPS* terecht in hun opinie hebben gesteld[68]. Voor wat de GPI betreft blijft het COC evenwel de bevoegde toezichthouder.

43. Het COC is dan ook voorstander van de ontwikkeling van een eigen intern wetgevend kader en stelt dus voor om niet te wachten op eventuele aankomende Europese regelgeving rond testomgevingen voor het gebruik ervan door de geïntegreerde politie, waarin het COC een rol kan spelen, bijvoorbeeld in een systeem van voorafgaande machtiging dat evident wel nadere studie en uitwerking vraagt.

OM DEZE REDENEN,

Het Controleorgaan op de Politionele Informatie,
verzoekt kennis te nemen van alle elementen van dit advies.

Aldus goedgekeurd door het Controleorgaan op de Politionele Informatie op 24 januari 2022.

Voor het Controleorgaan,

De voorzitter,
Philippe ARNOULD

[68] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 juni 2021, https://edps.europa.eu/Opinions | European Data Protection Supervisor (europa.eu), zie p. 18, nr. 66.