

Bijdrage voor het mondeling overleg met de Minister van Justitie in het kader van het JBZ overleg op 28 juni 2005 door de fractie van het CDA (woordvoerder H. Franken)

Betreft:

Ontwerp kaderbesluit over de bewaring van gegevens die zijn verwerkt en opgeslagen in verband met het aanbieden van openbare elektronische communicatiediensten of gegevens in openbare communicatienetwerken met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme.

JBZ dossier 4.0.6 kamerstuk nr. 23490

Allereerst wil ik graag mijn erkentelijkheid betuigen voor het feit, dat wij nu met de Minister over dit onderwerp van gedachten kunnen wisselen.. Op 15 februari 2005 en 22 februari 2005 heeft dit onderwerp op de agenda gestaan van het JBZ overleg, waarbij namens de CDA fractie kritische vragen zijn gesteld. De Minister van Justitie heeft hierop bij brief van 5 april 2005 geantwoord, doch deze beantwoording is door de gehele JBZ-commissie niet bevredigend geacht. Het ligt dan ook voor de hand om de belangrijkste punten uit de discussie nog eens de revue te laten passeren.

Ik ga ervan uit en ben mij er terdege van bewust, dat de bestrijding van ernstige strafbare feiten en zeker terrorisme van eminent belang is en zeker ook in het algemeen belang offers vraagt van de burger. Dit neemt niet weg, dat de wenselijke reikwijdte van een eventuele preventieve bewaarplicht enerzijds afhankelijk is van de klaarblijkelijke behoefte aan verkeers- en locatiegegevens bij de opsporingsdiensten en justitie in concrete gevallen en anderzijds van de weging van de gevolgen van zo'n algemene bewaarplicht voor de persoonlijke levenssfeer van burgers, en van de praktische en financiële gevolgen voor telecommunicatieaanbieders en de overheid. Daarbij geldt dan nog dat een eventueel aan de aanbieders op te leggen bewaarplicht beperkt dient te zijn tot uitsluitend gegevens die ten behoeve van commerciële of zakelijke doeleinden worden bewaard. Blijkens de gewisselde documenten, zowel in Brussel als in Den Haag, blijkt niet dat er een afweging is gemaakt, waarmee met de genoemde factoren serieus wordt rekening gehouden.

In de eerste plaats is niet duidelijk wat onder “verkeersgegevens” moet worden verstaan. Er zijn immers twee niveaus waarop men iets kan vastleggen: 1^e met betrekking tot de

adressering en het tijdstip (wie heeft wanneer waarheen iets verzonden) en 2^o met betrekking tot het “loggen” van de inhoud van het verkeer (wat).

Aan de hand van deze “verkeersgegevens” kan men zien, dat de machine heeft aangestaan maar niet wie deze heeft bediend of dat degene, die de machine bediende, op een bepaald tijdstip aanwezig was. Het is immers mogelijk dat er meerdere gebruikers schuilgaan achter één IP-adres. In veel bedrijven bijvoorbeeld wordt gebruik gemaakt van “Network Address Translation”, waardoor alle werknemers via één IP-adres naar buiten gaan. Dat doen veel bedrijven om security-redenen om te voorkomen, dat er vanaf internet een aanval op individuele computers zal worden gedaan. Zij laten dus al het verkeer via een centrale firewall lopen.

Men kan aan de hand van verkeersgegevens dus weten van welke webserver een machine iets opvraagt, maar niet of de gebruiker het zelf onder ogen heeft gekregen of welke website op die server het betreft en of het wel die webserver was of een andere dienst op diezelfde machine. Als men zich alleen richt op het vastleggen van de adressering en tijdstippen kan men dus nauwelijks iets relevants waarnemen.

Wat de inhoud van het verkeer betreft heeft de Minister aangegeven, dat het niet de bedoeling is om van de inhoud van door middel van telecommunicatie verzonden berichten kennis te nemen. Toch zou volgens de overgelegde stukken de stelselmatige kennisneming van verkeers- en locatiegegevens de mogelijkheid bieden een min of meer volledig beeld te krijgen van bepaalde aspecten van iemands leven. In dat geval is sprake van een inbreuk op de eerbiediging van de persoonlijke levenssfeer. Dit is mijn tweede punt.

Een inbreuk op de eerbiediging van de persoonlijke levenssfeer kan op grond van art. 8, tweede lid, van het EVRM gerechtvaardigd zijn, wanneer deze beperking bij de wet is voorzien en dit in het belang van enkele genoemde doelen “in een democratische samenleving noodzakelijk” is. Dit noodzaakcriterium wordt in de rechtspraak van het Europese Hof in Straatsburg nader ingevuld aan de hand van de beginselen van proportionaliteit, subsidiariteit en van een “pressing social need”.

In de bijdrage van mijn fractie voor de brief van de bijzondere commissie voor de JBZ-Raad van 22 februari 2005 heb ik namens mijn fractie hierover vragen gesteld, die – helaas – niet zijn beantwoord. Ik heb hier cijfervoorbeelden genoemd waaruit blijkt dat – in ieder geval ook voor de Nederlandse situatie – een redelijke verhouding tussen doel en middelen ontbreekt, omdat de bewaarplicht niet alleen ongeschikt, maar ook niet nodig is en voor de betrokkenen een onredelijke belasting betekent. Gezien het volume van de te bewaren gegevens, vooral op

het gebied van het internet, zal een zinvolle interpretatie van de gegevens totaal onmogelijk zijn. Voor wat betreft de hoeveelheid data, die volgens het besluit werkelijk zouden moeten worden bewaard, geeft de rapporteur van het EP, Alexander Nuno Alvaro, een aardig voorbeeld. Hij geeft aan – en blijktens informatie bij kenners van telecommunicatie en internetcommunicatie is mij gebleken, dat dit voorbeeld op juiste berekeningen is gebaseerd – dat in het net van een grote internetserversprovider bij de huidige verkeersintensiviteit reeds een hoeveelheid van 20-40.000 Terabyte wordt gegenereerd. Dat is een gegevensvolume dat met ongeveer 4mln.km gevulde dossierordners overeenkomt – dat zijn 10 dossierstapels die elk van de aarde tot de maan zouden reiken. Uit deze geweldige hoeveelheden verkeer zouden de verkeersgegevens van alle klanten moeten worden gedestilleerd, naar schatting 7% van de totale hoeveelheid. Maar omdat de netwerken van providers het verkeer van klanten via heel veel verschillende servers afhandelen, kunnen de complete verkeersgegevens van een klant alleen worden bemachtigd door een volledige tap op elke klant te zetten, dus inclusief de inhoud. Daaruit moet de provider dan de verkeersgegevens distilleren. Zonder extreem complexe en zeer kostbare databases zou een zoekoperatie op deze gegevens met gebruik van de thans bestaande techniek 50 tot 100 jaar duren. Blijkens informatie uit Nederland is mij gebleken, dat bij het routeringsknooppunt van Nederland de 50Gb grens reeds is overschreden. Dit betekent dat alle providers van Nederland samen in totaal meer dan 50Gb per seconde zouden moeten opslaan en bewerken om er de verkeersgegevens uit te destilleren. De huidige datastroom in het verkeersknooppunt beslaat 10 CD-ROMS per seconde (of 1½ DVD per seconde) en deze hoeveelheid neemt naar ieders verwachting de komende jaren alleen maar verder toe, bijvoorbeeld door de opkomst van internetvideo. Echter ook wanneer men een uitsplitsing van de opslag over een aantal diensten aanbieders realiseert, zal het aantal gegevens gigantisch zijn en de kosten zodanig toenemen, dat daarmee het criterium van proportionaliteit wordt geschonden.

In de stukken heeft de Minister zich beroepen op een berekening, die is gemaakt door KPMG Informatie Risk Management, waarbij is uitgegaan van een internetverkeer in Nederland van gemiddeld 25Gb per seconde. Dit gegeven berust op een aanname in het Stratix-rapport van augustus 2003 en is inmiddels (zoals uit mijn eerder aangegeven voorbeelden blijkt) alweer sterk verouderd.

Een ander aspect is nog, dat de verkeersgegevens van internetverkeer die wel zouden kunnen worden vastgelegd, onbruikbaar zijn voor analyse achteraf (er kan bijvoorbeeld geen verschil worden gemaakt tussen de ene mail en de andere) en niet bruikbaar zijn als bewijsmateriaal omdat ze eenvoudig vervalst en gemanipuleerd kunnen worden. In het klassieke vaste

telefoonnetwerk lijkt dit punt gemakkelijker te kunnen worden opgelost en in beeld gebracht, maar hier hebben de ontwikkelingen de laatste jaren verre van stilgestaan. Op technisch niveau is de klassieke telefonie immers aan het einde van haar bestaan. Vaste telefonie is naar verwachting van de sector binnen enkele jaren vrijwel volledig opgeslokt door VoIP, waarmee telefonie internet is geworden en de beoogde traceerbaarheid, die nu nog bij telefonie mogelijk is, verdwijnt. Ook mobiele telefonie is aan het overgaan op internetgedreven technologie (zoals UMTS), waarmee gesprekken op ieder gewenst moment ook via niet traceerbaar dataverkeer zijn te voeren. Telefonie verkeersgegevens zijn dus binnenkort net zo goed niets meer waard voor de opsporing.

Het internet is (dankzij de door de Europese Unie gepromote IPv6-standaard) binnenkort voorzien van 10 tot de macht 38 IP-nummers, die in grote en kleine blokken worden uitgedeeld. Dat is een miljard keer een miljard keer een miljard keer meer adressen dan vandaag de dag. Daarmee zal het fenomeen van het eenmalige IP-adres zijn ingang doen: voor ieder verschillend mailtje gebruikt men automatisch een ander IP-adres, voor het bezoeken van het web per site desnoods weer een ander. In een dynamische netwerktopologie zoals het internet die iedere dag verandert, leidt dat tot het volledig vaporiseren van informatie in een tijdsbestek van dagen. Gegevens willen bewaren is dan volledig een virtuele activiteit.

Een derde punt:

Van effectiviteit van de maatregel kan echt geen sprake zijn. Voor diegenen, die niet zijn gesteld op inmenging van de overheid, of ze nu kwaad in de zin hebben of niet, is het triviaal om maatregelen te nemen om echt alle informatie voor die overheid onzichtbaar te maken. Met de meest eenvoudige middelen die op ieder systeem aanwezig zijn (zoals het gebruik maken van webmail, het sturen van een mail via een eigen mailservers of een machine buiten Europa, het plaatsen van informatie op een publieke website, het gebruik van een proxy of het versleutelen van het volledige verkeer) verdwijnt ieder restantje van betekenis uit de toch al niet zinnig interpreteerbare gegevens. Het vastleggen van internetverkeer en telefonieverkeer zal voor het tegenhouden of achteraf aanpakken van kwaadwillenden geen enkel positief resultaat hebben; zij omzeilen een dergelijke naïeve beleidsmaatregel bijzonder gemakkelijk. Bovendien zal de wetenschap dat communicatiegegevens van iedereen worden vastgelegd, het gedrag van burgers zodanig veranderen dat er straks minder bruikbare justitiële informatie zal zijn dan nu. Het aftappen van een internetverbinding zal dan niet meer zinvol mogelijk zijn.

Voor (mobiele telefonie) geldt in de huidige situatie ook dat je er eenvoudig anoniem mee kunt bellen. De omloopsnelheid van mobiele telefoons is op dit moment 16 maanden: veel

jonge mensen nemen zelfs vaker een nieuw mobiel apparaat, niet zelden ook met een nieuw nummer. Telefoons worden vaak tweedehands verkocht en SIM-kaarten met een nieuw nummer kosten vrijwel niets meer. Voor een crimineel is het geen enkele moeite om regelmatig van nummer te veranderen. En ook zonder wisselen kun je anoniem zijn, ondermeer via het doorkoppelen van een aantal 0909-nummers. Er zijn veel van dat soort nummers die goedkope verbindingen leveren, ook naar het buitenland. Met UMTS kan men gewoon VoIP-bellen over de datalijn en dat is niet traceerbaar.

Van belang is wel, dat de verplicht opgeslagen gegevens aantrekkingskracht zullen uitoefenen op criminele (en misschien zelfs ook op commerciële) gebruikers. Het bewaren van zoveel gegevens brengt een enorm veiligheidsrisico met zich mee.

Graag ontvang ik commentaar van de Minister over deze opmerkingen met betrekking tot de proportionaliteit en de effectiviteit van de voorgestelde maatregel. In dit verband teken ik aan, dat de Minister op mijn vragen over dit onderwerp in de brief van 22 februari van dit jaar heeft gewezen op een onderzoek dat op zijn initiatief door de Erasmus Universiteit is ingesteld naar nut en noodzaak van de bewaring van telecommunicatiegegevens ten behoeve van de criminaliteitsbestrijding. Daarbij heeft de Minister aangegeven, dat dit onderzoek inzicht zou moeten verschaffen in de samenstelling van de verkeersgegevens, die door politie en justitie worden gevorderd alsook in het belang van de verschillende gegevens voor het resultaat van het opsporingsonderzoek. Bovendien zou dit onderzoek duidelijkheid moeten verschaffen welke effecten een bewaarplicht heeft op de doorlooptijden van strafvorderlijke onderzoeken. Deze vragen gaan echter geheel voorbij aan mijn opmerkingen over de effectiviteit van de bewaarplicht en houden geen enkel verband met de afweging tussen het opsporingsbelang en lasten voor burgers en bedrijven. Als ik het goed zie kan een beantwoording van de onderzoeksvragen ook geen inzicht geven in het eventuele nut en de noodzaak van de bewaarplicht. Nu het onderzoeksrapport is verschenen blijkt dit vermoeden te worden bevestigd. Het rapport geeft aan, dat bij de onderzochte 65 dossiers in nagenoeg alle gevallen de gewenste gegevens konden worden verstrekt zonder een wettelijke bewaarplicht. Het rapport geeft geen enkel argument waarbij nut en noodzaak van zo'n bewaarplicht wordt onderbouwd. De vragen van proportionaliteit en efficiency komen niet aan de orde. Er worden alleen wensenlijstjes van politieambtenaren genoteerd. Dat is wel iets anders.

Een vierde punt:

Ik denk aan de kosten, die voor Europese telecommunicatie en internetproviders zullen ontstaan. Daarover heeft de Minister alleen geantwoord, dat het marktsysteem geen blokkade mag vormen voor het denken over een bewaarplicht van telecommunicatie en internet verkeersgegevens. Het kostenaspect zou naar mijn mening echter wel een rol moeten spelen bij de afwegingen. Is het de Minister bekend dat één storage device om (slechts) 96TP op te slaan (read only) ongeveer € 700.000,- kost? Een kleine ISP met ongeveer 2½% marktaandeel zal 10 van dergelijke devices nodig hebben. Daarnaast zal het gereedmaken van het netwerk voor een dergelijke kleine provider reeds ongeveer € 50.000,- kosten met daarboven de kosten voor opslag en stroom van ongeveer € 25.000,- per maand. De directe kosten voor het internetgebruik, die natuurlijk aan de consument in rekening zullen worden gebracht, zullen daarom substantieel hoger worden. Dit geldt overigens niet voor Amerikaanse aanbieders, aangezien in de Verenigde Staten geen bewaarplicht geldt.

Tenslotte na mijn kritische opmerkingen, die overigens onderschreven worden door talloze deskundigen (ook die werkzaam zijn bij politie en justitie) wil ik de Minister enige alternatieven niet onthouden. Voor de opsporingactiviteit is infiltratie in internetgemeenschappen een effectief middel. Daarnaast beschikt het justitiële apparaat sinds het Cybercrimeverdrag over de mogelijkheid om tot bevrozing van gegevens over te gaan. Hiermee kunnen resultaten worden bereikt waarmee men wel de misdaad kan bestrijden.

Daarom Nederland wordt er niet veiliger van wanneer we de postbode gaan verplichten tot het administreren van iedere brief die hij bezorgt. En het vastleggen van alle gegevens van het internetverkeer is net zo bizar als iedereen te verplichten om een zuurstofmasker te dragen en de uitgeademde lucht van iedereen op te vangen en te analyseren. De hoop dat men met een dergelijke maatregel boeven of terroristen vangt, is vergeefs, want de trillingen van de lucht kan je niet meevangen.