Recht en risico

Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens

Aernout Schmidt en Gerrit-Jan Zwenne*

Op 28 juli 2005 kregen we de toen meest recente versie onder ogen van een in Brussel circulerend voorstel voor een richtlijn over een bewaarplicht van verkeersgegevens.[1] We duiden het aan als 'het Voorstel'.

Het Voorstel is een opmerkelijk staaltje van het reactievermogen van de Europese wetgever. In juni dit jaar heeft het Europees Parlement immers laten weten zich niet te kunnen vinden in de grondslag van het Ontwerp Kaderbesluit[2] over de bewaarplicht van verkeersgegevens.[3] Naar aanleiding daarvan zoekt de preambule van het Voorstel dan ook keurig naar een grondslag in de eerste, in plaats van in de derde pijler.[4] Het betreft nu een uitwerking van de Richtlijn privacy en elektronische communicatie.[5] Enerzijds verlangt deze richtlijn in artikel 6 dat telecomaanbieders en Internet Service Providers[6] (ISPs), de verkeersgegevens waarover zij beschikken verwijderen zodra deze niet langer nodig zijn voor de communicatie of de facturering. Anderzijds biedt de richtlijn in artikel 15 de mogelijkheid om daarvan per lidstaat bij wet af te wijken en het bewaren van verkeersgegevens voor te schrijven indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale veiligheid of voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Aan dit artikel 15 is door de verschillende lidstaten op verschillende wijzen invulling gegeven – zozeer, dat harmoniserende maatregelen geboden worden geacht. Het Voorstel is een aanzet tot een richtlijn die daarin beoogt te voorzien. In deze bijdrage willen wij nagaan wat het Voorstel, als dat ongewijzigd zou worden aangenomen, betekent.

Over het Ontwerp Kaderbesluit is in de afgelopen periode indringend gediscussieerd, zowel door belangengroeperingen als in onze beide parlementaire kamers.[7] Het Voorstel maakt die discussie opnieuw los, zij het dat door de nieuwe grondslag de procedures rond vaststelling, aanvaarding en implementatie veranderen. Wij willen ons in deze bijdrage niet richten op of uitlaten over formele argumenten tegen het Voorstel. We zien in het op zo korte termijn opduiken van het Voorstel een teken van urgentie, een urgentie die is gevoed door terroristische aanslagen en die breed wordt gevoeld in politiek Europa. Voorts zien wij geen aanleiding te verwachten dat het privacyargument met succes als veto zal kunnen werken in een maatschappelijk klimaat dat vervuld is van vrees voor terrorisme – misschien beter gezegd: vrees voor het risico van terroristische aanslagen. Evenmin overtuigen ons de technische en kostenargumenten die (eveneens vanuit een janee benadering) suggereren dat de bewaarplicht niet zinvol te realiseren is, onder meer omdat veel van de te bewaren gegevens nu al *de facto* worden bewaard door telecomaanbieders, ISPs en andere dienstverleners zoals Google.[8] We benaderen de geharmoniseerde bewaarplicht vanuit de hypothese dat die er komen zal. Het gaat bij de komst van de bewaarplicht onzes inziens niet om het *of*, maar om het *hoe*. Het evenwicht tussen privacy en preventie moet ergens worden gezocht.

Waar? We gaan op zoek naar argumenten. Voor criteria gaan we te rade bij een benadering waarover de Raad van Europa het in 2002 eens is geworden. We bezien daarna wat het Voorstel betekent, ook in het licht van de recente nationale wetgeving.

* Prof. mr. Aernout 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. Gerrit-Jan Zwenne is advocaat bij Bird & Bird in Den Haag. Daarnaast is ook hij verbonden aan eLaw@Leiden en fellow bij het E.M. Meijers Instituut.

1 Het Voorstel is (met moeite) zo hier en daar wel op internet te vinden. Zie bijvoorbeeld: http://quintessenz.at/doqs/000100003296/2005__05__21,New__Draft__Framework__Decision__on__the__retention__of__data__by__the__British__Home__Office.pdf. Ten behoeve van de lezers van deze bijdrage is het Voorstel ook toegankelijk gemaakt via www.rechteninformatica.leidenuniv.nl onder menu-optie <bronnen>.

2 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 prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, 28 April 2004. Het kaderbesluit is te vinden via http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf of (gemakkelijker) via het verkeersgegevensdossier op de website van Bits of Freedom: www.bof.nl.

3 Vgl. het negatieve advies over de rechtsgrondslag van het kaderbesluit van 31 maart 2005 van het Committee on Civil Liberties, Justice and Home Affairs van het Europees Parlement. Ook de Commissie heeft zich trouwens negatief uitgelaten over het kaderbesluit, zie werkdocument (SEC(2005) 420, 22 maart 2005. Een en ander is te vinden via het verkeersgegevensdossier op de website van Bits of Freedom of via de website van Statewatch, resp. www.bof.nl en www.statewatch.org.

4 D.w.z. art. 95 van het EG-Verdrag i.p.v. art. 31, eerste lid, onder c, en art. 34, tweede lid, onder b, van het EU-verdrag.

5 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* L 201/37

6 D.w.z. aanbieders van openbare elektronische communicatienetwerken en -diensten resp. openbare telecommunicatienetwerken en diensten in de zin van art. 1.1, onder e t/m i en art. 1.1, onder ee en ff, van de Telecommunicatiewet. In deze bijdrage worden de onderscheiden partijen aangeduid als 'telecomaanbieders en ISPs', of ook wel tezamen als 'de aanbieders'.

7 Zie bijvoorbeeld het verslag van commissieoverleg van 12 april 2005 en de moties-Vendrik van 26 mei 2005, *Kamerstukken II* 2005/06, 23 490, nrs. 371 t/m 373.

8 '[...] Google verzamelt geen unieke informatie over u (zoals uw naam, e-mail adres, etc.) behalve als u die informatie uitdrukkelijk en bewust verstrekt. Google noteert informatie zoals tijdstip [...] en IP adres van elke zoekvraag [...]' Dit is een citaat uit Google's *privacy policy*.

Vervolgens gaan we op zoek naar de praktische betekenis van het Voorstel door na te gaan wat dat inhoudt voor de praktijk van de telecommunicatie en het internet. Ten slotte brengen we onze bevindingen in verband met de drie criteria van artikel V uit de 'Guidelines'.

We ontkomen er niet aan ons nu en dan op glad ijs te begeven: de beoordeling van het Voorstel is immers niet alleen een juridische. Het gaat om de betekenis van voorgenomen recht, in een politiek bewogen context. In die context is de vrees voor risico's prominent aanwezig. Het risico van een zelfmoordaanslag, het risico van een fundamentalistische tweedeling in de samenleving, het risico van willekeurig bestuur, het risico van een open samenleving die zich sluit. Het recht levert bijdragen bij het tegemoet treden daarvan, maar leidt in geen van die gevallen tot een causale keten die de risico's kan wegnemen. We zullen nagaan wat de voorgestelde regeling inhoudt en welke reacties zij vermoedelijk zal oproepen om tot aanbevelingen te komen waarvan wij menen dat die de maatschappelijke functie van ons rechtssysteem onder de druk van die risico's kunnen bewaken.

Criteria

Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische communicatienetwerk of voor de facturering ervan.[9] Het zijn gegevens óver de communicatie, maar niet de inhoud daarvan.[10] Dus niet wat er wordt besproken in een telefoongesprek, maar wie er met wie belt, wanneer dat gebeurt, hoelang het gesprek duurde, van welke plek er wordt gebeld, of het een mobiel of vast gesprek was, voor wie het email- of sms-bericht bestemd is en wat de omvang daarvan was, hoelang u ingelogd was bij uw ISP, welke web-pagina's u heeft bezocht, enzovoorts. Als zodanig zijn verkeersgegevens nuttig gebleken bij het opsporen en voorkomen van criminaliteit en terrorisme.[11] Het bewaren en beschikbaar hebben van de gegevens wordt dan ook wel gezien als een essentieel onderdeel van de informatiehuishouding van opsporingsautoriteiten. De urgentie van het reguleren ervan is in Nederland tot uitdrukking gekomen in een reeks recente activiteiten van de wetgever en het bestuur. Om een paar voorbeelden te noemen:

- De wet van 18 maart 2004 tot wijziging van het wetboek van strafvordering en andere wetten in verband met de aanpassing van de bevoegdheid tot het vorderen van gegevens telecommunicatie.[12]
- Het besluit van 3 augustus 2004, houdende de aanwijzing van de gegevens over de gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker die van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst kunnen worden gevorderd.[13]
- Het concept wetsvoorstel Politiegegevens, waarvan de consultatie is afgerond, en dat is toegezonden aan de Raad van State.[14]
- Het concept wetsvoorstel Verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, waarover de Raad van State in juni 2005 adviseerde.[15]
- Het convenant over de samenwerking tussen de Algemene en de Militaire Inlichtingen en Veiligheidsdiensten van 8 juli 2005.[16]

Hoewel de eerste contouren van deze wetgevende activiteiten dateren van vóór 11 september 2001 – wij doelen op het rapport van de Commissie-Mevis[17] – wordt algemeen aangenomen dat de urgentie voor de wetgever ligt in het toegenomen risico van terroristische aanslagen in de Westerse wereld. De maatschappelijke discussie die is gevolgd op de gebeurtenissen van 11 september 2001 is niet eenduidig. Er zijn uitingen van radicaliserende uitwassen binnen het Islamitische deel van de Westerse wereld (Madrid, Londen, de moord op Van Gogh in Amsterdam). Er zijn ook uitingen van radicalisering jegens de islam (moskee-brandstichtingen, uitingen in de geest van Hirsi Ali, Ellian, Wilders). Daartegenover stellen zich belangengroeperingen, wetenschappelijke auteurs en anderen door te wijzen op geheel andere gevaren voor het bestaan van onze rechtsstaat.[18] In deze stukken overheerst de logica dat men de rechtsstaat niet kan beschermen door hem op te heffen. Ten slotte kan een enkele bijdrage worden genoemd, die een vooral pragmatisch-rationeel karakter draagt.[19]

Er lijkt overigens, blijkens eerdergenoemde wetgevingsactiviteiten, breder steun dan voorheen voor de vermindering van de rechtsbescherming van de individuele burger. In het

9 Art. 2, onder b, Richtlijn 2002/58/EC, art. 11.1, onder b,Tw.

10 Ekker wijst erop dat het onderscheid tussen enerzijds gegevens over de communicatie (d.w.z. verkeersgegevens) en anderzijds gegevens over de inhoud in de context van internet diffuus kan zijn. Zie A. Ekker, 'Publiekrechtelijke bescherming van verkeersgegevens', in Asscher en Ekker (red.), *Verkeersgegevens; Een juridische en technische inventarisatie*, Otto Cramwinckel Uitgeverij 2003, p. 48; zie verder ook A. Escudero-Pascual en I. Hosein, 'The hazards of technology-neutral policy: questioning lawful access to traffic data', *Communications of ACM*, VOL47, (April 2004), http://is.lse.ac.uk/staff/hosein/pubs/acm-1905__prepub.pdf.

11 In een bijlage bij zijn kamerbrief van 14 februari 2005 geeft minister Donner een aantal voorbeelden, zie *Kamerstukken II* 2004/05, 23 490, nr. 360.

12 *Stb*. 2004, 394.

13 *Stb*. 2004, 394.

14 Concept wetsvoorstel Regels inzake de verwerking van politiegegevens (Wet politiegegevens), te vinden via de website van het Ministerie van Justitie: www.justitie.nl/Images/Verwerking %20politiegegevens__tcm74-34079.pdf.

15 Het concept wetsvoorstel Verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, ook te vinden via de website van het Ministerie van Justitie: www.justitie.nl/Images/11__60010.doc.

16 Convenant van 8 juli 2005 tussen de Minister-President, Minister van Algemene Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie inzake de samenwerking tussen de AIVD en MIVD (niet te verwarren met het Convenant MIVD-AIVD, *Stcrt.* 2003, 195 en het Convenant CT infobox, *Kamerstukken II* 2004/05, 29754. nr. 21), te vinden via www.mindef.nl/Images/Convenant%20AIVD-MIVD.%20versie077net3__tcm6-42706.pdf of via de website van Bit of Freedom: www.bof.nl

17 Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvordelijk onderzoek*, mei 2001.

18 Om er enkele te noemen: E. Myjer, 'Rechten van de mens en bestrijding van terrorisme; enige opmerkingen over de Europese aanpak en over de rol van de officier van justitie', *Trema*, oktober 2003, nr. 8, p. 336-342; P.H.P.H.M.C. van Kempen, 'Terrorismebestrijding door marginalisering strafvorderlijke waarborgen', *NJB* 2005, nr.8, p.397-400; T. Prakken, 'Naar een cyclopisch strafrecht', *NJB* 2004, p. 2340, 2342-2343; H. van Gunsteren, *Gevaarlijk veilig*, 2005; G. Mak, *Gedoemd tot kwetsbaarheid*, 2005.

19 A. Patijn, Opslag van verkeersgegevens? *Computerrecht*, 2003, afl. 2 en: L.F. Asscher en A.H. Ekker (red.) *Verkeersgegevens, een juridische en technische inventarisatie*, Otto Cramwinckel Uitgever 2003.

20 We wijzen voor dit laatste op de motie van Van der Vlies waarin wordt aangespoord tot 'een opsporingsactie naar haatzaaiende websites en aanverwante strafbare gedragingen op internet' en waarin een wetsvoorstel 'strafbaarstelling verheerlijking van terroristische misdrijven en de ontzetting van de uitoefening van bepaalde beroepen' wordt aangekondigd, *Kamerstukken II* 2004/05, 29 754, nr. 24.

21 Illustratief is de correspondentie van minister Donner en de Eerste Kamer, *Kamerstukken I* 2004/05, 23 490, nrs. AR en AS. Zie ook: *Stcrt.* 2005, nrs. 11, 34, 69, 96, 106, 118, 121 en 134.

22 Zie ook: E. Myjer 2003.

bijzonder op de gebieden van privacy en vrijheid van meningsuiting[20] ten gunste van de informatiemacht van het bevoegd gezag bij de opsporing van strafbare feiten en het voorkomen van terroristische aanslagen. De discussie is caleidoscopisch van aard. Incompatibele argumenten vlogen in het parlement over en weer.[21]

Om bij te dragen aan een zinvol debat ligt het voor de hand om aansluiting te zoeken bij de volgende drie uitgangspunten waarover tenminste de Raad van Europa het eens is:[22]

1. *Instrumenten*. Er is gerichte aandacht nodig voor de verbetering van de instrumenten waarmee het risico voor terroristische aanslagen kan worden aangepakt. Dit uitgangspunt berust op de vaststelling dat het gevaar voor terroristische aanslagen reëel is en dat, tegelijkertijd, het instrumentarium van de overheid om zijn burgers daartegen te beschermen gebreken vertoont. Het gaat immers om een nieuw en goeddeels onbekend gevaar dat zich kenmerkt doordat (i) zoveel mogelijk, willekeurige slachtoffers worden gemaakt, doordat (ii) daarbij gebruik wordt gemaakt van de voor de Westerse wereld wezensvreemde zelfmoordmethode, doordat (iii) er een groot, internationaal en vrijwel ongrijpbaar daderpotentieel blijkt te zijn en doordat (iv) daarbij de bereidheid tot daadwerkelijk gebruik van massavernietigingswapens (indien beschikbaar) helemaal niet denkbeeldig is.
2. *Oorzaken*. Er is gerichte aandacht nodig voor het tegengaan van de oorzaken van terrorisme. Dit uitgangspunt berust op de vaststelling dat instrumenten uit het strafrecht en uit de strafvordering niet in staat zijn (en er ook niet op gericht zijn) om de voedingsbodem voor terrorisme weg te nemen.
3. *Mensenrechten*. Bij dat alles dienen de fundamentele waarden (lees: mensenrechten) te worden geëerbiedigd. Dit uitgangspunt berust op de vaststelling dat het ineens en alom in de Westerse samenleving gegroeide én geuite wantrouwen tegen moslims in het algemeen door zijn discriminerend karakter een voedingsbodem legt voor polarisatie en daarmee zelfs voor een versterking van het aantal potentiële terroristen.[23]

Van belang is daarbij de uitwerking die aan deze uitgangspunten zijn gegeven, met name in artikel V van de 'Guidelines of the Comittee of Ministers of the Council of Europe on Human Rights and the fight against Terrorism' van 11 juli 2002:

> *Artikel V. Collection and processing of personal data by any competent authority in the field of State security:* Within the context of the fight against terrorism, the collection and processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular: (1) are governed by appropriate provisions of domestic law; (2) are proportionate to the aim for which the collection and the processing were foreseen; (3) may be subject to supervision by an external independent authority.

Tegen de achtergrond van de drie criteria uit artikel V willen we het Voorstel lezen, analyseren en beoordelen.

Betekenis van het Voorstel

Om te begrijpen wat het Voorstel betekent zetten we het af tegen de (overigens deels zeer recente) huidige regelingen.

De huidige regelingen

De wet maakt onderscheid tussen enerzijds verplichtingen om gebruikers- en verkeersgegevens te verstrekken en anderzijds de verplichtingen om deze gegevens te bewaren. Daarnaast zijn er nog de verplichtingen om gegevens te achterhalen. De regeling is verspreid neergelegd in bepalingen van de Telecommunicatiewet (Tw), het Wetboek van Strafvordering (Sv), de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) en een handvol onderliggende besluiten. Het geheel is niet gemakkelijk te doorgronden. Het uitgangspunt is dat de bewaar- en achterhaalverplichtingen ten dienste staan aan de verstrekkingsplicht. Maar het is niet zo dat er ten dienste van *alle* verstrekkingsplichten inderdaad bewaar- of achterhaalverplichtingen zijn. In een aantal gevallen is er wél sprake van een verplichting om gegevens te verstrekken, maar niet om deze gegevens te bewaren of te achterhalen. In dergelijke gevallen is de telecomaanbieder alleen gehouden de gegevens te verstrekken indien en voorzover hij daarover de beschikking heeft. Van belang is dan dat ter bescherming van de persoonlijke levenssfeer van abonnees en eindgebruikers ook is voorgeschreven dat aanbieders gegevens niet langer bewaren dan nodig voor hun bedrijfsvoering.[24]

De verplichtingen om gegevens te verstrekken aan politie en justitie, en inlichtingendiensten staan in de artikelen 13.2a en 13.4 Tw, welke bepalingen zijn ingevoegd respectievelijk aangepast bij de Wet vorderen gegevens telecommunicatie.[25] In artikel 13.2a, eerste lid, Tw staat dat aanbieders van openbare telecommunicatienetwerken en -diensten moeten voldoen aan vorderingen op grond van artikel 126n of 126u Sv dan wel artikel 28 van de Wiv. Dit betekent dat aanbieders gehouden zijn om op verzoek van een officier van justitie of de AIVD cq. MIVD[26] gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker, als er sprake is van een verdenking van ernstig misdrijf[27] en gegevens van belang zijn voor het onderzoek daarnaar. Het verzoek om gegevensverstrekking kan alleen betrekking hebben op gegevens die zijn opgesomd in het Besluit vorderen gegevens telecommunicatie.[28] Dit betreft achtereenvolgens de naam, adres en woonplaatsgegevens van de gebruiker en degene met wie deze verbinding heeft gehad of geprobeerd heeft te hebben, de datum en het tijdstip van de verbinding of de poging daartoe, de locatiegegevens cq. gegevens betreffende de geografische positie van de randapparatuur, de nummers van de gebruikte randapparatuur en de soorten van gebruikte diensten met de daarbij behorende gegevens. Als degene die de rekening betaalt voor de afgenomen diensten een ander is dan de gebruiker zelf, moeten ook de gegevens van deze persoon worden verstrekt.

23 Zie ook: E. Myjer 2003.
24 Art. 11.5 en 11.5a Tw.
25 Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie, *Stb*. 2004, 105.
26 Resp. Algemene Inlichtingen- en Veiligheidsdienst ('AIVD') en Militaire Inlichtingen- en Veiligheidsdienst ('MIVD').
27 D.w.z. misdrijven i.d.z.v. art. 67, eerste lid, Sv, waarvoor een bevel tot voorlopige hechtenis kan worden gegeven.
28 Besluit vorderen gegevens telecommunicatie, *Stb.* 2004, 394.

Aan deze gegevensverstrekkingsverplichting zijn geen bewaar- of achterhaalverplichtingen verbonden. Wel zijn er voorschriften over de procedures volgens welke deze gegevens moeten worden verstrekt. Deze zijn opgenomen in het Besluit verstrekking gegevens telecommunicatie,[29] dat overigens niet is gebaseerd op de grondslag die artikel 13.2a, tweede lid, Tw daarvoor biedt.[30] Voorzover het gaat om gegevens betreffende de naam-, adres- en woonplaats van de gebruiker en diens nummer moeten de gegevens in begrijpelijke vorm worden verstrekt. Ook moet er gebruik worden gemaakt van het systeem en de procedures van het Centraal informatiepunt onderzoek telecommunicatie (CIOT), zoals bedoeld in voornoemd besluit.[31] Voorzover het gaat om andere gegevens bestaan er andere, in de wetgeving niet nader genoemde procedures.[32] In artikel 13.4, eerste lid, Tw is een andere gegevensverstrekkingsverplichting opgenomen. In dit artikel staat dat aanbieders van openbare telecommunicatienetwerken en -diensten moeten voldoen aan een vordering op grond van artikel 126na, eerste lid, en artikel 126ua Sv, dan wel op grond van artikel 29 Wiv. Deze verplichting heeft betrekking op naam-, adres-, postcode- en nummergegevens, alsmede op gegevens over het soort van de gebruikte dienst. Aan deze verstrekkingsverplichting zijn, anders dan die van artikel 13.2a Tw, wel bewaar- en achterhaalverplichtingen verbonden. Om te kunnen voldoen aan de verstrekkingverplichting zijn aanbieders op grond van artikel 13.4, tweede lid, Tw gehouden om bij AMvB aan te wijzen gegevens drie maanden te bewaren, en dat vanaf het moment dat de gegevens voor het eerst worden verwerkt. De gegevens die onder deze bewaarplicht vallen worden opgesomd in weer een ander besluit, het Besluit bijzondere vergaring nummergegevens telecommunicatie.[33] Het betreft gegevens over de tijdstippen waarop telecommunicatie heeft plaatsgevonden, de met die tijdstippen en de desbetreffende telecommunicatie corresponderende nummers, en bij welk basisstation elk van deze gegevens zijn binnengekomen.

Op welke wijze de onderscheiden bewaar- en verstrekkingsverplichtingen zijn ingevuld is niet duidelijk. Een overzichtelijke regeling daarvan is in openbaar toegankelijke bronnen niet te vinden.

Aanpassing als gevolg van het voorstel

Het voorstel is nogal beknopt, en laat veel vragen onbeantwoord. In deze paragrafen geven we de kern van enkele bepalingen weer om erbij aan te geven wat de belangrijkste verschillen en overeenkomsten met de bestaande regeling zijn en welke vragen dat oproept.

Welke gegevens moet worden bewaard? welke niet?

Het Voorstel heeft, zo blijkt uit artikel 2, tweede lid, betrekking op de verkeers- en locatiegegevens, alsmede op de 'daarmee verband houdende gegevens die nodig zijn om om de abonnee of gebruiker te identificeren'.[34] Deze gegevens moeten worden bewaard, zo blijkt uit artikel 4, eerste lid, voorzover ze nodig zijn om de bron, bestemming, tijdstip en duur van de communicatie te traceren en te identificeren, alsmede voorzover ze nodig zijn om de soort van de communicatie, de randapparatuur en de locatie daarvan, te identificeren. Zeg maar: alles wat nodig is om te achterhalen wie met wie, wanneer en waar, hoe en hoelang heeft gebeld of anderszins heeft gecommuniceerd via elektronische communicatie.

In de Annex bij het Voorstel worden de te bewaren gegevens enigszins gespecificeerd. Het blijkt dat het in het bijzonder gaat om de volgende gegevens:

- *data necessary to trace and identify the source and the destination of communications on fixed network telephony, mobile telephony, internet access and internet communication services (IP address user, user ID, connection label, NAW subscriber; IP address recipient, NAW subscriber).*
- *data necessary to identify date, time and duration of a communication (fixed and mobile telephony: start and end; internet access and communication services: date and time of login and log-off of the internet sessions based on a certain time zone).*
- *data to identify the type of communication (telephony: e.g., voice, SMS conference call, multi media). Data necessary to identify the communication device or what purports to be the communication device (Mobile: IMSIs, IMEIs; internet access and Services: calling telephone number for dial-up access, ADSL or other end point of the originator, the MAC address or other machine identifier of the originator of the communication).*
- *data necessary to identify the location of mobile communication equipment (Cell IDs from start to finish; data mapping between Cell IDs and their geographical locations at the time of the communication).*

Het is duidelijk dat de hoeveelheid te bewaren gegevens niet gering is. Er moeten verschillende soorten gegevens worden bewaard. En dat moet gebeuren 'per communicatie', dat wil zeggen in het geval van telefoonverkeer: per gesprek. Wat dat precies betekent voor internetverkeer is minder duidelijk: per chat, per webpagina, per sessie?[35] Afhankelijk van de betekenis die aan het begrip 'type internet-communicatie' zal worden toegekend, verwachten we hier dan ook de nodige praktische problemen.[36] Het is duidelijk dat het Voorstel in dit opzicht in potentie sterk kan afwijken van de bestaande regeling. Hier treedt een bezwaar tegen het regelen van de bewaarplicht op de overigens zo populaire 'techniekonafhankelijke' wijze: door in functionele termen te spreken laat de wetgever het *de facto* aan de uitvoerende instanties over om te bepalen welke gegevens precies nodig zullen zijn.

Wat verder opvalt is dat het blijkens de Annex gaat om de gegevens die nodig zijn om de abonnee of gebruiker ('subscriber(s) or registered user(s)') te identificeren. De defini-

29 Besluit van 26 januari 2000, *Stb.* 2000, 71, zoals gewijzigd bij Besluit van 16 december 2002, *Stb.* 2003, 22.

30 Zie art. V Wet vorderen gegevens telecommunicatie, *Stb.* 2004, 105.

31 Zie de Nota van Toelichting bij het Besluit van 3 augustus 2004 tot vaststelling van het tijdstip van inwerkingtreding van de Wet vorderen gegevens telecommunicatie en het Besluit vorderen gegevens telecommunicatie, *Stb.* 2004, 394, p. 4-5; zie Nijboer/Knol 2005 *(T&C Telecommunicatierecht)*, art. 13.2a, aant. 3.

32 Nijboer/Knol 2005 *(T&C Telecommunicatierecht)*, art. 13.2a, aant. 3 en art. 13.4, aant. 4.

33 Besluit bijzondere vergaring nummergegevens telecommunicatie, *Stb.* 2002, 38, zoals gewijzigd bij Besluit van 16 december 2003, *Stb.* 2003, 31.

34 Dit is onze vertaling van 'traffic data and location data, as well as the related data necessary to identify the subscriber or user'.

35 Browsen is bijvoorbeeld *stateless*, dat wil zeggen dat er eigenlijk geen sprake is van gesprekken of 'sessies', maar van enkelvoudige berichten. Sessies kunnen wel degelijk worden opgebouwd op internet, maar daarvoor is een protocol vereist. Protocols zijn syntactische taal-afpraken, doorgaans niet gebonden aan regulering. Interessante varianten hiervan zijn de zeer gebruikelijke SSH en TLS protocols, die ge-encrypte (dus beveiligde) verbindingen leggen (noodzakelijk voor elke vorm van e-commerce). Zij werken op een hoger niveau dan, of 'boven op' TCP/IP.

36 Wat bijvoorbeeld problematisch kan zijn is het gebruik van IP-poorten om internetcommunicatie te relateren aan bepaalde toepassingen. Slechts een klein gedeelte van die poortnummers heeft een standaardbetekenis, en er zijn honderdduizenden verschillende internettoepassingen.

tie gaat daarmee verder dan de doelstelling van artikel 1, waarin alleen wordt gesproken over het identificeren van de gebruiker (*to identify the user*). Dit betreft misschien een verschrijving. Interessanter is of de gebruiker die communiceert inderdaad met de te bewaren gegevens kan worden geïdentificeerd. Dit lijkt in elk geval problematisch als het gaat om gestolen mobiele telefoons of telefoongesprekken gevoerd door bezoekers. Ook zal het lastig zijn om internetverkeer, dat wordt gegenereerd door anderen dan degene die het abonnement met de ISP heeft afgesloten, te relateren aan degene die daadwerkelijk van de internetverbinding gebruik maakt (bijvoorbeeld in een internetcafé). Voor identificatie van gebruikers is aanvullende techniek vereist die nog lang geen gemeengoed is, maar die er misschien op termijn wel zal komen (een 'digitaal paspoort' of iets dergelijks).[37]

Een belangrijk verschil met de huidige regeling is de omvang van de verplichting ten aanzien van het bewaren van gegevens: niet alleen die welke toch al voor de bedrijfsvoering nodig zijn, maar die welke nodig zijn voor het identificeren van gebruikers, alsmede de verkeersgegevens die nodig zijn voor de preventie, de opsporing en de vervolging van strafbare feiten. Van aanbieders wordt verwacht dat zij een rol gaan spelen bij de uitvoering van de taken van politie- en justitie, en de inlichtingendiensten. Er is sprake van het uitbesteden van deze taken aan telecomaanbieders en ISPs. Op zichzelf is dit niet nieuw. Al enige tijd schrijft de wet voor dat de aanbieders ervoor zorgdragen dat hun netwerken aftapbaar zijn.[38] En ook in andere domeinen, zoals de belastingheffing en de anti-witwaswetgeving, is er al lange tijd sprake van uitbesteding van publiekrechtelijke taken aan particulieren, met name aan werkgevers en financiële instellingen.

Maar dat doet er niet aan af dat een dergelijke uitbesteding van publiekrechtelijke taken aan particulieren, hoewel misschien efficiënt of effectief, niet vanzelfsprekend kan zijn, en zeker niet waar het gaat om opsporing. Het is evident dat extra waarborgen zijn vereist ter bescherming van die particulieren en degenen op wie de gegevens betrekking hebben. Welke mechanismen zijn er om te voorkomen dat telecomaanbieders en ISPs niet worden overvraagd? Hoe wordt gewaarborgd dat niet al te gemakkelijk wordt verlangd dat de gegevens worden bewaard? Worden daarbij alle relevante belangen wel afgewogen? Wanneer gebeurt dat eigenlijk, en waar precies? In het Voorstel wordt deels een antwoord gegeven op dergelijke vragen. Het blijkt dat er jaarlijks wordt gespecificeerd welke gegevens moeten worden bewaard. Dit gebeurt onder een onduidelijk democratisch te legitimeren procedure in een polderachtig gezelschap, dat wordt aangeduid als het 'Platform for Law Enforcement, Electronic Communications and Data Protection'. Zorgelijk, en zeer in afwijking van de huidige regeling.

De specificaties van te bewaren gegevens in de Annex laten verder nog ruimte voor speculatie. Onduidelijk is wat moet worden verstaan onder 'connection labels' en onder 'type of communication'. Met name wanneer onder 'labels' mede wordt verstaan de informatie die aan hyperlinks worden gekoppeld.[39] Er is overtuigend betoogd dat bij internetcommunicatie het onderscheid tussen verkeersgegevens en *content* niet duidelijk kan worden vastgesteld, zeker niet wanneer hierbij gebruik wordt gemaakt van techniekonafhankelijke formulering.[40] Verder lijken ons de belangrijkste problemen die met de specificaties in de Annex samenhangen enerzijds de vluchtigheid van die specificaties en anderzijds de kwaliteit van de bewaarde gegevens in het licht van de doelstelling. Zoals de recente Brein zaak[41] heeft laten zien is het, door het gebruik van dynamische IP-adressen niet ondenkbaar dat fouten worden gemaakt. Ook kunnen adressen onder vrijwel elk *operating system* worden aangepast of gemanipuleerd ('gespoofed'). En voor het sluiten van een contract met een ISP bestaat geen identificatieplicht. Om het in termen van de discussies over politiegegevens te zeggen: de bewaarde gegevens bevatten, met name wanneer het om professionele criminaliteit gaat,[42] veel 'zachte' informatie.

Uit de formulering ('prevention, investigation, detection and prosecution') blijkt dat het strafrecht als instrument een steeds pro-actievere rol krijgt toebedeeld en dat de taken van inlichtingen- en opsporingsdiensten steeds verder vervlochten raken. Dat geeft nogal eens aanleiding tot problemen. Zo bleek recentelijk de bewijskracht van de door inlichtingendiensten verkregen informatie beperkt omdat de rechter zich onvoldoende in staat achtte zich een oordeel te vormen over rechtmatigheid van de verkrijging van de informatie en de inhoudelijke juistheid daarvan.[43]

Wie moeten gegevens bewaren en verstrekken, en wie niet?

Uit artikel 1, eerste lid, en artikel 3, tweede lid, van het Voorstel kan worden opgemaakt dat de bewaarverplichtingen van toepassing zijn op alle aanbieders die bij de een of andere vorm van openbare elektronische communicatie zijn betrokken. Dat is niet gering. Niet alleen omdat dat betekent dat heel veel aanbieders met de verplichtingen te maken krijgen – uit het register op de website van OPTA blijkt dat er in Nederland iets minder dan 600 aanbieders als zodanig zijn geregistreerd – maar ook omdat veel elektronische communicatie verloopt via meerdere netwerkaanbieders. Voor pakketgeschakelde internetdiensten geldt zelfs dat de pakketten die tezamen een emailbericht (chatsessie, internet-telefoongesprek, mp3-download enz.) vormen, langs verschillende wegen en langs verschillende aanbieders worden vervoerd. Al deze tussenliggende dienstverleners moeten alle verkeersgegevens bewaren. En dat leidt er dus toe dat van elke communicatie meerdere malen de verkeersgegevens moeten worden opgeslagen.

Iets anders is dat de werking van het Voorstel is beperkt tot *openbare* elektronische communicatie. Alleen aanbieders van openbare elektronische communicatiediensten zijn gehouden verkeersgegevens te bewaren, aanbieders van niet-openbare diensten zijn dat niet. De openbaarheid van de diensten is dus een belangrijk onderscheidend criterium. Dat is niet nieuw. Ook in de huidige wetgeving is de openbaarheid het criterium aan de hand waarvan wordt bepaald of verplichtingen met betrekking tot verkeersgegevens van toepassing zijn. Openbaarheid is evenwel geen eenduidig criterium. De wet zegt in artikel 1.1, onder g, Tw, dat er sprake is van een

37 Dat de daaraan ook in de EU nog niet wordt gedacht blijkt uit art. 2 van het Voorstel.

38 Art. 13.1 e.v. Tw

39 In feite zijn dit vaak aan het http-commando GET gekoppelde zoekspecificaties.

40 Zie o.m. A. Escudero-Pascual en I. Hosein, 'The hazards of technology-neutral policy: questioning lawful access to traffic data', *Communications of ACM*, VOL47, (April 2004), http://is.lse.ac.uk/staff/hosein/pubs/acm-1905__prepub.pdf; Ekker 2003, p. 48.

41 Vzr. Rb Utrecht 12 juli 2005, LJN AT9073.

42 Juist de professionele criminaliteit zal zich de moeite getroosten zoveel mogelijk gebruik te maken van de zwakke plekken in het recht.

43 Zie bijv. Hof Den Haag 21 juni 2004, LJN AP2058.

openbare dienst als deze beschikbaar is voor het publiek. Om dat te verduidelijken geeft de parlementaire geschiedenis een toelichting met de kenmerken van een cirkelredenering. Er is sprake is van een openbaar netwerk of dienst als:

> *[...] de betreffende [...] dienst beschikbaar is voor het publiek. Daarmee wordt bedoeld dat de betreffende dienst openbaar wordt aangeboden en beschikbaar is voor eenieder die van dat aanbod gebruik wil maken tegen de in het openbare aanbod vermelde condities. Het gaat er om dat door de condities die voor het aanbod gelden de kring van degenen die van het aanbod gebruik kunnen maken niet zodanig beperkt is dat niet van een openbaar aanbod gesproken kan worden.*[44]

Openbaar is dus alles wat niet zodanig is beperkt dat niet meer kan worden gesproken van openbaar. Uit betrekkelijk recent onderzoek blijkt dan ook dat er geen sprake is van 'een duidelijke invulling van het begrip', alsmede dat 'aan de houdbaarheid van het begrip [valt] te twijfelen'.[45] Voor zover ons bekend hebben discussies over de openbaarheid van diensten en netwerken zich vooral voorgedaan waar het ging om de registratie door OPTA op grond van artikel 2.1 Tw, maar toch ook waar het ging om de toepassing van de aftapverplichtingen van artikel 13.1 Tw.[46] Invoering van vergaande bewaarverplichtingen kan dergelijke discussies op scherp zetten. Interessant zal bijvoorbeeld zijn in hoeverre politie en justitie zich erin kunnen vinden dat Surfnet en Wireless Leiden, aanbieders die omvangrijke groepen van eindgebruikers bedienen maar niet bij OPTA als openbare aanbieders zijn geregistreerd, niet te maken hebben met gegevensverstrekkings- en bewaarverplichtingen.[47] Het is niet onaannemelijk dat er zich in de nabije toekomst meer voorbeelden zullen aandienen waaruit blijkt dat de grenzen van wat geldt als openbaar en wat niet, onduidelijk zijn.[48] Op dit moment ook kan de vraag worden gesteld of de gebruikers die deelnemen aan een peer-to-peer netwerk als KaZaA, Bittorrent of Freenet zelf ook moeten worden gezien als openbare aanbieders. En hetzelfde geldt voor thuisgebruikers die om wat voor reden dan ook hun draadloze thuisnetwerken niet hebben beveiligd tegen gebruik door derden. Deze gebruikers stellen de eigen apparatuur en infrastructuur te beschikking aan iedereen die daarvan gebruik wil maken. En dat zou kunnen worden gezien als het aanbieden van openbare telecommunicatie. De vraag is of deze gebruikers zelf ook openbare aanbieders zijn. En of van hen ook wordt verlangd dat zij verkeers- en gebruiksgegevens gaan bewaren.

Deze vragen zijn nog niet goed te beantwoorden, en dat geeft te denken. Waar het gaat om niet geringe inbreuken op de persoonlijke levenssfeer van heel veel gebruikers, mag worden verwacht dat de wet voldoende bepaald is. Voorzover dat al niet direct volgt uit het wetmatigheidvereiste van artikel 10 van het Europees Verdrag voor de Rechten van de Mens,[49] is dat wat ons betreft een vereiste van fatsoenlijke wetgeving. Daarnaast, en misschien niet veel minder belangrijk, is dat onduidelijkheid over de reikwijdte van de verplichtingen een beperking kan betekenen voor de innovatie in de telecomsector.[50]

Voor welke doeleinden moeten de gegevens worden bewaard?

Het Voorstel is duidelijk als het gaat om de doeleinden waarvoor de gegevens moeten worden bewaard. Uit artikel 1, eerste lid, en artikel 3, tweede lid, wordt duidelijk dat het erom gaat dat de gegevens beschikbaar zijn ten behoeve van het voorkomen, opsporing en vervolging van strafbare feiten (*the prevention, investigation, detection and prosecution of criminal offences*). De gegevens worden dan ook uitsluitend voor deze doeleinden en in specifieke gevallen verstrekt aan de bevoegde.

Het gaat dus om het verstrekken van gegevens in specifieke gevallen aan bevoegde autoriteiten. Of, en zo ja hoe, dit zal gaan afwijken van de huidige regeling is evenwel onduidelijk. Ook omdat de wijze van verstrekken van verkeersgegevens onder de huidige regeling niet expliciet is gemaakt. We weten niet eens goed hoe het verstrekken nu precies gaat (en of de gevolgde procedures voor de verschillende aanbieders gelijk zijn), noch onder welk regiem de verstrekte gegevens verder worden bewaard, verwerkt en beveiligd.[51] Deze stand van zaken vormt een risico voor de rechtsbescherming, omdat controle daarmee eigenlijk ondoenlijk is geworden. Dit is minder aanvaardbaar, naarmate de machtspositie van de bevoegde autoriteiten sterker wordt en de beschikbaar gestelde gegevensverzamelingen omvangrijker.

What else is new?

De bewaarduur die in artikel 5 van het Voorstel wordt geregeld betreft een duidelijke afwijking ten opzichte van de huidige regeling: telefonieverkeersgegevens moeten één jaar worden bewaard. Thans is dat drie maanden. Internetverkeersgegevens moeten zes maanden worden bewaard. Dat hoeft thans niet. Ook de termijn waarbinnen de gegevens ter beschikking moeten kunnen worden gesteld is nieuw. Artikel 6 van het Voorstel spreekt over 'without undue delay', dat wel als 'onverwijld' zal worden vertaald. Dit is, met de bewaarplicht als zodanig, nieuw.

Het Voorstel bepaalt in artikel 7 dat de aanbieders jaarlijks empirische gegevens moeten verschaffen aan de Europese Commissie over het aantal informatieverzoeken en over de tijd die het heeft gekost daarop te antwoorden. De plicht voor aanbieders om direct te rapporteren aan de Commissie is nieuw. Uit deze verplichting kan overigens worden afgeleid dat het niet de bedoeling is dat de gegevens op een centraal punt zullen worden bewaard onder gezag van de overheid. De formulering van dit artikel lijkt voorts uit te sluiten, dat het aanbieders vrij staat om de databanken waarin zij de verkeersgegevens bewaren direct toegankelijk maken voor de bevoegde autoriteiten. Dit is mogelijk een afwijking van de werkwijze die thans ten aanzien van gebruikersgegevens wordt gevolgd: de tekst van het Besluit vorderen telecommunicatiegegevens is over dit punt niet consistent en lijkt die mogelijkheid open te laten. We willen erop wijzen dat onafhankelijke statistische

44 *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 72.

45 H. Dries, S.J.H. Gijrath en P.C. Knol, *Openbaarheid van netwerken en diensten in de Telecommunicatiewet*, Sdu Uitgevers 2003.

46 Om te ontkomen aan aftapverplichtingen stellen kleinere aanbieders zich wel op het standpunt dat zij geen openbare telecommunicatie aanbieden. Het Agentschap Telecom, de toezichthouder voor deze verplichtingen, gaat daar niet altijd mee akkoord.

47 Surfnet biedt haar diensten aan universiteiten en onderwijsinstellingen aan; Wireless Leiden levert WiFi-diensten aan zo een 4000 abonnees in de regio Leiden.

48 Zo heeft OPTA besloten dat de ene universiteit wel een openbare dienst aanbiedt, en de andere universiteit niet.

49 Vgl. de volgende, nog steeds actuele overweging van het Europees Hof voor de Rechten van de Mensen in het *Sunday Times*-arrest: *[...] a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable citizens 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*, EHRM 26 april 1979, *NJ* 1980, 146, *NJCM-bulletin* 1979, p. 62-63.

50 Vgl. Dries, Gijrath en Knol 2003, p. 103.

51 In het Besluit beveiliging gegevens aftappen telecommunicatie, *Stb.* 2003, 472, zijn wel regels opgenomen over de beveiliging van gegevens met betrekking tot aftappen.

rapportages door de aanbieders van essentieel belang kunnen zijn voor de rechtsbescherming. Het komt ons overigens voor dat van de kant van de Commissie nadere voorschriften zullen moeten worden geformuleerd om te voorkomen dat de vorm van deze rapportages per aanbieder en per lidstaat te zeer gaat divergeren.

In artikel 8 bepaalt het Voorstel dat aanbieders een passende vergoeding moeten krijgen voor de aantoonbare kosten die zij hebben gemaakt als gevolg van de verplichtingen van de richtlijn (*appropriate compensation for demonstrated additional costs [...] as consequence of the directive*). Ook dit is nieuw, en lijkt in te houden dat de verrekening van de kosten naar de consument via de fiscus is gedacht.

Bij de bespreking van welke gegevens moeten worden bewaard (par. 3.2.1) bleek al dat er een onafhankelijk platform met 'polderlobbysamenstelling' zal komen. Dat platform beziet jaarlijks of de specificatie van te bewaren gegevens moet worden aangepast. Dit is ook nieuw. Het platform kan een belangrijke rol spelen door die jaarlijkse aanpassing precies en techniekgeoriënteerd te formuleren. De introductie van nieuwe communicatieprotocols op netwerkniveau is geen kwestie die van vandaag op morgen is gerealiseerd. Vanuit democratisch oogpunt lijkt het ontegenzeggelijk een stap terug dat het aan een dergelijk platform wordt overgelaten om te bepalen welke gegevens moeten worden bewaard.

De implicaties van het voorstel

Bij onze poging te achterhalen wat het Voorstel betekent hebben we vastgesteld dat er nogal wat onduidelijkheden zijn. Toch proberen we de te verwachte gevolgen voor verschillende belanghebbenden te schetsen.

Voor de opsporings- en veiligheidsdiensten

Voor de opsporingsdiensten betekent de bewaarplicht een verbetering van hun informatiepositie, een instrument dat hen in beginsel in staat stelt hun taak beter uit te voeren dan voorheen. Het betekent eveneens een uitbreiding van hun taak. Het doorzoeken van grote hoeveelheden gegevens om daar chocola van te maken vraagt om bijzondere deskundigheid. Zeker, wanneer het ook nog eens om 'zachte' informatie gaat. Het beheren van grote verzamelingen tot personen herleidbare informatie legt bovendien een last op de organisatie; het gaat daarbij voornamelijk om beheer, geautoriseerde toegang en beveiliging. Onzeker is, of hierbij de regiems voor tijdelijke politieregisters zullen gelden, en zo ja, of deze toereikend zijn.[52] Ten slotte zal moeten worden verzekerd dat het materiaal als bewijsmateriaal kan dienen wanneer daartoe aanleiding bestaat. Ook dat stelt bijzondere eisen aan het beheer. De recente evaluatie van de Wet bijzondere politieregisters stemt niet optimistisch aangaande de beschikbaarheid van de daartoe benodigde *IT-governance*[53] en ook niet over de expertise, de rechtskennis, en het IT-verantwoordelijkheidsbesef die daarvoor nodig zijn.[54] We achten het aannemelijk dat met de bewaarplicht ook het toezicht op het rechtmatig en doelmatig gebruik van de bijbehorende bevoegdheden zal moeten worden versterkt.

Een en ander wordt nog verder gecompliceerd zodra we de behoefte aan interregionale en internationale gegevensuitwisseling voor opsporing en preventie in de beschouwing betrekken. Wanneer we bovendien in overweging nemen dat het de Nederlandse politie-organisatie in de afgelopen twintig jaar niet is gelukt om te komen tot een ordentelijk geautomatiseerde interregionale uitwisseling van informatie uit de tijdelijke registers die worden aangelegd voor opsporingsprojecten van zware criminaliteit, dan ligt het voor de hand de hierboven genoemde belemmeringen serieus te nemen. Kortom: de bewaarplicht heeft in de praktijk alleen zin, wanneer er aanmerkelijke inspanningen zijn verricht om de relevante kwaliteiten in de politie-organisatie daadwerkelijk te bewerkstelligen. Het gaat hierbij niet (alleen) om techniek.[55]

Het is overigens onzeker of de bewaarplicht van verkeersgegevens voor internetverkeer voor de veiligheidsdiensten veel nieuwe informatie zal gaan opleveren. Het is een publiek geheim[56] dat sinds geruime tijd alle internetverkeer (naast verkeersgegevens ook de inhoud) door binnenlandse en buitenlandse veiligheidsdiensten wordt opgevangen en (automatisch) wordt geanalyseerd met het oog op onze veiligheid.[57] In dit verband is de te verwachten uitwerking van het Voorstel mogelijk zelfs negatief: wanneer bewaarplicht ertoe gaat leiden dat (zoals hieronder wordt betoogd) intensiever gebruik gaat worden gemaakt van overigens allang beschikbare encryptie- en anonimiseringsmethoden, dan zou dit de effectiviteit van de grootschalige analyse van elektronisch berichtenverkeer ernstig kunnen aantasten.

Het is voorts waarschijnlijk dat de opsporings- en veiligheidsdiensten een stem zullen krijgen in de specificatie van welke de verkeersgegevens (zullen) zijn die moeten worden bewaard. Het is opmerkelijk (maar ook niet uitzonderlijk) dat het bepalen van de inhoud van informatieplichten doorgaans in overleg tussen belangrijke spelers wordt vastgesteld zonder dat de subjecten daarin een stem hebben.[58] Wat dit betreft vertoont de regeling in het Voorstel democratische tekortkomingen.

Ten slotte moet worden aangenomen dat er, door het enkele beschikbaar komen van meer informatie die bovendien als 'zacht' moet worden beoordeeld, niet alleen effectiever kan worden gewerkt door de opsporings- en veiligheidsdiensten,

52 Het rapport van de Commissie Strafvorderlijke Gegevensvergaring in de Informatiemaatschappij (Commissie-Mevis) gaat daar wel van uit. Daarbij dient evenwel te worden overwogen dat het regime voor politieregisters niet is gericht op het beheren en ontsluiten van grote hoeveelheden informatie waarvan moet worden aangenomen dat het overgrote deel *niets* met criminaliteit van doen heeft.

53 De kunst van het aansturen van ICT-processen door het 'management' in plaats van andersom.

54 Zie ook: *Evaluatie wet bijzondere politieregisters*, WODC, 's-Gravenhage 2005; H.H. Kielman en W.I. Koelewijn, 'Minder registers, meer gegevens', *Ars Aequi* 2005 nr. 6, p. 451-457. Overigens, de rapportages van de Algemene Rekenkamer en van de Inspectie Openbare Orde wijzen in eenzelfde richting.

55 De stand van de techniek is niet de oorzaak. Over de technische problemen die het integreren, beveiligen en toegankelijk maken van omvangrijke, heterogene en complexe commerciële gegevensverzamelingen zouden belemmeren horen we het bedrijfsleven zelden klagen – ook niet na omvangrijke fusies.

56 Vgl. P. Radden Keefe, *Chatter. Dispatches from the Secret World of Global Eavesdropping*, Random House 2005; R. O'Harrow, *No Place to Hide*, Free Press 2005.

57 De namen waaronder deze activiteiten bekend staan zijn wisselend. Echelon is het bekendst geworden. Zie bijvoorbeeld: *Kamerstukken II* 2004/05, 26 671, nr . 10, p. 7.

58 Zie daarover G.J. Zwenne, *Belastingheffing en informatieplichten*, (diss. Leiden), Sdu 1998, voor de wijze waarop wordt bepaald welke informatie de banken aan de fiscus verstrekken.

maar dat er ook meer fouten zullen worden gemaakt. Daarmee moet in de praktijk van de toekomst rekening worden gehouden, zowel in de sfeer van de compensatie, als in de sfeer van de (straf)rechtspraak waar 'zacht' materiaal ter bewijsvoering wordt aangeboden.

Voor de telecomaanbieders en ISPs

Voor Nederlandse telecomaanbieders en ISPs betekent de voorgestelde regeling extra taken, en daarmee, extra kosten. Deze kosten spelen een belangrijke rol in de maatschappelijke discussie over de bewaarplicht. Dat lijkt ons niet terecht, en niet zozeer omdat het Voorstel voorziet in vergoeding van de aantoonbaar extra gemaakte kosten. Ook als in aanmerking wordt genomen dat de extra kosten uiteindelijk toch op de een of andere manier worden verhaald op de consument (ofwel via de prijs van zijn abonnement, ofwel via de belastingheffing), dan nog is het de vraag of de discussie vooral over de kosten moet gaan. Een KPMG-onderzoek terzake[59] laat zien dat het opslaan van *alle* verkeer door een centrale overheidsinstantie ongeveer € 9.4 miljoen per jaar zou gaan kosten. Aannemende dat er meer dan 9.4 miljoen abonnementen in Nederland zijn,[60] dan is de met het voorstel gemoeide prijsstijging voor de consument verwaarloosbaar, tenminste, wanneer die kostendekkend wordt verrekend. Een risico dat het kostenaspect zou kunnen betekenen is dat de mededinging tussen aanbieders erdoor wordt verstoord – als de ene aanbieder meer moet betalen dan de andere. Gelet op de mededingings-alertheid van de aanbieders en toezichthouders lijkt dat risico niet heel groot. Bovendien zijn daar wel oplossingen voor te bedenken.

Het Voorstel betekent ook een verlichting van de taak van de telecomaanbieders en ISPs: er wordt iets geregeld, dat niet geregeld was. En die regeling ontslaat de aanbieders van de verantwoordelijkheid na te gaan of het verzoek van de bevoegde autoriteiten een *gerechtvaardigd* verzoek is, en daarmee komt voor hen een aansprakelijkheidsrisico tegenover hun contractanten te vervallen. Dat heeft gevolgen voor het toezicht: de controle van de aanbieders op het gebruik van bewaarde gegevens voor preventie en opsporing door de overheid komt daarmee immers te vervallen.

Het Voorstel brengt voorts een economische *win-win* figuur in stelling waarvan wij voorspellen dat hij in de huidige bestuurscultuur vergaande gevolgen hebben zal. Het bewaren is voor zowel overheid als de aanbieder *efficiënter*, wanneer de aanbieder domweg van alle verkeer automatisch een kopie doorsluist naar een centraal punt dat door de overheid wordt gerund. Dat daaraan nu al wordt gedacht blijkt uit het eerder aangehaalde rapport van KPMG, waarin deze variant expliciet is doorgerekend. Naar wij moeten aannemen is dat in overeenstemming met de opdracht van het Ministerie van Justitie gebeurd. Niet geheel onbegrijpelijk vanuit het gezichtspunt van een ministerie, dat zich verantwoordelijk voelt voor de kwaliteit van bewaren en bewerken van een zo omvangrijke hoeveelheid de burger kwetsbaar makend materiaal. Hier dreigt iets eigenaardigs te gebeuren: omdat het efficiënter en doelmatiger is om het bewaren en bewerken van *alle* tot de persoon herleidbare verkeersgegevens over te laten aan het landsbestuur gaan we dat maar doen, ook als de instantie waartegen de grondrechten beschermen die bescherming en het toezicht daarop zelf ter hand neemt. Dat kan natuurlijk niet. Ook zou het extra risico's met zich brengen doordat de benodigde kwaliteiten niet altijd tot de kerncompetenties van het landsbestuur worden gerekend.

We wezen er al eerder op dat het Voorstel deze lezing ook niet toelaat, gelet op de rapportageverplichting die wordt opgelegd aan de telecomaanbieders en ISPs. We wezen ook op de betekenis die zo een plicht hebben kan voor het toezicht. Toch zal het, vermoeden we, een hele toer zijn deze figuur goed te implementeren in Nederland. De centrale organisatie is er al (het Informatiepunt). De gebruikersgegevens worden daar nu al volcontinu en volautomatisch naar doorgesluisd door de aanbieders. Om dat met verkeersgegevens niet ook te gaan doen zal vrijwel alle betrokkenen inefficiënt en onlogisch voorkomen.

Hoe dan ook, mocht de bewaarplicht toch feitelijk worden verwezenlijkt bij de telecomaanbieders en ISPs, dan ontstaan hier dezelfde plichten en taken ten aanzien van de bewaarde gegevens als bij de opsporings- en veiligheidsdiensten ten aanzien van de opgevraagde gegevens. We hebben overigens aanmerkelijk minder twijfels over de aanwezigheid bij de aanbieders van de benodigde kennis over IT-governance, van expertise, van wetskennis en van IT-verantwoordelijkheidsbesef dan bij de politie-organisatie: ze behoren wél tot de kerntaken van telecomaanbieders en ISPs en laten doorgaans weinig te wensen over. Het is dan ook eigenlijk jammer dat een brancheorganisatie voor ISPs, zoals de NLIP, juist in de laatste tijd maar een beperkt draagvlak blijkt te hebben. Als er al een centraal punt nodig is, zou dat bij de aanbieders wellicht in betere handen kunnen zijn.

Voor het Informatiepunt en het Agentschap

Als gezegd: het ligt meer voor de hand om inrichting en beheer van een centraal informatiepunt voor zowel gebruikers- als verkeersgegevens over te laten aan de ISPs en om het toezicht over te laten aan het Agentschap Telecom. Een analoge organisatorische figuur is succesvol gebleken in de informatie-afhandeling tussen banken en het toezicht daarop door de centrale bank. Maar we laten ons verleiden alvast te gaan denken aan oplossingen. Zoals de zaken er nu voor staan zullen de telecomaanbieders en ISPs individueel grote verzamelingen van gebruikers- en verkeersgegevens gaan aanleggen, waartoe de toegang zal worden geregeld via het Informatiepunt – een uitbreiding van de taken van dit punt, ook en vooral wanneer het niet over een eigen, volledige verzameling verkeersgegevens zal gaan beschikken – waarop weer toezicht zal moeten worden gehouden door het Agentschap Telecom. Daarmee ontstaat de verrassende figuur dat het Ministerie van Economische Zaken tot taak krijgt om toe te zien op een deel van de informatieverwerking van de opsporings- en veiligheidsdiensten die onder Justitie en Binnenlandse Zaken ressorteren. Hiervoor kan wel iets beters worden bedacht.

Voor e-commerce

Het aanleggen en beschikbaar houden van de elektronische communicatie over publieke netwerken volledig dekkende verzamelingen gebruikers- en verkeersgegevens voor pre-

59 Ministerie van Justitie, Platform Interceptie, Decryptie en Signaalanalyse, *Onderzoek naar de opslag van historische verkeersgegevens van telecommuniactie-aanbieders*, KPMG EDP Auditors 2004.

60 Cumulatief: vaste en mobiele telefonie, internet. Zie ook de jaarverslagen van OPTA (www.opta.nl).

ventie, opsporing en vervolging van strafbare feiten betekent voor het bedrijfsleven dat veel van het commerciële gegevensverkeer zal worden opgeslagen en voorwerp wordt van opsporingsactiviteiten. Daaraan zijn risico's verbonden. Ten eerste: wanneer die verzameling in verkeerde handen komt, kan daaruit bedrijfsgevoelige informatie worden afgeleid. Voorts zullen bedrijven, wanneer er al sprake is van strafbare feiten via communicatie-infrastructuren, er veelal de voorkeur aan geven deze intern of 'onder de pet' af te handelen.[61] Verder is het onduidelijk hoe lang het zal gaan duren alvorens de genoemde informatieverzamelingen zullen worden ingezet bij de opsporing van (bijvoorbeeld) fiscale misdrijven en criminaliteit die inbreuk maakt op de intellectuele eigendom. Deze omstandigheden zouden ertoe kunnen bijdragen dat het bedrijfsleven beleid ontwikkelt om veel meer dan thans gebruikelijk is gebruik te gaan maken van private netwerken en/of van beveiligingstechniek, een trend die thans al gaande is bij de versleutelde spraak- en internetcommunicatie.

Voor e-government

Een van de gevolgen van het Voorstel is, dat ook gebruikers- en verkeersgegevens van veel overheidscommunicatie zal worden vastgelegd, in elk geval voor zover deze wordt doorgeleid over openbare infrastructuren.[62] Ook hiervan kan de impuls uitgaan dat de overheid veel meer dan thans gebruik zal gaan maken van versleutelde spraak- en internetcommunicatie. Gelet op de mogelijkheden die meer in het algemeen bestaan om met name onversleutelde internetcommunicatie af te luisteren of af te tappen ('sniffen'), is dit zelfs een wenselijke ontwikkeling. Wij verbazen ons bijvoorbeeld over de kennelijke politieke aanvaardbaarheid van de volgende mededeling,[63] door de minister gedaan in antwoord op een vraag over de beveiliging tegen computercriminaliteit bij de overheid zelf:

> *De overheid maakt op sommige gebieden* [sic!] *reeds gebruik van encryptie. Zo wordt bijvoorbeeld voor de uitwisseling van persoonsgegevens binnen het GBA- en LRD-systeem en voor de paspoortaanvraag tussen gemeente en drukker gebruik gemaakt van Public Key versleutelingsoftware. Daarnaast heeft de Nederlandse overheid middels het programma PKI overheid het gebruik van Public Key encryptie voor zowel authenticatie, identificatie en voor vertrouwelijke communicatie bevorderd en mogelijk gemaakt.*

Uit dit antwoord lijkt te kunnen worden opgemaakt dat de overheid nog niet erg ver is met de beveiliging van zijn elektronische gegevensverkeer.

Voor de innovatie

Implementatie van het Voorstel kan op twee manieren iets betekenen voor de innovatieve kracht van Europa: (a) direct, door de impuls tot het ontstaan van een belangrijke nieuwe vraag en (b) indirect, door bijdragen aan de maatschappelijke voorwaarden die uitnodigen tot het ontplooien van onderzoeks- en R&D bedrijvigheid.

Een directe invloed gaat uit van de vraag naar ICT-diensten die kunnen ondersteunen bij de taak om voor preventie en opsporing relevante en meer specifieke informatie te destilleren uit de grote verkeersgegevensverzamelingen die beschikbaar komen. In samenhang met de internationale aan Echelon verwante projecten is daaraan al een impuls gegeven, een impuls die na 9/11 nog aanmerkelijk is verhevigd.[64] Op dit moment zijn op dit gebied veel activiteiten gaande – activiteiten die doorgaans berusten op de toepasbaarheid van onderzoek op het gebied van de Artificiële Intelligentie. Zo kunnen grote verzamelingen e-mail worden geanalyseerd door gebruik te maken van combinaties van grammaticale analyses, thesauri, doelgerichte taxonomieën, geografische databases en zoekprofielen. Onderzoek naar de verbetering van dergelijke technieken[65] wordt ruimhartig gefinancierd. De resultaten zullen hun toepassing zonder twijfel gaan vinden bij het analyseren van verkeersgegevens. Indirect zal dit mede leiden tot het besef dat onbeveiligde elektronische communicatie *de facto* niet kan worden opgevat als vertrouwelijk of zelfs maar betrouwbaar. En dat zal weer leiden tot de algemene vraag naar beveiliging van elektronische communicatie – een toename die nu al tot uitdrukking komt in de groeicijfers van beveiligde mobiele telefonie. Het lijkt ons evenmin uitgesloten dat een wildgroei zal ontstaan op de markt voor adresversluierende proxy-serverdiensten.

Meer in het algemeen verwachten we dat de tegengestelde, evenwichtzoekende krachten die de beschikbaarheid en de beveiliging van elektronische communicatie in elkaars armen gevangen houden kunnen escaleren. Elke ontwikkeling die de toegankelijkheid vergroot heeft dan het gevolg dat meer werk wordt gemaakt van beveiliging – en vice versa. Wanneer het verwezenlijken van de bewaarplicht ertoe leidt dat beveiligde spraak- en internetcommunicatie met versluierde adressering net zo algemeen beschikbaar komt en net zo gemakkelijk te realiseren valt als nu het beveiligen van internetverkeer,[66] dan komt de betekenis van de hierboven genoemde geavanceerde analyse-instrumenten in gevaar. En dat zal weer om een nieuwe reactie vragen.

Intussen is elke uitbreiding van de beveiliging naar zijn aard een extra belemmering voor het gebruik. Genoemde escalatie speelt zich af in de context van globaliserende verhoudingen. En het is de vraag, of de specifiek Europees-Nederlandse resultaten ervan zullen bijdragen aan de voorwaarden waaronder het Nederlandse bedrijfsleven zich internationaal zal kunnen ontplooien.

Voor de criminaliteit

Het voorstel heeft verschillende gevolgen voor verschillende vormen van criminaliteit. Voor de bestrijding van terrorisme zal er – wanneer de inlichtingen- en veiligheidsdiensten thans reeds beschikken over Echelon-achtige informatiebronnen[67] – niet veel veranderen. Hoogstens valt te verwachten dat terroristische netwerken in de toekomst meer en betere beveiliging beschikbaar zullen krijgen door de hierboven genoemde innovatie. Voor de 'gewone' criminaliteit is er een grote verandering: de beschikbare opsporingsmogelijkheden worden door de algemene beschikbaar- en doorzoekbaarheid van alle verkeersgegevens, in samenhang met geavanceerde zoek- en

61 Zie bijvoorbeeld *Kamerstukken II* 2004/05, 26 671, nr. 10.

62 Daarmee lijkt weinig mis. In tegendeel: die informatie kan nog van belang zijn voor het toezicht.

63 *Aanhangsel Handelingen II* 2004/05, nr. 1162.

64 Keefe 2005; O'Harrow 2005.

65 Ook voor de analyse van audio- en beeldmateriaal.

66 Als met behulp van TLS of SSL: in het adresvenster van de browser staat dan https:// in plaats van http://.

67 Wij gaan daar vanuit, mede gelet op de sterke impuls die van de aanslagen van 9/11 en daarna is uitgegaan op internationale samenwerking tussen veiligheidsdiensten. Zie ook: O'Harrow 2005.

verwerkingstechnieken aanmerkelijk versterkt. De effectiviteit ervan is afhankelijk van de manier waarop toegang tot en gebruik van het materiaal voor de opsporingsdiensten zal worden geregeld, en hoe effectief het toezicht daarop zal zijn. Wij verwachten dat onder de noemer van terrorismebestrijding vooral de mogelijkheden voor het tegengaan van 'gewone' criminaliteit zullen worden versterkt.

Voor de burger

We verwachten voor de burger dat het Voorstel, in elk geval in potentie, verdergaande inbreuken op zijn persoonlijke levenssfeer en, daarmee, verdere beperkingen van zijn autonomie tot gevolg zullen hebben. Deelname aan het maatschappelijke leven is inmiddels niet goed meer mogelijk zonder gebruik te maken van elektronische communicatie. En het gebruiken van elektronische communicatie brengt met zich dat veel van de individuele keuzen geregistreerd worden door telecomaanbieders of ISPs en, via het Voorstel, in beginsel bekend worden bij de autoriteiten. De individuele burger wordt tegen het ongelegitimeerd gebruik daarvan beschermd door de grondrechten en de wettelijke uitwerking daarvan. De effectiviteit van die bescherming en het vertrouwen daarin zal van doorslaggevende betekenis zijn voor de vrijheid waarin de burger gebruik zal kunnen en willen maken van elektronische communicatie. Het is een kenmerk van onze democratie dat de burger op de regulering en inrichting daarvan geen directe invloed heeft en moet hopen op de steun van organisaties die voor zijn belangen opkomen. De Consumentenbond en de stichting Bits of Freedom zijn dergelijke organisaties. Voor de burger zal veel afhangen van de wijze waarop zij hem zullen vertegenwoordigen bij het optuigen van de instituties (en het bijbehorende toezicht) die uiteindelijk zullen uitmaken hoe het Voorstel zal worden verwezenlijkt in Nederland. Wij vrezen dat een te sterke nadruk op principes en beginselen daarbij weinig zal uithalen. Lessig wees er terecht en overtuigend[68] op, hoezeer de architectuur van de elektronische communicatie van betekenis is voor de regulering van het gebruik ervan. De beschikbaarheid van verkeersgegevens bij telecomaanbieders en ISPs is een architectuurkenmerk van elektronische communicatie. Principieel bezwaar tegen die beschikbaarheid leidt onvermijdelijk tot praktisch bezwaar tegen elektronische communicatie *tout court*. Wie zo ver niet wil gaan, is erop aangewezen zijn aandacht te richten op de manieren waarop toegang tot en gebruik van die informatie ordentelijk kunnen en zullen worden gereguleerd en, daarmee, op de manieren waarop effectief toezicht kan en zal worden verwezenlijkt en adequate schadevergoedingen kunnen en zullen worden toegekend wanneer fouten zijn gemaakt.

Afsluitende opmerkingen

De juridische kwaliteit van het Voorstel wordt doorgaans geplaatst in het teken van het legitieme evenwicht tussen het recht tot verwerken van persoonsgegevens door bevoegde autoriteiten ten behoeve van opsporing en preventie van criminaliteit aan de ene kant en het recht op een persoonlijke levenssfeer ten behoeve van de individuele mogelijkheden zich vrij te ontplooien en te uiten anderzijds. Het hierboven aangehaalde artikel V van de Guidelines of the Comittee of Ministers of the Council of Europe on Human Rights and the fight against Terrorism van 11 juli 2002 stelt daar drie eisen aan: (1) dat die verwerking adequaat is gereguleerd door nationale wetgeving,[69] (2) dat die verwerking wordt onderworpen aan extern en onafhankelijk toezicht[70] en (3) dat die verwerking proportioneel is in relatie tot het doel ervan.[71]

Adequate regulering door nationale wetgeving

Zolang er nog geen wetsvoorstellen zijn die het Voorstel implementeren, kan over adequate nationale regelgeving natuurlijk geen oordeel worden gegeven. Maar we kunnen uiteraard wel een oordeel geven over het Voorstel. En daarbij ligt het voor de hand dat we ook kijken naar de huidige wettelijke regelingen voor de verwerking van persoonsgegevens ten behoeve van opsporing en preventie. Als wij een en ander vanuit de bovengenoemde drie in de Guidelines geïdentificeerde criteria bezien, komen wij tot de volgende kanttekeningen:

De huidige regeling heeft een rommelig en onoverzichtelijk karakter, veroorzaakt door een combinatie van regelingen van verschillend niveau en onlogische datering, en het ontbreken van enkele uitvoeringsregelingen. Wij zijn er niet een-tweedrie van overtuigd dat implementatie van het Voorstel daar vanzelf verandering inbrengt. Dat zou wel moeten.

Ook de onzekerheid die bestaat over de uitleg van kernbegrippen als 'openbaar' en de te bewaren gegevens is een tekortkoming voor een wettelijke regeling die zich daarop richt. In dit opzicht brengt het Voorstel geen verbetering, eerder het omgekeerde. Daarmee ontstaat een onaanvaardbare spanning met het wetmatigheidsvereiste, dat niet voor niets onderdeel uitmaakt van regelingen ter bescherming van de persoonlijke levenssfeer.

Ten slotte valt een belangrijk deel van de huidige verwerking buiten de toepasselijke wettelijke regeling omdat deze berust op vrijwillige beschikbaarstelling door ISPs volgens ondershandse procedures. Hieraan zou een eind moeten komen.

Wij zijn geneigd de huidige wettelijke regeling vanuit juridisch gezichtspunt niet adequaat te achten en zien in de eerder aangehaalde uitspraak van het Europees Hof voor de Rechten van de Mens steun voor dit oordeel. Als het recht onvoldoende houvast gaat bieden om een heldere rol te spelen wanneer er in de praktijk iets fout gaat of scheef groeit, dan kan het recht juist in die gevallen zijn rol minder goed spelen in relatie tot het risico van willekeurig bestuur.

De onderwerping aan extern en onafhankelijk toezicht

Ook over dit criterium valt niet anders te oordelen dan aan de hand van de bestaande regeling. Wij sluiten ons aan bij het oordeel van Kielman en Koelewijn, die uit evaluaties van de Wet politieregisters en uit mededelingen daarover van de kant van het College bescherming persoonsgegevens afleiden dat het toezicht niet alleen onvoldoende is geregeld, maar ook onvoldoende wordt verwezenlijkt.[72] We zouden ons er – met

68 Steeds overtuigender, eigenlijk, wanneer men zich bedenkt dat zijn *Code and other Laws of Cyberspace* uit 1999 dateert.

69 *[...] governed by appropriate provisions of domestic law [...].*

70 *[...] may be subject to supervision by an external independent authority [...].*

71 *[...] proportionate to the aim for which the collection and the processing were foreseen [...].*

72 Kielman en Koelewijn 2005.

onze ervaring – niet meer over moeten verbazen, maar doen dat toch. Schandalen als die bij Enron, Ahold, WorldCom en Parmelat hebben ertoe geleid dat het toezicht op de gegevensverwerking van beursgenoteerde bedrijven in de laatste jaren zeer sterk is verbeterd. Het ware wenselijk wanneer ook aan de verantwoordelijke overheidsfunctionarissen de verplichting werd opgelegd persoonlijk garant te staan voor de kwaliteit van de verslaglegging over de verwerking. En voor de rapportage over de procedures (de *policies*) die daartoe intern worden ingesteld, gebruikt en gehandhaafd.[73] En in aanvulling daarop: welke instantie ook zal worden belast met het toezicht op de verkeersgegevensverwerking, die instantie dient – onzes inziens – met zwaarder geschut te worden uitgerust en te werken dan thans gebruikelijk is bij de meeste externe, onafhankelijke toezichthouders, gericht op de overheid. Ook hier, als niet in adequate handhaving en toezicht is voorzien, treedt het risico van willekeurig bestuur naar de voren.

De proportionaliteit van de verwerking

De proportionaliteit van het bewerken van de volledige verzameling van verkeersgegevens ten behoeve van preventie en opsporing is voorwerp van heftige discussie, en zal dat vermoedelijk ook blijven. Eigenlijk geeft dit eerder aan hoe weinig betekenisvol het vereiste van proportionaliteit soms kan zijn bij politieke dilemma's die verdeeldheid veroorzaken. Voor de één is het vanzelfsprekend dat het beschikbaar houden en verwerken van een hoeveelheid informatie waarvan niet meer dan 0.0000001 promille[74] effectief zal kunnen worden gebruikt onmogelijk proportioneel kan zijn – zeker niet, wanneer die gegevensverzameling de potentie heeft om significante aspecten van het persoonlijke leven van vrijwel alle burgers bekend te maken. Voor de ander is het risico van terroristische aanslagen zo verontrustend, dat élk verzet tegen verdere offers op het gebied van de persoonlijke levenssfeer onbegrijpelijk voorkomt. Interessant is, dat dit vraagstuk zich schijnt te lenen voor rechtseconomische analyse.[75] Wij verwachten evenwel niet dat die discussie zal kunnen worden beslecht door dergelijke rationele analyses. We denken overigens evenmin dat juridische expertise daarbij van doorslaggevende betekenis zal zijn. Daarmee geraken we dus buiten onze eigen gebiedjes.[76] Het risico van ideologisch verhardende verdeeldheid is hier aan de orde – tussen wie in grondrechten gelooft en wie in een recht op een veilige samenleving.

Recht en risico

Het gaat om het vormen van nieuw recht als politieke reactie op – geenszins fictieve – maatschappelijke risico's.[77] Het risico van terroristische zelfmoordacties is (voor ons) nog betrekkelijk nieuw. Hoewel het Voorstel mede is ingegeven ter instrumentatie van de preventie en opsporing van terroristische aanslagen lijkt het daarvoor niet veel extra te bieden, tenminste wanneer ons vermoeden juist is dat de veiligheidsdiensten al over verkeersgegevens beschikken. Het Voorstel is wel van praktische betekenis voor de preventie en opsporing van 'gewone' (al dan niet georganiseerde) criminaliteit. Het risico van willekeurig bestuur wordt onzes inziens in het Voorstel onvoldoende onder ogen gezien, hetgeen tot uiting komt in bijzonder weinig aandacht voor het toezicht op het legitieme gebruik van de bewaarde gegevens. Aandacht bij de implementatie voor dit punt is dan ook van groot belang. Het risico dat individuele ontplooiings- en uitingsmogelijkheden op grote schaal worden beperkt (het risico van een open samenleving die zich sluit) leeft nog vaag in ons collectieve geheugen. Afhankelijk van de mate waarin de burger vertrouwt op het legitieme gebruik van de bewaarde gegevens wordt dit risico beter in toom gehouden.

Het Voorstel schiet onzes inziens hier in zijn huidige vorm tekort omdat het onvoldoende voorziet in waarborgen voor en toezicht op legitiem gebruik van de bewaarde gegevens. Het risico van verhardende ideologische verdeeldheid in de samenleving openbaart zich in twee vormen. De eerste betreft de tegenstelling tussen moslimfundamentalisten en nationalisten. Het recht kan hier een bijdrage leveren door niet te discrimineren, aldus de Raad van Europa. Men zou, in het spoor daarvan, op prudentie hopen bij het gebruik van de bewaarde gegevens. Aan het recht hoeft niet veel te gebeuren in dit opzicht, er bestaat immers al een verbod op discriminatie. De handhaving laat nog wel eens te wensen over. De tweede relevante tegenstelling kan ontstaan tussen wie gelooft in de mensenrechten en wie gelooft in een recht op bescherming ten koste van de mensenrechten. Deze vormen de twee gezichten van de Januskop die het Voorstel introduceert: verkeersgegevens als wondermiddel tegen terrorisme voor de een – als belemmering van de individuele vrijheid voor de ander. Wij gaan dat probleem niet oplossen.[78] Het gaat hier ook eerder om een culturele dan om een rationele tegenstelling. Door een juridische bril betekent dat wel, dat aan beide culturen recht moet worden gedaan: ieder het zijne. En dat houdt weer in dat we aanbevelen om in de regeling van de verwerking van verkeersgegevens ten behoeve van terrorisme- en criminaliteitsbestrijding toereikende voorzieningen op te nemen ter compensatie van die gevallen, waarin fouten zijn gemaakt – fouten waarvan het aantal onvermijdelijk zal toenemen. Als dat het risico is dat onder de druk van de dreiging van terrorisme moet worden genomen, moeten we het ook onder ogen durven zien.

73 Rond de Amerikaanse Sarbanes-Oxley wet van 2002 is een vertrouwenwekkende praktijk ontstaan van toezicht op interne bedrijfsgegevensverwerking. Daarvan valt onzes inziens voor de Nederlandse overheid het een en ander op te steken.

74 Zie bijvoorbeeld de bijdrage van H. Franken aan het debat met de Minister van Justitie in de Eerste Kamer: http://www.ejure.nl/mode=display/downloads/dossier__id=193/id=270/050628__Franken__bewaarplicht.pdf.

75 Zij het in de privaatrechtelijke sfeer: Kai-Ling Hui en I.P.L. Ping, The Economics of Privacy, *Handbook of Information Systems and Economics*, 2005, http://www.comp.nus.edu.sg/~lung/The-Economics-of-Privacy.pdf; curieus is in dit verband: R.A. Posner, *Orwell versus Huxley: Economics, Technology, Privacy, and Satire*, University of Chicago Law School, John M. Olin Law & Economics Working Paper No. 89, November 1999, http://papers.ssrn.com/sol3/papers.cfm?abstract__id=194572#PaperDownload.

76 D.w.z. recht en informatica resp. telecommunicatie- en privacyrecht.

77 Daardoor kan de kwaliteit van ons eigen rechtssysteem in het gedrang komen, in casu doordat het verandert onder invloed van de op stapel staande aanpassingen ten behoeve van de beteugeling van terrorisme en ten koste van de bescherming van de privacy. Over de duurzaamheid van ons rechtssysteem is wel verdedigd dat jurisdictie, legitimiteit, integriteit en stabiliteit de relevante beoordelingscriteria zijn. De eerste drie hiervan zijn hierboven impliciet aan de orde geweest. De verdeeldheid over de vraag of het Voorstel nu wel of niet proportioneel is raakt aan het vraagstuk van de stabiliteit. Zie A.H.J. Schmidt, *Bedreigen Computers ons Rechtssysteem?* Universiteit Leiden 2004. http://www.rechteninformatica.leidenuniv.nl/content__docs/Medewerkers/Aernout__Schmidt/oratie-schmidt-1.pdf.

78 Voor mogelijk relevante politiek-wetenschappelijke benaderingen van dergelijke risico's verwijzen we gaarne naar M. Smits, *Monsterbezwering – De culturele domesticatie van nieuwe technologie*, Boom 2002, dat weer mede is gebaseerd op: M. Douglas en A. Wildavsky, *Risk and culture - An essay on the selection of technical and environmental dangers*, Berkeley 1982.