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

2321

Vragen van het lid **De Wit** (SP) aan de minister van Justitie over *de voorgestelde bewaarplicht van dataverkeersgegevens.* (Ingezonden 1 september 2005)

1
Bent u bekend met het feit dat de voorgestelde bewaarplicht voor dataverkeersgegevens makkelijk te omzeilen is?[1]

2
Kunt u ingaan op maatregelen als het inloggen op iemand anders zijn draadloze Wlan-netwerk, het gebruiken van een prepaid gsm, het chatten buiten Europa, het gebruiken van de eigen server met een eigen versleutelde inhoud, het inbellen naar een land waar internetverkeer niet wordt gemonitord, het verklaren van mail-verkeer als een besloten netwerk, het gebruiken van een anonymous en versleutelde proxy, het gebruiken van Tor, dat fungeert als een Proxy en internetverzoeken langs veel verschillende computers routeert, het gebruiken van het open-sourceproject Freenet dat de informatie en de ontvanger beschermt, en het gebruik van een versleutelde tunnel om een verbinding ver buiten Europa tot stand te brengen?[1]

3
Acht u de voorgestelde verplichting om gegevens van circa 450 miljoen Europeanen te bewaren nog effectief als deze maatregelen bestaan waarmee zij voor een deel van de bevolking niet zal werken? Kunt u uw antwoord toelichten?

4
Acht u het zinvol om de voorgestelde bewaarplicht te implementeren? Zo ja, waarom? Zo neen, bent u voornemens dit spoedig voor te stellen aan uw Europese collega ministers?

5
Kunt u deze vragen beantwoorden vóór het Kamerdebat van 6 september a.s. over de JBZ-raad inzake de bewaarplicht?

[1] Webwereld, 29 augustus jl.

Antwoord

Antwoord van minister **Donner** (Justitie). (Ontvangen 6 september 2005)

1
Nee. De bewaarplicht is niet eenvoudig te omzeilen. Gelet op vraag 2 is vermoedelijk bedoeld dat de registratie van gegevens eenvoudig te omzeilen is. Uit het antwoord op vraag 2 moge blijken dat ook daarvoor geldt dat vermijden van ieder spoor niet eenvoudig is. Overigens stel ik vast dat met betrekking tot vrijwel ieder opsporingsmiddel geldt dat het op bepaalde wijzen ontlopen kan worden. Door handschoenen aan te trekken ontloopt men de kans door middel van vingerafdrukken te worden opgespoord. Door de telefoon niet te gebruiken kan men niet worden afgeluisterd. Toch blijven het nemen van vingerafdrukken en het afluisteren van telefoongesprekken waardevolle instrumenten van opsporing.

2
Uit de genoemde technische mogelijkheden neem ik aan dat de vraag berust op een onlangs in Webwereld verschenen artikel. Dat artikel gaat evenwel uit van een te breed scala aan internetverkeersgegevens en niet van de gegevens die voortvloeien uit het kaderbesluit.
Hieronder zal ik evenwel ingaan op ieder van de genoemde tips:
– Het gebruik van een draadloos netwerk van een ander, in cafés of op zogenaamde hotspots zal het moeilijker maken om gebruik van een Internetaansluiting te herleiden naar een individu. Het is als zodanig niet anders dan het gebruik van een telefoon in een café. Het spoor kan echter wel leiden naar deze locatie, vanaf daar zal de recherche verder moeten speuren. Soms leidt dit tot resultaten, doordat bijvoorbeeld ooggetuigen de gebruiker gezien hebben, andere keren loopt het spoor dood. Toch leidt het beide keren tot inzichten over de verdachte en zijn communicatiegebruik. Dit betekent dus dat het volgen van het spoor niet zonder meer nutteloos is voor de opsporing. Tevens kunnen de

KVR23769
2040520650
0405tkkvr2321
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2005

gegevens op de (misbruikte) Internetaansluiting mogelijk sporen opleveren indien deze nog aanwezig zijn.
– Het gebruik van een prepaid GSM is zeer bekend als middel om communicatie niet tot een individu te laten herleiden. Toch blijkt keer op keer dat uit de analyse van de verkeersgegevens het wel degelijk mogelijk is voor de opsporing om belangrijke aanwijzingen te vinden die leiden tot de daders. Voorzover internetgebruik herleidbaar is naar internettoegang via een bepaald prepaid GSM, is dat een spoor dat gevolgd kan worden en dat via het combineren van sporen kan leiden tot een bepaalde verdachte. Zoals ook in de brief gesteld, hier zijn afdoende juridische en technische middelen voor.
– Chatten buiten Europa: Indien een van de partijen zich in Nederland dan wel Europa bevindt kan via de sporen in het netwerk achterhaald worden hoe de contacten zijn verlopen. Om die reden is door de opsporing in eerste instantie gevraagd om tevens de verkeersgegevens van het Internetgebruik te bewaren. Echter in het voorliggende Kaderbesluit is dit komen te vervallen. Daadoor is het moeilijker om de bronnen van de informatiestromen op het Internet te traceren. in tegenstelling tot wat Webwereld suggereert volgt niet uit het ontwerp kaderbesluit dat bijgehouden moet worden naar welke webadressen een gebruiker surft. Ook als binnen de EU gebruik gemaakt wordt van chat op websites, of middels games, hoeft daar onder het kaderbesluit geen registratie door de aanbieder van plaats te vinden. Een eigen server is ook in mijn brief aan uw Kamer al genoemd als een mogelijkheid om het vastleggen van met wie de gebruiker gemaild heeft te omzeilen. De gegevens van bijvoorbeeld bedrijfse-mail vallen niet onder de reikwijdte van het ontwerp kaderbesluit. Mocht een spoor echter leiden naar een dergelijke server, dan kan dit spoor verder gevolgd worden naar de klant bij wie die server in eigendom is (door bijv de creditcard betaling hiervoor te volgen). Tevens kunnen loggegevens op de server sporen opleveren vanaf welke Internetaansluiting wordt ingelogd (door bijvoorbeeld forensisch onderzoek te doen naar de harde schijf van de computer).
– Het inbellen naar een land waar niet gemonitord wordt: hoewel dit zal leiden tot het niet registreren van het gebruik van Internet bij een ISP (dienstaanbieder) in Nederland, zal dit wel leiden tot het registreren van een telefonieverbinding tussen Nederland en dat land bij een Nederlandse telefoonmaatschappij (netwerkaanbieder). Afhankelijk van de verkeersgegevens die bekend zijn en de wijze waarop gerechercheerd wordt kan een IP-adres uit het land waarnaar ingebeld is middels een verzoek om rechtshulp leiden naar een Nederlands telefoonnummer of kunnen de analyse van telefoniegegevens in Nederland leiden naar een telefoonaansluiting in dat land.
– Besloten dienst: het is mij niet geheel duidelijk wat Webwereld hier mee bedoelt. Vermoedelijk verwijst dit naar een besloten telecommunicatienetwerk of -dienst. Het is correct dat besloten telecommunicatienetwerken en -diensten niet onder de reikwijdte van de verplichting vallen. Een aanbieder kan niet zelf bepalen of zijn telecommunicatienetwerk of -dienst besloten is, maar dit zal een gevolg zijn van het netwerk of de dienst die hij aanbiedt en de wijze waarop dit gebeurt.
– Anonymous proxies en remailers. Het gebruik van proxies en remailers is onder andere bij spammers een veel gebruikte techniek om ontdekking van de daadwerkelijke verzender van de mail te verhullen. Ook hier blijkt dat een combinatie aan sporen wel degelijk kan leiden tot het vinden van de bron van de communicatie. Het is juist dat dit het soms minder eenvoudig voor de opsporing maakt; de Campina-zaak geeft echter aan dat dit niet altijd een beletsel is voor de opsporing. Het gebruik van TOR en Freenet (http://tor.eff.org en http://freenet.sourceforge.net/). Dit zijn programma's die het mogelijk maken om te communiceren via het Internet, zonder dat deze communicatie eenvoudig herleidbaar is tot (het IP-adres van) de gebruiker. Dit maakt verkeersanalyse door derden moeilijker. Het bewaren van internetverkeer op het niveau van IP-pakketten valt echter niet onder de bewaarplicht zoals deze uit het kaderbesluit voortvloeit. Het gebruik van TOR en Freenet maken het voor de opsporing complexer maar niet onmogelijk. Deze systemen berusten op het doorschakelen van de informatie over meerdere schakelsystemen. Juist, indien de historische verkeersgegevens bewaard blijven is terug rechercheren van de routering nog mogelijk.
– Het gebruik van tunnels om internetverkeer te versleutelen en langs punten elders op het Internet te leiden is van belang voor de beveiliging van de inhoud van het bericht. De verkeersgegevens zijn niet versleuteld. Immers de centrales in de netwerken kunnen geen versleutelde informatie verwerken. Via de netwerkaanbieder zijn de verkeersgevens van de tunneling te achterhalen.

3 en 4
Beide vragen antwoord ik bevestigend.
Verkeersgegevens zijn van groot belang voor de opsporing. De opsporing heeft weliswaar de bevoegdheid om de verkeersgegevens op te vragen maar in de praktijk zullen deze gegevens veelal zijn vernietigd vanwege de EU-privacyrichtlijn.
Bij de beantwoording van deze vraag wil ik nadrukkelijk verwijzen naar de brief die ik aan uw Kamer gestuurd heb op 5 september, waarin ik voor ieder van de te bewaren gegevens ook in ga op de mate waarin de verplichting ontweken kan worden. Het artikel van Webwereld geeft tips voor hoe je als gebruiker kan «proberen» om je gegevens af te schermen voor de nieuwsgierige blik van anderen. Daarbij wil ik nog eens melden dat waar daders een motivatie hebben om geen sporen na te laten, dit voor slachtoffers veelal niet het geval zal zijn. Vooropgesteld moet ook worden dat het feit dat het volgen van sporen niet altijd tot de verdachte leidt, niet betekent dat het bewaren van die gegevens geen nut zou hebben. Er dient altijd een afweging te zijn tussen nut voor de opsporing en de mogelijkheden en kosten voor het bedrijfsleven om deze gegevens te registreren en op te slaan. Ik meen dat de huidige versie van het ontwerp Kaderbesluit daarin een voldoende balans heeft gevonden.

5
Ja.