INHOUDSTAFEL

VERSLAG OPGESTELD IN HET KADER VAN HET TOEZICHTS-ONDERZOEK NAAR ONRECHTMATIGE TOEGANGEN TOT DATABANKEN DOOR LEDEN VAN DE POLITIEDIENSTEN[1]

1. ALGEMENE INLEIDING

1.1. Probleemstelling en algemene context

1. Na eerder al de aandacht te hebben gevestigd op die problematiek, wees het Vast Comité P in zijn jaarverslag 2005 op het bestaan van aanwijzingen voor een mogelijke normvervaging binnen de politiediensten met betrekking tot het gebruik van de hen ter beschikking gestelde databanken[2]. In 2009 merkte het Vast Comité P opnieuw op dat sommige leden van de politie nog steeds hun individuele toegang tot vertrouwelijke gegevens bleken te misbruiken voor persoonlijke doeleinden, zowel in de politionele als in de externe databanken waartoe zij vanuit hun hoedanigheid toegang hebben, zoals het rijksregister of het register van ingeschreven voertuigen[3]. In dat verband beval het Vast Comité P een geheel van goede praktijken aan en verzocht het de leiding van de politiediensten om de personeelsleden te sensibiliseren en te informeren. Die aanbeveling werd herhaald in het jaarverslag 2010[4].

2. De mogelijke inbreuken op de persoonlijke levenssfeer door de leden van de politiediensten, een recht gewaarborgd door de Grondwet, is een rechtstreekse bezorgdheid van het Comité P daar zij behoren tot zijn wettelijke opdrachten. Een eerste (meer) diepgaande analyse van de situatie werd verricht in het kader van het jaarverslag 2013 dat werd goedgekeurd door de parlementaire begeleidingscommissie op 7 januari 2015.

---

[1] Dossier nr. 21530/2015.

[2] Activiteitenverslag 2005 van het Vast Comité van Toezicht op de politiediensten, *Parl. St.*, Kamer, 2006-2007, nr. 3112/001 en Senaat, 2006-2007, nr. 3-2410/1, p. 53-57.

[3] Activiteitenverslag 2009 van het Vast Comité van Toezicht op de politiediensten, *Parl. St.*, Kamer, 2010-2011, nr. 1165/001 en Senaat, 2010-2011, nr. 5-754/1, p. 169-171.

[4] Die aanbeveling luidde als volgt: "*Daarom beveelt het Comité P aan dat iedere politiemedewerker enkel gebruik maakt van zijn persoonlijke login en paswoord, bij elke raadpleging de reden ervoor registreert zoals voorgeschreven en na elke consultatie steeds de toegang tot de databanken afsluit. De leiding zou haar medewerkers hieraan geregeld moeten herinneren evenals aan het feit dat hierop controle gebeurt. Het is ook aanbevolen dat politiemedewerkers in de uitvoering van hun opdrachten gegevens over familieleden of vrienden niet zelf opzoeken in de databanken*.".

Tabel 1: Inbreuken op de persoonlijke levenssfeer geteld in 2013 (aantal aantijgingen)[5]

Aard van de aantijgingen van inbreuken op de persoonlijke levenssfeer	2013	%	Vastgestelde disfuncties	%
Onrechtmatige toegang tot databanken	126	72,41%	64	36,78%
Andere vormen van inbreuken op de persoonlijke levenssfeer	48	27.59%	11	6,31%
Totaal	174	100,00%	75	43,09%

Bron: Database van het Comité P

3. Er werd vastgesteld dat 72,41% van de aantijgingen van mogelijke inbreuken op de persoonlijke levenssfeer in de klachten en aangiften geregistreerd in 2013 in de database van het Comité P betrekking hadden op onrechtmatige toegang tot databanken. Voor 36,78% van die aantijgingen werd een disfunctie vastgesteld. De andere vormen van inbreuken op de persoonlijke levenssfeer hielden hoofdzakelijk verband met de onrechtmatige verspreiding van informatie alsook met het onrechtmatig vergaren of archiveren van informatie.

Tabel 2: Dossiers bij het Comité P geregistreerd in het kader van de functionaliteit "databanken" (aantal dossiers)[6]

Dossiers met betrekking tot databanken	2012	2013	2014	2015
	148	138	84	83

Bron: Database van het Comité P

4. Ter informatie, het aantal dossiers geregistreerd in het kader van de functionaliteit "databanken" daalt in de periode 2012-2015 met 43,91%.

1.2. Doel van het onderzoek

5. Aangezien de onrechtmatige toegang tot databanken voortduurt, heeft het Vast Comité P beslist om een toezichtsonderzoek te openen teneinde, onder meer, te achterhalen om welke redenen de onrechtmatige raadplegingen blijven voortbestaan en na te gaan op welke wijze ter zake aan preventie en bestraffing wordt gedaan. Het onderzoeksveld werd beperkt tot de toegangen tot de databanken die de leden van de politiediensten het meest gebruiken in de uitoefening van hun functie. Het is de bedoeling om aanbevelingen te formuleren die kunnen leiden tot een noemenswaardige verbetering van de situatie.

[5] De analyse van de dossiers 2013 betreffende inbreuken op de persoonlijke levenssfeer geregistreerd in de database van het Comité P werd verricht door die dossiers één voor één nauwgezet te bestuderen. Het is de aantijging van inbreuk op de persoonlijke levenssfeer die als basis voor de telling gediend heeft, waarbij een dossier verschillende aantijgingen van inbreuken op de persoonlijke levenssfeer kan bevatten. Aangezien dit soort van analyse veel tijd in beslag neemt, werd niet overgegaan tot analyse van de dossiers 2012 en 2014 om een tendens te verkrijgen.

[6] De dossiers die geregistreerd zijn in het kader van de functionaliteit "databanken" houden voor het merendeel verband met de onrechtmatige toegang tot databanken.

1.3. Gestelde onderzoeksdaden

6. De nodige inlichtingen betreffende de informatie en de sensibilisering van de leden van de politiediensten, de procedure voor de opsporing van misbruiken met databanken, de procedure voor de toegangsmachtigingen en het ontwerp van richtlijn tot regeling van de toegang, het gebruik en de controle van de ICT-middelen werden binnen de federale politie vergaard. Daartoe werden onder meer de directie van de politionele informatie en de ICT-middelen ('*Information and Communication Technology'*) (hierna DRI) en de dienst "Beveiliging van de informatie en de persoonlijke levenssfeer" geraadpleegd. De gegevens uit de jurisprudentiegegevensbank van de Tuchtraad werden geëxploiteerd om de kennis over het fenomeen verder aan te vullen. De korpschefs van drie lokale politiezones werden ook geraadpleegd om een zicht te krijgen op de wijze waarop de controle ter zake praktisch en concreet werd uitgeoefend. De voorzitter van het Controleorgaan van het politionele informatiebeheer, de commissaris-generaal van de federale politie en de voorzitter van de Vaste commissie van de lokale politie werden verzocht om hun kanttekeningen en hun reacties te kennen te geven op het ontwerp van onderzoeksverslag.

1.4. Structuur van het verslag

7. In dit verslag komen achtereenvolgens aan bod: de modaliteiten voor de toegang van de leden van de politiediensten tot de databanken, de maatregelen genomen om misbruiken te voorkomen, een overzicht van de opgemerkte disfuncties en hun bestraffing, de moeilijkheden om misbruiken vast te stellen, de redenen waarom men zich onrechtmatig toegang blijft verschaffen tot de databanken, de denkpistes om hier doeltreffender tegen te strijden en het formuleren van conclusies en concrete aanbevelingen. Tot slot is de analyse weergegeven van de reacties van de belanghebbende partijen die werden bevraagd, gevolgd door het slotcommentaar van het Vast Comité P.

2. VASTSTELLINGEN

2.1. Toegang tot databanken door politiediensten

2.1.1. Normatief raamwerk

8. Krachtens artikel 44/1, § 1, van de wet van 5 augustus 1992 op het politieambt[7] (hierna WPA), kunnen de politiediensten gegevens van persoonlijke aard en inlichtingen verwerken in het kader van de uitoefening van hun opdrachten van bestuurlijke politie en van gerechtelijke politie voor zover deze laatste toereikend, terzake dienend en niet overmatig van aard zijn in het licht van de doeleinden van bestuurlijke en van gerechtelijke politie waarvoor ze verkregen worden en waarvoor ze later verwerkt worden. Artikel 44/4 § 2 stelt dat de ministers van Binnenlandse Zaken en van Justitie, elk binnen het kader van hun bevoegdheden, bij richtlijn de maatregelen bepalen die nodig zijn om het beheer en de veiligheid, waaronder in het bijzonder de aspecten met betrekking tot de betrouwbaarheid, de vertrouwelijkheid, de beschikbaarheid, de traceerbaarheid en de integriteit van de persoonsgegevens en de informatie die worden verwerkt in de gegevensbanken bedoeld in artikel 44/2, te verzekeren. Op Europees

[7] *BS* 22 december 1992.

niveau werd onlangs een verordening uitgevaardigd betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[8].

9. De ministeriële richtlijn MFO-3[9] beschrijft uitvoerig de modaliteiten voor de toegang tot en de raadpleging van databanken toegankelijk voor de leden van de politiediensten.

10. De artikelen 54 tot en met 56 van de deontologische code van de politiediensten[10] herinneren de leden van de politiediensten aan de regels met betrekking tot de eerbied voor de persoonlijke levenssfeer en de vergaring, het beheer en de raadpleging van de informatie. De schending van die regels kan aanleiding geven tot tuchtstraffen.

11. Op strafrechtelijk vlak zijn een aantal misdrijven voorzien. Krachtens de punten 1° en 3° van artikel 39 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens[11] wordt met een geldboete van 100€ tot 100.000€ gestraft de verwerking van persoonsgegevens met overtreding van de algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens vermeld in artikel 4 van de wet van 8 december 1992 (waaronder de principes van de vergaring van gegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en de uitsluiting van een verdere verwerking die onverenigbaar is met die doeleinden) (art. 39, 1°) alsook de verwerking van persoonsgegevens met schending van de artikelen 6, 7 of 8 van de wet van 8 december 1992 die betrekking hebben op de zogenaamde gevoelige gegevens[12], de gegevens die de gezondheid betreffen en de gerechtelijke gegevens (art. 39, 2°). Indien de onrechtmatig verkregen gegevens worden bekendgemaakt aan derden, kan artikel 458 van het Strafwetboek betreffende de schending van het beroepsgeheim ook van toepassing zijn. Die bepaling voorziet een gevangenisstraf van 8 dagen tot 6 maanden en een geldboete van 100€ tot 500€. Artikel 550bis, §1, van het Strafwetboek straft met een gevangenisstraf van 3 maanden tot 1 jaar en/of een geldboete van 26€ tot 25.000€ "*hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft*"; wanneer het misdrijf gepleegd wordt met bedrieglijk opzet, wordt de gevangenisstraf verzwaard en bedraagt ze 6 maanden tot 2 jaar. Artikel 151 van het Strafwetboek straft met een gevangenisstraf van 15 dagen tot 1 jaar de daden van willekeur die inbreuk maken op door de Grondwet gewaarborgde vrijheden en rechten en die bevolen of uitgevoerd worden door een openbaar officier of ambtenaar, door een drager of agent van het openbaar gezag of van de openbare macht.

12. De ministeriële omzendbrief GPI 75[13] wijst er nogmaals op dat iedere raadpleging door een personeelslid van de politiediensten slechts mag uitgevoerd worden voor zover zij

---

[8] Verordening 2016/679 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

[9] Gemeenschappelijke richtlijn MFO-3 van de Ministers van Justitie en van Binnenlandse Zaken betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie.

[10] Koninklijk besluit van 10 mei 2006 houdende vaststelling van de deontologische code van de politiediensten (*BS* 30 mei 2006).

[11] *BS* 18 maart 1993.

[12] Met name de persoonsgegevens waaruit de raciale of ethnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de verwerking van persoonsgegevens die het seksuele leven betreffen.

[13] Ministeriële omzendbrief GPI 75 van 15 oktober 2013 - Gemeenschappelijke richtlijn van de Ministers van Justitie en Binnenlandse Zaken betreffende de door de politiediensten na te leven procedureregels in het kader van

gerechtvaardigd is door een operationele behoefte (met andere woorden, wanneer zij binnen zijn/haar opdrachten van bestuurlijke of gerechtelijke politie kadert) en dat de raadpleging van de Algemene nationale gegevensbank (hierna ANG) voor privédoeleinden in het bijzonder een inbreuk vormt op de persoonlijke levenssfeer die strafbaar is gesteld. Die ministeriële omzendbrief voorziet ook in de aanwijzing van contactpersonen binnen de politiediensten voor de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna CBPL).

13. Artikel 9 van de 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[14] heeft een artikel 44/3 ingevoegd in de wet op het politieambt, waarvan het eerste lid een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer bij de politiediensten in het leven roept. Die consulent heeft onder andere als opdracht het opstellen, het toepassen, het bijwerken en het controleren van een beleid inzake de beveiliging en de bescherming van de persoonlijke levenssfeer. De regels volgens dewelke de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer zijn opdrachten uitvoert kunnen bepaald worden in een koninklijk besluit.
Dat nieuwe artikel 44/3, § 2 WPA voorziet trouwens de creatie van een platform voor de veiligheid en de bescherming van de gegevens dat belast wordt met het waken over de gecoördineerde realisatie van het werk van de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer. De samenstelling en de nadere werkingsregels van dat platform werden vastgelegd in het koninklijk besluit van 6 december 2015 betreffende de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer en het platform voor de veiligheid en de bescherming van de gegevens. Dat is van kracht geworden op 1 maart 2016.

2.1.2. Toegankelijke databanken

14. De voornaamste politionele databank is de ANG. Dat is een relationele politionele databank waarin entiteiten (personen, organisaties, vervoermiddelen, plaatsen, voorwerpen en nummers) geregistreerd zijn voor zover zij minstens gelinkt kunnen worden aan een voorzien feit of een gerechtelijk onderzoek en voor zover de voorwaarden voor de registratie vervuld zijn.

15. In het kader van de uitoefening van hun opdrachten van bestuurlijke en gerechtelijke politie hebben de leden van de politiediensten ook toegang tot diverse databanken. De voornaamste zijn het RRN (Rijksregister / Registre National), het CWR (Centraal wapenregister), SIDIS (Système d'information des détentions / Detentie-informatiesysteem) en de DIV (databank inschrijving van voertuigen).

2.1.3. Toegang tot de databanken in de praktijk

16. De leden van de politiediensten moeten in zeer veel situaties overgaan tot bevragingen van databanken. Het is dus onmogelijk om *a priori* alle situaties te bepalen waarin die bevragingen

---

de onrechtstreekse toegang tot de persoonsgegevens die zij in het kader van de uitoefening van hun opdrachten van gerechtelijke en bestuurlijke politie verwerken in de algemene nationale gegevensbank.

[14] *BS* 15 oktober 2013.

rechtmatig kunnen worden gedaan (identiteitscontroles, onderzoeken, opdrachten inzake verkeer, enz.). Het is in feite de specifieke context en het specifieke normatief raamwerk die bepalen of het lid van de politiedienst rechtmatig kan overgaan tot de bevraging van deze of gene databank.

17. De bevraging van de databanken kan rechtstreeks gebeuren door het lid van de politiedienst dat daartoe gemachtigd is door gebruik te maken van de portaalsite van de politie die diverse toepassingen voorstelt die de raadpleging mogelijk maken maar ook, in voorkomend geval, door gebruik te maken van de mobiele terminals. De raadpleging kan ook gebeuren via een derde, meer bepaald wanneer het lid van de politiedienst niet de mogelijkheid heeft om daar zelf toe over te gaan (bijvoorbeeld een politieambtenaar die overgaat tot de controle van een persoon op het terrein) of via specifieke terminals in het kader van gespecialiseerde functies binnen de politie. Bij bevraging van de databank "controle" van de ANG is de fysieke aanwezigheid van de gecontroleerde entiteit of haar toereikende fysieke lokalisatie in de ruimte verplicht om de uitvoering van eventueel te nemen maatregelen mogelijk te maken. De databank "controle" wordt '*in real time*' bijgewerkt en biedt de leden van de politiediensten de mogelijkheid om zich ervan te vergewissen dat een entiteit (persoon, vervoermiddel, nummer, voorwerp) niet geseind staat met een te nemen maatregel (aanhouding, doorgedreven controle, enz.).

18. De toegangen tot de belangrijkste databanken worden geregistreerd (identificatiegegevens van het personeelslid, werkpost, gegevens waarop de bevraging van de databank betrekking heeft, resultaat van de bevraging en geregistreerde reden voor de raadpleging). De raadplegingen (bijvoorbeeld het lezen of afdrukken van een proces-verbaal) met behulp van ISLP ('*Information System for Local Police*') of FEEDIS ('*Feeding Information System*' van de federale politie) worden ook geregistreerd.

2.2. Maatregelen om misbruik te voorkomen

2.2.1. Permanente nota van de federale politie

19. In 2007 werd een permanente nota[15] van de commissaris-generaal van de federale politie, opgesteld door de directie van de operationele politionele informatie, gericht aan alle diensten van de geïntegreerde politie. In die nota worden de wettelijke voorschriften, de principes inzake verwerking van operationele informatie, de verantwoordelijkheden en verplichtingen van de gebruikers, diverse preventieve maatregelen beschreven, alsook de controle op en de afhandeling van de schendingen. Met goedkeuring van de VCLP, werden de korpschefs van lokale politie verzocht om dezelfde preventieve maatregelen op hun niveau toe te passen. Die permanente nota van de commissaris-generaal van de federale politie werd in die tijd verspreid, in afwachting van de goedkeuring van boek 4 betreffende de bescherming van de persoonlijke levenssfeer van de ministeriële omzendbrief MFO-3. Het was de bedoeling dat de richtlijnen vervat in de permanente nota in dat boek 4 zouden worden opgenomen, maar dat boek is uiteindelijk nooit verschenen.

[15] Permanente nota CGO-2007/3141 van 09/10/2007 van de commissaris-generaal van de federale politie betreffende de raadpleging van politionele databanken of van databanken ter beschikking gesteld van de politiediensten.

2.2.2. Informeren en sensibiliseren van het personeel

20. Begin 2004 wees een informatiebulletin[16] de personeelsleden er nogmaals op dat het verboden is om databanken voor privédoeleinden te raadplegen. Ingevolge de verspreiding van de permanente nota van de commissaris-generaal van 9 oktober 2007 behandelden verscheidene interne documenten onderwerpen die verband hielden met de problematiek. Op niet-exhaustieve wijze kunnen we de volgende documenten aanhalen:

1) het bulletin "Info Nieuws" nr. 1808 van 18 oktober 2007 betreffende het actieplan tegen het onrechtmatig gebruik van informatie dat, onder meer, beschrijft wat een onrechtmatige raadpleging is en handelt over de controleprocedure die binnen de geïntegreerde politie ingevoerd is en aanmaant om de reden voor de raadpleging in te vullen. Het bulletin "Infodoc" nr. 140 van oktober-november 2007 handelt ook over het specifiek actieplan tegen het onregelmatig gebruik van informatie;

2) de permanente nota DGS/DSJ-2008/4535/AJO van 31 januari 2008 van de commissaris-generaal van de federale politie gericht aan alle entiteiten van de geïntegreerde politie waarin in herinnering wordt gebracht dat de persoonsgegevens in het bezit van de politiediensten enkel mogen worden overgemaakt aan de bestemmelingen voorzien door artikel 44/1, 3e en 5e lid van de WPA;

3) het informatiebulletin "CGO News" van 7 juli 2011 dat de regels inzake raadpleging van politionele databanken opfrist;

4) de tijdelijke nota CGO-2011/5273 van 25 oktober 2011 van de directeur CGO gericht aan alle entiteiten van de geïntegreerde politie betreffende de modaliteiten om toegang te hebben tot de foto's die beschikbaar zijn bij raadpleging van het RRN;

5) het informatiebulletin "CGO News" van 12 mei 2014 betreffende de raadpleging van databanken waarin de basisregels voor de raadpleging van databanken toegankelijk voor de politiediensten uitvoerig beschreven zijn;

6) de informatiebulletins "DRI News" nr. 112 van 24 juni 2016 en "Info Nieuws" nr. 2405 van 24 juni 2016 betreffende de technische aanpassingen doorgevoerd in het kader van de SSO ('*Single Sign On'*) ingevolge de aanbevelingen uitgevaardigd in 2015 in het kader van de evaluatie van de werkgroep SCHEVAL[17]. Dat is een technische ontwikkeling om de "*logins*" te harmoniseren en om te verhinderen dat een "Windows"-gebruiker anders zou zijn dan een "Portal"-gebruiker[18] op een werkstation;

7) het bulletin "Info Nieuws" nr. 2407 van 8 juli 2016, "*Databanken, integriteit en persoonlijke levenssfeer*", omvat de nieuwe aanpak van DRI en haar actieplan;

---

[16] Federale politie, Directie van de interne relaties, Informatiebulletin "Info Nieuws" nr. 1541, *Gebruik van informatie voor privédoeleinden*, 12/05/2004.

[17] De werkgroep SCHEVAL ('*Schengen Evaluation Working Group*') heeft onder meer als taak om te evalueren op welke wijze de ondertekenaars van het Schengenverdrag de regels naleven en of de Lidstaten voldoende voorbereid zijn om die toe te passen. Bij de federale politie zijn verscheidene actieplannen ontwikkeld om tegemoet te komen aan de geformuleerde aanbevelingen.

[18] Portaalsite op het intranet van de politie die beschikbaar is op bepaalde werkstations die toegang geven tot de databanken die toegankelijk zijn voor de leden van de politiediensten.

8) het bulletin "DRI News" nr. 114 van 18 augustus 2016 betreffende de wachtwoorden heeft betrekking op het gebruik van wachtwoorden die voldoen aan minimale criteria[19].

21. In het verlengde van de permanente nota van de commissaris-generaal van 9 oktober 2007 en van het actieplan ter bestrijding van misbruiken werd een specifieke ruimte, gewijd aan onrechtmatige raadplegingen van gegevens, gecreëerd op het intranet van de politie. Die ruimte wordt beheerd door DRI. Via dat kanaal hebben leden van de politiediensten toegang tot diverse publicaties (nota's, informatiebladen, enz.) alsook tot de wetgeving ter zake. Er is ook een quiz voorhanden zodat de personeelsleden hun kennis kunnen testen. Er kan worden vastgesteld dat die site[20] minder vaak geraadpleegd werd in de periode 2009-2014. Daarbij moet echter rekening worden gehouden met het feit dat de site voornamelijk "documentaire" ondersteuning biedt en dat de meeste documenten voorhanden zijn binnen de politiediensten. Aangezien de politie de problematiek van de onrechtmatige raadplegingen vanaf 2007/2008 ernstig beginnen aan te pakken is, is de specifieke belangstelling van in het begin waarschijnlijk wat weggeëbd met de tijd.

22. Een waarschuwing herinnert de leden van de politiediensten die de portaalsite van de politie betreden om de databanken te bevragen er systematisch aan dat de raadplegingen geregistreerd worden, gecontroleerd kunnen worden en dat de informatie alleen maar verwerkt mag worden in het kader van opdrachten van bestuurlijke en/of gerechtelijke politie.

23. Gelet op die verschillende maatregelen om het personeel te informeren en te sensibiliseren kan worden gesteld dat de leden van de geïntegreerde politie voldoende geïnformeerd blijken te zijn over de verplichte regels en de beperkingen inzake de raadpleging van de hen ter beschikking gestelde databanken. Dat is trouwens de reden waarom DRI wenst over te gaan van het louter sensibiliseren naar het bewustmaken van de leden van de politiediensten.

2.2.3. Beheer van de toegangsmachtigingen

24. Het is DRI die instaat voor het beheer, de controle en de ondersteuning op het vlak van de toekenning van de toegangen tot de ondersteunende databanken en tot de ANG[21]. Het komt de politieverantwoordelijken toe om de toegangen zo te personaliseren dat ze in overeenstemming zijn met de taken die worden uitgeoefend door de betrokken personeelsleden. Het principe is dus om de personeelsleden enkel toegang toe te kennen tot de toepassingen die voor hen echt bruikbaar zijn[22]. Soms worden de aanvragen tot toegang die vragen oproepen herzien met de aanvrager (bijvoorbeeld aanvragen tot toegang voor de totaliteit van een dienst of aanvragen tot toegang tot operationele databanken voor personeelsleden die louter administratieve functies bekleden). DRI behandelt dagelijks gemiddeld tien mails die verband houden met aanvragen tot toegang voor personeelsleden van de geïntegreerde politie. Wanneer een lid van de politiediensten zich in non-activiteit bevindt ingevolge zijn pensioen of wegens een verlof van lange duur, wordt zijn status gewijzigd in de databank voor personeelsbeheer, wat automatisch leidt tot de intrekking van zijn toegangsmachtigingen tot de databanken. In het kader van haar taken kan DRI ook "signalen" sturen aan de politieverantwoordelijken op basis van de

---

[19] De federale politie heeft een permanente nota CG-ISPO-20165/1858 van 29/04/2016 betreffende informatiebeveiliging opgesteld. Daarin is onder meer een minimumstandaard bepaald voor de creatie en het gebruik van wachtwoorden die ingevoerd moeten worden binnen de informaticasystemen die zij beheert of ter beschikking stelt van gebruikers. Die nota is van toepassing op alle gebruikers van die systemen.

[20] Gemiddeld aantal bezoeken van de site per maand: 437,5 bezoeken in 2009, 738,4 in 2010, 549,8 in 2011, 359,8 in 2012, 274,4 in 2013 en 197,9 in 2014.

[21] DRI houdt zich ook bezig met de toegangen tot niet-concrete feiten wat de lokale politie betreft.

[22] De toegangen tot de databanken zijn persoonsgebonden, databank per databank.

vaststellingen die ze onder andere doet aan de hand van het toegangsbeheerprogramma (bijvoorbeeld een toegang die gedurende lange tijd niet gebruikt werd, zou de werkelijke behoefte van de betrokken gebruiker ter discussie kunnen stellen). Er is voorzien dat die aanpak zal worden uitgewerkt met de VCLP in het kader van de komende acties.

25. Het "standaardprofiel" waarmee de leden van de politiediensten de basistaken die hen toevertrouwd zijn kunnen vervullen (onthaal/interventie/'*community policing*', …) omvat over het algemeen (maar niet noodzakelijkerwijs) de toegang tot de toepassingen "Controle", "Raadpleging concrete feiten", "DIV niet-dringend", "RPO" (opzoekingen op basis van onvolledige nummerplaten), "RRN", "CWR", "SIDIS" en "mailing". De toegang tot andere meer specifieke toepassingen zoals de raadpleging van niet-concrete feiten, van onderzoeken of van de fototheek is voorbehouden aan de personeelsleden die meer specifieke functies vervullen, zoals de leden van de gerechtelijke diensten of van de CIDA's (communicatie- en informatiediensten van het arrondissement). Eind mei 2015 had 84,60% van de leden van de politiediensten (operationele leden en CALog's) toegang tot de toepassing "raadpleging" van de ANG. 81,20% had toegang tot de toepassing "controle". 89% van de leden van de geïntegreerde politie had toegang tot het RRN eind juli 2015. Dat er een vrij groot aantal personeelsleden toegang heeft tot het RRN wordt verklaard door het feit dat die databank onontbeerlijk is in de uitvoering van politieopdrachten zowel voor de leden van het operationeel kader (opmaak van processen-verbaal, huiszoekingen, interventies, seiningen, identiteitscontroles, ...) als voor sommige CALog's die taken uitvoeren ter ondersteuning van hun operationele collega's (onthaal, registratie in de databanken, enz.). De verschillen in aantal toegekende toegangen voor de verschillende toepassingen zijn logisch. Ze tonen aan dat er een onderscheid wordt gemaakt tussen de personeelsleden bij de toekenning van de toegangen.

2.2.4. Reden voor de raadpleging

26. De permanente nota van de commissaris-generaal van de federale politie van 9 oktober 2007 beveelt aan om de reden voor de raadpleging van de databanken op te geven wanneer dat mogelijk is en meer specifiek wanneer de raadpleging werd verricht ten bate van een ander lid van de politiediensten. Zoals in dat document aangegeven, is die praktijk niet altijd noch in alle omstandigheden mogelijk. Denk in dat verband bijvoorbeeld aan de personeelsleden die de databanken intensief raadplegen (personeel van de CIDA's, functioneel beheerders in de politiezones, personeel in de lokale dispatchings, enz.) voor wie het nagenoeg onmogelijk zou zijn om te voldoen aan een verplichting om een reden voor de raadpleging op te geven.

27. In de praktijk heeft het lid van de politiedienst dat een databank raadpleegt de mogelijkheid om de reden voor de raadpleging te registreren in een veld dat daarvoor voorzien is. Voor de raadpleging van foto's van het RRN is de opgave van een reden voor de raadpleging verplicht. Die reden moet voldoende duidelijk zijn om gemakkelijk de rechtmatigheid van de raadpleging te kunnen vaststellen. Een informatieblad[23] zet er nogmaals nadrukkelijk toe aan om het veld "reden voor de raadpleging" te gebruiken, dat trouwens beschouwd wordt als een echt geheugensteuntje omdat de inhoud van dat veld geregistreerd is in de "*loggings*", net zoals de andere bewerkingen gedaan in de betrokken toepassing.

[23] Federale politie, CGO, CGO News nr. 43, *Raadpleging van databanken*, 12/05/2014.

2.2.5. "Logging" van het gebruik en controles a posteriori van de toegangen

28. Elk gebruik van de toepassingen van de ANG, het RRN en de DIV wordt geregistreerd in een *"logging"* die gedurende vijf jaar beschikbaar is. Krachtens de ministeriële omzendbrief MFO-3, kunnen de "*logging*"-gegevens gebruikt worden om de wettelijkheid van het gebruik van de databanken te controleren, om preventieve controles uit te voeren van de raadplegingen en controles verricht door de leden van de politiediensten, alsook voor operationele doeleinden om, onder meer, na te gaan of een persoon of een vervoermiddel gecontroleerd werd door een politiedienst.

29. Met goedkeuring van de VCLP, overhandigt DRI elke maand de "*loggings*" van de raadplegingen aan de politieverantwoordelijken (korpschefs van de lokale politie of directeurs van de diensten van de federale politie) van een Franstalige politiezone, een Nederlandstalige politiezone en een dienst van de federale politie. Een tiental representatieve personeelsleden wordt bij toeval gekozen binnen elke politiedienst die de controle beoogt (leden van het operationeel of administratief korps, externe consultants, leden van de centrale diensten of van de antennes, enz.). De gegevens van de "*loggings*" hebben betrekking op periodes van verscheidene dagen (week en weekend) van de maand voorafgaand aan de uithaling van de gegevens. Op meer onregelmatige wijze voert DRI controles uit op basis van de media-actualiteit (bijvoorbeeld bij de verkiezing van Miss België om eventuele raadplegingen van gegevens uit het RRN uit nieuwsgierigheid op te sporen). Telkens wordt de aandacht van de politieverantwoordelijken gevestigd op het wettelijk kader inzake raadplegingen van databanken, op het bestaan van een site speciaal gewijd aan die problematiek op de portaalsite van de politie alsook op de noodzaak om de nodige maatregelen te nemen wanneer onregelmatigheden vastgesteld worden. Het komt de lokale en federale politieverantwoordelijken toe om over te gaan tot de nodige verificaties om de rechtmatigheid vast te stellen van de raadplegingen die gedaan zijn door hun personeelsleden. DRI benadrukt dat de controles niet als hoofddoel hebben om de "*loggings*" op zich te verwerken, maar veeleer om, op gepersonaliseerde en concrete wijze, de verantwoordelijken van de politiediensten te responsabiliseren voor de problematiek van de onrechtmatige raadplegingen en hen er, bijgevolg, toe aan te zetten om op hun niveau proactief de nodige maatregelen te nemen. DRI is zich ervan bewust dat de aldus georganiseerde controle niet significant is in het licht van het aantal controles die dagelijks worden uitgevoerd in de databanken binnen de geïntegreerde politie. Niettemin moet die controle, in principe, *in fine* kunnen leiden tot een meer significant aantal controles. Aangezien de controles verricht worden met inachtneming van de autonomie van de lokale politiezones, is geen feedback vereist.

30. Drie lokale politiezones die kort daarvoor dergelijke "*loggings*" gekregen hadden, werden eind 2015 bevraagd om informatie te verkrijgen over de wijze waarop die controles concreet werden aangepakt. Twee van de drie politiezones hebben de "*logging*" die hen overgemaakt was geëxploiteerd. De derde zone heeft het document helemaal niet geëxploiteerd wegens de werklast die ermee gepaard gaat. Een politiezone heeft aan elk betrokken personeelslid de listing van de geselecteerde raadplegingen overhandigd met de vraag om schriftelijk, voor elk van die raadplegingen, de refertes te verduidelijken van de documenten die de raadplegingen kunnen rechtvaardigen (bijvoorbeeld een nummer van proces-verbaal of een informatiefiche). Op basis van de geleverde informatie werden bijkomende verificaties verricht door de verantwoordelijke voor de controle om de rechtmatigheid van de raadpleging na te gaan. Wanneer een controle niet gerechtvaardigd kon worden door het bestaan van een document, maakte het personeelslid daarvan gewag in zijn verslag zonder dat die raadplegingen als dusdanig beschouwd worden als onrechtmatig of problematisch. In de andere politiezone bestond de controle uit het leggen van een verband tussen de gedane raadplegingen en een

document geregistreerd op basis van het dienstrooster van de betrokken medewerkers. Aan het personeel werd geen bijkomende informatie gevraagd.

31. De informatie vergaard naar aanleiding van de bevraging van de drie politiezones is erg fragmentarisch en ze kan dus niet geëxtrapoleerd worden naar alle politiediensten. Toch kunnen er enkele lessen uit worden getrokken. Het voornaamste doel van de controles *a posteriori* bestaat erin de politieverantwoordelijken te sensibiliseren voor de problematiek. Hoewel die doelstelling inderdaad zo behaald kan worden, is het de controle van de legitimiteit van de raadplegingen die klaarblijkelijk de hoofdbekommernis is van de politieverantwoordelijken die gelast zijn om concreet over te gaan tot de controle. Ze voeren die controle uit afhankelijk van hun eigen perceptie en rekening houdend met de werklast die hij met zich brengt. De minutieuze verificatie van de legitimiteit van de raadplegingen vergt immers een niet te verwaarlozen werklast. Een bevraagde korpschef heeft, trouwens, voorgesteld dat de diepgaande controles beperkt zouden zijn tot de raadplegingen waarvoor er "tekenen" zijn die wijzen op een eventueel problematische situatie teneinde de werklast te beperken. Hoewel zijn bestaan een pluspunt is en het een lovenswaardig doel nastreeft, lijkt het nuttig om zich vragen te stellen bij de opportuniteit om een controlesysteem te handhaven dat berust op de verificatie van de rechtmatigheid van raadplegingen die bij toeval geselecteerd zijn, los van elk concreet element van vermoeden van disfunctie. Rekening houdend met de geringe frequentie van de controles, heeft de verhoopte sensibilisering van de politieverantwoordelijken bovendien waarschijnlijk een beperkt blijvend effect.

32. Het controlesysteem zou binnenkort een ontwikkeling moeten doormaken. DRI is van plan te stoppen met de controles *a posteriori* in hun huidige vorm, aangezien alle politiediensten één keer onderworpen geweest zijn aan de controleprocedure die ingevoerd werd in het verlengde van de permanente nota van de commissaris-generaal van de federale politie uit 2007.

2.2.6. Ontwerprichtlijn tot regeling van de toegang, het gebruik en de controle van de ICT-middelen binnen de federale politie

33. De laatste hand wordt gelegd aan een richtlijn tot regeling van de toegang, het gebruik en de controle van de ICT-middelen binnen de federale politie. Die richtlijn is tevens van toepassing op het gebruik van ICT-middelen die elke verwerking van gevoelige persoonsgegevens mogelijk maken en, meer in het bijzonder, de informatie en de persoonsgegevens geregistreerd in de databanken beoogd in artikel 44/2 van de WPA en de gegevens betreffende de gezondheid. Gelet op de gevoeligheid van die gegevens, is voorzien dat specifieke regels worden uitgevaardigd.

34. De federale politie is kennelijk de enige overheidsinstelling die een richtlijn uitgewerkt heeft die van toepassing is op een zo verscheiden aantal ICT-middelen. Ze wil de naleving van het fundamenteel recht van de gebruikers op eerbiediging van hun privacy in de werkrelatie verzoenen met de behoeften van een goede werking van de federale politie. Ze somt duidelijk de verboden activiteiten op en beschrijft ook de algemene modaliteiten voor de uitoefening van de controle die op vier beginselen berust: finaliteitsbeginsel, proportionaliteitsbeginsel, subsidiariteitsbeginsel en transparantiebeginsel.

35. De voorziene controle moet minstens berusten op een van de volgende finaliteiten:

1) de vaststelling van strafrechtelijke inbreuken, meer bepaald eerrovende, van feiten in strijd met de goede zeden;

2) de bescherming van de informatie die betrekking heeft op de operationele werking van de politie en van de informatie waaraan een beschermingsgraad gekoppeld is;
3) de beveiliging en/of de goede technische werking van de informaticasystemen van de politie in het algemeen;
4) de naleving van de richtlijn en van de regels inzake het gebruik van ICT-middelen die van kracht zijn binnen de federale politie alsook van de deontologische code.

36. De controle moet ook worden verricht in naleving van de proportionaliteits- en subsidiariteitsbeginselen, wat impliceert dat de inzameling van persoonsgegevens beperkt is tot hetgeen strikt noodzakelijk is in het kader van de doeleinden van de controle, dat de ingezamelde gegevens toereikend, terzake dienend en niet overmatig van aard zijn in het licht van die doeleinden en dat de doelgerichte controles punctueel en gerechtvaardigd moeten zijn door aanwijzingen die een anomalie of een wederrechtelijk gebruik van de ICT-middelen doen vermoeden.

37. Krachtens het transparantiebeginsel moeten de leden van de federale politie op collectief en individueel vlak ingelicht worden over het controlebeleid dat ten aanzien van hen wordt gevoerd, over het soort controle en over de wijze waarop die wordt uitgevoerd.

38. De controle bestaat uit twee stappen: een algemene controle en een doelgerichte, geïndividualiseerde controle. De doelgerichte controles zijn punctueel en gerechtvaardigd door aanwijzingen die een anomalie of een wederrechtelijk gebruik van de ICT-middelen doen vermoeden.

39. De ontwerprichtlijn werd voorgelegd aan de VCLP voor informeel advies en de inbreng van dat orgaan werd in de tekst geïntegreerd. Ze werd voorgelegd aan het syndicaal overleg in juli 2016 en zou in werking moeten treden begin 2017, meer bepaald na de opmaak van een communicatieplan.

2.2.7. Actieplan in het kader van het goed gebruik van politionele databanken of databanken ter beschikking gesteld van de politie

40. Een nieuw actieplan waarvan de grote lijnen draaien rond de raadpleging van maar ook de toegang tot de databanken werd onlangs in plaats gesteld door DRI. De voornaamste assen van dat actieplan zijn:

1) de opvolging en het beheer van de toegangen en de raadplegingen;
2) de doelgerichte preventieve controle van de raadplegingen;
3) de uitbreiding van het toepassingsveld tot de niet-operationele databanken;
4) de ondersteuning van DRI in de initiatieven die op lokaal niveau genomen worden om ter zake een actieplan op te maken;
5) de communicatie die niet alleen altijd transparant moet zijn maar ook meer gediversifieerd door tevens de acties gevoerd door DRI en de verkregen resultaten te vermelden.

2.3. Disfuncties

2.3.1. Bijkomende analyse

41. Ter aanvulling van de gedetailleerde analyse van de klachten en aangiften 2013 gemeld aan het Comité P inzake inbreuken op de persoonlijke levenssfeer verricht in het kader van het jaarverslag 2013, werd een analyse gemaakt van de gedepersonaliseerde gegevens uit de "jurisprudentiegegevensbank" van de Tuchtraad voor de periode 2012-2015. Hierdoor kan men relevante informatie verkrijgen betreffende de bewezen disfuncties. De gedepersonaliseerde kwalificaties van de tuchtvergrijpen leveren echter weinig contextgegevens op.

42. Voor die analyse werd de tuchtstraf opgelegd aan een lid van de geïntegreerde politie als basis gebruikt voor de telling. Die basis verschilt van de basis gebruikt bij de analyse van de gegevens van het Comité P (aantijgingen van onrechtmatige toegangen naar aanleiding van klachten en aangiften in 2013). Het is dus niet mogelijk om de cijfers van beide analyses rechtstreeks te vergelijken.

2.3.2. Omvang van de beteugeling in tuchtzaken

Tabel 3: Opgelegde tuchtstraffen (aantal tuchtstraffen)

Tuchtstraffen	2012	2013	2014	2015	Periode 2012-2015
	48	59	63	40	210

Bron: Jurisprudentiegegevensbank van de Tuchtraad

43. In de periode 2012-2015 wordt een daling met 16,66% van het aantal tuchtstraffen vastgesteld. De algemene tendens is negatief, wat neigt aan te tonen dat het fenomeen verdwijnt of dat de bestraffing ter zake minder doeltreffend of intensief is. Die aanzienlijke daling in percenten moet echter gerelativeerd worden rekening houdend met de geringe cijfers waarvan sprake. Bovendien is er waarschijnlijk een *dark number* gelet op de moeilijkheid om de disfuncties op te sporen (zie *infra*). De in 2015 opgelegde tuchtstraffen hebben betrekking op ongeveer 0,08% van de leden van de geïntegreerde politie[24].

[24] Op basis van 49 218 leden van de geïntegreerde politie geteld in mei 2015.

Tabel 4: "Tuchtrechtelijke" gevolgen gemeld aan het Comité P[25] (aantal bewezen aantijgingen van onrechtmatige toegangen)

"Tuchtrechtelijke" gevolgen	2013	%
Terechtwijzing (opmerkingen, functioneringsnota's, enz.)	15	23,44%
Lichte tuchtstraffen	13	20,31%
Zware tuchtstraffen	6	9,38%
Seponering maar minnelijke schikking	4	6,25%
Tuchtdossier met onbekende beslissing	1	1,56%
Voorlopige schorsing met inhouding van wedde	1	1,56%
Onvoldoende informatie	24	37,50%
Totaal	64	100,00%

Bron: Database van het Comité P

44. In 2013 werden naar aanleiding van de 64 bewezen aantijgingen van onrechtmatige toegangen voornamelijk maatregelen van terechtwijzing (23,44%) en lichte tuchtstraffen (20,31%) genomen. Er dient opgemerkt dat 12 andere tuchtdossiers nog hangend waren (aantijgingen van onrechtmatige toegangen niet noodzakelijk bewezen) toen de feiten aan het Comité P werden gemeld. Het verschil tussen de cijfers uit de jurisprudentiegegevensbank van de Tuchtraad en die uit de database van het Comité P is waarschijnlijk, ten dele, te wijten aan het feit dat de analyse van de gegrondheid van de aantijgingen van onrechtmatige toegangen niet afgerond was toen de feiten aan het Comité P gemeld werden.

2.3.3. Context van de onrechtmatige toegangen

Tabel 5: Context van de bestrafte onrechtmatige toegangen (aantal tuchtstraffen)

Context	2012	2013	2014	2015	Periode 2012-2015	%
Buiten beroepsverband	46	57	60	33	196	93,33%
Binnen beroepsverband	1	1	1	0	3	1,43%
Onbepaald	1	1	2	7	11	5,24%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

45. Hoofdzakelijk raadplegingen van databanken buiten beroepsverband maken het merendeel uit van de bestrafte onrechtmatige toegangen (93,33%). 77,78% van de aantijgingen van onrechtmatige toegangen geregistreerd in de database van het Comité P in 2013 kaderden ook

[25] In toepassing van artikel 14bis, 2de lid, van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

buiten het beroepsverband (9,52% in beroepsverband en 12,70% in een onbepaalde context). Die raadplegingen zijn hoofdzakelijk ingegeven door privéredenen.

46. Niettegenstaande er weinig informatie beschikbaar is over de context van de bestrafte feiten, kan worden opgemerkt dat in vier gevallen de raadpleging van de databanken gebeurd is door gebruik te maken van de informaticatoegang van een andere politieambtenaar. In twee gevallen werd de raadpleging gevraagd aan een collega. In één geval werd een drogreden gebruikt voor de raadpleging.

2.3.4. Terugkeer van onrechtmatige toegangen

Tabel 6: Herhaling van de bestrafte onrechtmatige toegangen (aantal tuchtstraffen)

Herhaling	2012	2013	2014	2015	Periode 2012-2015	%
Eenmalige onrechtmatige toegang	17	21	16	10	64	30,48%
Verscheidene onrechtmatige toegangen	20	21	16	8	65	30,95%
Talrijke onrechtmatige toegangen	1	4	6	7	18	8,57%
Onbepaald	10	13	25	15	63	30,00%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

Tabel 7: Recidive van de bestrafte leden van de politiediensten (aantal tuchtstraffen)

Recidive	2012	2013	2014	2015	Periode 2012-2015	%
Recidive	0	0	3	0	3	1,43%
Geen recidive	48	59	60	40	207	98,57%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

47. Het aantal dossiers in het kader waarvan talrijke onrechtmatige toegangen vastgesteld werden is, gelukkig maar, vrij gering (8,57% van de tuchtstraffen en 10,32% van de aantijgingen in 2013 in de database van het Comité P). Wel te betreuren is dat het percentage van gevallen waarin sprake is van verscheidene onrechtmatige toegangen zo hoog is (30,95% van de tuchtstraffen en 23,02% van de aantijgingen in 2013 in de database van het Comité P). De recidivegraad is kennelijk zeer laag.

2.3.5. Betrokken personeelsleden

Tabel 8: Kader waartoe de bestrafte leden van de politiediensten behoren (aantal tuchtstraffen)

Kader	2012	2013	2014	2015	Periode 2012-2015	%
CALog	4	5	10	1	20	9,52%
Agent van politie	7	6	4	2	19	9,05%
Basiskader	26	34	36	31	127	60,48%
Middenkader	7	11	10	5	33	15,71%
Officierenkader	4	3	2	1	10	4,76%
Aspirant-inspecteur	0	0	1	0	1	0,48%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

Tabel 9: Component van de geïntegreerde politie waartoe de bestrafte leden van de politiediensten behoren (aantal tuchtstraffen)

Component van de geïntegreerde politie	2012	2013	2014	2015	Periode 2012-2015	%
Lokale politie	41	47	51	32	171	81,43%
Federale politie	7	12	12	8	39	18,57%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

Tabel 10: Taalrol van de bestrafte leden van de politiediensten (aantal tuchtstraffen)

Taalrol	2012	2013	2014	2015	Periode 2012-2015	%
Franstalig	24	29	33	25	111	52,86%
Nederlandstalig	24	30	29	15	98	46,66%
Duitstalig	0	0	1	0	1	0,48%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

48. Het standaardprofiel van het lid van de politiedienst dat onrechtmatig een databank raadpleegt lijkt dus dat te zijn van een lid van de lokale politie dat behoort tot het operationele basiskader. Dat blijken (in verhouding tot de personeelsformatie) meer leden van Franstalige politiediensten te zijn, tenzij de opsporing van misbruiken actiever gebeurt in het Franstalige gedeelte.

2.3.6. Geraadpleegde databanken en gebruik van gegevens

Tabel 11: Databanken geraadpleegd door de bestrafte leden van de politiediensten (aantal tuchtstraffen)[26]

Geraadpleegde databanken	2012	2013	2014	2015	Periode 2012-2015	%
RRN	19	31	13	4	67	31,90%
ANG	12	14	2	2	30	14,28%
DIV	7	4	5	4	20	9,52%
ISLP/FEEDIS	4	5	5	1	15	7,14%
Onvoldoende gepreciseerd	16	18	44	31	109	51,90%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

49. Die cijfers moeten worden vergeleken met de aantijgingen van onrechtmatige toegangen geregistreerd in 2013 in de database van het Comité P: RRN (40,48% van de aantijgingen van onrechtmatige toegang), DIV (11,11%), ANG (8,73%) en ISLP (4,76%). De toegangen tot het rijksregister maken dus onveranderlijk het grootste deel uit van de onrechtmatige toegangen. De tuchtstraffen voor de onrechtmatige toegangen tot het RRN lijken fel af te nemen in 2014 en vooral in 2015. Het is niettemin mogelijk dat nogal wat onrechtmatige toegangen tot het RRN die twee afgelopen jaren niet duidelijk vermeld waren in de omschrijving van de bestrafte tuchtvergrijpen.

50. De raadplegingen van gegevens uit het RRN blijken de meest ernstige inbreuken op de persoonlijke levenssfeer van de burger in te houden. Niettemin moet men er rekening mee houden dat de onrechtmatige raadplegingen van andere gegevens die ter beschikking staan van de leden van de politiediensten vaak door de slachtoffers ervaren worden als meer ernstige inbreuken op de "*privacy*" (informatie over opsluitingen of gepleegde feiten bijvoorbeeld).

Tabel 12: Gebruik van de onrechtmatig verworven informatie door de bestrafte leden van de politiediensten (aantal tuchtstraffen)

Gebruik van de verworven informatie	2012	2013	2014	2015	Periode 2012-2015	%
Verspreiding van informatie aan derden	13	10	6	4	33	15,71%
Aanhalen van de informatie	0	3	0	0	3	1,43%
Actief gebruik (contacteren, enz.)	1	0	1	0	2	0,95%
Onbepaald	34	46	56	36	172	81,91%
Totaal	48	59	63	40	210	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

[26] In het kader van een zelfde tuchtstraf kunnen verscheidene gegevensbanken geraadpleegd zijn. Het percentage wordt berekend in verhouding tot het aantal tuchtstraffen voor de periode 2012-2015.

51. In 81,91% van de gevallen zijn de redenen voor het gebruik van de informatie niet uitdrukkelijk vermeld. Wanneer het gebruik van de informatie precies gekend is, dan gaat het hoofdzakelijk om de verspreiding van de informatie aan derden of om het aanhalen van die informatie.

2.3.7. Aard van de tuchtstraffen

Tabel 13: Aard van de tuchtstraffen (aantal tuchtstraffen)

Aard van de tuchtstraffen	2012	2013	2014	2015	Periode 2012-2015	%	Periode 2001-2015	%
Waarschuwing	13	17	17	9	56	26,66%	141	27,65%
Blaam	17	25	24	12	78	37,14%	201	39,41%
Inhouding van wedde	7	8	15	13	43	20,48%	89	17,45%
Schorsing	6	8	7	1	22	10,48%	43	8,43%
Terugzetting	1	0	0	0	1	0,48%	15	2,94%
Ontslag van ambtswege	4	1	0	5	10	4,76%	21	4,12%
Totaal	48	59	63	40	210	100,00%	510	100,00%

Bron: Jurisprudentiegegevensbank van de Tuchtraad

52. In de meeste gevallen worden lichte tuchtstraffen opgelegd, klaarblijkelijk omdat het gaat om onrechtmatige raadplegingen zonder specifiek gebruik van de informatie. Er kunnen ook tuchtstraffen opgelegd worden voor andere feiten dan de onrechtmatige toegangen tot de databanken (bewuste verspreiding van informatie aan derden, ongepast aanhalen van informatie, enz.). Zij zijn uiteraard van aard om de opgelegde tuchtstraf te verzwaren. De percentages voor de periode 2012-2015 en voor de periode 2001-2015 zijn over het algemeen vrij gelijksoortig.

2.3.8. Organisatorische disfuncties

53. De tuchtstraffen worden gewoonlijk opgelegd voor individuele disfuncties en niet voor organisatorische disfuncties zodat de analyse van de jurisprudentiegegevensbank van de Tuchtraad geen grote hulp is. De analyse van de aantijgingen van onrechtmatige toegangen geregistreerd in 2013 in de database van het Comité P heeft het alleen maar mogelijk gemaakt om enkele organisatorische disfuncties op te sporen: in het kader van een geschil met een collega, een politieambtenaar heeft een "*logging*" verkregen betreffende de raadplegingen gedaan op zijn naam doordat hij zijn vraag gemotiveerd heeft door een interne controle, een aspirant-politieambtenaar heeft de toegang van zijn mentor gebruikt voor onrechtmatige doeleinden en een lokale politiezone heeft een proactieve opvolging niet uitgevoerd.

54. Om eventuele organisatorische en structurele disfuncties binnen de politiediensten te kunnen opsporen, moeten vrij zware specifieke onderzoeksdaden worden gesteld. Het is dus niet mogelijk om in dit stadium tot een besluit hieromtrent te komen. Door de invoering van de functie van consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer zou het in de toekomst mogelijk moeten zijn om de eventuele organisatorische problemen die zich op dat vlak voordoen in de politiekorpsen gestructureerd en verplicht aan te pakken.

2.3.9. Beteugeling in strafzaken

Tabel 14: Gerechtelijke gevolgen voor de betrokken leden van de politiediensten (aantal aantijgingen van onrechtmatige toegangen)

Gerechtelijke gevolgen	2013	%
Seponering	20	22,73%
Minnelijke schikking	14	15,91%
Dagvaarding om voor de correctionele rechtbank te verschijnen	1	2,28%
Onbekend	52	59,09%
Totaal	88	100,00%

Bron: Database van het Comité P

Tabel 15: Redenen voor de seponering (aantal aantijgingen van onrechtmatige toegangen)

Reden voor de seponering door de parketten	2013	%
Geen misdrijf	2	10,00%
Onvoldoende bewijzen	2	10,00%
Onvoldoende bezwaren	3	15,00%
Bovenmatige gevolgen van de strafvervolging	2	10,00%
Doorverwijzing naar strafbemiddeling	1	5,00%
Occasioneel feit	1	5,00%
Onbekend	9	45,00%
Totaal	20	100,00%

Bron: Database van het Comité P

55. De aantijgingen die op gerechtelijk vlak behandeld werden hebben vooral aanleiding gegeven tot minnelijke schikkingen in strafzaken, één enkel geval heeft geleid tot correctionele vervolging. Het plan van de minister van Justitie is erop gericht om de criminaliteit op meer doeltreffende wijze aan te pakken. Rekening houdend met die tendens is het weinig waarschijnlijk dat een verzwaring van de bestraffing inzake gewone onrechtmatige toegangen zonder specifiek gebruik van de onrechtmatig geraadpleegde gegevens overwogen kan worden. In ieder geval is het Comité P, net als in het verleden, van plan om de onrechtmatige toegang tot databanken die het vaststelt systematisch aan te geven aan het parket.

2.4. Moeilijkheid om misbruiken vast te stellen

56. De onrechtmatige toegangen tot de databanken zijn vrij gemakkelijk vast te stellen in geval van klacht of aangifte wanneer precieze elementen het mogelijk maken om de opzoekingen te sturen en te beperken. Dat is niet het geval wanneer bijvoorbeeld de raadpleging verricht werd met behulp van de toegang van een ander personeelslid, zonder dat een reden voor de

raadpleging opgegeven is, of wanneer de onderzoeksdaden betrekking hebben op mogelijke, weinig gecontextualiseerde misbruiken.

57. De vaststelling van het rechtmatige karakter van de raadplegingen kan enorm vergemakkelijkt worden wanneer de reden voor raadpleging op voldoende duidelijke wijze geregistreerd is voor de controleur en het personeelslid dat zich moet rechtvaardigen. Naar aanleiding van een recent onderzoek van de Dienst Enquêtes P heeft de analyse van de reden voor de raadplegingen van foto's in het RRN binnen een politiezone - die noodzakelijkerwijs ingevuld moet worden - aan het licht gebracht dat slechts 12,1%[27] van de raadplegingen gemotiveerd was door een voldoende duidelijke referentie. In de andere gevallen lieten de gebruikte motiveringen niet toe om onmiddellijk en gemakkelijk de link te leggen tussen de raadpleging van het RRN en het dossier dat aanleiding gegeven heeft tot de raadpleging. Algemeen gesproken, blijkt vaak uit de gevoerde onderzoeken dat de geregistreerde redenen voor de raadpleging onvoldoende zijn om de raadplegingen van de databanken te kunnen rechtvaardigen.

58. Wanneer er geen reden voor de raadpleging geregistreerd is, wanneer de reden voor de raadpleging onvoldoende duidelijk is of wanneer het lid van de politiedienst zich de raadpleging en haar context niet herinnert, is het nodig om bijkomende, lastige verificaties te doen om het verband aan te tonen met een opdracht van gerechtelijke of bestuurlijke politie. Talrijke verificaties van dit type voor een groot aantal raadplegingen kunnen onmogelijk overwogen worden gezien de werklast die ermee gepaard gaat.

2.5. Voortduren van de onrechtmatige raadplegingen

59. Dat de onrechtmatige raadplegingen voortduren, ondanks de preventieve en repressieve maatregelen, kan worden verklaard door verschillende factoren. Vooreerst dient vastgesteld dat de meeste onrechtmatige toegangen aan het licht komen via klachten en aangiften, omdat sommige feiten de aandacht getrokken hadden van de slachtoffers of de aangevers (bijvoorbeeld de dader van de onrechtmatige toegang haalt informatie-elementen aan die enkel beschikbaar zijn door de raadpleging van een specifieke databank). Een onrechtmatige toegang die zich beperkt tot de eenvoudige kennisname van de informatie, waaraan geen "ruchtbaarheid" gegeven wordt of die niet wijst op een disfunctie, zal moeilijk opspoorbaar zijn. Temeer daar de kans dat een doorsneelid van de politiediensten onderworpen wordt aan een controle inzake een eventuele onrechtmatige toegang erg klein is gelet op de huidige controle-instrumenten. Een andere verklarende factor berust op een zeker "begrip" voor de raadplegingen die weliswaar onrechtmatig zijn maar als "aanvaardbaar" worden beoordeeld gelet op de aard van de onderliggende motivering (bijvoorbeeld de bezorgdheid over de nieuwe gezinsomgeving van zijn kinderen) of wegens de "relatieve" ernst van de raadplegingen zelf (bijvoorbeeld de raadpleging van zijn eigen RRN-gegevens of de raadpleging van gegevens uit loutere nieuwsgierigheid). Het grote aandeel van de onrechtmatige toegangen die aanleiding hebben gegeven tot een terechtwijzing (23,44% van de bewezen aantijgingen van onrechtmatige toegangen in 2013) illustreert die vaststelling. *Pro memorie*, bij de analyse van de klachten en aangiften ter kennis gebracht van het Comité P in 2013 was ook vastgesteld dat iets meer dan een derde (35,79%) van de bewezen aantijgingen van onrechtmatige toegangen op tuchtrechtelijk vlak uitsluitend intern bleek te zijn afgehandeld door de politiediensten zonder dat de feiten ter kennis werden gebracht van de gerechtelijke overheid.

[27] Over een periode van bijna drie jaar.

2.6. Denkpistes

2.6.1. Algemeen

60. Er kunnen verschillende pistes verkend worden om bijkomende of alternatieve oplossingen te voorzien voor het bestaande arsenaal van preventieve en repressieve maatregelen. De veranderingen mogen er echter niet toe leiden dat de taak van de leden van de politiediensten administratief verzwaard wordt of dat zij gaan aarzelen om de databanken te raadplegen, wat in zijn geheel schadelijk zou zijn voor de uitvoering van het politiewerk. Er moet een evenwicht worden gezocht tussen het voorkomen van misbruiken en de operationele politionele doeltreffendheid.

61. De creatie van de functie van consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer bij de politiediensten, zoals voorzien door artikel 44/3 WPA, biedt een duidelijke kans om de politieverantwoordelijken daadwerkelijk bewust te maken van de problematiek van de onrechtmatige toegangen tot de databanken en om het stadium te overstijgen van het louter informeren en sensibiliseren van de leden van de politiediensten.

2.6.2. Voorkomen van misbruiken

- *Registreren van de reden voor de raadpleging*

62. De registratie van de reden voor de raadpleging is een ontradend en preventief middel tegen misbruiken. De registratie van een drogreden kan, in voorkomend geval, immers beschouwd worden als informaticafraude en een rem zetten op de onrechtmatige raadplegingen. Er kunnen echter contra-indicaties zijn voor het verplichten van die registratie, bijvoorbeeld wanneer gevoelige gegevens verwerkt worden door bepaalde politiediensten of wanneer de verplichting van die praktijk een te grote administratieve extra belasting met zich zou meebrengen gelet op het volume van de te verwerken gegevens (functioneel beheerders bijvoorbeeld).

63. De loutere registratie van een reden levert echter in haar eentje niet het bewijs van de rechtmatigheid van een raadpleging. Tijdens onderzoeken naar verdenkingen van onrechtmatige raadplegingen maken enkel meer doorwrochte verificaties het mogelijk om vast te stellen of ze al dan niet rechtmatig zijn gebeurd. Er kan immers nooit worden uitgesloten, ook al zijn dit erg zeldzame gevallen, dat een drogreden voor de raadpleging geregistreerd werd. De reden is dus, in werkelijkheid, een geheugensteuntje voor het lid van de politiediensten dat in staat moet zijn om de rechtmatigheid van zijn raadpleging te bewijzen. Tevens moet worden benadrukt dat de vaststelling van het rechtmatige karakter van de raadpleging slechts in hoge mate vergemakkelijkt kan worden wanneer de geregistreerde reden voldoende duidelijk is, zowel voor de “controleur” als voor het personeelslid dat zich dient te rechtvaardigen.

64. Zoals we gezien hebben, is de registratie van de reden voor de raadpleging op dit ogenblik enkel verplicht voor de raadpleging van de foto’s van het RRN. Diverse politionele documenten die handelen over de thematiek van de raadpleging van de databanken zijn echter, net als het Vast Comité P, blijven aanbevelen en aanmoedigen dat er voor alle raadplegingen een voldoende duidelijke reden zou worden geregistreerd. Niettegenstaande sommige diensten

die praktijk verplicht gemaakt hebben[28], hebben velen dat, schijnbaar, niet gedaan of hebben ze dat gedaan zonder een echte controle op de toepassing van die maatregel.

65. Daarnaast moet worden vastgesteld dat de modaliteiten voor de registratie van de reden voor de raadpleging de gebruiker van de portaalsite van de politie er op dit ogenblik niet toe aanzetten om een reden op te geven. Zijn aandacht wordt immers niet gevestigd op het feit dat de raadplegingen geregistreerd worden en dat strafrechtelijke en tuchtrechtelijke vervolging mogelijk is in geval van misbruik. Het veld "reden voor de raadplegingen" is enkel toegankelijk via een keuzemogelijkheid die tussen andere keuzemogelijkheden staat wanneer men de sessie aanvat.

- *Technische preventie*

66. Meer algemeen gesproken, zou het opportuun zijn om, indien mogelijk, technische oplossingen en oplossingen op het vlak van informatica, uit te werken om de onrechtmatige toegangen tot de databanken te kunnen voorkomen, en dit zo doeltreffend mogelijk en zonder extra administratieve belasting voor de gebruiker. Die benadering vergt echter een analyse vanwege de politiediensten met betrekking tot de haalbaarheid om doeltreffende oplossingen uit te werken, zowel op technisch als op budgettair vlak, rekening houdend met de al vastgelegde prioriteiten.

- *Gegrondheid van de toekenning van de toegangen tot de databanken*

67. De verantwoordelijkheid voor de toekenning van de toegangen tot de databanken komt de lokale en federale politieverantwoordelijken toe. De lokale politiezones beheren op autonome wijze de toegangen tot de ANG. Gelet op de werkingsfilosofie van de geïntegreerde politie, levert DRI hulp aan de beheersverantwoordelijken en stuurt ze hen "signalen" wanneer problematische situaties ontdekt worden. Er is dus, strikt genomen, geen controle *sensu stricto* op de toekenning van de toegangen.

68. De toekenning van een toegang tot een databank moet doordacht en geïndividualiseerd gebeuren, zonder systematisme of automatisme. Het enige criterium waarop ze gebaseerd mag zijn, is de functie uitgeoefend door het lid van de politiedienst. Ze moet rekening houden met de werkelijke situaties en specificiteiten van de politiedienst en zich beperken tot de strikt noodzakelijke toegangen die het de leden van de politiediensten mogelijk maken om hun taken doeltreffend te vervullen. De noodzaak voor een lid van de politiediensten om *permanent en individueel* te beschikken over een toegang tot een databank om zijn opdrachten concreet op doeltreffende wijze te vervullen zou een criterium moeten zijn dat geregeld geëvalueerd wordt door de politieverantwoordelijken. Die meer geavanceerde evaluatie kan concreet enkel worden verricht door DRI.

[28] De directeur van de operationele politionele informatie van de federale politie (voorheen CGO) heeft bijvoorbeeld sinds 2009 voorgeschreven dat alle leden van zijn dienst die toegang hebben tot gegevensbanken door hun functie en voor de uitoefening van hun activiteiten de reden voor elke raadpleging verricht in de politionele gegevensbanken of in de gegevensbanken ter beschikking gesteld van de politiediensten duidelijk kenbaar moeten maken.

- *Uitvoering van de controles*

69. De aanpak van de controles wordt herzien op het niveau van de federale politie. Een controleproces dat berust op een fase van opsporing van potentieel verdachte situaties die, indien nodig, gevolgd wordt door diepgaande en doelgerichte controles naar de omstreden raadplegingen is meer opportuun dan een controleproces dat steunt op verificaties van raadplegingen die willekeurig gekozen zijn zonder enige reden tot verdenking. Een harmonisatie van de controle in die zin voor de volledige geïntegreerde politie is wenselijk.

2.6.3. Beteugeling van misbruiken

70. Zoals in het verleden, zal het Vast Comité P de klachten en aangiften hem gericht waarvoor er vermoedens van onrechtmatige toegangen tot de databanken zijn systematisch blijven aangeven aan de gerechtelijke overheden. Het Vast Comité P kan de verschillende politieverantwoordelijken er enkel aan herinneren dat ze hetzelfde moeten doen wanneer ze misbruiken ontdekken, en dit overeenkomstig de bepalingen van het artikel 29 van het Wetboek van Strafvordering. Op het niveau van de politie lijkt het bovendien verstandig om na te denken over bijkomende maatregelen die het ontradende karakter van de tuchtrechtelijke of strafrechtelijke vervolging kunnen versterken teneinde recidive te vermijden.

3. REACTIES EN COMMENTAAR VAN DE BELANGHEBBENDE PARTIJEN

3.1.1. Controleorgaan van het politionele informatiebeheer

71. De problematiek van de toegang tot de databanken, en meer in het bijzonder tot de ANG, is een hoofdbekommernis van het COC. Uit de observaties verricht in de loop van de eerste helft van 2016 zijn de volgende punten als de meest gevoelige naar voren gekomen:

1) het uitwerken op het niveau van de geïntegreerde politie van een beleid voor de raadpleging van de databanken in overeenstemming met de WPA, de Privacywet (wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens) en de deontologische code van de politiediensten;

2) het sensibiliseren van de personeelsleden voor de raadplegingen van de databanken;

3) het invoeren van een verplichte "*login*" voor elk personeelslid alsook de verplichting om de reden voor de raadpleging of voor de controle te vermelden;

4) het uitwerken van een coherent beleid inzake toegangsbeheer rekening houdend met het "*need to know*"-principe veeleer dan het "*nice to know*"-principe, waarbij dit beleid zich ook moet bemoeien met de intrekking van toegangen;

5) het implementeren van controles door de diverse diensten op verschillende niveaus (lokaal, bovenlokaal) maar ook door de bevoegde controleorganen;

6) het beklemtonen van de rol en van de taken vervuld door de centrale functies in het kader van het beheer en de doorstroming van de informatie: consulent voor de veiligheid, functioneel beheerders, korpschefs van de lokale politie, diensten intern toezicht en DRI;

7) de rol en het beleid van DRI moeten centraal zijn en bepalend zijn voor het opstellen van regels met betrekking tot de toegangen tot en de raadpleging van databanken;

8) het COC ziet gaarne de geleidelijke ontwikkelingen betreffende het SSO en het eenvormig maken van de procedure van de wachtwoorden;

9) de richtlijn betreffende de toegang, het gebruik en de controle van de ICT-middelen van de federale politie zal aandachtig worden bestudeerd nadat ze verschenen is.

72. Met betrekking tot de aanbevelingen geformuleerd door het Comité P onderstreept het COC:

1) dat, naast het uitwerken van preventieve en functionele maatregelen op menselijk en technisch vlak door de diensten van de lokale politie en van de federale politie, een belangrijke maatregel ligt in het invoeren van regelmatige controles zowel intern als extern door de bevoegde controleorganen;

2) dat de rol van de consulent voor de veiligheid essentieel is;

3) dat het absoluut noodzakelijk is om een eenduidige identificatie te hebben van de gebruiker en de invoering van een geldige reden voor de raadpleging in alle gevallen (behalve duidelijk beperkte uitzonderingen) voor alle toepassingen. In dat verband lijkt het ook aanbevolen dat de toegang in raadpleging of in controle niet mogelijk gemaakt wordt wanneer die elementen ontbreken. Tot slot zouden de toepassingen zich automatisch moeten sluiten na een zekere tijd van inactiviteit om te vermijden dat ze onrechtmatig gebruikt worden door iemand anders.

73. Het COC verduidelijkt dat het niet zal nalaten om de evolutie van het dossier op te volgen in de komende maanden en onderstreept dat de opvolging van de toegangen en raadplegingen, wat hem betreft, ook betrekking heeft op de raadpleging van internationale databanken en, vooral, de raadpleging van gemeenschappelijke databanken die recentelijk gecreëerd werden in bepaalde politiezones[29].

3.1.2. Federale politie

74. De commissaris-generaal onderstreept dat de politiediensten nooit ongevoelig gebleven zijn voor de problematiek en dat de opmerkingen van het Comité P niet zonder reactie gebleven zijn, en dit sinds 2005. Vanuit de vaste overtuiging dat het noodzakelijk is om te blijven strijden tegen het onrechtmatig gebruik van de databanken, zal ze erop toezien dat de problematiek van de onrechtmatige toegangen of raadplegingen wordt aangepakt voor alle

[29] Het COC verwijst naar de toepassing “Infotheek” ontwikkeld door de politiezone Westkust (informaticatool voor informatie-uitwisseling) waarover het begin 2016 een eerste tussentijds verslag opgesteld heeft.

databanken, zowel operationele als administratieve, die ter beschikking gesteld worden van de politiediensten.

75. De federale politie formuleert enkele preciseringen en commentaren bij bepaalde punten van het verslag, meer in het bijzonder wat de finaliteit van de controles uitgevoerd door DRI betreft. De aangebrachte preciseringen en commentaar werden geïntegreerd in de tekst zelf van het verslag.

3.1.3. Vaste commissie van de lokale politie

76. De VCLP verheugt zich erover dat ze geraadpleegd werd over het ontwerpverslag en hoopt dat dit zal bijdragen tot de verdere ontwikkeling van een politieorganisatie eigen aan een democratische samenleving, met een bijzondere aandacht voor het waarborgen van de grondwettelijke rechten en vrijheden van elkeen. Ze meent dat het verslag een volledig overzicht geeft van de bestaande regelgeving en procedures alsook van de inspanningen, zowel de preventieve als de reactieve, die worden geleverd om de inbreuken op de *privacy* van burgers door onheus gebruik van databanken te voorkomen en uit te roeien. Ze wijst erop dat het aantal geregistreerde inbreuken en de gevolgen die eraan worden gegeven zeer beperkt zijn. De aard en de context waarin de inbreuken worden gepleegd, zijn ook weinig bekend. Ze preciseert ook dat de reactie op misbruik veelal niet "empathisch" te noemen is.

77. Rekening houdend met het voorgaande, maakt de VCLP zich ernstig zorgen over het *dark number* en het gegeven dat voornamelijk politioneel-technische oplossingen worden voorgesteld. Ze meent dat zij er niet toe zullen bijdragen dat de misbruiken uit de wereld worden geholpen. Ze benadrukt ook dat het raadplegen van databanken een elementaire handeling binnen het politiewerk is en dat de overheden er zich moeten voor behoeden bijkomende regels en procedures in het leven te roepen die niet gebruiksvriendelijk zijn. Door een overdaad aan vooraf te verrichten administratieve handelingen van allerlei aard zou het politiewerk immers worden ondermijnd.

78. De VCLP merkt op dat het preventieve luik, zoals het nu opgebouwd is, met allerlei '*infonews*', berichten en instructies op 'Portal', zonder meer, tenzij een verwijzing naar de verwachte gedragingen van het personeel, slechts een beperkte impact heeft op het terrein. Er is veel meer nodig om bewust omgaan met informatie te realiseren. De onderwerpen moeten dagelijks mondeling worden besproken. Coaching en opvolging op het terrein door leidinggevenden moeten soelaas bieden opdat vanuit een waardengerichte politieorganisatie, die weet waarvoor zij staat, de medewerkers het intrinsiek vanzelfsprekend zouden vinden om geen misbruik van databanken te plegen. In dat verband kan de boodschap van de VCLP als volgt worden samengevat: "uitspreken, bespreken, afspreken en aanspreken". Binnen de politie ligt de nadruk vooral op het "uitspreken", en dan wel op schriftelijke wijze. Er wordt ook enige aandacht besteed aan het "aanspreken", maar dat is momenteel nog beperkt. De VCLP is echter geen voorstander van enige overreactie op dit vlak. Ze pleit integendeel voor een resoluut investeren in het "bespreken" en het "afspreken". Die aspecten zijn niet echt vanzelfsprekend in de hedendaagse politiecultuur noch in de reguliere werking van de politiediensten.

79. De VCLP merkt ten slotte op dat er veel verwacht wordt van de nieuwe functie van consulent "veiligheid en bescherming van de informatie". Ze wijst erop dat een dergelijke functie niet altijd als prioritair beschouwd wordt gelet op de politiecultuur, die operationeel van inslag is, en dat de invoering van de nieuwe functie een impact op de begroting zal hebben. De politieorganisatie lijkt er niet toe geneigd te zijn intern een opleiding te ontwikkelen en te

organiseren, wat ertoe leidt dat de politiediensten hun heil extern gaan zoeken, in de privé. Indien die weg wordt ingeslagen, worden de politiediensten nog extra op kosten gejaagd, ten nadele van het specifieke politiewerk. De uniformiteit naar benadering en de concrete inhoud van de opleiding zal dan een illusie zijn.

3.1.4. Aanvullende beschouwingen van het Vast Comité P

80. Het onderzoeksgebied werd bewust beperkt tot de toegangen tot de klassieke databanken die gebruikt worden door de meeste leden van de politiediensten in de uitoefening van hun activiteiten, aangezien zij het voorwerp uitmaken van haast alle gekende disfuncties. Dat sluit het bestaan van disfuncties in het kader van het gebruik van andere databanken natuurlijk niet uit.

81. Er is waarschijnlijk een *dark number* waarvan de omvang op dit ogenblik onmogelijk kan worden ingeschat. Men kan redelijkerwijs aannemen dat dit grotendeels het gevolg is van het feit dat het moeilijk is om de onrechtmatige toegangen op te sporen omdat zij "verdrinken" in de massa raadplegingen die volkomen legitiem worden verricht in de databanken. Indien er geen bijzondere omstandigheden of kenmerken zijn die er de aandacht op vestigen, is de kans dat disfuncties worden opgemerkt dus gering.

82. Zelfs al kan ze altijd verbeterd worden, die kennis bestaat sinds jaren en is voldoende duidelijk opdat de leden van de politiediensten goed op de hoogte zouden zijn van de beperkingen ter zake. Elke keer dat er een informatiebulletin verschijnt, kunnen de politieverantwoordelijken zich de problematiek (meer) eigen maken. Alles hangt dan af van de wijze waarop de informatie door hen behandeld wordt. Een gewone informatieverspreiding die zich beperkt tot het doorsturen of aanplakken van de informatieblaadjes is uiteraard niet van aard om een blijvende impact te hebben op het personeel. Het Vast Comité P kan alleen maar wensen dat de politieverantwoordelijken zich actief inzetten opdat het concept '*privacy*' over het algemeen en in het kader van de raadpleging van de databanken in het bijzonder concreet geïntegreerd zou worden in de gewone politiewerking. Om dat te realiseren, hoeft niet gewacht te worden op de implementatie van specifieke structuren die middelen vragen die thans niet noodzakelijkerwijs voorhanden zijn noch op de formulering van een specifieke aanbeveling. Er kan veel worden gedaan zonder buitengewone middelen en daarbij kan men verdergaan dan de louter occasionele aandacht die besteed wordt aan het fenomeen wanneer een disfunctie ontdekt wordt of wanneer een informatieblad verschijnt.

83. De vorige beschouwingen tonen inderdaad het belang aan om te werken op het culturele aspect. De leden van de politiediensten moeten zich bewust zijn van het feit dat de samenleving en de burgers zich meer en meer bezorgd tonen over het behoud van het recht op privacy. Dat dit recht geschaad wordt door personen die een deel van de openbare macht in handen hebben is moeilijk aanvaardbaar. De werkelijke integratie van het concept '*privacy*' in de politiecultuur is de beste bescherming tegen misbruiken. Sommige korpsen en diensten hebben al lovenswaardige initiatieven ter zake ontwikkeld of zijn daarmee bezig. Het is dus niet aangewezen om een algemene aanbeveling te formuleren die zich op uniforme wijze tot iedereen zou richten. De situatie moet geanalyseerd worden op het niveau van de verschillende korpsen van lokale politie en van de diensten van de federale politie. De objectieve tekenen dat de politieverantwoordelijken proactief rekening houden met de problematiek zullen, ongetwijfeld, "*markers*" zijn om de wil om de *privacy* te integreren in de politiecultuur te beoordelen. In dat verband wil DRI in de toekomst de nadruk leggen op het responsabiliseren en het bewustmaken voor de problematiek.

84. De hier geformuleerde aanbevelingen zijn uiteraard geen wondermiddel om het fenomeen volledig en definitief uit te roeien. De hiervoor aangehaalde cultuurverandering kan niet op korte termijn verwacht worden en moet dus gepaard gaan met een arsenaal van maatregelen die erop gericht zijn om het onrechtmatig gebruik van databanken, zoveel mogelijk, te voorkomen. Die maatregelen zijn voornamelijk bedoeld om de kans op misbruik te beperken en er tegelijkertijd op toe te zien dat er geen afbreuk wordt gedaan aan de operationaliteit van de politie of dat de intervenanten op het terrein die als een te grote administratieve belasting zouden ervaren. De aanbevelingen zijn voldoende genuanceerd, soepel en aanpasbaar opdat de politieverantwoordelijken de problematiek zouden kunnen bevatten in functie van de werkelijke toestand op het terrein zonder overdreven te reageren en zonder de overgrote meerderheid van de leden van de politiediensten die niet over de schreef gaan te bestraffen. Het Vast Comité P pleit er uiteraard voor dat de nodige middelen in de toekomst kunnen worden vrijgemaakt voor de concrete implementatie van de nieuwe specifieke politiestructuur voorzien in het kader van de *privacy* alsook voor de snelle implementatie van een interne opleiding bij de politie voor de toekomstige consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer.

85. In hoofdzaak, sluit het Vast Comité P zich aan bij de beschouwingen en aanbevelingen geformuleerd door de belanghebbende partijen. Het Comité P neemt meer in het bijzonder de beschouwingen en aanbevelingen over die het COC geuit heeft met betrekking tot de noodzaak om de gebruiker op eenduidige wijze te identificeren, waarbij een geldige reden voor de raadpleging (behalve voor duidelijk afgebakende uitzonderingen) wordt ingevoerd voor alle toepassingen en de toepassingen automatisch worden afgesloten na enige tijd van inactiviteit om onrechtmatig gebruik op andermans naam te vermijden. De dynamiek die bij de federale politie leeft, zou ten volle benut moeten worden om de initiatieven te ontwikkelen die nodig zijn om aanbevelingen te concretiseren die de situatie kunnen verbeteren in overleg met de lokale politie.

4. CONCLUSIES

86. De gekende onrechtmatige raadplegingen van de databanken ter beschikking gesteld van de politiediensten zijn hoofdzakelijk gepleegd buiten het beroepsverband. Allemaal kunnen ze mogelijkerwijs inbreuken op de persoonlijke levenssfeer van de burger inhouden.

87. De analyse van de instrumenten die voorhanden zijn om dit fenomeen te bestrijden toont aan dat:

1) de maatregelen genomen op het vlak van het sensibiliseren en het informeren van leden van de politiediensten voldoende lijken;

2) de registratie van de reden voor de raadpleging ten stelligste aangeraden maar nog altijd niet verplicht is, behalve voor de raadpleging van de foto's van het RRN. Die praktijk zet echter een rem op de ongeoorloofde raadplegingen, brengt de leden van de politiediensten verantwoordelijkheidsbesef bij en vergemakkelijkt de eventuele onderzoeken en de rechtvaardiging van de toegangen tot de databanken;

3) verscheidene elementen pleiten voor een evolutie van het controlesysteem dat op het ogenblik *a posteriori* is: controles die berusten op de verificatie van de rechtmatigheid

van willekeurig geselecteerde raadplegingen zijn niet erg geschikt om de politieverantwoordelijken te sensibiliseren, impact op de sensibilisatie van politieverantwoordelijken is waarschijnlijk weinig blijvend, de kans dat leden van de politiediensten die onrechtmatige raadplegingen hebben gedaan worden onderworpen aan een controle is erg gering en heeft dus een vrij beperkt ontradend aspect, responsabilisering van de lokale politiediensten is voor verbetering vatbaar gelet op feit dat de controle gecentraliseerd is op het niveau van de federale politie die, bovendien, daarover een reflectie opgestart is;

4) een controle op de toekenning van de toegang tot de databanken *sensu stricto* niet bestaat. DRI levert hulp aan de politieverantwoordelijken door "signalen" uit te zenden wanneer problematische situaties ontdekt worden. De gegrondheid van de toekenning van permanente toegangen tot de databanken moet geëvalueerd worden rekening houdend met de specificiteiten van de verschillende politiediensten en met de opdrachten die de personeelsleden daadwerkelijk uitvoeren.

5. AANBEVELINGEN

5.1. Preventieve maatregelen

88. Het is absoluut noodzakelijk dat de politieverantwoordelijken overgaan tot een *kritisch en geïndividualiseerd* onderzoek naar aanleiding van de toekenning van de toegangsmachtigingen tot de databanken. Dat kritische onderzoek zou niet alleen uit eigen beweging uitgevoerd moeten worden in geval van verandering van functie of van wijziging in de toebedeling van de opdrachten van de personeelsleden maar ook geregeld (bijvoorbeeld naar aanleiding van de evaluatie van het personeel). De verantwoordelijken zouden zich ervan moeten vergewissen dat hun personeelsleden er *effectief en concreet*, in functie van de specificiteiten van de politiedienst, van organisatorische verplichtingen en van werkelijk uitgevoerde opdrachten, behoefte aan hebben om *permanent en individueel* te beschikken over toegangen tot de databanken.

89. Rekening houdend met de voordelen die de registratie van de reden voor de raadpleging biedt, lijkt het opportuun om die praktijk verplicht te maken voor alle raadplegingen van de databanken binnen de geïntegreerde politie, waarbij voor de politieverantwoordelijken de mogelijkheid wordt voorzien om er beperkend en gemotiveerd van af te wijken teneinde te kunnen tegemoetkomen aan de specificiteiten of contra-indicaties binnen hun dienst. Die gemotiveerde afwijkingen zouden tijdelijk of permanent kunnen worden toegekend, voor de raadpleging van alle of sommige databanken, in specifiek bepaalde omstandigheden of voor welbepaalde opdrachten. De verplichting om in het veld "reden voor de raadplegingen" een element te registreren dat het mogelijk maakt om eenduidig het personeelslid te identificeren dat een raadpleging vraagt door tussenkomst van een collega zou ook onmiddellijk veralgemeend moeten worden. In dat opzicht zou het vergemakkelijken van de registratie van de reden voor de raadpleging om de praktijk vanzelfsprekender en gebruiksvriendelijker te maken een meerwaarde zijn (verbetering van de interface van de raadpleging van de databanken).

90. Het is wenselijk om de preventie op technisch vlak en op het vlak van informatica om onrechtmatige toegangen te voorkomen uit te werken. Er zou onder andere aan de gebruiker van de portaalsite van de politie kunnen worden voorgesteld om het veld "reden voor de

raadpleging" in te vullen voor de eigenlijke raadpleging, om de identificatie te voorzien van de werkelijke aanvrager van een raadpleging of om de toegang tot de databanken te beperken tot de entiteiten die gecodeerd zijn in een dossier geopend in ISLP.

91. Als de politieverantwoordelijken specifieke maatregelen zouden nemen om recidive te voorkomen in hoofde van de leden van de politiediensten die schuldig bevonden zijn aan onrechtmatige raadpleging van een databank, zou de doeltreffendheid van de bestraffing ter zake kunnen toenemen. Dat zou bijvoorbeeld kunnen gaan over de intrekking van de machtiging tot *rechtstreekse* toegang tot een of meer databanken voor een zekere duur of de uitoefening door de politieverantwoordelijken van controles *a posteriori* gericht op het betrokken personeelslid gedurende een bepaalde periode.

5.2. Controlemaatregel

92. De uitvoering van controles *a posteriori* zou verplicht moeten gemaakt worden door elk korps en elke dienst van de geïntegreerde politie. De principes en de grote lijnen van die controles zouden het voorwerp moeten uitmaken van een overleg tussen de componenten van de geïntegreerde politie op basis van de richtlijn van de federale politie die binnenkort van kracht zal worden. Die nieuwe benadering zou de volgende essentiële kenmerken moeten vertonen:

1) de controles zouden moeten worden uitgevoerd in naleving van de algemene beginselen van finaliteit, proportionaliteit, subsidiariteit en transparantie;

2) de controles zouden geregeld en uit eigen beweging uitgevoerd moeten worden door de lokale en federale politiediensten met de steun van DRI teneinde rekening te houden met de specificiteiten inherent aan elke politiedienst. Elk personeelslid zou geregeld aan bod moeten komen in de controleprocedure om de kans om onrechtmatige toegangen op te sporen significant te doen toenemen. De personeelsleden die vrijgesteld zijn van de verplichting om een reden voor de raadpleging te registreren zouden ook aan die controles onderworpen moeten worden om na te gaan of zij geen misbruik maken van die faciliteit en of de beperkingen van de toegekende vrijstelling goed nageleefd worden. De frequentie van de controle zou bepaald moeten worden afhankelijk van de omvang van elke politiedienst of elk politiekorps en afhankelijk van de steun die geleverd kan worden door de federale politie. De organisatie van die controles zou idealiter kunnen worden toevertrouwd aan de toekomstige consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer;

3) de concrete en praktische modaliteiten voor de registratie van de redenen voor de raadpleging zouden moeten worden vastgelegd op het niveau van de verschillende lokale politiekorpsen en diensten van de federale politie zodat zij niet alleen relevant en "sprekend" zouden zijn voor de controleurs maar ook voor de leden van de politiediensten opdat zij hun raadplegingen, zo nodig, gemakkelijk zouden kunnen rechtvaardigen (performante functie van geheugensteun);

4) de eigenlijke controle zou moeten berusten op een algemeen onderzoek van de raadplegingen dat erop gericht is om eventuele abnormale situaties op te sporen op basis van relevante criteria en indicatoren. De indicatoren van mogelijke onrechtmatige toegangen zouden globaal kunnen worden bepaald maar ook afhankelijk van de situatie

en de specificiteiten van de politiekorpsen of -diensten. Er zouden ook indicatoren bepaald moeten worden op basis van een kritische analyse van de beroepsactiviteiten om eventuele onrechtmatige praktijken op te sporen die niet altijd noodzakelijkerwijs evident zijn voor de leden van de politiediensten en die misschien routinematig uitgevoerd worden (bijvoorbeeld het uitvoeren van controles in de ANG in het kader van administratieve dossiers). Op niet-limitatieve wijze zouden de volgende elementen, bijvoorbeeld, indicatoren kunnen zijn die kunnen leiden tot een meer diepgaande controle van de raadplegingen van een aan de controle onderworpen lid van de politiediensten:

- afwezigheid van registratie van een reden voor de raadpleging terwijl het lid van de politiedienst niet werd vrijgesteld van die verplichtingen door de politieverantwoordelijken;
- inschrijving van een reden voor de raadpleging die onvoldoende relevant is of die duidelijk in tegenspraak is met de lokale voorschriften;
- uitvoering van een abnormaal aantal raadplegingen;
- uitvoering van raadplegingen op ongewone uren in vergelijking met de dienstprestaties van het gecontroleerde personeelslid;
- raadplegingen betreffende andere personeelsleden van de zone of de politiedienst waartoe het personeelslid behoort;
- raadplegingen die lokale politieke verantwoordelijken, lokale vooraanstaande figuren als voorwerp hebben;

5) indien potentieel ongewone situaties worden ontdekt, zou moeten worden overgegaan tot diepgaande, doelgerichte controles van de omstreden raadplegingen. Zij zouden bestaan uit vragen om rechtvaardiging gericht aan de betrokken personeelsleden teneinde hun rechtmatigheid vast te stellen.

5.3. Concretisatie

93. Het is wenselijk dat de geformuleerde aanbevelingen tegenstelbaar worden gesteld aan alle korpsen en diensten van de geïntegreerde politie. Die doelstelling zou bijvoorbeeld bereikt kunnen worden door ze te integreren in de richtlijn MFO-3.

6. OPVOLGING

94. De inplaatsstelling van de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer en van het platform voor de veiligheid en de bescherming van de gegevens biedt voor de politiediensten een kans om een gestructureerde reflectie in het leven te roepen en om een echt beleid uit te werken dat er meer bepaald op gericht is om onrechtmatige raadplegingen van de databanken te voorkomen. Hoewel er op dit ogenblik geen geactualiseerde situatie voorhanden is, lijkt de ontplooiing van dit nieuwe instrument verre van beëindigd te zijn binnen de politiediensten. Een probleem van middelen staat de inplaatsstelling van het platform voor de veiligheid en de bescherming van gegevens in de weg. Er werd gezocht naar het specifieke opleidingsaanbod maar dat kon nog niet worden geconcretiseerd.

95. Het Vast Comité P is van plan om de wijze waarop de diensten van de geïntegreerde politie een beleid inzake veiligheid en bescherming van de persoonlijke levenssfeer bepalen en uitvoeren aandachtig op te volgen. Die opvolging zal meer in het bijzonder de gelegenheid zijn

om zich ervan te vergewissen of er rekening gehouden is met de aanbevelingen geformuleerd inzake de strijd tegen onrechtmatige toegangen van de databanken.

96. BIJLAGE

97. De lijst met gebruikte afkortingen.

BIJLAGE

GEBRUIKTE AFKORTINGEN

Afkorting	Betekenis
ANG	Algemene nationale gegevensbank
CALog	Administratief en logistiek kader van de politie
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
CIDA	Communicatie- en informatiedienst van het arrondissement
CWR	Centraal wapenregister
DGR	Algemene directie van het middelenbeheer en de informatie van de federale politie
DIV	Dienst voor inschrijvingen van voertuigen
DRI	Directie van de politionele informatie en de ICT-middelen van de federale politie
FEEDIS	'*Feeding Information System*' – Informaticatoepassing gebruikt binnen de federale politie
ICT	'*Information and Communication Technology*'
ISLP	'*Information System for Local Police*' – Politioneel informaticasysteem gebruikt in de lokale politiezones
MFO-3	Gemeenschappelijke richtlijn MFO-3 van 14 juni 2002 van de Ministers van Justitie en van Binnenlandse Zaken betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie
Portal	Portaalsite van de politie
Privacywet	Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens
RPO	Toepassing "onvolledige nummerplaten"
RRN	Rijksregister / Registre National
SCHEVAL	'*Schengen Evaluation Working Group*'
SIDIS	Système d'information des détentions / Detentie-informatiesysteem
SSO	'*Single Sign On*' – Technische aanpassing bedoeld om de informatica-'*logins*' van de politie te harmoniseren
VCLP	Vaste Commissie van de lokale politie
WPA	Wet van 5 augustus 1992 op het politieambt