INHOUDSTAFEL

Toezichtsonderzoek naar de middelen die door de geïntegreerde politie worden ingezet om de risico's gebonden aan de toegang tot de politionele informatie in te perken, in het bijzonder voor de informatie betreffende het operationeel domein en/of de zogenaamd gevoelige informatie

1 SITUERING EN SAMENVATTING VAN HET ONDERZOEK

Het Vast Comité P heeft een opvolgingsonderzoek gevoerd naar de aanbevelingen die het had geformuleerd in het toezichtsonderzoek naar de middelen die door de geïntegreerde politie worden ingezet om de risico's gebonden aan de toegang tot de politionele informatie in te perken, in het bijzonder voor de informatie betreffende het operationeel domein en/of de zogenaamd gevoelige informatie.

De bedoeling van het aanvankelijk onderzoek was een stand van zaken op te maken van de beveiliging van de toegang tot de politionele informatie in de politiediensten. In het kader van dat onderzoek waren de volgende aanbevelingen geformuleerd:

- in deze tijden van budgettaire beperkingen, aan de "verleiding" weerstaan om de investeringen in beveiliging (van informatie of andere) tot het uiterste te beperken;
- de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer zo snel mogelijk aanwijzen en de uitoefening van hun opdrachten vergemakkelijken;
- snel aan het programma van de politiescholen een specifieke opleiding toevoegen voor de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer die het kader overschrijdt van de loutere informatie en die handelt over de management-, informatica- en wettelijke aspecten van die functie;
- op middellange termijn, rekening houdend met de snelle evolutie van de omgeving (technologieën, bedreigingen, praktijken,…), zal de functie ondersteund moeten worden door geregelde bijscholingen die in de toekomstige opleidingsplannen voorzien moeten worden;
- de onafhankelijkheid die moet worden toegekend aan de rol van consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer in acht nemen en die rol niet toekennen als cumul bij bepaalde andere functies, meer in het bijzonder die van systeembeheerder.

Om die opvolging uit te voeren, werden eind 2016 gesprekken gevoerd met de verantwoordelijken van het Commissariaat-generaal - CG/Information Security & Privacy Office (ISPO). Er werd rekening gehouden met het normatief raamwerk dat op Europees vlak opgesteld was.

2 ONDERZOEKSBEVINDINGEN

2.1 AANWIJZING VAN CONSULENTEN IN DE POLITIEKORPSEN

Het koninklijk besluit betreffende de consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer werd bekendgemaakt op 6 december 2015. De federale politie heeft de lijst opgesteld van de consulenten die binnen haar component aangewezen waren en gaat de namen (± 50 personen) zeer binnenkort meedelen aan het Controleorgaan (COC) en aan de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL).

De lokale politiezones moeten ook de naam van de aangewezen personen meedelen aan beide voornoemde instanties. De federale dienst ISPO heeft geen zicht op het lokaal niveau maar de Vaste Commissie van de lokale politie (VCLP) heeft verduidelijkt dat, in de meeste gevallen, de politiezones hun consulent hebben aangewezen[1]. Er wordt aan herinnerd dat, gezien de beheersautonomie gebonden aan de politiestructuur op twee niveaus, niet voorzien is om een consulent aan te wijzen voor het geheel van de geïntegreerde politie.

---

[1] Soms wordt deze functie uitgeoefend voor verschillende lokale politiezones.

Op federaal vlak werd het functieprofiel van de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer opgenomen in de OT3 (organieke tabel opgesteld ingevolge de optimalisatie van de federale politie) op gedeconcentreerd niveau.

In 2012 heeft de Europese Unie beslist om de bescherming van de persoonsgegevens te hervormen en om een nieuwe verordening in te voeren. In april 2016 werden twee teksten gepubliceerd: de AVG (de Algemene verordening gegevensbescherming, ook wel GDPR genoemd, wat staat voor General data protection regulation)[2] voor alle sectoren (privé en overheid) alsook een richtlijn voor het domein van politie en justitie[3]. Die twee teksten zullen in Belgisch recht omgezet moeten worden tegen uiterlijk mei 2018 en zullen grondige wijzigingen aanbrengen aan de wet op de bescherming van de persoonlijke levenssfeer en aan de wet op het politieambt.

2.2 OPLEIDINGEN AANGEBODEN IN DE POLITIESCHOLEN

Wat de opleidingen betreft, moeten twee domeinen worden onderscheiden: privacy en veiligheid. De opleidingen voor de veiligheidsconsulenten zijn nog niet effectief. Er zijn verscheidene partnerschappen voorzien met andere overheidsdiensten maar om diverse redenen konden zij nog niet in plaats worden gesteld. Inzake privacy is er geen opleiding die structureel verstrekt wordt.

Er wordt een modulaire opleiding inzake bescherming van persoonsgegevens uitgewerkt. Twee modules werden al gegeven eind 2015-begin 2016. Ze handelden over "bescherming van persoonsgegevens: basisconcepten en algemene principes" en "bescherming van persoonsgegevens: specifiek karakter van operationele gegevens". Deze opleiding is hoofdzakelijk bestemd voor personeelsleden van de federale politie maar leden van de lokale politie kunnen er ook aan deelnemen.

Andere thematische modules zouden moeten volgen: specificiteit van operationele gegevens, toepassing van de interne richtlijn[4] "ICT-privacy" houdende de regels inzake gegevens met betrekking tot toegangsbadges, telefoonnummers, gsm-nummers, gebruik van en toezicht op ICT-netwerken in ruime zin, enz.

De opleidingen worden ontwikkeld met de hulp van actoren zoals DGR-DRI (Directie van de politionele informatie en de ICT-middelen) en Interpol. Maar er dient op te worden gewezen dat de kennis ter zake berust bij enkele personen.

2.3 OPRICHTING VAN HET PLATFORM VOOR DE VEILIGHEID EN DE BESCHERMING VAN DE GEGEVENS

In dit stadium bestaat het platform nog niet. Hoewel het koninklijk besluit van 14 november 2006 betreffende de organisatie en de bevoegdheden van de federale politie in artikel 2.1°.e) het volgende stelt: *"in overleg met de Vaste Commissie van de lokale politie, de bepaling van normen en een gestandaardiseerde aanpak inzake veiligheid van de informatie en bescherming van de persoonlijke levenssfeer van toepassing op de federale politie of op heel de geïntegreerde politie"*, had de dienst ISPO op het ogenblik van ons bezoek geen stappen ondernomen om de inplaatsstelling van dat platform te coördineren gelet op zijn capaciteitsgebrek. Intussen werden met de VCLP stappen gezet om dat platform op te richten.

Het platform voor de veiligheid en de bescherming van de gegevens zou tevens als opleidingsplaats dienst moeten doen.

---

[2] Deze verordening (EU) 2016/679 is van kracht geworden op 24 mei 2016, maar vanaf die datum is een overgangsperiode van 2 jaar voorzien. De Privacycommissie, de ondernemingen en de organisaties hebben tot 25 mei 2018 de tijd om zich te schikken naar de eisen van de AVG (bron: https://www.privacycommission.be).

[3] Richtlijn (EU) 2016/680.

[4] Deze richtlijn bevindt zich in de finale ontwikkelingsfase. Ze zal van toepassing zijn zodra ze verspreid is.

2.4 UITWERKING VAN HET BELEID INZAKE BEVEILIGING EN BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER BINNEN DE POLITIEKORPSEN

Het politiewerk wordt sowieso complex gemaakt door het feit dat er gegevens van allerlei aard moeten worden beheerd, operationele gegevens zijn daar slechts een deel van.

Zoals eerder aangehaald, heeft de Europese Unie het wettelijk kader hervormd om de gegevens te beschermen en een nieuwe beschermingsverordening in plaats te stellen. Sommige bepalingen van de AVG en de richtlijn (EU) 2016/680[5] bestemd voor de sectoren politie en strafrechtspleging zullen moeten worden verduidelijkt door het Belgisch recht tegen uiterlijk mei 2018. De andere Belgische bepalingen met betrekking tot de CBPL en de concrete maatregelen zullen overigens ook moeten worden aangepast om in overeenstemming te zijn met de AVG.

Via de dienst ISPO neemt de federale politie deel aan de Europese werkzaamheden en aan de coördinatievergaderingen die worden geleid door de FOD Justitie en tot doel hebben om deze teksten tegen 2018 toe te passen.

Op basis van de volledige titel van de richtlijn "politie justitie" zou men kunnen vermoeden dat ze enkel van toepassing is op de opdrachten van gerechtelijke politie, terwijl zij ook betrekking heeft op de activiteiten van bestuurlijke politie. Wanneer de politiediensten persoonsgegevens verwerken voor andere doeleinden, bijvoorbeeld in het kader van personeelsbeheer, zal de AVG echter van toepassing zijn.

In vergelijking met de huidige wetgeving versterkt de AVG de rechten van personen met betrekking tot hun persoonsgegevens. Daartoe zijn de rollen en de verantwoordelijkheden van de toezichthoudende autoriteit[6], van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming gevoelig uitgebreid, wat alleen maar een positieve invloed kan hebben op de algemene beveiliging van gegevens, het voorwerp van dit onderzoek. De AVG schuift ook bepaalde procedures en technieken naar voren zoals de anonimisering, de pseudonimisering en de versleuteling.

De richtlijn "politie justitie" voorziet de mogelijkheid tot inperking van de rechten van de betrokkene om ingelicht te worden over een verwerking van zijn gegevens, om er toegang toe te hebben alsook om ze recht te zetten of te wissen, wanneer de uitoefening van die rechten bijvoorbeeld onderzoeken zou kunnen belemmeren, misdrijven voorkomen of opsporen of de openbare veiligheid beschermen. Er dient opgemerkt dat de richtlijn de nadruk legt op het feit dat het in een democratische samenleving belangrijk is dat deze beperkingen beantwoorden aan de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit. Daarnaast heeft deze richtlijn ook als doel de grensoverschrijdende uitwisseling van politionele informatie te vergemakkelijken.

Wat de politiezones betreft, is het waarschijnlijk dat sommige zones verder staan in de uitwerking van hun beleid inzake beveiliging van gegevens en privacy maar de federale politie heeft daar geen zicht op. Men moet beseffen dat het "beleid" een ruim concept is en dat het bijvoorbeeld geconcretiseerd zou kunnen worden in een huishoudelijk reglement, al naar gelang wat de zone beslist.

2.5 SYNERGIEËN MET HET CENTRUM VOOR CYBERSECURITY BELGIË (CCB) OF ANDERE INSTELLINGEN

Inzake informatiebeveiliging stelt het CCB veiligheidsnormen, -standaarden en -richtlijnen op voor de informatiesystemen van de overheidsdiensten, het coördineert die en ziet toe op hun naleving. Het CCB werkt ten bate van het volledige grondgebied (privé-publiek, burgers, …) en werkt samen met andere diensten waaronder de politiediensten, volgens de verkregen informatie.

---

[5] Richtlijn "politie justitie": richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

[6] De richtlijn eist dat er minstens een onafhankelijke toezichthoudende autoriteit wordt opgericht die nagaat of de richtlijn wordt toegepast.

Inzake opvolging van cyberaanvallen worden de bedreigingen voortdurend opgevolgd door de federale politie in overleg met het CCB en de andere FOD's. Informatie en ervaringen worden uitgewisseld en daarna verder verspreid onder de leden van de politiegemeenschap en aan externe diensten. Niettemin is er nog geen structuur op poten gezet om te communiceren met de politiezones.

3 CONCLUSIES

De maatregelen die moeten worden toegepast inzake informatiebeveiliging en eerbiediging van de privacy, uiteengezet in het aanvankelijk onderzoek, zijn nog niet helemaal doorgevoerd. Het gaat immers om een gespecialiseerde materie die voortdurend verandert en uitgaat van het internationaal vlak. De expertise en de kennis om de concepten en principes te bevatten en ze te concretiseren in een normatief raamwerk bevinden zich bij een beperkt aantal deskundigen; bovendien is de hoeveelheid van de door de politiediensten te verwerken gegevens erg groot en is de aard van die gegevens erg divers.

De inplaatsstelling van deze maatregelen wordt geremd door o.m. een gebrek aan capaciteit en bepaalde andere prioriteiten. Het beleid inzake beveiliging en privacy behoort tot de bevoegdheid van elk politiekorps. De federale politie heeft geen zicht op de initiatieven genomen door de politiezones. Aangezien de politiestructuur niet voorziet in een orgaan voor de coördinatie inzake informatiebeveiliging en bescherming van de persoonlijke levenssfeer tussen de twee politieniveaus, zullen er waarschijnlijk initiatieven moeten komen vanuit het lokale niveau om het platform te concretiseren of om de toekomstige actoren aan te wijzen. Er is wel het coördinatiecomité van de geïntegreerde politie (CCGPI)[7], maar dat comité is vooreerst belast met de politionele strategie.

2018 wordt een sleuteljaar want in dat jaar moeten de meest veeleisende Europese richtlijnen inzake beveiliging van persoonsgegevens, zijnde de AVG en de richtlijn (EU) 2016/680, in Belgisch recht zijn omgezet.

De politiediensten zullen dus op dat ogenblik klaar moeten zijn. Het lijkt nodig om de maatregelen die in ontwikkeling zijn, zoals de opleiding van de consulenten, het coördinatieplatform, de coördinatie tussen de politiezones onderling en tussen de politiezones en de federale politie, van nu af aan af te toetsen aan de omzetting in Belgisch recht van de AVG en van de richtlijn "politie justitie". Zo zou de opleiding van de consulenten nu al rekening moeten houden met de grotere rol en de toegenomen verantwoordelijkheden van de toekomstige functionaris voor gegevensbescherming.

Door van alle actoren van politie en justitie te eisen dat ze meer aandacht besteden aan de bescherming van de persoonsgegevens waarover ze beschikken en door hen beter bewust te maken van de risico's waaraan ze blootstaan, zouden deze teksten een positieve invloed moeten hebben op de verbetering van de beveiliging van politionele gegevens in ruime zin.

Het Comité P stelt vast dat de politiediensten zich terdege bewust zijn van de externe dreiging die uitgaat van criminele en terroristische organisaties. Niettemin wenst het Comité P nogmaals te wijzen op het bestaan van een interne "dreiging" in de vorm van kwaadwillige acties maar ook (en wellicht vaker) fouten of slordigheden bij het bewaren of het overmaken van gegevens, en dat hiermee absoluut rekening dient te worden gehouden bij het ontwerpen van informatiesystemen en het opstellen van procedures (*cf.* de "privacy by design" aanbevolen door de AVG).

---

[7] 26 MAART 2014 - wet houdende optimalisatiemaatregelen voor de politiediensten, invoeging van artikel 8ter in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.