



## Aanbeveling nr 03/2013 van 24 april 2013

**Betreft:** aanbeveling uit eigen beweging over het gebruik van traceertoestellen door politiediensten ten aanzien van hun personeelsleden (CO-AR-2011-014)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 30;

Gelet op het verslag van de heer Stefan Verschuere;

Brengt op 24 april 2013 de volgende aanbeveling uit:

## I. CONTEXT

### A. Gebruik van traceertoestellen bij de politie

1. Reeds enkele jaren installeert de politie in hun voertuigen traceertoestellen of ze stellen ze ter beschikking van hun personeelsleden. Met deze apparatuur kunnen de leden gelokaliseerd worden of kunnen er gegevens worden ingewonnen en geanalyseerd over het gebruik van de voertuigen of de voorwerpen die ze vervoeren (bijvoorbeeld een wapen of defibrillator<sup>1</sup>). Het zijn meestal privébedrijven die de traceersystemen ontwikkelen en aanbieden maar ze kunnen ook intern uitgewerkt worden door de politiediensten zelf of andere overheidsdiensten (zoals de civiele bescherming).
2. Bepaalde apparaten kunnen uitsluitend voertuigen lokaliseren terwijl andere het gebruik van het voertuig zelf kunnen volgen. In dit laatste geval kan de apparatuur vergeleken worden met een "zwarte doos" die een serie gegevens over het voertuig opslaat.
3. Onder de bestaande systemen is er het "AVL" systeem (Automated Vehicule Location). Dit systeem lokaliseert een voertuig (via een GPS of radiosignaal, zoals bijvoorbeeld het ASTRID-netwerk). De toestellen zijn altijd zo geconfigureerd dat zij verbonden zijn met een personeelslid, aangezien zij via een authenticatie of identificatie geactiveerd worden door de bestuurder.
4. Er bestaan ook andere apparaten die eerder gegevens verzamelen waarmee de historiek van het voertuiggebruik kan worden getoond. De verzamelde gegevens zijn :
  - vaartvermeerderingen van het voertuig
  - bruske remmingen
  - remafstanden
  - aansteken van zwaailichten
  - sirenegebruik
  - gebruik van dimlichten
  - gebruik van een gun lock
  - impactdetectie
  - afgelegde afstand
  - rijdata en -uren
  - geolocatie van de voertuigen

---

<sup>1</sup> De samenwerking die bestaat tussen de politie en de brandweer om defibrillators te lokaliseren toont aan dat het traceren ook de activiteiten kunnen betreffen die niet tot de belangrijkste verantwoordelijkheden van de politie behoren.

- onderhoudshistoriek van het voertuig
5. Draagbare traceertoestellen kunnen ook één bepaald personeelslid lokaliseren. Deze toestellen worden gebruikt om de sectie te lokaliseren waartoe het lid van de politiedienst behoort en ze worden hoofdzakelijk gebruikt bij gezamenlijke operaties waaraan personeelsleden uit verschillende korpsen deelnemen (verschillende lokale politiezones, of lokale en federale politie).
  6. En tot slot nam de Commissie kennis van een voorstel tot samenwerking tussen politie en brandweer. Dit voorstel maakt het mogelijk de defibrillatoren op te sporen die in sommige politieauto's geïnstalleerd werden. Bij noodgevallen kan het toestel getraceerd worden dat zich het dichtst bij de plaats bevindt waar het nodig is. Zo is het mogelijk om beroep te doen op de nooddiensten die zich het dichtst bij de plaats van de interventie bevinden. Dit soort traceren is dus niet verbonden met een voertuig maar eerder met de defibrillator zelf.
  7. De Commissie verzocht de Federale politie over dit onderwerp al in oktober 2011 om informatie. Alvorens deze aanbeveling goed te keuren, raadpleegde de Commissie, de Vaste Commissie Lokale Politie, de Federale politie en het Comité P. Op 12 november 2011 vond er in de lokalen van de Politie van Brussel Noord met de Federale politie ook een vergadering plaats om hun ervaringen te bespreken die ze hebben opgedaan met de traceertoestellen die al in bepaalde voertuigen werden geïnstalleerd en de systemen die mogelijks in de toekomst kunnen worden aangewend.

## **B. traceertoestellen die gegenereerde gegevens gebruiken**

8. De traceertoestellen kunnen in meerdere contexten gebruikt worden. Zo is er het **operationeel aspect**; deze toestellen kunnen in reële tijd een voertuig of team lokaliseren. Op die manier is er een beter beheer mogelijk van de interventies, in functie van de beschikbare elementen die zich het dichtst bij het voorval bevinden maar ze dienen ook om een team in moeilijkheden efficiënt hulp te kunnen bieden, voertuigen te begeleiden bij prioritaire evenementen of bij specifieke politieke operaties zoals manifestaties, sportwedstrijden, enz. Het staat vast dat het traceren van defibrillatoren tijdwinst oplevert om een persoon in nood te helpen.
9. Het **logistiek aspect** van de traceertoestellen (en meer bepaald de systemen voor "fleetmanagement", laat toe dat het onderhoud efficiënter verloopt, bijv. voor de reparatie van bepaalde mechaniek of stukken. Ook het beheer van het wagenpark verloopt efficiënter omdat de afgelegde afstand per voertuig of de rijd- en stoptijden gekend zijn.

10. Bepaalde "fleetmanagement" systemen kunnen ook de **bestuurder bijstaan** en hem met een geluidssignaal verwittigen om schade te vermijden aan technische onderdelen zodat de motor na een bepaalde tijd of lage batterijstand blijft functioneren.
11. Een dergelijk toestel staat ook in voor de **beveiliging** van het voertuig omdat het niet kan starten zonder een activeringsbadge en het belet dat het voertuig wordt gestolen. De badge kan ook verbonden zijn met een beveiligingsmechanisme om te beletten dat het dienstwapen dat in het voertuig zit, wordt bemachtigd.
12. En tot slot kunnen de traceertoestellen ook de gebruikers **controleren** (de personeelsleden van de politie), à charge of à décharge van de gebruikers. De identificatie van de bestuurder laat bijvoorbeeld toe om bij een incident te bepalen wie daadwerkelijk achter het stuur zat tijdens het incident. Zo kunnen bepaalde niet-toegestane gedragingen geïdentificeerd worden en aan een persoon worden toegeschreven zoals bruusk remmen (dat een rijstijl weergeeft), overdreven snelheid (al dan niet gerechtvaardigd), het gebruik van het zwaailicht en de sirene, of de snelheid net voor een ongeval).
13. De politiediensten die een dergelijk systeem invoerden, konden een gevoelige daling vaststellen van het aantal incidenten en gevallen van voortijdige slijtage (remmen, banden,...)<sup>2</sup>. Er is ook gebleken dat deze systemen hebben toegelaten om bepaald rijgedrag te herkaderen of om te dienen als bewijs bij een incident met derden (al dan niet gebruik van zwaailicht, rijnsnelheid,...).
14. De doorgifte van de verzamelde gegevens en de toegang tot die gegevens kunnen technisch gezien op verschillende manieren gebeuren. Uit de informatie die de verschillende politiezones hebben verstrekt, zijn dit de meest courante communicatiemethodes:
  - een eerste bestaat erin om alle informatie van de "zwarte doos" van het voertuig over te dragen via een fysieke drager (usbstick of badge) naar de computer van de politieautoriteit belast met de verwerking van de informatie. In dit eerste geval worden de gegevens niet extern verwerkt en zijn ze niet toegankelijk voor externe leveranciers;
  - een tweede methode bestaat erin om de verzamelde gegevens te verstrekken aan een bedrijf<sup>3</sup> dat een fleetmanagementsysteem aanbiedt (meestal draadloos, zoals bijvoorbeeld per GPRS-pakket via het gsm-netwerk) en de bevoegde politieautoriteit op afstand via een specifieke applicatie een toegang te geven tot die gegevens. In dit geval

---

<sup>2</sup> Zie bijvoorbeeld antwoord van de Minister op de mondelinge vraag nr. P1536 van Michel Doomst, Kamer, 52 Plen. 135.

<sup>3</sup> Of de verwerker dat het bedrijf kiest om de gegevens te bewaren.

bewaart het bedrijf (of zijn verwerker) dat het systeem levert, de gegevens gedurende een door hem bepaalde termijn<sup>4</sup>;

- en tot slot kunnen de gegevens ook zonder fysieke drager rechtstreeks verstrekt worden via hertz transmissie naar de politieserver op een interne server, zonder via een derde te passeren.

15. Informatica- en softwareapplicaties maken het mogelijk dat de gegevens kunnen worden verwerkt, dat ze toegankelijk zijn en dat ze kunnen onderzocht worden, bijvoorbeeld door geglobaliseerde of gedetailleerde verslagen (per chauffeur of per voertuig) te maken. De toegang tot die gegevens kan eveneens op afstand gebeuren, al naargelang de configuratie van het gekozen traceersysteem en de technische configuraties.

## **II. ONDERWERP VAN DEZE AANBEVELING**

16. De Commissie stelt vast dat de verwerkte gegevens betrekking hebben op zowel het gebruik van de voertuigen als het gedrag van de gebruikers, meer bepaald de korpsleden van de politie. In bepaalde bestaande systemen, moeten die korpsleden zich overigens identificeren met een badge waarmee ze het voertuig kunnen starten of waarmee ze toegang kunnen hebben tot bepaalde lokalen van de politiepost. Daaruit blijkt dus dat het gebruik van badges verbonden aan een traceersysteem deel uitmaken van een breder controlesysteem. Deze aanbeveling zal zich niet buigen over deze bijzondere systemen.

17. De Commissie heeft begrepen dat de federale politie bij bepaalde opdrachten (zoals geldtransporten) nu al gebruik maakt van traceertoestellen en dat bepaalde lokale politiezones eveneens dergelijke systemen gebruiken<sup>5</sup>.

18. De Commissie heeft geen volledig zicht op de verschillende functies en toepassingen van de traceersystemen daar waar ze tot nu toe werden geïnstalleerd. Inderdaad, de verschillende politiezones die beslisten om een dergelijk systeem te implementeren, hebben niet noodzakelijk voor hetzelfde systeem of dezelfde leverancier gekozen. Dit betekent dat niet alle diensten op dezelfde manier werken, dezelfde gegevens verzamelen of dezelfde kenmerken vertonen.

19. De Commissie is er zich bewust van dat deze traceertoestellen talrijke gegevens verwerken, waaronder ook persoonsgegevens. Daarom achtte zij het nuttig om op grond van de WVP,

---

<sup>4</sup> Een leverancier gaf de Commissie als voorbeeld een dienstenaanbieder van fleetmanagement die de gegevens gedurende een jaar bewaart.

<sup>5</sup> Antwoord op de schriftelijke vraag van Dirk Claes nr. 4-6579 van 27 januari 2010 aan de Minister van Binnenlandse Zaken, parlementaire vragen, senaat, zitting 2009-2010, mondelinge vraag nr. P1536 van Michel Doomst, Kamer 52, PLEN 135.

nader te omschrijven onder welke voorwaarden het gebruik van die traceertoestellen binnen de politiediensten kan worden omkaderd, en om hierover praktische richtlijnen uit te vaardigen.

### III. TOEPASSELIJKE WETTEN

#### A. Het grondrecht opgenomen in artikel 22 van de Grondwet

20. Artikel 22 van de Grondwet bepaalt "*Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht*". Dit artikel moet begrepen worden in het licht van artikel 8 van het EVRM, dat ook van toepassing is op de werkplaats<sup>6</sup>.

#### B. Het geheim van de elektronische communicaties

21. De **artikelen 314bis en 259bis van het Strafwetboek** bestraffen respectievelijk eenieder (artikel 314bis §1) of ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft (artikel 259bis, §1) die:

- "*ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie;*
- "*ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen*".

22. **Artikel 124 van de wet van 13 juni 2005** betreffende de elektronische communicaties (hierna de WEC) bepaalt: "*Indien men daartoe geen toestemming heeft gekregen van alle andere, direct of indirect betrokken personen, mag niemand :*

- 1° *met opzet kennis nemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is;*
- 2° *met opzet de personen identificeren die bij de verzending van de informatie en de inhoud ervan betrokken zijn;*

---

<sup>6</sup> EVRM, Niemitz vs. Duitsland, 16 december 1992, Serie A, nr. 251, Halford vs. Verenigd Koninkrijk, 25 juni 1997, Rec III, blz.39.

*3° onverminderd de toepassing van de artikel en 122 en 123, met opzet kennis nemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon;  
4° de informatie, identificatie of gegevens die met of zonder opzet werden verkregen, wijzigen, schrappen, kenbaar maken, opslaan of er enig gebruik van maken.”*

23. De Commissie meent dat indien de communicatie van locatiegegevens binnen het toepassingsgebied van deze bepalingen kunnen vallen, wel moet worden nagegaan dat artikel 123 WEC, de betrokken politieautoriteit niet in de weg staat aangezien de bedoelde communicaties persoonlijk aan haar geadresseerd zijn.
24. De Commissie oordeelde inderdaad reeds dat artikel 124 WEC toelaat dat de ontvangers van de communicatie wettig gebruik kunnen maken van de communicatie die aan hen persoonlijk werd gericht mits de WVP wordt nageleefd<sup>7</sup>.

### **C. Bescherming van locatiegegevens**

25. Krachtens artikel 123 WEC mogen uitsluitend operatoren van mobiele netwerken locatiegegevens gebruiken op voorwaarde dat de verwerking past in het kader van de levering van een dienst met verkeersgegevens of locatiegegevens.
26. De locatiegegevens die in de traceertoestellen worden geëxploiteerd, hebben geen betrekking op deze bepalingen aangezien die gegevens niet gegenereerd worden door een operator van een mobiel netwerk maar GPS-gegevens zijn die rechtstreeks afkomstig zijn van een geolocatieterminal.
27. De Commissie benadrukte reeds dit onderscheid met de hiernavolgende conclusie: *“Bijgevolg zijn de abonnees en gebruikers van dit type dienst enkel beschermd door de algemene wet betreffende de persoonlijke levenssfeer en niet door de specifieke, bijkomende regels betreffende de elektronische communicatie. De gebruikers van dit type dienst krijgen dus minder bescherming aangeboden en er is een verschil in bescherming naargelang de locatiedienst gebruik maakt van locatiegegevens afkomstig van een communicatienetwerk (bijvoorbeeld op basis van gsm-antennes) of van een externe bron of netwerk (bijvoorbeeld op basis van gps-informatie)”<sup>8</sup>.*

---

<sup>7</sup> Zie Aanbeveling nr. 07/2011 van 21 december 2011 betreffende de registratie van telefonische oproepen van en naar politiecommissariaten en ziekenhuizen.

<sup>8</sup> Advies nr. 18/2007 van 27 april 2007 betreffende het wetsvoorstel tot wijziging van de wet betreffende de elektronische communicatie teneinde de persoonlijke levenssfeer beter te beschermen in het kader van de op locatiegegevens gebaseerde diensten of locatiediensten via mobiele telefoon.

28. Daaruit volgt dat artikel 123 WEC niet van toepassing is op de traceertoestellen omdat de locatiegegevens niet verwerkt worden door operatoren van communicatiediensten maar door een derde, een verstrekker van diensten op grond van de locatiegegevens die de "zwarte doos" van het voertuig levert<sup>9</sup>. De Groep van het artikel 29 is eveneens van mening dat de Richtlijn 2002/58 EG (ook de "*Richtlijn e-privacy*" genoemd, waarvan artikel 9 naar Belgisch recht werd omgezet door artikel 123 van de WEC) op een dergelijke verwerking van locatiegegevens niet van toepassing is zelfs als deze verwerking gebeurt via een openbaar netwerk voor elektronische communicaties<sup>10</sup>.

#### **D. Verwerking van persoonsgegevens en toepassing van de WVP**

29. De locatiegegevens van voertuigen, materieel of toestellen die verbonden zijn met de bestuurder en de passagiers van een voertuig, zijn persoonsgegevens zoals bedoeld in de WVP aangezien die informatie betrekking kan hebben op een geïdentificeerde of identificeerbare persoon, bedoeld onder artikel 1, §1 van de WVP. Ook de locatiegegevens van een sectie genereert persoonsgegevens als een traceertoestel door een van zijn leden wordt gedragen en het mogelijk wordt de verplaatsingen van een lid van de politiediensten te identificeren.

30. De bepalingen van de WVP zijn van toepassing op de verwerking van gegenereerde gegevens door traceertoestellen zodra die gegevens persoonsgegevens zijn als bedoeld in artikel 1, §1 van de WVP en het een volledig geautomatiseerde verwerking betreft<sup>11</sup>.

31. Deze aanbeveling onderzoekt in hoeverre de traceersystemen die de politiediensten gebruiken, in overeenstemming zijn met de WVP. Voor wat de verwerking van persoonsgegevens betreft is deze wet de toepasselijke referentietekst ter zake.

### **IV. NA TE LEVEN BEGINSELS UITGAANDE VAN DE WVP**

#### **1. Doeleinden**

32. Krachtens artikel 4, §1 van de WVP moet iedere persoonsgegevensverwerking zoals een traceersysteem, beantwoorden aan welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden die de installatie en het gebruik ervan rechtvaardigen.

---

<sup>9</sup> Namelijk via een draadloze verzending naar de server van de leverancier van het fleetloggingsysteem, hetzij via een fysieke doorgifte naar het informaticasysteem van de politiepost die de gegevens centraliseert.

<sup>10</sup> Opinion 13/2011 adopted on 16 May 2011 on Geolocation services on smart mobile devices, WO 185, §4.2.1

<sup>11</sup> Artikel 3 van de WVP.



33. De Commissie noteert meerdere door de politiediensten nagestreefde doeleinden voor het gebruik van traceergegevens die in aanmerking kunnen komen en als rechtmatig kunnen worden beschouwd:

- **veiligheid van de voertuigen en leden van de politiediensten:** de traceersystemen maken het bijvoorbeeld mogelijk de leden van de politiediensten te lokaliseren mochten ze problemen of moeilijkheden hebben (en wanneer er met de centrale niet gecommuniceerd kan worden); bepaalde toestellen verhinderen dat niet bevoegde personen de wapens die in de wagen vastzitten of het voertuig zelf zouden kunnen gebruiken;
- **beheer van het wagenpark:** bepaalde traceertoestellen kunnen de staat van het wagenpark opvolgen en melden of er onderhoud of vervanging van doen is. Op individueel niveau kan de bestuurder nuttige informatie ontvangen, zoals een geluidssignaal bij zwakke batterijen, defecte onderdelen of abnormaal motorgebruik;
- **operationeel beheer in het kader van politieopdrachten:** de lokalisering in reële tijd leidt tot een grotere doeltreffendheid van de interventies en ingezette eenheden maar dient ook om een team in moeilijkheden te lokaliseren. Dit doeleinde doorkruist in meerdere opzichten het doeleinde dat betrekking heeft op de veiligheid van de leden van de politiediensten en voertuigen;
- tot slot is het ook mogelijk om met bepaalde traceertoestellen de gebruikers (personeelsleden van de politie) te **controleren**. Met behulp van die toestellen kunnen de leden van de politiediensten gecontroleerd worden op het gebruik dat ze gemaakt hebben van het voertuigen (bruusk remmen, uren en duur van het gebruik, rijnsnelheid, opzettelijk gebruik van zwaailichten,...) maar ook over hun verplaatsingen, dankzij de geolocatie;
- daarnaast kunnen de beschikbare gegevens gebruikt worden – à charge of à decharge – bij een **klacht over het gedrag van een lid van de politiediensten** ten opzichte van een individu (bijvoorbeeld bij een ongeval, of laattijdige aankomst ter plaatse,...). Het gebruik van die gegevens in het kader van een tucht- of gerechtelijke procedure is dus een ander mogelijk doeleinde.

34. Gelet op de specificiteit van de opdrachten van de politie, stelt de Commissie vast dat deze doeleinden moeten worden beschouwd als rechtmatig gelet op de voorschriften inzake

veiligheid, doeltreffendheid en organisatie die de politiediensten moeten naleven. Toch kunnen deze doeleinden - hetzij in hun geheel, hetzij afzonderlijk - in andere sectoren - hetzij openbare of private - niet automatisch erkend worden als rechtmatig, zonder dat de gevallen waarin er een gegevensverwerking wordt verricht, aan een concreet onderzoek worden onderwerpen.

35. De Commissie herinnert er ook aan dat de verzamelde gegevens niet mogen worden aangewend voor andere doeleinden dan deze die heel precies en voorafgaandelijke aan de geplande verwerking werden bepaald. Daarbij moet rekening worden gehouden met alle relevante factoren, met name de redelijke verwachtingen van de betrokkene en de toepasselijke wettelijke en reglementaire bepalingen<sup>12</sup>. Het blijft natuurlijk de verantwoordelijke voor de verwerking die zal beoordelen of het gebruik van de gegevens (met name voor tucht- of strafrechtelijke vervolging) verenigbaar is met de oorspronkelijke gegevensinzameling waarbij hij zal uitgaan van de relevante factoren en met name de verstrekte informatie aan de betrokken personen.
36. Bovendien wil de Commissie eraan herinneren dat de bekendmaking van de doeleinden waarvoor de gegevens worden gebruikt, toelaat om de bewaartermijn van deze gegevens te bepalen overeenkomstig de principes uiteengezet in deze aanbeveling onder punten 64 en volgende.

## **2. Toelaatbaarheid van de verwerking**

37. Een verwerking van persoonsgegevens kan slechts worden verricht in een beperkt aantal gevallen, opgesomd in artikel 5 van de WVP.
38. Volgens de Commissie is het in het kader van een arbeidsrelatie niet zonder gevaar als de toestemming van de werknemer de basis vormt voor een wettelijke grond van een verwerking op basis van artikel 5 a) van de WVP. In deze specifieke context berust de toestemming niet op een evenwichtige machtsverhouding terwijl de vereiste toestemming vrij moet zijn en op informatie moet berusten<sup>13</sup>.

---

<sup>12</sup> Artikel 4, 2° van de WVP.

<sup>13</sup> Aanbeveling uit eigen beweging nr. 08/2012 van 2 mei 2012 betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer, punt 53.

39. De Commissie is evenwel van oordeel dat de wettelijke basis in dit specifieke geval haar grond vindt in andere toelaatbare gevallen vermeld onder *littera c), e)* of *f)* van artikel 5<sup>14</sup>.
40. **Aangaande de doeleinden betreffende de veiligheid van de voertuigen en de leden van de politiediensten, het wagenparkbeheer en het operationeel beheer**, acht de Commissie de gegevensverwerking toelaatbaar krachtens *littera c)* en *e)* van artikel 5 van de WVP. De verwerking van gegenereerde gegevens door traceertoestellen stellen de politiediensten in staat om hun wettelijke opdrachten te vervullen en hun opdrachten van openbaar belang te verzekeren die hen door de wet zijn toevertrouwd<sup>15</sup>. Met de gegevens die de traceertoestellen verwerken, kunnen de politiediensten onder optimale omstandigheden hun opdrachten doeltreffend vervullen, de burgers hebben immers het recht hebben om dit van dergelijke diensten te verwachten.
41. **Aangaande de doeleinden van controle en beheer van klachten over het gedrag van een lid van de politiediensten**, is de Commissie van mening dat de verwerking van gegevens toegelaten is krachtens *littera f)* van artikel 5 van de WVP. Het doeleinde van controle op de personeelsleden verhindert dat er misbruik gemaakt wordt van zwaailichten, ongepast gebruik van de sirene, ...) maar het kan ook een bewijsmiddel zijn in geval er een betwisting is rond het gedrag van een personeelslid.
42. De Commissie stelt daarnaast vast dat het wettelijk belang dat de politiediensten nastreven met deze verwerkingen, gedeeltelijk samenvalt met het belang van de maatschappij, dat een bepaalde logistieke efficiëntie wenst, een doeltreffend beheer van de openbare middelen en een gepaste uitoefening van de opdracht van openbaar belang waarmee de politiediensten belast zijn. Om die redenen en gelet op het belangenevenwicht dat krachtens artikel 5, f) van de WVP werd verwezenlijkt, laat toe te besluiten dat de verwerking voor de doeleinden van controle en klachtenbeheer aanvaardbaar zijn.
43. Gelet op wat voorafgaat, beschouwt de Commissie de hierboven beschreven verwerkingen aanvaardbaar krachtens artikel 5 *f)* voor het doeleinde controle en klachtenbeheer en krachtens artikel 5 *c)* en *e)* voor de andere doeleinden.

---

<sup>14</sup> Opinion 13/2011 van de Groep van het artikel 29, en de Aanbeveling uit eigen beweging van de Commissie nr. 07/2011 van 21 december 2011 betreffende de registratie van telefonische oproepen van en naar politiecommissariaten en ziekenhuizen, punten 22 en volgende.

<sup>15</sup> De politieautoriteiten moeten inderdaad de uitvoering garanderen van diverse opdrachten die hen door de wet werden toegekend. Zie hiervoor de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus en meer specifiek de artikelen 44, 97, 98, 99, 120, 124, het koninklijk besluit van 10 mei 2006 houdende vaststelling van de deontologische code van de politiediensten, de wet van 13 mei 1999 houdende het tuchtstatuut van de personeelsleden van de politiediensten, koninklijk besluit van 26 november 2001 tot uitvoering van de wet van 13 mei 1999 houdende het tuchtstatuut van de personeelsleden van de politiediensten.

### 3. Proportionaliteit

44. Krachtens artikel 4, 3° van de WVP moeten de verwerkte gegevens toereikend, ter zake dienend en niet overmatig zijn. Dit betekent dat de gegevens van deze verwerking moeten worden beperkt tot wat strikt noodzakelijk is om de vastgestelde doeleinden te verwezenlijken.
45. Bovendien mag de verwerking van de ingewonnen gegevens (geolocatie, snelheid, remmingen, zwaailichten, impactdetectie, etc.) uitgaande van de gerechtvaardigde, nagestreefde doeleinden die de verantwoordelijke voor de verwerking nastreeft en die hierboven worden beschreven, de privacy van de leden van de politiediensten niet disproportioneel aantasten.
46. Aangaande het **doeleinde van controle** van de activiteiten van de leden van de politiediensten, verduidelijkt de Commissie dat deze controle uitsluitend onder goed omkaderde omstandigheden mag gebeuren. De systematische en/of individuele controles mogen niet de grondnorm zijn en moeten een uitzondering blijven.
47. Een **permanente controle** van de gegevens van een personeelslid van de politie mag inderdaad slechts plaatsvinden in de door de verantwoordelijke voor de verwerking van gerechtvaardigde gevallen. De analyse van de gegevens over het gedrag of de activiteiten van een personeelslid is slechts wettelijk als er ernstige aanwijzingen bestaan die een laakbaar, ongepast of verboden gedrag doen vermoeden, of als er bijzondere omstandigheden zijn die rechtvaardigen dat de verzamelde gegevens worden geraadpleegd. Er wordt bijvoorbeeld gedacht aan een ongeval met een voertuig waarbij er twijfels ontstaan over de echtheid van het verhaal van de betrokken personen of nog, bij het abnormaal gebruik van een voertuig, convergerende klachten of aanwijzingen over misbruik tijdens politionele interventies, of het misbruik van politiematerieel (zwaailichten, sirenes, rijnsnelheid,...).
48. Voor **de andere doeleinden die niet de controle betreffen**, wordt de opvolging in reële tijd van de voertuigen en hun inzittenden op basis van geolocatiegegevens in een streven naar meer doeltreffende interventies, eveneens als proportioneel beschouwd. Hetzelfde geldt voor de analyse van geglobaliseerde en niet-geïndividualiseerde gegevens waarmee de verantwoordelijke voor de verwerking een zicht krijgt op de staat van de voertuigen, de slijtage van de voertuigen of het aantal afgelegde kilometers met het voertuig.

49. De bewaring en de automatische analyse van gegevens voor systematische en niet doelgerichte controle van de personeelsleden van de politiediensten wordt daarentegen als disproportioneel beschouwd.
50. De traceerfuncties moeten kunnen gedeactiveerd worden in het geval een personeelslid buiten de diensturen gebruik maakt van een dienstvoertuig, bijvoorbeeld wanneer hij het voertuig naar huis meeneemt omdat hij de dag erna ergens een werkvergadering heeft. Een permanente tracement van dit voertuig buiten de diensturen kan als disproportioneel aanzien worden omdat er in dit precieze geval andere, meer geschikte middelen kunnen worden aangewend om het voertuig te lokaliseren, bijvoorbeeld door de hiërarchie of de dispatching te laten weten dat het voertuig buiten de diensturen zal gebruikt worden voor dienstonodigheden.
51. De Commissie sluit niet uit dat er nog andere gevallen bestaan waarbij een geïndividualiseerde analyse van de gegevens gerechtvaardigd is maar deze moeten geval per geval worden beoordeeld<sup>16</sup>.
52. Indien de verzamelde gegevens zouden worden gebruikt om de activiteiten van een personeelslid van de politie te controleren voor disciplinaire doeleinden, moet de hiërarchische overste bij de aangifte van een incident waarbij een personeelslid betrokken is, dit personeelslid oproepen zodat hij hierover uitleg kan verschaffen. Een interpretatie van brute gegevens en het onmiddellijk opleggen van een sanctie zonder dat de betrokkene de mogelijkheid kreeg om zijn interpretatie van de hem betreffende traceergegevens te geven, zijn handelingen die niet alleen het principe van de tegensprekbaarheid aantasten maar ook artikel 12bis van de WVP.

#### **4. Transparantie**

53. Overeenkomstig artikel 9, §1 van de WVP, herinnert de Commissie eraan dat vooraleer met de verwerking wordt gestart, de leden van de politiediensten van de belangrijkste elementen van die verwerking van hun persoonsgegevens moeten worden ingelicht <sup>17</sup>.
54. Zo beveelt de Commissie aan om ten minste de volgende gegevens te verstrekken aan de betrokken personeelsleden van de politie:

---

<sup>16</sup> We denken onder meer aan een controle van de interventies van patrouilles, om zich te verzekeren van hun aanwezigheid ter plaatse, of om zich ervan te verzekeren dat de richtlijnen die de leden van de politiediensten hebben gekregen werden nageleefd en als die niet werden nageleefd kan vooraf worden bekendgemaakt dat hun activiteiten zullen gecontroleerd worden.

<sup>17</sup> Aanbeveling uit eigen beweging van de Commissie nr. 07/2011 van 21 december 2011 betreffende de registratie van telefonische oproepen van en naar politiecommissariaten en ziekenhuizen, punten 30 en volgende.

- identiteit van de verantwoordelijke voor de verwerking (bijvoorbeeld het hoofd van de betrokken zone);
- doeleinden van de verwerking;
- soort verwerkte gegevens;
- bewaarduur van de gegevens;
- bestemmingen van die gegevens;
- het bestaan van een recht op toegang, verbetering en schrapping en de manier waarop dit recht wordt uitgeoefend;
- identiteit of de functie van de personen die toegang (kunnen) hebben tot die gegevens;
- de raadplegingsmodaliteiten (wie, op welke frequente, in welke gevallen);
- de modaliteiten van de voorgenomen verwerking (bijvoorbeeld: informatie over de periodiciteit en het bestaan van een doelgerichte dan wel systematische registratie, informatie over een eventuele desactivering van het systeem als het lid van de politiediensten naar huis gaat en de te volgen procedure.

55. Deze informatie kan worden verstrekt via elke nuttige drager (dienstorders, interne omzendbrieven, e-mail, prikbord, intranet, etc.) die het hoofd van de betrokken politiedienst geschikt acht zodat hij zich er kan van verzekeren dat alle betrokken personen bij de verwerking daar kennis hebben kunnen van nemen.

56. De Commissie raadt aan om voor dit soort gegevensverwerking een voorafgaand overleg te houden met de vakbonden van de betrokken beroepsgroep zodat ook zij goed ingelicht zijn van de verwerking en de nagestreefde doeleinden.

57. De syndicale regelgeving in politiezaken verenigt overigens de syndicale organisaties om in een voorafgaand overleg de maatregelen goed te keuren die betrekking hebben op de organisatie van het werk<sup>18</sup>.

## **5. Recht op toegang, verbetering en schrapping**

58. Krachtens artikel 10 van de WVP, beschikken de betrokken personen over een recht op toegang tot hun gegevens waarbij de verantwoordelijke voor de verwerking verplicht is om de gegevens - die het voorwerp uitmaken van een verwerking - op een begrijpelijke manier mee te delen.

---

<sup>18</sup> Wet van 24 maart 1999 Wet tot regeling van de betrekkingen tussen de overheid en de vakverenigingen van het personeel van de politiediensten (artikel 6 tot 8); Koninklijk besluit van 8 februari 2001 tot aanwijzing van de grondregelingen in de zin van artikel 3, eerste lid, 1°, van de wet van 24 maart 1999 tot regeling van de betrekkingen tussen de overheid en de vakverenigingen van het personeel van de politiediensten.

59. Artikel 12 van de WVP erkent eveneens een recht op verzet in bepaalde precieze gevallen<sup>19</sup>, een recht op verbetering van de onjuiste, onvolledige of irrelevante gegevens en een recht op schrapping als die gegevens langer worden bewaard dan de tijd die nodig is om het doeleinde waarvoor ze werden verwerkt, te verwezenlijken.
60. De Commissie bevestigt dat dit recht op toegang voor de leden van de politiediensten van wie de gegevens worden verwerkt daadwerkelijk mogelijk moet zijn. Zij moeten erover ingelicht worden tot wie zij hun verzoek om toegang moeten richten om kennis te kunnen nemen van de hen betreffende, verwerkte gegevens.
61. Als bovendien blijkt dat de verwerkte gegevens onjuist zijn, kunnen de leden van de politiediensten, nadat ze hebben aangetoond dat het gegeven gecorrigeerd moet worden, hun recht op verbetering doen gelden.
62. De leden van de politiediensten mogen vragen hun gegevens te laten schrappen als de bewaring ervan niet langer gerechtvaardigd is omdat de behoefte waarvoor die gegevens oorspronkelijk werden verwerkt, niet langer bestaat (zie punt 6 hieronder dat handelt over de bewaartermijn).

## **6. Bewaartermijn**

63. De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt<sup>20</sup>.
64. Daaruit vloeit voort dat de bewaartermijn van de gegevens beperkt moet worden in de tijd en proportioneel moet zijn ten aanzien van het gebruik dat gemaakt wordt van de gegevens. Het is dus de verantwoordelijke voor de verwerking die voor ieder doeleinde een passende bewaartermijn moet bepalen.
65. Als deze principes worden toegepast, zou de bewaring van het gegeven dat bewijst dat een of ander lid van de politiediensten ter plaatse was, van kortere duur moeten zijn dan het gegeven waarmee er statistieken kunnen worden opgemaakt over het gebruik van een voertuig tijdens de levensduur ervan.

---

<sup>19</sup> De betrokken persoon moet aantonen dat hij ernstige en gerechtvaardigde redenen heeft die verband houden met een bijzonder situatie om zich tegen de verwerking van zijn gegevens te verzetten.

<sup>20</sup> Artikel 5, 5) van de WVP.

66. Ook de gegevens die kunnen aangewend worden om een lid van de politiediensten een tucht- of strafrechtelijke straf op te leggen mogen niet langer worden bewaard dan de verjaringstermijn van de straf- of tuchtperiode, tenzij er andere doeleinden zouden bestaan die een langere bewaartermijn rechtvaardigen.
67. Gelet op de talrijke doeleinden die traceersystemen nastreven en de veelheid aan bewaartermijnen die daaruit kunnen voortvloeien, is de Commissie van oordeel dat een unieke bewaarperiode van zes maanden als proportioneel kan worden beschouwd. Uit de informatie van de Commissie blijkt overigens dat de politiediensten deze termijn hebben weerhouden en overigens overeenstemt met de verjaartermijn bij disciplinaire aangelegenheden. De Commissie sluit evenwel niet uit dat onder bepaalde omstandigheden, een langere bewaartermijn gerechtvaardigd kan zijn. De politiediensten zullen echter elementen moeten inroepen die een bewaartermijn van langer dan zes maanden kunnen rechtvaardigen.
68. De geanonimiseerde gegevens daarentegen, namelijk die gegevens die niet langer aan een persoon kunnen worden verbonden, mogen langer worden bewaard omdat zij niet langer persoonsgegevens zijn en dus niet meer onderworpen aan de WVP.

## **7. Beveiliging van de gegevens**

69. Krachtens artikel 16 van de WVP, heeft de verantwoordelijke voor de verwerking de plicht om alle noodzakelijke, technische en organisatorische maatregelen te nemen zodat de gegevens beveiligd zijn tegen niet-gemachtigde of incidentele vernietiging, verlies, wijzigingen en toegang en iedere andere niet gemachtigde verwerking van de persoonsgegevens. De geschiktheid van die maatregelen hangt enerzijds af van de stand van de techniek en de daaraan verbonden kosten en anderzijds van de aard van de te beveiligen gegevens en de potentiële risico's. De verantwoordelijke voor de verwerking moet rekening houden met de "referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens", terug te vinden op haar website<sup>21</sup> en de "Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens" die gepubliceerd werden op de website van Privacycommissie. De Commissie verwijst eveneens naar haar Aanbeveling nr. 01/2013

---

21

[http://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen\\_voor\\_de\\_beveiliging\\_van\\_elke\\_verwerking\\_van\\_persoonsgegevens.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens.pdf)



uit eigen beweging betreffende de na te leven veiligheidsmaatregelen ter voorkoming van gegevenslekken<sup>22</sup>.

70. De verantwoordelijke voor de verwerking moet een limitatief aantal personen aanduiden voor wie de toegang tot de gegevens strikt noodzakelijk is om de verwerking uit te voeren. Alleen de personen met een functioneel belang mogen dus toegang hebben tot de gegevens en ze verwerken. Dit betekent ook dat de logistieke, technische maar ook organisatorische middelen moeten worden ingezet om te verhinderen dat deze gegevens toegankelijk zijn voor andere dan de aangeduide personen<sup>23</sup>.
71. De verantwoordelijke voor de verwerking moet eveneens alles in het werk stellen om de gegevens te updaten, om de onjuiste, onvolledige of irrelevante gegevens of de gegevens die niet overeenkomstig de artikelen 4 tot 8 van de WVP werden verkregen en verwerkt, te verbeteren of te schrappen. Hij moet er ook op toezien dat de toegang tot de gegevens en de verwerkingsmogelijkheden voor personen die onder zijn gezag werken, beperkt worden tot wat noodzakelijk is voor de noodwendigheden van de dienst<sup>24</sup>. Dit veronderstelt dus dat de toegang tot deze gegevens beveiligd is en uitsluitend voorbehouden aan de personen die gemachtigd zijn ze te raadplegen.
72. En tot slot moet de verantwoordelijke voor de verwerking erop toezien dat de programma's die de geautomatiseerde verwerkingen van de persoonsgegevens uitvoeren, in overeenstemming zijn met de aangifte die bij de Commissie werd ingediend<sup>25</sup>.
73. de Commissie verzoekt dat de verantwoordelijke voor de verwerking in iedere lokale politiezone een contactpersoon aanduidt tot wie de Commissie zich kan wenden in verband met de verwerking van de gegevens die de traceertoestellen inzamelen<sup>26</sup>.
74. Indien de verantwoordelijke voor de verwerking<sup>27</sup> een gegevensverwerker kiest, moet die laatste voldoende garanties kunnen bieden aangaande de getroffen technische en organisatorische beveiligingsmaatregelen voor de verwerkingen<sup>28</sup>. Deze verplichting is zeer belangrijk omdat is vastgesteld dat het dikwijls privéondernemingen zijn die gegevens

---

<sup>22</sup> Aanbeveling uit eigen beweging van 21 januari 2013.

<sup>23</sup> Bijvoorbeeld korpsoversten, directeurs, tuchtoverheden, toezichthoudende overheden van de politiediensten en de gerechtelijke autoriteiten.

<sup>24</sup> Artikel 16, §2 van de WVP.

<sup>25</sup> Artikel 16, §2 van de WVP.

<sup>26</sup> Overeenkomstig artikel 44/2 van de wet van 5 augustus 1992 betreffende het politieambt.

<sup>27</sup> In onderhavig geval de Federale politie, of , voor wat de lokale politie aangaat, de politiezone.

<sup>28</sup> Artikel 16, §1 van de WVP.

verwerken, waarop een bijzondere bescherming rust omdat ze betrekking hebben op politieactiviteiten. De keuze van een externe dienstenverstreker is dus primordiaal om er zeker van te kunnen zijn dat de gegevens niet toegankelijk zullen zijn voor derden, en beveiligd tegen iedere niet gemachtigde toegang.

75. De Commissie herinnert er overigens aan dat de betrekkingen tussen de verantwoordelijke voor de verwerking en het bedrijf dat traceersystemen aanbiedt in een schriftelijk contract moeten worden afgesloten. Daarnaast moet dit contract de aansprakelijkheid van de gegevensverwerker bepalen ten aanzien van de verantwoordelijke voor de verwerking, en vermelden dat de gegevensverwerker uitsluitend kan handelen in opdracht van de verantwoordelijke voor de verwerking en dat hij, in toepassing van artikel 16, §3 van de WVP<sup>29</sup> dezelfde verplichtingen moet naleven als de verantwoordelijke voor de verwerking.
76. Deze beveiligingsinstructies verplichten dus de betrokken politiedienst om alle gepaste maatregelen te nemen die garanderen dat de gegevens die de gegevensverwerker voor zijn rekening verwerkt, beveiligd zijn. De verantwoordelijke voor de verwerking blijft immers altijd aansprakelijk.

## **8. Aangifte van de verwerking**

77. De Commissie vestigt ten slotte de aandacht erop dat van iedere gegevensverwerking aangifte moet worden gedaan overeenkomstig artikel 17 van de WVP. Iedere politiedienst die traceergegevens verwerkt, moet dus daarvan aangifte doen aangezien deze verwerkingen niet worden vrijgesteld van de aangifteplicht. Deze verwerking staat inderdaad niet vermeld onder de gevallen, opgesomd in Afdeling II, Hoofdstuk VII van het Koninklijk besluit van 13 februari 2001 tot uitvoering van de WVP.

## **BESLUIT**

De Commissie dringt erop aan dat wanneer een politiekorps een traceersysteem invoert, alle hierboven uiteengezette principes evenals de voorschriften van de WVP volledig naleeft en dat bij deze verwerkingen bijzonder rekening wordt gehouden met de beginsels inzake proportionaliteit, transparantie, de informatieverstrekking aan het personeel van de politiediensten, de bewaartermijn van de ingewonnen gegevens en met de beveiliging van de verwerking.

---

<sup>29</sup> Dit artikel bepaalt dat "Eenieder die handelt onder het gezag van de verantwoordelijke voor de verwerking of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verantwoordelijke voor de verwerking verwerken, behoudens op grond van een verplichting door of krachtens een wet, een decreet of een ordonnantie".

Zij beveelt bijgevolg aan:

1. dat gegevens verzameld door traceersystemen worden beperkt tot de gegevens die toereikend, ter zake dienend en niet overmatig zijn voor het bereiken van het (de) aangekondigde doeleinde(n);
2. dat iedere verantwoordelijke voor de verwerking duidelijk de doeleinden bepaalt waarvoor hij een traceertoestel installeert;
3. dat de gegevens verzameld door de traceersystemen niet worden aangewend voor permanente controles op de personeelsleden en dat een arbeidsreglement of een gelijkwaardig instrument, het gebruik van gegevens voor controledoeleinden voldoende omkadert;
4. dat de personeelsleden van de politie met alle mogelijke middelen klaar en duidelijk geïnformeerd worden over de gegevens die over hen worden ingewonnen, alsmede over de doeleinden die deze gegevensverwerking nastreeft, de wijze van toegang en controle, de bewaartermijn evenals alle andere informatie beschreven onder punt 55 van deze aanbeveling;
5. dat de verwerking van de gegevens die het traceersysteem verzamelde wordt aangegeven bij de Commissie met vermelding van de nagestreefde doeleinden;
6. dat de bewaartermijn van de persoonsgegevens die werden verzameld door traceertoestellen maximum zes maanden bedraagt tenzij uitzonderlijke omstandigheden een langere bewaartermijn rechtvaardigen;
7. dat de politiediensten die dergelijke traceertoestellen invoeren, toereikende beveiligingsmaatregelen nemen en dat een schriftelijk contract de eventuele betrekkingen regelt met de externe leverancier als bedoeld in de punten 70 en volgende van deze aanbeveling en dat deze maatregelen met name betrekking hebben op de toegangsmodaliteiten tot de gegevens en de loggings van de toegangen.

De Wnd. Administrateur,

De Voorzitter,

(get.) Patrick Van Wouwe

(get.) Willem Debeuckelaere