Daar kon je op wachten: richtlijn bewaarplicht ongeldig verklaard

Gerrit-Jan Zwenne en Frank Simons[*]

In wat door verschillende commentatoren wordt aangeduid als een 'landmark decision' heeft het Hof van Justitie van de Europese Unie op 8 april jl. de Europese dataretentierichtlijn (2006/24/EG) ongeldig verklaard. Daarmee zijn er serieuze twijfels ontstaan over de houdbaarheid van de bewaarplicht op grond waarvan telecom- en internetaanbieders in Nederland gehouden zijn om bel- en internetgegevens te bewaren voor gebruik door politie, justitie en inlichtingendiensten.

1. Inleiding

Het komt niet vaak voor dat een richtlijn ongeldig wordt verklaard.[1] En toch was het niet voor iedereen een heel grote verrassing dat het Hof van Justitie van de Europese Unie daartoe overging in zijn uitspraak van 8 april jl. in de zaken C-293/12 en C-594/12.[2] De uitspraak is relevant voor de nationale wetten waarmee de lidstaten de richtlijn hebben geïmplementeerd en bewaarplichten in aan telecom- en internetaanbieders hebben opgelegd. Echter de betekenis ervan gaat veel verder. In de uitspraak komt het hof met een aantal criteria die zonder meer relevant zijn voor bestaande en nieuwe wet- en regelgeving gericht op het voor politie en justitie, en inlichtingendiensten, beschikbaar maken van uiteenlopende gegevens.

In deze bijdrage een bespreking van de bewaarplicht en de gevolgen van het arrest daarvoor. Om het geheugen op te frissen beginnen wij met een korte bespreking van wat onze nationale bewaarplicht omvat (par. 2), waarna wij ingaan op de uitspraak van het Hof (par. 3) om vervolgens daaraan schetsmatig enige duiding te geven (par. 4).

2. Onze bewaarplicht

De dataretentierichtlijn legt aan EU-lidstaten de verplichting op om ervoor zorg te dragen dat telecom- en internetaanbieders een aantal categorieën van bel- en internetgegevens gedurende ten minste zes en ten hoogste 24 maanden beschikbaar houden voor gebruik in het kader van strafvordering en inlichtingen en veiligheid. In Nederland is de bewaarplicht uiteindelijk, na veel discussie in de volksvertegenwoordiging en daarbuiten,[3] geïmplementeerd in art. 13.2a van de Telecommunicatiewet (hierna: Tw). [4]

In het tweede lid van deze bepaling wordt aan aanbieders van openbare telecommunicatienetwerken of –diensten de verplichting opgelegd om de in de bijlage bij de wet aangewezen verkeers- en locatiegegevens, voorzover deze in het kader van de door hen aangeboden netwerken of diensten worden gegenereerd of verwerkt, te bewaren ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.

In dat verband wordt onder verkeersgegevens verstaan de gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan (art. 11.1, onder b, Tw). Onder locatiegegevens worden de gegevens verstaan die worden verwerkt in een openbaar elektronisch communicatienetwerk of –dienst waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven (art. 11.1, onder b, Tw). In aanvulling daarop vallen onder de bewaarplicht ook de beschikbare gegevens betreffende zogeheten 'oproeppoging zonder resultaat', dat wil zeggen gegevens over de communicatie waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord (art. 13.2a, eerste lid, onder b).

In alle gevallen gaat het om zogenoemde metagegevens over wie, waar, wanneer en met wie communiceert, en niet om de inhoud van de communicatie. Voor internetverkeer moet bijvoorbeeld wél worden bewaard op welke momenten en met

---

* Frank Simons is advocaat bij Bird & Bird LLP te Den Haag, evenals Gerrit-Jan Zwenne die daarnaast hoogleraar Recht en de informatiemaatschappij is in Leiden.

1. Zie voor verschillende andere voorbeelden van ongeldig verklaarde richtlijnen: T.A.J.A. Vandamme, *The invalid directive : the legal authority of a union act requiring domestic law making*, (diss UVA) 2005.
2. In zijn conclusie van 12 december 2013, ECLI:EU:C:2013:845, in deze zaken had Advocaat-Generaal Cruz-Villalón al geoordeeld dat de richtlijn onverenigbaar met het Handvest van de grondrechten. Hij stelt evenwel de wetgever van de Unie een redelijke termijn te geven om de vastgestelde ongeldigheid ongedaan te maken.
3. Zie bijv. 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, alsmede A.H.J. Schmidt & G-J. Zwenne, 'Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatieverkeersgegevens', *Mediaforum* 2005-9, p. 292-302 en het vervolg daarop G-J. Zwenne en A.H.J. Schmidt, 'Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens', *Mediaforum* 2008/7-8, p. 278-285 en G-J. Zwenne en F. Simons, 'Duitse bewaarplicht ongrondwettig. En in Nederland?', *IR* 2010, nr. 3, p. 87-94.
4. *Stb*. 2009, 333.

welk IP-adres een (ADSL-, kabel- of mobiele) internetverbinding wordt opgezet, en aan welke adressen e-mails worden verstuurd, maar níet welke websites (URL's) worden bezocht of wat de inhoud is van verzonden of ontvangen e-mails.[5]
Voor de duur van de bewaartermijn wordt onderscheid gemaakt naar enerzijds telefoongegevens (of eigenlijk: 'gegevens in verband met telefonie over een vast of mobiel netwerk)[6] en anderzijds internetgegevens ('gegevens in verband met internettoegang, e-mail over het internet en internettelefonie').[7] Voor telefoongegevens geldt een bewaartermijn van twaalf maanden, voor de internetgegevens werd aanvankelijk uitgegaan van eenzelfde termijn, maar die werd op aandringen van de Eerste Kamer uiteindelijk teruggebracht tot 6 maanden.[8]
De bewaarde gegevens kunnen gedurende deze bewaartermijnen bij de aanbieders worden opgevraagd door de officier van justitie (OvJ) en de inlichtingen- en veiligheidsdiensten, de AIVD en MIVD[9], maar alleen voor het onderzoeken, opsporen of vervolgen van ernstige misdrijven. In de wetstekst (art. 13.2a, tweede lid, Tw) is immers niet zonder reden de beperking opgenomen dat de gegevens worden bewaard ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven, zijnde de misdrijven waarvoor voorlopige hechtenis mogelijk is of die in georganiseerd verband zijn beraamd of gepleegd en die een ernstige inbreuk op de rechtsorde opleveren, alsmede terrorisme.[10]

3. De uitspraak

In de uitspraak beoordeelt het Hof de richtlijn, niet de nationale wetten waarmee deze is geïmplementeerd. Niettemin heeft de uitspraak ook voor die nationale wetgeving betekenis, al was het maar omdat voor de onderbouwing van het invoeren van nationale bewaarplichten niet meer alleen kan worden verwezen naar de gehoudenheid van lidstaten om de richtlijn om te zetten in nationaal recht.
Aanleiding voor de procedure bij het Hof waren prejudiciële vragen van de Ierse High Court en het Oostenrijkse Verfassungsgerichtshof. De beide rechtscolleges verzochten het Hof om de geldigheid van de richtlijn te toetsten aan onder andere de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie,[11] die zien op respectievelijk het recht op eerbiediging van het privé-leven (incl. familie- en gezinsleven) en het daaraan verwante recht op bescherming van persoonsgegevens.
Om te beginnen stelt het Hof vast dat de aan telecom- en internet aanbieders opgelegde bewaarplicht op zich al een inmenging vormt in de door art. 7 van het Handvest gewaarborgde recht op privacy.[12] De toegang van de bevoegde nationale autoriteiten tot de gegevens vormt volgens het Hof een aanvullende inmenging in dat fundamentele recht. [13]
Daarbij betekent de richtlijn ook een inmenging in het door art. 8 van het Handvest gewaarborgde fundamentele recht op bescherming van persoonsgegevens, aangezien zij voorziet in de verwerking van persoonsgegevens. [14]
Bovendien gaat het naar het oordeel van het Hof om een zeer ruime en bijzonder zware inmenging ('*wide-ranging […] and particularly serious interference'*) in deze fundamentele rechten en kan de omstandigheid dat de gegevens worden bewaard en later worden gebruikt zonder dat de betrokkenen wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden:

> 'Vastgesteld moet worden dat richtlijn 2006/24 een zeer ruime en bijzonder zware inmenging vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde fundamentele rechten, zoals de advocaat-generaal met name in de punten 77 en 80 van zijn conclusie heeft opgemerkt. Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de abonnee of de geregistreerde gebruiker hierover wordt ingelicht, bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, zoals de advocaat-generaal in de punten 52 en 72 van zijn conclusie heeft opgemerkt'.[15]

Daarmee is evenwel nog niet gezegd dat de bewaarplicht onverenigbaar zou zijn met het Handvest. Het bestrijden van internationaal terrorisme en ernstige criminaliteit kan in beginsel een dergelijke inmenging rechtvaardigen. De wijze waarop de bewaarplicht in de richtlijn is geregeld, acht het Hof om twee redenen evenwel niet evenredig.

Onvoldoende duidelijke en precieze regels en criteria

In de eerste plaats bevat de richtlijn volgens het Hof onvoldoende duidelijke en precieze regels en criteria betreffende de omvang van de inmenging in de door de genoem-

5. Dat laat overigens onverlet dat de officier van justitie dergelijke gegevens kan opvragen, bijv. op grond van art. 126nd Sv, als die voor andere doeleinden worden bewaard.
6. O.a. telefoonnummers van oproeper en opgeroepene, datum en tijdstip van de oproep, locatie van de oproeper.
7. O.a. de zgn. gebruikersidentificaties, datum en tijdstip van log-in en log-off.
8. Zie Wetsvoorstel Wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang, e-mail over het internet en internettelefonie *Kamerstukken II* 2009/2010-2010/2011, 32 185, nrs. 1-13 en *Kamerstukken I* 2010/11, 32 185, A, alsmede *Stb.* 2011, 350.
9. De desbetreffende bevoegdheden van de OvJ resp. AIVD/MIVD zijn geregeld in art. 126n, 126u en 126zh Sv, resp. art. 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002).
10. *Kamerstukken I* 2007/08, 31 145, B, p. 3 en C, p. 4. In het licht van recente voorbeelden van gebruik van telecomtapgegevens in kartelonderzoeken is het overigens niet ondenkbaar dat ook toezichthouders, in weerwil van wat de wetgever daarover heeft gezegd, proberen om toegang te verkrijgen tot de bewaarde verkeers- en locatiegegevens in het kader van bestuursrechtelijke toezicht- en handhavingstrajecten – iets wat een schoolvoorbeeld zou zijn van 'function creep' of 'mission creep'; zie F. Simons en G-J. Zwenne 'Hof van Justitie: Europese bewaarplicht telecomgegevens strijdig met privacygrondrechten', *Tijdschrift voor Toezicht*, 2014/2. Zie ook B.D.P. van der Eijk 'Bewaar- en weggooiverplichtingen in de strijd tegen copyrightinbreuk - annotatie bij HvJEG, 19 april 2012, C301/06 (Bonnier Audio c.s.)', *IR* 2013, nr. 3, p. 83-86.
11. Handvest van de grondrechten van de Europese Unie, *PbEU* 2007/C 303/01.
12. Overw. 34.
13. Overw. 35.
14. Overw. 36.
15. Overw. 37.

de fundamentele rechten. Dat geldt voor de reikwijdte van de bewaarplicht zelf, voor de begrenzing van de toegang tot de gegevens door bevoegde autoriteiten en voor de termijn waarvoor de gegevens moeten worden bewaard.
Wat betreft de reikwijdte van de bewaarplicht overweegt het Hof dat die betrekking heeft op gegevens betreffende alle eindgebruikers van telecomnetwerken (d.w.z. nagenoeg iedereen), met inbegrip van al degenen tegen wie geen enkele verdenking van ernstige criminaliteit bestaat. In dat verband wijst het hof er ook op dat de bewaarplicht zich zelfs uitstrekt tot de communicatie van degenen met een beroepsgeheim ('zakengeheim'), zoals advocaten en artsen. Ookis de bewaarplicht volgens het hof onvoldoende duidelijk afgebakend, zoals wat betreft periode en geografische locatie waarop de gegevens betrekking hebben. Het Hof zegt het zo:

> 'Richtlijn 2006/24 is om te beginnen algemeen van toepassing op alle personen die gebruikmaken van, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. […]
> Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.'[16]

Verder is volgens het Hof onvoldoende duidelijk wanneer en onder welke voorwaarden nationale autoriteiten toegang tot de gegevens kunnen hebben. De richtlijn volstaat met het voorschrijven dat lidstaten moeten zorg dragen voor procedures met betrekking tot wie toegang hebben tot de gegevens, maar voorziet er niet in dat er alleen sprake zou moeten zijn van toegang tot de bewaarde gegevens als dat nodig is ter voorkoming of bestrijding van welbepaalde gevallen van ernstige criminaliteit:[17]

> '[De] richtlijn 2006/24 [bevat] niet alleen geen beperkingen, maar ook geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. […]
>
> Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. […] In het bijzonder bevat richtlijn 2006/24 geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel. Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. […].'[18]

Ook over de bewaartermijn geeft de richtlijn volgens het Hof onvoldoende duidelijke en precieze regels, onder meer omdat geen onderscheid wordt gemaakt tussen de bewaartermijn voor categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel:

> 'Wat […] de termijn betreft gedurende welke de gegevens worden bewaard, bepaalt artikel 6 van richtlijn 2006/24 dat deze gedurende ten minste zes maanden moeten worden bewaard, zonder dat enig onderscheid wordt gemaakt tussen de in artikel 5 van deze richtlijn genoemde categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen.
> Bovendien varieert de bewaringstermijn van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is.' [19]

Een en ander maakt volgens het Hof dat niet is gewaarborgd dat de zeer ruime en bijzonder zware inmenging in de fundamentele rechten daadwerkelijk wordt beperkt tot wat strikt noodzakelijk is.[20]

Onvoldoende bescherming tegen misbruik en onrechtmatige toegang

In de tweede plaats vindt het Hof dat de richtlijn onvoldoende garanties biedt dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en onrechtmatige toegang. Dit onder andere omdat de richtlijn niet voorschrijft dat gegevens binnen de EU worden opgeslagen waardoor onvoldoende is gewaarborgd dat een onafhankelijk autoriteit toezicht kan houden op de beveiliging van de gegevens:

> 'Bovendien moet […] worden vastgesteld dat richtlijn 2006/24 onvoldoende garanties biedt dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan, zoals wordt vereist door artikel 8 van het Handvest. In de eerste plaats bevat artikel 7 van richtlijn 2006/24 geen specifieke regels die aangepast zijn aan de enorme

16. Overw. 58 t/m 59.
17. Overw. 57 t/m 64.
18. Overw. 60 t/m 62.
19. Overw. 63 t/m 64.
20. Overw. 65.

> hoeveelheid gegevens die volgens deze richtlijn moeten worden bewaard, alsook aan het gevoelige karakter van deze gegevens en aan het risico dat zij op onrechtmatige wijze zullen worden geraadpleegd […]. In de tweede plaats schrijft deze richtlijn niet voor dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard, zodat niet ten volle is gewaarborgd dat een onafhankelijke autoriteit toezicht houdt op de inachtneming van de in de twee vorige punten bedoelde vereisten inzake bescherming en beveiliging […].'[21]

Een en ander brengt het hof tot het oordeel dat de EU-wetgever met de vaststelling van de dataretentierichtlijn de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, eerste lid, van het Handvest in acht dient te nemen. En dat brengt met zich dat de richtlijn ongeldig is.[22]

4. Wat nu?

De dataretentierichtlijn trad zo een acht jaar geleden in werking en heeft vanaf dat moment een bestaan geleid dat als moeizaam kan worden gekarakteriseerd. In verschillende lidstaten liet de implementatie van de richtlijn lang op zich wachten, mede in verband met moeilijke keuzes waarbij privacybescherming moest worden afgewogen tegen de noodzaak om criminaliteit te bestrijden.[23] En in een aantal gevallen, namelijk in Bulgarije, Roemenië, Cyprus, Duitsland en Tsjechië, oordeelden de constitutionele rechtscolleges dat de nationale wetten ter implementatie van de richtlijn geheel of gedeeltelijk onhoudbaar waren wegens strijd met privacygrondrechten.[24]

Zoals gezegd is in Nederland het wetsvoorstel voor de bewaarplicht,[25] na enige discussie in de Tweede Kamer en veel meer discussie in de Eerste Kamer, al met al betrekkelijk ongeschonden aangenomen. Wel laaide de discussie over de evenredigheid van de bewaarplicht van tijd tot tijd weer op. Dat gebeurde meestal naar aanleiding van publicaties waaruit de beperkte toegevoegde waarde van de bewaarde gegevens bleek.[26]

Het meest recent voorbeeld[27] betreft het door WODC uitgevoerde evaluatie-onderzoek van de bewaarplicht dat de Minister van Veiligheid en Justitie op 12 februari 2014 aan de Tweede Kamer zond.[28] In het rapport doet WODC verslag van haar onderzoek naar het gebruik van de bewaarde gegevens bij de opsporing. Een van de conclusies was dat weliswaar telefoongegevens veelvuldig worden opgevraagd en geanalyseerd, maar dat bewaarde internetgegevens betrekkelijk weinig worden gebruikt. In dat verband kwam het WODC tot het oordeel dat de bewaarplicht voor wat betreft de internetgegevens achterhaald is:

> '[d]oor de voortschrijdende technische ontwikkelingen [..] de huidige bewaarplicht voor internetgegevens grotendeels achterhaald is'.

Het WODC acht dat onwenselijke en dringt aan op een zorgvuldige heroverweging van de regeling. Het lijkt overigens sceptisch over de bewaarplicht, getuige de opmerking in het rapport dat:

> 'het er [...] naar uit [ziet] dat met het opvragen van telecommunicatiegegevens in de toekomst steeds minder nuttige informatie kan worden opgevraagd.'[29]

Uit een kamerbrief van de Minister van Economische Zaken blijkt dat de regering van plan is de consequenties van de uitspraak van het Hof mee te nemen in de herziening van onze nationale bewaarplicht naar aanleiding van het evaluatierapport.[30] En de bewindspersonen verantwoordelijk voor Veiligheid en Justitie, die gaan over degenen die gebruik maken van de bewaarde gegevens (de zgn. behoeftestellers), hebben laten weten de uitspraak van het Hof eerst nader te willen bestuderen voordat zij daaraan conclusies verbinden. Daarbij willen zij ook het advies van de Raad van State en het College bescherming persoonsgegevens betrekken.[31] Uiteraard valt er weinig op aan te merken dat het advies van de beide instanties wordt afgewacht. Ons komt het voor dat de uitspraak van het Hof hoe dan ook weinig ruimte laat voor het ongewijzigd handhaven van de bewaarplicht van art. 13.2a Tw. In de uitspraak stelt het Hof immers dat de toegang tot de bewaarde telecomgegevens moet zijn beperkt tot wat strikt noodzakelijk is voor het voorkomen, opsporen of vervolgen van ernstige criminaliteit. En dat lijkt, ook in het licht van het evaluatierapport, moeilijk te onderbouwen. Op grond van de bewaarplicht lijkt veel meer te worden bewaard dan voor dat doel nodig is. In elk geval zal het niet

---

21. Overw. 66 t/m 68.
22. Overw. 69, 71 en dictum.
23. Meest recent HvJEU, 30 mei 2013, C-270/11 (Commissie/Zweden); zie verder C. Jones & B. Hayes, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, November 2013, <http://secile.eu/data-retention-in-europe-case-study/>.
24. Zie G-J. Zwenne en en F. Simons, 'Duitse bewaarplicht ongrondwettig. En in Nederland?', *IR* 2010, nr. 3; zie ook Chris Jones & Ben Hayes, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, November 2013, <http://secile.eu/data-retention-in-europe-case-study/>.
25. Wetsvoorstel Wet bewaarplicht telecommunicatiegegevens, *Kamerstukken II* 2006/07-2007/08, 31 145 nrs. 1-26 en *Kamerstukken I* 2007/08-2013/14, A-Y.
26. Zoals Vgl. L. Essers, 'Bewaarplicht telecomgegevens nutteloos', *Webwereld* 16 december 2010; BTG, Wet bewaarplicht telecomgegevens schiet zijn doel voorbij, 17 februari 2014 http://btg.org/2014/02/17/wet-bewaarplicht-telecomgegevens-schiet-zijn-doel-voorbij/.
27. Een ander voorbeeld betreft C. Jones & B. Hayes, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, November 2013, <http://secile.eu/data-retention-in-europe-case-study/>. De via een Wob-verzoek openbaargemaakte Nederlandse inbreng voor dit onderzoek (brief van Minister van Justitie aan GG Home Affairs van de Europese Commissie d.d. 2 september 2010, kenm. 5666946/10) leidde overigens ook al tot enige discussie.
28. *Kamerstukken II* 2013/14, 33 870, nr. 1 (met bijlage).
29. Bijlage bij *Kamerstukken II* 2013/14, 33 870, nr. 1, p. 149.
30. *Kamerstukken II* 2013/14, 26 643, nr. 313, p. 2.
31. Zie *Kamerstukken II* 2013/14, 31 145, nr. Y en Kamerbrief van de Minister van Economische Zaken van 16 mei 2013 (kenm. DGETM-TM/14065161); intussen is al wel initiatiefwetsvoorstel ingediend dat beoogt de bewaarplicht grotendeels wil afschaffen (*Kamerstukken II* 2013/14, 33 939, nr. 2).

meevallen om aan te tonen dat voor dit doel niet met minder gegevens kan worden volstaan.
Ook plaatst het Hof vraagtekens bij de omstandigheid dat gegevens moeten worden bewaard zonder dat er ook maar in enige mate een verband is vastgesteld met die criminaliteit. Het Hof suggereert met zoveel woorden dat ten minste wordt onderzocht of de bewaarplicht niet kan worden beperkt tot de gegevens die betrekking hebben op een bepaalde periode, of een bepaalde geografische zone, of een kring van bepaalde personen die op een of andere wijze kunnen zijn betrokken bij ernstige criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van ernstige criminaliteit.
Wellicht nog het meest eenvoudig is het voorzien in verdergaande procedurele waarborgen, zoals het voorzien in meer uitgewerkte objectieve criteria op basis waarvan kan worden bepaald wie wel en wie niet toegang kunnen hebben tot de bewaarde gegevens en tot welke gegevens die toegang moet worden beperkt, een en ander afhankelijk van de omstandigheden van het geval.[32] Ook het voorzien in voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie lijkt betrekkelijk eenvoudig te verwezenlijken.

5. Ter afsluiting

In het licht van het voorgaande is het onvermijdelijk dat de bewaarplicht zoals die is opgenomen in de Telecommunicatiewet op korte termijn moet en zal veranderen.
Wat ons betreft behoort de uitspraak van het Hof echter ook bredere implicaties te hebben, namelijk wat betreft het meer in algemene zin waarborgen van grondrechten in de context van strafvorderlijke toegang tot de grote hoeveelheden elektronische gegevens die in het internettijdperk beschikbaar zijn.
Het Hof spreekt zich immers niet alleen uit over het bewaren van telecomgegevens, maar (vooral) ook over de toegang daartoe door bevoegde autoriteiten. De desbetreffende overwegingen van het Hof zijn evengoed toepasbaar op andere vormen van toegang tot elektronische gegevensverzamelingen[33] en de nieuwe bevoegdheden die worden voorgesteld in het kader van het Wetsvoorstel bestrijding cybercrime (zgn. Computercriminaliteit III).
Wetgeving moet staan voor duurzaamheid en rechtszekerheid, en mag niet verworden tot een wegwerp-artikel,[34] zeker niet als die wetgeving raakt aan fundamentele rechten. Van de wetgever mag worden verwacht dat hij daarvoor zorgdraagt. Wat ons betreft moet de uitspraak dan ook vooral worden opgevat als een serieus te nemen aanwijzing dat de wetgever zich niet te gemakkelijk daarvan af maakt.

32. Wat betreft proportionaliteit kan bijvoorbeeld relevant zijn of een beperkte set gegevens over belgedrag van een bepaalde verdachte wordt opgevraagd, of dat een vordering ziet op gegevens van álle bellers die gedurende een bepaalde periode via telecommasten in een bepaald gebied hebben gebeld.
33. Zie bijv. art. 126nd Sv.
34. Vgl. het Jaarverslag 2013 van de Raad van State, april 2014, p. 43.