Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2007–2008

31 145 Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens)

B

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR JUSTITIE[1]

Vastgesteld 8 juli 2008

Het voorbereidend onderzoek heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

Inleiding

De leden van de **CDA**-fractie hebben met belangstelling, doch ook met enige bevreemding kennis genomen van het wetsvoorstel over het bewaren van elektronische gegevens. Zij gaan ervan uit en zijn zich terdege bewust van het feit, 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 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 aan de aanbieders op te leggen bewaarplicht beperkt dient te zijn tot uitsluitend gegevens die ten behoeve van commerciële of zakelijke doeleinden worden bewaard. Hieruit volgt dat er een afweging moet worden gemaakt waarbij met alle genoemde factoren serieus rekening wordt gehouden en over deze afweging verantwoording wordt afgelegd.

De Eerste Kamer heeft zich bij de behandeling van het ontwerpkaderbesluit, waarin de thans aan de orde zijnde materie werd geregeld, steeds kritisch opgesteld en ten slotte aan dit besluit haar instemming onthouden. Ook bij de inbrengvergaderingen met betrekking tot de tot stand te brengen Richtlijn hebben alle partijen in de JBZ-commissie van de Eerste Kamer zich kritisch opgesteld met betrekking tot de noodzaak en meer

[1] Samenstelling:
Holdijk (SGP), Dölle (CDA), Tan (PvdA), Van de Beeten (CDA) (voorzitter), Broekers-Knol (VVD), De Graaf (VVD), Kneppers-Heynert (VVD), Kox (SP), Westerveld (PvdA) (vicevoorzitter), Russell (CDA), Engels (D66), Franken (CDA), Peters (SP), Quik-Schuijt (SP), Haubrich-Gooskens (PvdA), Ten Horn (SP), Janse de Jonge (CDA), Koffeman (PvdD), Böhler (GL), Van Bijsterveld (CDA), Strik (GL), Lagerwerf-Vergunst (CU), Rehwinkel (PvdA), Duthler (VVD) en Yildirim (Fractie-Yildirim).

KST120849
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2008

specifiek met betrekking tot de proportionaliteit van de voorgestelde maatregel.

Vanzelfsprekend erkennen de aan het woord zijnde leden de plicht tot implementatie van Richtlijn 2006/24/EG, doch hierbij lijkt sprake te zijn van een daadwerkelijke schending van het bepaalde in artikel 8 EVRM, zodat de uit laatstgenoemd artikel voortvloeiende principiële vragen naar noodzaak c.q. proportionaliteit van de maatregel aan de orde zijn.

Over de introductie van een bewaarplicht van telecommunicatiegegevens voor aanbieders van telecommunicatiediensten is in de Tweede Kamer uitgebreid gediscussieerd. De discussiepunten betroffen – zoals bekend – voornamelijk nut en noodzaak van de bewaarplicht, de bewaartermijn, kosten, effectiviteit en privacybescherming. De leden van de **VVD**-fractie hebben kennis genomen van deze discussie en achten deze voldoende afgerond.

Met de bewaartermijn van 12 maanden kunnen deze leden goed leven. Een goede balans is volgens hen gevonden tussen het doel waarvoor de telecommunicatiegegevens worden bewaard, te weten onderzoeken, opsporen en vervolgen van ernstige criminaliteit aan de ene kant en de inbreuk op de bescherming van de persoonlijke levenssfeer aan de andere kant.

De leden van de **PvdA**-fractie hebben met waardering kennis genomen van de parlementaire behandeling van wetsvoorstel 31 145. Deze waardering betreft niet de inhoud van het wetsvoorstel, maar de gedegen parlementaire behandeling die dit ten deel is gevallen waarin alle aspecten van het onderwerp aan de orde zijn gesteld, gewogen en uiteindelijk neergeslagen in een politiek compromis. Zij wensen de regering, bij de behandeling van dit wetsvoorstel in de *Kamer van Reflectie*, de volgende inbreng voor te leggen uitmondend in een tweetal gerichte vragen.

Met belangstelling hebben de leden van de fracties van **ChristenUnie** en **SGP** kennisgenomen van zowel het wetsvoorstel als de schriftelijke en mondelinge behandeling in de Tweede Kamer. Zij zijn verheugd dat het amendement van het lid Anker is aangenomen, waardoor de door de regering voorgestelde bewaartermijn van 18 maanden is terug gebracht naar 12 maanden. Ook de verkorting van de oorspronkelijke evaluatieperiode van 5 jaar naar 3 jaar kan hun goedkeuring wegdragen. Immers, een maatregel die bewerkstelligt dat belangrijke gegevens van grote groepen personen, ongeacht of zij verdachte van een strafbaar feit zijn of niet, gedurende langere periode wordt bewaard, dient in het licht van de vereiste proportionaliteit effectief te zijn. Een evaluatie-onderzoek kan op dit punt uitsluitsel geven en dient wat de leden van deze fracties betreft dan ook niet te lang op zich te laten wachten. De leden van de aan het woord zijnde fracties hebben slechts enkele vragen.

De leden van de fractie van **GroenLinks** zijn zich bewust van de beperkte toets van onderhavig wetsvoorstel: de richtlijn zelf is immers een vaststaand feit, de toets beperkt zich tot de wijze van implementatie door de Nederlandse regering. Daarbij valt op dat de regering de implementatie aangrijpt om meer te doen dan de richtlijn verlangt, door de bewaartermijn op 12 maanden te stellen in plaats van de verplichte zes maanden.

De leden van de fractie van **D66** hebben met zekere gevoelens van aarzeling kennis genomen van het voorstel. Deze leden onderschrijven op zichzelf genomen de strekking daarvan, voorzover het voorziet in het garanderen en beschikbaar stellen van telecommunicatiegegevens voor een bepaalde tijd ten bate van de bestrijding van ernstige vormen van

criminaliteit. Zij hebben echter zorgen over de waarborging van de privacy van burgers en willen ook op enkele andere punten een vraag stellen.

De leden van de fractie van de **SP** zijn buitengewoon bezorgd over het voorliggende implementatievoorstel, zeker nu het nog verder gaat dan waartoe de te implementeren richtlijn Nederland verplicht. Deze leden hadden al grote moeite met de ontwerpkaderrichtlijn en vinden de nu door de regering gedachte uitbreiding van de bewaartermijn van zes naar twaalf maanden volstrekt onvoldoende gemotiveerd. Deze leden zijn bevreesd dat hier een enorme vracht informatie verzameld en bewaard gaat worden, waarmee art. 8 EVRM geschonden wordt zonder dat nut, noodzaak een proportionaliteit ervan wordt aangegeven. Deze leden vrezen ook dat de kosten die gepaard gaan met deze gigantische opslag van gegevens op enig moment kunnen leiden tot de gedachte dat we toch «iets» met die gegevens moeten doen, om de kosten te rechtvaardigen. Deze leden willen graag weten of de regering deze zorgen deelt en zo ja, waarom toch gekozen wordt voor deze «overdadige» implementatie van de richtlijn?

Reikwijdte van de richtlijn

Als doel van de voorgestelde maatregel wordt genoemd het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Kan de regering aangeven aan welke misdrijven hier wordt gedacht? Wordt bij de kwalificatie «ernstig» alleen gedacht aan een of meer categorieën van delicten of vallen hier ook andere soorten van crimineel gedrag onder? Is uiteindelijk de in het Wetboek van Strafrecht opgenomen strafbedreiging bepalend voor de te onderzoeken groep misdrijven, en zo ja waar ligt de grens om van wel of niet ernstige misdrijven te spreken? Hoe hebben andere lidstaten aan dit criterium invulling gegeven? Is er sprake van een catalogus van delicten? Graag ontvangen de leden van de **CDA**-fractie een antwoord op deze vragen.

Bewaartermijn

De regering motiveert de noodzaak van de bewaarverplichting – een motivering die ook wordt vereist in het geval dat in de implementatiewet voor een ruimere termijn dan de voorgeschreven minimum periode van zes maanden wordt gekozen – met een verwijzing naar de behoeften van politie en justitie en het onderzoek van de Erasmus Universiteit Rotterdam (EUR).[1] Behoeften van politie en justitie kunnen als zodanig, althans zonder nadere onderbouwing, eerder als een wens («nice to have») dan als een noodzaak («must») worden aangemerkt. Gaarne zien de leden van de **CDA**-fractie de onderbouwing als noodzaak tegemoet, zodat de conclusie kan worden getrokken dat het om meer dan een wenselijkheid gaat om de verkeersgegevens langer dan de in Richtlijn 2002/58/EG genoemde termijn en zeker langer dan de in Richtlijn 2006/24/EG voorgestelde termijn van zes maanden te bewaren.

Het rapport van de EUR kan – naar de mening van de leden van de CDA-fractie – in het geheel niet als een onderbouwing van een langere dan de minimumtermijn worden beschouwd. Het blijkt immers dat de vraagstelling en de gehanteerde onderzoeksmethode daar niet op zijn geënt. De vraagstelling is gericht op de wijze van uitvoering van de bestaande bevoegdheid «tot het vorderen van gegevensverkeer» en het aangeven van knelpunten daarbij en tevens op de mogelijke gevolgen van een verruiming van de bewaringstermijn in de praktijk.

[1] Kamerstuk II, 23 490, nr. 379.

De onderzoekers hebben voor de uitvoering van hun opdracht slechts 65 opsporingsdossiers tot hun beschikking gekregen waarin verkeersgegevens van vaste en mobiele telefonie een belangrijke rol speelden. In die dossiers waren de benodigde verkeersgegevens steeds beschikbaar. Daaruit volgt reeds dat een verlenging van de om commerciële redenen aangehouden bewaartermijn, die in overeenstemming is met Richtlijn 2002/58/EG, niet noodzakelijk zou zijn.

Er waren voor het onderzoek te weinig dossiers voorhanden waarin verkeersgegevens met betrekking tot internet een rol speelden, zodat voor die categorie op basis van dossieronderzoek met betrekking tot nut en noodzaak van het verruimen van de bewaartermijn geen wetenschappelijk verantwoorde conclusies waren te trekken. (blz. 29 rapport) «Om toch enige conclusies te kunnen trekken is het onderzoek uitgebreid met een aantal interviews met internetdeskundigen van de politie.» (blz. 30 rapport) Op basis van deze gesprekken en niet op basis van onderzoek naar het feitelijk gebruik van verkeersgegevens is de conclusie getrokken dat een bewaartermijn van één jaar voor alle gegevens, zowel van telefonie als van internetverkeer, wenselijk is.

Met de aldus tot stand gekomen conclusie dat een bewaarplicht wenselijk zou zijn, is evenwel niet voldaan aan het noodzakelijkheidscriterium van artikel 8 EVRM. Zie hiervoor EHRM 25 maart 1983, Silver and others vs United Kingdom, nr. 97, waarin is vermeld: «the adjective *necessary* is not synonymous with *indispensable*, neither has it the flexibility of such expressions as *admissible*, *ordinary*, *useful*, *reasonable* or *desirable* ...». De conclusie is, dat de door het EVRM vereiste onderbouwing van de proportionaliteit ontbreekt en de noodzaak van het bewaren van internetgegevens (in ieder geval voor een periode langer dan 6 maanden) niet is aangetoond.

In dit verband verwijzen de aan het woord zijnde leden naar het manifest van 15 hoogleraren in het ICT-recht dan wel in de computerbeveiliging of het strafrecht, dat is gepubliceerd in NRC Handelsblad van 21 mei 2008. Bij de ondertekenaars bevindt zich de hoogleraar die als supervisor optrad bij het onderzoek dat heeft geleid tot het geciteerde rapport van de EUR. Deze betoogt in dit artikel met zijn collega's, dat – als de regering de plicht tot implementatie van Richtlijn 2006/24/EG laat prevaleren boven de eisen van artikel 8 EVRM – een bewaartermijn van 6 maanden niet moet worden overschreden.

De leden van de **SP**-fractie sluiten zich graag bij deze vragen van het CDA aan.

De leden van de **PvdA**-fractie stellen vast dat met dit wetsvoorstel in zoverre sprake is van een «kop» op Europese regelgeving dat hier verder wordt gegaan dan de Europese regelgever voor de bestrijding of het voorkomen van terroristische aanslagen en ernstige criminaliteit noodzakelijk acht. In de visie van deze leden betekent dit dat op de regering een bijzondere verantwoordelijkheid rust om aan te geven waarom zij de met dit wetsvoorstel teweeggebrachte inbreuk op de persoonlijke levenssfeer noodzakelijk acht en als middel voor de te bereiken doelen proportioneel. Deze bijzondere verantwoordelijkheid betreft dan in het bijzonder de nationale «kop» van zes maanden. Deelt de regering deze vaststelling?

Kan de regering, alle argumenten voor en tegen die in de parlementaire voorbereiding zijn gewisseld gehoord en gewogen hebbend, nog eens aangeven waarom zij de positie is blijven betrekken die zij heeft betrokken? Waarom acht zij het verder gaan dan de EU noodzakelijk acht voor ons land geïndiceerd? Welk doel of welke doelen staan haar voor

ogen met een wettelijke bewaarplicht van langer dan zes maanden en waarom acht zij het, gehoord ook alle in de voorbereiding ingebrachte – en door hem ook ten dele onderschreven – relativeringen, aannemelijk dat die doelen ook als gevolg van de onderhavige langere bewaarplicht *in een substantieel aantal gevallen* (proportionaliteit) bereikt zullen worden?

Kan de regering in de beschouwing over met name de substantiële slagingskans onderscheid maken tussen het doel van a) het voorkomen van terroristische aanslagen, b) het opsporen van daders van ernstige criminaliteit en c) het oplossen van gepleegde criminaliteit?

Tijdens de plenaire bespreking in de Tweede Kamer heeft de minister van Justitie over het onderzoek naar de moord op de Hells Angels in Oirsbeek gezegd dat «gelukkig de gegevens van 18 tot 24 maanden eerder bij dit onderzoek nog bij de telecombedrijven beschikbaar waren». Naar aanleiding van deze opmerking vragen de leden van de fracties van **ChristenUnie** en **SGP** zich af of dit betekent dat telecombedrijven en internetproviders de gegevens weliswaar minimaal 12 maanden moeten bewaren, maar vervolgens niet verplicht zijn deze gegevens na de bewaartermijn 12 maanden te vernietigen. Als deze vraag bevestigend beantwoord wordt, is de vervolgvraag of de telecombedrijven en internetproviders verplicht zijn op enig moment de gegevens te vernietigen en zo ja, op welke termijn?

Is de regering het met de leden van de **GroenLinks**-fractie eens dat een ingrijpende inbreuk op de privacy als het bewaren van persoonlijke gegevens gelegitimeerd moet zijn door het aantonen van nut en noodzaak? Kan zij ingaan op de uitkomsten van diverse onderzoeken, waaruit blijkt dat nut en noodzaak van een langere beschikbaaarheid dan zes maanden van verkeersgegevens niet zijn aangetoond? Een langere termijn blijkt uit deze onderzoeken nauwelijks invloed te hebben op het opsporingspercentage van de betreffende misdrijven. De leden refereren hier aan het onderzoek van het Max Planckinstituut in Freiburg en een onderzoek van het Bundeskriminalamt uit 2005. Ook wetenschappers van diverse disciplines hebben benadrukt dat niet overtuigend is aangetoond dat de bewaarplicht tot het oplossen van veel misdrijven leidt.[1] Kan de regering uitleggen op welke wijze de Nederlandse situatie een bewaartermijn van een jaar rechtvaardigt, terwijl Duitsland, Finland, Tsjechië en Zweden een termijn van zes maanden voldoende achten?

De bewaring van verkeersgegevens

Het moet de regering evenals de leden van de **CDA**-fractie bekend zijn, dat de hoeveelheid van de te bewaren gegevens een enorme omvang heeft. Uit de geweldige hoeveelheden zouden de verkeersgegevens van alle gebruikers moeten worden gedestilleerd. Maar omdat de netwerken van providers het verkeer van klanten via heel verschillende servers afhandelen, kunnen de complete verkeersgegevens van een klant alleen worden bemachtigd door een volledige tap op elke klant te zetten, dat wil zeggen inclusief de inhoud. Daaruit moet de provider dan de verkeersgegevens destilleren. Zonder extreem complexe en zeer kostbare databases zullen deze zoekoperaties met behulp van de bestaande techniek vele mensjaren duren.

Bij de berekeningen die door de minister van Justitie zijn gebruikt, wordt verwezen naar stukken uit 2005 (KPMG Informatie Risk Management), dat is gebaseerd op het Stratix rapport, dat stamt uit 2003, en van VKA (Verdonck, Klooster& Associates), dat is opgesteld in samenwerking met Lucent Technologies uit 2006. De in deze rapporten gehanteerde gegevens zijn inmiddels (sterk) verouderd. Het internetverkeer is in de tussentijd explosief toegenomen. Bovendien hebben de ontwikkelingen met betrek-

[1] NRC Handelsblad, 2 april 2008.

king tot de vaste en mobiele telefonie ook niet stilgestaan. De vaste telefonie, die kennelijk als model heeft gediend voor het opzetten van de bewaarplicht, is aan het einde van haar bestaan. Binnen enkele jaren zal deze vrijwel volledig zijn opgeslokt door Volp, 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 ook op ieder moment zijn te voeren via niet traceerbaar dataverkeer.

Het internet is (dankzij de door de EU 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 x een miljard x een miljard meer adressen dan heden. 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 netwerktypologie zoals het internet die iedere dag verandert, leidt dat tot een volledig vaporiseren van informatie in een tijdsbestek van dagen. Gegevens willen bewaren is dan volledig een virtuele activiteit. Hoe plaatst de regering deze – hier nog slechts rudimentair beschreven ontwikkelingen – in de beantwoording van de vraag naar nut en noodzaak van de voorgestelde bewaarplicht dan wel naar de proportionaliteit daarvan?

Ook de leden van de **SP**-fractie hebben de indruk dat de regering niet precies voor ogen heeft tot welke praktische gevolgen het invoeren van deze ongemotiveerd lange bewaartermijn zal kunnen leiden. Zij zien graag een degelijker onderbouwing van de kant van de regering.

Nu de gegevens door de telecomaanbieders zelf moeten worden opgeslagen rijst bij de leden van de fractie van **D66** de vraag op grond van welke argumenten op dit punt de keuzes voor nadere regulering in een AMvB zijn gemaakt. Specifiek bedoelen deze leden welke gegevens op welke wijze opgeslagen dienen te worden, hoe deze gegevens beschikbaar kunnen worden gemaakt voor de opsporingsdiensten, hoe deze adequaat beschermd kunnen worden en hoe wordt gecontroleerd dat er met deze privacy gevoelige gegevens correct wordt omgegaan.

Gegevensbeveiliging en gegevensbescherming

Als de leden van de **CDA**-fractie het goed zien, zijn digitale data erg kwetsbaar voor zowel grootschalige als kleinschalige (gerichte) manipulatie op afstand. Zolang het triviaal is om de PC van een ander op afstand over te nemen als de gebruiker een standaardbrowser met standaardinstellingen heeft, of het een leek in een paar van het internet af te plukken stappen lukt om anoniem van iemand een router te hacken met een simpel javascript en er botnets zijn met honderdduizenden PC's die klaar staan om kwaadwillend gedrag te maskeren (bijvoorbeeld via spamruns), is het een fictie om enkel digitale data richtinggevend te achten voor een effectieve opsporing, simpelweg omdat het te gemakkelijk is om een ander verdacht te maken en onmogelijk om te bewijzen dat daar geen reden voor is geweest. Samengevat lijkt het dat dataretentie een bron van schijnveiligheid is, omdat a. verkeersgegevens nooit kunnen aantonen dat een individu verkeer heeft veroorzaakt en b. criminelen eenvoudig valse sporen kunnen uitzetten als afleiding van hun werkelijke activiteiten. Gaarne vernemen de aan het woord zijnde leden het standpunt van de regering met betrekking tot deze analyse.

De leden van de **GroenLinks**-fractie vernemen graag of de regering op de hoogte is van de uitkomsten van de expertmeeting die de Eerste Kamer heeft gehouden op 20 maart 2008 met betrekking tot gegevensbescher-

ming?[1] Kunt u op basis van de in de Senaat breed gedragen criteria die de heer Franken daar heeft opgesomd waaraan wetgeving met betrekking tot gegevensbescherming zou moeten voldoen, een legitimering geven van de door u voorgestelde implementatiewet? Kort gezegd behelsden deze criteria noodzaak, inclusief effectiviteit en hanteerbaarheid, proportionaliteit, een privacy impact assessment, controlemogelijkheid, onder andere door een goede rechtsbescherming, en een horizonbepaling waardoor de wet tijdig opnieuw wordt beschouwd.

De verhouding tot het recht op bescherming van de persoonlijke levenssfeer

Het noodzaakcriterium, dat is geformuleerd in artikel 8 EVRM, is in casu van toepassing omdat het dan weliswaar niet de bedoeling is om van de inhoud van door middel van telecommunicatie verzonden berichten kennis te nemen, doch het stelselmatig (kunnen) kennisnemen van verkeers- en locatiegegevens de mogelijkheid geeft een min of meer volledig beeld te verkrijgen van bepaalde aspecten van iemands leven. Hierdoor kan volgens de leden van de **CDA**-fractie sprake zijn van een inbreuk op de eerbiediging van de persoonlijke levenssfeer. Een beperking daarop is slechts toelaatbaar wanneer deze beperking bij de wet is voorzien en deze in het belang van enkele in de verdragsbepaling genoemde doelen in een democratische samenleving noodzakelijk is. Het Europese Hof in Straatsburg heeft dit criterium nader ingevuld aan de hand van de beginselen van proportionaliteit en subsidiariteit en van een «pressing social need».

Wat is de mening van de regering naar aanleiding van de eerste stelling in het manifest van de hoogleraren, dat is gepubliceerd in NRC Handelsblad van 21 mei 2008, die inhoudt, dat onschuldige burgers last zullen krijgen van fouten die onvermijdelijk in de praktijk zullen worden gemaakt? Een huiszoeking en het nemen van dwangmaatregelen vindt soms plaats op grond van onjuiste telecommunicatiegegevens. Hoe goed de bedoelingen ook mogen zijn, meer gegevens zullen leiden tot meer en meer ernstige fouten. Ook kan het gebeuren, dat gegevens ongewenst «op straat» komen. In Engeland is al een aantal incidenten geweest waarbij data van miljoenen mensen uit de macht van de beheerder zijn geraakt. Daarbij komt dat verkeersgegevens niet alleen voor de overheid een interessante bron van informatie vormen. Uit een set identificerende gegevens van provider AOL wisten gebruikers in korte tijd identificerende en chantabele gegevens te extraheren. Omdat gericht en ongericht kan worden gezocht (datamining), vormt de dataset achter dataretentie de heilige graal voor de georganiseerde misdaad, aangezien de toegang tot die data deuren opent voor corruptie op grote schaal.

De leden van de **VVD**-fractie hebben een vraag over de waarborging van de kwaliteit van de te bewaren gegevens. De ervaring leert dat met name veel internetproviders hieraan geen prioriteit geven en hun gegevensbeveiliging niet goed op orde hebben. Het waarborgen van de kwaliteit van gegevens is een onderdeel van de bescherming van de persoonlijke levenssfeer. Hoe gaat de regering bevorderen dat de providers maatregelen zullen treffen om de kwaliteit van de gegevens – we spreken ook wel van juistheid en volledigheid van gegevens – te waarborgen?

Een tweede vraag van de leden van de **PvdA**-fractie betrof de risico's van het opslaan en gedurende geruime tijd ter beschikking hebben en houden van persoonsgegevens. Is de regering het met ons eens dat de kans dat er bij de opslag van gegevens fouten worden gemaakt en dat die fouten nadien niet gemakkelijk hersteld kunnen worden toenemen naarmate de bewaartermijn langer is? In hoeverre zijn de bestaande ICT-systemen op

[1] Kamerstuk 31 200 VI, F.

deze ingrijpende taakopdracht toegerust? Welke mogelijkheden heeft de burger om dergelijke fouten te (laten) herstellen? Aan welke termijn van implementatie denkt de regering in dit verband?

De leden van de fractie van **GroenLinks** verzoeken de regering in te gaan op de kritiek van het College Bescherming Persoonsgegevens (CBP), dat de huidige vage begrenzing van het recht op toegang tot de data in strijd is met artikel 4 van de Richtlijn? Kan zij daarbij ook ingaan op de door het CBP genoemde uitspraak van het BverfG van 4 april 2006? Is de regering bereid om de wet in overeenstemming met artikel 4 te brengen, en zo ja op welke wijze?

Door middel van het bewaren van verkeers- en locatiegegevens met betrekking tot internettoegang, e-mail en (internet)telefonie wordt door opsporingsinstanties over een langere periode inzicht verkregen in de communicatiegegevens van een persoon die niet verdacht wordt van een strafbaar feit. De leden van de **D66**-fractie realiseren zich terdege het belang van de beschikbaarheid van dit type gegevens in een opsporingsonderzoek naar ernstige strafbare feiten. Met bijvoorbeeld het CBP vragen zij zich echter af in hoeverre de na amendering van achttien naar twaalf maanden teruggebrachte bewaartermijn op gespannen voet blijft staan met het fundamentele recht op eerbiediging van de persoonlijke levenssfeer, zoals verankerd in artikel 8 van het Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Nog steeds kan immers nog steeds van een lange bewaartermijn worden gesproken. In ons omringende landen als Duitsland, Oostenrijk, Luxemburg, Finland, Zweden en Tsjechië bijvoorbeeld is gekozen voor een bewaartermijn van zes maanden. Graag vragen deze leden de regering hoe nu moet worden aangekeken tegen de situatie dat de bewaartermijn in dit voorstel niet synchroon loopt met de ons omringende landen? Hoe moet de eerbiediging van artikel 8 EVRM, en de daarin vervatte proportionaliteitseis ingeval van een inbreuk op de privacy worden bezien, nu er een rechtsongelijkheid wordt gecreëerd tussen de burgers van de verschillende Europese landen? In hoeverre sluiten de nu ontstane verschillende regimes aan bij de oproep van de Europese Commissie tot harmonisatie van deze termijnen?

Gevolgen van aanhangige rechtszaken

Bundesverfassungsgericht

De leden van de **CDA**-fractie zijn geïnteresseerd in de uitkomst van de opdracht die het Bundesverfassungsgericht (BVerfG) in zijn uitspraak van 11 maart 2008 aan de Duitse regering heeft gegeven over de uitwerking van de bij de implementatiewet vastgestelde bewaarplicht.[1] In deze opdracht is de vraag opgenomen in hoeverre voor opsporingsonderzoeken effectief voordelen blijken en welke de daaraan (voor de burger) verbonden nadelen zijn.

Hoe beoordeelt de regering de uitspraak van het Bundesverfassungsgericht van 11 maart 2008, dat de toepassing van de Duitse implementatiewet gedeeltelijk diende te worden opgeschort vanwege het risico van schending van artikel 10 lid 1 van de Duitse Grondwet? Kunt u de scenario's schetsen die aan de orde kunnen zijn in het geval het BverfG ook in de bodemprocedure de toepassing verbiedt? Is het recht op bescherming van de persoonlijke levenssfeer in Duitsland beter gewaarborgd dan in Nederland? Graag ontvangen de leden van de **GroenLinks**-fractie een toelichting.

[1] BVerfG, 1 BvR 256/08 van 11 maart 2008.

Europees Hof van Justitie

Het gegeven dat Ierland een procedure bij het Hof van Justitie heeft aangespannen[1], laat naar het oordeel van de leden van de fracties van **ChristenUnie** en **SGP** onverlet dat Nederland gebonden is de Europese richtlijn te implementeren. Echter, wat zou de consequentie zijn als de door Ierland aangespannen procedure resulteert in een vaststelling van het Hof van Justitie dat de dataretentierichtlijn tot stand is gekomen op basis van een onjuiste rechtsgrondslag? Blijft de wet bewaarplicht telecommunicatiegegevens, ervan uitgaande dat deze wet wordt aangenomen, dan ongewijzigd van kracht? Ook de leden van de **D66**-fractie ontvangen graag een reactie op deze rechtszaak.

Situatie in andere lidstaten

De leden van de **CDA**-fractie vernemen graag de visie van de regering op de (conclusies van de) onderzoeken, die in Duitsland zijn gedaan door respectievelijk de brancheorganisatie Bitkom en door het Max Planck Instituut voor buitenslands en internationaal strafrecht. Naar het laatstgenoemde onderzoek wordt verwezen in de reeds aangehaalde uitspraak van het BVerfG, bij welke uitspraak de Duitse implementatiewet voor een belangrijk deel is opgeschort. De Duitse regering achtte het aantal van 467 strafdossiers dat in deze studie is gebruikt, te gering. (NB. In het onderzoek van de EUR werden slechts 69 dossiers gebruikt, terwijl er voor onderzoek naar internetgebruik in het geheel geen dossiers voorhanden waren.)

Kosten voor gegevensbewaring

De leden van de **CDA**-fractie wijzen nog eens op de kosten, die providers moeten maken om de enorme hoeveelheden gegevens op te slaan. Reeds het verschil voor een bewaartermijn van 12 of van 6 maanden moet vele miljoenen euro's bedragen. De aanbieders moeten zelf de investeringskosten dragen en de kosten van exploitatie en onderhoud die voortvloeien uit de verplichting van hoofdstuk 13 Telecomwet. Alleen de directe personele en administratieve kosten voor het plaatsen van een tap en voor een informatieverstrekking komen voor rekening van de overheid. Die investeringskosten moeten ook door kleine providers worden gemaakt, waarbij geldt dat bij de hierboven genoemde dynamische IP-adressen (die per seconde kunnen wisselen) de gebruikersnaam met alle inlogtijd en uitlogtijd moet worden opgeslagen. Dit moet ook gebeuren bij elk spambericht. En dat terwijl spam ruim 90% van het email verkeer uitmaakt. Deze kosten zullen natuurlijk aan de consument in rekening worden gebracht. Hierdoor ontstaat een concurrentievoordeel voor providers, die hun servers buiten de EU hebben staan en deswege niet verplicht zijn deze kosten te maken, en voor providers in landen, zoals Duitsland, die niet boven de zesmaandstermijn uitgaan. De aan het woord zijnde leden zouden graag een up to date overzicht ontvangen van de geschatte kosten en vergoedingen die daartegenover worden gesteld.

Een andere vraag van de leden van de **VVD**-fractie betreft de in de Tweede Kamer aanvaarde motie-De Wit[2]. Deze motie roept de regering op met voorstellen te komen tot een meer rechtvaardige vergoeding van de kosten van providers. Welke criteria hanteert de regering bij het uitwerken van de motie? Houdt hij bijvoorbeeld rekening met de kosten van aanschaf van extra capaciteit en software, het treffen van procedures en maatregelen en het treffen van beveiligingsmaatregelen? Hoe geeft hij invulling aan het begrip «meer gerechtvaardigd» uit de motie?

[1] Zaak C-301/06 – Ierland v. Raad van de Europese Unie en Europees Parlement.
[2] Kamerstuk 31 145, nr. 15.

Voor kleinere providers zal het relatief duurder zijn om aan de bewaarplicht te voldoen dan voor grotere bedrijven. Deze laatste groep heeft zijn eigen informatiehuishouding meestal al op orde, en heeft beveiligingsmaatregelen getroffen. Hoe werkt dat uit op de concurrentiepositie? Houdt hij daar rekening mee? Hoe is dat in andere lidstaten geregeld?

Ook de leden van de **SP**-fractie willen graag van de regering vernemen hoe die de kosten, samenhangend met een bewaartermijn van 12 maanden, inschat en hoe de regering de uitvoering van de motie-De Wit gestalte denkt te geven.

In de Staatscourant van 26 mei 2008 wordt gesteld, zo lezen de leden van de fracties van **ChristenUnie** en **SGP**, dat als gevolg van de kosten voor het bedrijfsleven de kleinere internetproviders een concurrentieachterstand dreigen op te lopen, waardoor de markt verstoord wordt. Op welke wijze denkt de regering de motie-De Wit om de kosten van het opslaan rechtvaardig te verdelen, uit te gaan voeren?

Dan enkele vragen van de leden van de **GroenLinks**-fractie over de financiering van de uitvoering van de bewaarplicht. Kan de regering al in grote lijnen schetsen op welke wijze u de motie-De Wit gaat uitvoeren om een rechtvaardige kostenvergoedingssystematiek te bereiken? Op welke wijze gaan andere lidstaten om met betrekking tot het dragen van de kosten?

Overig

Er zijn diverse – voor iedereen gemakkelijk toegankelijke – publicaties over de manieren waarop de bewaarplicht kan worden omzeild. De wetenschap van een mogelijk opvragen van verkeersgegevens zal de burger – in ieder geval de kwaadwillende burger – aanleiding geven om software te kopen, of van gratis ter beschikking gestelde software als Sabayon Linux gebruik te maken waarmee men zonder gegevens op de harde schijf weg te schrijven anoniem kan surfen, gamen, mailen, chatten, downloaden en browsen. Als een gebruiker van dergelijke software zijn computer afsluit, is er geen enkel «bewijs», niet bij de ISP en niet bij de gebruiker. Ook door het gebruik van bedrijfsmail en e-maildiensten als Hotmail, MSN, Skype en Hyves – welk gebruik op grote schaal voorkomt – zijn geen relevante verkeersgegevens te achterhalen. Aangezien de lijst van mogelijkheden tot omzeilen vrijwel onuitputtelijk is, vragen de leden van de **CDA**-fractie zich af waarop de regering nog enig nuttig effect van de voorgestelde regeling baseert. Deze vraag geldt voor de maatregel in het algemeen, maar zeker ook voorzover deze verder reikt dan de zesmaandstermijn die ons door de EU wordt opgelegd.

De in artikel 13.19 opgenomen evaluatiebepaling schrijft voor dat de evaluatie slechts een drietal bepalingen betreft. De reikwijdte van deze evaluatie is voor de leden van de **D66**-fractie niet geheel helder. In hoeverre kan nu worden gesproken van een duidelijk omschreven kader waarbinnen geëvalueerd dient te worden?
In het Wetboek van Strafvordering is in 2006 met de invoering van de Wijzigingswet Computercriminaliteit II[1] artikel 126ni opgenomen. In dit artikel is een specifieke bewaarplicht opgenomen, gekoppeld aan een korte bewaartermijn, namelijk maximaal negentig plus negentig dagen. Dit artikel stelt naast een specifieke bewaarplicht en een stringente bewaartermijn aanvullende eisen aan de verstrekking van gegevens. Waarom is niet meer aansluiting gezocht bij dit regime?

[1] Kamerstukken 26 671.

De leden van de commissie zien de antwoorden op bovenstaande vragen met belangstelling tegemoet.

De voorzitter van de commissie voor Justitie,
Van de Beeten

De griffier van de commissie voor Justitie,
Kim van Dooren