



CONTROLEORGaan OP DE POLITIEInFORMATIE

Uw referentie

Onze referentie

Bijlage(n)

Datum

DA240032

23.10.2024

Betreft: Advies betreffende een ontwerp van gemeenschappelijke dwingende richtlijn van de ministers van Justitie en van Binnenlandse Zaken aangaande de koppeling van de ISLP-basisgegevensbanken via de tool PoliceSearch@GPI (GPI 105).

Het Controlegeorgaan op de politie informatie (hierna afgekort 'COC' of 'Controlegeorgaan').

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 'WVG') inzonderheid het artikel 59 §1, 2^e lid, artikel 71 en Titel 7, inzonderheid artikel 236.

Gelet op de wet van 3 december 2017 tot oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort 'WOG'), inzonderheid artikel 4 § 2, 4^{de} lid:

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna 'WPA').

Gelet op de *Law Enforcement Directive* 2016/680 van 27 april 2016 (hierna '*LED*').

Gelet op het verzoek van de ministers van Justitie en van Binnenlandse Zaken door het Controlegeorgaan ontvangen op 27 augustus 2024 om een advies te verstrekken op een ontwerp van gemeenschappelijke dwingende richtlijn van de ministers van Justitie en van Binnenlandse Zaken aangaande de koppeling van de ISLP-basisgegevensbanken via de tool PoliceSearch@GPI (GPI 105) ;

Gelet op het Advies van 12 december 2022 van het Controlegeorgaan op de politie informatie betreffende de gegevensbeschermingseffectbeoordeling met betrekking tot PoliceSearch@GPI, niet openbaar gemaakt;

Gelet op het verslag van de heer Ronny Saelens, Lid-Raadsheer *a.i.* van het Controlegeorgaan.

Brengt op 23 oktober 2024 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 2016/679¹ en de Richtlijn 2016/680² heeft de wetgever de taken en opdrachten van het Controleorgaan grondig gewijzigd. Artikel 4 § 2, vierde lid, van de organieke wet van 3 december 2017 betreffende de oprichting van een Gegevensbeschermingsautoriteit (hierna afgekort '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. Het betekent onder meer dat het Controleorgaan ook bevoegd is wanneer politiediensten persoonsgegevens verwerken die buiten de opdrachten van bestuurlijke en gerechtelijke politie vallen, bijvoorbeeld in het kader van sociaaleconomische doeleinden of human resources verwerkingen. 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, 2^e lid en 236 §2 WVG, artikel 36.4 van de AVG en artikel 28.2 van de Richtlijn politie-justitie). 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 2 (voor de operationele verwerkingen) van de WGB⁴. Daarnaast heeft het COC ook een ambtshalve adviesopdracht voorzien in artikel 236 §2 WVG en een algemene voorlichtingsopdracht van het brede publiek, betrokkenen, verwerkingsverantwoordelijken en verwerkers in de materie van het privacy – en gegevensbeschermingsrecht voorzien in artikel 240 WVG.

2. Wat betreft derhalve in het bijzonder de verwerkingsactiviteiten in 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 politieambt⁵.

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 en Justitie' of *Law Enforcement Directive (LED)*).

³ Artikel 4 §2, 4^e lid WOG.

⁴ Artikel 71 §1, 3^e lid WVG.

⁵ Artikelen 59 §1, 2^e lid en 236 § 2 WVG.

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 verleend⁶.

4. Het Controleorgaan is 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 persoonsgegevens*" 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.

5. Het COC is tot slot ook belast, in het kader van de dataretentie wetgeving, op grond van artikel 126/3 §1, 8^e lid van de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna afgekort 'WEC'), zoals gewijzigd door de wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten (*BS* van 8 augustus 2022), met de validatie van de statistieken met betrekking tot het aantal strafbare feiten en de bewaringstermijn voor elk gerechtelijk arrondissement en elke politiezone in het kader waarvan het al zijn bevoegdheden uitoefent die hem zijn toegekend bij titel 7 van de wet van 30 juli 2018. Het is daarnaast ook nog belast, in toepassing van artikel 42 § 3, 2^{de} en 3^{de} lid WPA met de controle van de vorderingen van de Cel Vermiste Personen van de federale politie tot opvraging van de gegevens met betrekking tot de elektronische communicatie betreffende de vermiste persoon.

6. Het Controleorgaan is bevoegd om advies te verlenen over aspecten met betrekking tot de verwerking van informatie en persoonsgegevens en de bescherming van het privéleven door de verwerking van persoonsgegevens voor zover deze betrekking hebben op of in verband staan met de operationele en niet-operationele werking van de politiediensten en/of het personeel van de geïntegreerde politie (hierna 'GPI'⁷) en/of voor zover de voor advies voorgelegde ontwerp tekst een impact heeft op de politieke informatiehuishouding in het algemeen.

⁶ Artikel 71 §1, derde lid *juncto* 236 § 3 WVG.

⁷ Geïntegreerde politie – Police Intégrée.

7. Het Controleorgaan is daarnaast niet enkel een gegevensbeschermingsautoriteit maar een toezichthouder die evenzeer wettelijk belast is met de legaliteit, efficiëntie, effectiviteit en economie van de politionele informatiehuishouding⁸.

II. Voorwerp van de aanvraag en voorgaanden

8. Het ontwerp van gemeenschappelijke dwingende richtlijn van de ministers van Justitie en van Binnenlandse Zaken (hierna 'het ontwerp van richtlijn') heeft tot doel om een oplossing te bieden voor de huidige situatie waarin de basisgegevensbanken van de politiediensten van elkaar losstaan zonder dat er een technische verbinding tussen deze gegevensbanken wordt gemaakt. Zoals in het ontwerp van richtlijn wordt opgemerkt, hebben de politiezones en de entiteiten van de Algemene directie van de bestuurlijke politie hun eigen (lokale) basisgegevensbanken, het zogenaamde ISLP (*Integrated System for the Local Police*), die niet met elkaar verbonden zijn waardoor de politionele gegevens (informatie en persoonsgegevens) niet rechtstreeks toegankelijk zijn voor de andere politie-entiteiten⁹. Om de politionele gegevens in de diverse ISLP's rechtstreekse toegankelijk te maken voor de geïntegreerde politie (GPI¹⁰), werd de 'tool'/applicatie PoliceSearch@GPI ontwikkeld.

9. Zoals in het ontwerp van richtlijn wordt opgemerkt¹¹, werd een Gegevensbeschermingseffectbeoordeling opgemaakt en het Controleorgaan geraadpleegd in toepassing van art. 59 §1 WVG. In dat verband werden door het Controleorgaan een aantal aanbevelingen uitgebracht in zijn advies van 12 december 2022¹². Het Controleorgaan stelt vast dat in het ontwerp van richtlijn de aanbevelingen in rekening worden gebracht¹³.

III. Opmerkingen

10. Volgens de stellers van het ontwerp van richtlijn is de tool 'PoliceSearch@GPI' een belangrijke stap in de tenuitvoerlegging van een aanbeveling van de parlementaire onderzoekscommissie naar de terroristische aanslagen van 22 maart 2016 teneinde "*de verzuiling van informatie en dus het gebrek aan informatiedeling te verhelpen*"¹⁴. Volgens de stellers "*pleit de parlementaire onderzoekscommissie*

⁸ Activiteitenverslag 2021, randnummers 3, 52 en in het bijzonder 71: "*Het COC heeft echter allerm minst alleen oog voor dataprotectie; het heeft evenzeer veel aandacht en is bevoegd voor alle andere operationele aspecten van de politionele informatiehuishouding*"; www.controleorgaan.be artikel 71 §1 WVG.

⁹ Ontwerp van richtlijn, p. 2.

¹⁰ Geïntegreerde politie – Police Intégrée.

¹¹ Ontwerp van richtlijn, p. 7.

¹² Advies DI220014 van 12.12.2022 betreffende de gegevensbeschermingseffectbeoordeling met betrekking tot *Police Search* GPI, niet gepubliceerd.

¹³ Dit valt uit het ontwerp van richtlijn af te leiden, p. 7-8.

¹⁴ Ontwerp van richtlijn, p. 2.

duidelijk voor een cultuuromslag”, onder meer in die zin dat “*we het 'need to know' -principe moeten vervangen door het 'need to share' -principe (...)*”¹⁵. (onderlijning COC)

11.1. Dat de voormelde onderzoekscommissie zou hebben gepleit voor het “***vervangen***” (“*remplacer*”), moet evenwel sterk genuanceerd worden en in perspectief worden geplaatst. Het eerste vermelde principe staat immers niet in de weg van het twee vermelde principe, wat overigens ook blijkt uit punt 3.3. van het ontwerp van richtlijn. Vandaar dat de onderzoekscommissie ‘duidelijk’ stelt dat tussen beide principes een evenwicht moet worden gezocht¹⁶. De interpretatie van de stellers van het ontwerp is bovendien in die zin zeer merkwaardig nu, in weerwil van hun interpretatie van de visie van de parlementaire onderzoekscommissie van **2016**, de (Europese) wetgever in **2018** en **2019** het principe van *need to know* in de Europese wetgeving, enerzijds, en (omgezet) in de WVG en de WPA, anderzijds, stevig heeft verankerd (artikelen 56 WVG en 44/2 § 2 WPA). In die zin moet er rekening mee worden gehouden dat de uit 2016 daterende gedane aanbevelingen van de toenmalige onderzoekscommissie, naast het feit dat het inderdaad louter om ‘aanbevelingen’ gaat, er logischerwijze, ook geen rekening werd gehouden met de nadien tot stand gekomen dwingende Europese en Belgische wet- en regelgeving die uiteraard thans voorrang genieten.

11.2. Het *need to share* principe is één van de essentiële aspecten van een efficiënte informatieverwerking door de politiediensten, terwijl het *need to know* principe in verband staat met de rechtmatigheid en wettelijkheid van de verwerking (verwerkingsbevoegdheid) in functie van de rol en het uitgeoefende ambt van het lid van de geïntegreerde politie (gegevensbeschermingsrechtelijk). Het ene principe staat dus niet in de weg van het andere principe. Integendeel, ze zijn complementair, hoewel, de in de hiërarchie der normen, evident de wettelijkheid en rechtmatigheid (zoals opgenomen in de Europese en nationale normen) boven de operationele efficiëntie staat. Een bepaalde gewenste politionele verwerking mag nog zo efficiënt zijn of lijken, zij moet voorafgaandelijk en in de eerste plaats wettelijk en rechtmatig zijn.

12. Volgens de stellers van het ontwerp van richtlijn “(biedt) *de tool een oplossing voor de huidige situatie waarin die basisgegevensbanken 'informatie-eilanden' zijn die losstaan van elkaar zonder technologische bruggen ertussen*”¹⁷.

Om drie hierna vermelde redenen komt dit argument het Controleorgaan vreemd voor.

Ten eerste is het de Belgische wetgever zelf die in 2014 de bewuste en uitdrukkelijke keuze heeft gemaakt om (1) het bewaren van politionele gegevens (informatie en persoonsgegevens) in de

¹⁵ Ontwerp van richtlijn, p. 3., met verwijzing naar het parlementair verslag van deze onderzoekscommissie: Parl. St. Kamer 2016-2017, nr. 54-1752/008, 258.

¹⁶ Ibidem.

¹⁷ Ontwerp van richtlijn, p. 2.

daartoe specifiek opgerichte operationele gegevensbanken vast te leggen en (2) de basisgegevensbanken als 'eilanden'¹⁸ te beschouwen, wat niet meteen uiting geeft aan het principe van een 'geïntegreerde' politie, dat noodzakelijkerwijs ook een 'geïntegreerde informatiehuishouding' veronderstelt.

Ten tweede brengt het 'koppelen' van de basisgegevensbanken door middel van een 'tool' daarin geen verandering, behalve dan op louter operationeel vlak. Zoals het stellers van het ontwerp van richtlijn opmerken, wordt sinds 2021 de onderlinge koppeling tussen deze gegevensbanken en andere waartoe de politiediensten wettig toegang hebben, nader geregeld door de gemeenschappelijke dwingende richtlijn van de ministers van Justitie en van Binnenlandse Zaken van 4 augustus 2021. De rechtsgrond van deze richtlijn is vastgelegd in artikel 44/4 § 4 van de WPA¹⁹. In de hypothese dat de basisgegevensbanken geen 'informatie-eilanden' zouden zijn, maakt dit een gemeenschappelijke bindende richtlijn van beide politieministers op zich niet overbodig, integendeel. Als we op basis van dezelfde hypothese ervan uitgaan dat de politiediensten, onder voorwaarden, in principe toegang zouden moeten (kunnen) hebben tot politionele gegevens die door de geïntegreerde politie in (geïntegreerde) politiesystemen worden verwerkt, dan kan de vaststelling van de nadere operationele spelregels in een bindende richtlijn van de politieministers ongetwijfeld bijdragen tot een geïntegreerd politioneel verwerkingsbeleid.

Ten derde is, in het raam van de functionaliteiten van de MFO6²⁰, sinds 2014 reeds een tool ter beschikking ten behoeve van de SICAD-AIK²¹, die iedere dag een statische flow van de ISLP gegevens overmaakt van de politiezones en de lijnseenheden van DGA²² naar de arrondissementeel bevoegde AIK (de zogenaamde "24uurs flux") die verder verwerkt werd in de toepassing "Infosuite". Bovendien hadden voor de invoering van de 24uurs flux en Infosuite de meeste SICAD-AIK reeds toegangsrechten op de ISLP basisgegevensbanken van de politiezones van hun arrondissement. Dit vloeide voort uit artikel 23 van de Wet van 18 maart 2014²³ dat artikel 44/11/2 WPA m.b.t. de basisgegevensbanken. Met andere woorden, de notie "informatie-eilanden" moet met de nodige nuance worden begrepen.

¹⁸ Zoals de stellers van het ontwerp van richtlijn de wettelijke regeling van de operationele gegevensbanken omschrijven (p. 2, ontwerp van richtlijn).

¹⁹ Gemeenschappelijke bindende richtlijn van de ministers van Justitie en van Binnenlandse Zaken aangaande de nadere regels betreffende de koppeling van de gegevensbanken bedoeld in artikel 44/2 of met andere gegevensbanken waartoe de politiediensten toegang hebben door of krachtens de wet of internationale verdragen die België binden.

²⁰ Gemeenschappelijke en dwingende richtlijn MFO-6 van de Ministers van Justitie en Binnenlandse Zaken van 9 januari 2003 betreffende de werking en organisatie van de arrondissementele informatiekruispunten.

²¹ De Arrondissementele Informatiekruispunten als onderdeel van de Communicatie- en Informatiedienst van het Arrondissement (SICAD) voor het verwerken van de informatie in tweede lijn, volgend op het *real time* gebeuren.

²² Algemene directie van de bestuurlijke politie.

²³ Wet van 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering

A) Wat is de 'tool' PoliceSearch@GPI ?

13. PoliceSearch@GPI wordt door de stellers van het ontwerp van richtlijn voorgesteld als een 'tool' die opzoeken in zowel gestructureerde als niet gestructureerde gegevens van de ISLP basisgegevensbanken mogelijk maakt op basis van een nationale en lokale indexering van politionele gegevens die zich in deze basisgegevensbanken bevinden waardoor deze (quasi) in *real time* kunnen geraadpleegd worden²⁴. De nationale indexering maakt een beperktere opzoeking mogelijk van gegevens op basis van een vooraf bepaalde filter over alle ISLP basisgegevensbanken heen, terwijl de lokale index een weliswaar diepgaander bevraging toelaat, evenwel uitsluitend op gegevens van de gekozen ISLP basisgegevensbank waarop de gebruiker rechten heeft, en in functie van diens rechten op deze ISLP basisgegevensbank in kwestie.

De 'tool' maakt het daardoor ook mogelijk dat politionele informatie en persoonsgegevens kunnen worden geraadpleegd vóórdat deze in de Algemene Nationale Gegevensbank (ANG) wordt geregistreerd. Opdat politionele gegevens in de ANG wordt verwerkt, moet deze immers een validatieproces doorlopen. Daardoor is er tussen het verzamelen van politionele gegevens en het registreren ervan in de ANG een bepaalde tijdspanne waarbij de politonele gegevens niet in de ANG toegankelijk zijn, terwijl deze politionele gegevens zich wel in basisgegevensbanken bevinden. PoliceSearch@GPI maakt dus de **niet gevalideerde** politionele gegevens ook toegankelijk voor alle politiediensten. Met deze 'tool' worden met één opzoeking enkele politionele gegevens raadpleegbaar die in andere basisgegevensbanken (dan degenen waarin ze initieel werden gevat) worden verwerkt. De definitie van 'gevalideerde gegevens' blijft evenwel onzeker voor het COC. Daar waar in het niet openbaar gemaakt Advies van 12 december 2022 inzake de *DPIA* van PoliceSearch@GPI (DI220014) door het Controleorgaan vastgesteld wordt dat er geen duidelijke definitie is van wat 'gevalideerde gegevens' nu eigenlijk zijn, geeft het ontwerp richtlijn nu wel een duidelijk omschrijving, doch het reduceert de gevalideerde gegevens louter tot de gegevens uit de processen-verbaal in de ANG alsmede de te nemen maatregelen. Hieruit leidt het COC af, dat de opstellers van de richtlijn de informatie uit informatierapporten (RIR) of onderzoeksrapporten (DOS) – al dan niet opgenomen in de ANG - per definitie als 'niet gevalideerd' aanzien. Ook dit verdient naar het oordeel van het COC nog verdere nuance.

14. PoliceSearch@GPI is dus geen alternatief voor de ANG, maar versnelt de toegang tot ('niet-gevalideerde') politionele gegevens én geeft tegelijkertijd, met uitzondering van bepaalde categorieën

²⁴ Ontwerp van richtlijn, p. 4-5.

persoonsgegevens (zie verder), zicht op de beschikbare van (een omvangrijke hoeveelheid) politionele (persoons)gegevens (in verband met een bepaald persoon of andere entiteiten zoals voertuigen, organisaties of voorwerpen).

B) Wie is de verwerkingsverantwoordelijke?

15. PoliceSearch@GPI wordt voorgesteld als een indexeringsstelsel dat door de federale politie, met name DRI, wordt beheerd. Het Controleorgaan stelt vast dat, in tegenstelling tot wat in de gegevensbeschermingseffectbeoordeling (*DPIA*²⁵) het geval is, in het ontwerp van richtlijn **geen** verwerkingsverantwoordelijke wordt aangeduid. Nochtans is dit wel het geval in de *DPIA*, waarin de ministers van Justitie en van Binnenlandse Zaken, ieder in het kader van zijn respectievelijke bevoegdheden, als verwerkingsverantwoordelijke worden aangeduid, aangezien PoliceSearch@GPI door de indieners van de *DPIA* – en door het Controleorgaan - als een basisgegevensbank wordt beschouwd, zoals vastgelegd in artikel 44/4 § 1, 1^{ste} en 2^{de} lid WPA. De stellers van het ontwerp worden verzocht hierin duidelijkheid te brengen en een formele verwerkingsverantwoordelijke(n) aan te duiden. Immers, de verwerkingsplicht heeft een verantwoordingsplicht in verband met de naleving van titel 2 van de WVG en de WPA en moet onder meer in dat verband de rechten van de betrokkenen (burgers) faciliteren en laten uitoefenen, zoals bepaald in de artikelen 36 tot en met 40 WVG, en artikel 42 WVG. In dat verband heeft de betrokkene tevens een voorziening in rechte tegen de verwerkingsverantwoordelijke. Het moet voor de betrokkene logischerwijze dan ook duidelijk zijn wie de verwerkingsverantwoordelijke is die hij/zijn kan aanspreken of tegen wie hij/zij zich kan richten.

C) De werkmethode van PoliceSearch@GPI

16. Het Controleorgaan stelt met genoeg vast dat de aanbeveling 1 uit zijn Advies DI220014 inzake het cascadesysteem werd overgenomen in het ontwerp van richtlijn. Ook met de aanbeveling 3 inzake de context gebaseerde toepassing, de logbestanden en de duidelijke reden raadpleging werd rekening gehouden in het ontwerp, net zoals met de aanbevelingen 4 en 5 over respectievelijk de kwaliteitscontrole en de bewaartermijnen, al dient een en ander nog verder te evolueren.

17.1. Het Controleorgaan heeft evenwel een aantal opmerkingen met betrekking tot de werkmethode van de 'tool' en de daaruit voortvloeiende profielen. In het licht van de bescherming van de privacy, en klaarblijkelijk als antwoord van de steller van het ontwerp van richtlijn op de aanbeveling 2 uit het COC Advies DI220014 inzake de proportionaliteit van de toegangen, begrijpt het Controleorgaan dat bij het gebruik van de tool de indexing van bepaalde categorieën persoonsgegevens wordt

²⁵ *Data Protection Impact Assessment.*

uitgesloten, althans wat betreft de rechtstreekse indexering ervan. Dit leidt tot de contradictorische situatie waarbij het concreet voorbeeld van de voordelen van de werking van *PoliceSearch@GPI* in punt 1.5 van het ontwerp van richtlijn inzake informatie over zeden gerelateerde feiten inzake een mogelijke pedofiel in de PZ Westkust, die vijf minuten later beschikbaar zou moeten zijn voor de PZ Mons-Quevy, technisch onmogelijk wordt gemaakt omwille van de zogenaamde *privacy by design* regels in punt 2.3.1 van het ontwerp van richtlijn, die zedenmisdrijven a priori lijken uit te sluiten, gevolgd door andere uitsluitingen op het vlak van de informatierapporten en de rapporten voor het coördineren van onderzoeken.

17.2. Deze contradictie is exemplarisch voor het spagaat van de uitersten van het spectrum waarin de politiecultuur zich bevindt op het vlak van informatiebeheer. Enerzijds is er een bij wijlen irrationele 'vrees' voor politionele gegevensverwerkingen op zich waarbij zoveel als mogelijk aan de basis wordt uitgesloten, ervan uitgaande dat er 'niets meer kan of mag'. Anderzijds is er de harde en pure zgn. 'operationele handhaving - en efficiëntie gedreven' houding waarbij zoveel mogelijk gegevens ter beschikking wordt gesteld voor een zo groot mogelijk aantal medewerkers, ervan uitgaande dat het doel de middelen heiligt, onder het motto 'beter te veel dan te weinig'. Beide uitersten blinken uit in het ontbreken van de noodzakelijke nuances die tot uitdrukking komen in het politioneel gegevensbeschermingsrecht en kunnen samengevat worden in het drieluik wettelijkheid, noodzaak en proportionaliteit van de politionele verwerkingen die, in samen lezing met het geïntegreerde karakter van de GPI, het 'DNA' (zouden moeten) uitmaken van een geïntegreerde strategie van informatiedeling.

17.3. Dit spagaat vertaalt zich in het (contraproductief of minstens weinig doordacht) toepassen van het uitsluiten van bepaalde categorieën van persoonsgegevens en feiten, terwijl het aantal (niet-exhaustieve) *use cases* waarin de noodzaak én de proportionaliteit van deze uitgesloten gegevens aanwezig is nochtans ten overvloede blijkt.

1. De uitsluiting van slachtoffers

De slachtoffers van strafbare feiten behoren tot een categorie van persoonsgegevens waarvoor een wettelijke basis voor de politionele verwerking in de ANG voorzien is in art 44/5 §3,9°. De noodzaak en de proportionaliteit voor het consulteren van dergelijke gegevens blijkt uit onderstaande drie voorbeelden van *use cases*:

- de opvolging van recente feiten en gebeurtenissen, de geïntegreerde fenomeenopvolging en het identificeren van verbanden maar inzonderheid de opvolging van dader- en slachtoffergroepen door het SICAD-AIK in het raam van de basisfunctionaliteiten van hun werking zoals onder meer omschreven in de MFO6;
- de opvolging van een bepaald persoon die (te) veel aangiftes doet van verlies of diefstal van zijn/haar identiteitskaart op een (te) korte tijdsperiode door hetzij een lokale politiezone, hetzij

een SICAD-AIK, hetzij een gedeconcentreerde federale gerechtelijke politie (FGP), hetzij een centrale directie van federale gerechtelijke politie (DGJ);

- politiediensten moeten en kunnen in bepaalde omstandigheden namen en identiteiten verwerken van natuurlijke personen als hun naam als alias wordt misbruikt, met zeer vaak bijzonder nadelige gevolgen voor de betrokken persoon. Een tweede lijnsverificatie van een slachtoffer van identiteitsfraude naar aanleiding van een *hit* via de ANG Controle bij een grenscontrole omdat zijn naam als alias wordt gebruikt kan geoptimaliseerd worden middels een gebruik van PoliceSearch@GPI door een opzoeking te doen op de betrokken persoon als slachtoffer. Onafhankelijk van het feit of de betrokken persoon over een attest van klachtneerlegging beschikt (in de praktijk blijkt dat vaak om diverse redenen niet het geval te zijn) zou een opzoeking middels PoliceSearch@GPI inzicht kunnen verschaffen in het feit of de betrokken persoon al dan niet al klacht heeft ingediend wegens misbruik van zijn identiteit waardoor het oponthoud tot een minimum kan worden beperkt.

2. De uitsluiting van minderjarigen

De enige wettelijke beperking inzake de categorieën van minderjarigen voor wat de ANG verwerkingen betreft is voorzien in artikel 44/7, 2^e lid WPA: *“Wat de registratie in de ANG betreft van de gegevens bedoeld in artikel 44/5, § 3, 1^o, met betrekking tot een minderjarige jonger dan 14 jaar, is de toestemming van de bevoegde magistraat vereist.* Met andere woorden, de enige beperking die de wetgever hier oplegt betreft minderjarigen jonger dan 14 jaar, en enkel voor de categorie van verdachten en veroordeelde personen. De noodzaak en de proportionaliteit voor het (kunnen) consulteren van gegevens van minderjarigen blijkt uit onderstaande twee voorbeelden van *use cases*:

- de opvolging van recente feiten en gebeurtenissen met betrokkenheid van minderjarige daders, de geïntegreerde fenomeenopvolging en identificeren van verbanden tussen feiten met betrokkenheid van minderjarigen, de opvolging van dadergroepen die minderjarigen gebruiken door het SICAD-AIK in het raam van de basisfunctionaliteiten van hun werking zoals omschreven in de MFO6 (denk aan (georganiseerde) diefstallen door rondtrekkende dadergroepen);
- de casussen van de herhaalde onrustwekkende verdwijning van minderjarigen (art 44/5 §3, 4^o), waarbij bijvoorbeeld de Cel Verdwijningen snel en efficiënt kennis moet krijgen van voorgaande feiten teneinde een zicht te krijgen op het gedrag van een vermiste minderjarige.

3. De uitsluiting van zedenfeiten

In het licht van hogervermelde mechanismes, inzonderheid voor de werking van de SICAD-AIK en de werking van de centrale directies van de federale gerechtelijke politie die ook verder nog worden toegelicht, is het voor het COC allerm minst duidelijk waarom zedenfeiten *ab initio* worden uitgesloten. Als enige motivering wordt gesteld dat deze uitsluiting is ingegeven *“om de privacy van de slachtoffers te beschermen”* (blz. 10 in fine, punt 2.3.1, 4^e § van het ontwerp van richtlijn).

Deze vage en weinig zeggende motivering, waarmee (wellicht ongewild) meteen ook privacy van verdachten van zedenmisdrijven (beweerdelijk) wordt beschermd, overtuigt niet; men ziet ook niet in waarom de slachtoffers van alle andere soorten misdrijven in het strafwetboek en de bijzondere strafwetten zich dan niet op die beweerde privacybescherming zouden moeten kunnen beroepen. Bovendien is al evenmin duidelijk waarom als feit '37 A tot S'²⁶ wordt vermeld, terwijl in het licht van de reeds besproken beperking op minderjarigen '37 T' *niet* staat vermeld, terwijl deze feitcategorie betrekking heeft op mensenhandel meer bepaald de seksuele uitbuiting ten aanzien van minderjarigen. Bovendien wordt, zoals hoger vermeld, in punt 1.5 van het ontwerp van richtlijn net als voorbeeld van de geïntegreerde werking, een feit van pedofilie aangehaald, wat als feit 37 K onder de uitsluitingen lijkt te vallen ... ?

4. De uitsluiting van 'gevoelige' gegevens

Onder de term 'gevoelige gegevens' lijken de gegevens onder embargo, de gegevens van onderzoeken, de gegevens onder beperkende gebruikerscodes (de zogenaamde codes 00 en 01) van zowel de RIR als de DOS, alsmede bepaalde gegevens van administratieve aard te vallen.

Uit een samen lezing van de bepalingen van de fiches B31²⁷, B42²⁸ en C13²⁹ van de MFO3, en in het licht van *supra* – en *infra* - vermelde mechanismes, inzonderheid (maar niet uitsluitend) voor de werking van de SICAD-AIK en de werking van de centrale directies van DGJ, die ook verder nog worden toegelicht, begrijpt het COC niet waarom er geen onderscheid wordt gemaakt tussen drie afzonderlijke finaliteiten inzake de gevoeligheid zoals deze worden omschreven in het ontwerp richtlijn:

- het embargo, met als rechtsgrond art 44/8 WPA en een beslissing op niveau van het federaal parket en als gevolg een uitstel tot voeding van de ANG;
- het gebruik van beperkende gebruikerscodes, met als reglementaire grond de MFO3, en met nog een duidelijke toegankelijkheid onder welomschreven omstandigheden voor het SICAD-AIK, alsmede de centrale directies van DGJ;

De derde finaliteit wordt gevormd door redenen van administratieve aard die buiten de operationele, politionele verwerkingen vallen en waarvan men zich de vraag moet stellen, of ze *überhaupt* hun plaats hebben in een basisgegevensbank. Het COC begrijpt al helemaal niet waarom gegevens over afwezigheden of ziekte het voorwerp zouden moeten uitmaken van een vating in de module "meldingen" van ISLP. Minstens op het vlak van ziektes gaat het om een gezondheidsgegeven dat ingevolge de AVG aan een bijzondere aandacht en beperkte(re) verwerkingsmogelijkheid is onderworpen, dat uiteraard volledig buiten de operationele, politionele verwerkingen valt.

²⁶ Dit is de code die door het Openbaar Ministerie aan dergelijke feiten wordt gerelateerd.

²⁷ Het opstellen van gerechtelijke informatierapporten, niet-gepubliceerd.

²⁸ Het overmaken en het gebruik van kopieën van PV en informatierapporten om documentaire doeleinden, niet gepubliceerd.

²⁹ Coördinatie van de onderzoeken, niet gepubliceerd.

17.4. In het licht van wat hierboven werd uiteengezet is op het vlak van de beperkende gebruikerscodes, gezien de hen toegekende taken minstens een rol weggelegd voor de SICAD-AIK's alsmede de centrale directies DGJ voor dit soort van gegevens.

De fiche B42 van de MFO3 omvat de regels inzake het overmaken en het gebruik van kopieën van PV en informatierapporten om documentaire doeleinden aan de centrale directies van DGJ (DJSOC³⁰). De overmaking ervan is beperkt tot een aantal gevallen: in het raam van de kwaliteitscontrole en voor het informeren van gespecialiseerde politiediensten voor de fenomeenopvolging waarvoor hun steun en coördinatie noodzakelijk is.

De hierboven reeds geciteerde MFO6 bevat de acht basisfunctionaliteiten van de SICAD-AIK werking. Middels deze acht basisfunctionaliteiten staan de SICAD-AIK in voor de exploitatie van de informatie ten behoeve van de politieoverheden en politiediensten, voor zover deze exploitatie, gelet op de eigen mogelijkheden van de politiediensten, een meerwaarde betekent zowel op operationeel vlak, als op het vlak van de ontwikkeling van het veiligheidsbeleid in de domeinen van bestuurlijke en gerechtelijke politie. Met andere woorden, voor die gegevens waarvoor het proportioneel en noodzakelijk is, kan PoliceSearch@GPI een grote bijdrage leveren voor een snellere en geïntegreerde werking van de SICAD-AIK alsmede de centrale directies van DGJ als aanvulling, maar niet ter vervanging, van reeds bestaande tools.

17.5. Het (on)rechtstreeks uitoefenen van de rechten.

Onafhankelijk van de problematiek omtrent het al dan niet rechtstreeks uitoefenen van de rechten van de betrokken persoon, hebben zowel de toezichthouder alsmede de betrokken DPO ('s) nood aan een klaar en duidelijk overzicht van de verwerkingen ten aanzien van een betrokken persoon. In de huidige toestand van het informatiebeheer worden de persoonsgegevens verwerkt in de gegevensbanken zoals voorzien in art 44/2 WPA. Een transversale opzoekingsmogelijkheid binnen alle categorieën van verwerkte persoonsgegevens in de ISLP basisgegevensbanken faciliteert dit werk aanzienlijk, al geeft PoliceSearch@GPI niet alle door de politie verwerkte informatie in (basis)gegevensbanken weer, laat staan dat het probleem van de bijzondere gegevensbanken erdoor verholpen zou zijn of worden. Inderdaad, transversale opzoeken in andere basisgegevensbanken zoals FEEDIS³¹ of CAD³² zijn niet mogelijk middels PoliceSearch@GPI al is er vanuit CAD wel een (gedeeltelijke) flux naar ISLP. Het COC wil hier voor alle duidelijkheid stellen, dat de basisgegevensbanken voor onderzoeken³³ buiten beschouwing worden gelaten in dit voorbeeld en in het licht van onderhavig advies. Immers, de koppeling van dergelijke gegevensbanken impliceert strengere voorwaarden inzake de noodzaak en de proportionaliteit van de toegangen en verwerkingen,

³⁰ Serious and Organised Crime.

³¹ Feeding Information System, basisgegevensbank in gebruik bij de FGP

³² Computer Aided Dispatching, basisgegevensbank in gebruik bij de SICAD-CIC

³³ Zoals GES (Gestion d'Enquêtes) met inbegrip van de bijhorende tools zoals de verwerking van telefoniegegevens

alsmede strengere technische en organisatorische maatregelen. Hoe dan ook staat vast dat ook voor de finaliteit van het (on)rechtstreeks uitoefenen van de rechten de meerwaarde van PoliceSearch@GPI aanzienlijk is.

18. Hoewel het Controleorgaan het opzet van deze werkmethode *sensu lato* kan bijtreden, daar er terdege rekening werd gehouden met de in het COC Advies DI220014 geformuleerde aanbevelingen, rijst de vraag of de uitsluiting van de rechtstreekse kennisneming van de voormelde categorieën consequent en wel altijd goed doordacht is, of zelfs de opzet van PoliceSearch@GPI niet (bewust of onbewust) in het werkveld een (niet noodzakelijke) beperking oplegt. In alle geval nodigt het Controleorgaan de stellers van de richtlijn uit:

- om de geïdentificeerde uitstluitingen *ab initio* te herbekijken en te heroverwegen;
- deze te plaatsen in het licht van een geïntegreerde werking door ze te koppelen aan **bijkomende profielen** die rekening houden met:
 - o de finaliteiten van de SICAD-AIK en de centrale directies van DGJ;
 - o de finaliteiten van de DPO en van diensten Intern Toezicht;
 - o de finaliteiten van de toezichthouder.

OM DEZE REDENEN,

Het Controleorgaan op de Politie Informatie,

verzoekt de aanvrager gevolg te geven aan de hogervermelde opmerkingen.

Advies goedgekeurd door het Controleorgaan op de Politie Informatie op 23 oktober 2024

Voor het Controleorgaan,

De Voorzitter *a.i.*,
Frank SCHUERMANS (GET)