COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

College Bescherming Persoonsgegevens

ONDERZOEK CIOT-BEVRAGINGEN

Onderzoek Regionaal Politiekorps Haaglanden
z2010-00169

Rapport definitieve bevindingen
april 2011

DATUM 21 april 2011

INHOUDSOPGAVE

SAMENVATTING EN CONCLUSIES

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is ingesteld bij Besluit verstrekking gegevens telecommunicatie (hierna: het Besluit) van 26 januari 2000. Het CIOT-Informatiesysteem (CIS) stroomlijnt op geautomatiseerde wijze het vragen van informatie (door opsporings- en veiligheidsdiensten) en de beantwoording daarvan (door aanbieders van openbare telecommunicatiediensten en –netwerken) door tussenkomst van het CIOT. Het aantal bevragingen van het CIOT is de afgelopen jaren substantieel toegenomen. Zo is het totale aantal bevragingen toegenomen van 1,7 miljoen in 2007 tot 2,8 miljoen in 2008 en tot ruim 2,9 miljoen in 2009. Een dergelijk massaal gebruik van de bevoegdheid om persoonsgegevens op te vragen in het kader van een (opsporings)onderzoek vraagt dat de wettelijke waarborgen zorgvuldig worden nageleefd. In dit onderzoek is ten aanzien van een aantal waarborgen nagegaan of deze worden nageleefd.

Het College bescherming persoonsgegevens (CBP) heeft in 2010 in het kader van zijn toezichthoudende taak een onderzoek verricht op grond van de Wet bescherming persoonsgegevens (Wbp) en de Wet politiegegevens (Wpg) naar de naleving van de voorschriften in het kader van de CIOT-bevragingen bij het CIOT, het regionaal politiekorps Haaglanden en de Dienst Nationale Recherche (DNR). Onderzocht is:

1. Worden de bevragingen op het CIS alleen door daartoe bevoegden (geautoriseerde ambtenaren) uitgevoerd?
2. Wordt bij no-hit-bevragingen en andere vorderingen die rechtstreeks aan de telecommunicatieaanbieders worden verzonden, gebruik gemaakt van voldoende beveiliging?
3. Worden de CIOT-bevragingen rechtmatig uitgevoerd?

Bij het korps Haaglanden zijn alle drie de vragen onderzocht.

In het kader van de eerste onderzoeksvraag heeft het CBP onderzocht of de toekenning en registratie van een CIS-autorisatie zodanig is ingevuld dat dit voldoende waarborgen biedt dat ongeoorloofde toegang tot het CIS wordt voorkomen en of er controle plaatsvindt op de toegekende autorisaties.
Op grond van de bevindingen van het onderzoek komt het CBP daarbij tot de volgende conclusies.

Ten aanzien van toekenning van autorisaties:

- Uit het onderzoek is gebleken dat een vastgelegde formele procedure voor het toekennen van autorisaties door de korpsbeheerder aan medewerkers van het korps Haaglanden voor de verwerking van politiegegevens, inclusief de bevraging van het CIS, niet aanwezig is. Hiermee wordt niet voldaan aan de vereisten die de NEN-norm op dit punt stelt en wordt in strijd gehandeld met artikel 6 lid 1 j° artikel 4 lid 3 Wpg.
- Het CBP stelt vast dat de autorisaties van de bevoegde autoriteiten, i.c. de medewerkers van het korps Haaglanden, niet rechtsgeldig overeenkomstig artikel 5 lid 1 Besluit zijn afgegeven. De invoer van een verzoek door de bevoegde autoriteit, i.c. een daartoe aangewezen opsporingsambtenaar van korps Haaglanden, om verstrekking van informatie is daarmee in strijd met artikel 5 lid 1 Besluit.

Ten aanzien van de controle op toegekende autorisaties:

- Tijdens het onderzoek door het CBP is door het korps Haaglanden een autorisatieoverzicht overgelegd. Daarmee is voldaan aan de verplichting een schriftelijke vastlegging van de toekenning van de autorisaties bij te houden. Hiermee is op dit punt in overeenstemming gehandeld met artikel 32 lid 1 onder c Wpg.
- Het CBP constateert dat het aantal op het autorisatieoverzicht vermelde geautoriseerde medewerkers bij BRI, zijnde 25, niet in overeenstemming is met het aantal medewerkers dat uit hoofde van hun taak belast is met het uitvoeren van CIOT-bevragingen, te weten zes. Het CBP is van oordeel dat de autorisatie van de overige 19 medewerkers bij BRI, gelet op het doel waarvoor zij beschikken over die autorisatie, niet in overeenstemming is met het vereiste dat alleen ambtenaren van politie worden geautoriseerd voor de verwerking van politiegegevens ter uitvoering van de politietaak waarmee zij zijn belast. Het CBP concludeert in dit kader dat de autorisatie van de 19 extra medewerkers bij BRI in strijd is met artikel 6 lid 3 Wpg.
- Wegens het ontbreken van een vastgelegde formele procedure voor de intrekking van autorisaties tot het CIS wordt niet voldaan aan de vereisten die de NEN-norm daaraan stelt. Hiermee wordt in strijd gehandeld met artikel 4 lid 3 j° artikel 6 lid 1 Wpg.

Voorts heeft het CBP onderzocht of bij no-hit-bevragingen en andere vorderingen die rechtstreeks aan de telecommunicatieaanbieders worden verzonden, gebruik gemaakt wordt van voldoende beveiliging, en of en zo ja, welke beveiligingsmaatregelen bij rechtstreekse gegevensuitwisseling zijn toegepast.
Op grond van de bevindingen van het onderzoek komt het CBP daarbij tot de volgende conclusie.

- De verzending van zogeheten 'no-hit'-faxen en van overige vorderingen in het kader van strafvordering die rechtstreeks tot de telecommunicatieaanbieders zijn gericht, vindt plaats via openbare telefoonlijnen zonder additionele beveiligingsmaatregelen. Nu de NEN-norm voorschrijft dat bij verzending van gevoelige gegevens ter bescherming van gevoelige informatie die wordt verzonden over communicatielijnen en openbare netwerken bijzondere beheersmaatregelen dienen te worden getroffen om de vertrouwelijkheid en integriteit daarvan te waarborgen en hierin niet is voorzien, is niet voldaan aan de eisen van de NEN-norm op dit punt. Er is dan ook geen sprake van een passend beveiligingsniveau. Dit is in strijd met artikel 4 lid 3 Wpg.

Het CBP heeft tien CIOT-bevragingen geselecteerd en onderzocht op de vraag of deze bevragingen op onderdelen rechtmatig zijn uitgevoerd, waarbij één bevraging uit twee onderdelen bleek te bestaan, zodat elf bevragingen zijn beoordeeld. De geselecteerde bevragingen zijn onderzocht op de aanwezigheid van de grondslag uit het Wetboek van Strafvordering waarop de bevraging is gebaseerd en het verband tussen bevraging en het gebruikte referentienummer waaronder de bevraging is uitgevoerd, ter controle of de bevraagde gegevens hun grondslag vinden in het achterliggende onderzoeksdossier.

Op grond van de bevindingen van het onderzoek komt het CBP daarbij tot de volgende conclusie.

- Van de elf onderzochte bevragingen zijn er zes bevragingen voor zover onderzocht in overeenstemming met artikel 3 lid 2 Wpg.
- Vijf bevragingen zijn in strijd met artikel 3 lid 2 Wpg omdat daarbij telkens een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbrak, terwijl bij één daarvan tevens de vordering door de officier van justitie ontbrak. Dit leidt tot de conclusie dat het korps Haaglanden zich voor vijf onderzochte CIOT-bevragingen niet kan verantwoorden. Hiermee wordt in strijd gehandeld met artikel 3 lid 2 Wpg.

1 INLEIDING

1.1 Achtergrond onderzoek

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is ingesteld bij Besluit verstrekking gegevens telecommunicatie (hierna: het Besluit) van 26 januari 2000. Het CIOT valt op grond van artikel 2 van het Besluit onder de verantwoordelijkheid van de minister van Justitie. Het CIOT-Informatiesysteem (CIS) stroomlijnt op geautomatiseerde wijze het vragen van informatie (door opsporings- en veiligheidsdiensten) en de beantwoording daarvan (door aanbieders van openbare telecommunicatiediensten en –netwerken) door tussenkomst van het CIOT. De informatie die gevraagd wordt betreft bijvoorbeeld de naam-, adres- en woonplaatsgegevens behorend bij een telefoonnummer. In geval dat informatie wordt gevraagd over internetaansluitingen gaat het bijvoorbeeld naast naam-, adres- en woonplaatsgegevens ook om gebruikte e-mailadressen.

Het aantal bevragingen van het CIOT is de afgelopen jaren substantieel toegenomen. Zo is het totale aantal bevragingen toegenomen van 1,7 miljoen in 2007 tot 2,8 miljoen in 2008 en tot ruim 2,9 miljoen in 2009. Een dergelijk massaal gebruik van de bevoegdheid om bovengenoemde persoonsgegevens op te vragen in het kader van een (opsporings)onderzoek vraagt dat de wettelijke waarborgen zorgvuldig worden nageleefd. In dit onderzoek is ten aanzien van een aantal waarborgen nagegaan of deze worden nageleefd.

1.2 Doel, reikwijdte en uitvoering van het onderzoek

In het kader van de toezichthoudende taak heeft het College bescherming persoonsgegevens (CBP) een ambtshalve onderzoek verricht conform artikel 60 Wet bescherming persoonsgegevens (Wbp) en artikel 35 Wet politiegegevens (Wpg) naar de naleving van voorschriften in het kader van CIOT-bevragingen bij het CIOT, het regionaal politiekorps Haaglanden en de Dienst Nationale Recherche (DNR).

Het betreft de volgende onderzoeksvragen:

1. Worden de bevragingen op het CIS alleen door daartoe bevoegden (geautoriseerde ambtenaren) uitgevoerd? Voor de beantwoording van deze vraag is onderzocht of de toekenning en registratie van een CIS-autorisatie zowel bij het CIOT zelf als bij de korpsen zodanig is ingevuld dat dit voldoende waarborgen biedt dat ongeoorloofde toegang tot het CIS wordt voorkomen. Voorts is onderzocht of er controle plaatsvindt op de toegekende autorisaties.
2. Wordt bij no-hit-bevragingen en andere vorderingen die rechtstreeks aan de telecommunicatieaanbieders worden verzonden, gebruik gemaakt van voldoende beveiliging? Voor de beantwoording van deze vraag is onderzocht of en zo ja, welke beveiligingsmaatregelen bij rechtstreekse gegevensuitwisseling zijn toegepast.
3. Worden de CIOT-bevragingen rechtmatig uitgevoerd? Voor de beantwoording van deze vraag heeft het CBP onderzocht of de geselecteerde bevragingen op een van de grondslagen van het Wetboek van Strafvordering[1] hebben plaatsgevonden en is door toetsing aan de hand van de vereiste stukken van het dossier het

[1] Zie voor de uitwerking hiervan het juridisch kader onder 5.2

verband tussen de bevraging en het referentienummer waaronder de bevraging heeft plaatsgevonden gecontroleerd.

Bij het CIOT heeft het CBP, gezien de taak van het CIOT, alleen de eerste vraag onderzocht. Bij DNR en het korps Haaglanden zijn alle drie de vragen onderzocht. Per onderzochte dienst is een rapport opgesteld. Dit rapport betreft de resultaten van het onderzoek bij het korps Haaglanden.

Het CBP heeft het regionaal politiekorps Haaglanden bezocht op 2, 12, 23 en 25 maart 2010. Tijdens het onderzoek ter plaatse zijn voor de eerste twee onderzoeksvragen interviews gehouden en is aanvullend schriftelijk materiaal geanalyseerd. Voor de beantwoording van de derde onderzoeksvraag naar de rechtmatigheid van de bevragingen is een dossieronderzoek uitgevoerd. De interviews en het dossieronderzoek hebben plaatsgevonden op de locatie Leidschendam en op het Hoofdbureau van het korps Haaglanden.
Op grond van het bepaalde in artikel 60 lid 2 Wbp is het rapport van voorlopige bevindingen op 16 december 2010 aan de korpsbeheerder toegezonden en is hij in de gelegenheid gesteld zijn zienswijze kenbaar te maken.
Bij brief van 22 februari 2011 heeft de korpsbeheerder van het regionaal politiekorps Haaglanden zijn schriftelijke reactie gegeven op de voorlopige bevindingen. Dit heeft niet geleid tot wijzigingen in de bevindingen en conclusies van het onderzoek. Naar aanleiding van de reactie van de korpsbeheerder van het KLPD betreffende de tekst van het rapport over het onderzoek bij de DNR heeft het CBP een aanpassing in de tekst aangebracht (onder 3.1.1 ten aanzien van de BBNP). De reactie van de minister van Veiligheid en Justitie inzake het onderzoek bij het CIOT heeft daarnaast geleid tot een aanpassing in de tekst onder 3.1.1 (laatste alinea) en 3.1.2 ten aanzien van mandatering.

1.3 Wettelijk kader

De bevindingen in dit onderzoek zijn getoetst aan artikel 5 lid 1 Besluit verstrekking gegevens telecommunicatie, de artikelen 3 lid 2, 4 lid 3, 6 lid 1 en 3, en 32 Wet politiegegevens en de artikelen 126n, 126na, 126u, 126ua, 126zh, 126zi en 126ii van het Wetboek van Strafvordering ten aanzien van de vraag of de rechtsgrondslag waaronder de bevraging is uitgevoerd is gebaseerd op de desbetreffende artikelen met vorderingsbevoegdheden en de daarbij behorende voorwaarden.

2 ORGANISATIE

Bij het regionaal politiekorps Haaglanden is de bevoegdheid om CIOT-bevragingen uit te voeren ondergebracht bij de Directie Opsporing. De Directie Opsporing bestaat uit twee diensten: Bureau Regionale Informatie (BRI) en Bureau Regionale Recherche (BRR). BRI voert alle CIOT-bevragingen uit die in het kader van onderzoeken bij de lokale bureaus van het korps Haaglanden plaatsvinden. De CIOT-bevragingen bij BRR betreffen bevragingen in het kader van de grotere regionale rechercheonderzoeken.

3 TOEGANG TOT HET CIS DOOR HET KORPS HAAGLANDEN

Het CBP heeft onderzocht of aan de voorwaarden is voldaan om politieambtenaren van het korps Haaglanden toegang te verlenen tot het CIS.

3.1 Toekenning van autorisaties bij het korps Haaglanden

3.1.1 Norm

Inleiding
Het Besluit regelt dat de minister van Justitie is belast met het langs geautomatiseerde weg doorgeleiden door middel van het CIOT van verzoeken om en verstrekkingen van informatie. De webbased applicatie die het CIOT heeft ontwikkeld voor het opvragen van identificerende gegevens van telecomdiensten wordt het CIS genoemd. De minister van Justitie is de verantwoordelijke voor de verwerking van gegevens in het CIS. Voor het gebruik van het CIS dient, aldus de handleiding CIOT InformatieSysteem (CIS 3.1) [2], iedere gebruiker op de hoogte te zijn van de richtlijnen die gelden op het gebied van informatiebeveiliging. Hierbij wordt verwezen naar de geldende wet- en regelgeving, zoals het Besluit. Daarnaast kent het CIS een aantal aanvullende uitgangspunten, onder meer dat iedere ambtenaar die met het CIS werkt een persoonlijk account krijgt en daarmee inlogt op het CIS nadat hij een eigen certificaat toegekend heeft gekregen en dit vervolgens heeft geïnstalleerd.

De procedure CIS-accounts[3] regelt het specifieke proces van account-toekenning door het CIOT, onder verantwoordelijkheid van de minister van Justitie. Op grond van de hierin beschreven procedure kan een gebruiker alleen toegang verkrijgen tot de CIOT webbased applicatie indien hij beschikt over een CIS-account, over een door het CIOT uitgegeven certificaat en een door de lokale beheerder van zijn korps of opsporingsdienst verstrekte autorisatie[4].

Uit bovenstaande volgt dat sprake is van een dubbele autorisatie teneinde de ambtenaar van politie van het korps Haaglanden toegang te verlenen tot het CIS, namelijk zowel door de beheerder van het korps als door de minister van Justitie[5].

A. *Norm autorisatie door de korpsbeheerder*
De ambtenaar van politie is alleen aan te merken als bevoegde autoriteit in de zin van artikel 1, aanhef en onder d, Besluit indien hij door de beheerder van het korps daartoe is aangewezen. De toegang tot het CIS impliceert de verwerking van politiegegevens die voortkomen uit de bevraging. Hiervoor dient de ambtenaar van politie door zijn korpsbeheerder geautoriseerd te zijn. Dit volgt uit artikel 4 lid 3 Wpg waarin aan de verantwoordelijke de verplichting wordt opgelegd om passende technische en organisatorische maatregelen te nemen om politiegegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen

[2] *Handleiding CIOT InformatieSysteem (CIS 3.1),* Ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie, versie 2.2, augustus 2007.
[3] *Procedure CIS-accounts CIOT informatiesysteem versie 3.1*, Ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie, versie 2.0, 11 mei 2007.
[4] Idem, p. 4.
[5] Zoals hierna beschreven onder *B. Norm autorisatie door de minister van Justitie*.

garanderen een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de politiegegevens met zich meebrengen. Toegangsbeveiliging door middel van autorisaties is hiervan een uitwerking, nader bepaald in artikel 6 Wpg: de verantwoordelijke moet een systeem van autorisaties onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Politiegegevens kunnen slechts worden verwerkt door ambtenaren van politie die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt. Dit is een autorisatie op een 'need to know'- basis, dus voor zover zij deze gegevens nodig hebben voor de verwerking van politiegegevens ter uitvoering van de onderdelen van de politietaak waarmee zij zijn belast.

Op grond van artikel 38 lid 3 Politiewet 1993, waarbij de minister van BZK regels kan geven over onder meer de informatiebeveiliging, heeft de minister de Regeling Informatiebeveiliging Politie (RIP) vastgesteld. De RIP is algemeen van karakter. Ingevolge artikel 2 lid 1 RIP is deze regeling van toepassing op het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.
In 2002 is bij de RIP als leidraad het Basisbeveiligingsniveau Nederlandse Politie (BBNP) opgesteld. Dit document is echter sterk verouderd, zodat het niet langer toereikend is als standaard voor informatiebeveiliging bij de politiekorpsen. Nu er in de RIP slechts is voorzien in een algemene regeling voor informatiebeveiliging en hierin niet specifiek iets opgenomen is over autorisaties, sluit het CBP voor de beoordeling of sprake is van passende technische en organisatorische beveiligingsmaatregelen aan bij de nadere invulling die daaraan wordt gegeven in onderdelen van de Code voor Informatiebeveiliging, de NEN-ISO/IEC 27002:2007 norm (hierna de NEN-norm) [6]. De NEN-norm is een gezaghebbende norm voor informatiebeveiliging en wordt algemeen aanvaard en erkend daar waar het beveiliging van informatie betreft. Als een organisatie voldoet aan de NEN-norm, gaat het CBP ervan uit dat ook wordt voldaan aan artikel 4 lid 3 Wpg. Dit sluit niet uit dat het korps eventueel ook op andere wijze kan aantonen dat wordt voldaan aan artikel 4 lid 3 Wpg.

Op grond van de NEN-norm in verband met artikel 4 lid 3 Wpg dient voor de toekenning van autorisaties aan medewerkers van korps Haaglanden ten behoeve van de bevraging van het CIS en de daaruit voortvloeiende verwerking van politiegegevens een formele procedure te zijn vastgesteld[7]. Deze procedure betreft de beheersing van toewijzing van toegangsrechten tot informatiesystemen, waarin alle fasen in de levenscyclus van gebruikerstoegang worden vastgelegd.

B. Norm autorisatie door de minister van Justitie

De gegevensverwerkingen binnen het CIOT vallen onder de werking van de Wbp, onder verantwoordelijkheid van de minister van Justitie. Op grond van artikel 13 Wbp dienen door de verantwoordelijke passende technische en organisatorische maatregelen getroffen te worden om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen.

[6] NEN-ISO/IEC 27002:2007, 11.2 Beheer van toegangsrechten van gebruikers, p. 70.

[7] NEN-ISO/IEC 27002:2007, 11.2 Beheer van toegangsrechten van gebruikers, p. 70.

Het autoriseren voor de toegang tot het CIS door de minister van Justitie maakt onderdeel uit van deze maatregelen. Dit autorisatievereiste is nader geregeld in artikel 5 lid 1 Besluit. Een verzoek van de bevoegde autoriteit kan alleen in het CIS worden ingevoerd door een door de minister van Justitie geautoriseerde (opsporings)ambtenaar die daartoe gebruik maakt van een hem toegekende toegangscode. Het belang hiervan ligt in de omstandigheid dat de gegevens die het betreft van gevoelige aard kunnen zijn, zodat toegang daartoe gestructureerd en bovendien niet door willekeurige personen plaats moet kunnen vinden. De omstandigheid dat de autorisatie wordt toegekend door de minister van Justitie benadrukt het gewicht van de maatregel.

Het toekennen van autorisaties kan de minister van Justitie ingevolge artikel 10:12 Algemene wet bestuursrecht (Awb) door middel van een mandaatbesluit overdragen aan personen die werkzaam zijn onder zijn verantwoordelijkheid. Een algemeen mandaat van deze strekking dient ingevolge artikel 10:5 Awb schriftelijk te worden verleend.

3.1.2 Bevindingen toekenning van autorisaties

A. *Autorisatie door de korpsbeheerder*

Uit het onderzoek is gebleken dat de toekenning van autorisaties aan medewerkers van korps Haaglanden ten behoeve van de bevraging van het CIS en de daaruit voortvloeiende verwerking van politiegegevens als volgt is geregeld. De voor het uitvoeren van CIOT-bevragingen beschikbare autorisaties zijn bij het korps Haaglanden aan medewerkers van BRI en BRR toegekend. Uit de interviews is gebleken dat een medewerker door het CIOT wordt geautoriseerd op voordracht van de lokale beheerder van het korps. De ploegchef BRI of coördinator BRR vraagt per e-mail of telefonisch bij de lokale beheerder een CIS-autorisatie voor een medewerker aan. De ploegchef BRI en de coördinator BRR zijn ervoor verantwoordelijk dat alleen medewerkers worden geautoriseerd die werkzaam zijn bij BRI of BRR en uit hoofde van hun taak toegang tot het CIS moeten hebben en hebben uit dien hoofde dan al een eerste beoordeling gemaakt of een medewerker in aanmerking komt voor een CIS-autorisatie. Toestemming voor de aanvraag van de gebruiker moet gebaseerd zijn op het systeem van autorisaties van het korps. De lokale beheerder controleert de aanvraag op volledigheid en bericht de ploegchef of coördinator of de aanvraag in behandeling wordt genomen. De lokale beheerder stuurt de aanvraag ondertekend per fax naar het CIOT. Van het CIOT ontvangt de lokale beheerder een ontvangstbevestiging en het bericht dat de aanvraag in behandeling wordt genomen. Naar aanleiding van de beoordeling door het CIOT ontvangt de gebruiker uiteindelijk, indien aan alle voorwaarden uit de CIS-procedure van het CIOT is voldaan, via de lokale beheerder de benodigde informatie om het CIS te kunnen bevragen. De toegangscode maakt hiervan onderdeel uit. Deze werkwijze voor het proces van toekenning van een autorisatie komt overeen met de procedure aanvragen CIS-accounts van het CIOT.
Voornoemde procedure is door het korps Haaglanden niet in een formele procedure vastgelegd, maar vindt volgens een intern afgesproken werkwijze plaats.

Beoordeling

Ingevolge artikel 6 lid 1 Wpg dient de korpsbeheerder een systeem aan te houden voor de toekenning van autorisaties voor de verwerking van politiegegevens, waarin

is vastgelegd aan welke politieambtenaren bepaalde autorisaties mogen worden toegekend, inclusief autorisaties tot het CIS. De wijze waarop deze toekenning van autorisaties plaatsvindt, dient op grond van de NEN-norm in een formele procedure te zijn vastgelegd. Uit het onderzoek is gebleken dat toekenning van een CIS-autorisatie volgens een intern afgesproken werkwijze plaatsvindt, maar niet in een formele procedure is vastgelegd. Hiermee wordt niet voldaan aan de vereisten die de NEN-norm op dit punt stelt en wordt in strijd gehandeld met artikel 6 lid 1 Wpg j° artikel 4 lid 3 Wpg.

B. *Autorisaties door de minister van Justitie*

Teneinde een bevoegde autoriteit, zijnde een door de beheerder van het korps aangewezen opsporingsambtenaar, toegang te kunnen verlenen tot het CIS houdt het CIOT de CIS-procedure aan. De medewerker ontvangt op deze manier onder meer de toegangscode die hij nodig heeft om een verzoek in het CIS te kunnen invoeren ingevolge artikel 5 lid 1 Besluit. Voor de toegang tot het CIS is een autorisatie door de minister van Justitie vereist. De minister van Justitie kan dit mandateren aan medewerkers van het CIOT. In het Mandaatbesluit CIOT 2000 geeft de minister van Justitie aan de directeur van het CIOT de bevoegdheid om namens de minister besluiten te nemen ten aanzien van – kort gezegd – het beheer. Uit het onderzoek is gebleken dat de toekenning van autorisaties aan medewerkers van de bevoegde autoriteiten plaatsvindt door medewerkers van afdeling Exploitatie en Beheer van het CIOT.

Beoordeling

Uit het Mandaatbesluit CIOT 2000 blijkt dat is voorzien in een rechtsgeldig mandaat waarmee de directeur van het CIOT namens de minister van Justitie autorisaties tot het CIS kan verlenen aan de bevoegde autoriteiten. Het mandaatbesluit CIOT 2000 voorziet niet in de mogelijkheid van ondermandaat zodat autorisaties enkel door de directeur van het CIOT kunnen worden toegekend.Het CBP stelt vast dat nu de autorisaties van de bevoegde autoriteiten, i.c. de medewerkers van het korps Haaglanden, niet door de directeur van het CIOT zijn toegekend deze niet rechtsgeldig overeenkomstig artikel 5 lid 1 Besluit zijn afgegeven. De invoer van een verzoek door de bevoegde autoriteit, i.c. een daartoe aangewezen opsporingsambtenaar van korps Haaglanden, om verstrekking van informatie is daarmee in strijd met artikel 5 lid 1 Besluit.

3.2 Controle op toegekende autorisaties

Controle kunnen uitoefenen op toegekende autorisaties impliceert dat deze toekenningen vastgelegd moeten zijn. Zonder deze vastlegging kan controle immers niet plaatsvinden. Vervolgens dient als gevolg van die controle vastgesteld te kunnen worden of de werkelijke situatie overeenkomt met de vastlegging en met de vereisten die worden gesteld aan autorisaties.

3.2.1 Norm

A. *Registratie van autorisaties*

Artikel 4 lid 3 Wpg legt aan de verantwoordelijke de verplichting op om passende technische en organisatorische maatregelen te nemen om politiegegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. In de artikelen 33, 34 en 35

Wpg is geregeld dat op de rechtmatige verwerking van gegevens interne en externe controle plaatsvindt. Om deze controle mogelijk te maken is de protocolplicht neergelegd in artikel 32 Wpg. Hierin is onder meer bepaald dat de verantwoordelijke zorg draagt voor de schriftelijke vastlegging van de toekenning van de autorisaties, zoals bedoeld in artikel 6 Wpg.

B. Controle op noodzaak verleende autorisaties
Voornoemde verplichting de toekenning van autorisaties vast te leggen biedt, zoals gezegd, aan de verantwoordelijke de mogelijkheid de toekenning van autorisaties te controleren. Voor deze controle is van belang te constateren dat uit artikel 6 lid 1 Wpg volgt dat de verantwoordelijke een systeem van autorisaties onderhoudt dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Deze vereisten zien eveneens op reeds toegekende autorisaties. Bovendien autoriseert de verantwoordelijke ingevolge artikel 6 lid 3 Wpg de ambtenaren van politie die onder zijn beheer vallen voor de verwerking van politiegegevens ter uitvoering van de onderdelen van de politietaak waarmee zij zijn belast.

Om te kunnen vaststellen of de controle hierop door het korps voldoende wordt uitgeoefend, sluit het CBP ook hier aan bij de NEN-norm. Hierin is voorgeschreven dat formele procedures dienen te zijn vastgesteld voor de beheersing van toewijzing van toegangsrechten tot informatiesystemen, in welke procedures alle fasen in de levenscyclus van gebruikerstoegang behoren te worden vastgelegd[8]. Deze procedure moet ook voorzien in het onmiddellijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd of de organisatie hebben verlaten[9].
De doelstelling hiervan is de toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen, zoals ook bedoeld in de artikel 4 lid 3 j° artikel 6 lid 1 Wpg, zodat de NEN-norm een uitwerking vormt van deze wettelijke normen.

3.2.2 Bevindingen

A. Registratie van autorisaties
Tijdens het onderzoek ter plaatse heeft het CBP van de lokale beheerder een autorisatieoverzicht ontvangen van de geregistreerde gebruikers. Uit dit overzicht blijkt dat 25 medewerkers van BRI en 19 medewerkers van BRR over toegang tot het CIS beschikken. Dit komt overeen met het aantal geregistreerde medewerkers op het overzicht dat het CBP van het CIOT heeft ontvangen.

Beoordeling
Tijdens het onderzoek is een autorisatieoverzicht overgelegd. Daarmee is voldaan aan de in artikel 32 Wpg bedoelde verplichting een schriftelijke vastlegging van de toekenning van de autorisaties bij te houden. Hiermee is op dit punt in overeenstemming gehandeld met artikel 32 lid 1 onder c Wpg.

B. Controle op noodzaak verleende autorisaties

[8] NEN-ISO/IEC 27002:2007, 11.2 beheer toegangsrechten gebruikers, p. 70.

[9] NEN-ISO/IEC 27002:2007, 11.2.1 registratie gebruikers, p.70.

Zoals bovenvermeld heeft het CBP tijdens het onderzoek ter plaatse een autorisatieoverzicht ontvangen van de geregistreerde gebruikers. Uit dit overzicht blijkt dat 25 medewerkers van BRI en 19 medewerkers van BRR over toegang tot het CIS beschikken. Bij BRI zijn naast de zes medewerkers van de Front-Office voor wie het bevragen van het CIS tot hun taak behoort nog 19 andere medewerkers geautoriseerd. Deze zijn werkzaam binnen andere taakvelden. Uit de interviews blijkt dat BRI meer medewerkers heeft geautoriseerd om het risico te vermijden dat in populaire verlofperiodes niemand aanwezig is die CIOT-bevragingen kan uitvoeren.

Uit het onderzoek blijkt voorts dat een autorisatie om verschillende redenen kan worden ingetrokken. Ten eerste is een certificaat maximaal één jaar geldig en dient de medewerker jaarlijks opnieuw een certificaat bij het CIOT aan te vragen. Hiertoe krijgt de lokale beheerder bericht van het CIOT. De lokale beheerder moet controleren of alle autorisaties nog actueel zijn en verlengd dienen te worden. Daarnaast kan een autorisatie worden ingetrokken bij uitdiensttreding of wijziging van een functie van een medewerker of bij vermoedens van fraude.

Uit het interview met de lokale beheerder blijkt dat indien een medewerker het korps Haaglanden verlaat, van functie wijzigt of de autorisatie niet meer gebruikt, de lokale beheerder op verzoek van de ploegchef BRI of de coördinator BRR de autorisatie in de applicatie blokkeert en dit schriftelijk aan het CIOT meldt. Na controle wordt het account door het CIOT ingetrokken en wordt via de lokale beheerder de medewerker hiervan schriftelijk op de hoogte gesteld. Het korps Haaglanden heeft deze werkwijze voor het intrekken van een account niet in een formele procedure vastgelegd.

Beoordeling
Het CBP constateert dat het aantal op het autorisatieoverzicht vermelde geautoriseerde medewerkers bij BRI, zijnde 25, niet in overeenstemming is met het aantal medewerkers dat uit hoofde van hun taak belast is met het uitvoeren van CIOT-bevragingen, te weten zes. Het CBP is van oordeel dat de autorisatie van de overige 19 medewerkers bij BRI, gelet op het doel waarvoor zij beschikken over die autorisatie, niet in overeenstemming is met het vereiste dat alleen ambtenaren van politie worden geautoriseerd voor de verwerking van politiegegevens ter uitvoering van de politietaak waarmee zij zijn belast. Het CBP concludeert in dit kader dat de autorisatie van de 19 extra medewerkers bij BRI in strijd is met artikel 6 lid 3 Wpg.

Het CBP stelt vervolgens vast dat een CIS-account onder bepaalde omstandigheden kan worden ingetrokken en dat bij het korps hiertoe een intern afgesproken werkwijze wordt gebruikt. Een formele procedure voor het intrekken van een autorisatie is niet beschikbaar. Wegens het ontbreken van een vastgestelde formele procedure voor de intrekking van autorisaties voor het CIS wordt niet voldaan aan de vereisten die de NEN-norm op dit punt daaraan stelt[10]. Hiermee wordt in strijd gehandeld met artikel 4 lid 3 j° artikel 6 lid 1 Wpg.

[10] NEN-ISO/IEC 27002:2007, 11.2.1 registratie gebruikers, p.70.

4 BEVEILIGING VAN VERZENDING VAN GEGEVENS DOOR HET KORPS HAAGLANDEN AAN TELECOMMUNICATIEAANBIEDERS

4.1 Onderzoek van verzending van gegevens aan telecommunicatieaanbieders

Het CBP heeft onderzoek verricht naar de beveiliging die door de korpsen wordt gebruikt bij rechtstreekse verzending van gegevens aan telecommunicatieaanbieders zonder tussenkomst van het CIOT. De verzending van gegevens door de telecommunicatieaanbieders valt buiten de scope van dit onderzoek.

4.2 Norm

Artikel 4 lid 3 Wpg legt aan de verantwoordelijke de verplichting op om passende technische en organisatorische maatregelen te treffen ter beveiliging van de gegevens die aan de telecommunicatieaanbieders worden verzonden. Passende technische en organisatorische maatregelen betekenen in dit verband dat de verantwoordelijke voldoende waarborgen treft zodat gegevens die rechtstreeks bij de telecommunicatieaanbieder worden bevraagd, zodanig worden beveiligd dat voorkomen wordt dat de gegevens onrechtmatig worden verwerkt of verloren kunnen gaan. Dergelijke passende technische en organisatorische maatregelen moeten ook worden getroffen bij de verzending van gegevens. Aangezien het hier mede om gegevens met een gevoelig karakter gaat, weegt de keuze van de beveiliging die voor de verzending van gegevens wordt gebruikt des te zwaarder.

Hieruit volgt dat de aanvragen die door de korpsen rechtstreeks bij de telecommunicatieaanbieders worden gedaan dusdanig moeten zijn beveiligd dat (achteraf) kan worden vastgesteld dat de gegevens die aan de telecommunicatieaanbieder zijn verstuurd onderweg niet zijn afgetapt of gewijzigd.

Om te kunnen vaststellen dat gegevens niet zijn gewijzigd of afgetapt sluit het CBP ook hier aan bij de NEN-norm waarin is vastgelegd dat bijzondere beheersmaatregelen dienen te worden getroffen om de vertrouwelijkheid en integriteit te waarborgen van gegevens die via openbare netwerken worden verzonden en om aangesloten systemen en toepassingen te beschermen[11]. De NEN-norm[12] vereist dat de organisatie voor de uitwisseling van informatie technologie toepast, waarmee de vertrouwelijkheid en integriteit van gegevens wordt gewaarborgd. In dit verband schrijft de NEN-norm voor dat ter bescherming van gevoelige informatie die wordt verzonden over communicatielijnen bijzondere beheersmaatregelen worden getroffen zoals het gebruik van encryptie[13].

4.3 Bevindingen

Bevindingen
De vorderingen van gegevens door het korps Haaglanden bij de telecommunicatieaanbieders kunnen betrekking hebben op het alsnog opvragen van gebruikersgegevens na een 'no-hit'-melding door het CIOT op vordering van een

[11] NEN-ISO/IEC 27002:2007, 10.6, p.53 en 10.6.1, p.54.

[12] NEN-ISO/IEC 27002:2007, 10.6.1 p. 54

[13] NEN-ISO/IEC 27002:2007, 12.3, p.90, 91.

opsporingsambtenaar[14] dan wel de officier van justitie[15] of tot het in opdracht van de officier van justitie vorderen van verkeersgegevens, locatiegegevens, identificerende gegevens of zelfs toekomstige gegevens, onder vermelding van het misdrijf waar het onderzoek betrekking op heeft. De combinatie van bijvoorbeeld identificerende gegevens met gegevens van een misdrijf levert gevoelige gegevens[16] op. Verkeersgegevens die kunnen worden opgevraagd betreffen gegevens over een bepaalde periode waarin per gesprek het tijdstip, de duur van het gevoerde gesprek en het nummer van de persoon met wie is gebeld is vermeld.

Uit de interviews blijkt dat er voor de rechtstreekse bevragingen bij de telecommunicatieaanbieders een interne afgesproken procedure wordt gevolgd. De procedure voor 'no-hit'-bevragingen en overige vorderingen op verzoek van de officier van justitie verloopt als volgt.
Indien een geautomatiseerde CIOT-bevraging als resultaat een 'no-hit' heeft, wordt een 'no-hit-fax' uitgeprint. Deze 'no-hit-fax' wordt aan de aanvrager uit het onderzoeksteam verstrekt. Indien het onderzoeksteam besluit dat de bevraging in het kader van het onderzoek van belang is wordt de 'no-hit'-procedure opgestart. Hiervoor wordt een proces-verbaal 'aanvraag vordering gegevens verstrekking ex artikel 126nc WvSv' opgesteld en aan de Unit Landelijke Interceptie (ULI) van het KLPD gestuurd. De ULI schrijft voor dat een 'no-hit'-aanvraag alleen per fax kan worden aangeleverd. Hierbij wordt gebruik gemaakt van openbare telefoonlijnen zonder additionele beveiligingsmaatregelen. De ULI verstuurt vervolgens de fax naar de telecommunicatieaanbieder waarop de gegevens betrekking hebben. Ook deze fax wordt over een gewone openbare telefoonlijn zonder gebruik te maken van additionele beveiligingsmaatregelen aan de telecommunicatieaanbieder verzonden. Uit de interviews met de lokale beheerder en de medewerkers die de bevragingen uitvoeren is voorts gebleken dat ook de overige vorderingen over een openbare telefoonlijn zonder additionele beveiligingsmaatregelen worden verzonden.

Beoordeling
Uit het onderzoek is gebleken dat de 'no-hit'-faxen en overige vorderingen in het kader van strafvordering door het korps Haaglanden via een openbare telefoonlijn zonder beveiliging worden verzonden aan de ULI en de telecommunicatieaanbieders. De NEN-norm schrijft voor dat ter bescherming van gevoelige informatie die wordt verzonden over communicatielijnen en openbare netwerken bijzondere beheersmaatregelen dienen te worden getroffen om de vertrouwelijkheid en integriteit daarvan te waarborgen[17]. Aangezien hier sprake is van verzending van gevoelige gegevens, betreffende vorderingen in het kader van strafvordering, is het CBP van oordeel dat het korps Haaglanden hier bijzondere beheersmaatregelen had behoren te treffen. Nu de verzending plaatsvindt via openbare telefoonlijnen zonder additionele beveiligingsmaatregelen is daarin niet voorzien, zodat niet is voldaan aan de eisen van de NEN-norm op dit punt. Er is dan ook geen sprake van een passend beveiligingsniveau. Dit is in strijd met artikel 4 lid 3 Wpg.

[14] In geval van verdenking van een misdrijf.

[15] In geval van verdenking van een misdrijf als omschreven in artikel 67 lid 1 WvSv.

[16] Het betreft hier 'gevoelige gegevens' in de zin van artikel 5 Wpg.

[17] NEN-ISO/IEC 27002:2007, 10.6, p.53 en 10.6.1, p.54; 12.3, p.90, 91.

5 De rechtmatigheid van de bevragingen

5.1 Onderzoek rechtmatigheid van bevragingen

Het CBP heeft tien geselecteerde CIOT-bevragingen onderzocht op de vraag of deze bevragingen op onderdelen rechtmatig zijn uitgevoerd. Om deze bevragingen te onderzoeken hebben vier onderzoeken ter plaatse plaatsgevonden, te weten op 2, 12, 23 en 25 maart 2010.

5.2 Norm

Ten behoeve van een (opsporings)onderzoek kunnen door opsporingsdiensten de volgende gegevens worden gevorderd: naam, adres, postcode, woonplaats, nummer en soort dienst -de zogeheten gebruikersgegevens- van een gebruiker van telecommunicatie. Dit heeft niet alleen betrekking op gegevens ten aanzien van telefonie, maar ook van internet- en e-mailgebruik. In het CIOT-Informatiesysteem (CIS) vindt op geautomatiseerde wijze de vergelijking plaats tussen de bevragingsgegevens afkomstig van politie en opsporingsdiensten en de bestanden van de telecommunicatieaanbieders. Deze gegevens worden door politiekorpsen en opsporingsdiensten verwerkt onder het regime van de Wpg.

Artikel 3 lid 2 Wpg bepaalt dat politiegegevens slechts worden verwerkt voor zover zij rechtmatig zijn verkregen. Voor een rechtmatige verwerking van CIOT-gegevens geldt onder meer als voorwaarde dat de rechtsgrondslag waaronder de bevraging is uitgevoerd moet zijn gebaseerd op de desbetreffende artikelen met vorderingsbevoegdheden in het Wetboek van Strafvordering (WvSv) en dat de daarbij behorende voorwaarden moeten zijn nageleefd.

De desbetreffende artikelen met vorderingsbevoegdheden in het WvSv worden in het onderstaande behandeld.

Op grond van artikel 126na WvSv kan een opsporingsambtenaar in geval van verdenking van een misdrijf en in het belang van het onderzoek gebruikersgegevens vorderen. Voor die vordering is verplicht gesteld dat daarvan een proces-verbaal wordt opgemaakt, waarin onder meer moet zijn vermeld welke gegevens worden gevorderd.
Artikel 126n WvSv geeft aan de officier van justitie de bevoegdheid in geval van verdenking van een misdrijf als omschreven in artikel 67 lid 1 WvSv -dat zijn de misdrijven waarvoor voorlopige hechtenis is toegelaten- in het belang van het onderzoek, zogeheten verkeersgegevens[18] te vorderen. Deze bevoegdheid omvat ook het vorderen van gebruikersgegevens, die –in tegenstelling tot verkeersgegevens- via het CIOT kunnen worden bevraagd. Voor deze vordering geldt eveneens dat het opmaken van een proces-verbaal verplicht is met onder meer de vermelding daarin van de gevorderde gegevens.
Wanneer de officier van justitie in een opsporingsonderzoek een telefoontap noodzakelijk acht is het gebruikelijk om voorafgaand het CIOT te bevragen ten aanzien van het af te luisteren telefoonnummer ter verificatie van de identiteit van de

[18] Verkeersgegevens zijn gebelde nummers met bijbehorende tijdstippen en de duur van elk gevoerd gesprek.

gebruiker. Het bevel tot het meewerken aan het opnemen van telecommunicatie op grond van artikel 126m WvSv dat zich richt tot de telecommunicatieaanbieder, wordt in die gevallen gecombineerd met een vordering op grond van artikel 126n WvSv in een zogeheten combivordering.

Artikel 126ua WvSv omschrijft voor de opsporingsambtenaar een overeenkomstige bevoegdheid als in artikel 126na, maar dan in het geval van een redelijk vermoeden van misdrijven beraamd of gepleegd in georganiseerd verband, zoals omschreven in artikel 126o lid 1 WvSv. Ook hier gelden dezelfde vereisten ten aanzien van een daartoe opgemaakt proces-verbaal en de vermelding van de gevorderde gegevens. In artikel 126u WvSv wordt een overeenkomstige bevoegdheid als in artikel 126n WvSv voor de officier van justitie omschreven voor het geval van misdrijven in georganiseerd verband en met dezelfde daarvoor geldende voorwaarden ten aanzien van het op te maken proces-verbaal en de vermelding van de gevorderde gegevens.

Artikel 126zi WvSv omschrijft de bevoegdheid van een opsporingsambtenaar om in het belang van het onderzoek gebruikersgegevens te vorderen in geval van aanwijzingen van een terroristisch misdrijf. Onder een terroristisch misdrijf wordt verstaan de in artikel 83 Wetboek van Strafrecht opgesomde misdrijven, die met een terroristisch oogmerk worden gepleegd. Ook hier gelden dezelfde voorwaarden ten aanzien van het opmaken en de inhoud van het proces-verbaal als hiervoor genoemd. In artikel 126zh WvSv is de overeenkomstige bevoegdheid als in artikel 126n WvSv voor de officier van justitie omschreven voor het geval van aanwijzingen van een terroristisch misdrijf en met dezelfde daarvoor geldende voorwaarden ten aanzien van het op te maken proces-verbaal en de vermelding van de gevorderde gegevens.

Ten slotte kan op grond van artikel 126ii WvSv de officier van justitie in geval van een verkennend onderzoek naar de voorbereiding van de opsporing van terroristische misdrijven, in het belang van het onderzoek gebruikersgegevens vorderen. Ook hier gelden dezelfde voorwaarden ten aanzien van het opmaken en de inhoud van het proces-verbaal als hiervoor genoemd.

5.3 Bevindingen dossieronderzoek

Het CBP heeft bij het eerste onderzoek ter plaatse bij Bureau BRR met behulp van de lokale beheerder voor het CIS bij het korps zes onderzoeksdossiers verzameld van lopende zaken waarin CIOT-bevragingen werden uitgevoerd en die op dat moment daar in behandeling waren. Het betrof hierbij steeds bevragingen uitgevoerd op basis van artikel 126n WvSv. Deze bevragingen zijn in de samenvatting en in de bijlage aangeduid met A1 tot en met A6. Het geselecteerde dossier A6 bleek twee CIOT-bevragingen te bevatten. Deze zijn als A6a en A6b weergegeven.
Bij het tweede bezoek aan het korps heeft het CBP een aanvullende selectie uitgevoerd. Eerst zijn twee bevragingen geselecteerd die op andere gronden dan artikel 126n WvSv zijn uitgevoerd, eveneens met behulp van de lokale beheerder aan de hand van het CIOT-overzichtscherm voor bevragingen. Vervolgens zijn twee bevragingen geselecteerd die betrekking hadden op de vordering van internetgegevens, welke selectie werd uitgevoerd met behulp van de groepschef BRI uit gearchiveerde mappen met de berichtenafhandeling van CIOT-bevragingen. Deze bevragingen zijn in de samenvatting en de bijlage aangeduid als B1 tot en met B4.

De geselecteerde bevragingen zijn onderzocht op de aanwezigheid van de grondslag uit het WvSv waarop de bevraging is gebaseerd en het verband tussen bevraging en het gebruikte referentienummer waaronder de bevraging is uitgevoerd. Dit laatste om te controleren of de bevraagde gegevens hun grondslag vinden in het achterliggende onderzoeksdossier. Het vermelde referentienummer heeft betrekking op het onderzoeksnummer, proces-verbaalnummer of parketnummer van het dossier.

Daarbij heeft het CBP de volgende vereisten in aanmerking genomen:

1. Dat het desbetreffende artikel met vorderingsbevoegdheid in het WvSv (grondslag) wordt genoemd en dat het proces-verbaal van aanvraag van de vordering deze grondslag van bevraging vermeldt.
2. Dat het proces-verbaal van aanvraag van de vordering de gegevens die worden gevorderd vermeldt.
3. Dat het proces-verbaal van aanvraag van de vordering vermeldt of de vordering door een officier van justitie dan wel een opsporingsambtenaar is gedaan.

Voor het uitvoeren van de controle is allereerst essentieel dat op basis van de gegevens op het overzichtsscherm van uitgevoerde bevragingen in het CIS door het korps een afdruk uit het CIS wordt getoond waarop de precieze bevraagde gegevens zijn vermeld. Aan de hand van deze bevraagde gegevens dienen uit het onderzoeksdossier de vereiste achterliggende stukken te worden verzameld, waarna de bovengenoemde controle kan plaatsvinden.

Geconstateerd is dat bij vrijwel geen enkel dossier de benodigde documentatie volledig en geordend werd aangeleverd. Het gevolg hiervan was dat er meerdere bezoeken moesten worden afgelegd om de aanvullende bescheiden alsnog te kunnen inzien.

Het CBP heeft de beschrijving van de onderzochte bevragingen alsmede de beoordeling daarvan per dossier opgenomen in de bijlage bij dit rapport. In het onderstaande volgt een samenvatting daarvan.

5.4 Samenvattende beoordeling dossieronderzoek

Het CBP heeft tien CIOT-bevragingen geselecteerd en onderzocht op de vraag of deze bevragingen op onderdelen rechtmatig zijn uitgevoerd. Eén van deze geselecteerde bleek -zoals hierboven vermeld- uit twee onderdelen te bestaan, zodat elf bevragingen zijn beoordeeld. Van de onderzochte bevragingen voldoen zes bevragingen (bevraging A1, A2, A3, A4, A5 en A6b) aan de eerder genoemde vereisten waaraan is getoetst en deze zijn daarmee in overeenstemming met artikel 3 lid 2 Wpg. Bij deze bevragingen waren de achterliggende bescheiden aanvankelijk niet de juiste en konden deze pas nadat het CBP hier aanvullend om had gevraagd, bij een vervolgonderzoek ter plaatse worden ingezien.
De overige vijf bevragingen (bevraging A6a, B1, B2, B3 en B4) zijn in strijd met artikel 3 lid 2 Wpg omdat daarbij telkens een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbrak, terwijl bij één daarvan (A6a) tevens de vordering door de officier van justitie ontbrak.
Dit leidt tot de conclusie dat het korps Haaglanden zich voor vijf onderzochte CIOT-bevragingen niet kan verantwoorden. Hiermee wordt in strijd gehandeld met artikel 3 lid 2 Wpg.

6 CONCLUSIE

Op grond van de bevindingen van het onderzoek komt het CBP met betrekking tot het korps Haaglanden tot de volgende conclusies.

Ten aanzien van toekenning van autorisaties bij het korps Haaglanden:

- Uit het onderzoek is gebleken dat een vastgelegde formele procedure voor het toekennen van autorisaties door de korpsbeheerder aan medewerkers van het korps Haaglanden voor de verwerking van politiegegevens, inclusief de bevraging van het CIS, niet aanwezig is. Hiermee wordt niet voldaan aan de vereisten die de NEN-norm op dit punt stelt en wordt in strijd gehandeld met artikel 6 lid 1 j° artikel 4 lid 3 Wpg.
- Het CBP stelt vast dat de autorisaties van de bevoegde autoriteiten, i.c. de medewerkers van het korps Haaglanden, niet rechtsgeldig overeenkomstig artikel 5 lid 1 Besluit zijn afgegeven. De invoer van een verzoek door de bevoegde autoriteit, i.c. een daartoe aangewezen opsporingsambtenaar van korps Haaglanden, om verstrekking van informatie is daarmee in strijd met artikel 5 lid 1 Besluit.

Ten aanzien van de controle op toegekende autorisaties:

- Tijdens het onderzoek door het CBP is door het korps Haaglanden een autorisatieoverzicht overgelegd. Daarmee is voldaan aan de verplichting een schriftelijke vastlegging van de toekenning van de autorisaties bij te houden. Hiermee is op dit punt in overeenstemming gehandeld met artikel 32 lid 1 onder c Wpg.
- Het CBP constateert dat het aantal op het autorisatieoverzicht vermelde geautoriseerde medewerkers bij BRI, zijnde 25, niet in overeenstemming is met het aantal medewerkers dat uit hoofde van hun taak belast is met het uitvoeren van CIOT-bevragingen, te weten zes. Het CBP is van oordeel dat de autorisatie van de overige 19 medewerkers bij BRI, gelet op het doel waarvoor zij beschikken over die autorisatie, niet in overeenstemming is met het vereiste dat alleen ambtenaren van politie worden geautoriseerd voor de verwerking van politiegegevens ter uitvoering van de politietaak waarmee zij zijn belast. Het CBP concludeert in dit kader dat de autorisatie van de 19 extra medewerkers bij BRI in strijd is met artikel 6 lid 3 Wpg.
- Wegens het ontbreken van een vastgelegde formele procedure voor de intrekking van autorisaties tot het CIS wordt niet voldaan aan de vereisten die de NEN-norm daaraan stelt. Hiermee wordt in strijd gehandeld met artikel 4 lid 3 j° artikel 6 lid 1 Wpg.

Ten aanzien van de beveiliging van verzending van gegevens door het korps aan telecommunicatieaanbieders:

- De verzending van zogeheten 'no-hit'-faxen en van overige vorderingen in het kader van strafvordering die rechtstreeks tot de telecommunicatieaanbieders zijn gericht, vindt plaats via openbare telefoonlijnen zonder additionele beveiligingsmaatregelen. Nu de NEN-norm voorschrijft dat bij verzending van gevoelige gegevens ter bescherming van gevoelige informatie die wordt verzonden over communicatielijnen en openbare netwerken bijzondere beheersmaatregelen dienen te worden getroffen om de vertrouwelijkheid en

integriteit daarvan te waarborgen en hierin niet is voorzien, is niet voldaan aan de eisen van de NEN-norm op dit punt. Er is dan ook geen sprake van een passend beveiligingsniveau. Dit is in strijd met artikel 4 lid 3 Wpg.

Ten aanzien van de rechtmatigheid van de onderzochte bevragingen:

- Van de elf onderzochte bevragingen zijn er zes bevragingen voor zover onderzocht in overeenstemming met artikel 3 lid 2 Wpg.
- Vijf bevragingen zijn in strijd met artikel 3 lid 2 Wpg omdat daarbij telkens een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbrak, terwijl bij één daarvan tevens de vordering door de officier van justitie ontbrak. Dit leidt tot de conclusie dat het korps Haaglanden zich voor vijf onderzochte CIOT-bevragingen niet kan verantwoorden. Hiermee wordt in strijd gehandeld met artikel 3 lid 2 Wpg.

Deze definitieve bevindingen zijn aldus vastgesteld op 21 april 2011.

Voor het College bescherming persoonsgegevens,

mw.mr.dr. J. Beuving
collegelid

BIJLAGE

Bijlage bij hoofdstuk 5 van het rapport van het CIOT-onderzoek bij het korps Haaglanden

Bespreking per dossier

Bevraging A1 is uitgevoerd in 2009 op grond van artikel 126n WvSv op vordering van de officier van justitie. Uit het proces-verbaal van aanvraag blijkt dat het bevraagde telefoonnummer was opgeslagen in de mobiele telefoon van het slachtoffer. Voor het tappen van dit telefoonnummer heeft de officier van justitie op de dag van de bevraging mondeling toestemming gegeven. Een combivordering artikel 126m/n WvSv in dat verband is drie dagen later schriftelijk vastgelegd, waarbij is vermeld dat het een schriftelijke vastlegging betreft van de mondelinge vordering.

Beoordeling
Bevraging A1 bleek na controle te voldoen aan de door het CBP onderzochte vereisten en is in zoverre in overeenstemming met artikel 3 lid 2 Wpg.

Bevraging A2 is uitgevoerd in 2010 op grond van artikel 126n WvSv op vordering van de officier van justitie. Uit het proces-verbaal van aanvraag volgt dat het bevraagde telefoonnummer twee dagen eerder is gebleken uit een tapverslag dat is opgemaakt naar aanleiding van een al lopende tap op een telefoonnummer in het onderzoek. Aanvankelijk ontbreken stukken met betrekking tot de vorderingen. Na navraag blijkt dat voor het tappen van het bevraagde telefoonnummer de officier van justitie de dag na de bevraging een artikel 126m WvSv vordering heeft afgegeven. Drie dagen daarna volgt een vordering op grond van artikel 126n WvSv met betrekking tot het bevraagde nummer.

Beoordeling
Bevraging A2 bleek na controle te voldoen aan de door het CBP onderzochte vereisten en is in zoverre in overeenstemming met artikel 3 lid 2 Wpg.

Bevraging A3 is een bevraging naar drie telefoonnummers uitgevoerd in 2010 op grond van artikel 126n WvSv op vordering van de officier van justitie. Uit het aanvraagproces-verbaal blijkt dat de bevraagde telefoonnummers behoren bij meerdere verdachten die uit het onderzoek naar voren zijn gekomen. Drie dagen na de bevraging volgt een combivordering artikel 126m/n WvSv ten aanzien van deze nummers.

Beoordeling
Bevraging A3 bleek na controle te voldoen aan de door het CBP onderzochte vereisten en is in zoverre in overeenstemming met artikel 3 lid 2 Wpg.

Bevraging A4 is uitgevoerd in 2009 op grond van artikel 126n WvSv op vordering van de officier van justitie. Uit het aanvraagproces-verbaal blijkt dat het bevraagde telefoonnummer een nummer betreft waarnaar een ander uit het onderzoek gebleken nummer werd doorgeschakeld. Een combivordering artikel 126m/n WvSv betreffende het bevraagde telefoonnummer is vijf dagen voor de bevraging afgegeven.

Beoordeling
Bevraging A4 bleek na controle te voldoen aan de door het CBP onderzochte vereisten en is in zoverre in overeenstemming met artikel 3 lid 2 Wpg.

Bevraging A5 is uitgevoerd in 2009 op grond van artikel 126n WvSv op vordering van de officier van justitie. Uit het aanvraagproces-verbaal blijkt dat de aanvraag is gedaan met het oog op het tappen van telefoons. Bevraagd is de combinatie van postcode en huisnummer van een verdachte. Uit de bevraging blijken twee telefoonnummers. Een combivordering artikel 126m/n WvSv ten aanzien van één van deze nummers volgt een dag later.

Beoordeling
Bevraging A5 bleek na controle te voldoen aan door het CBP onderzochte vereisten en is in zoverre in overeenstemming met artikel 3 lid 2 Wpg.

Bevraging A6a is uitgevoerd in 2009 op grond van artikel 126n WvSv op vordering van de officier van justitie. Uit het aanvraagproces-verbaal blijkt dat in het onderzoek een tap is geplaatst op een telefoonnummer van verdachte 1. Uit deze tap is vervolgens een telefoonnummer van verdachte 2 gebleken. Om uit te zoeken van welke telefoonnummers deze verdachte nog meer gebruik maakt is het CIOT bevraagd op postcode en huisnummer van verdachte 2. Aanvankelijk ontbreken de bijbehorende vorderingen. Na navraag wordt het dossier aangevuld met een vordering artikel 126n WvSv ten aanzien van het telefoonnummer van verdachte 1, gedateerd zeven weken voor de bevraging, en een combivordering artikel 126m/n WvSv ten aanzien van het telefoonnummer van verdachte 1 die mede betrekking heeft op het vorderen van de nummers waarmee gebeld wordt. Deze combivordering is vier weken voor deze bevraging afgegeven. Een zelfstandige vordering ten aanzien van de bevraging op postcode en huisnummer van verdachte 2 is niet aangetroffen noch een daarop betrekking hebbend aanvraagproces-verbaal.
Bevraging A6b is ongeveer 3 maanden na bevraging A6a uitgevoerd in hetzelfde onderzoek en eveneens op grond van artikel 126n WvSv op vordering van de officier van justitie. Bevraagd is het telefoonnummer van verdachte 2 zoals dit was gebleken uit de telefoontap op het nummer van verdachte 1. Een combivordering artikel 126m/n WvSv met betrekking tot het bevraagde telefoonnummer volgt zes dagen later.

Beoordeling
Ten aanzien van **Bevraging A6a** is geen aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens aangetroffen en evenmin de hierop betrekking hebbende vordering door de officier van justitie, zodat de bevraging in zoverre in strijd is met artikel 3 lid 2 Wpg. Ten aanzien van **Bevraging A6b** is voldaan aan de door het CBP onderzochte vereisten en is de bevraging in zoverre in overeenstemming met artikel 3 lid 2 Wpg.

Bevraging B1 is uitgevoerd in 2010 op grond van artikel 126na WvSv door een opsporingsambtenaar. Blijkens een proces-verbaal van de aanvraag vordering verkeersgegevens betreft het een bevraging in een onderzoek dat op dezelfde datum is gestart als de bevraging is uitgevoerd. De twee bevraagde telefoonnummers zijn niet dezelfde als de in het proces-verbaal vermelde. Uit een proces-verbaal van de aanleiding van het onderzoek blijkt dat het tweede bevraagde nummer uit een eerder onderzoek in 2008 naar voren is gekomen als een telefoonnummer dat bij één van de medeverdachten in het onderzoek in gebruik was. Aanvankelijk bleek niet op grond waarvan het eerste nummer was bevraagd. Uit nageleverde informatie is gebleken dat dit telefoonnummer naar voren is gekomen uit een eerder strafdossier waarin deze medeverdachte een betrokkene was bij een door een ander gedane aangifte en waarbij als contactgegevens de beide bevraagde telefoonnummers waren opgegeven. Een proces-verbaal waarin de bevragende opsporingsambtenaar de beide bevraagde telefoonnummers heeft vermeld is niet aangetroffen.

Beoordeling
Bevraging B1 is uitgevoerd op grond van artikel 126na WvSv. Uit de stukken van het

onderzoek is voor wat betreft één bevraagd nummer de herkomst af te leiden, voor wat betreft het andere bevraagde nummer is de herkomst gebleken aan de hand van gegevens uit een ander dossier, maar dat nummer is niet gedocumenteerd in een proces-verbaal. Omdat een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbrak, is de bevraging in zoverre in strijd met artikel 3 lid 2 Wpg.

Bevraging B2 is uitgevoerd in 2010 op grond van artikel 126na WvSv door een opsporingsambtenaar. Een proces-verbaal van relaas vermeldt dat het onderzoek is gestart op de dag voorafgaande aan de bevraging. Bevraagd is één telefoonnummer. Voor het tappen van het telefoonnummer van de verdachte heeft de officier van justitie op de dag van de bevraging mondeling toestemming gegeven, een combivordering artikel 126m/n WvSv in dat verband is vier dagen later aangevraagd. Een proces-verbaal van aanvraag waarin de opsporingsambtenaar de bevraagde gegevens heeft vermeld is niet aangetroffen.

Beoordeling
Bij **Bevraging B2** ontbrak het vereiste proces-verbaal van aanvraag met vermelding van het bevraagde nummer, zodat de bevraging in zoverre in strijd is met artikel 3 lid 2 Wpg.

Bevraging B3 is uitgevoerd in 2010 op grond van artikel 126na WvSv door een opsporingsambtenaar. Het betreft de bevraging van een IP-adres dat door de verdachte zou worden gebruikt. Dit IP-adres is overgenomen van een consumentenwebsite waarop vermeld stond dat dit IP-adres door de verdachte is gebruikt. Naast het proces-verbaal van aangifte werd geen afzonderlijk proces-verbaal van aanvraag aangetroffen waarin de opsporingsambtenaar de grondslag voor het bevraagde IP-adres heeft vermeld.

Beoordeling
Bij **Bevraging B3** ontbreekt het vereiste aanvraagproces-verbaal met vermelding van het bevraagde nummer, zodat de bevraging in zoverre in strijd is met artikel 3 lid 2 Wpg.

Bevraging B4 is uitgevoerd in 2010 op grond van artikel 126na WvSv door een opsporingsambtenaar. Het betreft de bevraging van IP-adressen. Aangifte van het misdrijf is twee weken eerder opgenomen. Daarop heeft de opsporingsambtenaar een vordering tot verstrekking van identificerende gegevens gericht aan een sociale netwerksite om de IP-adressen waarmee binnen een bepaalde periode is ingelogd op de betreffende specifieke netwerkpagina op te vragen. De hieruit volgende vier IP-adressen zijn vervolgens bij het CIOT bevraagd. De vermelding van de bevraagde gegevens zijn niet terug te vinden in een relevant aanvraagproces-verbaal.

Beoordeling
Bij **Bevraging B4** zijn de bevraagde IP-adressen af te leiden uit de stukken, maar zijn deze niet afzonderlijk gedocumenteerd.Omdat een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbrak, is de bevraging in zoverre in strijd met artikel 3 lid 2 Wpg.