

Opmerkingen bij het wetsvoorstel

Wet bewaarplicht telecommunicatiegegevens

Er is nog steeds veel discussie over de verplichting voor telecom- en internetaanbieders om telecomgebruiksgegevens te bewaren, ten behoeve van het onderzoek naar, en de opsporing en vervolging van ernstige criminaliteit. Eerder plaatsten wij in dit tijdschrift kritische kanttekeningen bij een voorstel voor een richtlijn dat een dergelijke verplichting in de lidstaten beoogde te introduceren. In deze bijdrage een bespreking van het wetsvoorstel en de daarin gemaakte keuzes.

**Gerrit-Jan Zwenne &
Aernout Schmidt***

Inleiding

In september 2005 plaatsten wij kritische kanttekeningen bij de eerste voorstellen waarmee de Europese Commissie inder tijd de bewaarplicht wilde introduceren in Europa.¹ Sindsdien is er veel gebeurd. In mei 2006 is de richtlijn, de dataretentierichtlijn 2006/24/EG,² in werking getreden. Vervolgens is een conceptwetsvoorstel³ ter consultatie voorgelegd aan marktpartijen en andere *stakeholders*. Aansluitend is in september 2007 het wetsvoorstel voor de Wet bewaarplicht telecommunicatiegegevens (TK 31 145)⁴ naar het parlement gestuurd, waarover zowel in de Tweede Kamer als daarbuiten⁵ uitvoerig is gediscussieerd.

Onlangs heeft de Tweede Kamer de behandeling van het wetsvoorstel afgerond. Er is een handvol amendementen ingediend, waarvan één – een record? – binnen drie dagen nadat het wetsvoorstel naar de kamer was gestuurd.⁶ Een en ander heeft geleid tot een aantal aanpassingen van het oorspronkelijke voorstel, waarvan verreweg de meeste aandacht is uitgegaan naar het verkorten van de voorgestelde bewaartermijn van 18 tot 12 maanden.

In deze bijdrage bespreken wij het wetsvoorstel en de daarin gemaakte keuzes, alsmede de implicaties daarvan. Onze conclusies stemmen niet bijzonder vrolijk. De bewaartermijn is dan wel verkort, maar daarmee zijn veel van de indertijd door ons geuite zorgen niet weggenomen. Integendeel. Wij stellen vast dat met het wetsvoorstel *de facto*, willens en wetens, grote risico's worden genomen met de rechtsstatelijkheid van ons bestel.⁷

Om de onzekere basis van de richtlijn, en dus ook van het wetsvoorstel, te illustreren, gaan wij in deze bijdrage eerst kort in op de procedure die Ierland is begonnen bij het Europees Hof van Justitie (EHvJ) over de juridische grondslag van de richtlijn. Vervolgens bespreken wij het wetsvoorstel en geven wij aan wat naar onze mening daaraan opmerkelijk is. Wij sluiten dan af met korte samenvatting van wat wij zien als opmerkelijkheden.

Grondslag: harmonisering of handhaving?

De grondslag van de richtlijn ligt in artikel 95 van het EG-verdrag. Deze bepaling ziet op het nemen van maatregelen inzake de onderlinge aanpassing (d.w.z. harmonisering) van

* Prof. mr. A.H.J. Schmidt is directeur van eLaw@Leiden, centrum voor recht in de informatiemaatschappij van de Universiteit Leiden, alsmede fellow bij het E.M. Meijers Instituut, het onderzoeksinstituut van de Leidse rechtenfaculteit. Mr. G.-J. Zwenne is advocaat bij Bird & Bird in Den Haag. Daarnaast is hij als universitair hoofddocent verbonden aan eLaw@Leiden en fellow bij het E.M. Meijers Instituut.

1 A.H.J. Schmidt & G.-J. Zwenne, 'Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens', *Mediaforum* 2005-9, p. 292-302.

2 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *PbEG* 13 april 2006, L105/54-62.

3 Zie de website van het Ministerie van Economische Zaken: www.ez.nl in de rubriek 'onderwerpen' onder 'elektronische communicatie' en vervolgens 'wet- en regelgeving'.

4 Voluit: 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), *Kamerstukken II* 2007-2008, 31 145, nrs. 1-14.

5 Zie bijv. H. Franken, 'Wie wat bewaart heeft wat', *RM Themis* 2007/4, p. 125-126; 'Vrijwillig op weg naar de politiestaat', *NRC Handelsblad* 2 april 2008; 'Niets verkeerd met bewaren van telefoongegevens', *NRC Handelsblad* 7 april 2008; 'Data retentie helpt nauwelijks' *NRC Handelsblad* 10 april 2008.

6 *Kamerstukken II* 2006-2007, 31 145, nr. 6.

7 Wij zien dit bevestigd in recente rechtspraak uit Duitsland, waarin de rechter overging tot een vergaande beperking van de mogelijkheden voor autoriteiten om gebruik te maken van de bewaarde telecomgegevens, zie: Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08; zie daarover *Kamerstukken II* 2006-2007, 31 145, nr. 13 (Amendement Pechtold) en *Hand. II* 2007-2008, nr. 83, p. 5808, 5824, alsmede *Aanl. hand. II* 2007-2008, nr. 1898.

wettelijke en bestuursrechtelijke bepalingen die de werking van de interne markt betreffen. Een voor de hand liggende vraag is of de richtlijn wel echt beoogt een bijdrage te leveren aan de totstandkoming van de interne markt, ofwel de vraag of de gemeenschapswetgever de bewaarplicht inderdaad kan invoeren door middel van een richtlijn gebaseerd op voor- noemde bepaling uit het verdrag.

De opstellers van de richtlijn menen, uiteraard, van wel. In de preambule van de richtlijn wordt gezegd dat er sprake is van:

...aanzienlijke [...] juridische en technische verschillen tussen de nationale bepalingen op het gebied van het bewaren van gegevens ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

Vervolgens stelt de preambule, zonder enige toelichting, dat deze ‘aanzienlijke verschillen’ de werking van de interne markt voor elektronische communicatie belemmeren, omdat:

[d]e aanbieders van diensten immers worden geconfronteerd met uiteenlopende voorschriften wat betreft de categorieën te bewaren verkeers- en locatiegegevens, de bewaringsvoorwaarden en bewa- ringstermijnen.

Erg overtuigend is dat niet. Uiteenlopende voorschriften zien wij overal en zijn als zodanig zelden voldoende reden om over te gaan tot harmonisatie. Ook lijkt de ruime bandbreedte die de richtlijn geeft, zich niet te verhouden met harmonise- ring. Wie zich verdiept in de richtlijn krijgt het gevoel dat deze beoogt de veiligheid te bevorderen, en niet verschillen in nati- onale wetten beoogt weg te werken. Als dat zo is past de in de richtlijn geregelde bewaarplicht niet zozeer in de zogenoemde eerste pijler (interne markt) maar veeleer in de derde pijler (vei- ligheid).⁸

Wat dat kan betekenen blijkt uit het bekende passagiersge- gevensarrest van het Europees Hof van Justitie.⁹ In dit arrest ging het om de doorgifte van deze gegevens door luchtvaart- maatschappijen aan de VS voor het bestrijden van terrorisme. Het Hof oordeelde dat deze doorgifte plaatsvond ter waarbor- ging van de openbare veiligheid en de wetshandhaving, en dus niet om de werking van de interne markt te verbeteren. Volgens het Hof deed daar niet aan af dat de gegevens waren verzameld in het kader van de dienstverlening van de vliegtuigmaat- schappijen. Om deze reden kon de voor deze gegevens getrof- fen regeling niet worden gebaseerd op een grondslag in de eer- ste pijler.

Waar het gaat om de bewaarplicht van telecommunicatie- gegevens lijkt dat niet anders. De telecomgegevens zijn welis- waar verzameld in het kader van de telecomdienstverlening, maar de richtlijn verlangt dat ze worden bewaard en beschik- baar gehouden voor veiligheids- en handhavingdoeleinden. De grondslag daarvoor ligt daarom niet in de eerste, maar in de derde pijler. Dat is, in het kort, wat Ierland heeft betoogd

in de procedure die deze lidstaat bij het Hof heeft ingesteld.¹⁰ En, zoals bij de passagiersgegevens, lijkt het niet uitgesloten dat het Hof oordeelt dat er een andere grondslag moet worden gevonden voor het invoeren van de bewaarplicht in de lidsta- ten.

Als wij uitgaan van wat er gebeurde in de passagiersgege- venszaak, wordt de dataretentierichtlijn, die dan allang in de lidstaten had moeten zijn geïmplementeerd, nietig verklaard. Echter, of dat tot een resultaat zal leiden dat beter aan onze zor- gen tegemoet komt, moet worden betwijfeld. Het alternatief zou, zoals eerder geprobeerd, wel weer eens een zogenoemde kaderbesluit kunnen zijn.¹¹ En daarop valt in termen van priva- cybescherming, rechtstatelijkheid en democratische legitime- ring veel aan te merken.¹²

Het wetsvoorstel

Het wetsvoorstel strekt tot implementatie van de datare- tentierichtlijn. Zoals gezegd beoogt deze richtlijn, volgens de opstellers ervan, te komen tot harmonisatie van de wettelijke bepalingen waarbij aan aanbieders van elektronische commu- nicatiediensten of -netwerken verplichtingen worden opge- legd inzake het bewaren van bepaalde telecomgegevens – dit om te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige crimina- liteit, zoals gedefinieerd in de nationale wetgevingen van die lidstaten. De richtlijn en het wetsvoorstel willen dus zekerstel- len dat politie, justitie en inlichtingendiensten (in het jargon: ‘de behoeftestellers’) kunnen beschikken over bel- en internet- gegevens van telecomgebruikers, als ze deze nodig hebben om ernstige misdrijven aan te pakken.

Welke gegevens moeten worden bewaard?

De richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke personen en rechtspersonen, alsmede op de daarmee verbundene houdende gegevens die nodig zijn om abone- nes of geregistreerde gebruikers te identificeren.¹³ Het gaat om de gegevens over de communicatie, en niet over de inhoud daarvan.¹⁴ Dus niet om wát allemaal in uw telefoongesprek is gezegd, maar om de datum en het tijdstip waarop u belde, hoe- lang uw gesprek duurde, het nummer van degene met wie u belde, enz. Bij mobiele gesprekken gaat het om gegevens over de locatie van uw handset (zgn. CellID). En bij internetgebruik gaat het om log-in en log-off gegevens, IP-adressen en derge- lijke.

Voor een overzicht van de gegevens die volgens de richtlijn moeten worden bewaard, verwijzen wij naar het overzicht in de tabel [zie p. 280].

In de richtlijn wordt duidelijk gemaakt dat deze communica- tiegegevens betrekking kunnen hebben op zowel abonnees als gebruikers. Voor de omschrijving van de ‘abonnee’ wordt uit-

8 Zie hierover uitgebreid: F. Bignami, ‘Privacy and Law Enforcement in the Euro- pean Union: The Data Retention Directive’, *Chicago Journal of International Law*, Vol. 8 No. 1, October 2007, p. 233-255.

9 EHVJ 30 mei 2006, C317/04 en C-318/04; daarover: P. De Hert & G-J. Zwenne, ‘Over passagiersgegevens en preventieve misdaadbestrijding binnen de Euro- pese Unie’ *NJB* 2007/27, p. 1662-1679.

10 Het beroep heeft zaaknummer C-301/06 en is op 6 juli 2006 ingesteld bij het Hof.

11 Draft Framework Decision on the retention of data processed and stored in

connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of preven- tion, investigation, detection and prosecution of crime and criminal offences including terrorism, 28 April 2004.

12 Vgl. P. Blok, ‘Rechtszaak van het Europees Parlement is geen zegen voor privacy van de luchtvaartreiziger’, *NJB* 2006/23, p. 1367; zie ook onze opmerkingen over het ontwerp kaderbesluit in: Schmidt & Zwenne 2005, p. 292-302.

13 Art. 1, tweede lid, richtlijn.

14 Art. 1, tweede lid, en art 5, tweede lid, richtlijn.

Tabel I: Overzicht van te bewaren gegevens (o.g.v. art. 5, eerste lid, richtlijn en art. 13.2a, tweede lid, j° bijlage, wetsvoorstel)

| | vaste telefonie | mobiele telefonie | internettoegang, e-mail, internettelefonie |
|---|--|---|--|
| a) bron van de communicatie | <ul style="list-style-type: none"> • telefoonnummer van oproeper • naam en adres van abonnee of geregistreerde gebruiker • in geval van call forwarding of call transfer: ook het nummer waarnaar de oproep is doorgeleid | <ul style="list-style-type: none"> • telefoonnummer van oproeper • naam en adres van abonnee of geregistreerde gebruiker • in geval van call forwarding of call transfer: ook het nummer waarnaar de oproep is doorgeleid*) | <ul style="list-style-type: none"> • toegewezen gebruikersidentificatie(s) • gebruikersidentificatie en telefoonnummer toegewezen aan communicatie die publieke telefoonnetwerk binnenkomt • naam en adres van de abonnee of de geregistreerde gebruiker aan wie het IP-adres, de gebruikersidentificatie of het telefoonnummer was toegewezen op het tijdstip van de communicatie |
| b) bestemming van de communicatie | <ul style="list-style-type: none"> • opgeroepen telefoonnummers incl. de nummers waarnaar werd doorgeleid in geval van call forwarding of call transfer • naam (namen) en adres(sen) van abonnee(s) en geregistreerde gebruiker(s) | <ul style="list-style-type: none"> • opgeroepen telefoonnummers incl. de nummers waarnaar werd doorgeleid in geval van call forwarding of call transfer • naam (namen) en adres(sen) van abonnee(s) en geregistreerde gebruiker(s) | <ul style="list-style-type: none"> • de gebruikersidentificatie of telefoonnummer van beoogde ontvanger(s) van internet-telefoonoproep, • naam (namen) en adres(sen) van abonnee(s) of geregistreerde gebruiker(s) en gebruikersidentificatie van de beoogde ontvanger van de communicatie |
| c) datum, tijdstip en duur van de communicatie | <ul style="list-style-type: none"> • datum en tijdstip van aanvang en einde van de verbinding | <ul style="list-style-type: none"> • datum en tijdstip van aanvang en einde van de verbinding | <ul style="list-style-type: none"> • datum en tijdstip van log-in en log-off van internetessie gebaseerd op bepaalde tijdzone, samen met (statisch of dynamisch) IP-adres, dat door de aanbieder van internettoegangsdienst aan communicatie is toegewezen, en gebruikersidentificatie van de abonnee of geregistreerde gebruiker • datum en tijdstip van log-in en log-off van e-maildienst of internettelefoniedienst gebaseerd op bepaalde tijdzone |
| d) type van de communicatie | <ul style="list-style-type: none"> • de gebruikte telefoondienst | <ul style="list-style-type: none"> • de gebruikte telefoondienst | <ul style="list-style-type: none"> • i.g.v. e-mail en internet-telefonie: de gebruikte internetdienst |
| e) (vermoedelijke) apparatuur | <ul style="list-style-type: none"> • oproepende en opgeroepen nummer(s) | <ul style="list-style-type: none"> • oproepende en opgeroepen nummer(s) • International Mobile Subscriber Identity (IMSI) van oproepende en opgeroepen deelnemer • International Mobile Equipment Identity (IMEI) van oproepende en opgeroepen deelnemer • in geval van vooraf betaalde, anonieme diensten: datum en tijdstip van de eerste activering van de dienst en aanduiding (CellID) van de locatie van waaruit de dienst is geactiveerd | <ul style="list-style-type: none"> • inbellende nummer voor inbelverbinding, • digital subscriber line (DSL) of ander eindpunt van initiatiefnemer van communicatie |
| f) locatie van mobiele apparatuur | n.v.t. | <ul style="list-style-type: none"> • locatieaanduiding (CellID) bij begin van verbinding • gegevens voor identificatie van geografische cells middels referentie aan hun locatieaanduiding (CellID) gedurende de periode dat de communicatiegegevens worden bewaard • bovenstaande gegevens gedurende de communicatie (EXTRA!) | n.v.t. |

*) De Nederlandstalige versie van de richtlijn vermeldt – naar moet worden verondersteld: ten onrechte – niet dat deze gegevens ook moeten worden bewaard als het gaat om mobiele telefonie; in de anderstalige versies worden deze gegevens zowel bij vaste als mobiele telefonie genoemd.

gegaan van de omschrijving in de kaderrichtlijn (2002/21/EG): ‘abonnee is de natuurlijke of rechtspersoon die partij is bij een overeenkomst met een aanbieder van openbare elektronische communicatiediensten voor de levering van die diensten.’¹⁵ Voor het begrip ‘gebruiker’ gaat de datarentierichtlijn uit van een eigen, ruimere begripsomschrijving dan de kaderrichtlijn: de gebruiker kan in de datarentierichtlijn zowel een natuurlijke persoon zijn als een rechtspersoon, die eventueel zonder geabonneerd te zijn, gebruik maakt van een openbare elektronische communicatiedienst.

Aanvankelijk was de regering van plan om de lijst met te bewaren gegevens op te nemen in een AMvB. In verschillende adviezen over het conceptwetsvoorstel werd daartegen bezwaren geuit. Het College Bescherming Persoonsgegevens (CBP) wees erop dat de gemeenschapswetgever, op uitdrukkelijk verzoek van het Europees Parlement, ervoor heeft gekozen om de te bewaren gegevens in de richtlijn zelf op te nemen, en niet in een bijlage. Ook wees het CBP op de Aanwijzingen voor de regelgeving, waaruit het opmaakt dat de meest gewichtige onderdelen, zoals bij dit wetsvoorstel de te bewaren gegevens, in wet zelf moeten worden vastgelegd.¹⁶

Om aan deze bezwaren tegemoet te komen is in het wetsvoorstel ervoor gekozen om de gegevens op te nemen in een bijlage bij de Telecommunicatiewet. Uit deze bijlage blijkt dat, als het aan de regering ligt, niet alleen de in de richtlijn opgesomde gegevens moeten worden bewaard. In aanvulling op de gegevens over de locatie(s) bij begin en einde van een mobiel gesprek worden in de bijlage ook de locatiegegevens genoemd die worden verwerkt *tijdens* de mobiele communicatie.

In enkele adviezen en reacties¹⁷ over het conceptwetsvoorstel is opgemerkt dat het wetsvoorstel daarmee buiten de reikwijdte van de richtlijn treedt. Volgens het CBP is het bewaren van deze gegevens disproportioneel, omdat dit neerkomt op een indringende, alomvattende surveillance van de verplaatsingen van zeer grote aantallen onverdachte burgers. Verder wijst het CBP erop dat er over dit onderwerp uitgebreid is gediscussieerd in het Europees Parlement, waarna deze gegevens vervolgens niet in de richtlijn zijn opgenomen. En, juist omdat deze gegevens niet zijn opgenomen, komt de Duitse wetgever tot de vaststelling dat de bewaarplicht proportioneel is.

De regering is daarvan niet onder de indruk. In de MvT merkt zij, nogal omstandig, op dat deze gegevens nodig zijn om met behulp van een zogenoemde bestandsanalyse gebruiksgegevens van prepaidbellers te achterhalen. Als de locatiegegevens niet zouden worden bewaard, zegt de regering dreigend, moeten de gebruiksgegevens van prepaidbellers op andere wijze worden achterhaald. En dat kan, bijvoorbeeld, door van de telecomaانبieders te verlangen dat zij de identiteit van deze bellers gaan vastleggen. Ofwel een identificatieplicht voor prepaidbellers.¹⁸

Zo een identificatieplicht staat overigens ook om andere redenen al enige tijd op het wensenlijstje van de behoeftezoekers.¹⁹

In het kader van de voorbereiding van de richtlijn is verder enige discussie geweest over telefoonoproepen die wel tot een verbinding hebben geleid maar onbeantwoord zijn gebleven of via het netwerkbeheer zijn beantwoord. De gegevens over deze ‘oproepingen zonder resultaat’ vallen onder de bewaarplicht, voorzover deze door de aanbieders bij het aanbieden van de elektronische communicatiediensten worden gegenereerd, verwerkt en opgeslagen of gelogd.²⁰ In de MvT wordt daarover opgemerkt dat dergelijke gegevens, voorzover bekend, in Nederland niet worden opgeslagen.²¹ De verplichting tot het bewaren van deze gegevens lijkt derhalve, vooralsnog, niet relevant.

Wat volgens de regering niet hoeft te worden bewaard en vastgelegd, zijn de gegevens over bezochte websites, alsmede gegevens betreffende e-mailberichten die via veel gebruikte webdiensten als Hotmail, Yahoo of Gmail worden ontvangen of verzonden. Hetzelfde geldt voor de communicatie die plaatsvindt via chatwebsites of sociale netwerksites als Hyves of LinkedIn. Over de reden waarom deze gegevens niet onder de bewaarplicht zouden vallen is de parlementaire geschiedenis niet erg duidelijk. In het debat merkt de minister op dat de Telecommunicatiewet alleen van toepassing is op openbare telecommunicatiediensten en/of -netwerken. Verder geeft hij aan dat bedrijfsmail en voornoemde webmaildiensten niet vallen onder de werking van de Nederlandse Telecommunicatiewet.²²

Voorzover het gaat om bedrijfsmail kunnen wij dit volgen. In de parlementaire geschiedenis wordt wellicht bedoeld te zeggen dat berichten die binnen een bedrijfsnetwerk worden uitgewisseld geen openbaar karakter hebben – er kan alleen gebruik van worden gemaakt door werknemers binnen een bedrijf – en dat zou inderdaad betekenen dat die berichten niet onder de werking van de wet vallen.²³ Voorzover het gaat om de webmaildiensten is niet helemaal duidelijk waarom de minister meent dat de bewaarplicht niet zou gelden. Veel van deze diensten hebben zonder meer een openbaar karakter, en dat kan dus niet de reden zijn waarom deze niet onder de wet zouden vallen. En anders dan in de parlementaire geschiedenis wel wordt gesuggereerd is het ook niet per se zo dat dit geen telecommunicatiediensten zijn²⁴ en daarom niet onder de wet vallen.²⁵ Evenmin is het altijd zo dat de Nederlandse telecommunicatiewetgeving niet van toepassing zou kunnen zijn op buitenlandse aanbieders of op diensten die vanuit het buitenland worden aangeboden.²⁶ Als deze diensten in Nederland worden aangeboden, kan de wet van toepassing zijn, zij het dat de uitvoerbaarheid en handhaving in de praktijk zeer lastig (zometer onmogelijk) zal zijn. Ook niet helemaal juist lijkt de suggestie dat het niet direct relevant is of de diensten gratis worden aangeboden.²⁷ Onjuist, omdat de wet van toepassing

15 Art. 2, eerste lid, richtlijn j° art. 2, onder k, van de kaderrichtlijn (2002/21/EG).

16 *Kamerstukken II 2006-2007*, 31 145, nr. 3, p. 37; Advies van het CBP 22 januari 2007.

17 Zie m.n. Advies van ACTAL van 18 januari 2008, p. 3; Reactie van Telecomaانبieders van 18 januari 2008, p. 5; Advies van het CBP van 22 januari 2007, p. 7.

18 *Kamerstukken II 2006-2007*, 31 145, nr. 3, p. 9-10 en 38 alsmede nr. 9, p. 22-23.

19 Zie ‘Identificatie bij prepaid bellen nodig’ en ‘Identificatie bij prepaid bellen zinloos’ *NRC Handelsblad* resp. 9 en 10 mei 2008; alsmede R. D. Chavannes, ‘Veel taps, weinig verantwoording’, *Mediaforum* 2008-6, p. 245.

20 Art. 3, tweede lid, richtlijn; zie daarover ov. 12 van de richtlijn.

21 *Kamerstukken II 2006-2007*, 31 145, nr. 3, p. 46-47.

22 *Kamerstukken II 2006-2007*, 31 145, nr. 3, p. 37, nr. 8, p. 5, nr. 9, p. 6, alsmede *Hand.*

II 2006-2007, nr. 83, p. 5836-5837, 5843-5845.

23 Zie H. Dries, S. Gijrath en P.C. Knol, *Openbaarheid van netwerken en diensten in de Telecommunicatiewet*, Den Haag: Sdu Uitgevers 2003.

24 *Hand. II 2006-2007*, nr. 83, p. 5835.

25 Het criterium is of het al dan niet gaat om een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, zijnde transmissiesystemen die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, ongeacht de aard van de overgebrachte informatie. Zie art. 1.1, onder e en f, Tw.

26 Vgl. *Hand. II 2006-2007*, nr. 83, p. 5836.

27 *Kamerstukken II 2006-2007*, 31 145, nr. 9, p. 6.

is op diensten die ‘gewoonlijk tegen vergoeding worden aangeboden’,²⁸

Over een en ander valt nog heel veel meer te zeggen, maar dat doen wij hier niet.²⁹ Wij volstaan met de vaststelling dat niet duidelijk blijkt wie onder de bewaarplicht vallen, en wie niet. Wij menen dat daaraan niet gemakkelijk voorbij kan worden gegaan. De bewaarplicht betekent vergaande inbreuken op de persoonlijke levenssfeer van veel, heel veel gebruikers en verlangt een niet geringe inspanning van telecoaanbieder en ISP's. En dan mag worden verwacht dat de wet voldoende bepaald is – al was het maar als vereiste van fatsoenlijke wetgeving.³⁰ Verder zijn er natuurlijk vragen over effectiviteit en, daarmee verband houdend, vragen over proportionaliteit van de bewaarplicht. Hoe effectief is een wet als die, om wat voor reden dan ook, niet van toepassing kan zijn op (en/of niet uitvoerbaar is door) aanbieders van veelgebruikte alternatieve diensten?³¹

Daar komt bij dat de integriteit en authenticiteit van de te bewaren gegevens niet altijd zo zeker is als wordt verondersteld. Het gaat om gegevens waarvan wij weten dat de kwaliteit, in eventuele bewijsvoering achteraf, maar ook bij verstoringen vooraf, kwetsbaar is. Het is bekend dat de telecom- en internet-infrastructuren (nog) niet goed zijn te beveiligen tegen identiteitsfraude ('spoofen'). De vraag is dan hoe te bewijzen dat u niet op de plaats delict was als uw mobiele telefoon is gestolen? Of hoe kunt u aantonen dat een e-mailbericht niet door uzelf, maar door een ander werd verzonden?

Hoelang moeten de gegevens worden bewaard?

De bewaartermijn is, misschien niet helemaal onterecht, tot dusver het meest bediscussieerde onderwerp van het wetsvoorstel. De richtlijn geeft de bandbreedte: de gegevens moeten minimaal zes en maximaal 24 maanden worden bewaard, waarbij de termijn begint te lopen op het moment dat de gegevens zijn gegenereerd (of eigenlijk: 'vanaf het tijdstip waarop deze gegevens voor de eerste maal zijn verwerkt').³² In het oorspronkelijke wetsvoorstel zette de regering in op 18 maanden.³³ Vanuit de Tweede Kamer werd vrijwel direct aangedrongen op zes maanden.³⁴ Uiteindelijk is het, na enige discussie in de krant en parlement, 12 maanden geworden.³⁵ Alles overziend lijkt het dat de voor- en tegenstanders van een langere bewaartermijn elk zes maanden hoger respectievelijk lager hebben ingezet, om uit te komen op de termijn van een jaar, waar de meeste lidstaten voor lijken te gaan kiezen.³⁶

Op welke wijze moeten de gegevens worden bewaard?

De richtlijn laat in het midden *hoe* de gegevens moeten worden bewaard. Waar het de richtlijn om gaat is dat de gegevens beschikbaar zijn voor politie, justitie en inlichtingendiensten ten behoeve van het onderzoek naar en opsporing en vervolging van ernstige criminaliteit. Hoe de lidstaten dat regelen mogen zij zelf bepalen. In de preambule geeft de richtlijn wel aan dat moet worden voorkomen dat dezelfde gegevens dubbel worden bewaard.³⁷ Tegelijkertijd stelt de richtlijn nadrukkelijk dat niet wordt beoogd om de technologie voor de bewaring van de gegevens te harmoniseren: de keuze van deze technologie moet door de lidstaten worden gemaakt.³⁸

In het wetsvoorstel zelf is over de wijze van bewaren niets bepaald. Wel voorziet het in de mogelijkheid van een AMvB, waarin regels worden gesteld met betrekking tot de wijze waarop de gegevens beschikbaar worden gehouden. Vooral nog lijkt daarbij het uitgangspunt te zijn dat de aanbieders de gegevens kunnen bewaren op de voor hen minst belastende wijze. Aanbieders hebben zo de mogelijkheid om de implementatie maximaal te laten aansluiten bij hun huidige werkwijze.

Deze keuze voor decentrale opslag lijkt niet zozeer ingegeven door principiële overwegingen – bijvoorbeeld met betrekking tot de mogelijkheden van aanbieders om enig zicht te hebben op de omvang van het gegevensgebruik door behoeftestellers,³⁹ maar vooral om praktische redenen: behalve dat daarmee het draagvlak voor het voorstel bij aanbieders wordt verbreed, zou de implementatie anders ook veel te lang gaan duren. Volgens de MvT is tijdige implementatie alleen mogelijk als wordt uitgegaan van decentrale opslag.⁴⁰ Voor andere oplossingen (lees: centrale opslag) wordt uitvoerig overleg en afstemming voorzien over de technische en organisatorische aspecten, en dan wordt zeker de in de richtlijn gestelde implementatietermijn bij lange na niet gehaald.

Overigens: veel lidstaten hebben gebruik gemaakt van de in artikel 15, derde lid, van de richtlijn geboden mogelijkheid om de implementatie van de verplichting voor internetgebruiksgegevens met 18 maanden uit te stellen, te rekenen vanaf 15 maart 2009. Om onduidelijke redenen heeft Nederland er evenwel voor gekozen voor een uitstel van ten hoogste 18 maanden, te rekenen de datum van de *inwerkingtreding van de richtlijn*, wat neerkomt op een uitstel van enige maanden. Volgens onze berekening had Nederland deze verplichting uiterlijk begin november 2007 in nationale wetgeving moeten omzetten.

28 Een van de criteria is of de dienst 'gewoonlijk tegen vergoeding wordt aangeboden'; zie weer art. 1.1, onder e en f, Tw.

29 Vgl. onze opmerkingen over openbare karakter van telecomdiensten als die van Wireless Leiden en Surfnet, in Schmidt & Zwenne 2005, p. 297.

30 In Schmidt & Zwenne 2005, p. 297, voetnoot 49, wezen wij op de volgende, nog steeds actuele overweging van het Europees Hof voor de Rechten van de Mensen in het bekende Sunday Times-arrest: '... a norm cannot be regarded as a "law" unless it is formulated with sufficient precision. To enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail'; aldus EHRM 26 april 1979, NJ 1980, 146, NJCM-bulletin 1979, p. 62-63.

31 Hand. II 2006-2007, nr. 83, p. 5836.

32 Art. 13.4, eerste lid, onder c, Tw.

33 In het Advies van het CBP van 22 januari 2008, p. 3-4, wordt erop gewezen dat het geconsulteerde conceptwetsvoorstel op enkele plaatsen nog uitgaat van een bewaartermijn van 12 maanden, welke termijn aansluit bij eerdere toezeggingen van de minister.

34 Kamerstukken II 2006-2007, 31 145, nr. 6 (Amendement Pechtold).

35 Kamerstukken II 2006-2007, 31 145, nr. 14 (Amendement Anker).

36 Vgl. Hand. II 2007/08, 83, p. 5844-5845; zie verder ook Kamerstukken II 2006-2007, 31 145, nr. 5, p. 2-3.

37 Ov. 13 van de richtlijn.

38 Ov. 23 van de richtlijn.

39 Vgl. Advies CBP van 22 januari 2007.

40 Kamerstukken II 2006-2007, 31 145, nr. 3, p. 16.

Aanbieders kunnen dus vooralsnog de gegevens bewaren op de wijze van hun keuze. Het wetsvoorstel neemt daarmee – op het eerste gezicht – afstand van de benadering die bij eerdere gelegenheden wel door de minister werd verdedigd en waarbij de gegevens centraal worden opgeslagen. In dit model zouden de gegevens regelmatig (zeg: dagelijks) door aanbieders worden geupload naar een centrale databank. Vervolgens zouden de bevoegde autoriteiten, de zogenoemde behoeftezoekers, de gegevens daar weer uithalen als zij deze nodig hebben.

In dit centrale model zou kunnen worden gekozen voor een *blackbox*-benadering, waarbij de aanbieders niet weten wat er gebeurt met de door hen aangeleverde gegevens en dus niet kunnen weten naar wie de behoeftezoekers onderzoek doen. Een dergelijke benadering heeft, vanuit het perspectief van de behoeftezoekers, het voordeel dat onderzoeken eenvoudiger geheim kunnen worden gehouden. Een ander voordeel is dat het, in elk geval voor de behoeftezoekers, veel efficiënter zal zijn om de gegevens via een eenvormige (geautomatiseerde) procedure uit een centrale databank te halen, in plaats van het telkens opvragen bij verschillende aanbieders. Om deze reden wordt dit centrale opslagmodel gebruikt bij de al enige tijd geldende beperkte bewaarplicht voor gegevens over mobiele abonnees.⁴¹ In zijn advies over het concept-wetsvoorstel dringt het College van Procureurs Generaal dan ook aan op zo een centraal opslagmodel.

Het CBP is het daar niet mee eens. In zijn advies op het conceptwetsvoorstel wijst het erop dat de richtlijn vereist dat wordt voorkomen dat gegevens twee keer worden bewaard. Het redeneert vervolgens er bij een centrale opslagmodel sprake zal zijn van dubbele opslag, omdat dat aanbieders de gegevens zelf ook moeten opslaan ten behoeve van de eigen bedrijfsvoering. Ons komt deze redenering voor als een niet ongevaarlijke juridisch-technische ‘vondst’, die moeilijk houdbaar is.⁴² Ook gaat deze redering voorbij aan de werkelijke risico’s van centrale opslag. Deze risico’s volgen uit de bekende juridisch-politieke adagia: ‘kennis is macht’ en ‘macht corrupteert’ wanneer die niet in evenwicht wordt gehouden. De centrale opslag van telecomgegevens, gekoppeld aan ontoereikend toezicht (waarover later meer) vormen een gevaar voor de democratische rechtsstaat – ook wanneer dat gevaar democratisch wordt gedoogd. Of, nauwkeuriger: juist dan.

De overwegingen waarom in het wetsvoorstel is gekozen voor decentrale opslag geven overigens weinig vertrouwen dat niet op enig moment, zodra de opwindingsfase over het wetsvoorstel wat is afgenomen, toch nog wordt gekozen voor gecentraliseerde opslag en een *blackbox*-model voor het gegevensgebruik door behoeftezoekers.

Het meest opmerkelijke is dan dat wij hebben te maken met een wetsvoorstel over het bewaren van verkeersgegevens, waaruit niet – ook niet nadat dit door de Tweede Kamer is behandeld – kan worden gelezen op welke wijze de gegevens moeten worden bewaard en beschikbaar gesteld.

Aan wie moeten de gegevens worden verstrekt en voor welke criminaliteit?

De te bewaren gegevens moeten, aldus artikel 1, eerste lid, van de richtlijn, beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, zoals gedefinieerd in de nationale wetgeving. Verder stelt artikel 4 van de richtlijn dat de gegevens slechts aan ‘bevoegde nationale autoriteiten’ worden verstrekt, en dat dan alleen ‘in welbepaalde gevallen’.⁴³ Van belang is wat hier moet worden begrepen onder ‘ernstige criminaliteit’, ‘bevoegde nationale autoriteiten’ en onder ‘welbepaalde gevallen’. Wij lopen een en ander af.

Ernstige criminaliteit

De gegevens moeten beschikbaar zijn voor ‘ernstige criminaliteit’. Daaronder worden de misdrijven verstaan bedoeld in artikel 67, eerste lid, Wetboek van Strafrecht (Sr). Ofwel de misdrijven waarop een gevangenisstraf staat van 4 jaar of meer, én een aantal andere misdrijven, zoals onder andere het verspreiden van opruiende geschriften (art. 132 Sr), computervredbreuk (art. 138a Sr), heling (art. 417bis Sr), schuldwitwassen (art. 420quater Sr) en dergelijke. Het gaat dus, zoals ook in het parlement werd opgemerkt,⁴⁴ niet alleen om terrorisme of zeer ernstige criminaliteit.

Bevoegde nationale autoriteiten

De gegevens mogen alleen aan ‘bevoegde nationale autoriteiten’ worden verstrekt. Er lijkt weinig twijfel over te kunnen zijn dat onder ‘de bevoegde nationale autoriteiten’ alleen politie, justitie en inlichtingendiensten kunnen worden verstaan. Een andere, ruimere uitleg verhoudt zich slecht met de tekst van artikel 4 van de richtlijn, alsook met de verwijzingen in het wetsvoorstel naar bepalingen in het Wetboek van Strafvordering en de Wet op de inlichtingen- en veiligheidsdiensten 2002. Uitgesloten is dus de verstrekking aan (vertegenwoordigers van) auteursrechthebbers, die de gegevens wellicht goed kunnen gebruiken om illegale uploaders aan te pakken.⁴⁵ Een interessante, nog onbeantwoorde vraag is in hoeverre het wetsvoorstel daarmee een einde zou kunnen maken aan de praktijk waarbij internetaanbieders onder bepaalde voorwaarden gehouden zijn gegevens over hun abonnees te verstrekken aan voornoemde auteursrechtenorganisaties.⁴⁶

Welbepaalde gevallen

De gegevens mogen slechts ‘in welbepaalde gevallen’ worden verstrekt. In het kader van de privacywetgeving, met name artikel 7 van de Wet bescherming persoonsgegevens, is een vergelijkbaar welbepaaldheidsvereiste ingevuld. Het komt erop neer dat voldoende duidelijk moet zijn wanneer er gegevens moeten worden verstrekt, en wanneer niet. Anders gezegd, er moet sprake zijn van een zeker kader waarbinnen kan worden getoetst of de gegevens nodig zijn, of niet.⁴⁷

41 Besluit bijzondere vergaring nummergegevens, *Stb.* 2002, 31.

42 Wie verkeersgegevens moet bewaren moet – in termen van databases – een of meer tabellen genereren, waarin de verkeersgegevens van berichten wel beschikbaar zijn, maar de inhoud niet. Dit impliceert hoe dan ook een noodzakelijke verdubbeling, ook bij de aanbieders, met name wanneer deze de logs voor de bedrijfsvoering korter willen bewaren dan de wettelijke termijn voor verkeersgegevens voorschrijft.

43 *Kamerstukken II* 2006–2007, 31 145, nr. 3, p. 10.

44 *Hand. II* 2006–2007, 31 145 nr. 83, p. 5813.

45 Zie G.-J. Zwenne, ‘Annotatie bij EHVJ 29 januari 2008, C-275/06 (*Promusicae/Telefónica*)’, *Tijdschrift voor internetrecht* 2008/2, p. 42–44.

46 HR 25 november 2005 LJN AU4019.

47 Vgl. De Vries (*T&C Telecommunicatiericht*) art. 7 Wbp, aant. 1a.

In het parlementaire debat vult de minister dit in. Op de vraag wat heeft te gelden als een welbepaald geval geeft hij het volgende antwoord:

Een verkennend onderzoek, in verband met aanwijzingen van het beramen of plegen van terroristische misdrijven, kan naar mijn oordeel worden beschouwd als een welbepaald geval, als bedoeld in de richtlijn.⁴⁸

Aangenomen mag worden dat dergelijke ‘aanwijzingen’ kunnen worden geconcretiseerd en zonodig geverifieerd. Uiteindelijk zal de telemaanbieder toch op de een of andere manier moeten kunnen nagaan of er voldoende grond is om de gegevens aan een behoeftesteller te verstrekken. De vraag is dan of de aanbieder dat inderdaad zal kunnen doen, in aanmerking nemend dat behoeftestellers niet vanzelfsprekend geneigd zullen zijn om aan te geven naar wie onderzoek wordt gedaan en waarom. Ook om deze reden ligt het voor de hand dat, vanuit die behoeftestellers, op enig moment toch wordt aangestuurd op de centrale opslag met blackbox-karakter, waarover wij in het voorgaande al spraken.

Van belang is dan om – al was het maar uit overwegingen van efficiëntie – in de toekomst een centraal verificatiepunt in het leven te roepen en om een wettelijke grondslag te scheppen die het CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) tot contactpunt tussen informatievrager en aanbieder laat zijn, en deze met de nodige bevoegdheid bekleedt. Een probleem daarbij zal zijn dat het CIOT, als onderdeel van het ministerie van Justitie, controles moet inbouwen op de operationele taakuitvoering van datzelfde ministerie, van welke taakvoering de inhoud vooralsnog onduidelijk is. Het risico is dan dat de specificatie en bijbehorende automatisering van deze taakvoering ofwel te hoog gegrepen blijken, ofwel worden overgelaten aan de discretie van systeemontwerpers.

In zijn algemeenheid is het opmerkelijk dat bij de behandeling van het wetsvoorstel nauwelijks aandacht is besteed aan de conclusies uit het in augustus 2007 uitgebrachte rapport ‘Data voor daadkracht’, dat op uitnodiging van de Minister van Binnenlandse Zaken is samengesteld door de daartoe ingestelde commissie.⁴⁹ Van belang zijn vooral de volgende conclusies daaruit:

(1) Gegevens in externe gegevensbestanden hebben in de afgelopen decennia een steeds grotere betekenis voor het veiligheidsdomein gekregen. Desondanks krijgt het proces van inwinnen van gegevens uit die bestanden door inlichtingen- en opsporingsdiensten weinig tot geen bestuurlijke en politieke aandacht.

(17) Het complex van deelsystemen voor het inwinnen van gegevens uit externe databases voldoet niet aan de daaraan te stellen normen van grondslag en vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid.

Opmerkelijk is dan ook dat het wetsvoorstel niet voorziet in de opheldering van essentiële onduidelijkheden over (i) het door de aanbieders te maken onderscheid tussen legitieme en illegitieme informatievragen en (ii) de kwaliteitsbewaking van de eigen informatiehuishouding.

48 Kamerstukken II 2007-2008, 31 145, nr. 9, p. 30.

49 Kamerstukken II 2006-2007, 30 800 VII, nr. 65; Zie de website van het ministerie van Binnenlandse Zaken www.minbzk.nl zoekterm ‘datavoordaadkracht’.

50 Kamerstukken II 2006-2007, 31 145, nr. 3, p. 16 en 50; zie ook het Advies van het CBP van 20 januari 2008, p. 9; Advies van College van Procureurs Generaal van 9 februari 2008, p. 3-4.

51 Aldus ook de slotline van Advies van College van Procureurs Generaal van 9

Wat is de leveringstermijn?

In de richtlijn staat dat de bewaarde gegevens ‘onverwijld’ aan de bevoegde autoriteiten moeten worden verstrekt als deze daarom verzoeken. Het wetsvoorstel vult dit niet nader in. Evenals de richtlijn stelt het voorgestelde artikel 13.4, eerste lid, dat aanbieders onverwijld voldoen aan vorderingen tot het verstrekken van de gegevens. Wat dat in de praktijk betekent is afhankelijk van de afspraken tussen openbaar ministerie, politie en de inlichtingen- en veiligheidsdiensten enerzijds en de aanbieders. En die zijn, aldus de MvT, bepalend, vooral afhankelijk van de aard van de gegevens, de inrichting van de bedrijfsvoering en de staat van de techniek in het bedrijf van de betreffende aanbieder.

Aan het voorschrijven van dwingende leveringstermijnen zijn extra administratieve lasten verbonden. Om deze reden wordt het begrip ‘onverwijld’ in dit verband gemakshalve opgevat als ‘zo spoedig als de inrichting van de bedrijfsvoering en de stand der techniek van het betreffende bedrijf dat mogelijk maakt’. In de MvT wordt nog wel opgemerkt dat volgens de huidige afspraken de gegevens in beginsel binnen vijf dagen worden geleverd en in noodgevallen zo spoedig mogelijk.⁵⁰

Over de leveringstermijn valt overigens op te merken dat deze, waar het gaat om geautomatiseerde processen, in de praktijk weinig echte beperkingen hoeft op te leveren.⁵¹

Wie betaalt dit allemaal?

De vraag naar wie wat betaalt pleegt tot de belangrijkste onderwerpen van de Nederlandse politiek te worden gerekend. Ook in de discussies over de bewaarplicht is dit een belangrijk onderwerp gebleken. Er is veel over gezegd en er valt ongetwijfeld nog wel meer over te zeggen.⁵² Duidelijk is en blijft dat de kosten hoe dan ook uiteindelijk worden afgewenteld op de consument of belastingbetaler, wat vaak verschillende aanduidingen zijn voor een en dezelfde persoon. Om deze reden gaan wij daarop thans niet verder in.

Toezicht en terugkoppeling

Belangrijker vraagstukken lijken ons het ‘onafhankelijke toezicht’ dat in art. 9 van de richtlijn wordt voorgeschreven en de ‘statistische informatie’ die volgens artikel 10 van de richtlijn jaarlijks moet worden teruggekoppeld naar de Commissie.

Het onafhankelijke toezicht lijkt – volgens het wetsvoorstel – te worden opgedragen aan het Agentschap Telecom, een onderdeel van het Ministerie van Economische zaken dat zich vooralsnog naar eigen zeggen vooral bezighoudt met de frequentieruimte. Het is blijkens de navolgende citaten nog niet erg ingesteld op de komende taakverzwaring:⁵³

De drie hoofdtaken van Agentschap Telecom zijn het verwerven, uitgeven en beschermen van frequentieruimte.

februari 2008, p. 4.

52 Vgl. Rb. Den Haag 21 februari 2007, LjN AZ9109; Rb Rotterdam 25 april 2007 LjN BA5125; zie ook weer R.D. Chavannes, ‘Veel taps, weinig verantwoording’, *Mediaforum* 2008-6, p. 245.

53 Zie de website van het Agentschap Telecommunicatie: www.agentschap-telecom.nl.

en:

Agentschap Telecom is de toezichthouder, uitvoerder en expert voor het gehele elektronische communicatiedomein.

Anders dan uit deze taakomschrijving kan worden opgemaakt houdt het Agentschap zich echter ook bezig met het toezicht op de aftapverplichtingen en dergelijke. In zoverre lijkt het niet onlogisch om het toezicht op naleving van de bewaarplichtbepalingen bij het Agentschap te leggen. Althans, voorzover het gaat om de naleving door de aanbieders. Dat ligt natuurlijk anders als het gaat om de door behoeftestellers na te leven bepalingen. Onafhankelijk toezicht door een overheidsagentschap op het gebruik van bewaarde verkeersgegevens door diezelfde overheid is naar ons oordeel een figuur die om redenen van rechtsstatelijkheid ondubbelzinnig kan worden verworpen.

Al met al lijkt het wetsvoorstel ervan uit te gaan dat het onafhankelijke toezicht kan worden beperkt tot de naleving van de bewaarplicht door de telecoaanbieders. Dit is opmerkelijk en zorgelijk, zelfs als impliciet wordt verondersteld dat dit toezicht kan worden gedaan door bijvoorbeeld het CBP.

De beperkte aandacht voor toezicht op behoeftestellers is des te zorgelijker wanneer in aanmerking wordt genomen dat het wetsvoorstel ook maar weinig aandacht heeft voor de implementatie van de door artikel 10 en 14 van de richtlijn voorgeschreven verplichting tot jaarlijkse statistische verantwoording over het gebruik van de bewaarde gegevens. Uit de MvT blijkt dat dit gaat worden geregeld bij AMvB en dat er een Commissie statistische informatie wordt ingesteld.⁵⁴ Maar hoe een en ander wordt geregeld is opnieuw nog niet erg duidelijk. Opmerkelijk. Want die statistische verantwoordingsplicht is één van de belangrijkste mogelijkheden om boven tafel te krijgen hoe vaak (al dan niet met succes) van de bewaarde gegevens gebruik wordt gemaakt door de behoeftestellers.

Wij moeten raden naar de beweegredenen van regering en parlement om de wijzen waarop aan deze belangrijke verplichtingen inhoud zal worden gegeven niet in het wetsvoorstel zelf te willen vastleggen. Wij kunnen ons niet aan de indruk onttrekken dat de regering er de voorkeur aan geeft deze informatie om – overigens moeilijk te volgen – redenen van effectieve opsporing zoveel als mogelijk geheim te houden.⁵⁵ Daarmee wordt op de koop toe genomen dat er informatie komt te ontbreken die misschien zou kunnen worden gebruikt om op

zinnvolle wijze te discussiëren over de effectiviteit en proportionaliteit van de bewaarplicht. Van iets dergelijks lijkt overigens ook sprake te zijn bij de aftapverplichting.⁵⁶

Ter afsluiting: opmerkelijkheden

Wij sluiten af met een korte samenvatting van wat wij opmerkelijk vinden in het wetsvoorstel:

1. We hebben te maken met een wetsvoorstel over het bewaren van verkeersgegevens waaruit niet – ook niet nadat dit door de Tweede Kamer is behandeld – kan worden gelezen op welke wijze de gegevens moeten worden bewaard en beschikbaar gesteld.
2. Het wetsvoorstel voorziet niet in de opheldering van essentiële onduidelijkheden over (i) hoe de aanbieders onderscheid kunnen maken tussen legitieme en illegitieme informatievragen en (ii) de kwaliteitsbewaking van de eigen informatiehuishouding voor de opsporing.
3. De eensgezindheid waarmee regering en parlement bij formulering en behandeling van het wetsvoorstel achterwege laten om vorm te geven aan effectieve en onafhankelijke vormen van toezicht op en terugkoppeling over de wijzen waarop de overheid van zijn nieuwe mogelijkheden en bevoegdheden gebruik maakt.

Onze conclusie is dat regering en parlement met dit wetsvoorstel *de facto* en gezamenlijk, willens en wetens, en in afwijking van de strekking van de richtlijn, grote risico's nemen met de rechtsstatelijkheid van ons bestel – veel groter dan wij in onze eerdere bijdrage in dit tijdschrift voorzagen. We willen niet uitsluiten dat de toegenomen bereidheid daartoe werd en wordt gevoed door de verontrustende groei in gevoeligheid voor populistisch appel bij het Nederlandse electoraat. Veel van de rechtswetenschappelijk gestoelde *misgivings* over de bewaarplicht worden met de formulering en behandeling van het wetsontwerp bevestigd en winnen aan concrete urgentie.

De Eerste Kamer is nu aan zet. Wij zijn benieuwd naar zijn oordeel.

Op deze tekst is een Creative Commons-Licentie (by-nc-nd 2.5 Netherlands) van toepassing. Zie voor gebruiksvoorwaarden: <http://creativecommons.org/licenses/by-nc-nd/2.5/nl>. Een tekst met enige links staat op <http://weblog.leidenuniv.nl/users/zwenneji> en <http://zwenneblog.weblog.leidenuniv.nl>.

⁵⁴ Vgl. *Kamerstukken II 2006-2007*, 31 145, nr. 3, p. 18, 43 en 50; nr. 9, p. 13, 27-29; *Hand II 2006-2007*, nr. 83, p. 5836.

⁵⁵ In de MvT wordt deze, weinig vertrouwenwekkende opmerking gemaakt: 'Voor wat betreft de gegevens die worden opgevraagd door de inlichtingen- en veiligheidsdiensten, geldt dat de informatie over de toepassing van deze bevoegdheden door de diensten staatsgeheim is. Over de toepassing van de bevoegdheden kan vertrouwelijk verantwoording worden afgelegd aan de commissie voor

de inlichtingen- en veiligheidsdiensten van de Tweede Kamer. Statistische informatie met betrekking tot de verstrekking van gegevens aan deze diensten – indien voorhanden – zal dan ook nimmer beschikbaar kunnen komen voor de Commissie [d.w.z. de Commissie statistische informatie]'. *Kamerstukken II 2006-2007*, 31 145, nr. 3, p. 19; idem: *Hand II 2006-2007*, nr. 83, p. 5836.

⁵⁶ R.D. Chavannes, 'Veel taps, weinig verantwoording', *Mediaforum* 2008-6, p. 245.