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 Dienst Nationale Recherche
z2010-00170

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 DNR 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 de DNR 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 Wpg j° artikel 4 lid 3 Wpg.
- Het CBP stelt vast dat de autorisaties van de bevoegde autoriteiten, i.c. de medewerkers van de DNR, 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 de DNR, 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 is door de DNR een autorisatieoverzicht van de toegekende autorisaties tot het CIS overgelegd. Dit autorisatieoverzicht was niet volledig zodat niet is voldaan aan de verplichting zorg te dragen voor de schriftelijke vastlegging van de toekenning van autorisaties. Dit is in strijd met artikel 32 lid 1 onder c Wpg.
- Uit het onderzoek is gebleken dat het intrekken van autorisaties van medewerkers van de DNR voor het CIS niet is vastgelegd in een formele procedure. Derhalve wordt niet voldaan aan de vereisten die de NEN-norm op dit punt stelt en 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 van de officier van justitie 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 twee bevragingen voor zover onderzocht in overeenstemming met artikel 3 lid 2 Wpg.
- Negen bevragingen zijn in strijd met artikel 3 lid 2 Wpg. In twee gevallen omdat geen verband was vast te stellen tussen de bevraagde gegevens en het daarbij gebruikte referentienummer enerzijds en de vereiste vordering en aanvraagproces-verbaal met het daarbij vermelde referentienummer anderzijds. In vier gevallen omdat niet kon worden vastgesteld welke gegevens feitelijk waren bevraagd, zodat het verband met het dossier niet kon worden vastgesteld. In een volgend geval omdat zowel de vordering door de officier van justitie als een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbraken. In een ander geval omdat geen verband kon worden vastgesteld tussen de

bevraagde gegevens en de vereiste vordering en aanvraagproces-verbaal en ook niet kon worden vastgesteld wanneer de bevraging precies had plaatsgevonden en op welke rechtsgrondslag. Tenslotte een geval waarin het vereiste aanvraagproces-verbaal ontbrak.
Dit leidt tot de conclusie dat de DNR zich voor negen 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 de DNR.

Het CBP heeft de DNR op de locatie Amsterdam bezocht op 8 maart 2010 en 6 april 2010 en bij een aanvullend onderzoek op 9 november 2010 op de locatie Driebergen. Tijdens het onderzoek ter plaatse zijn voor wat betreft 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.
Op grond van het bepaalde in artikel 60, tweede lid, Wbp is het rapport van voorlopige bevindingen op 16 december 2010 aan de korpsbeheerder van het Korps Landelijke Politiediensten toegezonden en is hij in de gelegenheid gesteld zijn zienswijze kenbaar te maken.
Bij brief van 24 februari 2011 heeft de korpsbeheerder 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 zijn reactie betreffende de geldigheid van de BBNP heeft het CBP een aanpassing in de tekst aangebracht onder 3.1.1. 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

De DNR maakt onderdeel uit het van het Korps Landelijke Politiediensten (KLPD). De CIOT-bevragingen worden op zes locaties[2] uitgevoerd. Voor het onderzoek zijn de locaties Amsterdam en Driebergen bezocht.

[2] Amsterdam, Zwolle, Zoetermeer, Son en Breugel, Woerden en Driebergen.

3 TOEGANG TOT HET CIS DOOR DE DIENST NATIONALE RECHERCHE

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

3.1 Toekenning autorisaties bij de Dienst Nationale Recherche

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) [3], 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[4] 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[5].

Uit bovenstaande volgt dat sprake is van een dubbele autorisatie teneinde de ambtenaar van politie van de DNR toegang te verlenen tot het CIS, namelijk zowel door de beheerder van het korps als door de minister van Justitie[6].

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 beheerder van het KLPD, waaronder de DNR valt, is ingevolge artikel 38 lid 3 Politiewet 1993 de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK)[7]. De toegang tot het CIS impliceert de verwerking van politiegegevens die voortkomen uit de bevraging. Hiervoor dient de ambtenaar van

[3] *Handleiding CIOT InformatieSysteem (CIS 3.1),* Ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie, versie 2.2, augustus 2007.
[4] *Procedure CIS-accounts CIOT informatiesysteem versie 3.1*, Ministerie van Justitie, Centraal Informatiepunt Onderzoek Telecommunicatie, versie 2.0, 11 mei 2007.
[5] Idem, p. 4.
[6] Zoals hierna beschreven onder *B. Norm autorisatie door de minister van Justitie*.
[7] Thans valt, ingevolge de kabinetsformatie en de daaruit volgende portefeuilleverdeling, het korpsbeheerderschap over het KLPD onder de verantwoordelijkheid van de minister van Veiligheid en Justitie. In de wetgeving is daartoe nog de minister van BZK aangewezen.

politie door de 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 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). 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 ook eventueel 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 de DNR ten behoeve van de bevraging van het CIS en de daaruit voortvloeiende verwerking van politiegegevens een formele procedure te zijn vastgesteld[8]. 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

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

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.
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 de DNR ten behoeve van de bevraging van het CIS en de daaruit voortvloeiende verwerking van politiegegevens als volgt is geregeld. Een CIS-autorisatie moet met toestemming van de chef Opsporing of chef Ondersteuning worden aangevraagd bij de functioneel beheerder recherche van de DNR te Zoetermeer. Toestemming voor de aanvraag moet gebaseerd zijn op het systeem van autorisaties van het korps. De functioneel beheerder recherche controleert de aanvraag en stuurt deze aanvraag aan de lokale beheerder van de DNR in Driebergen. De lokale beheerder verzamelt de gegevens die nodig zijn en stuurt de aanvraag ondertekend per e-mail naar het CIOT. Van het CIOT wordt een ontvangstbevestiging ontvangen 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. De werkwijze voor het proces van toekenning van een autorisatie komt overeen met de procedure CIS-accounts van het CIOT, met uitzondering van de door de lokale beheerder uit te voeren controle van de aanvraag, die elders door de functioneel beheerder recherche DNR wordt uitgevoerd.
Voornoemde procedure is door de DNR 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[9]. 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 autoriteit 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 de DNR, 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 de DNR, 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 op basis 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

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

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, inclusief de afmelding van gebruikers die niet langer toegang tot de betreffende informatiesystemen nodig hebben[10]. 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 in Amsterdam heeft de lokale beheerder verklaard dat er 15 medewerkers voor het CIOT-informatiesysteem zijn geautoriseerd. Het CBP heeft van de lokale beheerder per e-mail een autorisatieoverzicht ontvangen van de geregistreerde gebruikers van het CIS. Hierop zijn 14 medewerkers vermeld die over toegang tot het CIS beschikken. De 15de geautoriseerde medewerker is echter niet in het overzicht opgenomen.

Beoordeling
Hoewel een overzicht van toegekende autorisaties voor het CIS is ontvangen blijkt dit niet volledig te zijn, zodat niet is voldaan aan de verplichting zorg te dragen voor de schriftelijke vastlegging van de toekenning van autorisaties. Dit is in strijd met artikel 32 lid 1 onder c Wpg.

B. *Controle op noodzaak verleende autorisaties*
Uit de interviews is gebleken 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

[10] NEN-ISO/IEC 27002:2007, 11.2, p. 70.

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. Er vindt bij de DNR naast de jaarlijkse controle of een certificaat moet worden verlengd geen controle plaats of de geadministreerde medewerkers nog in dienst zijn.

Indien een medewerker de DNR verlaat, van functie wijzigt of de autorisatie niet meer gebruikt, blokkeert de lokale beheerder op verzoek van de chef Opsporing de autorisatie in de applicatie en stuurt de lokale beheerder een fax aan het CIOT met het verzoek om de autorisatie bij het CIOT in te trekken. Na controle wordt het account door het CIOT ingetrokken en wordt via de lokale beheerder de medewerker hiervan schriftelijk op de hoogte gesteld. Deze intern afgesproken werkwijze is door het korps niet in een formele procedure vastgelegd.

Beoordeling
Het CBP constateert op grond van bovenstaande dat de verstrekte accounts jaarlijks worden gecontroleerd als aan het CIOT moet worden gemeld dat een certificaat moet worden verlengd of kan worden ingetrokken. Het CBP stelt voorts vast dat een CIS-account onder bepaalde omstandigheden kan worden ingetrokken en dat het korps hiertoe een intern afgesproken werkwijze gebruikt. Voor het intrekken van een CIS-account blijkt geen formele procedure beschikbaar te zijn.
Het CBP concludeert dan ook dat door het ontbreken van een vastgelegde formele procedure voor de intrekking van autorisaties voor het CIS niet wordt voldaan aan de vereisten die de NEN-norm daaraan stelt[11]. Hiermee wordt in strijd gehandeld met artikel 4 lid 3 j° artikel 6 lid 1 Wpg.

4 Beveiliging van verzending van gegevens door de Dienst Nationale Recherche 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

[11] NEN-ISO/IEC 27002:2007, 11.2.1, p.70.

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[12]. De NEN-norm[13] 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[14].

4.3 Bevindingen

Bevindingen
De vorderingen van gegevens door de DNR bij de telecommunicatieaanbieders kunnen betrekking hebben op het alsnog opvragen van gebruikersgegevens na een 'no-hit'-melding door het CIOT op vordering van een opsporingsambtenaar[15] dan wel de officier van justitie[16] 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 waarop het onderzoek betrekking heeft. De combinatie van bijvoorbeeld identificerende gegevens met gegevens van een misdrijf levert gevoelige gegevens[17] 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 intern afgesproken procedure wordt gevolgd. De procedure voor 'no-hit'-bevragingen en overige vorderingen op verzoek van de officier van justitie verloopt als volgt.
Indien de uitkomst van een bevraging bij het CIOT een 'no-hit' betreft, wordt het 'no-hit-bericht' door de infodesk aan de aanvrager van de DNR gestuurd. In het onderzoeksteam wordt vervolgens besloten of een 'no-hit'-procedure wordt opgestart. Hiervan is sprake indien het onderzoeksteam het telefoonnummer in het kader van het onderzoek van belang vindt. De aanvrager achterhaalt eerst via de OPTA welke

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

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

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

[15] In geval van verdenking van een misdrijf.

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

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

provider bij het desbetreffende telefoonnummer hoort. De aanvrager bericht de infodesk dat de 'no-hit' bij de achterhaalde provider moet worden nagevraagd. De 'no-hit' wordt per fax bij de provider aangevraagd. De fax wordt over een openbare telefoonlijn aan de telecommunicatieaanbieder verzonden zonder additionele beveiligingsmaatregelen. De overige vorderingen op last van de officier van justitie worden eveneens per fax over een openbare telefoonlijn zonder beveiliging verzonden. Het ontvangen antwoord van de provider wordt door de infodesk per e-mail aan de aanvrager via het interne netwerk, dat wel beveiligd is, gestuurd.

Beoordeling
Uit het onderzoek is gebleken dat de 'no-hit'-faxen en overige vorderingen in het kader van strafvordering door de DNR via een openbare telefoonlijn zonder beveiliging worden verzonden aan 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[18]. Aangezien hier sprake is van verzending van gevoelige gegevens, betreffende vorderingen in het kader van strafvordering, is het CBP van oordeel dat de DNR 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.

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 drie onderzoeken ter plaatse plaatsgevonden, te weten op 8 maart 2010, 6 april 2010 en aanvullend op 9 november 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

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

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[19] 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 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

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

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 uit een overzicht van CIOT-bevragingen in het CIS met behulp van de lokale beheerder een selectie gemaakt van bevragingen. Het betrof bevragingen met verschillende rechtsgrondslagen. Tijdens de uitvoering van het dossieronderzoek bij het eerste onderzoek ter plaatse is nog een bevraging geselecteerd, niet vanuit het CIOT-overzichtsscherm maar vanuit de Basisvoorziening Opsporing (BVO). Deze bevragingen zijn in de samenvatting en in de bijlage aangeduid met A1 tot en met A7. Het geselecteerde dossier A1 bleek twee CIOT-bevragingen te bevatten. Deze zijn als A1a en A1b weergegeven. In een derde onderzoek ter plaatse zijn aanvullend nog drie bevragingen geselecteerd uit dezelfde periode als de eerste selectie. Deze bevragingen zijn hierna aangeduid met B1 tot en met B3.

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 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 vrijwel geen enkel dossier direct compleet is aangeleverd. Het achterhalen van de bijbehorende documentatie werd voor een groot deel van de dossiers uitgevoerd vanuit de BVO, maar dit leverde voor een aantal dossiers niet de benodigde informatie op. De aangeleverde documentatie was veelal onduidelijk en

het vereiste veel uitzoekwerk om alleen al te kunnen vaststellen welke informatie nog ontbrak. Vervolgens werd de aanvullende documentatie uitgezocht en nageleverd, waarvoor in een enkel geval nog een nazending per e-mail nodig was.

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 van de beoordeling.

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 twee bevragingen (bevraging A2 en A4) aan de eerder genoemde vereisten waaraan is getoetst en deze zijn daarmee in overeenstemming met artikel 3 lid 2 Wpg.
De overige negen bevragingen zijn in strijd met artikel 3 lid 2 Wpg. Twee daarvan (bevraging A1a en A1b) omdat geen verband was vast te stellen tussen de bevraagde gegevens en het daarbij gebruikte referentienummer enerzijds en de vereiste vordering en aanvraagproces-verbaal met het daarbij vermelde referentienummer anderzijds. Vier andere bevragingen (A3, A6, B1 en B2) omdat niet kon worden vastgesteld welke gegevens feitelijk waren bevraagd, zodat het verband met het dossier niet kon worden vastgesteld. Een volgende bevraging (A5) omdat zowel de vordering door de officier van justitie als een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbraken. Een andere bevraging (A7) omdat geen verband kon worden vastgesteld tussen de bevraagde gegevens en de vereiste vordering en aanvraagproces-verbaal en ook niet kon worden vastgesteld wanneer de bevraging precies had plaatsgevonden en op welke rechtsgrondslag. Tenslotte een bevraging (B3) omdat het vereiste aanvraagproces-verbaal ontbrak.
Dit leidt tot de conclusie dat de DNR zich voor negen 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 de DNR tot de volgende conclusies.

Ten aanzien van toekenning van autorisaties bij de DNR:

- Uit het onderzoek is gebleken dat een vastgelegde formele procedure voor het toekennen van autorisaties door de korpsbeheerder aan medewerkers van de DNR 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 Wpg j° artikel 4 lid 3 Wpg.
- Het CBP stelt vast dat de autorisaties van de bevoegde autoriteiten, i.c. de medewerkers van de DNR, 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 de DNR, 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 is door de DNR een autorisatieoverzicht van de toegekende autorisaties tot het CIS overgelegd. Dit autorisatieoverzicht was niet volledig zodat niet is voldaan aan de verplichting zorg te dragen voor de schriftelijke vastlegging van de toekenning van autorisaties. Dit is in strijd met artikel 32 lid 1 onder c Wpg.
- Uit het onderzoek is gebleken dat het intrekken van autorisaties van medewerkers van de DNR voor het CIS niet is vastgelegd in een formele procedure. Derhalve wordt niet voldaan aan de vereisten die de NEN-norm op dit punt stelt en 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 de DNR aan de telecommunicatieaanbieders:

- De verzending van zogeheten 'no-hit'-faxen en van overige vorderingen van de officier van justitie 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 twee bevragingen voor zover onderzocht in overeenstemming met artikel 3 lid 2 Wpg.
- Negen bevragingen zijn in strijd met artikel 3 lid 2 Wpg. In twee gevallen omdat geen verband was vast te stellen tussen de bevraagde gegevens en het daarbij gebruikte referentienummer enerzijds en de vereiste vordering en aanvraagproces-verbaal met het daarbij vermelde referentienummer anderzijds. In vier gevallen omdat niet kon worden vastgesteld welke gegevens feitelijk waren bevraagd, zodat het verband met het dossier niet kon worden vastgesteld. In een volgend geval omdat zowel de vordering door de officier van justitie als een aanvraagproces-verbaal dat betrekking had op de bevraagde gegevens ontbraken. In een ander geval omdat geen verband kon worden vastgesteld tussen de bevraagde gegevens en de vereiste vordering en aanvraagproces-verbaal en ook niet kon worden vastgesteld wanneer de bevraging precies had plaatsgevonden en op welke rechtsgrondslag. Tenslotte een geval waarin het vereiste aanvraagproces-verbaal ontbrak.
  Dit leidt tot de conclusie dat de DNR zich voor negen 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 het rapport van het CIOT-onderzoek bij de Dienst Nationale Recherche

Bespreking per dossier

Bevraging A1 is uitgevoerd in 2010 op grond van artikel 126n WvSv, op vordering van de officier van justitie. Uit het onderzoeksdossier blijkt dat op die datum twee bevragingen hebben plaatsgevonden onder de referentie van hetzelfde parketnummer, die hierna worden aangeduid als A**1a** en A**1b**.
Bevraging A**1a** betreft een telefoonnummer dat naar voren is gekomen uit een al lopende telefoontap in het onderzoek en betreft een nummer waarmee het getapte nummer contact had. De combivordering artikel 126m/n WvSv ten aanzien van het getapte nummer is 15 dagen voor de bevraging gedateerd en heeft ook betrekking op nummers waarmee het getapte nummer contact heeft. Het bij de bevraging vermelde parketnummer blijkt niet te behoren bij de verdachte op wiens naam de telefoontap is uitgevoerd, maar blijkt het parketnummer van een medeverdachte uit het onderzoek te zijn.
Bevraging A**1b** betreft eveneens een telefoonnummer dat naar voren is gekomen uit een al lopende telefoontap in het onderzoek en betreft een nummer waarmee het getapte nummer contact had. De combivordering artikel 126m/n WvSv is 20 dagen voor de bevraging gedateerd en heeft ook betrekking op nummers waarmee het getapte nummer contact heeft. Het bij de bevraging vermelde parketnummer blijkt niet te behoren bij de verdachte op wiens naam de telefoontap is uitgevoerd, maar blijkt het parketnummer van een medeverdachte uit het onderzoek te zijn.

Beoordeling
Bij **Bevraging A1a** en **Bevraging A1b** is een onjuist parketnummer als referentie bij de CIOT-bevraging vermeld; het betrof hier parketnummers van (twee verschillende) medeverdachten in het onderzoek. Omdat hierbij geen verband was vast te stellen tussen de bevraagde gegevens en het daarbij gebruikte referentienummer enerzijds en de vereiste vordering en aanvraagproces-verbaal met het daarbij vermelde referentienummer anderzijds, is niet voldaan aan de door het CBP onderzochte vereisten. De bevragingen zijn in zoverre in strijd 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. De bevraagde gegevens betreffen een zogenaamde bulkbevraging, waarbij een groot aantal telefoonnummers is bevraagd die als contacten naar voren komen uit een al lopende telefoontap in het onderzoek. Naar aanleiding van deze telefoontap is een combivordering artikel 126m/n WvSv 22 dagen voor de bevraging verleend, waarin tevens gevorderd wordt om alle telefoonnummers waarmee het getapte nummer contact heeft bij het CIOT te bevragen.

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 uitgevoerd in 2009 op grond van artikel 126na WvSv door een opsporingsambtenaar. Uit de stukken blijkt niet welke gegevens zijn bevraagd, alleen dat twee vragen zijn gesteld, waarop twee antwoorden zijn ontvangen. Een aanvraagmutatie in BVO van dezelfde datum omschrijft een vordering op grond van artikel 126nd WvSv tot het bevragen van de nummers die hebben gebeld naar twee genoemde telefoonnummers. Bij de stukken bevindt zich een

combivordering artikel 126m/n WvSv, gedateerd drie weken voor de CIOT-bevraging, die tevens betrekking heeft op uit te voeren CIOT-bevragingen en de gegevens waarmee de getapte telefoonnummers contact hebben gehad. Uit een getoond tapverslag dat hierop betrekking heeft, blijkt dat contact is geweest is met twee telefoonnummers. De betrokken medewerkers van DNR hebben gesteld dat het, gelet op het overeenkomende mutatienummer in BVO en het bij de bevraging vermelde nummer, aannemelijk is dat de twee bevraagde nummers dezelfde zijn als de twee nummers die in de BVO-mutatie zijn genoemd.

Beoordeling
Uit het onderzoek naar **Bevraging A3** kon niet worden vastgesteld dat de in de getoonde stukken vermelde telefoonnummers dezelfde waren als de bij het CIOT bevraagde nummers. Omdat niet kon worden vastgesteld welke gegevens feitelijk waren bevraagd, kon het verband daarvan met het dossier niet worden vastgesteld. Hierdoor is niet voldaan aan de door het CBP onderzochte vereisten. De bevraging is in zoverre in strijd met artikel 3 lid 2 Wpg.

Bevraging A4 is uitgevoerd in 2009 op grond van artikel 126na WvSv door een opsporingsambtenaar. Eén telefoonnummer is bevraagd. Als onderliggende stukken werd getoond een BVO-mutatie die betrekking had op de telefoontap van een ander nummer in het onderzoek, waarvoor zes dagen vóór de bevraging een combivordering artikel 126 m/n WvSv was afgegeven. Aanvankelijk bleek het verband niet tussen het bevraagde nummer en het nummer waarop de telefoontap liep. Na navraag is een tapverslag getoond waaruit het bevraagde nummer naar voren komt. Een proces-verbaal van aanvraag verstrekking gebruikersgegevens is door de opsporingsambtenaar opgemaakt op dezelfde dag als de bevraging.

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 126u WvSv, op vordering van de officier van justitie. Er zijn 30 vragen gesteld aan het CIOT. Een proces-verbaal aanvraag verstrekking gebruikersgegevens is door een opsporingsambtenaar opgemaakt op dezelfde dag als de bevraging. Hierin wordt melding gemaakt van een aantal verdachten. Aanvankelijk is niet duidelijk welke gegevens zijn bevraagd en wat het verband daarvan is met deze verdachten. Na navraag is een aantal stukken getoond dat betrekking heeft op de genoemde verdachten en daarnaast een mutatie in BVO waaruit de bevraagde gegevens blijken alsmede het verband met deze verdachten. Een vordering door de officier van justitie ontbreekt, evenals een aanvraagproces-verbaal met vermelding van de bevraagde gegevens.

Beoordeling
Van **Bevraging A5** zijn de bevraagde gegevens niet terug te vinden in een proces-verbaal van aanvraag, terwijl een vordering door de officier van justitie ontbreekt, zodat in zoverre niet is voldaan aan de door het CBP onderzochte vereisten en de bevraging op dat punt in strijd is met artikel 3 lid 2 Wpg.

Bevraging A6 is uitgevoerd in 2009 op grond van artikel 126n WvSv, op vordering van de officier van justitie. Aanvankelijk zijn de bijbehorende stukken niet in BVO terug te vinden. Na nalevering van stukken blijkt dat aan het CIOT bij deze bevraging 17 vragen zijn gesteld, maar er is geen informatie beschikbaar welke gegevens zijn bevraagd. Aan de hand van het mutatienummer in BVO wordt een proces-verbaal van de start van het onderzoek getoond, gedateerd 9 weken vóór de

onderzochte bevraging. Een tapbevel alsmede een combivordering artikel 126u/t WvSv is afgegeven een week na start van het onderzoek, maar kan niet in verband worden gebracht met de bevraagde gegevens.

Beoordeling
Bij **Bevraging A6** verwees het vermelde referentienummer naar een dossier waarin informatie over de bevraagde gegevens ontbrak. Omdat niet kon worden vastgesteld welke gegevens feitelijk waren bevraagd, kon het verband daarvan met het dossier niet worden vastgesteld. Hierdoor is niet voldaan aan de door het CBP onderzochte vereisten. De bevraging is in zoverre in strijd met artikel 3 lid 2 Wpg.

Bevraging A7 is uitgevoerd in 2009. Aangezien deze bevraging vanuit de BVO was geselecteerd, waren de exacte gegevens ten aanzien van datum, rechtsgrondslag en referentienummer uit het CIOT-overzicht van uitgevoerde bevragingen niet bekend. In BVO bevond zich een mutatie die melding maakt van de bevraging van één telefoonnummer onder vermelding van een parketnummer en de bevraging van dat nummer op grond van artikel 126n WvSv, op vordering van de officier van justitie. Ook na het tweede onderzoek ter plaatse en na aanvullende informatie van het korps daarover per e-mail, konden de gegevens ten aanzien van bevragingsdatum, rechtsgrondslag en referentienummer niet worden vastgesteld. In de aanvullende informatie stelt DNR dat niet met zekerheid is vast te stellen dat de bevraging is uitgevoerd op de datum die volgt uit de informatie in BVO. Dit lijkt DNR wel aannemelijk omdat op die datum een zogenaamde bulkbevraging is gedaan met als referentie een ander parketnummer dat tot een overkoepelend onderzoek behoort. Als grondslag voor het bevraagde nummer wordt een tapverslag getoond van een al lopende telefoontap in de zaak met het betreffende parketnummer, waaruit volgt dat door één van de verdachten het bevraagde nummer wordt genoemd. Dit verslag dateert echter van een week na de vermoedelijke bevragingsdatum, terwijl volgens een medewerker van het onderzoeksteam pas hieruit het te bevragen nummer bekend werd.

Beoordeling
Bij **Bevraging A7** bleken de gegevens ten aanzien van de rechtsgrondslag, de datum van bevraging en het parketnummer feitelijk niet aanwezig. Omdat geen verband kon worden vastgesteld tussen de bevraagde gegevens en de vereiste vordering en aanvraagproces-verbaal en ook niet kon worden vastgesteld wanneer de bevraging precies had plaatsgevonden en onder welke rechtsgrondslag, is hierdoor niet voldaan aan de door het CBP onderzochte vereisten. De bevraging is in zoverre in strijd met artikel 3 lid 2 Wpg.

Bevraging B1 is uitgevoerd in 2009 op grond van artikel 126ua WvSv door een opsporingsambtenaar en heeft betrekking op vier bevraagde gegevens. Ingezien is een proces-verbaal van aanvraag, opgemaakt op de datum van de bevraging door de opsporingsambtenaar. Het proces-verbaal is geregistreerd onder één van de twee nummers die in de bevraging als referentienummer zijn opgenomen en vermeldt als grondslag artikel 126ua Sv. Hierin is gerelateerd dat uit de informatie van het onderzoek vier mobiele telefoonnummers zijn gebleken, die vervolgens bij het CIOT zijn bevraagd. Een CIOT-afdruk van de bevraagde gegevens is niet beschikbaar.

Beoordeling
Omdat in het onderzoek naar **Bevraging B1** niet kon worden vastgesteld welke gegevens feitelijk bij het CIOT zijn bevraagd, kon het verband tussen de bevraagde gegevens en het desbetreffende referentienummer niet worden vastgesteld en is niet voldaan aan de door het CBP onderzochte vereisten. De bevraging is 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 CIOT-afdruk van de bevraagde gegevens is niet beschikbaar. Een BVO-mutatie, gedateerd op de bevragingsdatum en met een registratienummer dat overeenkomt met het referentienummer van de bevraging, vermeldt dat drie dagen voordien een bepaald telefoonnummer naar voren is gekomen uit een in het onderzoek lopende telefoontap. Na navraag bij de medewerkers van het onderzoeksteam is een combivordering artikel 126m/n WvSv getoond, afgegeven door de officier van justitie 6 dagen voor de uitvoering van de bevraging, met vermelding van een parketnummer dat niet overeenkomt met het bij de bevraging vermelde referentienummer. Ook is getoond een proces-verbaal van aanvraag vordering artikel 126m/n WvSv, gedateerd de dag vóór de afgegeven vordering, met betrekking tot een aan te vragen telefoontap en bevraging van het CIOT in dat verband.

Beoordeling

In het onderzoek naar **Bevraging B2** kon niet worden vastgesteld welke gegevens feitelijk bij het CIOT zijn bevraagd, zodat het verband tussen de bevraagde gegevens en het desbetreffende referentienummer niet kon worden vastgesteld en is niet voldaan aan de door het CBP onderzochte vereisten. De bevraging is in zoverre in strijd met artikel 3 lid 2 Wpg.

Bevraging B3 is uitgevoerd in 2009 op grond van artikel 126n WvSv door de officier van justitie en heeft betrekking op één bevraagd nummer. In BVO bevindt zich een mutatie van de datum van de bevraging en met een registratienummer dat overeenkomt met het bij de bevraging vermelde referentienummer, waarin vermeld is dat uit een lopende telefoontap drie telefoonnummers zijn gebleken waarvan er één nummer bij het CIOT is bevraagd.
Na navraag bij de medewerkers van het onderzoeksteam is een CIOT-afdruk nagezonden waaruit het bevraagde telefoonnummer blijkt en de daaraan ten grondslag liggende combivordering artikel 126m/n Sv, opgemaakt op de dag na de bevraging door de officier van justitie. Het bevraagde nummer heeft betrekking op het nummer waarop de telefoontap is aangevraagd. Het bijbehorende proces-verbaal van aanvraag ontbreekt echter en is ook niet nagezonden nadat daartoe aan de DNR de gelegenheid was geboden.

Beoordeling

Van **Bevraging B3** ontbrak het vereiste proces-verbaal van aanvraag, zodat in zoverre niet is voldaan aan de door het CBP onderzochte vereisten en de bevraging op dat punt in strijd is met artikel 3 lid 2 Wpg.

** ** **