Ministerie van Veiligheid en Justitie

Postbus 20011 2500 EA Den Haag

de Voorzitter van de Tweede Kamer der Staten Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-generaal Veiligheid
Bestuur en Organisatie

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.minbzk.nl

Kenmerk
2011-0000072466

Datum 17 maart 2011
Betreft Naleving voorschriften bevragingen via CIOT

Samenvatting
De afgelopen jaren is er steeds aandacht geweest voor de juiste naleving van voorschriften rond bevragingen van identificerende gegevens via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Er zijn verbeteringen aangebracht door (bijzondere) opsporings-, inlichtingen en veiligheidsdiensten (hierna BOID-en). Toch zijn er ook signalen dat nog niet alle BOID-en alle waarborgen in acht nemen bij bevragingen. Strikte naleving is echter vereist. Daarom zijn aanvullende maatregelen getroffen waarover ik u wil informeren. Voorbeelden van maatregelen zijn het aanschrijven van verantwoordelijken voor de naleving, het stellen van een uiterste termijn waarbinnen aan de vereisten moet worden voldaan en intensivering van de controle op naleving van de voorschriften. Ik hecht eraan u nu te informeren omdat ik de situatie urgent acht, van oordeel ben over voldoende informatie te beschikken om passende maatregelen te treffen en u een actueel totaalbeeld van de materie wil geven.

1. CIOT

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is een instantie van het ministerie van Veiligheid en Justitie die in 2002 is opgericht. Het CIOT is opgericht om administratieve lasten van (bijzondere) opsporings-, inlichtingen en veiligheidsdiensten(hierna BOID-en) en de aanbieders van telecommunicatiediensten en –netwerken (hierna: telecomaanbieders) te verminderen. Een opsporingsambtenaar kan op grond van artikel 126na van het Wetboek van Strafvordering in geval van verdenking van een misdrijf en in het belang van het onderzoek een vordering doen aan een telecomaanbieder om de naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst (hierna: naw-gegevens) te verstrekken[1]. Tot 2002 werd iedere vordering door een

[1] *Behalve voor strafvorderlijke doeleinden kan de verstrekking van naw-gegevens ook gevorderd worden voor hulpverlening in noodsituaties door opsporingsdiensten. Daarnaast kunnen de inlichtingen- en veiligheidsdiensten de verstrekking van gegevens vorderen ten*

opsporingsambtenaar afzonderlijk gericht aan een telecomaanbieder. Dit leidde tot veel administratieve handelingen en hoge kosten bij de telecomaanbieders en bij BOID-en. Sinds 2002 verstrekken telecomaanbieders iedere dag hun naw-gegevens aan het CIOT. Deze gegevens worden door het CIOT 24 uur bewaard en vervolgens vernietigd. De gegevens zijn geplaatst in het CIOT Informatiesysteem. Een beperkt aantal opsporingsambtenaren per organisatie hebben een autorisatie tot dit systeem en kunnen de naw-gegevens opvragen conform de bevoegdheden van artikel 126na van het Wetboek van Strafvordering en de voorschriften van het Besluit verstrekking gegevens telecommunicatie (Besluit CIOT).

2. Normenkader

Voor het CIOT, de aanvragende organisatie en voor de telecomaanbieders zijn normen van toepassing. Deze normen zijn vastgelegd in wet- en regelgeving, in Service Level Agreements en in nadere kaders, zoals de "Blauwdruk bevragingen via het CIOT" en de "Referentie procesbeschrijving bevraging met behulp van CIOT". Hierin zijn onder meer minimaal in acht te nemen beheersingsmaatregelen opgenomen. Deze normen vormen het toetsingskader voor de Departementale Auditdienst (DAD) van mijn ministerie. In het Besluit CIOT is vastgelegd dat de DAD jaarlijks een audit uitvoert naar de naleving van de voorschriften bij de bevragingen via het CIOT.
Ik vind strikte naleving van deze normen van groot belang, omdat daarmee inbreuken op de persoonlijke levenssfeer die plaatsvinden in het kader van opsporingsonderzoeken en inlichtingen- en veiligheid met voldoende waarborgen worden omgeven. Om deze reden verwelkom ik de bijdrage die het College bescherming persoonsgegevens (Cbp) als toezichthouder hieraan levert.

3. Audits

In 2007 en in 2008 zijn door de DAD audits uitgevoerd bij een aantal BOID-en[2]. In de audits is onder meer gekeken naar de rechtmatigheid van de bevragingen die door de BOID-en worden gedaan. Daarbij is geconstateerd dat er, wisselend per BOID, onvolkomenheden zijn in het proces van bevraging. In een enkel geval kon de rechtmatigheid van een bevraging niet worden vastgesteld. In de auditrapportages zijn voorstellen gedaan voor verbetering van het bevragingsproces. In 2009 is een *follow-up* uitgevoerd naar de opvolging van de aanbevelingen uit de audit 2008. Uit de resultaten van deze *follow-up* audit blijkt dat de belangrijkste punten waarover de aanbevelingen zijn gedaan betreffen het delegeren van bevoegdheden, formele autorisaties, de rechtsgrondslagen en de rechtmatigheid van bevragingen en de documentatie van de werkwijze en de instructie. Bij de *follow-up* audit is geconstateerd dat de situatie in 2009 nog voor het overgrote deel ongewijzigd was.

---

behoeve van inlichtingenverzameling. Ik zal geen nadere toelichting geven op vordering van verstrekking van gegevens door inlichtingen- en veiligheidsdiensten.

[2] *In deze brief zal ik geen nadere toelichting geven op de naleving van de voorschriften bij bevragingen via het CIOT door inlichtingen- en veiligheidsdiensten.*

Deze bevindingen hebben ertoe geleid dat de toenmalige ministers van Justitie en Binnenlandse Zaken en Koninkrijksrelaties in 2010 brieven hebben gestuurd aan de verantwoordelijken voor de naleving van de voorschriften, zoals de korpsbeheerders van de regiokorpsen. Door middel van deze brieven zijn partijen geïnformeerd over de in audits geconstateerde tekortkomingen bij het opvragen van gegevens via het CIOT. Daarbij is gevraagd om te toetsen of het proces van bevragingen via het CIOT voldoet aan de normen die zijn gesteld in wet- en regelgeving en de afspraken met het CIOT. Meer in het bijzonder is aandacht gevraagd voor het delegeren van bevoegdheden, de formele autorisatie, de rechtmatigheid van bevragingen, de documentatie van de werkwijze en de instructie. In de gevallen dat niet aan deze normen wordt voldaan, is gevraagd een verbeterplan op te stellen teneinde de tekortkomingen weg te nemen. Vanuit het ministerie van Veiligheid en Justitie is ondersteuning aangeboden voor het opstellen van een verbeterplan.

4. Reacties op verzoek

Van alle BOID-en is een reactie ontvangen op genoemde verzoeken. Een aantal BOID-en heeft een "in control verklaring" gegeven. Dat betekent dat zij hebben aangegeven te voldoen aan alle regels. Een ander deel van de BOID-en heeft te kennen gegeven aan verbeteringen te werken. De meeste van deze BOID-en hebben gesteld de zaken uiterlijk januari 2011 op orde te hebben. Een beperkt aantal BOID-en stelde op een tijdstip na 1 januari 2011 in control te zijn, omdat zij, volgens eigen opgave, meer tijd nodig hebben voor het realiseren van het verbeterplan.
Er kan gesteld worden dat er over het geheel genomen door de BOID-en aandacht aan het onderwerp is besteed en er daadwerkelijk verbeteringen zijn aangebracht, of in uitvoering zijn.

5. Review

Eind 2010 is door de DAD een *review* gehouden bij drie van de BOID-en die hadden aangegeven "in control" te zijn. Het betrof de politiekorpsen Gelderland-Zuid en Friesland en de Fiscale Inlichtingen en Opsporingsdienst (FIOD). Het doel van de *review* was om steekproefsgewijs na te gaan of betreffende BOID inderdaad volgens alle voorschriften handelde. Politiekorps Friesland en de FIOD bleken conform de normen te handelen, terwijl bij het politiekorps Gelderland-Zuid bleek dat niet alles volgens de normen was ingericht. Het korps Gelderland Zuid heeft een verbeterplan opgesteld en toegezegd de verbeteringen uit te voeren.
De leden van de vaste commissies voor de JBZ-Raad en voor Justitie van de Eerste Kamer hebben mij gevraagd geïnformeerd te worden over de uitkomsten van deze *review*.

6. Onderzoek door College bescherming persoonsgegevens (Cbp)

In 2010 heeft het Cbp, in het kader van de toezichthoudende taak, ambtshalve onderzoek verricht naar de naleving van de voorschriften bij bevragingen via het CIOT. Er is onderzoek gedaan bij het CIOT en bij twee politiekorpsen, namelijk het politiekorps Haaglanden en de Dienst Nationale Recherche (DNR), onderdeel van

het Korps Landelijke Politiediensten (KLPD). Onderzocht is onder meer de rechtmatigheid van bevragingen via het CIOT en de autorisaties van opsporingsambtenaren voor de toegang tot het informatiesysteem van het CIOT. Het feitelijke onderzoek bij het CIOT vond plaats in februari 2010, en bij de politiekorpsen in maart, april en november 2010. Per onderzochte organisatie is een rapport met voorlopige bevindingen opgesteld. In december 2010 heeft het Cbp drie rapporten met voorlopige bevindingen aan betreffende organisaties aangeboden. Het Cbp heeft tot 1 maart 2011 de tijd gegeven om schriftelijk te reageren op de voorlopige bevindingen. Voor die datum hebben de drie organisaties hun reacties aan het Cbp gestuurd. In de volgende fase zal het Cbp de reacties bestuderen, de rapporten afronden en vervolgens publiceren.
Ik wil benadrukken dat ik grote waardering heb voor de bijdrage die het Cbp als toezichthouder hieraan levert.
Het beeld dat uit de reacties van de onderzochte organisaties naar voren komt is dat strikte naleving van de voorschriften, ondanks goede intenties, nog steeds niet voldoende is geborgd. Omissies en gebreken waren bijvoorbeeld dat de politiekorpsen de procedures voor het toekennen of intrekken van autorisaties niet formeel hadden vastgelegd, dat de werkwijze het bemoeilijkte om de grondslag van de bevragingen terug te vinden en dat de autorisatieverlening door het CIOT formeel niet was afgedekt. Door mij en betreffende organisaties zijn onmiddellijk acties ondernomen om omissies en gebreken te herstellen of op korte termijn in orde te brengen.

7. Urgentie

Hiervoor heb ik een aantal positieve en een aantal negatieve kanttekeningen gemaakt bij de bestaande praktijk rondom waarborgen bij het maken van inbreuken op de persoonlijke levenssfeer. De voorschriften voor de bevragingen via CIOT zijn vastgesteld als waarborgen voor de bescherming van de privacy van burgers. Ik vind de bescherming van de privacy van burgers van dermate groot belang dat ik met hoge urgentie, op basis van de hiervoor genoemde negatieve kanttekeningen, een aantal maatregelen heb getroffen. Ik ben van mening dat ik thans over voldoende informatie beschik om een aantal relevante acties uit te kunnen voeren en ik acht het niet verantwoord te wachten met het treffen van maatregelen tot het moment het Cbp de onderzoeksrapporten publiceert. De burger moet erop kunnen vertrouwen dat de overheid alles in het werk stelt om tekortkomingen te herstellen, zeker als de bescherming van de persoonlijke levensfeer van de burger in het geding is.
Overigens is er onlangs ook een verzoek om openbaarmaking van stukken over dit dossier bij mij ingediend. Dit verzoek is momenteel nog in behandeling.

8. No-hit bevragingen

Naast bevragingen via het CIOT worden door BOID-en onder meer ook naw-gegevens rechtstreeks bij telecomaanbieders gevraagd. Veel van deze vragen naar naw-gegevens zijn het gevolg van een "no-hit"-melding door het CIOT systeem. Wanneer sprake is van een "no-hit" heeft de bevraging via het CIOT geen resultaat

opgeleverd. Een "no-hit" kan het gevolg zijn van het feit dat het CIOT alleen actuele gegevens (maximaal 24 uur oud) kan verstrekken.
Door het Cbp is de veiligheid aangekaart van verbindingen die worden gebruikt bij deze bevragingen buiten het CIOT om. Hierbij wordt gebruik gemaakt van faxen.
De Wet bescherming persoonsgegevens (Wbp) en de Wet politiegegevens (Wpg) stellen dat passende technische en organisatorische maatregelen moeten worden getroffen bij verzending van gegevens. Bij de beoordeling wat passend is, spelen veel factoren een rol, zoals de mate van gevoeligheid van de gegevens, het risico in de praktijk van onrechtmatig verwerking of verlies van gegevens via het gebruikte middel, de stand van de techniek en de haalbaarheid van de maatregelen. Deze factoren dienen tegen elkaar te worden afgewogen.
Een belangrijk risico bij faxen betreft fouten bij het menselijk handelen, zoals het intikken van het verkeerde nummer, waardoor de fax niet bij de juiste persoon of instantie uitkomt. Dit risico kan worden beperkt door middel van maatregelen, zoals het gebruik van voorgeprogrammeerde nummers. Een ander aandachtspunt is de omgeving waarin de fax staat. In dit verband kunnen risicobeperkende maatregelen bestaan uit het beveiligen van de ruimte of het verlenen van beperkte toegang tot de ruimte waar de fax staat. Bij mij bestaat de indruk dat er bij de BOID-en voldoende aandacht is voor dergelijke risico's.
Onrechtmatige verwerking (tappen of wijzigen) van informatie bij het gebruik van faxen acht ik niet waarschijnlijk, mede gelet op beveiligingsmaatregelen die telecomaanbieders in Nederland rond hun infrastructuur hebben getroffen.
Ik ben van mening dat beveiligingsmaatregelen getroffen moeten worden waar daar aanleiding toe is en waar dat redelijkerwijs kan: de praktische aspecten en (financiële) consequenties van beveiliging moeten daarbij niet uit het oog worden verloren.

9. Maatregelen

Gelet op de hiervoor genoemde negatieve signalen heb ik, naast de hiervoor genoemde specifieke acties betreffende het CIOT en de DNR:

a. een hernieuwd beroep gedaan op de korpsbeheerders en verantwoordelijken voor andere BOID-en om aandacht te besteden aan de naleving van voorschriften bij bevragingen via het CIOT. Zij hebben hierover een brief ontvangen.
b. Daarnaast heb ik een uiterste termijn vastgesteld waarbinnen BOID-en aan alle vereisten rond bevragingen via het CIOT moeten voldoen. Door mij wordt 1 mei 2011 een realistische en haalbare datum geacht. Indien een BOID na 1 mei 2011 niet alle vereisten voldoet, zal de toegang tot het systeem van het CIOT voor betreffende BOID tijdelijk worden afgesloten, tot het moment de BOID heeft aangetoond wel aan de eisen te voldoen. Betreffende BOID zal gedurende de periode dat de toegang tot het systeem van het CIOT is afgesloten gebruik kunnen maken van de voorzieningen bij andere BOID-en die wel toegang hebben. Het opsporingsbelang komt daardoor niet in het geding.
c. De controle op de naleving van de voorschriften zal worden geïntensiveerd: tussen 1 mei en 1 juli 2011, zal een zestal quick scans worden uitgevoerd bij BOID-en. Indien er bij deze quick scans tekortkomingen worden geconstateerd,

dan zal dat direct leiden tot (tijdelijke) afsluiting van de toegang van betreffende BOID tot het systeem van het CIOT.

d. De korpschef van het Korps Landelijke Politiediensten (KLPD) zal, namens de BOID-en, voor 1 april 2011 een haalbaarheidsstudie uitvoeren naar technische en organisatorische maatregelen ter verdere beveiliging van verzoeken om naw- gegevens die aan telecomaanbieders worden verzonden. Onderzocht zal worden of het wenselijk is om deze verzoeken van de BOID-en in de toekomst alleen via de Unit Landelijke Interceptie van het KLPD te verzenden. Deze centralisatie komt de beheersbaarheid ten goede. Tot slot zal onderzocht worden of het aantal no-hit bevragingen gereduceerd kan worden.

De Minister van Veiligheid en Justitie,

I.W. Opstelten