Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2004–2005

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2324

Vragen van het lid **De Wit** (SP) aan de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties over *de bewaarplicht.* (Ingezonden 19 juli 2005)

1
Kunt u de uitspraak bevestigen dat «Wat we [het ministerie van Justitie] willen weten zijn de personalia achter het IP-nummer. En we willen inzicht in alle individuele bewegingen op het internet»?[1]

2
Klopt het dat u en de AIVD anticiperen op de bewaarplicht waartegen recent nog een motie is aangenomen?[2] Baseert u dit op de wens van de Britse regering voor een dergelijke bewaarplicht?[1] Steunt u, in strijd met de hier genoemde motie, de ontwikkeling van een Europese vergaarplicht?

3
Hoe bent u van plan achter de «personalia achter het IP-nummer» te komen? Gaat u daarvoor gebruik maken van uw huidige bevoegdheden onder bijvoorbeeld de Telecommunicatiewet of bent u voornemens daarvoor een systeem op te stellen analoog aan dat van het Centraal Informatiepunt Opsporing Telecommunicatiegegevens (CIOT) waarbij deze wet wordt omzeild door vanaf een server direct te gaan zoeken in de gegevens van de Internet Service Providers (ISP's)?[3]

4
In hoeverre is het gebruik van een eigen server die direct is gekoppeld aan de databestanden van telecommunicatiebedrijven of ISP's voor de vergaring van gegevens in overeenstemming met de Telecommunicatiewet, die stelt dat er toestemming vereist is voor de vergaring van bepaalde gegevens en dat deze met medewerking van de organisaties die ze opgeslagen hebben dient te geschieden? Deelt u de mening dat de Kamer hierover voldoende is ingelicht?

5
Klopt het dat IP-nummers in veel gevallen niet persoonsgebonden zijn, zodat een IP-nummer aan meerdere mensen op dezelfde dag kan zijn toegekend door een ISP? Deelt u de mening dat hierdoor bij de opsporing van iemand die een verdachte handeling heeft gepleegd op het internet onder een bepaald IP nummer, een ander persoon dan de dader als verdachte kan worden aangewezen? Acht u dit aanvaardbaar en zorgvuldig? Wat doet u om dit te voorkomen? Is deze werkwijze transparant voor controle door het ministerie en de Kamer? Kunt u uw antwoord toelichten?

6
Klopt het dat de AIVD de verkeersgegevens wil gebruiken voor datamining, waardoor er zogenaamde «fishing-operations» ontstaan, met andere woorden gegevens van niet-verdachte personen worden gebruikt buiten hun medeweten en toestemming, als ware zij verdachte personen? Klopt het dat dergelijke «fishing-operations» verboden zijn? Klopt het dat u de details van deze plannen nog niet aan de Kamer heeft voorgelegd? Waarom niet?

[1] Fem Business, 16 juli jl.
[2] Kamerstuk 23 490 nummer 372.
[3] Algemeen Dagblad, 15 juli jl.

Antwoord

Antwoord van minister **Donner** (Justitie), mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties. (Ontvangen 6 september 2005)

1
De journalisten van FEM Business hebben contact gehad met de woordvoerder van het ministerie van Justitie. De in het artikel aangehaalde zinnen geven de inhoud van dat gesprek niet volledig weer. De woodvoerder heeft aangegeven dat over de bewaarplicht een discussie wordt gevoerd met de Tweede Kamer en in de Europese Unie en dat de uitkomsten hiervan afgewacht moeten worden. Ter illustratie zijn vervolgens op basis van het rapport van de Erasmus Universiteit enkele

KVR23772
2040518550
0405tkkvr2324
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2005

voorbeelden genoemd van de behoefte van de opsporing.

2
In het debat met de Kamer heb ik steeds aangegeven voorstander te zijn van een bewaarplicht voor telecommunicatiegegevens. Reeds in het BNC fiche betreffende dit onderwerp heb ik aangegeven dat het Nederlandse standpunt ten aanzien van een bewaarplicht voor telecommunicatiegegevens in beginsel positief is, waarbij wel de nodige aandacht dient te worden geschonken aan de wijze waarop deze verplichting wordt ingevuld. Ik heb de motie van de Kamer ook niet zo begrepen dat het principe van de bewaarplicht onaanvaardbaar werd geacht, als wel de wijze waarop hieraan in (eerdere versies van) het Kaderbesluit invulling werd gegeven.

3
Op grond van artikel 126NA van het Wetboek van Strafvordering zijn opsporingsmabtenaren bevoegd identificerende gegevens bij telecommunicatieaanbieders te vorderen. Langs die weg kunnen personalia achter een IP nummer worden gevorderd.
Wat betreft het CIOT merk ik het volgende op.
De werkzaamheden van het CIOT zijn geregeld in het Besluit verstrekking gegevens telecommunicatie[1], een algemene maatregel van bestuur op grond van artikel 13.4 van de Telecommunicatiewet.
Het is daarom onjuist te stellen dat door de werkzaamheden van het CIOT de bepalingen van de Telecommunicatiewet werden omzeild.

4
De verstrekking door de telecommunicatiedienstverleners langs geautomatiseerde weg en doortussenkomst van het CIOT van bepaalde gegevens waarover zij uit hoofde van hun normale bedrijfsvoering beschikken, zoals de naam- en adresgegevens van abonnees, is in overeenstemming met het Besluit verstrekking gegevens telecommunicatie.
Momenteel geldt dit besluit nog niet voor aanbieders van diensten voor internettoegang.
De bedoelde gegevens worden elk etmaal geactualiseerd. Zij blijven eigendom van de aanbieders en vallen ook onder de verantwoordelijkheid van die aanbieders. Het CIOT verzorgt namens de Minster van Justitie de toegang tot deze gegevensbestanden ten behoeve van de behoeftestellers. De aanbieders behoren geen inzicht te hebben in de bevragingen. De bestanden moeten voor deze wijze van onderzoek toegankelijk gemaakt worden. Dat kan op een server van de aanbieders of van het CIOT. Zo nodig wordt bewerkersovereenkomst tussen de aanbieders en het Ministerie van Justitie gesloten.
Op de correctheid van deze bewerkersovereenkomst binnen het wettelijke kader wordt ook door het College bescherming persoonsgegevens toezicht gehouden. Ik deel de mening dat de kamer hierover voldoende is geïnformeerd.

5
In de komende wijziging van het Besluit verstrekking gegevens telecommunicatie zal geen verplichting voor het beschikbaar houden van het dynamische IP-adres opgenomen worden. Alleen als een IP-adres contractueel aan een klant is toebedeeld, zal de aanbieder dit moeten opnemen in het bestand dat middels het CIOT beschikbaar gesteld wordt. Zij zijn dan ook niet beschikbaar voor de bevraging langs geautomatiseerde weg door tussenkomst van het CIOT.
Dynamische IP-adressen zijn uitsluitend nodig voor het tijdelijk tot stand brengen van een sessie van internettoegang, die technisch gesproken niet gekoppeld is aan een specifieke gebruiker om de toegang mogelijk te maken, daarmee is het een verkeersgegeven, dat niet onder de reikwijdte van het CIOT-besluit valt.
Dit betekent niet dat er geen wens bij de opsporingsdiensten is om de dynamische IP-adressen gekoppeld aan een datum en tijd en NAW-gegevens van de gebruiker of abonnee middels het CIOT beschikbaar te krijgen. Voor de opsporing is een accurate registratie van datum en tijd dan van groot belang, omdat een IP-adres inderdaad op dezelfde dag aan verschillende personen kan worden toegewezen. De aanbieders hebben historische gegevens over deze koppeling voor hun bedrijfsvoering vrijwel nooit nodig. Zij bewaren deze gegevens daarom voor een korte tijd. In eventuele strafzaken zal het OM ook aan moeten tonen dat de tijdstippen van gebruik van een bepaald IP-adres correleren met andere de andere gegevens waar het OM haar zaak op baseert. De discussie over het verplicht bewaren van het gebruik van dynamische IP-adressen en het aanleveren van deze gegevens via het CIOT vindt nu plaats in het kader van de Europese initiatieven voor de invoering van een bewaarplicht voor telecommunicatie-verkeersgegevens. Dit is echter niet het doel van de huidige wijziging van het CIOT-besluit.

6
De AIVD komt, evenals de MIVD, op basis van artikel 12 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) in algemene zin de bevoegdheid toe tot het verwerken van gegevens. «Datamining» – opgevat als één van de mogelijke technieken bij het verwerken van gegevens – kan derhalve onder deze bevoegdheid worden begrepen. Het gaat daarbij niet om «fishing operations».
Deze term suggereert dat zonder vooropgezet doel en zonder dat daartoe concrete aanleiding bestaat gegevensbestanden worden doorzocht. Iedere gegevensverwerkende activiteit van de dienst dient conform artikel 12 van de WIV 2002 te geschieden voor een bepaald doel en noodzakelijk te zijn voor een goede taakuitvoering van de diensten. Voorts dient een en ander in overeenstemming met de wet en op zorgvuldige wijze te geschieden. Op de rechtmatige uitvoering van de wet wordt door de onafhankelijke Commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten toegezien.
«Fishing operations» vinden dan ook niet plaats en zouden indien deze wel zouden plaatsvinden niet in overeenstemming met artikel 12 van de wet zijn. Het is evident dat het voor een goede taakuitvoering van de diensten in het kader van onder andere het voorkomen en bestrijden van terroristische activiteiten, het wenselijk is om die gegevens te kunnen verwerken die daaraan kunnen bijdragen. Dat kunnen dus ook verkeersgegevens zijn, zij het dat voor «datamining» men wel over een grote hoeveelheid gegevens dient te beschikken. Op dit moment bestaat voor aanbieders van openbare telecommunicatienetwerken en -diensten overigens slechts de verplichting om ad hoc en in

geïndividualiseerde gevallen deze gegevens te verstrekken. In de brief van 15 juli 2004 van de minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de minister van Defensie, aan de Tweede Kamer betreffende de voorgenomen wijzigingen van onder meer de Wiv 2002[2] is medegedeeld dat de wet meer armslag zou moeten bieden om grote bestanden met persoonsgegevens van niet-verdachte personen te kunnen doorzoeken, omdat dat thans op gespannen voet kan komen met de huidige wettekst. In het wetsvoorstel, waarin de zogeheten «post-Madrid maatregelen» zijn verwerkt wordt dit onderdeel uitgewerkt. Dit wetsvoorstel zal eind dit jaar aan de Tweede Kamer worden aangeboden.

[1] Staatsblad 2000, 71.
[2] Kamerstuken II 2003/2004, 29 200 VII, nr. 61.