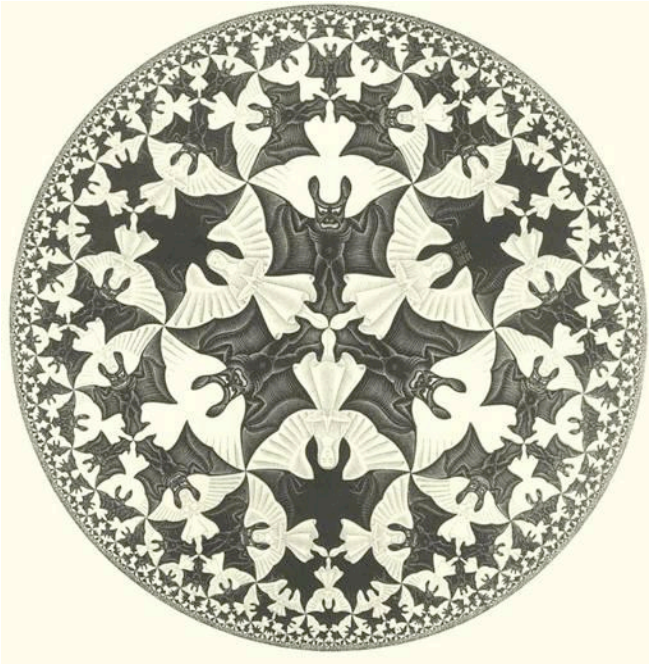
# ALLES ONDER CONTROLE?

*EEN KRITISCHE BLIK OP DE DOOR DE DATARETENTIERICHTLIJN IN HET LEVEN GEROEPEN DRIEHOEKSVERHOUDING TUSSEN DE WET BEWAARPLICHT TELECOMMUNICATIEGEGEVENS, DE STRAFVORDERLIJKE TOEGANGSBEVOEGDHEDEN VAN OPSPORINGSDIENSTEN EN HET RECHT OP PRIVACY VAN DE NEDERLANDSE BURGER*



*- M.C. Escher, Hemel en Hel, ca. 1965*

A.M. ARNBAK, JULI 2009.

# ALLES ONDER CONTROLE?

*EEN KRITISCHE BLIK OP DE DOOR DE DATARETENTIERICHTLIJN IN HET LEVEN GEROEPEN DRIEHOEKSVERHOUDING TUSSEN DE WET BEWAARPLICHT TELECOMMUNICATIEGEGEVENS, DE STRAFVORDERLIJKE TOEGANGSBEVOEGDHEDEN VAN OPSPORINGSDIENSTEN EN HET RECHT OP PRIVACY VAN DE NEDERLANDSE BURGER*

"Privacy is like oxygen. We really appreciate it only when it is gone."[1]

21 JULI 2009
A.M. ARNBAK, 5749131
MASTERSCRIPTIE INFORMATIERECHT
BEGELEIDER: MR. DRS. J.V.J. VAN HOBOKEN
TWEEDE LEZER: PROF. DR. N.A.N.M. VAN EIJK
INSTITUUT VOOR INFORMATIERECHT, UNIVERSITEIT VAN AMSTERDAM
A.ARNBAK@STUDENT.UVA.NL; TELEFOON: +31 - (6) 24 53 44 40
WENSLAUERSTRAAT 8-2HOOG, 1053 BA AMSTERDAM

[1] C.J. Sykes, in: R. Whitaker, *The End of Privacy: How Total Surveillance Is Becoming a Reality,* New Press 1998, nr. 33.

# INHOUDSOPGAVE

# VERKLARING VAN AFKORTINGEN

| | |
|---|---|
| A-G | Advocaat-generaal |
| AIVD | Algemene Inlichtingen- en Veiligheidsdienst |
| AMvB | Algemene Maatregel van Bestuur |
| art. | artikel |
| Art. 29 WG | Artikel 29 Werkgroep, het Europese samenwerkingsverband van nationale toezichthouders op de bescherming van persoonsgegevens |
| BVerfG | Bundesverfassungsgericht, het Duitse Constitutionele Hof |
| CBP | College Bescherming Persoonsgegevens |
| CBS | Centraal Bureau voor de Statistiek |
| CIOT | Centraal Informatiepunt Onderzoek Telecommunicatie |
| CTIVD | Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten |
| EHRM | Europees Hof voor de Rechten van de Mens (Straatsburg) |
| EVRM | Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden |
| Gw | Grondwet |
| HvJEG | Hof van Justitie van de Europese Gemeenschappen (Luxemburg) |
| HR | Hoge Raad der Nederlanden |
| ICT | Informatie- en Communicatietechnologie |
| ILETS | International Law Enforcement Telecommunications Seminar |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| jo. | juncto (in verband met) |
| MIVD | Militaire Inlichtingen- en Veiligheidsdienst |
| MvA | Memorie van Antwoord |
| MvT | Memorie van Toelichting |
| OM | Openbaar Ministerie |
| OvJ | Officier van Justitie |
| Stb. | Staatsblad van het Koninkrijk der Nederlanden |
| StPO | Strafprozessordnung (het Duitse Wetboek van Strafvordering) |
| Sr | Wetboek van Strafrecht |
| Sv | Wetboek van Strafvordering |
| Tw | Telecommunicatiewet |
| VoIP | Voice over IP |
| Wbp | Wet bescherming persoonsgegevens |
| Wiv | Wet op de inlichtingen- en veiligheidsdiensten 2002 |
| WODC | Wetenschappelijk Onderzoek- en Documentatiecentrum (Ministerie van Justitie) |

# INLEIDING

"Deze opslagwaanzin moet zo snel mogelijk verdwijnen."[2] Als veertien hooggeleerde heren op de opiniepagina van dagblad *Trouw* in dergelijke bewoordingen uit de heup schieten, staat er iets belangrijks te gebeuren. Op de vooravond van de plenaire behandeling in de Eerste Kamer van het wetsvoorstel 'Wet bewaarplicht telecommunicatiegegevens', de implementatiewet van de dataretentierichtlijn, vlammen de vonken bij de hoogleraren regelrecht uit de pen. De nood is hoog, want het wetsvoorstel vormt na de aanname van een nieuwe paspoortwet "een volgende bouwsteen van de controlestaat."[3] Ondanks het advies van de hoogleraren om de bewaartermijn in het wetsvoorstel terug te brengen naar de Europese minimumtermijn van zes maanden, gaat de Eerste Kamer uiteindelijk akkoord met een termijn van twaalf maanden voor telefoniegegevens, zes maanden voor internetgegevens. Met deze kortere termijn voor internetgegevens weet Minister Hirsch Ballin de steun van de ChristenUnie, en daarmee een meerderheid in de Eerste Kamer veilig te stellen. De termijn zal overigens niet in dezelfde wet, maar via een aparte reparatiewet geregeld worden; het is dus nog maar de vraag of de Tweede Kamer met deze reparatiewet instemt.

Hoe dit politieke proces zich ook zal voltrekken, het verplicht bewaren van telecommunicatiegegevens van alle burgers om hun beschikbaarheid voor opsporingsonderzoek te garanderen, oftewel dataretentie, is door de jaren heen nooit zonder controverse geweest – en zal de komende jaren nog vaak ter discussie staan. Met de uitspraak van de Grand Chamber van het Hof van Justitie te Luxemburg op 10 februari jl. is dan wel komen vast te staan dat de Europese wetgever in art. 95 EG-verdrag de juiste rechtsgrondslag voor de dataretentieverplichtingen heeft gekozen; desalniettemin blijven belangrijke vragen, bijvoorbeeld over de verenigbaarheid met de fundamentele rechten van burgers via art. 6 EU-verdrag, onbeantwoord.

Deze scriptie sluit aan bij deze actualiteit, door kritisch te reflecteren op de met dataretentie in het leven geroepen driehoeksverhouding tussen de nieuwe beschikbaarheidsverplichtingen voor aanbieders in de Telecommunicatiewet, de toegangsbevoegdheden van opsporingsdiensten in het Wetboek van Strafvordering en de bescherming van de persoonlijke levenssfeer van burgers zoals neergelegd in art. 8 EVRM. Daartoe staat de volgende onderzoeksvraag centraal:

> *In hoeverre heeft de wetgever zich bij de behandeling van de Wet bewaarplicht telecommunicatiegegevens rekenschap gegeven van de verhouding tussen de formele beschikbaarheidsverplichtingen voor aanbieders, de toegangsbevoegdheden van opsporingsdiensten en het recht op privacy van burgers?*

In deze onderzoeksvraag is bewust gekozen voor de begrippen 'beschikbaarheidsverplichtingen' en 'toegangsbevoegdheden'. Met de keuze voor 'beschikbaarheidsverplichtingen' kunnen de ontwikkelingen met betrekking tot telecommunicatiegegevens in een breder kader geplaatst worden, in tegenstelling tot het begrip 'dataretentie'. De term 'toegangsbevoegdheden' prevaleert hier boven

---

[2] Veertien hoogleraren, *We vallen ten prooi aan Europese opslaghysterie*, 'Trouw', 26 juni 2009, te vinden via: <http://www.trouw.nl/opinie/podium/article2798570.ece/We_vallen_ten_prooi_aan_Europese_opslaghysterie_.html> [geraadpleegd juli 2009].

[3] Idem.

'strafvorderlijke bevoegdheden', omdat het conceptueel nauwkeuriger relateert aan telecommunicatiegegevens. Tevens wordt hiermee een scherp onderscheid gemaakt tussen toegang tot de persoonsgegevens versus het gebruik ervan. Voor opsporingsambtenaren blijkt dit onderscheid overigens problematisch te zijn.[4]

Dit onderzoek tracht de centrale onderzoeksvraag stapsgewijs te behandelen, waarbij knelpunten in de driehoeksverhouding worden gesignaleerd en mogelijke alternatieven worden geboden. Voor het noodzakelijke begrip van de oorsprong van de in deze scriptie centraal staande vraagstukken, wordt allereerst de turbulente ontstaansgeschiedenis van de dataretentierichtlijn besproken. Hierop volgt een prospectieve analyse van de implicaties van de 'Wet bewaarplicht telecommunicatiegegevens'. Op basis van deze analyse wordt in hoofdstuk 3 overwogen, of deze implicaties verenigbaar zijn met het recht op privacy zoals neergelegd in art. 8 EVRM – één van de elementaire vragen die door het Hof van Justitie niet werd beantwoord. Recente jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) te Straatsburg lijkt daarbij een belangrijke rol te zullen spelen. In hoofdstuk 4 wordt de aanzet gegeven tot enkele alternatieve wetgevingsmaatregelen, die de uit het onderzoek voortkomende knelpunten kunnen ondervangen. De uiteengesponnen draden worden tot slot samengeknoopt in een samenvattende conclusie, een opsomming van de aanbevelingen aan Kamerleden en een aanzet tot mogelijk vervolgonderzoek.

Deze scriptie tracht een nieuw licht te werpen op de Wet bewaarplicht telecommunicatiegegevens. Achter de specifieke aanbevelingen schuilt de boodschap dat de regulering van telecommunicatiegegevens voortaan een meer samenhangende visie vergt, die recht doet aan de belangen van aanbieders, opsporingsdiensten en – niet in de laatste plaats – burgers. Dat de wetgever zich tot nu toe nauwelijks realiseerde dat formele beschikbaarheidsverplichtingen, toegangsbevoegdheden en het recht op privacy onlosmakelijk met elkaar zijn verbonden, wekt de indruk dat de wetgever de talrijke en brede implicaties van dataretentie nog onvoldoende in ogenschouw heeft genomen.

[4] Zie par. 2.1.

# 1. HET HISTORISCHE PERSPECTIEF

Opsporingsdiensten zijn vandaag de dag afhankelijk van de gegevens die de aanbieders verwerken in het kader van de eigen bedrijfsvoering.[5] De wens om iets aan deze afhankelijkheid te doen wordt in vervulling gebracht met het instellen van een Europese bewaarplicht in richtlijn 2006/24/EG (hierna: dataretentierichtlijn),[6] "teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit."[7] In dit hoofdstuk volgt een reconstructie van de totstandkoming van de dataretentierichtlijn. Uit deze reconstructie volgt inzicht in de aard van dataretentie, de invloed van het Europees constitutionele recht op de vormgeving van de Europese bewaarplicht en een inleiding van de juridische vraagstukken die in deze scriptie centraal staan.

De definities van de persoonsgegevens die in deze scriptie behandeld worden, zijn te vinden in richtlijn 2002/58/EG (hierna: E-privacyrichtlijn).[8] Het betreft steeds de gegevens die nodig zijn om de inhoud van telecommunicatie te transporteren, oftewel een verbinding tot stand te brengen, en niet de inhoud zelf.[9] *Verkeersgegevens* ex art. 2 sub b E-privacyrichtlijn (art. 11.1 sub b Tw) worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.[10] *Locatiegegevens* ex art. 2 sub c E-privacyrichtlijn (art. 11.1 sub d Tw) geven de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbare elektronische communicatiedienst aan.[11] De term *telecommunicatiegegevens* wordt gebruikt als verzamelterm voor de twee eerdergenoemde begrippen.[12]

## *1.1. Uitgangspunt beschikbaarheid van telecommunicatiegegevens*

De strikte hoofdregel van art. 6 richtlijn 97/66/EG,[13] die voorschrijft dat verkeersgegevens direct na beëindiging van de oproep anoniem gemaakt moeten worden tenzij er sprake is van verwerking voor legitieme bedrijfsdoeleinden,[14] geldt als de uitgangspositie als het gaat om de verwerking van persoonsgegevens in de Europese telecommunicatiesector. Ten grondslag aan deze uitgangspositie ligt het beginsel van doelbinding uit overweging 28 en art. 6 lid 1 sub b en sub e richtlijn 95/46/EG (hierna:

---

[5] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.8.
[6] PG EG L 105, 13 apr. 2006, p. 0054-0063.
[7] Art. 1 Dataretentierichtlijn; *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.1.
[8] PG EG L 201, 31 juli 2002, p.0031-0047.
[9] Al kunnen bij de conceptuele scheiding van inhoud en transport de nodige vraagtekens geplaatst worden, zie par. 3.2.1.
[10] Voor een uitgebreide lijst aan voorbeelden van verkeersgegevens: Stratix 2003, p.37-42.
[11] Overweging 14 E-privacyrichtlijn: "Locatiegegevens kunnen verwijzen naar de breedte, de lengte en de hoogte van de eindapparatuur van de gebruiker, de reisrichting, de nauwkeurigheidsgraad van de locatiegegevens, de identificatie van de netwerkcel waarin de eindapparatuur zich op een bepaald tijdstip bevindt, en het tijdstip waarop de locatiegegevens zijn opgeslagen." Het gaat bij locatiegegevens zoals omschreven in de E-privacyrichtlijn niet om de locatiegegevens die ook verkeersgegevens kunnen zijn, maar alleen om de gegevens die specifiek iets zeggen over de locatie van de gebruiker.
[12] De wetgever heeft dit ook gedaan, vgl. de Wet bewaarplicht telecommunicatiegegevens, *Kamerstukken II* 2006-2007, 31145, nr. 2.
[13] PB L 24, 03 jan. 1998, p.1.
[14] Zoals facturering en de verkoop van eigen telecommunicatiediensten, zie verder art. 6 lid 2, 3 en 4 97/66/EG.

Privacyrichtlijn),[15] dat op zijn beurt weer voortspruit uit de beginselen van behoorlijke gegevensverwerking uit het Databeschermingsverdrag van de Raad van Europa van 1981.[16] Uitzondering op deze hoofdregel zijn de vraagstukken van nationale veiligheid en opsporing, die niet beheerst worden door gemeenschapsrecht. Dergelijke gevoelige onderwerpen blijven binnen het domein van nationale lidstaten op grond van art. 3 lid 2 95/46/EG jo. art. 14 lid 1 richtlijn 97/66/EG.

## 1.2. Eerste voortekenen dataretentie telecommunicatiegegevens

Alhoewel dataretentie in 2006 is verwezenlijkt in de Europese Gemeenschap, bestaat de wens daartoe bij de opsporingsdiensten in ieder geval sinds medio jaren '90. Dit blijkt uit verslagen van meerdere ontmoetingen van Ministers van Justitie en opsporingsdiensten van verschillende landen in uiteenlopende samenwerkingsverbanden. In 1997 kwam dataretentie al ter sprake tijdens een meeting van Ministers van Justitie en Binnenlandse Zaken op de G8 top in Washington.[17] Het ging hier om het bewaren van verkeersgegevens door Internet Service Providers als reactie op de explosieve groei van internetgebruik. De art. 29 WG, het samenwerkingsverband van Europese toezichthouders op de gegevensbescherming, reageert in aanbeveling 3/99 op deze plannen met de stellingname dataretentie te verbieden omdat een verbod de "doeltreffendste manier is om onaanvaardbare risico's voor de bescherming van de persoonlijke levenssfeer te voorkomen."[18] De behoeftestellers lijken enkele maanden later niet onder de indruk van deze aanbeveling: "all delegations are to consider options for improving the retention of data by Communication Service Providers",[19] luidt de oproep tijdens het International Law Enforcement Telecommunications Seminar (ILETS), een internationaal samenwerkingsverband van behoeftestellers geïnitieerd door de Amerikaanse FBI in 1993. Dataretentie is hier al uitgebreid van verkeersgegevens die door ISPs worden verwerkt, naar telecommunicatiegegevens die door alle aanbieders van communicatiediensten in het kader van de dienstverlening worden opgeslagen.

Wat opvalt aan deze eerste voortekenen van dataretentie is dat behoeftestellers blijkbaar een groot belang hebben bij de sturing van de werking van telecommunicatietechnologie, zodat handelingen via ICT niet buiten hun bereik zullen plaatsvinden. Dit is al in 1999 overtuigend, en eigenlijk steeds overtuigender, betoogd door Lessig.[20] De behoeftestellers pakken dit vanaf het

[15] PB EG L 281, 23 nov. 1995, p.0031-0050.
[16] Trb. 1988, 7.
[17] Meeting of Justice and Interior Ministers of the G8, December 9-10 1997, Communique, Washington D.C. December 10, Communique Annex: Principles and Action Plan to combat High-Tech Crime.
[18] WP 29, *Aanbeveling 3/99 over de bewaring van verkeersgegevens door Internetaanbieders voor wetshandhavingsdoeleinden*, 9 september 1999, 5089/99/NL/Def., p.7.
[19] Draft Report ILETS conference '99, *Reconciling data protection and privacy requirements in the 21st Century*, 16-18 Nov. 1999, Saint Cyr au Mont d'Or, p.7. Het rapport is te vinden via: <www.statewatch.org/news/2001/may/ILETS99-report.doc> [geraadpleegd juli 2009]. Het ILETS heeft als eerste doelstelling om de zogenaamde International User Requirements (IUR), ontwikkeld door de Amerikaanse federale opsporingsdienst FBI in 1992, in de Westerse wereld te promoten. Op 15 januari 1995 werden zij overgenomen door de EU in de Council Resolution of 17 January 1995 on the lawful interception of telecommunications, Official Journal of the European Communities, 96/C 329/01.
[20] L. Lessig, *Code and other laws of cyberspace*, New York: Basic Books 1999. Zie tevens Zwenne & Schmidt 2005, p.302.

allereerste begin van de grootschalige uitrol van zowel internet als mobiele telecommunicatie gecoördineerd aan, in internationaal verband.[21]

## 1.3. De E-privacyrichtlijn

Deze prille voortekenen van dataretentie komen in het jaar 2000 voor het eerst aan de oppervlakte bij de onderhandelingen over een nieuwe richtlijn, ter aanpassing van richtlijn 97/66/EG aan de nieuwe stand van de techniek en de markten.[22] Deze nieuwe richtlijn, die later bekend zal worden als de E-privacyrichtlijn 2002/58/EG, moet deel gaan uitmaken van een pakket richtlijnen – het zogenaamde 'Europees regelgevend kader' – dat techniekneutraliteit van de telecommunicatieregulering nastreeft.

De legitieme bedrijfsdoeleinden voor de verwerking van persoonsgegevens in de telecommunicatiesector worden enigszins uitgebreid,[23] maar de aanpassing van art. 14 richtlijn 97/66/EG in een nieuw art. 15 vormt het hete hangijzer bij de onderhandelingen. De eerste fase daarvan wordt gekenmerkt door grote onenigheid, zowel tussen de verschillende stakeholders als binnen de eigen gelederen. Zo bereiken de gezamenlijke Ministers van Justitie binnen de Raad van de Europese Unie (hierna: "de Raad") geen overeenstemming over het instellen van een expliciete Europese grondslag voor dataretentie in de nieuwe richtlijn.[24] België, de toen aanstaande voorzitter van de Raad, komt met een tussenweg: "traffic data can be processed for legitimate purposes as detemined by national law or applicable instruments."[25] Dataretentie kan impliciet hieruit voorvloeien, maar niet expliciet uit deze tussenweg in het eerste voorstel van de Raad worden afgelezen. Voorzitter Stefano Rodota van de art. 29 WG reageert op dit eerste voorstel met een brief aan de zittend voorzitter van de Raad (Zweden), alsmede de president van het Europees Parlement en Commissievoorzitter Prodi, waarin hij oproept om de verleiding van dataretentie te weerstaan ten gunste van de eerbiediging van de persoonlijke levenssfeer, het communicatiegeheim en een begrenzing van de verwerking van persoonsgegevens in de telecommunicatiesector.[26] Het Europees Parlement (hierna: "het Parlement") volgt de zienswijze van de art. 29 WG en voegt zelfs strenge passages, waarin dataretentie als wetgevingsmaatregel expliciet wordt verboden, toe aan het eerste voorstel van de Raad voor een nieuw artikel 15 in de nieuwe richtlijn.[27]

---

[21] Een overzicht van dergelijke initiatieven in Europa is te vinden op: <http://www.statewatch.org/soseurope.htm> [geraadpleegd juli 2009].Vooral de Enfopol (Enforcement Police) resoluties blijken controversieel, zie: <http://www.statewatch.org/eufbi/index.html> [geraadpleegd juli 2009].

[22] COM (2000) 385 def., p.2.

[23] 'Verkoop van telecommunicatiediensten' uit art. 6 lid 3 richtlijn 97/66/EG zal uiteindelijk veranderd worden in: "voor marketing van elektronische communicatiediensten of voor de levering van diensten met toegevoegde waarde" in art. 6 lid 2 E-privacyrichtlijn.

[24] Statewatch, *Data protection or data retention in the EU?*, Report on surveillance of telecommunications, juli 2001. Zie: <http://www.statewatch.org/news/2001/sep/01data.htm> [geraadpleegd juli 2009].

[25] Working Party on Telecommunications, *Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector*, 9337/01, 31 mei 2001.

[26] S. Rodota, *Letter to Mr. Persson*, Art. 29 Working Party, Brussels, 7 jun. 2001. De brief is te vinden op: <http://www.wired.com/politics/security/news/2001/06/44890> [geraadpleegd juli 2009].

[27] "Under the European Convention on Human Rights and pursuant to rulings issued by the Court of Human Rights, any form of wide-scale general or exploratory electronic surveillance is prohibited." A5-0374/2001, 24 oktober 2001, p.29. Deze reactie wordt gepubliceerd na 11 september, maar volgt op het voorstel van de Raad dat voor 11 september is gedaan.

Na de terroristische aanslagen van 11 september 2001 op militaire doelen en burgerdoelen in de Verenigde Staten is de onenigheid binnen de Raad verdwenen. Een maand na de aanslagen oefent President George W. Bush in een brief aan Commissievoorzitter Romani Prodi druk uit om de nieuwe richtlijn zo aan te passen dat dataretentie toegestaan is.[28] Kort daarop gaan zowel Raad als de Europese Commissie (hierna: "de Commissie") akkoord met een nieuwe tekst voor art. 15, die lidstaten expliciet een grondslag biedt om dataretentiemaatregelen te treffen in nationale wetgeving.[29] Na een verwerping van deze nieuwe tekst door het Parlement in tweede lezing,[30] openbaart zich tijdens het parlementaire debat in mei 2002 een compromis tussen de Raad en het Parlement: een expliciete grondslag voor dataretentie in art. 15, in ruil voor een garantie van de bescherming van de persoonlijke levenssfeer in overweging 11.[31] Een verklaring voor deze ommezwaai van het Parlement is mogelijkerwijs politieke druk vanuit de Commissie, die haast heeft omdat de nieuwe richtlijn onderdeel moet uitmaken van het Europees regelgevend kader – de overige vier richtlijnen zijn dan al lange tijd aangenomen.[32] De Commissie toont zich in een persconferentie op de dag van de stemming over het compromis dan ook tevreden, omdat het pakket telecomrichtlijnen hiermee is beklonken.[33] Na instemming van zowel Raad als Commissie wordt de nieuwe richtlijn 2002/58/EG, i.e. de E-privacyrichtlijn, op 12 juli ondertekend door Parlement en Raad.

Welke factoren hebben bijgedragen aan de expliciete grondslag voor dataretentie in art. 15 lid 1, en wat zijn de uitwerkingen ervan? Op de eerste plaats is de invloed van '9/11' op de totstandkoming van art. 15 lid 1 duidelijk aanwezig. Maar de aanslagen hebben frappant genoeg ook gevolgen voor de reikwijdte van dataretentie: de expliciete opname van dataretentie in art. 15 lid 1 verbindt de maatregel niet alleen met terrorismebestrijding, maar ook met de vervolging van strafbare feiten. Terrorisme verwordt zo tot een katalysator van de al langer bestaande wens van behoeftestellers de opsporingsmogelijkheden via een bewaarplicht telecommunicatiegegevens uit te breiden (zie par. 1.2.). Naast de factor terrorisme, hebben de haastige interne marktbelangen van de Commissie een belangrijke uitwerking op de uiteindelijke tekst van art. 15 lid 1. Druk vanuit de Commissie heeft waarschijnlijk bijgedragen aan de goedkeuring van het compromis door het Parlement, nadat het in eerste instantie fel tegen dataretentie gekant was. Opmerkelijk is daarbij dat dataretentie tijdens het gehele proces nooit aan een grondige analyse van de noodzakelijk en effectiviteit ervan onderworpen is geweest. De Commissie stelt het interne marktbelang duidelijk voorop en lijkt van de toevoeging aan art. 15 lid 1 niet al teveel te verwachten.[34]

De weerslag van het compromis is echter aanzienlijk,[35] omdat de Europese wetgever in de E-privacyrichtlijn een tegenstrijdig signaal afgeeft als het gaat om de regulering van beschikbaarheid van telecommunicatiegegevens in de Europese richtlijnen. Immers, art. 6 jo. art. 9 E-privacyrichtlijn en in

---

[28] "Revise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period." United States Mission to the European Union, *Proposals for US-EU counter-terrorism cooperation*, 16 oct. 2001. Zie: <http://www.statewatch.org/news/2001/nov/06Ausalet.htm> [geraadpleegd juli 2009].

[29] "To this end Member States may inter alia provide for the retention of data for a limited period justified on the grounds laid down in this paragraph, in accordance with the general principles of Community law."
SEC/2002/0124 def., 30 jan. 2002, onder artikel 15.

[30] A5-0130/2002, 22 apr. 2002, p.19.

[31] IP/02/783, 30 mei 2002.

[32] IP/02/783, 30 mei 2002.

[33] IP/02/783, 30 mei 2002.

[34] COM/2002/0338 def, 17 jun. 2002, punt 4 onder "Amendement 47 - Overweging 11; Amendement 46 - Artikel 15, lid 1."

[35] De dataretentierichtlijn zal uiteindelijk op art. 15 lid 1 E-privacyrichtlijn gebaseerd worden, zie par. 1.4.

meer algemene zin het beginsel van doelbinding uit overweging 28 en art. 6 lid 1 sub b/e Privacyrichtlijn gebieden het verwijderen dan wel anonimiseren van telecommunicatiegegevens, maar tegelijkertijd geeft art. 15 lid 1 E-privacyrichtlijn jo. art. 3 lid 2 Privacyrichtlijn aan lidstaten de expliciete mogelijkheid deze hoofdregel buiten beschouwing te laten, door dataretentiemaatregelen te treffen in nationale wetgeving. En al ziet de Commissie de expliciete grondslag slechts als een voorbeeld van een mogelijke maatregel die lidstaten zouden kunnen treffen,[36] het compromis zet de deur wagenwijd open voor lidstaten om dataretentieverplichtingen te treffen. Want kort na de ondertekening van de E-privacyrichtlijn ontstaan dergelijke dataretentiemaatregelen daadwerkelijk in enkele lidstaten, die blijkbaar op de inwerkingtreding zaten te wachten.[37] Zo wordt de ambivalentie van de Europese regulering van de beschikbaarheid van telecommunicatiegegevens dadelijk geëffectueerd.

Bovendien wordt de eerste mogelijkheid voor lidstaten om dataretentie voor opsporingsonderzoek in nationale wetgeving op te nemen geboden in een Europese richtlijn, in theorie een harmonisatiemaatregel van de Europese interne markt en niet bedoeld om opsporingsgerelateerde aangelegenheden te regelen.[38] Een juridische splijtzwam, zo betoogt deze scriptie, die in de daarop volgende jaren aanleiding zou vormen voor een turbulent totstandkomingsproces van de dataretentierichtlijn (par. 1.4.), een procedure bij het Hof van Justitie over de rechtsgrondslag in art. 15 lid 1 E-privacyrichtlijn van de dataretentierichtlijn (par. 1.5.) alsmede een discutabele Nederlandse implementatie van de dataretentierichtlijn (hfd. 2).

## 1.4. De dataretentierichtlijn

Art. 15 lid 1 E-privacyrichtlijn zal uiteindelijk de grondslag vormen voor een Europese algemene bewaarplicht telecommunicatiegegevens, die er in 2006 komt met de dataretentierichtlijn. De totstandkoming van deze richtlijn is niet zonder slag of stoot gegaan. Enkele relevante momenten worden hier uitgelicht,[39] waarbij opvalt dat er een aantal veelzeggende parallellen te trekken zijn met de totstandkoming van de E-privacyrichtlijn.

Twee weken na de terroristische aanslagen van 11 maart 2004 op forensentreinen in Madrid, anderhalf jaar na de ondertekening van de E-privacyrichtlijn, instrueren de dan verzamelde regeringsleiders de Raad van Ministers van justitie om uiterlijk in juni 2005 een Europese algemene bewaarplicht geregeld te hebben.[40] Vier lidstaten, waaronder het Verenigd Koninkrijk en Ierland, doen een maand later gezamenlijk een voorstel voor een ontwerp-Kaderbesluit om de verschillende wetgevingen met betrekking tot de bewaarplicht af te stemmen "met het oog op het voorkomen,

[36] COM/2002/0338 def, 17 jun. 2002, punt 4 onder "Amendement 47 - Overweging 11; Amendement 46 - Artikel 15, lid 1."
[37] Meer informatie over de dataretentie verplichtingen in verschillende Europese landen is te vinden in het dossier van European Digital Rights: <http://www.edri.org/issues/privacy/dataretention> [geraadpleegd juli 2009].
[38] In de Eerste pijler, de Europese Gemeenschap die in het leven is geroepen om economische samenwerking te stimuleren, en niet in de Derde pijler, waarin de samenwerking tussen lidstaten op het gebied van opsporingsgerelateerde aangelegenheden is geregeld. Het recht van de pijlers van de Europese Unie komt uitgebreid aan de orde in par. 1.4. e.v.
[39] Voor een uitgebreide bespreking van de totstandkoming van de richtlijn, wordt verwezen naar Mol Lous 2006 en Van Veen & Van Ginneken 2009.
[40] Raad van de Europese Unie, 25 mrt. 2004, *Declaration on combating terrorism*, p.4/5, zie: <http://consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf> [geraadpleegd juli 2009].

opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme."[41] Evenals bij de E-privacyrichtlijn vormt een terroristische aanslag de voedingsbodem voor een maatregel die niet alleen ziet op terrorismebestrijding, maar ook op de opsporing van allerlei andere strafbare feiten.

Het Europees constitutionele recht vormt een essentieel aspect van de totstandkoming van de Europese bewaarplicht. Als rechtsgrondslag van het ontwerp-Kaderbesluit wordt gekozen voor art. 31 lid 1 sub c en art. 24 lid 2 sub b titel VI van het EU-verdrag, een wetgevingsmaatregel in de zogenaamde *Derde pijler* van de Europese Unie. In deze Derde pijler wordt de samenwerking van politie en justitie in strafzaken geregeld, oftewel maatregelen van strafprocesrecht. Deze pijler is intergouvernementeel van aard; maatregelen van strafprocesrecht liggen politiek nu eenmaal gevoeliger dan economische georiënteerde wetgeving. De Raad heeft in de Derde pijler het recht van initiatief, en besluit bij unanimiteit. Het Europees Parlement hoeft slechts gehoord te worden, maar zal niet stemmen over een voorgenomen maatregel, terwijl het Hof van Justitie Kaderbesluiten marginaal toetst.[42] De macht van de puur Europese instituties is daarom beperkt in de Derde pijler.[43] Dit in tegenstelling tot de *Eerste pijler* van de Europese Unie, te weten de Europese Gemeenschappen (EG), waarin het harmoniseren van de Europese interne markt wordt geregeld en daarmee de economische samenwerking tussen lidstaten wordt gestimuleerd. De bevoegdheden van de Europese instituties manifesteren zich ten volle in deze Eerste pijler.[44] Zo ligt het initiatiefrecht niet bij de Raad maar bij de Commissie, waarna de zogenaamde 'codecisie procedure' van art. 251 EG-verdrag in werking treedt: dit houdt in dat wetgeving tot stand komt na een compromis tussen de Raad en het Parlement – zoals wij al zagen bij de E-privacyrichtlijn. De Raad neemt in deze pijler besluiten bij gekwalificeerde meerderheid, in tegenstelling tot het vereiste van unanimiteit in de Derde pijler. Het Hof van Justitie heeft volledige toetsingsbevoegdheid.[45]

Welnu, de kernpunten van het ontwerp-Kaderbesluit zijn een bandbreedte van bewaartermijnen tussen 12 en 36 maanden, waartussen lidstaten de in hun ogen redelijke termijn kunnen kiezen, alsmede een regeling inzake de toegang tot de verplicht bewaarde gegevens.[46] Het Europees Parlement neemt in juni 2005 unaniem een nota aan, waarin het concludeert dat het voorstel van de Raad disproportioneel is met het oog op de eerbiediging van de persoonlijke levenssfeer.[47] Daarnaast worden de effectiviteit en de noodzaak van de maatregel ter discussie gesteld, en het feit dat er niets is afgesproken over de kosten.[48] Naast deze inhoudelijke bezwaren heeft het Parlement ook een strategisch belang een maatregel in de Derde pijler af te keuren. Doorgang in de Derde pijler betekent immers uitsluiting van het debat over dataretentie zowel bij totstandkoming als evaluatie van een Europese bewaarplicht, en ontneemt het Parlement de zeggenschap over dataretentie in de toekomst. Zoals uiteengezet geldt dit strategische belang in gelijke zin voor de Commissie, terwijl de vooruitblik

[41] 8958/04, CRIMORG 36/TELECOM 82, 28 apr. 2004, p.1.
[42] Zie o.m. Van Veen & Van Ginneken 2009, p.6 onder verwijzing naar Kapteyn & Verloren van Themaat 2003.
[43] Van Veen & Van Ginneken 2009, p.6.
[44] Idem.
[45] Idem.
[46] De voorgestane regulering van de toegang omvatte het slechts toegang hoeven te verlenen tot de verplicht bewaarde gegevens aan andere lidstaten, indien de nationale autoriteiten van een lidstaat op grond van de eigen regels omtrent toegang de gegevens eveneens zouden mogen inzien. Vgl. Mol Lous 2006, p.353. Deze regeling was nodig in verband met het Verdrag van Straatsburg (*Trb.* 2000, 96) en de EU-Rechtshulpovereenkomst 2000.
[47] Smits 2006, p.151; EDRI, *EP rejects data retention proposal*, 15 jun. 2005, te vinden op: <http://www.edri.org/edrigram/number3.12/dataretention> [geraadpleegd juli 2009].
[48] Destijds niet alleen in de Nota Alvaro, maar ook door o.m. art. 29 WP Opinion 9/2004, 15 nov. 2004; art. 29 WP Opinion 4/2005, 21 okt. 2005; Breyer 2005.

van een verstoring van de Europese interne markt vanwege de uiteenlopende bewaartermijnen door het ontwerp-Kaderbesluit de Commissie op inhoudelijk vlak zorgen baart.

De Commissie initieert daarom enkele maanden later onderhandelingen voor een ontwerprichtlijn als alternatief voor het ontwerp-Kaderbesluit.[49] Kernpunten van dit Commissievoorstel zijn een bewaartermijn van 12 maanden voor telefoniegegevens en 6 maanden voor internetgegevens en een bijlage bij de richtlijn, waarin de categorieën gegevens die aanbieders verplicht moeten bewaren zijn opgenomen. Als ratio voert de Commissie aan dat een op te leggen Europese verplichting aan de aanbieders een maatregel is ter harmonisering van de Europese interne markt, oftewel om de toentertijd in sommige lidstaten geldende bewaartermijnen en andere verplichtingen voor aanbieders te harmoniseren. Het ontwerp-Kaderbesluit zou in strijd zijn met het 'communautaire recht' ex art. 47 EU-verdrag, mede gezien de raakvlakken van de daarin vervatte dataretentiemaatregelen met art. 15 lid 1 E-privacyrichtlijn. De maatregel moet daarom op art. 15 lid 1 E-privacyrichtlijn gebaseerd worden, zodat zij zich als lex specialis verhoudt ten opzichte van de E-privacyrichtlijn en de Privacyrichtlijn. In de zienswijze van de Commissie worden de drie richtlijn samen integraal van toepassing op de ingevolge de ontwerprichtlijn verplicht bewaarde categorieën telecommunicatiegegevens.

Dat de Europese dataretentieverplichtingen in een richtlijn gestalte hebben gekregen, is bekend. Dat geldt in mindere mate voor de wijze waarop de ontwerprichtlijn de codecisieprocedure doormaakte. De Raad blijkt het gehele onderhandelingsproces te hebben beheerst. Het Parlement en de Commissie hebben moeten toezien hoe hun standpunten de richtlijn nauwelijks gehaald hebben.[50] De richtlijn is daarenboven in een krappe drie maanden door de codecisieprocedure heen gedenderd.[51] Hoe is dit in zijn werk gegaan?

Op 12 oktober 2005 wordt binnen de Raad duidelijk dat dertien van de vijfentwintig lidstaten de idee van een richtlijn steunen, die dan voor het einde van hetzelfde kalenderjaar gerealiseerd moet zijn.[52] Deze kleine meerderheid komt tot stand na aandringen van voorzitter het Verenigd Koninkrijk, waar drie maanden eerder op 7 juli 2005 de terroristische aanslagen in de metro van Londen hebben plaatsgevonden. Net als bij de totstandkoming van art. 15 lid 1 van de E-privacyrichtlijn is er sprake van een terroristische aanslag en van tijdsdruk, omdat het erop Verenigd Koninkrijk gebrand is de richtlijn binnen de eigen voorzitterstermijn van de Raad af te handelen.[53] De hoofdreden voor deze haast ligt waarschijnlijk buiten het juridische domein.[54] Buiten de tijdsruk hebben de zowel de juridische diensten van de Raad als het Parlement geadviseerd de zienswijze van de Commissie te volgen, omdat een Kaderbesluit dat bewaartermijnen harmoniseert strijd met het Europees constitutionele recht zou kunnen opleveren.[55]

---

[49] COM/2005/438 def., 21 sept. 2005.
[50] A6-0365/2005, 28 nov. 2005.
[51] Een overzicht van de voorgeschiedenis van de dataretentierichtlijn is te vinden op: <http://www.europarl.europa.eu/oeil/FindByProcnum.do?lang=2&procnum=COD/2005/0182> [geraadpleegd juli 2009].
[52] Van Veen & Van Ginneken 2009, p.4, noot 13 onder verwijzing naar het verslag van de JBZ-raad, 12 okt. 2005.
[53] Idem.
[54] Zo zou het goed mogelijk kunnen zijn dat de volgende voorzitter van de Europese Raad een van de tegenstanders van de Europese bewaarplicht an sich, dan wel in de vorm van een richtlijn was. Gezien de met een Kaderbesluit vereiste unanimiteit, is een mogelijk veto van (de nationale parlementen van) andere lidstaten omzeild met de Britse manoeuvre naar een richtlijn.
[55] Conseil de l'Union Européenne, 7688/05, Bruxelles, le 5 avril 2005, p.8-10; Committee on Civil Liberties, Justice and Home Affairs, Brussels march 2005, 8958/2004 – C6-0198/2004 – 2004/0813(CNS). Zie tevens: <http://www.statewatch.org/news/2005/apr/02eu-data-retention.htm> [geraadpleegd juli 2009]. Dit punt wordt in par. 1.5. uitgediept.

Door deze gekwalificeerde meerderheid heeft de Raad een sterke onderhandelingspositie, omdat de maatregel zowel in de vorm van een richtlijn als een Kaderbesluit getroffen kan worden. Zich bewust van het feit dat er een Kaderbesluit dreigt en onder grote tijdsdruk neemt het Parlement op 28 november de eerste lezing van de Raad van het richtlijnvoorstel aan. Vertalingen ontbreken, de technische consequenties en de gevolgen voor de interne markt zijn niet goed bestudeerd; het Parlement verzucht dat dit hopelijk niet de regel wordt.[56] Drie dagen na de verschijning van deze eerste lezing van het Parlement laat de Raad in het openbaar zijn keuze definitief vallen op een richtlijn. Alleen Ierland en Slowakije stemmen tegen, alle andere lidstaten kunnen zich vinden in het voorstel.[57] Het Europees Parlement brengt vervolgens op 14 december zijn goedkeurend advies uit over het richtlijnvoorstel,[58] terwijl van de oorspronkelijke wensen van het Parlement nauwelijks iets terug is te vinden in de uiteindelijke richtlijn.[59] Nadat de Raad heeft ingestemd met het richtlijnvoorstel – Ierland en Slowakije stemmen wederom als enige lidstaten tegen – volgt de ondertekening van de dataretentierichtlijn op 21 februari 2006.

De uiteindelijke tekst van de richtlijn behelst evenals art. 15 van de E-privacyrichtlijn een ingrijpende verandering van de daarvoor geldende situatie met betrekking tot de beschikbaarheid van en toegang tot telecommunicatiegegevens, alsmede het recht op privacy van burgers. Voortaan worden de in art. 5 genoemde categorieën gegevens van alle Europese burgers verplicht bewaard om de beschikbaarheid voor opsporingsonderzoek te garanderen. De bewaartermijn wordt in art. 6 van de dataretentierichtlijn vastgesteld op 6 tot 24 maanden, waarbij het onderscheid tussen internet- en telefoniegegevens is verdwenen.[60] De toegang tot de gegevens is niet beperkt tot de 24 ernstige misdrijven ex art. 2 lid 2 Europees Aanhoudingsbevel, zoals het Parlement wenste, maar op grond van art. 1 lid 1 van de dataretentierichtlijn is de definiëring van ernstige criminaliteit in nationale wetgeving van lidstaten leidinggevend. Ex art. 4 worden de regels voor de toegang tot de gegevens overgelaten aan nationale lidstaten, die het recht op privacy van burgers daarbij dienen te respecteren.[61]

Terugkijkend op deze drie turbulente maanden, springen een aantal ontwikkelingen in het oog. Meest opvallend is dat maatregel onder druk van de Raad razendsnel is aangenomen in de Eerste pijler. Van Veen en Van Ginneken stellen dat de theoretische mogelijkheid dat de Raad zou uitwijken naar de Derde pijler het gehele totstandkomingsproces heeft beheerst, en spreken van een strijd tussen de verschillende Europese instituties over relatieve competentie, oftewel macht.[62] Zoals beschreven wilden het Parlement en de Commissie uitsluiting van het dataretentiedebat niet riskeren. Naast deze strijd is er sprake van een veranderend politiek klimaat ten gunste van het uitbreiden van de opsporingsbevoegdheden van behoeftestellers. Vergelijkbaar met de totstandkoming van art. 15 lid 1 E-privacyrichtlijn vormde de aanslagen in Londen een katalysator voor deze bevoegdheidsuitbreiding met het oog op het bestrijden van criminaliteit in brede zin, niet alleen met het oog op terrorismebestrijding.

---

[56] A6-0365/2005, p.35.
[57] PRES/05/296.
[58] A6-0365/2005, 14 dec. 2005.
[59] Van Veen & Van Ginneken 2009, p.2. Rapporteur Alvaro kan niet leven met het compromis en laat zijn naam schrappen van het eindresultaat. Zie Mol Lous 2006, p.355.
[60] Op basis van art. 12 lid 1 kan door lidstaten van deze bandbreedte naar boven worden afgeweken, indien specifieke omstandigheden een in de tijd beperkte verlenging van de termijnen rechtvaardigen. Kennisgeving aan overige lidstaten en de Commissie – die binnen zes maanden oordeelt of de maatregel geoorloofd is ex art. 12 lid 2 – is een vereiste.
[61] Zie par. 1.5.
[62] Van Veen & Van Ginneken, p.2.

De tijdsdruk, het strategische handelen van de Europese instituties en het veranderende politieke klimaat zijn niet zonder consequenties geweest. Ondanks het feit dat zowel de E-privacyrichtlijn als de dataretentierichtlijn specifieke bepalingen voor gegevensbescherming bevatten, was het waarborgen van de fundamentele rechten van burgers, zoals het recht op privacy, nooit maatgevend.[63] De door het Parlement in de nota Alvaro[64] opgeworpen vraagtekens bij de noodzakelijkheid en de effectiviteit van dataretentie zijn, evenals tijdens de totstandkoming van art. 15 E-privacyrichtlijn, niet grondig onderzocht. Daarbij bleven technische vraagstukken onbeantwoord en een impact assessment onuitgevoerd.[65] Het is tekenend dat de gemeenschapswetgever dergelijke gewichtige vraagstukken in de behandeling van de richtlijn nauwelijks aan de orde heeft laten komen.

Met de dataretentierichtlijn is de beschikbaarheid van telecommunicatiegegevens gegarandeerd en de privacy van burgers onderbelicht. Hoe staat het met de regulering van de toegang in de dataretentierichtlijn? De door het parlement voorgestane beperking van de toegangsbevoegdheden van opsporingsdiensten tot de gegevens heeft de richtlijn niet gehaald. De uitspraak van het Hof van Justitie over de rechtsgrondslag van de dataretentierichtlijn biedt een antwoord op deze vraag en maakt de voorgeschiedenis van de dataretentierichtlijn compleet.

## *1.5. Zaak C-301/06 bij het Hof van Justitie*

Met de ondertekening van de dataretentierichtlijn is de voorgeschiedenis van een Europese bewaarplicht nog niet voltooid. Terwijl in de lidstaten implementatiewetten worden voorbereid en behandeld, starten dezelfde twee lidstaten die steeds tegen de ontwerprichtlijn van de Commissie stemden – Ierland, gesteund door Slowakije[66] – op 6 juli 2006 een procedure bij het Hof van Justitie in Luxemburg, gericht op het ongeldig verklaren van de richtlijn omdat deze niet op een passende rechtsgrondslag vastgesteld zou zijn.[67] Het belangrijkste argument van Ierland is dat de richtlijn niet op art. 95 EG-verdrag (harmoniseren van de interne markt) kan worden gebaseerd, nu het zogenaamde "zwaartepunt"[68] van de maatregel het onderzoeken, opsporen en vervolgen van strafbare feiten betreft.[69] In de ogen van de eisers had de bewaarplicht in de Derde pijler van de Europese Unie vastgesteld moeten worden.

Op 10 februari 2009, drie jaar na ondertekening door de Raad, stelt het Hof Ierland in het ongelijk oordeelt het Hof dat de dataretentierichtlijn op de juiste grondslag, te weten art. 95 EG-verdrag is vastgesteld. Het Hof kan zich in grote lijnen vinden in de destijds door de Commissie aangevoerde ratio voor de ontwerprichtlijn. Vanwege de wijziging van de E-privacyrichtlijn die op art. 95 EG-

[63] Hijmans 2008, p.1792. In dit verband noemt Hijmans ook Kaderbesluit 2008/615/JBZ inzake de intensivering van de grensoverschrijdende samenwerking tussen lidstaten op het gebied van DNA-, vingerafdruk- en kentekengegevens (beter bekend als 'Prüm') en het voorstel voor een kaderbesluit van de Raad over het gebruik van gegevens van vliegtuigpassagiers in Europa, dat leidde tot het beruchte PNR-arrest van het Hof van Justitie (HvJEG 30 mei 2006, Parlement vs. Raad en Commissie, C-317/04 en C-318/04).
[64] Smits 2006, p.151; EDRI, *EP rejects data retention proposal*, 15 jun. 2005, te vinden op: <http://www.edri.org/edrigram/number3.12/dataretention> [geraadpleegd juli 2009].
[65] A6-0365/2005, p.35. Hijmans 2008, p.1973.
[66] PRES/05/296.
[67] HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council.
[68] Kapteyn & Verloren van Themaat 2003, p.264.
[69] HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 26.

verdrag is gebaseerd, kon de dataretentierichtlijn niet zonder schending van art. 47 EU-verdrag zijn grondslag in een andere bepaling vinden, bijvoorbeeld uit Titel VI (Derde pijler) van datzelfde EU-verdrag.[70] Daarbij verduidelijkt het Hof dat de richtlijn in geen enkele mate de toegang tot of het gebruiken van gegevens door bevoegde nationale wetgevingsautoriteiten reguleert,[71] maar in wezen de activiteiten van aanbieders van diensten treft, en dat de dataretentierichtlijn dientengevolge overwegend betrekking heeft op de werking van de interne markt.[72]

Op de argumentatie van het Hof is de nodige kritiek te leveren.[73] Zo is het maar de vraag of het afgezwakte voorstel van de Commissie zal bijdragen aan het harmoniseren van de interne markt.[74] Helaas stoelt het Hof deze zienswijze niet op een degelijke analyse van de bestaande en toekomstige verschillen in de lidstaten. Van Veen en Van Ginneken betogen daarentegen overtuigend dat de dataretentierichtlijn juist extra belemmeringen voor de interne markt in het leven roept, aangezien vele lidstaten nog geen operationele bewaarplicht hadden op het moment dat de dataretentierichtlijn deze verplichting oplegde.[75] Voorts is de beslissing om de overwegingen uit het PNR-arrest[76] niet te laten gelden in onderhavig geval eveneens te kort door de bocht gemotiveerd. Dat de dataretentierichtlijn "geen enkele regeling van de activiteiten van de overheid voor de wetshandhaving" bevat, druist immers in tegen de gehele essentie van de maatregel, zoals onder meer verwoord in overweging 8, 11 en art. 1 lid 1 dataretentierichtlijn. In een noot bij het arrest zet Teunissen uiteen dat dit standpunt moeilijk verdedigbaar is, nu opsporingsbevoegdheden een veel ruimer toepassingsbereik krijgen met de dataretentierichtlijn.[77] Op dit punt komt de scriptie uitgebreid terug (m.n. par. 2.4. en hfd. 3).

Ondanks deze kritiek verschaft de rechtsvinding door het Hof met deze uitspraak duidelijkheid over het toegangsvraagstuk in de dataretentierichtlijn. De dataretentierichtlijn deelt de bewaarplicht op in een formele Europese beschikbaarheidsverplichting voor aanbieders aan de ene kant, terwijl de regulering van de toegang tot deze gegevens aan de andere kant aan de lidstaten blijft voorbehouden. Deze formele scheiding van beschikbaarheid en toegang in de dataretentierichtlijn wordt door het Hof van Justitie bekrachtigd op Europees constitutioneelrechtelijke gronden. Het Hof gaat nog een stap verder, door te oordelen dat de dataretentierichtlijn niets regelt met betrekking tot de toegang. De bepalingen over toegang tot de gegevens in de richtlijn, met name vervat in art. 4 ("alleen in welbepaalde gevallen"), verworden de facto tot betekenisloze vermeldingen zonder harmoniserende werking.[78] Deze constatering van het Hof heeft verstrekkende gevolgen:[79] aan de ene kant is de beperking van de toegangsbevoegdheden van de Duitse opsporingsinstanties, opgelegd door het Duitse Federale Constitutionele Hof,[80] niet in strijd met het Europese constitutionele recht, terwijl onbeperkte

[70] Idem, punt 78.
[71] Later herhaalt het Hof nogmaals dat de dataretentierichtlijn geen enkele regeling van de activiteiten van de overheid voor de wetshandhaving behelst, HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 86-92.
[72] Idem, punt 83-85. De verschillen tussen al geldende dataretentieverplichtingen en tussen de te verwachten nieuwe regelingen, en het effect van deze uiteenlopende maatregelen op de werking van de interne markt, rechtvaardigde het nastreven van een harmonisering van deze maatregelen ten behoeve van de werking van de interne markt – zo oordeelt het Hof, HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 69-72.
[73] Zie uitgebreider Van Hoboken 2009, Teunissen 2009, Drijber 2009.
[74] Idem, punt 70.
[75] Van Veen & Van Ginneken 2009, p.8.
[76] HvJEG 30 mei 2006, Parlement vs. Raad en Commissie, C-317/04 en C-318/04.
[77] Teunissen 2009.
[78] HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 86-92.
[79] Van Hoboken 2009.
[80] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08.

toegangsbevoegdheden voor opsporingsdiensten in nationale wetgeving aan de andere kant niet in strijd zijn met de dataretentierichtlijn. Dit geldt in gelijke zin voor de zinsnede 'ernstige criminaliteit' uit art. 1 lid 1 dataretentierichtlijn; de richtlijn weerhoudt opsporingsdiensten er niet van verplicht bewaarde gegevens in te zien wanneer het lichtere vormen van strafbaar handelen betreft. Terwijl beschikbaarheid gegarandeerd is in de richtlijn, zegt deze al met al niets over de toegang tot die gegevens.

Het lijkt waarschijnlijk dat de gemeenschapswetgever de toegang überhaupt niet had kunnen beperken in de dataretentierichtlijn, vanwege de grondslag in art. 95 EG-verdrag. Advocaat-generaal Bot ziet zich op grond van de Europese constitutionele structuur gedwongen dit standpunt in te nemen, al is hij er niet gelukkig mee (de door de A-G gesignaleerde "coherentie" komt terug in par. 2.4.):

> "108. Deze scheidingslijn is zeker niet vrij van elke kritiek en kan in bepaalde opzichten kunstmatig lijken. Ik geef toe dat het beter zou zijn, de gehele problematiek van het bewaren van gegevens door de aanbieders van elektronische communicatiediensten en de wijze waarop zij samenwerken met de nationale wetshandhavingsautoriteiten te regelen in een enkele handeling die de coherentie tussen die twee elementen verzekert. Ook al valt dit te betreuren, de *constitutionele structuur van drie pijlers noopt ertoe, onderscheid te maken tussen de actieterreinen.* Het is in dit verband in de eerste plaats van belang de rechtszekerheid te waarborgen door de grens tussen de tot de verschillende pijlers behorende actieterreinen zoveel mogelijk te verduidelijken."[81]

Deze door het Europees constitutionele recht ingegeven problematiek – wanneer heeft een maatregel betrekking op de interne markt en wanneer op de opsporing – is niet alleen bij de dataretentierichtlijn aan de orde. In bredere zin komt zij tot uitdrukking wanneer gegevens die berusten bij bedrijven beschikbaar moeten worden gesteld voor de opsporing.[82] Hijmans wijdt dit aan de "onduidelijke afbakening"[83] die tussen de pijlers heerst, aangezien maatregelen vaak niet het een of het ander zijn, maar een beetje van allebei. Het stellen van regels inzake toegang tot de gegevens was slechts geoorloofd geweest als deze regels een zogenaamde "zwaartepunt" in interne marktoverwegingen hadden gevonden.[84] Het stellen van regels inzake de toegangsbevoegdheden zou dan van groter belang moeten zijn in het licht van de interne markt dan de opsporing van strafbare feiten. Mijns inziens een lastig te verdedigen stellingname; wellicht kunnen grote verschillen in nationale wetgevingen tussen aansprakelijkheid van aanbieders bij illegitieme informatievragen een rol spelen.[85]

Wat de oplossing van dit complexe vraagstuk ook zij, Hijmans ziet in het Verdrag van Lissabon met de opheffing van de Derde pijler een goede oplossing: "met het verdwijnen van de Derde pijler verdwijnt ook het probleem van de afbakening tussen de pijlers en een mogelijk juridisch vacuüm tussen die pijlers."[86] Het juridische vacuüm betreft bij de dataretentierichtlijn het ontbreken van voorwaarden c.q. beperkingen met betrekking tot de regulering van toegang tot verplicht bewaarde telecommunicatiegegevens vanwege het recht van de pijlers, niet zozeer vanwege het ontbreken van samenhang tussen beschikbaarheid en toegang. Zeer interessant voor het toekomstige debat inzake dataretentie is dus de constatering, dat er voor de scheiding tussen beschikbaarheid en toegang in de

[81] HvJEG 14 oktober 2008, nr. C-301/06, Conclusie A-G Y. Bot, nr. 108 (eigen cursivering). zie in gelijke zin Drijber 2009, p.261.
[82] Hijmans 2008, p.1794.
[83] Hijmans 2008, p.1792/1793.
[84] HvJEG 14 oktober 2008, nr. C-301/06, Conclusie A-G Y. Bot, nr. 77.
[85] Een interessante vervolgvraag is derhalve of aanbieders in de gehele Europese Unie een medewerkingsplicht hebben, zoals in Nederland het geval is (zie par. 2.2.2. en 2.2.3.).
[86] Hijmans 2008, p.1792/1793.

dataretentierichtlijn onder het Verdrag van Lissabon geen constitutioneelrechtelijke gronden bestaan.[87] Daarmee wordt alle onduidelijkheid weggenomen en kan aan de wens van A-G Y. Bot om dataretentie en toegang in 'een enkele handeling' te regelen gehoor worden gegeven.[88]

Tenslotte heeft de uitspraak van het Hof geen betrekking op een eventuele schending van de grondrechten van burgers, met name art. 8 EVRM.[89] De vraagstukken van effectiviteit en noodzakelijkheid, die al door het Parlement ter discussie zijn gesteld, zijn na de uitspraak evenmin beantwoord. Gezien aanhangige procedures in enkele lidstaten, zoals Duitsland en Ierland, zal het Hof van Justitie zich in de toekomst waarschijnlijk over dit vraagstuk, in de context van nationale implementaties en toegangsbevoegdheden, moeten buigen. Mogelijkerwijs zal de dataretentierichtlijn alsnog stranden op art. 8 EVRM. Lidstaten die geen bewaarverplichting in willen stellen, alsmede ondernemingen en burgers, hebben met de uitspraak wel duidelijkheid over de regulering van de toegang, maar dus nog steeds geen zekerheid over de verenigbaarheid met art. 8 EVRM. In hoofdstuk 3 staat daarom een analyse van deze verenigbaarheid van de dataretentierichtlijn, het Nederlandse implementatievoorstel en de strafvorderlijke toegangsbevoegdheden met art. 8 EVRM centraal.

## 1.6. Conclusie

Uit de voorgeschiedenis van de Europese bewaarplicht zijn een aantal aandachtspunten te identificeren, die op hun beurt weer eigen consequenties hebben. De Europese bewaarplicht is er gekomen in de vorm van dataretentierichtlijn, die een lex specialis is ten opzichte van de E-privacyrichtlijn, op zijn beurt weer een specifieke wetgevingsmaatregel gebaseerd op de Privacryrichtlijn uit 1995. Dit veronderstelt een samenhang tussen de richtlijnen, maar in feite staan de richtlijnen op gespannen voet met elkaar: zij stellen zich ten doel de persoonlijke levenssfeer te beschermen, maar wijken hier volledig vanaf door aanbieders te verplichten telecommunicatiegegevens voor een zekere periode te bewaren om de beschikbaarheid voor opsporingsdiensten te garanderen. De ambivalente boodschap van art. 6 jo. art. 9 versus art. 15 lid 1 E-privacyrichtlijn, "anonimiseren" versus "lidstaten kunnen aanbieders verplichten te bewaren ten behoeve van de opsporing", is met de dataretentierichtlijn nog sterker geworden: "anonimiseren" versus "alle aanbieders moeten bewaren." De Europese burger kan hieruit niet afleiden of Europa zijn persoonlijke levenssfeer nu eerbiedigt of van ondergeschikt belang acht.

Uit de voorgeschiedenis van de Europese bewaarplicht blijkt echter dat het eerbiedigen van de persoonlijke levenssfeer van de Europese burger onderbelicht was. Binnen politieke klimaat van de eerste helft van dit decennium streefde de Raad naar het uitbreiden van de opsporingsbevoegdheden, als gevolg van enkele terroristische aanslagen die als katalysator gefungeerd hebben voor een uitbreiding van deze bevoegdheden in veel bredere zin – niet alleen gerelateerd aan terrorismebestrijding. De Raad heeft de eigen wensen weten te verwezenlijken, in tegenstelling tot het Parlement dat in de afgelopen jaren weinig invloed heeft kunnen uitoefenen op het Europese wetgevingsproces inzake de bescherming van de persoonlijke levenssfeer, althans in de Europese elektronische communicatiesector. Het recht van de pijlers binnen de Europese Unie heeft waarschijnlijk

[87] Zie par. 5.3.
[88] Vgl. citaat op de vorige pagina, HvJEG 14 oktober 2008, nr. C-301/06, Conclusie A-G Y. Bot, nr. 108.
[89] HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 57.

bijgedragen aan een sterke onderhandelingspositie van de Raad, die de onderhandelingen over de uiteindelijke tekst van de dataretentierichtlijn onder opvoering van de tijdsdruk binnen een krappe drie maanden in zijn voordeel wist te beslechten. Dat de Commissie en het Parlement de eigen wensen vrij gemakkelijk lieten varen omdat zij uitsluiting van het dataretentiedebat niet wilden riskeren, lijkt een plausibele verklaring. Effectiviteit, noodzakelijkheid, technische uitvoerbaarheid en de impact op de interne markt en aanverwante economische effecten van dataretentie zijn tijdens de onderhandelingen van de dataretentierichtlijn niet of nauwelijks onderzocht. De uitspraak van het Hof over de rechtsgrondslag van de richtlijn heeft hier evenmin duidelijkheid over verschaft, waardoor tot op de dag van vandaag geen oordeel geveld is over de vraag of de dataretentierichtlijn de toets van art. 8 EVRM kan doorstaan.

Dezelfde uitspraak van het Hof bekrachtigt daarentegen wel de met de dataretentierichtlijn aangebrachte formele scheiding tussen de regulering van beschikbaarheid en toegang, nu de richtlijn in de huidige vorm niets regelt over de toegang tot de gegevens. Dat toegang alleen in "welbepaalde gevallen" ex art. 4 dataretentierichtlijn is toegestaan, verwordt met de uitspraak tot een vermelding. Wellicht is in het turbulente totstandkomingsproces uitgegaan van de veronderstelling dat de gemeenschapswetgever in de Eerste pijler niet gerechtigd is om regels over de toegang te stellen, op het eerste gezicht een bevoegdheid binnen de Derde pijler van de Europese Unie. Hoe dan ook komt dit juridische vacuüm met het Verdrag van Lissabon te vervallen en kan zodoende aan de wens van het Parlement en A-G Y. Bot, om regels inzake de toegang op te nemen in de richtlijn, gehoor worden gegeven. Vooralsnog is hiervan geen sprake: de dataretentierichtlijn bevat de verplichting voor aanbieders om specifieke persoonsgegevens te bewaren, terwijl de regulering van de toegang tot telecommunicatiegegevens het domein van de lidstaten blijft.

Al was de eerbiediging van de persoonlijke levenssfeer in de gehele voorgeschiedenis van de Europese bewaarplicht onderbelicht, zal de art. 8 EVRM discussie de komende jaren in het centrum van de aandacht komen te staan. Op een goed moment zal het Hof van Justitie zich over dit vraagstuk buigen. Dit geldt zowel voor de verenigbaarheid van de dataretentierichtlijn met art. 8 EVRM, als voor die van de verhouding tussen de overigens sterk uiteenlopende nationale implementaties en strafvorderlijke bevoegdheden. Voordat de art. 8 discussie in hoofdstuk 3 uitgebreid ter sprake komt, staan in het volgende hoofdstuk de regulering van beschikbaarheid en toegang in Nederland en de implicaties van het implementatievoorstel centraal.

# 2. HET NATIONALE PERSPECTIEF

De Nederlandse wetgever implementeert de dataretentierichtlijn in nationale wetgeving met het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens.[90] Het doel van het wetsvoorstel is opleggen van een bewaarverplichting van bepaalde categorieën telecommunicatiegegevens aan aanbieders voor een zekere periode, zodat deze gegevens gegarandeerd beschikbaar zijn voor onderzoeken, opsporen en vervolgen van ernstige misdrijven.[91]

In dit hoofdstuk volgt allereerst een uiteenzetting van de huidige situatie met betrekking tot de beschikbaarheid van en toegang tot telecommunicatiegegevens. Vervolgens worden de te verwachten implicaties van de dataretentierichtlijn en het momenteel in behandeling zijnde wetsvoorstel geanalyseerd. Met deze prospectieve analyse wordt inzicht geboden in de weerslag van het wetsvoorstel op de regulering van beschikbaarheid en toegang, een inzicht dat noodzakelijk is om de verenigbaarheid met art. 8 EVRM te kunnen toetsen in hoofdstuk 3.

## *2.1. Beschikbaarheid en toegang; gebruik?*

Zodra telecommunicatiegegevens gebruikt worden voor opsporingsonderzoek, doorlopen zij in ieder geval drie onderscheidenlijke stadia – 'beschikbaarheid', 'toegang' en 'gebruik'. Op het moment dat opsporingsdiensten telecommunicatiegegevens hebben opgevraagd bij een aanbieder, ziet specifieke wet- en regelgeving toe op de registratie daarvan en het verdere gebruik van die informatie door de opsporingsdiensten. Voor de meer dan 50.000 politiemensen in ons land is dit de Wet politiegegevens.[92] Mac Gillavry signaleert dat de verhouding tussen deze wet en het Wetboek van Strafvordering onduidelijk is, omdat er in de Wet politiegegevens onvoldoende oog is voor het feit dat de toegang tot telecommunicatiegegevens vooraleerst geregeld is in het Wetboek van Strafvordering.[93] Tegelijkertijd bevat het Wetboek van Strafvordering hier en daar voorschriften voor het gebruik van de informatie, zoals het gebruik van DNA-profielen ex 151a lid 6 Sv jo. 195a lid 4 Sv en de tapverslagen van art. 126dd Sv. Deze fragmentarische invulling van de informationele privacy van het 'onderzoekssubject' (lees: zowel verdachte- als niet-verdachte burgers), maakt het hanteren van de juiste rechtsgrondslag dan ook tot een complexe aangelegenheid voor de politie. In de praktijk worden hier vaak fouten gemaakt.[94]

Met de constatering dat de grens tussen toegang en gebruik in de wet- en regelgeving niet scherp getrokken en in de praktijk moeilijk hanteerbaar is, richt dit hoofdstuk zich alleen op de toegangsbevoegdheden tot telecommunicatiegegevens op grond van het Wetboek van Strafvordering en de beschikbaarheid ervan op grond van de Telecommunicatiewet. Het gebruik van de

[90] *Kamerstukken II*, 2006-2007, 31 145, nr.2, (Wet bewaarplicht telecommunicatiegegevens). Inmiddels geamendeerd, Kamerstukken I, 2008-2009, 31 145, nr. A.
[91] *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.1.
[92] *Stb.* 2007, 300.
[93] Mac Gillavry 2006, p.394. Mac Gillavry zoekt de verklaring hiervoor in het leerstuk informationele privacy, dat pas laat tot ontwikkeling kwam in de Nederlandse rechtsorde. Art. 10 van de Grondwet stamt bijvoorbeeld uit 1988, terwijl de basis van het Wetboek van Strafvordering eerder gelegd is.
[94] Mac Gillavry 2006, p.415-416. Zwenne & Schmidt 2005, p.298.

telecommunicatiegegevens komt bij de legitimering van de inbreuk op de persoonlijke levenssfeer (zie par. 3.3.1.) weer ter sprake.

## 2.2. Huidige situatie

### 2.2.1. Beschikbaarheid van telecommunicatiegegevens

De hoofdregels en de uitzonderingen uit de E-privacyrichtlijn zijn uitgewerkt in art 11.5 Tw voor verkeersgegevens en art. 11.5a Tw voor locatiegegevens. Art. 15 lid 1 E-privacyrichtlijn is geïmplementeerd in art. 11.13 Tw.[95] Destijds is de praktische betekenis van dit artikel in de parlementaire behandeling in de Eerste Kamer.[96] Het moest toezien op de situatie dat aan aanbieders een verzoek gedaan werd om op vrijwillige basis mee te werken aan opsporingsonderzoek. De aanbieder moest dit toen nog zelf overwegen, met name met relevante bepalingen van de Wet bescherming persoonsgegevens in het achterhoofd, en hoefde nog niet mee te werken.[97]

Ondanks de expliciete grondslag in art. 15 lid 1 E-privacyrichtlijn is er in de Nederlandse rechtsorde geen sprake van een algemene bewaarplicht van telecommunicatiegegevens. Sinds 1 maart 2002 bestaat er al wel een bijzondere bewaarplicht voor aanbieders van mobiele telecommunicatie ex art. 13.4 lid 2 Tw jo. art. 7 Besluit bijzondere vergaring nummergegevens telecommunicatie.[98] Aanbieders moeten gegevens over het tijdstip, het nummer en het basisstation gedurende drie maanden bewaren, teneinde de identificatie van prepaid bellers mogelijk te maken. Langer dan deze drie maanden, de tijd waarin andere verkeersgegevens gemiddeld bij aanbieders worden opgeslagen voor facturering, achtte de regering destijds een "te grote uitholling van het principe van zo spoedig mogelijk wissen of anonimiseren."[99] Daarnaast hebben opsporingsdiensten nog de mogelijkheid van het bevriezingsbevel van art. 126ni Sv, op basis waarvan aanbieders verplicht kunnen worden om bepaalde telecommunicatiegegevens voor een periode van negentig dagen niet te verwijderen. Deze periode kan met nog eens negentig dagen worden verlengd op grond van art. 126ni lid 5 Sv. Het vereiste voor effectueren van deze gerichte bewaarplicht is de verdenking van een misdrijf ex art. 67 lid 1 Sv, dat een ernstige inbreuk op de rechtsorde vormt.

Uit het inmiddels zes jaar oude rapport van Stratix Consulting Group B.V. blijkt, dat de bewaartermijnen van aanbieders in de praktijk destijds varieerden van enkele dagen tot een aantal maanden – in enkele gevallen is er zelfs sprake van onbeperkte opslag.[100] Een van de conclusies uit het rapport is dat de aanbieders een groot deel van de informatie, waaraan de opsporingsdiensten behoefte hebben, kunnen leveren dankzij de registratie ervan in het kader van de reguliere bedrijfsvoering.[101]

---

[95] De wetgever heeft met dit artikel willen verhelderen dat het aftappen en opnemen van telecommunicatie en de vordering van verkeersgegevens door opsporingsinstanties geoorloofd is op grond van art. 3 lid 2 95/46/EG jo. art. 15 lid 1 2002/58/EG: *Kamerstukken II*, 2003-2004, 28 851, nr. 3 (MvT), p.165.
[96] *Kamerstukken I*, 2003-2004, 28 851, nr. C (MvA), p.28.
[97] Inmiddels geldt er voor de aanbieders een medewerkingsverplichting, zie par. 2.2.2.
[98] *Stb.* 2002, 31.
[99] *Handelingen I*, 13. okt. 1998, nr. 3, p.46; *Kamerstukken II*, *II*, 1996-1997, 25 533, nr. A, p.19.
[100] Stratix 2003, p.3.
[101] Idem.

### 2.2.2. Toegang tot telecommunicatiegegevens

De toegang tot telecommunicatiegegevens in het kader van de opsporing van strafbare feiten wordt geregeld in het Wetboek van Strafvordering, in het bijzonder in de Wet vorderen gegevens telecommunicatie die sinds 2004 van kracht is.[102] Het valt buiten het bereik van dit onderzoek om alle toegangsbevoegdheden uit deze wet op te sommen, hier wordt stilgestaan bij het vorderen van telecommunicatiegegevens door de Officier van Justitie en van identificerende gebruiksgegevens door opsporingsambtenaren, veruit de meest voorkomende toegangsvorderingen voor opsporingsonderzoek.

De Officier van Justitie kan in het belang van opsporingsonderzoek telecommunicatiegegevens vorderen op grond van drie artikelen. Bij sprake van een aanwijzing van een terroristisch misdrijf baseert de Officier zijn vordering op art. 126zh lid 1 Sv, terwijl de vorderingsgrondslag van art. 126u lid 1 Sv gebruikt dient te worden bij een uit feiten en omstandigheden voortvloeiend redelijk vermoeden van misdrijven die in georganiseerd verband worden gepleegd, alsmede een ernstige inbreuk op de rechtsorde vormen. Meestal zal de grondslag van een verzoek om toegang tot telecommunicatiegegevens in art. 126n lid 1 Sv gevonden worden, bij de verdenking van een misdrijf zoals omschreven in art. 67 lid 1 Sv.[103] Wil de Officier toegang tot telecommunicatiegegevens afdwingen, zal er dus in ieder geval sprake moeten zijn van een misdrijf met een bepaalde ernst, waarbij art. 67 lid 1 Sv het eerste toetsingscriterium is. Art. 67 lid 1 Sv luidt als volgt:

> *Artikel 67*
>
> *[1.] Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van:*
>
> *a. een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld;*
>
> *b. een der misdrijven omschreven in de artikelen 132, 138a, 138b, 139c, 139d, eerste en tweede lid, 161sexies, eerste lid, onder 1°, en tweede lid,137c, tweede lid, 137d, tweede lid, 137e, tweede lid, 137g, tweede lid, 285, eerste lid, 285b, 300, eerste lid, 321, 323a, 326c, tweede lid, 350, 350a, 351, 395, 417bis en 420quater van het Wetboek van Strafrecht;*
>
> *c. een der misdrijven omschreven in:*
> *artikel 122, eerste lid, van de Gezondheids- en welzijnswet voor dieren;*
> *artikel 175, tweede lid, onderdeel b, of derde lid in verbinding met het eerste lid, onderdeel b, van de Wegenverkeerswet 1994;*
> *artikel 30, tweede lid, van de Wet buitengewone bevoegdheden burgerlijk gezag;*
> *de artikelen 52, 53, eerste lid en 54 van de Wet gewetensbezwaren militaire dienst;*
> *artikel 31 van de Wet op de kansspelen;*
> *artikel 11, tweede lid, van de Opiumwet;*
> *artikel 55, tweede lid, van de Wet wapens en munitie;*
> *de artikelen 5:56, 5:57 en 5:58 van de Wet op het financieel toezicht;*
> *artikel 11 van de Wet tijdelijk huisverbod.*

Sub a bevat een inzichtelijke ondergrens die een bepaalde ernst van misdrijven aangeeft. Achter onderdeel b staan delicten vermeldt waarvan de maximumstraf minder is dan vier jaren. Een aantal daarvan hebben nauwelijks een ernstig karakter, zoals al eens is opgemerkt in de Tweede Kamer,[104]

---

[102] *Stb.* 2004, 105. Ingevolge art. 126ng lid 1 Sv kunnen de algemene vorderingsbevoegdheden in het Wetboek van Strafvordering niet worden gebruikt voor het vorderen van telecommunicatiegegevens die op grond van art. 126n Sv of art. 126na Sv gevorderd moeten worden.

[103] De Officier van Justitie kan deze artikelen dus niet bij een verkennend onderzoek aanwenden. Dan ligt de grondslag in art. 126gg Sv en geldt overigens ook het criterium 'ernstige inbreuk op de rechtsorde'.

[104] *Hand. II*, 2006-2007, 31 145, nr. 83, p. 5813; Zwenne & Schmidt 2008, p.283.

bijvoorbeeld 'de heling van een goed' (art. 417bis Sr – om het even wat voor soort goed het hier betreft) en 'het door twee personen doen toekomen van een goed aan een derde persoon waarin een beledigende opmerking is vervat' (art. 137e lid 2 Sr). Tientallen misdrijven omschreven in sub c zijn wel erg triviaal, zoals 'het gebruiken van een hond als trekkracht' ex art 122 lid 1 jo 36 lid 1 jo. lid 2 Gezondheids- en welzijnswet voor dieren. In het verlengde hiervan zijn andere criteria voor toegang door de Officier verruimd met de Wet vorderen gegevens telecommunicatie. Zo hoeft een toegangsverzoek zich niet langer alleen op de verdachte, maar kan het zich tot alle betrokkenen bij het strafbare feit richten. Koops & Buruma stellen vast dat hiermee "in principe van iedereen gegevens [kunnen] worden opgevraagd."[105]

Over de frequentie van toegangsverzoeken door de Officier van Justitie is niets geregeld. Desgevraagd mag vorderingsbevoegdheid volgens de wetgever overeenkomen met stelselmatige observatie; het frequent opvragen van locatiegegevens geeft vrij nauwkeurig de geografische positie van personen aan, bijvoorbeeld tijdens een demonstratie.[106] Merkwaardig genoeg worden geen gegevens bijgehouden over hoe vaak Officieren van Justitie hun bevoegdheden gebruiken.[107] Tegelijkertijd blijkt de notificatieplicht van art. 126bb Sv[108] in de praktijk massaal te worden genegeerd, omdat notificatie geen prioriteit heeft binnen het OM en er geen sanctie staat op het uitblijven ervan.[109] Burgers krijgen soms pas na enige tijd, maar dus meestal nooit in de gaten of zij ooit 'onderzoekssubject' waren in het kader van de opsporing.

Behalve de Officier van Justitie, heeft ook de opsporingsambtenaar toegang tot telecommunicatiegegevens in het kader van opsporingsonderzoek. Op basis van de met de Wet vorderen gegevens telecommunicatie van 2004 aan het Wetboek van Strafvordering toegevoegde artt. 126na Sv, 126ua Sv en 126zi Sv[110] kunnen opsporingsambtenaren in de zin van art. 1 lid 1 sub d onder 1° Besluit verstrekking gegevens telecommunicatie[111] identificerende gebruiksgegevens vorderen bij aanbieders. 'Identificerende gebruiksgegevens' betreffen naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie alsmede e-mailadressen, IP-adressen, inlognamen, gebruikersnamen, en identificatienummers randapparatuur. De drempel om deze gegevens in te zien is lager dan bij de vorderingsbevoegdheid op grond van de artt. 126n/126u/126zh, namelijk 'verdenking van een misdrijf'. Het hoeft hier evenmin de verdachte te betreffen, ook betrokkenen kunnen geraadpleegd worden zolang dit 'in het belang van het onderzoek' is. Op basis van gebruiksgegevens wordt dus inzicht verkregen in sociale patronen en kunnen verbanden worden gelegd in het opsporingsonderzoek[112], bijvoorbeeld door alle personen X op te zoeken met wie

[105] Koops & Buruma 2007, p.85.
[106] *Kamerstukken II*, 2001-2002, 28 059, nr. 3 (MvT), p.8/9.
[107] *Kamerstukken II*, 2003-2004, 29 441, nr. 3 (MvT), p.5.
[108] Aan de notificatieplicht hoeft overigens pas te worden voldaan als de Officier het inzicht is toegedaan dat het onderzoek notificatie toestaat vanwege de toevoeging van de zinsnede "in het belang van het onderzoek" aan art. 126bb Sv, *Kamerstukken II*, 2003-2004, 29 441, nr. 3 (MvT), p.5.
[109] *Kamerstukken II*, 2004-2005, 30 164, nr. 5, p.7; Chavannes 2008. Het sanctioneren van misbruik van toegangsbevoegdheden was overigens een wens van het Europees Parlement die de uiteindelijke tekst van de dataretentierichtlijn niet haalde.
[110] De toegangscriteria 'verdenking', 'redelijk vermoeden' en 'aanwijzing' bij respectievelijk de artt. 126na, 126ua en 126zi Sv lopen parallel als bij de zojuist behandelde artt. 126n, 126u en 126zh Sv.
[111] *Stb.* 2000, 71. Art. 1 lid 1 sub d onder 1° luidt: "de beheerder van een politiekorps of het hoofd van een opsporingsdienst, dan wel de door de beheerder voor zijn korps of door het hoofd voor zijn dienst aangewezen opsporingsambtenaar."
[112] *Kamerstukken II*, 2001-2002, 28 059, nr. 3 (MvT), p.9; Koops & Buruma 2007, p. 87.

verdachte Y in periode rond strafbaar feit Z gebeld heeft en vervolgens van alle personen X de telecommunicatiegegevens rond die periode te vorderen bij aanbieders op grond van art. 126n lid 1 Sv. Het Kabinet beschouwt de reeks artikelen inzake gebruiksgegevens dan ook als "de basis voor strafrechtelijk onderzoek."[113]

Het verzoek om toegang door opsporingsambtenaren is niet direct gericht tot de aanbieders, maar geschiedt met tussenkomst van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) ex 126na lid 4 Sv jo. art. 3 lid 2 Besluit verstrekking gegevens telecommunicatie.[114] Aanbieders moeten een bestand aanmaken per gebruiker waarin de gebruiksgegevens zijn opgenomen, en uploaden naar deze database, waartoe opsporingsambtenaren overigens te allen tijde toegang hebben. Deze bestanden dienen iedere 24 uur geactualiseerd te worden door de aanbieders op grond van art. 3 lid 3 Besluit, terwijl inzage door opsporingsambtenaren zonder medeweten van aanbieders plaatsvindt (art. 5 lid 4 sub a Besluit).[115] In 2002 was de verwachting dat de nieuwe bevoegdheid op termijn zou kunnen leiden tot een toename van de verzoeken van 300% tot 900.000 verzoeken per jaar.[116] In 2007 was het aantal jaarlijkse verzoeken echter al gestegen naar 1.901.024, met een gemiddelde toename van 24,7% per jaar sinds 2004.[117] Er bestaat geen notificatieplicht richting gebruikers voor raadpleging van het CIOT.[118]

Evenals bij de vorderingsbevoegdheid van de Officier van Justitie, leiden bovenstaande constateringen tot de vaststelling dat de wettelijke drempel voor de uitoefening van de vorderingsbevoegdheid door opsporingsambtenaren laag is, dat de reikwijdte van de bevoegdheden niet gering is, terwijl 'onderzoekssubjecten' nooit te komen zullen komen of en hoe vaak hun gebruiksgegevens door opsporingsambtenaren bevraagd zijn via het CIOT.

De nationale veiligheid wordt bewaakt door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), alsmede de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Ingevolge de Wet op de inlichtingen- en veiligheidsdiensten 2002 (hierna: Wiv)[119] kunnen deze diensten zich wenden tot de aanbieders om ex art. 28 Wiv verkeersgegevens, ex art. 29 Wiv gebruiksgegevens te vorderen. De wetgever heeft voor de AIVD en MIVD alternatieve drempels geconstrueerd, waaraan voldaan moet zijn willen de diensten telecommunicatiegegevens kunnen vorderen. Allereerst is er een noodzakelijkheidscriterium in het kader van de onder 6 sub a en 6 sub d, alsmede 7 sub a, 7 sub c en 7 sub e Wiv genoemde taken. Naast de hierin neergelegde afbakening van functiegebieden, geldt tevens dat de telecommunicatiegegevens noodzakelijk moeten zijn ter vervulling van deze taken. Op de tweede plaats is er een zogenaamd proportionalisteitsvereiste ex art. 31 Wiv, dat wil zeggen dat een verzoek om toegang alleen geoorloofd als gegevens niet op andere wijze verkregen kunnen worden, via informatiebronnen die voor een ieder of exclusief voor de diensten toegankelijk zijn.

Voor de inlichtingen- en veiligheidsdiensten geldt geen notificatieplicht en zijn evenmin gegevens bekend over de aanlevering van gegevens door aanbieders. Het CBP is bovendien onbevoegd om onafhankelijk toezicht uit te oefenen over het gebruik van bevoegdheden door de inlichtingen- en veiligheidsdiensten. Dit toezicht is geplaatst bij een intern orgaan, namelijk de Commissie van Toezicht

---

[113] *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.32/33.
[114] *Stb.* 2000, 71. Zie tevens Smits 2006, p.156. Meer informatie over de werkwijze van het CIOT is te vinden via: <http://www.justitie.nl/onderwerpen/opsporing_en_handhaving/ciot/> [geraadpleegd juli 2009].
[115] *Stb.* 2000, 71, p.16.
[116] *Kamerstukken II*, 2001-2002, 28 059, nr. 3 (MvT), p.17.
[117] *Kamerstukken II*, 2007–2008, 31 444 VI, nr. 1, p.64.
[118] *Kamerstukken II*, 2003-2004, 29 441, nr. 3 (MvT), p.5.
[119] *Stb.* 2002, 148. Huidige regeling: *Stb.* 2005, 32.

betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) op grond van art. 64 e.v. Wiv. Gevraagd naar gegevens over de uitoefening van bevoegdheden door de diensten schuilt het Kabinet dit steevast onder het zogenaamde "staatsgeheim", nu gegevens inzicht zouden kunnen verschaffen over de werkwijze van deze diensten.[120]

Tot slot een korte opmerking over de aanbieders, voor wie een wettelijke medewerkingsverplichting geldt met betrekking tot toegangsverzoeken van opsporingsdiensten, de AIVD en de MIVD op grond van art. 13.2a Tw en art. 13.4 Tw. Bij een verzoek dienen zij de verkeers- en locatiegegevens, zoals opgesomd in art. 2 Besluit vorderen gegevens telecommunicatie,[121] te overleggen. Sinds de inwerkingtreding van de Wet vorderen gegevens telecommunicatie is dit geregeld in een AMvB en niet langer in een wet in formele zin, zodat de lijst met aan te leveren telecommunicatiegegevens eenvoudiger is aan te passen aan de technologische status quo.

### 2.2.3. Ontwikkelingen in strafvorderlijke bevoegdheden sinds de Commissie-Mevis

De Wet vorderen gegevens telecommunicatie ligt in het verlengde van het in mei 2001 verschenen rapport van de Commissie-Mevis,[122] dat concludeerde dat het toenmalige Wetboek van Strafvordering niet toereikend was.[123] De stand van de techniek had het Wetboek voorbijgesneld, zo signaleerde de Commissie-Mevis; waardevolle informatie werd dientengevolge misgelopen. Daarnaast was justitie te afhankelijk van de houders van gegevens voor de daadwerkelijke verstrekking daarvan, omdat zij op basis van het in art. 43 Wbp verankerde beginsel van doelbinding een eigen afweging moesten maken alvorens gegevens te verstrekken. In de praktijk verstrekten houders vrijwel altijd,[124] maar de theoretische mogelijkheid van de eigen afweging leidde tot rechtsonzekerheid. De belangrijkste aanbeveling van het rapport was een nieuw wetsvoorstel, waarmee de afhankelijkheid van de houder weggenomen werd.[125] Dit behelsde een ingewikkelde nieuwe regulering van de toegangsbevoegdheden, die op kleine details na vandaag de dag nog van kracht is. Het rapport beoogde de rechtsonzekerheid bij aanbieders te ondervangen, maar is zeer scherp aangevallen vanuit alle windhoeken van de academische wereld.[126] Het voornaamste punt van kritiek was het vooropstellen van het opsporingsbelang, terwijl de belangen en rechten van burgers veel te weinig aandacht en bescherming toekwam.

Een aantal maanden na het verschijnen van het rapport van de Commissie-Mevis vinden de terroristische aanslagen in de Verenigde Staten plaats. Op 5 oktober reageren de vijf verantwoordelijke Ministers in een gezamenlijke brief, waarin zij onder meer schrijven dat er sinds de aanslagen "nationaal en internationaal een breed en sterk draagvlak [is] ontstaan voor het intensiveren van de strijd tegen het

[120] *Kamerstukken II*, 2006-2007, 31 145, nr.5, p.4.
[121] *Stb.* 2004, 394.
[122] Commissie-Mevis 2001.
[123] *Kamerstukken II*, 2001-2002, 28 059, nr. 3 (MvT), p.6.
[124] Mac Gillavry 2004, p.204.
[125] Commissie-Mevis 2001, p.5, p.7, p.44, p.50; *Kamerstukken II*, 2001-2002, 28 059, nr. 3 (MvT), p.3.
[126] Bijvoorbeeld E.J. Dommering, *Het ongebreideld verzamelen van gegevens: de voorstellen van de Commissie-Mevis*, Netkwesties, 1 november 2001, <http://www.netkwesties.nl/editie24/column1.html> [geraadpleegd juli 2009]; E.C. Mac Gillavry, *De voortstellen van de Commissie-Mevis – dwangmiddelen voor de informatiemaatschappij*, NJB (76) 2001-30; maar jaren later ook nog in Koops & Buruma 2007, p.84.

terrorisme." In de brief wordt het Actieplan terrorismebestrijding en veiligheid uiteengezet.[127] Dit plan bevatte een 43-tal actiepunten om terrorisme aan te pakken, waarbij er prominente plaatsen waren gereserveerd voor het versterken van de informatiepositie van de overheidsdiensten, waaronder het uitbreiden van de inlichtingen- en veiligheidsdiensten (onder actie 1), het uitbreiden van de opsporings- en vervolgingscapaciteit (onder actie 14) en het treffen van technologische maatregelen, waaronder het invoeren van dataretentieverplichtingen (onder actie 17).

In de daaropvolgende jaren heeft de politiek vooral oog voor terrorismebestrijding en opsporing in meer algemene zin.[128] De voorstellen van de Commissie-Mevis worden tijdens de parlementaire behandeling dan ook zonder al teveel politieke weerstand in grote lijnen overgenomen in het Wetboek van Strafvordering. Het belang van het blijven beschermen van de persoonlijke levenssfeer van burgers wordt in het gehele Actieplan niet vermeld. Een herkenbare tekortkoming, die ook bij de totstandkoming van de dataretentierichtlijn gesignaleerd is (zie par. 1.4.).

De in de vorige paragraaf besproken Wet vorderen gegevens telecommunicatie is gebaseerd op de bevindingen van de Commissie-Mevis. De parlementaire behandeling van deze wet vangt aan op 24 oktober 2001 – ruim twee weken na het verschijnen van het Actieplan. De laagdrempelige toegangscriteria, het loslaten van de verdachte-eis, het karakter van stelselmatige observatie, de invoering van de vorderingsbevoegdheid voor opsporingsambtenaren, de medewerkingplicht voor aanbieders – deze reeks fenomenen vinden hun oorsprong in de nieuwe regulering van de toegang tot telecommunicatiegegevens met de Wet vorderen gegevens telecommunicatie.

De Wet computercriminaliteit II[129] en de Wet terroristische misdrijven,[130] beide in 2006 van kracht geworden, passen in dezelfde trend waarin de eerbiediging van de persoonlijke levenssfeer van ondergeschikt belang is ten opzichte van de uitbreiding van de opsporingsbevoegdheden. Met de Wet computercriminaliteit II worden vele delicten toegevoegd aan art. 67 lid 1 sub b Sv, waardoor ze binnen de reikwijdte van de aan telecommunicatiegegevens gerelateerde vorderingsbevoegdheid van de Officier van Justitie komen. De Wet terroristische misdrijven bevat onder meer een nieuwe artikel 126hh Sv, dat de Officier van Justitie de bevoegdheid geeft om gegevensbestanden te vorderen van publieke en particuliere instanties, teneinde deze onderling of in combinatie met gegevens uit andere bestanden te vergelijken, oftewel een grondslag voor de datamining van telecommunicatiegegevens. Lid 3 bevat een vrij inhoudsloze verwijzing naar de persoonlijke levenssfeer, namelijk dat deze "zo veel mogelijk wordt gewaarborgd." Ook al worden de risico's voor de privacy van burgers in de parlementaire behandeling door zowel Kamerleden als het College Bescherming Persoonsgegevens[131] onderkend, wordt het wetsvoorstel zonder significante weerstand aangenomen.

---

[127] *Kamerstukken II*, 2001-2002, 27 925, nr. 10, *Terroristische aanslagen in de Verenigde Staten*, Brief van de Minister-president, Minister van Algemene Zaken en van de Ministers van Justitie, van Binnenlandse Zaken en Koninkrijksrelaties, van Financiën en van Defensie.

[128] Smits 2006, p.148; Stevens, Koops & Wiemans 2004, p.1683.

[129] *Stb.* 2006, 300. Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie.

[130] *Stb.* 2006, 580. Wet van 20 november 2006 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven.

[131] Er hoeft geen sprake te zijn van concrete verdenking, er komen dus veel onverdachte personen in beeld bij art. 126na lid 1 Sv. De risico's zijn hier nog fundamenteler, nu personen onder dit artikel in beeld komen omdat zij, gezien bepaalde feiten en omstandigheden, behoren tot een bepaalde verzameling personen. Daarmee zijn discriminatie en willekeur reële risico's. *Kamerstukken II*, 2004-2005, 30 164, nr. F, p.2 e.v.

De tendens dat het spelersveld in de opsporing drastisch verandert nu er sprake is een steeds intensievere samenwerking tussen opsporingsdiensten en de private sector, is al langere tijd gaande en werd door veel commentatoren besproken.[132] Deze samenwerking heeft twee redenen, te weten privatisering en gemak voor opsporingsdiensten.[133] De privatisering, oftewel het uit handen raken van telecommunicatie-infrastructuren van de overheid aan het bedrijfsleven, voedt het belang dat behoeftestellers hebben bij het kunnen beïnvloeden van die infrastructuur, zoals in par. 1.2. al werd gesignaleerd.[134] Na de aanslagen van 11 september 2001 hebben overheden deze samenwerking met de opsporing geïntensiveerd.[135] In het begin is dit moeilijk waarneembaar geweest, een reden voor Birnhack & Elkin-Koren om dit proces in 2003 "the invisible hand" te noemen. Dit betreft "the re-emergence of the state in the digital environment",[136] nadat de staat daaruit was teruggetreden met halverwege de jaren '90. Inmiddels gaat de samenwerking veel verder. In vrijwel iedere branche van het bedrijfsleven is zij van kracht, vooral in de financiële- (banken en verzekeraars), medische-, logistieke- en telecommunicatiesector[137] – ook op Europese schaal.[138] Een belangrijke consequentie van deze samenwerking is het weglaten van de burger in het gehele proces van verstrekking. Door de besproken medewerkingsverplichting voor aanbieders is een wettelijke grondslag voor verstrekking ontstaan, en hoeven aanbieders het privacybelang van de gebruiker niet langer te beschermen. De belangen van opsporingsdiensten en bedrijven lopen bij verstrekking dus parallel,[139] de burger kan slechts toekijken[140] en hopen dat hij genotificeerd wordt. Mac Gillavry betoogd echter dat het privacybelang er in het proces van verstrekking tussen bedrijven en opsporingsinstanties wel degelijk toe doet, omdat "de burger gestigmatiseerd kan raken hetgeen zijn maatschappelijk functioneren kan beïnvloeden."[141] Mac Gillavry concludeert dat er door de intensieve samenwerking tussen bedrijfsleven en opsporingsinstanties geen feitelijke toegangsbelemmeringen meer zijn voor de inzage in persoonsgegevens.

De ontwikkeling dat de uitbreiding van de opsporingsbevoegdheden prevaleert boven de eerbiediging van de persoonlijke levenssfeer valt gezien het voorgaande in vier deelontwikkelingen te ontleden. De totstandkoming van nieuwe opsporingsbevoegdheden (artt. 126na lid 1 Sv en 126hh Sv), de toegenomen reikwijdte van bestaande bevoegdheden (de vervallen verdachte-eis), de grotere informatiemacht van opsporingsinstanties (de medewerkingplicht aanbieders) en de verregaande samenwerking opsporingsdiensten – bedrijfsleven. Deze vier ontwikkelingen komen overeen met vier van de zes

[132] Stevens, Koops & Wiemans 2004, p.1683; Smits 2006; Koops & Buruma 2007. Uitgebreid in het promotieonderzoek van Mac Gillavry 2004; Birnhack & Elkin-Koren 2003; en B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002.
[133] Mac Gillavry 2004, p.1.
[134] Tevens door bijvoorbeeld Birnhack & Elkin-Koren 2003, p.34 e.v.
[135] Birnhack & Elkin-Koren 2003, p.27.
[136] Birnhack & Elkin-Koren 2003.
[137] Voor een uitgebreide bespreking van de samenwerking tussen overheden en bedrijven in de praktijk en de sectoren die hier in het geding zijn, wordt verwezen naar Mac Gillavry 2004, hfd.4.
[138] Het kaderbesluit van de Raad over het gebruik van gegevens van vliegtuigpassagiers in Europa, dat leidde tot het beroemde PNR-arrest van het Hof van Justitie (C-317/04 en C-318/04) geldt als berucht voorbeeld, evenals de door Birnhack en Elkin-Koren expliciet besproken maatregel dataretentie, Birnhack & Elkin-Koren 2003, par. IV.B.2., p.37-41.
[139] Mac Gillavry 2004, p.203. In gelijke zin rnhack & Elkin-Koren, p.26.
[140] Mac Gillavry 2004, p.203/204 & p.585/586.
[141] Mac Gillavry 2004, p.204. Zie tevens het in par. 3.2.2. besproken risico van sociale exclusie.

trends die een studie van het Rathenau Instituut en TILT signaleert.[142] De studie, met de veelzeggende titel "van privacyparadijs tot controlestaat?", gaat in op de cumulatieve effecten van de veiligheidsmaatregelen in het kader van misdaad- en terreurbestrijding in de afgelopen decennia en de gevolgen daarvan voor het recht op privacy. De algemene conclusie is dat de impact van afzonderlijke maatregelen door de samenhang van die maatregelen versterkt wordt, met drastische gevolgen voor het recht op privacy.[143] In het voorgaande is dit onder meer duidelijk geworden middels de samenhang tussen de Wet vorderen gegevens telecommunicatie en de Wet computercriminaliteit II: de laatste wet brengt een aantal aan computercriminaliteit gerelateerde delicten binnen de vorderingsbevoegdheid van de Officier van Justitie, waardoor hij zich ook toegang kan verschaffen tot de telecommunicatiegegevens van de bij de van een computerdelict verdachte betrokken personen. In het vervolg van dit hoofdstuk wordt bezien hoe het Nederlandse implementatievoorstel van de dataretentierichtlijn past binnen de gesignaleerde trends en wat de mogelijke cumulatieve effecten van het voorstel en de geldende regulering van toegang tot telecommunicatiegegevens zouden kunnen impliceren.

## 2.3. Wet bewaarplicht telecommunicatiegegevens

De Wet bewaarplicht telecommunicatiegegevens[144] strekt tot wijziging van de Telecommunicatiewet en implementatie van de dataretentierichtlijn. Nu de toezegging van de Minister om de termijn voor internetgegevens terug te brengen tot zes maanden in een aparte reparatiewet zal worden voorgesteld, gaat het vervolg van deze paragraaf nog uit van de zojuist aangenomen wet, waarin de bewaartermijn voor zowel telefonie- als internetgegevens is gesteld op twaalf maanden. Zoals in de inleiding is besproken is het namelijk niet gegarandeerd dat de Tweede Kamer deze reparatiewet zondermeer zal aannemen.[145] Aangezien de wet nog niet gepubliceerd is, wordt in het vervolg nog de term 'wetsvoorstel' gehanteerd.

De totstandkoming en kernelementen van deze controversiële richtlijn werden in hoofdstuk 1 al besproken, in het hiernavolgende staan allereerst de hoofdpunten van het wetsvoorstel en vervolgens de consequenties voor de beschikbaarheid van en de toegang tot telecommunicatiegegevens voor opsporingsdiensten centraal. Geleidelijk zal blijken dat de beschikbaarheid en toegang niet los van elkaar opereren, zoals in de wet en de behandeling daarvan gesuggereerd wordt, maar interdependente begrippen zijn. Hierop wordt in par. 2.4. ingegaan.

---

[142] Rathenau/TILT 2007, p.10. De overige drie gesignaleerde ontwikkelingen zijn: I) "Opsporingsdiensten krijgen, zowel juridisch als technologisch, steeds meer mogelijkheden om (zelfstandig) onderzoek te verrichten." II) "Opsporingsdiensten hebben in toenemende mate toegang tot informatie van overige (semi-)overheidsdiensten die voor andere dan opsporingsdoeleinden is verzameld."

[143] Rathenau/TILT 2007, p.37.

[144] "Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens)", *Kamerstukken*, 31145.

[145] Zoals ook verwoord door GroenLinks-senator Strik, te lezen in het stenogram van de plenaire behandeling van wetsvoorstel 31 145 op 7 juli 2009, p.25, te raadplegen via: <http://www.eerstekamer.nl/behandeling/20090707/stenogram/f=y.pdf> [geraadpleegd juli 2009].

### 2.3.1. Hoofdpunten van het Wetsvoorstel[146]

Het wetsvoorstel strekt met name tot wijziging van hfd. 13 Tw, dat niet langer de titel «bevoegd aftappen» zal dragen, maar «bevoegd aftappen en toepassing van andere bevoegdheden op grond van het wetboek van strafvordering en de wet op de inlichtingen en veiligheidsdiensten 2002 in verband met telecommunicatie». Centraal staat de verplichting voor aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten telecommunicatiegegevens te bewaren gedurende twaalf maanden ex art. 13.2a wetsvoorstel. Ingevolge lid 1 sub a wordt in het voorstel geen onderscheid gemaakt tussen verkeers- en locatiegegevens. Lid 2 vermeldt de ratio achter de wet, te weten het bewaren van telecommunicatiegegevens ten behoeve van het opsporen van ernstige misdrijven. Lid 3 regelt de termijn, die na het Amendement Anker teruggebracht werd van 18 naar 12 maanden.[147] Het Amendement Pechtold,[148] dat in lijn met de adviezen van het de art. 29 Werkgroep en het CBP drie dagen na de aankondiging van het wetsvoorstel beoogde de termijn terug te brengen tot 6 maanden, werd niet aangenomen. Art. 13.10 wetsvoorstel verwijst naar de bijlage, die onderdeel zal gaan uitmaken van art. 13.2a Tw. In die bijlage staan de gegevens vermeldt die aanbieders moeten bewaren.

In art. 13.2b wetsvoorstel wordt art. 126hh Sv toegevoegd als grondslag van een vordering van opsporingsautoriteiten waar aanbieders aan moeten voldoen. Het Amendement Pechtold/Azough,[149] dat deze toevoeging trachtte te pareren, is niet aangenomen. Dientengevolge bevat het voorstel een expliciete grondslag voor datamining met betrekking tot de krachtens het voorstel verplicht bewaarde telecommunicatiegegevens.

Art. 13.4 wetsvoorstel gebiedt aanbieders onverwijld te voldoen aan een vordering op grond van art. 126n, 126na, 126u, 126ua dan wel een verzoek op grond van art. 28 Wiv tot verstrekking van telecommunicatiegegevens. De medewerkingverplichting van aanbieders blijft met het wetsvoorstel gehandhaafd. Art. 13.5 wetsvoorstel regelt de verplichting voor aanbieders tot geheimhouding en beveiliging van de gegevens tegen kennisneming van onbevoegden.

Op grond van art. 13.9 wetsvoorstel moet de Minister van Justitie elke drie jaar een evaluatieverslag naar de Kamer sturen, waarin doeltreffendheid en de effecten van de bewaarplicht besproken worden. Het amendement Anker bracht de evaluatietermijn terug van vijf jaar, die het Kabinet voor ogen had.[150]

### 2.3.2. Implicaties voor de beschikbaarheid van telecommunicatiegegevens

De beschikbaarheid van telecommunicatiegegevens komt in een geheel nieuwe situatie terecht. Hieraan zijn allerlei consequenties voor in Nederland opererende aanbieders verbonden, zoals investeringskosten van 75 miljoen euro in de eerste vijf jaar en jaarlijkse exploitatiekosten van circa 20

[146] *Kamerstukken I*, 2008-2009, 31 145, nr. A (GEWIJZIGD VOORSTEL VAN WET).
[147] *Kamerstukken II*, 2007-2008, 31 145, nr. 14.
[148] *Kamerstukken II*, 2007-2008, 31 145, nr. 6.
[149] *Kamerstukken II*, 2007-2008, 31 145, nr. 13.
[150] *Kamerstukken II*, 2007-2008, 31 145, nr. 14.

miljoen euro.[151] In sommige lidstaten worden deze kosten vergoed, in Nederland dienen aanbieders de kosten door te berekenen aan de consument.[152] Al zijn de financiële gevolgen voor het bedrijfsleven aanzienlijk, richt het vervolg van dit hoofdstuk zich op de implicaties van het wetsvoorstel voor de beschikbaarheid van en toegang tot telecommunicatiegegevens.

Allereerst wordt dataretentie met het wetsvoorstel de nieuwe hoofdregel voor de regulering van de beschikbaarheid van telecommunicatiegegevens. Voortaan zijn de gegevens voor een gegarandeerde periode van 12 maanden beschikbaar. Daarnaast wordt geen onderscheid gemaakt tussen verdachte of niet-verdachte burgers. Van alle burgers worden alle gegevens, die binnen een categorie zoals opgenomen in de bijlage vallen, opgeslagen ex 13.2a lid 2 wetsvoorstel.[153] Locatiegegevens zijn nu nog onderworpen aan veel strengere eisen voor verdere opslag ex 11.5a lid 1 Tw, maar voor de bewaarplicht geldt dit onderscheid niet langer. Met het wegvallen van onderscheid kan dus geconstateerd worden dat het een algehele, algemene bewaarplicht betreft. Bovendien gaat het Nederlandse wetsvoorstel verder dan de verplichtingen uit art. 5 dataretentierichtlijn, blijkens overweging 12 van de dataretentierichtlijn en art. 15 lid 1 E-privacyrichtlijn een minimumset van telecommunicatiegegevens. Lidstaten kunnen daarom categorieën gegevens toevoegen, en de Nederlandse wetgever geeft aan de sterke wens van behoeftestellers om de bewaring van locatiegegevens tijdens mobiele telefonie verplicht te stellen gevolg.[154] Saillant detail is dat deze gegevens na aandringen van het Europees Parlement niet zijn opgenomen in de richtlijn – een van de weinige wapenfeiten van het Parlement in de onderhandelingen – omdat ze een te vergaande inbreuk op de persoonlijke levenssfeer van gebruikers zouden maken.[155] Al met al is beschikbaarheid voor opsporingsdoeleinden door dataretentie voor een langere tijd, van meer soorten telecommunicatiegegevens en van alle gebruikers dus gegarandeerd. Het is trouwens maar de vraag of de AIVD en MIVD een bewaarplicht nodig hadden om deze mate van beschikbaarheid te garanderen. Naast de interceptiebevoegdheid van art. 24 Wiv, sprongen inlichtingendiensten in de afgelopen jaren niet bepaald nauwkeuriger om met hun wettelijke bevoegdheden.[156] De samenleving zal echter nooit inzicht krijgen in dergelijke "staatsgeheimen".[157]

Op de tweede plaats kondigt het Kabinet nu al aan dat de verplichtingen uit zowel dataretentierichtlijn als wetsvoorstel de komende jaren niet vastliggen maar aan verandering

---

[151] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.27 onder verwijzing naar het rapport van Verdonck, Klooster & Associates dat onderzoek deed naar dit specifieke vraagstuk; *Kamerstukken I*, 2008-2009, 31 145, nr. D, tijdens de recentere expertbijeenkomst zijn de bevindingen door de experts herhaald.

[152] Van Hoboken 2009. Meer informatie over de situatie in verschillende lidstaten is te vinden via *Kamerstukken I*, 2007-2008, 31 145, nr. C, p.28. Overigens betaalt de burger linksom (als belastingbetaler) of rechtsom (als consument) de rekening.

[153] Aldus worden met het wetsvoorstel de gegevens van niet-verdachte burgers bewaard, waar zij met de Wet vorderen gegevens telecommunicatie al van niet-verdachte burgers gevorderd konden worden. Dit is een voorbeeld van een cumulatief effect van verschillende wetgevingsmaatregelen zoals besproken in par. 2.2.3. Bij dit specifieke cumulatieve effect zal in de scriptie nog enkele malen expliciet worden stilgestaan.

[154] *Kamerstukken I*, 2007-2008, 31 145, nr. A, p.7, art. A sub e vijfde streepje. Deze gegevens zijn wenselijk voor de identificatie van prepaid bellers.

[155] Koops & Buruma 2007, p.88/89; Zwenne & Schmidt 2008, p.281.

[156] In 2005 wijzen Zwenne & Schmidt al op het dan sinds geruime tijd bekend zijn van een aantal programma's waarbinnen telecommunicatiegegevens door inlichtingendiensten in binnen- en buitenland worden opgevangen en (automatisch) geanalyseerd met het oog op terrorismebestrijding, zoals Echelon en het verzamelen van telecommunicatiegegevens van miljoenen Amerikanen door de Amerikaanse inlichtingendienst NSA. Zwenne & Schmidt 2005, p.298. *Kamerstukken II*, 2004-2005, 26 671, nr. 10, p.7; zie uitgebreid *Kamerstukken II 2001–2002*, 27 591, nr. 4; Rathenau/TILT 2007, p.57.

[157] *Kamerstukken II*, 2006-2007, 31 145, nr.5, p.4.

onderhevig zullen zijn. Regels over bewaartermijnen, de categorieën te bewaren gegevens en de toepasselijkheid van de bewaarplicht op nieuwe vormen van telecommunicatiediensten (zoals de webdiensten social networking, chatten, VOIP en webmail) mogelijk zullen worden aangepast aan de technologische- en juridische status quo. De Minister heeft nu al herhaaldelijk aangegeven de buiten het wetsvoorstel vallende telecommunicatiegegevens alsnog via andere wegen voor opsporingsonderzoek beschikbaar te maken,[158] en daarnaast de bewaartermijn te willen verhogen.[159] De evaluatie op uiterlijk 15 september 2010 door de Commissie ex art. 14 dataretentierichtlijn wordt genoemd als een mogelijk moment om dat te doen. De evaluatie van het wetsvoorstel na drie jaren op grond van art. 13.9 wetsvoorstel vormt een volgende gelegenheid om met soortgelijke maatregelen op nationale schaal te komen.[160] Desnoods biedt een beroep op de algemene uitzondering van art. 13 privacyrichtlijn perspectief.[161] Er lijkt de komende jaren hoe dan ook het een en ander te zullen veranderen aan de nu in de dataretentierichtlijn en het wetsvoorstel opgetekende verplichtingen.

Een derde implicatie is van meer fundamentele aard: opsporingsbelangen beheersen in de toekomst de regulering van de beschikbaarheid van telecommunicatiegegevens. Het beginsel van doelbinding van art. 6 jo. art. 9 E-privacyrichtlijn – anonimiseren nadat de verbinding is verbroken – wordt immers doorbroken, ten behoeve van het opsporingsbelang. De insteek was het beschermen van de persoonlijke levenssfeer tegen te lange opslag door de aanbieders. Daarnaast zorgde kostenbeheersing ervoor dat aanbieders telecommunicatiegegevens niet langer dan in het kader van hun bedrijfsvoering strikt noodzakelijk opslaan.[162] In essentie is dataretentie dus van strafprocesrechtelijke aard. Het directe verband tussen de termijn van de beschikbaarheid en het nut voor opsporingsonderzoek wordt ook onderkend door het Kabinet, dat aldus de strafprocesrechtelijke aard van de hernieuwde beschikbaarheid bevestigt.[163] Dit vormt een omslagpunt in de regulering van de beschikbaarheid van telecommunicatiegegevens: in de toekomst wordt deze beheerst door de afweging tussen grondrechten van burgers en het opsporingsbelang. Deze constatering heeft gevolgen voor de beoordeling van de verenigbaarheid van de hernieuwde regulering van beschikbaarheid met art. 8 EVRM, zoals in hoofdstuk 3 duidelijk zal worden.[164]

### 2.3.3. Implicaties voor de toegang tot telecommunicatiegegevens

Volgens het Kabinet zijn aan het wetsvoorstel geen implicaties voor toegang tot telecommunicatiegegevens verbonden.[165] Het voorstel zou er daarom "niet toe leiden dat er verdergaande inbreuken worden gemaakt op de rechten van burgers."[166] Waar de tweede stelling in hoofdstuk 3 behandeld zal worden, is de eerste stelling van het Kabinet onderwerp van deze paragraaf, waarin betoogd wordt dat het wetsvoorstel wel degelijk implicaties heeft voor de toegangsbevoegdheden van opsporingsdiensten.

---

[158] *Kamerstukken I*, 2007-2008, 31 145, nr. C, p.30.
[159] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.24.
[160] *Kamerstukken I*, 2008-2009, 31 145, nr. E, p.4/5.
[161] Van Hoboken 2009.
[162] *Kamerstukken I*, 2007-2008, 31 145, nr. C, p.15.
[163] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.7.
[164] Zie par. 3.2.3. & par. 3.3.1.
[165] *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.11.
[166] *Kamerstukken II*, 2007-2008, 31 145, nr.9, p.34; *Kamerstukken II*, 2008-2009, 31 145, nr. C, p.7 & p.26.

Dit is op de eerste plaats het geval, omdat de strafvorderlijke toegangsbevoegdheden van opsporingsdiensten door de toegenomen beschikbaarheid een ruimer toepassingsbereik krijgen.[167] Met betrekking tot de lengte van die beschikbaarheid, bevestigt de Minister het bestaan van een direct verband tussen de termijn van de beschikbaarheid en het nut voor opsporingsonderzoek.[168] Nu die beschikbaarheid met het wetsvoorstel voor een jaar gegarandeerd wordt, neemt de informatiepositie van opsporingsautoriteiten toe: voortaan kan de Officier van Justitie alle verkeersgegevens vorderen die een aanbieder in de afgelopen twaalf maanden heeft gegenereerd.[169] Artt. 126n/126u/126zh Sv krijgen derhalve een verstrekkend toepassingsbereik. Ook al voorziet het wetsvoorstel niet in concrete wijzigingen van de Wet vorderen gegevens telecommunicatie, is een cumulatief effect van dataretentie dat de met deze wet verruimde opsporingsbevoegdheden de facto in waarde toenemen.[170]

Behalve de samenhang met de Wet vorderen gegevens telecommunicatie, zijn de cumulatieve effecten van het wetsvoorstel met de andere vorderingsbevoegdheden in het Wetboek van Strafvordering onderbelicht. Er komen bijvoorbeeld veel meer telecommunicatiegegevens beschikbaar voor het voorbereidend onderzoek ex art. 126gg Sv, opgedragen door de Officier van Justitie en uitgevoerd door de opsporingsambtenaar en voor datamining ex art. 126hh Sv. Het Wetboek van Strafvordering bevat ongetwijfeld nog veel meer van de beschikbaarheid van telecommunicatiegegevens afhankelijke artikelen, die op deze indirecte wijze van veel groter betekenis worden voor opsporingsdiensten. Dit geldt in gelijke zin voor toekomstige strafvorderlijke bevoegdheden zoals het in behandeling zijnde nieuwe art. 29b Wiv.[171] Het inzicht in de cumulatieve effecten van het wetsvoorstel is dan ook een belangrijk punt voor vervolgonderzoek op deze scriptie.[172] Alles in ogenschouw nemende, zijn verdergaande inbreuken op de rechten van burgers waarschijnlijk, alleen al met de door de Minister aangekondigde toename van het aantal toegangsverzoeken tot telecommunicatiegegevens in de komende jaren.[173] Hier wordt in hoofdstuk 3 verdere aandacht aan besteed.

---

[167] Teunissen 2009.
[168] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.7.
[169] *Kamerstukken II*, 2001-2002, 28 059, nr. 3 (MvT), p.8/9.
[170] Zie par. 2.2.2: sinds de Wet vorderen gegevens telecommunicatie kunnen bijvoorbeeld ook telecommunicatiegegevens van niet-verdachte burgers gevorderd worden nu betrokkenheid bij de verdachte voldoende is. Dit leidt ertoe dat niet alleen van de verdachte, maar ook van niet-verdachte burgers meerdere categorieën telecommunicatiegegevens, van een langere periode toegankelijk zijn voor opsporingsdiensten.
[171] *Kamerstukken I & II*, 30 553. Het betreft hier het verzoek tot verstrekking van (delen van) een (geautomatiseerd) gegevensbestand bij aanbieder. De hiermee verkregen gegevens worden door de AIVD en MIVD gebruikt voor datamining en -profiling. Bij de bespreking van de implicaties van de nieuwe bevoegdheden wordt in de Memorie van Toelichting van 18 mei 2006 één regel gewijd aan de beschikbaarheid van telecommunicatiegegevens en de implicaties van de toegangsbevoegdheid: "bij dit alles geldt uiteraard dat de verplichting tot verstrekking slechts ziet op de gegevens die men in het kader van de eigen bedrijfsvoering voorhanden heeft en waarbij tevens in beginsel wordt aangesloten bij de wijze waarop deze door de bedrijven worden verwerkt; men heeft noch een bewaarplicht noch een vergaarplicht." *Kamerstukken II*, 2005-2006, 30 553, nr. 3 (MvT), p.11/12. Na een vraag van de PvdA-fractie komt het Kabinet in een latere reactie kort terug op de zojuist in werking getreden dataretentierichtlijn: de vorderingsbevoegdheid "kan dus ook zien op (delen van) geautomatiseerde gegevensbestanden met verkeers- en locatiegegevens als bedoeld in de dataretentierichtlijn." *Kamerstukken II*, 2005-2006, 30 553, nr. 7, p.12. Het is daarom des te opvallender hoezeer de parlementaire behandeling van dit voorstel eerder begon, vertraagd werd en sinds de behandeling van Wetsvoorstel Wet bewaarplicht telecommunicatiegegevens hiermee gelijke tred houdt.
[172] Zie par. 5.3.
[173] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.14. Dat ruimere opsporingsbevoegdheden leiden tot een toename aan toegangsverzoeken werd al duidelijk met de explosieve groei (jaarlijkse toename van 24,7%) van toegangsverzoeken door opsporingsambtenaren na de inwerkingtreding van de Wet vorderen gegevens telecommunicatie. Zie par. 2.2.2.

Op de tweede plaats kan worden vastgesteld, dat de toegang tot verplicht bewaarde telecommunicatiegegevens niet beperkt is tot 'ernstige misdrijven', terwijl het Kabinet hier wel van uitgaat.[174] Het Kabinet zoekt voor de duiding van 'ernstige misdrijven' aansluiting bij art. 67 lid 1 Sv, het artikel dat delicten bevat waarvoor voorlopige hechtenis is toegestaan.[175] Maar zoals in par. 2.2.2. al aan de orde kwam, wordt in sub b en met name in sub c van art. 67 lid 1 Sv verwezen naar een niet geringe hoeveelheid relatief lichte delicten waarvoor het predicaat 'ernstige misdrijven' te zwaar is – zoals ook al in de Tweede Kamer en door Zwenne & Schmidt is opgemerkt.[176] Nog belangrijker is de vaststelling, dat recentelijk een aantal relatief lichte delicten aan zowel sub b als sub c van art. 67 lid 1 Sv zijn toegevoegd en zeven wetsvoorstellen daarvoor momenteel in behandeling zijn.[177] Het Wetboek van Strafvordering heeft het begrip 'ernstige misdrijven' niet gedefinieerd, daarentegen heeft het een bijzonder dynamisch karakter in de Nederlandse rechtsorde. Nu is het zo dat lidstaten met de in par. 1.5. behandelde uitspraak een eigen bevoegdheid om dit soort maatregelen te nemen op basis van de dataretentierichtlijn, aangezien de dataretentierichtlijn de activiteiten van de overheid op strafvorderlijk gebied niet regelt.[178] Toch staat deze implicatie van dataretentie op de toegangsbevoegdheden tot de verplicht bewaarde telecommunicatiegegevens in contrast met het voorstel van het Europees Parlement om de toegang te beperken tot de 24 ernstige misdrijven die in art. 2 lid 2 Aanhoudingsbevel staan opgesomd[179] of de gedetailleerde catalogus van 'schwere Straftaten' in par. 100a lid 2 van het Duitse Wetboek van Strafvordering.[180] In tegenstelling tot de gemeenschapswetgever, kon de Nederlandse wetgever deze toegang evenals de Duitse wetgever beperken en een hogere drempel voor de toegang tot telecommunicatiegegevens construeren. Dat de wetgever dit niet heeft gedaan, brengt consequenties met zich mee voor de verenigbaarheid van het wetsvoorstel met art. 8 EVRM.[181]

Speciale aandacht dient uit te gaan naar de vorderingsbevoegdheden van gebruiksgegevens door opsporingsambtenaren, met tussenkomst van het CIOT. Het CIOT slaat de door aanbieders aangemaakte gebruiksgegevens niet op ingevolge art. 7 lid 2 Besluit verstrekking gegevens telecommunicatie. Vooralsnog hebben opsporingsambtenaren alleen toegang tot actuele gebruiksgegevens. De stap naar inzage in gebruiksgegevens van de afgelopen 12 maanden is echter klein, omdat art. 13.4 wetsvoorstel deze mogelijkheid schept in een wet in formele zin en de informatie waardevol kan zijn voor de opsporingsdiensten. Met een eenvoudige wijziging van art. 7 lid 2 van het Besluit zal het CIOT niet alleen actuele, maar alle verplicht bewaarde gebruiksgegevens kunnen opslaan. Deze vorderingsbevoegdheid bestaat overigens al voor 'normale' persoonsgegevens op grond van art. 126nc lid 1 Sv, zij het dat voor deze gegevens uiteraard geen bewaarplicht geldt. Bovendien hanteren opsporingsambtenaren in de praktijk vanwege de complexiteit van het strafprocesrecht een verkeerde grondslag voor de vordering van persoonsgegevens, terwijl de houders deze gegevens op

[174] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.14.
[175] "Aldus wordt bij de kwalificatie «ernstig» gedacht aan één of meer categorieën van delicten, zoals de delicten waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld *en de andere, in artikel 67, eerste lid, van het Wetboek van Strafvordering aangewezen misdrijven*." *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.4 (eigen cursivering).
[176] *Hand. II*, 2006-2007, 31 145, nr. 83, p. 5813; Zwenne & Schmidt 2008, p.283.
[177] Bijvoorbeeld de Wet kraken en leegstand (31 560, nr. 2) die derhalve de betrokkene bij een van het kraken van een pand verdachte persoon binnen de vorderingsbevoegdheid van de OvJ brengt.
[178] HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 86-92.
[179] Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002, PB EG L 190/01.
[180] Vergelijk par. 100g van het Duitse Wetboek van Strafvordering, in te zien via <http://bundesrecht.juris.de/stpo/__100a.html> [geraadpleegd juli 2009].
[181] Zie par. 3.3.1. & par. 3.3.2.3.

verzoek toch verstrekken.[182] Op basis van deze overwegingen baseer ik mijn verwachting dat de mogelijkheid dat opsporingsambtenaren toegang zullen krijgen tot verplicht bewaarde gebruiksgegevens – betrokkenheid bij de verdachte van 'een misdrijf' is hier het criterium – zich in de toekomst zal verwezenlijken.

### 2.3.4. Voortzetting van de ontwikkelingen in de strafvorderlijke bevoegdheden

In par. 2.2.3. werden vier trends gesignaleerd in de ontwikkeling van de strafvorderlijke bevoegdheden sinds de Commissie-Mevis, die een uitdijing van het opsporingsarsenaal illustreren.[183] Het voorstel past in deze trends, en behelst aldus een voortzetting van de ontwikkelingen sinds de Commissie-Mevis. De *informatiepositie* van opsporingsdiensten neemt toe, de *reikwijdte* van opsporingsbevoegdheden wordt groter en er is sprake van een impliciete uitbreiding van het toepassingsbereik van de *bevoegdheden*.

Dat de *samenwerking tussen de overheid en aanbieders* met dataretentie toeneemt, wordt als zodanig ook onderkend in de parlementaire behandeling.[184] Maar in feite is hier niet alleen een voortzetting van een ontwikkeling aan de orde, maar komt de samenwerking met dataretentie in een geheel nieuw licht te staan. Met dataretentie hebben opsporingsinstanties bovenop de deconstructie van toegangsbelemmeringen, tevens een belangrijke stap gezet richting het wegnemen van de feitelijke beschikbaarheidsbelemmeringen. Art. 1 van de dataretentierichtlijn laat geen twijfel bestaan over de intenties: de maatregel beoogt, middels het inschakelen van het bedrijfsleven, te "*garanderen* dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit."[185] Deze fundamentele stap die met dataretentie gezet wordt, moet niet alleen op zichzelf maar in relatie met zowel andere maatregelen als in temporeel perspectief beschouwd worden: het cumulatieve effect van dataretentie is het bijdragen aan het in een paar jaar tijd daadwerkelijk afbreken van alle barrières voor opsporingsdiensten, die vrijwel alle communicatieve handelingen van burgers gedurende een zekere periode kunnen traceren.

## *2.4. Interdependentie beschikbaarheid en toegang*

In par. 2.3.3. is al gewezen op de samenhang tussen het wetsvoorstel en de vorderingsbevoegdheden uit het Wetboek van Strafvordering, in het bijzonder de Wet vorderen gegevens telecommunicatie, alsmede op de cumulatieve effecten van de verschillende maatregelen.[186] Dit brengt ons op de in par. 1.5. uiteengezette formele scheiding van beschikbaarheid en toegang in de dataretentierichtlijn, die door het Hof van Justitie is bekrachtigd. De Minister beziet de beschikbaarheid van telecommunicatiegegevens

[182] Mac Gillavry 2004, p.203-204. Aanbieders en opsporingsinstanties blijken in de praktijk geen tegenstrijdige maar gelijke belangen te hebben bij verstrekking. Zie par. 2.1.
[183] Deze trends komen overeen met de bevindingen van de studie van het Rathenau Instituut en TILT, zie Rathenau/TILT 2007, p.10.
[184] o.m. *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.16. In gelijke zin Birnhack & Elkin-Koren 2003, p.37.
[185] Art. 1 Dataretentierichtlijn; *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.1.
[186] Rathenau/TILT 2007, p.7.

eveneens los van de strafvorderlijke bevoegdheden,[187] al bestaat in de Nederlandse rechtsorde het Europees recht van de pijlers uiteraard niet. Waar de gemeenschapswetgever wellicht constitutionele problemen voorzag met het stellen van regels voor de toegang tot telecommunicatiegegevens in de richtlijn, zitten dergelijke vraagstukken de nationale wetgever geenszins dwars.

Een synthese van de implicaties van het wetsvoorstel voor zowel beschikbaarheid van als toegang tot telecommunicatiegegevens leert dat de twee begrippen interdependent zijn. De grens tussen de door het strafprocesrecht beheerste regulering van de toegang en de vroeger van bedrijfsoverwegingen afhankelijke beschikbaarheid verdwijnt, nu die afhankelijkheid met dataretentie wordt weggenomen om beschikbaarheid voor opsporing te garanderen. De strafprocesrechtelijke aard van dataretentie, het ruimer worden van het toepassingsbereik van zowel huidige als toekomstige opsporingsbevoegdheden, de toegenomen informatiepositie van opsporingsdiensten door toegenomen beschikbaarheid en de intensieve samenwerking tussen het bedrijfsleven en de opsporingsdiensten vormen een bewijs hiervan. Er is met andere woorden sprake van een wederzijdse afhankelijkheid van beschikbaarheid en toegang, of beter geformuleerd een onafscheidelijke samenhang. De interdependentie van beschikbaarheid en toegang laat zich overtuigend aantonen met de opmerking van de Minister, dat er geen alternatieven bestaan om telecommunicatiegegevens op deze schaal voor opsporingsonderzoek beschikbaar te krijgen.[188] Als behoeftestellers toegang willen hebben tot vrijwel alle telecommunicatiegegevens van alle burgers gedurende een zekere periode, kan dit momenteel in Europa alleen via een algemene bewaarplicht gefaciliteerd worden.[189]

De logische consequentie van de interdependentie van beschikbaarheid en toegang is dat de regulering ervan in samenhang dient te geschieden. Dit is in lijn met de in par. 1.5. uiteengezette wens van de A-G in zaak C-301/06, die aangeeft in een enkele handeling "de coherentie tussen de twee elementen" te willen "verzekeren."[190] Het Europees Hof voor de Rechten van de Mens laat deze samenhang in het kader van de bescherming van art. 8 EVRM meewegen, net als het BVerfG.[191] Tijdens de parlementaire behandeling heeft de regulering van de toegang tot telecommunicatiegegevens echter geen rol van betekenis gespeeld. Op basis van Europees constitutioneel recht lijkt hier in eerste opzicht een juiste keuze, maar in hoofdstuk 3 zal blijken dat de verenigbaarheid van het wetsvoorstel met art. 8 EVRM hieronder te lijden heeft.[192]

## 2.5. Conclusie

Waar in de huidige situatie nog sprake is van het uitgangspunt van anonimiseren of verwijderen van telecommunicatiegegevens, gebiedt het wetsvoorstel om vrijwel al het telecommunicatieverkeer met

[187] Recent nog expliciet verwoord in de nadere Memorie van Toelichting: *Kamerstukken II*, 2008-2009, 31 145, nr. F, p.6. Daarnaast in: *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.10; *Kamerstukken II*, 2007-2008, 31 145, nr.9, p.34.
[188] *Kamerstukken II*, 2006-2007, 31 145, nr.9, p.19.
[189] In extremere zin behoort het afschaffen van de in art. 6 jo. art. 9 E-privacyrichtlijn neergelegde hoofdregels voor de bescherming van de persoonlijke levenssfeer in de Europese telecommunicatiesector op de langere termijn tot de mogelijkheden – naar Amerikaans model.
[190] HvJEG 14 oktober 2008, nr. C-301/06, Conclusie A-G Y. Bot, nr. 108.
[191] EHRM S. and Marper v. The United Kingdom, nr. 99; Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 149; zie tevens Groothuis 2006, p.808.
[192] Zie o.m. Van Hoboken 2009.

betrekking tot alle gebruikers voor twaalf maanden te bewaren, teneinde te garanderen dat de gegevens beschikbaar zijn voor de opsporing. Meer categorieën gegevens, voor langere tijd, van iedereen. Daarmee past het wetsvoorstel bewaarplicht telecommunicatiegegevens in een ontwikkeling sinds het rapport van de Commissie-Mevis, waarin een uitdijing van het opsporingarsenaal van opsporingsautoriteiten centraal staat. In het wetsvoorstel manifesteert zich een forse uitbreiding van de informatiepositie en het daadwerkelijke toepassingsbereik van opsporingsbevoegdheden.

Tegelijkertijd behelst het wetsvoorstel een fundamenteel nieuwe situatie voor de regulering van beschikbaarheid en toegang, omdat de beschikbaarheid van telecommunicatiegegevens voor andere dan bedrijfsdoeleinden voortaan beheerst wordt door het opsporingsbelang. Het Kabinetsstandpunt dat het bewaren van telecommunicatiegegevens onderscheiden moet worden van de toegangsbevoegdheden van opsporingsinstanties houdt met dataretentie geen stand. Beschikbaarheid en toegang zijn interdependent, met andere woorden bestaat er een onafscheidelijke samenhang tussen de twee begrippen. Opsporingsdiensten zijn met het intreden van de bewaarplicht niet langer afhankelijk van de telecommunicatiegegevens die in de maatschappij voorhanden zijn, maar hebben zich de beschikbaarheid van de gegevens toegeëigend. Het strafprocesrecht maakt voortaan een integraal onderdeel uit van de regulering van de beschikbaarheid van telecommunicatiegegevens, die in samenhang en niet los van toegang tot telecommunicatiegegevens gereguleerd dient te worden. Gezien de door de Minister aangekondigde uitbreidingen van de dataretentieverplichtingen bij toekomstige evaluaties en de reikwijdte van het wetsvoorstel is dit een belangrijke constatering.

Om de uitwerking van de interdependentie in concrete zin te onderzoeken, zijn een aantal specifieke ontwikkelingen uitgelicht – zoals het niet beperkt zijn van de toegang tot verplicht bewaarde telecommunicatiegegevens tot zwaarwegende gevallen vanwege de verwijzing in art. 126n lid 1 Sv naar art. 67 lid 1 Sv. Deze ontwikkelingen zijn van belang voor de analyse van de verenigbaarheid met art. 8 EVRM en zullen derhalve in het volgende hoofdstuk uitgebreid ter sprake komen. In algemene zin kan geconcludeerd worden dat uit de optelsom van het wetsvoorstel en de ontwikkelingen in de strafvorderlijke bevoegdheden sinds de Commissie-Mevis een cumulatief effect volgt: zowel feitelijke toegangs- als beschikbaarheidsbelemmeringen worden geleidelijk weggenomen. Dit lijkt onverenigbaar met art. 4 dataretentierichtlijn, maar de uitspraak van het Hof inzake de rechtsgrondslag van de dataretentierichtlijn bepaalde dat de nationale wetgever geen rekenschap hoeft te geven van de richtlijn als het gaat om de regulering van de toegang tot telecommunicatiegegevens.

Uit deze conclusie volgt de Nederlandse stand van zaken met betrekking tot de regulering van de beschikbaarheid van, en toegang tot telecommunicatiegegevens in het kader van de opsporing van strafbare feiten. De invloed van de nieuwe wet op de toegang, en vice versa, blijkt aanzienlijk. In het volgende hoofdstuk wordt bezien of de bewaarplicht en de daarmee onlosmakelijk verbonden toegangsbevoegdheden verenigbaar zijn met de vereisten van art. 8 EVRM, waarin het fundamentele recht op de eerbiediging van de persoonlijke levenssfeer van de burger is verankerd.

# 3. HET GRONDRECHTELIJKE PERSPECTIEF

In de literatuur worden drie grondrechten onderscheiden die op gespannen voet zouden staan met dataretentie, te weten de vrijheid van meningsuiting (art. 10 EVRM), het recht op eigendom (art. 1 Eerste protocol EVRM) en het recht op privacy (art. 8 EVRM).[193] Deze scriptie spitst zich toe op de vraag hoe dataretentieverplichtingen zich verhouden met de bescherming van de persoonlijke levenssfeer van de gebruikers van telecommunicatiediensten.[194] Zoals aangekondigd in de inleiding van deze scriptie, lijkt recente jurisprudentie van het EHRM hierin een belangrijke rol te zullen spelen. In par. 1.5. werd al opgeworpen dat de art. 8 EVRM discussie des te relevanter is geworden, nu Hof van Justitie in de komende jaren hoogstwaarschijnlijk een standpunt zal moeten innemen.[195] Overigens komt de Nederlandse burger slechts het minimale beschermingsniveau van art. 8 EVRM toe.[196] Vanwege de techniekafhankelijke formulering van de Grondwet, vallen telecommunicatiegegevens niet binnen haar bescherming.[197]

De bevindingen van dit hoofdstuk maken het grondrechtelijke perspectief op dataretentie en de samenhang tussen dataretentiemaatregelen en de Nederlandse strafvorderlijke bevoegdheden inzichtelijk. Als de wetgever zich op een adequate wijze rekenschap geeft van het door art. 8 EVRM geboden beschermingsniveau, volgen uit de analyse concrete alternatieven op de door de wetgever voorgestelde regulering van beschikbaarheid en toegang (hoofdstuk 4).

## *3.1. De toepasselijkheid van art. 8 EVRM*

Het recht op privacy bestaat uit verschillende dimensies. In de literatuur wordt niet op eenduidige wijze invulling gegeven aan deze dimensies,[198] maar duidelijk is dat de bescherming van het recht op privacy – of de eerbiediging van de persoonlijke levenssfeer – gespecificeerd kan worden in een sociale-, een informationele- en een communicatieve dimensie, naast de fysieke omgevingen zoals het eigen huis en

[193] Breyer 2005, Amici Curiae 2008, Ekker 2008, p.234-235: Dataretentie zou om twee redenen een inbreuk maken op het recht op vrije meningsuiting. Op de eerste plaats belemmert dataretentie de vrije toegang tot communicatiemiddelen, dat wil zeggen de vrijheid om zich onbevangen te uiten via telecommunicatie. Dit hangt samen met de inbreuk op het communicatiegeheim, alsmede mogelijke 'chilling effecten' die kunnen optreden door dataretentie (zie par. 3.2.). Op de tweede plaats worden telecommunicatiediensten significant duurder, terwijl lidstaten de aanbieders daarvoor niet hoeven te compenseren. Aldus wordt telecommunicatie wellicht onbetaalbaar voor het armste deel van de bevolking, zo luidt het argument. Het achterblijven van verplichte compensatie aan het bedrijfsleven kan ook inbreuk maken op het recht op eigendom, nu dataretentie de apparatuur van aanbieders inschakelt voor opsporingsbelangen, waardoor deze apparatuur niet langer gebruikt kan worden voor de eigen bedrijfsvoering.

[194] In de literatuur komt deze vraag naar voren als de meest relevante, zie o.m. Groothuis 2006, p. 800: "EG-lidstaten dienen de dataretentierichtlijn zoveel mogelijk EVRM-conform uit te leggen, en meer in het bijzonder met inachtneming van de jurisprudentie van het EHRM inzake art. 8 EVRM."

[195] HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council, punt 57. Van Hoboken 2009: "de uitspraak van het Hof geeft daarmee aanleiding het samenspel van retentie en toegang in de nationale regelingen opnieuw te bezien in het licht van de vereisten van Artikel 8 EVRM."

[196] Groothuis komt tot de conclusie dat "de Nederlandse grondwetgever derhalve niet bij machte [is] om bescherming te bieden. (...) Het beschermingsniveau reikt in de Nederlandse rechtsorde niet verder dan het minimum, namelijk van het EVRM." Groothuis 2006, p. 804

[197] Dommering 2000, p. 103.

[198] Vgl. bijvoorbeeld Dommering 2000 en Blok 2002.

het eigen lichaam. Deze sociale-, of relationele privacy ziet op het "recht van het individu op selectieve contactlegging, met als meest extreme vorm het recht om met rust te gelaten te worden."[199] De informationele privacy behelst een recht om selectief te zijn in het gebruik van persoonsgegevens door derden.[200] Het geeft het individu "zeggenschap over verzamelde, opgeslagen en (eventueel) aan derden geopenbaarde informatie die tot de persoon herleidbaar is."[201] Het communicatiegeheim, ook wel de communicatieve privacy, dient eindgebruikers het vertrouwen te geven dat zij ongehinderd, i.e. zonder meeluisteren, gebruik kunnen maken van telecommunicatiediensten.[202] Alle drie genoemde dimensies zijn aan de orde bij de beoordeling van de verenigbaarheid van dataretentie, in samenhang met de strafvorderlijke bevoegdheden, met het recht op privacy van de Europese burger.

In Europees verband wordt deze verschillende dimensies van het recht op privacy beschermt door één artikel, namelijk art. 8 EVRM:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Waar uit de termen 'family life', 'home' en 'correspondence' min of meer een object van bescherming kan worden afgeleid, geeft de notie 'private life' niet direct duidelijkheid over de feitelijke situaties waarin deze gerespecteerd dient te worden. Jacobs & White schrijven dat er geen uitputtende definitie van de term is. In een recente uitspraak geeft het Hof, onder verwijzing naar vele eerdere uitspraken, invulling welke aspecten in ieder geval onder 'private life' wordt verstaan. Ten behoeve van de helderheid zijn deze hieronder uitgelicht:

> 66. The Court recalls that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see Pretty v. the United Kingdom, no. 2346/02, § 61, ECHR 2002-III, and Y.F. v. Turkey, no. 24209/94, § 33, ECHR 2003-IX). It can therefore embrace multiple aspects of the person's physical and social identity (see Mikulić v. Croatia, no. 53176/99, § 53, ECHR 2002-I). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see, among other authorities, Bensaid v. the United Kingdom, no. 44599/98, § 47, ECHR 2001-I with further references, and Peck v. the United Kingdom, no. 44647/98, § 57, ECHR 2003-I). Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family (see mutatis mutandis Burghartz v. Switzerland, 22 February 1994, § 24, Series A no. 280-B; and Ünal Tekeli v. Turkey, no. 29865/96, § 42, ECHR 2004-X (extracts)). Information about the person's health is an important element of private life (see Z. v. Finland, 25 February 1997, § 71, Reports of Judgments and Decisions 1997-I). The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see in particular Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz, cited above, opinion of the Commission, p. 37, § 47, and Friedl v. Austria,

[199] Dommering 2000, p. 26. Tevens E.J. Dommering, noot bij HR 9 januari 1987 (*Bespiede Bijstandsmoeder*), Computerrecht 1987-2, p.114, punt 4. Overigens bestaan ook smallere definities van dit begrip in de literatuur, waarbij de focus niet ligt op de selectieve contactlegging, maar specifieker op de intieme relaties tussen mensen, zoals de gezinsrelaties en/of de seksuele relaties, bijvoorbeeld door Verhey en Gutwirth, vgl. Blok 2002, p. 87. Dit "right to be let alone" sluit direct aan bij de in 1890 gegeven definitie van privacy door rechtsgeleerden Warren en Brandeis, die algemeen beschouwd worden als initiatiefnemers van een afzonderlijke erkenning van het recht op privacy, Blok 2002, p. 198.

[200] A. Westin, *Privacy and freedom*, Bodley Head: London 1967, p. 7: "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

[201] Dommering 2000, p.50.

[202] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 120.

> judgment of 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45). The concept of private life moreover includes elements relating to a person's right to their image (Sciacca v. Italy, no. 50774/99, § 29, ECHR 2005-I).[203]

Jacobs & White voegen aan het 'right to establish and develop relationships with other human beings' de zienswijze van het Hof in de zaak *X. v. Iceland* toe:[204]

> "privacy comprises, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality."[205]

De verwezenlijking en ontwikkeling van een eigen persoonlijkheid worden dus ook beschermd onder art. 8 EVRM. De vier verschillende sferen moeten volgens Jacobs & White overigens niet als onderscheid maar als elkaar versterkende noties beschouwd worden, omdat het Hof in Straatsburg dit ook consequent heeft gedaan.[206] Het object van de bescherming ligt niet vast, maar is zeker als breed te karakteriseren. Zo is het conceptuele onderscheid tussen 'private life' en 'correspondence' opgeheven sinds de zaak *Klass and others v. Germany* in 1978.[207]

Art. 8 EVRM beschermt een belangrijk grondrecht voor burgers in een democratische samenleving, maar zoals lid 2 illustreert is deze bescherming niet absoluut. Een inbreuk op het recht op privacy door overheidsinstanties is in principe op grond van art. 8 lid 1 EVRM niet toegestaan, tenzij deze inbreuk gerechtvaardigd kan worden omdat deze voldoet aan de criteria van art. 8 lid 2 EVRM. Deze criteria worden besproken in par. 3.3.

Telecommunicatiegegevens vallen binnen de reikwijdte van art. 8 EVRM. Correspondentie vormt sinds *Klass and others v. Germany* een integraal onderdeel van het privéleven in de jurisprudentie van het EHRM.[208] Verkeersgegevens worden sinds de zaak *Malone v. The United Kingdom* in 1984 onder de bescherming van 'correspondence' gerekend.[209] In latere jurisprudentie heeft het Hof deze overwegingen consequent herhaald,[210] recent nog in de zaak *Copland v. The United Kingdom* waarin het Hof oordeelde dat de term 'private correspondence' naast de inhoud ook de verkeersgegevens over een communicatie betreft.[211] Dat de moderne categorieën telecommunicatiegegevens zoals opgesomd in art. 5 dataretentierichtlijn ook onder de bescherming van het EVRM vallen, wordt in de parlementaire behandeling en literatuur niet betwijfeld.[212] Dit spreekt vanzelf, aangezien juist deze nieuwe categorieën telecommunicatiegegevens, zowel in kwantitatieve- als kwalitatieve zin (zie par. 3.2.1.), een completer beeld geven van de communicatieve handelingen van de betrokkene dan de conventionelere telefoniegegevens.

---

[203] EHRM S. and Marper v. The United Kingdom, nr. 66.
[204] Jacobs & White 2006, p.245.
[205] EHRM X v. Iceland, nr. 11 (eigen cursivering).
[206] Jacobs & White 2006, p.246: "private life is a broad term not susceptible to exhaustive interpretation. It matters little if an interference is considered as interference with correspondence, or with privacy, (...) since these notions should be considered together rather than in isolation."
[207] EHRM Klass and others v. Germany, nr.26; Jacobs & White 2006, p.288.
[208] EHRM Klass and others v. Germany, nr.26; Jacobs & White 2006, p.288.
[209] EHRM Malone v. United Kingdom, nr. 84.
[210] Telecommunicatiegegevens zijn een "integral element in the communications made", zie: EHRM Malone v. United Kingdom, nr. 84; EHRM Valenzuela Contreras v. Spain, nr. 47; EHRM Amann v. Switzerland, nr. 43; EHRM P.G. and J.H. v. France, nr. 42.
[211] EHRM Copland v. The United Kingdom, nr. 43.
[212] Groothuis 2006, p.799.

Het EVRM is bindend voor de Europese Unie ex art. 6 lid 2 Verdrag van de Europese Unie.[213] Daarnaast zijn zowel het algemenere recht op respect voor het privéleven (art. 7) en het recht op de bescherming van persoonlijke gegevens (art. 8) expliciet vastgelegd in de 'Charter of Fundemental Rights of the European Union' (hierna: 'Charter').[214] Uit overweging 2 van de E-privacyrichtlijn blijkt dat het pakket van de drie richtlijnen in het bijzonder aansluiting zoekt bij art. 8 van de Charter, oftewel de bescherming van persoonlijke gegevens. Dit wordt bevestigd door het Hof van Justitie in de uitspraak *Promusicae v. Telefónica*.[215] Lidstaten van de EU dienen, als verdragspartij bij het EVRM, de mensenrechtenbepalingen te respecteren bij de omzetting van de Europese richtlijnen naar nationaal recht. Daarenboven zijn alle lidstaten van de EU eveneens lid van de Raad van Europa, en hebben zij derhalve de minimale bescherming die art. 8 EVRM biedt te respecteren.[216] Al met al kan worden vastgesteld, dat zowel de dataretentierichtlijn, het wetsvoorstel als de implicaties van het wetsvoorstel op de strafvorderlijke bevoegdheden zich binnen de werkingssfeer van art. 8 EVRM bevinden.

## 3.2. De inbreuk op art. 8 lid 1 EVRM

Het is evident dat er op een bepaald moment in het hele proces van dataretentie en strafvordering aan de persoonlijke levenssfeer wordt geraakt, zo weet ook het Kabinet. Het Kabinet staat niet veel langer stil bij de aard en mate van de inbreuk, maar neemt aan dat het wetsvoorstel een inbreuk vormt op art. 8 lid 1 EVRM, om vervolgens te concluderen dat er voldoende rechtvaardiging bestaat voor de inbreuk.[217] In de literatuur wordt de duiding van de inbreuk soms ook overgeslagen,[218] evenals in de rechtspraak.[219]

Maar niet alleen de vraag 'of' er inbreuk wordt gemaakt, ook de vraag 'in hoeverre' is van belang. De rechtvaardiging van art. 8 lid 2 EVRM kan pas ten volle aan de orde komen, als het moment en de aard van de inbreuk op art. 8 lid 1 EVRM duidelijk is.[220] Helaas is dit vraagstuk in de voorgeschiedenis van de Europese bewaarplicht nooit goed aan de orde gekomen. De onderbelichting van de persoonlijke levenssfeer en de tijdsruk uitgeoefend door de Raad en de Commissie (bij de totstandkoming van art. 15 lid 1 E-privacyrichtlijn) kunnen hierin een rol gespeeld hebben.[221] Op de vooravond van de implementatie van de bewaarplicht in nationale wetgeving, is inzicht in het moment en de aard van de inbreuk des te belangrijker geworden.

---

[213] Deze bepaling luidt: "De Unie eerbiedigt de grondrechten, zoals die worden gewaarborgd door het op 4 november 1950 te Rome ondertekende Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en zoals zij uit de gemeenschappelijke constitutionele tradities van de lidstaten voortvloeien, als algemene beginselen van het Gemeenschapsrecht.." OJ 2002/C 325/01.
[214] OJ 2000/C 364/01.
[215] HvJEG 29 januari 2008, nr. C-275/06, Promusicae v. Telefónica, nr.63-64.
[216] Groothuis 2006, p.796.
[217] *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.24; *Kamerstukken II*, 2007-2008, 31 145, nr.9, p.17 & 35; *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.12; *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.7.
[218] Bignami 2007, p.242.
[219] Het EHRM besteed consequent meer aandacht aan de rechtvaardiging van een inbreuk onder art. 8 lid 2 EVRM, zie Jacobs & White 2006. p.288. Bijvoorbeeld in EHRM S. and Marper v. The United Kingdom, nrs. 84-86, waar wel aandacht wordt besteed aan de vraag of vingerafdrukken onder de bescherming van art. 8 EVRM vallen, maar niet wat nu precies de inbreuk is van het bewaren van vingerafdrukken van niet-veroordeelde burgers, oftewel hoe deze bewaring hun recht op privacy schaadt.
[220] Jacobs & White 2006. p.288.
[221] Zie par. 1.6.

Voor de helderheid van het betoog is het vraagstuk in twee subparagrafen uitgesplitst in lijn met de uitspraak van het Duitse Constitutionele Hof – het Bundesverfassungsgericht (hierna: "BVerfG") – inzake de Duitse implementatiewet van de dataretentierichtlijn. In par. 3.2.2. wordt ingegaan op de vraag of alleen al de met de dataretentierichtlijn en het wetsvoorstel geregelde verplichting om telecommunicatiegegevens te bewaren een inbreuk op art. 8 lid 1 EVRM vormt, en onderzocht wat de aard van deze inbreuk is. In par. 3.2.3. komen de hernieuwde verhouding tussen beschikbaarheid en toegang, de implicaties voor de regulering ervan zoals beschreven in hoofdstuk 2, en de specifieke consequenties voor de toegang aan de orde in het licht van art. 8 lid 1 EVRM. In deze paragrafen manifesteert zich een geleidelijke intensivering van de inbreuk op art. 8 lid 1 EVRM naarmate de tekst vordert. Daarbij dient de uitgangspositie van vandaag de dag, zoals beschreven in par. 2.2.1., steeds in het achterhoofd gehouden te worden. Maar voordat de aard van de inbreuk op art. 8 lid 1 EVRM geanalyseerd kan worden, is inzicht in de aard van de gegevens die verplicht bewaard en toegankelijk worden essentieel.

### 3.2.1. Telecommunicatiegegevens

De bewaarplicht richt zich op de telecommunicatiegegevens opgesomd in art. 5 dataretentierichtlijn en de bijlage bij het wetsvoorstel. In aanvulling op identificatie,[222] effectueert een dataset van telecommunicatiegegevens over een periode van twaalf maanden nog voordat deze gekoppeld wordt aan andere data inzicht in indringende aspecten van het privéleven, zoals communicatiepatronen, gebruikte telecommunicatiediensten en de locatie van een gebruiker op een bepaald tijdstip.[223] Telecommunicatiegegevens vormen dus een zwaardere categorie persoonsgegevens dan vingerafdrukken, die met identificerende gebruiksgegevens te vergelijken zijn. Onverwerkte telecommunicatiegegevens zijn daarmee, in tegenstelling tot de stelling van het Kabinet,[224] veelzeggend. Merkwaardig genoeg wordt dit in een ander verband door de Minister onderkend, en ontkracht hij zijn eigen stelling – dat telecommunicatiegegevens op zichzelf niet veelzeggend zouden zijn – door de bewaarplicht te vergelijken met het bewaren van een gespecificeerde rekening.[225] Behalve dat uit deze rekening veel informatie gedestilleerd kan worden is dit een onnauwkeurige vergelijking, aangezien de gespecificeerde rekening veel minder informatie bevat dan de verplicht bewaarde gegevens op grond van de bijlage bij het wetsvoorstel, bijvoorbeeld geen locatiegegevens.[226]

De aard van de inbreuk op art. 8 lid 1 EVRM wordt vaak, ook door het Kabinet, gerelativeerd door te stellen dat de bewaarplicht niet ziet op gegevens die iets zeggen over de inhoud van de communicatie, maar slechts op het verkeer.[227] In dit kader gaat de stand van de techniek echter een niet te miskennen rol spelen. Zo recent als 3 juni jl. werd bekend dat aanbieders T-Mobile en Vodafone alle

[222] Vingerafdrukken bevatten "unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances." EHRM S. and Marper v. The United Kingdom, nr. 84.
[223] Asscher & Koops 2003, p.47/48.
[224] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.8: "Verkeersgegevens zijn niet erg veelzeggend zolang deze niet kunnen worden gekoppeld aan gedragingen van personen."
[225] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.5.
[226] Op de gespecificeerde rekening van T-Mobile staan datum, starttijd, type, bestemming (bijv. telefoonnummer), land, duur, bundel en kosten worden vermeld. Uit een gespecificeerde rekening wordt bijvoorbeeld niets duidelijk over de exacte locatie van de beller of de gebelde op een bepaalde tijdstip. Zie bijlage A bij deze scriptie.
[227] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.8.

onder hun verwerkte verkeersgegevens in relatie tot sms-berichten doorsturen naar de AIVD en dat daarbij inhoud wordt meegezonden, terwijl de aanbieders noch de AIVD inhoud (sms-header) van de verkeersgegevens kan scheiden vanwege tekortkomingen in de techniek.[228] De onlangs verwoorde stelling van de Minister dat er "over de inhoud van de gegevens niets wordt vastgelegd",[229] blijkt in de praktijk dus niet te kloppen. Dit werd ook al duidelijk in de parlementaire behandeling, toen het ging over de headers van e-mailberichten.[230] De techniek maakt het in meerdere gevallen dus nog niet mogelijk om de inhoud van de telecommunicatiegegevens te onderscheiden. Zo lang deze technologische tekortkoming niet is ondervangen, worden door de dataretentieverplichtingen mogelijkerwijs niet alleen telecommunicatiegegevens maar de facto ook inhoudsgegevens verplicht bewaard, terwijl de dataretentierichtlijn hiertoe de iure niet verplicht.

Daarnaast gaat Breyer in op het onderscheid tussen content en telecommunicatiegegevens en stelt hij, dat telecommunicatiegegevens "cannot be considered less privacy-invasive than the surveillance of the content of telecommunications."[231] Ten eerste voert hij aan dat telecommunicatiegegevens veel effectiever verwerkt worden dan content. Automatische verwerken, het aan de hand van bepaalde criteria doorzoeken en eenvoudig combineren met andere gegevens, is bijvoorbeeld minder makkelijk met content data. Een set telecommunicatiegegevens heeft ten tweede een gelijke of grotere informatiewaarde dan content data, omdat uit een set gegevens communicatie- en gedragspatronen ontstaan, waaruit sociale omgevingen en gefrequenteerde bestemmingen en bewegingen van individuen kunnen worden herleid. Asscher & Koops volgen ongeveer dezelfde redenering, en noemen daarbij dat art. 126n Sv dusdanig kan worden ingezet, dat de bevoegdheid het karakter van stelselmatige observatie krijgt.[232] Buiten de technologische tekortkomingen, is het dus ook zeer de vraag of content data meer inbreuk maken op art. 8 lid 1 EVRM dan telecommunicatiegegevens.

Vastgesteld kan worden dat telecommunicatiegegevens veel informatie bevatten over de betrokkene, dat die informatiewaarde volgens Breyer niet minder is dan die van communicatie-inhoud en dat de technologie het in bepaalde gevallen nog niet toelaat inhoud en telecommunicatiegegeven strikt te scheiden. Bovendien hebben Kabinet en Minister een onjuiste voorstelling van de aard van de persoonsgegevens die verplicht bewaard zullen worden door aanbieders.

### 3.2.2. Beschikbaarheid

In de zaak *S. and Marper v. The United Kingdom* van 8 december 2008 oordeelde de Grand Chamber van het EHRM dat alleen al het bewaren van gegevens een dermate indringende inbreuk op art. 8 lid 1

[228] <http://webwereld.nl/nieuws/58991/aivd-kan-onrechtmatige-sms-taps-niet-vernietigen.html> [geraadpleegd juli 2009]. Op basis van een rapport van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), in te zien via: <http://www.ctivd.nl/?download=CTIVD%20rapport%2019.pdf> [geraadpleegd juli 2009].
[229] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.8.
[230] Zo kan de afzender van een e-mailbericht volgens deskundigen, aan het woord in de expertbijeenkomst georganiseerd door de Eerste Kamer, alleen herleidt worden uit de zogenaamde "enveloppe-header van het berichtje en dat wordt gezien als de inhoud van het mailbericht." De Minister ontwijkt de vraag die de CDA-fractie hierover stelt, met het standpunt dat aanbieders de headers niet verplicht hoeven te bewaren en dat de afzender van een e-mailbericht herleidt kan worden uit andere verkeersgegevens. Volgens de experts kan op basis van die andere verkeersgegevens slechts worden aangegeven van dat de e-mail afkomstig is van de "Amsterdam Exchange of KPN", niet van welke eindgebruiker. *Kamerstukken II*, 2008-2009, 331 145, nr. D, p.13; *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.11.
[231] Breyer 2005, p.370; Amici Curiae 2008, p.6.
[232] Asscher & Koops 2003, p.91; zie tevens par. 2.2.2.

EVRM kan vormen, dat deze niet gerechtvaardigd wordt door het opsporingsbelang. Het betrof hier het door Engelse opsporingsautoriteiten in een gecentraliseerde databank bewaren van biometrische persoonsgegevens (DNA, weefsel en vingerafdrukken) van Engelse burgers die in aanraking zijn gekomen met justitie, maar niet veroordeeld werden. Onder verwijzing naar eerdere jurisprudentie van het Hof,[233] luidt zijn oordeel dat alleen al de bewaring van vingerafdrukken een schending van art. 8 lid 1 EVRM opleverde, nu de beschikbaarheid daarvan eventuele toegang door opsporingsdiensten in de toekomst mogelijk maakt.[234] Het EHRM geeft in deze uitspraak klip-en-klaar aan de interdependentie van beschikbaarheid en toegang mee te wegen bij de beoordeling van schendingen van art. 8 EVRM;[235] zonder beschikbaarheid van de gegevens is van toegang daartoe immers geen sprake. Het moment waarop de inbreuk aanvangt is hiermee helder: nog voordat de gegevens worden ingezien door opsporingsinstanties kan alleen al het bewaren van gegevens een schending opleveren van art. 8 EVRM. Het Kabinet is steevast van opvatting dat "niet zozeer de bewaring als wel het gebruik van de gegevens van belang is voor de beoordeling van de aantasting van de persoonlijke levenssfeer."[236] Gezien de recente uitspraak van het EHRM is de bewaring op zichzelf wel degelijk van belang voor deze beoordeling.

Wat is dan de aard van de inbreuk van dataretentie op art. 8 EVRM? De uitspraak van het BVerfG biedt inzicht hierin.[237] Het BVerfG oordeelt dat de bewaarplicht een bedreiging van de vrije informatie-uitwisseling en het vertrouwen in het communicatiegeheim impliceert.[238] Ook benadrukt het BVerfG dat dataretentie een zogenaamd 'chilling effect' heeft: het verhindert het op legitieme wijze ongehinderd gebruikmaken van telecommunicatie door burgers, uit angst voor daaruit voortvloeiende strafprocesrechtelijke maatregelen.[239] Dit chilling effect wordt volgens het BVerfG versterkt door de omstandigheid dat de opslag voor individu niet waarneembaar is.

Het is gemakkelijk om het 'chilling effect' als een weinig concrete schending van art. 8 lid 1 EVRM te beschouwen. Maar vanuit breder perspectief bezien, buiten het strikte rechtswetenschappelijke domein, kan de weerslag van chilling effecten op de persoonlijke levenssfeer inzichtelijk worden gemaakt. Elektronische telecommunicatie heeft vandaag de dag namelijk een steeds belangrijkere invloed op de vorming van de persoonlijkheid, waarvan de bescherming door het EHRM expliciet onder de reikwijdte van art. 8 lid 1 EVRM is gebracht (zie par. 3.1.). Dit kan verduidelijkt worden met de theorie over het 'reflexieve project van het zelf' van Frissen & De Mul en de in de informatiesamenleving veranderende rol van het individu in relatie tot zijn omgeving. Vermaard socioloog Anthony Giddens stelt, kort samengevat, dat globalisering, migratie, individualisering en het verlies van tradities hebben geleid dat het Westerse individu tot zichzelf wordt teruggeworpen met betrekking tot zijn culturele vorming.[240] De radicale twijfel van het individu die deze ontwikkeling tot

[233] EHRM S. and Marper v. The United Kingdom, nrs. 78-83.
[234] EHRM S. and Marper v. The United Kingdom, nr. 86.
[235] Zie par. 2.4.
[236] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.24; *Kamerstukken II*, 2007-2008, 31 145, nr. 9, p.17; *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.12. Recent nog in *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.8.
[237] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08.
[238] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 122-123.
[239] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 122-123; Ekker 2008, p.232. In par. 123 oordeelt het BVerfG: "Die anlasslose Vorratsspeicherung von Telekommunikations-Verkehrsdaten könne die Bevölkerung massiv einschüchtern." (einschüchtern = intimideren).
[240] A. Giddens, Modernity and Self-Identity, Cambridge: Polity Press 1991.

gevolg heeft, door andere commentatoren omschreven als "postmoderne onzekerheid",[241] zet het individu volgens Frissen & De Mul aan tot een alsmaar voortdurend "reflexief project" met betrekking tot de vorming van zijn identiteit, die nooit 'af' is.[242] Vandaag de dag is ICT dusdanig verweven met alle facetten van het dagelijks leven – in de woorden van Frissen "gedomesticeerd"[243] – dat telecommunicatie voor de identiteitsvorming en persoonlijke ontwikkeling onontbeerlijk raakt.[244] De mens, en vooral de jongere, kan niet buiten deze vormen van telecommunicatie.[245] Chilling effecten met betrekking tot het gebruik van telecommunicatie vormen vanwege dit toenemende belang van telecommunicatie voor de zelfontplooiing van het individu, en zijn veranderende rol in de gemeenschap, een ernstige inbreuk op art. 8 lid 1 EVRM. Daarbij dient aan de ene kant te worden aangetekend, dat de privacybeleving van met name jongeren met diezelfde gedaanteverandering van ICT meegaat. Aan de andere kant verzwaren chilling effecten de door het CBP verwoorde sociale exclusie van verdachten in de telecommunicatieomgeving, als gevolg van de wetenschap dat men middels verplicht bewaarde telecommunicatiegegevens in verband gebracht kan worden met een verdachte en dientengevolge in beeld komt van de opsporing.[246] De weerslag van uit dataretentie voortvloeiende chilling effecten op de verwezenlijking en ontwikkeling van een eigen persoonlijkheid is geen abstract gegeven, maar moet in het licht van art. 8 lid 1 EVRM serieus genomen worden: de helft van de Duitsers voelt zich sinds de dataretentiemaatregelen belemmerd bij het bespreken van persoonlijke aangelegenheden door de telefoon, zo blijkt uit recent kleinschalig onderzoek.[247] De vraag hoe Nederlanders op de bewaarplicht zullen reageren, vormt een belangrijk punt voor vervolgonderzoek.[248]

Breyer voegt in een artikel dat specifiek gewijd is aan de verenigbaarheid van dataretentie met art. 8 EVRM nog een aantal elementen aan de inbreuk op art. 8 lid 1 EVRM toe.[249] Zo is de bewaarplicht niet toegespitst op een verdacht individu, maar wordt de gehele bevolking onderworpen aan de bewaarplicht waardoor alle burgers in beeld kunnen komen van de opsporing.[250] De privacy wordt daarbij niet alleen in de publieke ruimte of op de werkvloer aangetast, ook in het eigen huis kunnen burgers niet ontkomen aan de bewaarplicht. Voorts kan het 'chilling effect' leiden tot ingetoomde politieke overtuigingen en verminderde deelname aan het democratische proces, uit angst voor represailles na kritiek op staatsinstituties.[251] In eerste opzicht klinkt dit laatste element als een kreet uit de verte, maar niemand weet in welke richting Europese samenlevingen zich binnen tien of twintig jaar kunnen ontwikkelen. Aan deze bloemlezing van de algemene risico's van dataretentie voor de

---

[241] J. de Mul (et al.), *ICT de baas?*, Onderzoeksprogramma Internet en Openbaar bestuur, 2001.
[242] De Mul & Frissen 2000, p.45: "identiteit is in deze nieuwe maatschappelijke context geen gegeven, maar een voortdurende opgave: de vraag 'wie ben ik?' is meer dan ooit aan de orde, waardoor dit reflexieve project van het zelf prominent op de agenda staat."
[243] ICT doet tegenwoordig, anders dan halverwege de jaren '90, zijn uiterste best om ons leven na te bootsen. Frissen 2007, p. 15. Zeer interessant is de oratie van Prof. Frissen: V. Frissen, *De domesticatie van de digitale wereld*, 25 juni 2004, <http://www.xpin.nl/materiaal/oratie_Valerie_Frissen.pdf> [geraadpleegd juli 2009]. Zie in het bijzonder noot 8.
[244] Breyer 2005, p.371.
[245] Frissen 2007, p. 10; C. Haythornthwaite & B. Wellman, *'The Internet in Everyday Life'*, 2002, p. 7.
[246] *Kamerstukken II*, 2004-2005, 30 164, nr. F, p.2 e.v.
[247] Ekker 2008, p.233 onder verwijzing naar: <http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf> [geraadpleegd juli 2009].
[248] Zie par. 5.3.
[249] Breyer 2005; Amici Curiae 2008 (een uitwerking van het artikel van Breyer).
[250] Reeds gesignaleerd in par. 2.3.2. en par. 2.3.3.
[251] Breyer 2005, p.371.

persoonlijke levenssfeer, kan mijns inziens in specifiekere zin nog worden toegevoegd dat het wetsvoorstel verder gaat dan art. 5 dataretentierichtlijn, door ook het bewaren van locatiegegevens tijdens mobiele telefoongesprekken verplicht te stellen (zie par. 3.3.2.4.). Zo schept dataretentie bijvoorbeeld de mogelijkheid om te traceren welke personen aan bepaalde demonstraties of vergaderingen hebben deelgenomen. Op dat moment is de inbreuk op een volgend grondrecht aan de orde, te weten de vrijheid van vergadering en vereniging zoals neergelegd in art. 11 lid 1 EVRM. Breyer stelt bovendien dat dataretentie niet te vergelijken is met eerdere aan telecommunicatiegegevens gerelateerde strafprocesrechtelijke maatregelen. Eindgebruikers zijn namelijk in geen enkel opzicht verantwoordelijk voor het creëren van het gevaar, terwijl telecommunicatiehandelingen niet plaatsvinden in specifiek risicovolle of gevaarlijke (netwerk)omgevingen.[252]

Daarmee belanden wij bij de overweging dat het strafprocesrecht voortaan een integraal onderdeel uitmaakt van de Europese en Nederlandse regulering van beschikbaarheid van telecommunicatiegegevens (zie par. 2.3.2., en over de interdependentie van beschikbaarheid en toegang in par. 2.4.). Dit aspect is mijns inziens van essentieel belang. Een van de uitgangspunten van het EVRM is de bescherming van het individu tegen inbreuken op zijn grondrechten in verticale relaties (staat-burger). Telecommunicatiegegevens worden niet voor wetenschappelijke doeleinden bewaard, maar om de opsporing te ondersteunen; dit verzwaart de inbreuk op art. 8 lid 1 EVRM.[253] Volgens het BVerfG hangt de omvang van mogelijke chilling effecten af van de voorwaarden waaronder de gegevens opgevraagd en gebruikt kunnen worden. Daarmee is niet alleen het EHRM, maar ook het BVerfG zich bewust van de interdependente relatie tussen beschikbaarheid en toegang.[254] Deze constatering vormt een vloeiende overgang naar de volgende paragraaf, die niet los maar in samenhang met deze paragraaf moet worden bezien.

### 3.2.3. Toegang en de hernieuwde verhouding met beschikbaarheid

De stelling van de Minister dat het verplicht bewaren van telecommunicatiegegevens van alle burgers voor een bepaalde periode niet erg relevant was voor de beoordeling van de aantasting van de persoonlijke levenssfeer[255] is niet juist, zo blijkt uit de vorige paragraaf. Juist de mogelijkheid van toegang kan burgers al aantasten in hun privacy, zo is betoogd. De daadwerkelijke toegangsverzoeken tot verplicht bewaarde telecommunicatiegegevens vormen derhalve zware inbreuken op de persoonlijke levenssfeer, zo oordeelt het BVerfG.[256] Allereerst verkrijgen opsporingsinstanties daadwerkelijk een compleet beeld van het communicatiegedrag van de betrokkene, zijn sociale contacten en het communicatiegedrag van personen met wie de betrokkene gecommuniceerd heeft gedurende een bepaalde periode. Op de tweede plaats noemt het BVerfG toegang tot de gegevens een onomkeerbare inbreuk, aangezien het veelvuldig een nieuwe grondslag vormt voor de toepassing van

[252] Breyer 2005, p.370; Amici Curiae 2008, p.6.
[253] EHRM S. and Marper v. The United Kingdom, nr. 67.
[254] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 122-123. Ekker omschrijft de zienswijze van het BVerfG als een erkenning van een "duidelijke samenhang". Ekker 2008, p.232.
[255] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.24; *Kamerstukken II*, 2007-2008, 31 145, nr. 9, p.17; *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.12. Recent nog in *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.8.
[256] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 155-159.

nadere dwangmiddelen die anders niet zouden worden toegepast. Dergelijke nadelige gevolgen van het opvragen van telecommunicatiegegevens kunnen later niet ongedaan gemaakt worden.

De voorwaarden waaronder toegang wordt verkregen door opsporingsdiensten zijn van enige invloed op de ernst van de inbreuk van toegang op art. 8 lid 1 EVRM,[257] aangezien soepele criteria chilling effecten en de inbreuk op het communicatiegeheim kunnen versterken. Het valt buiten het bereik van dit onderzoek om het samenspel van dataretentie en alle toegangsbevoegdheden in het Wetboek van Strafvordering te analyseren in het licht van art. 8 EVRM. Dit onderzoek zal zich moeten beperken tot de bespreking van vier specifieke ontwikkelingen van de Nederlandse situatie, die de inbreuk op art. 8 lid 1 EVRM ernstiger maken. De bewaartermijn, die door de Tweede Kamer al werd teruggebracht van 18 naar 12 maanden,[258] heeft een belangrijke invloed op de toegangsbevoegdheden. Dat niet voor de minimumtermijn van zes maanden is geopteerd, terwijl de inbreuk van dataretentie alsmede de toegangsbevoegdheden door een langere termijn verhevigt, vormt een eerste punt van aandacht (par. 3.3.2.1.). Dat de toegang tot de gegevens niet beperkt blijft tot 'ernstige misdrijven', zoals in par. 2.3.3. is besproken, is een volgende ontwikkeling die aan nader onderzoek wordt onderworpen. De verenigbaarheid met art. 8 EVRM van de verwijzing in onder meer art. 126n lid 1 Sv naar art. 67 lid 1 Sv (par. 3.3.2.2.) en het vorderen van verplicht bewaarde gebruiksgegevens door opsporingsambtenaren ex art. 126na lid 1 Sv (par. 3.3.2.3.) zijn respectievelijk de tweede en derde ontwikkeling die specifiek besproken zullen worden. De toegang van opsporingsdiensten tot verplicht bewaarde locatiegegevens gedurende mobiele communicatie komt aan bod in par. 3.3.2.4.

Het vijfde aandachtspunt betreft het gebrek aan controle op de opsporingsinstanties. In par. 2.2.2. werd al stilgestaan bij het uitblijven van notificatie van toegang tot telecommunicatiegegevens. Op grond van art. 126bb Sv is dit voor het vorderingsverzoek van art. 126n lid 1 Sv verplicht, als het onderzoek het toelaat, maar in de praktijk blijken opsporingsinstanties slordig om te springen met de notificatieplicht. Daarnaast is de uitoefening van de vorderingsbevoegdheden niet onderworpen aan een algemene registratieplicht.[259] Op zichzelf is dit een zorgwekkende constatering, omdat er blijkbaar geen sprake is van kwantitatieve controle op of verantwoording van de opsporingsinstanties – met uitzondering van het vorderen van gebruiksgegevens via het CIOT, dat jaarlijks niet minder dan circa twee miljoen keer geraadpleegd wordt.[260] Tegen deze achtergrond, is het verbazingwekkend dat de statistische verantwoordingsplichten van art. 10 jo. art. 14 dataretentierichtlijn niet zijn geïmplementeerd in het wetsvoorstel, en dat het parlement hier zo weinig bezwaar tegen heeft gemaakt.[261] Het ziet ernaar uit dat het parlement tevreden is met de toezeggen dit alsnog via een AMvB wordt geregeld, terwijl een statistische verantwoordingsplicht de belangrijkste vorm van controle op het gebruik van bevoegdheden door behoeftestellers is.[262] Gebrek aan controle maakt de inbreuk op art. 8 lid 1 EVRM ernstiger, omdat de burger in eerste instantie niets merkt van toegang tot de hem

[257] EHRM S. and Marper v. The United Kingdom, nr. 86; Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 149; Groothuis 2006, p.808.
[258] Zie de opmerking over de toezegging van de Minister op 7 juli jl. aan de Eerste Kamer aan het begin van par. 2.3. Al ziet deze toezegging op het terugbrengen van de bewaartermijn voor internetgegevens tot zes maanden, is het nog niet zeker of de reparatiewet waarin dit geregeld zal worden door de Tweede Kamer wordt aangenomen. Daarom wordt vooralsnog uitgegaan van een termijn van twaalf maanden voor zowel telefonie- als internetgegevens.
[259] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.18.
[260] Zie par. 2.2.2.
[261] Zwenne & Schmidt 2008, p.285.
[262] Idem.

betreffende telecommunicatiegegevens, en deze daarom niet goed kan aanvechten.[263] De vaak gemaakte vergelijking met het panopticum van Jeremy Bentham, de gevangenis met maar één bewaker die alle gevangen rustig houdt omdat zij nooit weten of zij überhaupt in de gaten gehouden worden, en de daaraan verbonden chilling effecten zijn hier aan de orde. In par. 3.3.2.5. wordt daarom uitgebreider stilgestaan bij dit gebrek aan controle op de controleurs.[264]

## 3.3. Rechtvaardiging van de inbreuk in de zin van art. 8 lid 2 EVRM

Nu de aard van de inbreuk van de bewaarplicht, de toegang tot verplicht bewaarde gegevens en specifieke toegangsbevoegdheden van Nederlandse opsporingsinstanties zijn besproken, kan worden bezien of er sprake is van rechtvaardiging van de inbreuk in de zin van art. 8 lid 2 EVRM. Er zijn drie cumulatieve criteria voor een rechtvaardiging van een inbreuk. Deze worden besproken, alvorens zij in de volgende paragrafen getoetst worden in lijn met de structuur van de bespreking van de inbreuk op art. 8 lid 1 EVRM in par. 3.2.2. en 3.2.3.

Allereerst moet de inbreuk een legitiem belang dienen. Al stelt Breyer dat opsporing in zichzelf niet dient ter preventie van wanordelijkheden of strafbare feiten en derhalve geen legitiem belang vormt in de zin van art. 8 lid 2 EVRM,[265] staat het EHRM doorgaans nauwelijks stil bij de vraag of opsporing een legitiem belang is, en wijdt het Hof een aantal zinnen aan deze kwestie om deze vraag vervolgens bevestigend te beantwoorden.[266] Aan dit criterium wordt derhalve geen verdere aandacht besteed.

Als tweede criterium voor de rechtvaardiging in de zin van art. 8 lid 2 EVRM geldt, dat een inbreuk 'bij wet voorzien' is. Dit criterium valt uiteen in drie deelcriteria.[267] Ten eerste moet de maatregel in nationale wetgeving zijn vastgelegd. De dataretentierichtlijn, het wetsvoorstel en ook aanverwante algemene maatregel van bestuur doorstaan dit criterium. De maatregelen zijn tevens voldoende 'toegankelijk voor het publiek'. Ten derde moet er sprake zijn van 'foreseeability'. Hier is sprake van een kwalitatief criterium, de onderhavige wetgeving moet met voldoende precisie zijn geformuleerd.[268] Deze zogenaamde 'test of foreseeability' is "not designed to secure absolute certainty, but a certain level of clarity is required."[269] De zaak *Liberty a.o. v. The United Kingdom* bevat een samenvatting van de jurisprudentie ten aanzien van dit derde deelcriterium voorzienbaarheid.[270] Burgers moeten de effecten van maatregel kunnen inschatten, zodat zij hun gedrag erop kunnen aanpassen. Daarnaast moet de wet in overeenstemming zijn met de algemene beginselen van de rechtsstaat, oftewel waarborgen bevatten tegen willekeur en misbruik. Vaste jurisprudentie hanteert drie praktischere handvatten die invulling geven aan dit kwalitatieve vereiste, te weten de notificatie,

[263] Chavannes 2008, p.245.
[264] Deze uitdrukking is ontleend aan Plato, die dit probleem als een van de centrale uitgangspunten neemt in zijn zoektocht naar de ideale staatsvorm. Zie o.m. Plato, *De ideale Staat*, Amsterdam: Athenaeum-Polak & Van Gennep 2005.
[265] Breyer 2005, p.369.
[266] EHRM S. and Marper v. The United Kingdom, nr. 100; Jacobs & White 2006, p.228. Amici Curiae, p.4.
[267] EHRM Huvig v. France, nr. 26.
[268] Zie bijvoorbeeld EHRM Silver a.o. v. The United Kingdom, nr. 87.
[269] EHRM Liberty a.o. v. The United Kingdom, nr. 62.
[270] EHRM P.G. and J.H. v. France, nr. 97; EHRM Huvig v. France, nr. 52.

beperking van de effecten van de maatregel en dat de test of foreseeability zwaarder wordt, naarmate het karakter van de inbreuk ernstiger is.[271] Dit vereiste komt aan de orde in par. 3.3.2.5.

Op de derde plaats moet de inbreuk op de persoonlijke levenssfeer 'in een democratische samenleving noodzakelijk' zijn**.** In de zaak *Silver a.o. v. The United Kingdom* vat het EHRM de jurisprudentie op dit punt uitvoerig samen.[272] Het noodzakelijkheidscriterium wordt verder ingevuld door het leerstuk van de 'pressing social need'. Er moet sprake zijn van een dringende maatschappelijke behoefte om het legitieme doel te vervullen ten koste van art. 8 lid 1 EVRM. Daarbij geldt dat 'noodzakelijk' geen synoniem van 'nodig' is, en niet de flexibiliteit van woorden als 'nuttig' of 'wenselijk' heeft. Daaraan relaterend is er het vereiste dat een maatregel 'proportionate to the legitimate aim pursued' moet zijn. Om aan dit proportionaliteitsvereiste te voldoen, dient een belangenafweging plaats te vinden tussen het nastreven van dit legitieme belang en de impact die dit heeft op het recht op privacy van burgers. Daarbij geldt dat de lat hoger komt te liggen naarmate de inbreuk op art. 8 lid 1 ernstiger is. Bij deze belangenafweging wordt een beoordeling van de effectiviteit en de subsidiariteit van de maatregel meegewogen, alsmede of er sprake is van beperkingen van de inmenging.[273] De relatie van deze aspecten met de pressing social need zorgt voor een spelingsruimte (of: onzekerheid) in de beoordeling van rechtvaardigingen onder lid 2 van art. 8 EVRM, immers: ook al is een maatregel weinig effectief, aan wie komt de beslissing toe of er sprake is van een dusdanig dringende maatschappelijke behoefte dat aan die geringe effectiviteit veel of juist weinig gewicht wordt toegekend? Proportionaliteit en 'pressing social need' zijn twee communicerende vaten, maar de mate waarin zij aan elkaar relateren is onhelder.

Lidstaten hebben daarom een bepaalde beoordelingsvrijheid, i.e. een margin of appreciation, bij deze belangenafweging. Soms is deze beoordelingsvrijheid ruim, soms zeer beperkt – afhankelijk van de omstandigheden van het geval.[274] Het Hof zet in de zaak *S. and Marper v. The United Kingdom* uiteen dat de reikwijdte van de margin of appreciation afhangt van vier factoren, te weten welk recht in kwestie wordt geschonden, het belang van dit recht voor het individu, de aard van die schending en het doel dat met de schending wordt nagestreefd. Als een "particularly important facet of an individual's existence or identity at stake" is, wordt de beoordelingsvrijheid van lidstaten beperkt. Als er aan de andere kant geen consensus bestaat in de lidstaten over hoe het geschonden recht optimaal beschermd kan worden, is de beoordelingsvrijheid groter.[275] De gronden die lidstaten aanvoeren dienen "relevant and sufficient"[276] te zijn, terwijl de uiteindelijke beslissing hierover toekomt aan het EHRM.[277] Aangezien dataretentie in een richtlijn wordt opgelegd aan alle lidstaten, is de margin of appreciation van afzonderlijke lidstaten niet aan de orde bij de beoordeling van dataretentie als zodanig, maar pas op het moment dat lidstaten in implementatiewetten afwijken van de met de dataretentierichtlijn voorgeschreven verplichtingen, dan wel bij het samenspel van dataretentie en specifieke bevoegdheden

[271] "the level of precision required depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed", EHRM Vogt v. Germany, nr. 48; Daarnaast in bijv. EHRM Silver a.o. v. The United Kingdom, nr. 88.
[272] EHRM Silver a.o. v. The United Kingdom, nr. 97; Jacobs & White 2006, p.232.
[273] EHRM Silver a.o. v. The United Kingdom, nr. 97; Jacobs & White 2006, p.232.
[274] Jacobs & White 2006, p.232.
[275] EHRM S. and Marper v. The United Kingdom, nr. 102.
[276] EHRM S. and Marper v. The United Kingdom, nr. 101.
[277] EHRM S. and Marper v. The United Kingdom, nr. 101.

van Nederlandse strafvorderlijke bevoegdheden.[278] Waar de margin of appreciation een rol kan spelen, wordt aandacht besteed aan dit vraagstuk.[279] Er wordt verder niet stilgestaan bij de merkwaardige ontwikkeling dat de wetgever op sommige gebieden de beoordelingsvrijheid incalculeerd, terwijl dit pas aan het EHRM is om de leer van de margin of appreciation wel of niet toe te passen.

Tot slot geldt dat de in art. 8 lid 2 EVRM genoemde belangen uitputtend zijn. In de praktijk kunnen lidstaten vrij eenvoudig een inbreuk onder een in lid 2 genoemd belang brengen.[280] Dit criterium doet daarom verder niet ter zake.

Groothuis observeert al in 2006 dat de bewijslast voor de inmenging op art. 8 EVRM is verschoven naar de lidstaten.[281] Van Hoboken ziet dit met de uitspraak van het Hof van Justitie in de zaak over de rechtsgrondslag van de dataretentierichtlijn bevestigd.[282] Dientengevolge zal worden onderzocht of de door het Kabinet naar voren gebrachte argumenten volstaan om de inbreuk te rechtvaardigen.

### 3.3.1. Beschikbaarheid

Een eerste vraag die kan worden beantwoord is die naar de voorzienbaarheid van de maatregel. Deze vraag spitst zich toe op verenigbaarheid met de algemene beginselen van de rechtsstaat in het algemeen, en waarborgen tegen willekeur en misbruik in het bijzonder. Het feit dat van alle burgers, verdacht of niet, telecommunicatiegegevens worden bewaard voor een langdurige periode zet Cooper aan tot de stelling dat er sprake is van willekeur, en daarmee van onvoldoende precisering van de maatregel.[283] Breyer is mijns inziens terecht de opvatting toegedaan dat deze willekeur afwezig is, omdat er simpelweg van alle burgers gegevens worden bewaard, waardoor er geen willekeurig onderscheid tussen verschillende burgers wordt gemaakt.[284] Het risico van misbruik van de verplicht bewaarde gegevens door de aanbieders is ondervangen door art. 13.5 wetsvoorstel, waarin het verbod op kennisneming door onbevoegden, geheimhouding en de beveiligingsverplichtingen van de aanbieders is geregeld.

De tweede vraag is die naar de noodzakelijkheid van dataretentie in een democratische samenleving. De bestrijding van terrorisme en de opsporing van strafbare feiten zijn van eminent belang in een democratische samenleving. Opsporingsautoriteiten beschikken daarom over een uitgebreid wettelijk instrumentarium om in te grijpen in de persoonlijke levenssfeer van burgers, ter behartiging van deze belangen (zie par. 2.2.). Met het wetsvoorstel zullen de gegevens met betrekking tot miljoenen communicaties per dag worden bewaard, gedurende 12 maanden. De Minister stelt vast dat "de gegevens zeer waardevol [zijn] in zeer veel onderzoeken die door de opsporingsdiensten worden gedaan. Daarmee staat voor mij het nut van de bewaarplicht vast."[285] Maar het vaststellen van het nut van de bewaarplicht, is echter nog niet voldaan aan het vereiste van noodzakelijkheid. Zoals

[278] Jacobs & White 2006, p.232.
[279] Zie par. 3.3.2.1. t/m par. 3.3.2.5.
[280] Jacobs & White 2006, p.226.
[281] Groothuis 2006, p.809.
[282] Van Hoboken 2009.
[283] Cooper 2003, p.8.
[284] Breyer 2005, p.367.
[285] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.3.

besproken geeft vaste jurisprudentie van het EHRM aan dat noodzakelijk niet hetzelfde betekent als nodig, nuttig of wenselijk. Een bewaarplicht zal het opsporingsonderzoek onmiskenbaar efficiënter en eenvoudiger maken, maar de daarmee is de noodzakelijkheid van de maatregel niet aangetoond.

De vraag is echter of er sprake is van een dringende maatschappelijke behoefte, een 'pressing social need' in de woorden van het EHRM, om de specifieke maatregel dataretentie te treffen. In par. 1.4 is reeds besproken dat er op Europees niveau nooit sluitend bewijs is geleverd van deze pressing social need, ze is door Europese instituties als het Parlement en de artikel 29 Werkgroep zelfs expliciet in twijfel getrokken.[286] Overigens bleek uit hoofdstuk 1 wel dat het politieke klimaat zich ten gunste van dergelijke maatregelen ontwikkelde. Toch heeft de Eerste Kamer bij de behandeling van het ontwerp-Kaderbesluit in 2004 haar goedkeuring aan een dergelijke maatregel onthouden, zo lang de noodzaak en proportionaliteit van de maatregel niet aangetoond konden worden.[287] Maar door de implementatieplicht van de dataretentierichtlijn is de noodzakelijkheidsvraag in de parlementaire behandeling verschoven van de vraag of er überhaupt een bewaarplicht moet komen, naar de noodzakelijkheid van een bepaalde bewaartermijn (zie par. 3.3.2.1.).[288] De noodzakelijkheid van de dataretentiemaatregel is met andere woorden niet zonder meer inzichtelijk gemaakt, terwijl het nut van de beschikbaarheid van telecommunicatiegegevens voor zich spreekt. Ook in de literatuur is de noodzakelijkheid van dataretentie consequent in twijfel getrokken.[289] Een tegengesteld geluid komt van Bignami, die zich kan vinden in het ontbreken van bewijs van de noodzaak van de maatregel omdat het leveren van dit bewijs "unrealistic" zou zijn.[290] Dat het onrealistisch zou zijn de noodzakelijkheid te moeten bewijzen, druist echter in tegen de gehele essentie van het vereiste. Zonder bewijs van een 'pressing social need', geen maatregel – zo luidt de vaste jurisprudentie van het EHRM.[291]

Het ontbreekt daarnaast aan feitelijke onderbouwing van de stellingen van de Minister. Nergens wordt met cijfers onderbouwd wat nu precies de aanleiding is voor het treffen van deze inbreukmakende maatregel voor 12 maanden, zoals stijgende criminaliteitscijfers of toenemende terroristische dreiging. Volgens cijfers van het CBS is er zelfs sprake van een consequente daling van de criminaliteit op alle fronten sinds 2002, terwijl het percentage opgehelderde misdrijven stijgt.[292] De samenvatting over de ontwikkeling van de criminaliteit in het recent gepubliceerde jaarbericht 2008 van het OM bevat het volgende fragment:[293]

> "Het OM kreeg in 2008 van de regiopolitiekorpsen 4% minder misdrijfzaken te verwerken dan in 2007: het aantal zaken daalde van 243.100 tot 233.600. De instroom vanuit de bijzondere opsporingsdiensten (FIOD-ECD, SIOD, AIVD) daalde met 7% van 17.900 tot 16.600. De daling geldt voor vermogensmisdrijven, geweldsmisdrijven,

---

[286] Smits 2006, p.151; EDRI, *EP rejects data retention proposal*, 15 jun. 2005, te vinden op: <http://www.edri.org/edrigram/number3.12/dataretention> [geraadpleegd juli 2009]; art. 29 WP Opinion 9/2004, 15 nov. 2004; art. 29 WP Opinion 4/2005, 21 okt. 2005.

[287] *Kamerstukken I*, 2004-2005, 23 490, nr. AM, tevens *Kamerstukken I*, 2004-2005, 23 490, nr. 372 (Motie-Vendrik c.s.); *Kamerstukken I*, 2008-2009, 31 145, nr. B, p.1.

[288] *Kamerstukken II*, 2006-2007, 31 145, nr.3 (MvT), p.24; *Kamerstukken II*, 2007-2008, 31 145, nr.9, p.17 & 35; *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.12; *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.7.

[289] Breyer 2005; Zwenne & Schmidt 2005; Groothuis 2006; Amici Curiae 2008.

[290] Bignami 2007, p.251.

[291] Zie par. 3.3.

[292] CBS StatLine, *Cijfers geregistreerde criminaliteit*, 18 juli 2008, in te zien via: <http://statline.cbs.nl/StatWeb/publication/default.aspx?DM=SLNL&PA=37932&D1=0%2c2-3&D2=0-1&D3=0&D4=a&HDR=T%2cG2%2cG3&STB=G1&VW=T> [geraadpleegd juli 2009].

[293] Jaarbericht Openbaar Ministerie, *Landelijk cijferboekje jaarbericht 2008*, peildatum 9 maart 2009, te downloaden via: < http://www.om.nl/actueel/publicaties/jaarbericht_2008/> [geraadpleegd juli 2009]. Een samenvatting is te vinden via: <http://www.om.nl/actueel/nieuws-_en/@150586/jaarbericht_om_2008/> [geraadpleegd juli 2009].

> drugsdelicten, verkeersmisdrijven en voor misdrijven op het terrein van de openbare orde, zoals vernieling en brandstichting. Ook de jeugdcriminaliteit - een van de prioriteiten van het OM - is gedaald. De instroom van het aantal minderjarige verdachten daalde met 6% van 37.900 in 2007 tot 35.500 vorig jaar. De cijfers van het OM bevestigen het beeld uit de laatste Veiligheidsmonitor dat we in Nederland minder criminaliteit ervaren in onze woonomgeving. Voelde in 2005 een derde van de inwoners zich wel eens onveilig, in 2008 was dat gedaald tot een kwart van de populatie."

De criminaliteit daalt op alle fronten en het OM is steeds beter in staat om misdrijven op te lossen, blijkt ook uit de cijfers van de behoeftestellers (OM).

Daarbij werd in par. 2.3.2. met Zwenne & Schmidt al gewezen op de – voor burgers niet te verifiëren – plausibele kanttekening dat de bewaarplicht weinig nieuwe informatie zal opleveren voor inlichtingendiensten,[294] terwijl de maatregel in art. 15 lid 1 E-privacyrichtlijn met het oog op terrorismebestrijding is getroffen. De gegarandeerde beschikbaarheid door dataretentie is al met al wel nuttig voor de opsporing van strafbare feiten, maar van een 'pressing social need' is nauwelijks sprake. Ik kan mij niet aan de indruk onttrekken, dat de wensen van de behoeftestellers sinds medio jaren '90 (zie par. 1.2.), het politieke klimaat na enkele terroristische aanslagen (zie par. 1.6.) en een voor de opsporing vanzelfsprekend nuttige uitbreiding van de beschikbaarheid de doorslag hebben gegeven tot het treffen van de maatregel, in plaats van een concrete, dringende behoefte in de maatschappij.[295]

Rechtvaardigt dataretentie ten behoeve van de opsporing van ernstige misdrijven de impact die de maatregel heeft op het recht op privacy van burgers? Gezien de in de parlementaire behandeling onderbelichte, maar de in par. 3.2.1. besproken aard van telecommunicatiegegevens en in par. 3.2.2. uiteengezette ernstige aard van de inbreuk op art. 8 lid 1 EVRM ligt de lat voor de weging van de proportionaliteit hoog. De effectiviteit van dataretentie maakt onderdeel uit van deze afweging. In de behandeling van het wetsvoorstel in de Eerste Kamer, en met name tijdens de expertbijeenkomst, komen echter enkele belangrijke technische aspecten aan het licht waaruit "scherpe conclusies"[296] kunnen worden getrokken voor wat betreft effectiviteit van dataretentie. Vele nieuwe vormen van telecommunicatie, zoals web based e-mail, buitenlandse chatprogramma's, fotouitwisselprogramma's via welke informatie uitgewisseld kan worden, social networking sites (Hyves) en niet in de laatste plaats VoIP diensten (Skype) vallen niet onder de bewaarplicht. Surfen over het web via een anonieme proxy server[297] buiten Europa kan hier ook toe gerekend worden. Juist meer ervaren criminelen, die eerder betrokken raken bij de ernstige criminaliteit die het Kabinet met de maatregel beoogd te bestrijden, zullen de bewaarplicht altijd weten te omzeilen.[298] Door Breyer en anderen wordt daarenboven aangegeven, dat de bewaarplicht zal leiden tot veel effectievere methoden van ontwijken van de bewaarplicht – bijvoorbeeld via anonimiseringstechnologieën.[299] En het relatief nieuwe fenomeen IP-spoofing, waarbij een gebruiker niet bewust is van het feit dat zijn IP-adres door iemand anders gebruikt wordt, zorgt ervoor dat handelingen op het internet nauwelijks herleid kunnen worden tot een persoon, nu het in de woorden van expert dhr. Niesen "vrijwel nooit met zekerheid is aan te tonen dat

---

[294] Zwenne & Schmidt 2005, p.298.
[295] Zie epiloog.
[296] *Kamerstukken I*, 2008-2009, 31 145, nr. E, p.2.
[297] Een proxy server is een server die tussen de computer en het internet staat. Bij gebruik van een proxy, wordt met een ander IP-adres over internet gesurft. Een lijst van proxy servers is te raadplegen via <http://www.stayinvisible.com/proxy_lists.html> [geraadpleegd juli 2009].
[298] *Kamerstukken I*, 2008-2009, 31 145, nr. D, p.14. In dezelfde zin ook Breyer 2005, p.369.
[299] Breyer 2005, p.371; Zwenne & Schmidt 2008.

telecommunicatiegegevens wel of niet aan een contractant toebehoren."[300] Hij vervolgt dat het "zeer wel mogelijk" is dat er onjuiste conclusies worden getrokken uit telecommunicatiehandelingen. Al met al treft de maatregel onschuldige burgers, die gebruik maken van meer traditionele vormen van telecommunicatie zoals (mobiele) telefonie en e-maildiensten van hun ISP, disproportioneel in hun privacybelang.

Deze opmerkingen dienen enigszins gerelativeerd te worden. Effectiviteit zal namelijk niet alleen afgemeten moeten worden aan de beschikbaarheid van gegevens; er dient ook gekeken te worden naar de waarde van beschikbare gegevens voor het opsporingsonderzoek. Het is daarbij aan de behoeftestellers, dan wel het Kabinet, om dit bewijs te leveren. Behoudens het door velen – onder meer de CDA-fractie in de Eerste Kamer[301] – bekritiseerde rapport 'wie wat bewaart, heeft wat' van de Erasmus Universiteit Rotterdam naar het gebruik van telecommunicatiegegevens in strafzaken, is de effectiviteit van de dataretentiemaatregel om ernstige misdrijven en terrorisme te kunnen bestrijden nooit bewezen. De effectiviteit van de maatregel werd in de literatuur zelfs vaak al in twijfel getrokken.[302] Resumerend is de effectiviteit van dataretentie niet geheel duidelijk, terwijl de inbreuk op privacy van juist onschuldige burgers onevenredig hoog is.

In het licht van de subsidiariteit bestaan er kortweg geen minder inbreukmakende alternatieven om telecommunicatiegegevens op deze schaal voor opsporingsonderzoek beschikbaar te krijgen.[303]

Dat zowel de dataretentierichtlijn als het wetsvoorstel geen beperkingen van de inbreuk bevatten verzwakt de rechtvaardiging van de in deze wetgeving getroffen dataretentiemaatregelen door art. 8 lid 2 EVRM volgens Van Hoboken aanzienlijk.[304] Waar mogelijk moet de inbreuk beperkt worden, zo zet het EHRM ook in de recente zaak *S. and Marper v. The United Kingdom* uiteen.[305] In par. 2.3.2. werd al stilgestaan bij de minimumharmonisatie in art. 5 dataretentierichtlijn, waardoor de categorieën te bewaren telecommunicatiegegevens door de richtlijn niet beperkt zijn. Art. 12 lid 1 dataretentierichtlijn biedt de expliciete mogelijkheid voor lidstaten om een langere bewaartermijn dan de in art. 6 voorgeschreven maximale 24 maanden te hanteren, waarbij de Commissie op grond van lid 2 zal onderzoeken hoe dit de werking van de interne markt beïnvloedt. Van een strikte beperking van de bewaartermijn is derhalve evenmin sprake. Het argument van Van Hoboken is des te sterker in het licht van het wetsvoorstel. Waar het HvJEG oordeelde dat de dataretentierichtlijn geen restricties op de toegang bevat en de A-G van mening is dat niet dit mogelijk was vanwege strijd met het Europese constitutionele recht (zie par. 1.5.), kent de nationale wetgever dergelijke belemmeringen niet. Dit is een relevante constatering voor rechtvaardiging van de in par. 3.2.3. gesignaleerde aandachtspunten, die onder par. 3.3.2. aan de orde komen.

Uit de overwegingen van het EHRM in de zaak *S. And Marper v. The United Kingdom* volgen enkele relevante parallellen in algemene zin voor de beoordeling van de proportionaliteit van de

---

[300] *Kamerstukken I*, 2008-2009, 31 145, nr. D, p.11.
[301] *Kamerstukken I*, 2008-2009, 31 145, nr. B, p.3: "het rapport van de EUR kan – naar de mening van de leden van de CDA-fractie – in het geheel niet al seen onderbouwing van een langere dan de minimumtermijn worden beschouwd." Het rapport is bovendien in wetenschappelijke kringen fel bekritiseerd, bijvoorbeeld door Smits 2006, p.154.
[302] O.m. art. 29 WP Opinion 9/2004, 15 nov. 2004; art. 29 WP Opinion 4/2005, 21 okt. 2005; Breyer 2005; Groothuis 2006; Amici Curiae 2008. Een tegengesteld geluid komt van Bignami, die zich kan vinden in het ontbreken van bewijs van de noodzaak van de maatregel, omdat dit "unrealistic" zou zijn. Bignami 2007, p.251. Mijns inziens druist dit in tegen het vereiste van noodzakelijkheid, zoals besproken gesteld door art. 8 lid 2 EVRM.
[303] *Kamerstukken II*, 2006-2007, 31 145, nr. 9, p.19.
[304] Van Hoboken 2009; Drijber 2009, p.261.
[305] EHRM S. and Marper v. The United Kingdom, nr. 99.

bewaarplicht.[306] Het EHRM oordeelde dat er sprake was van schending van art. 8 EVRM, onder meer vanwege de in par. 119 genoemde overwegingen:

> 119. In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed.[307] In particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

De dataretentierichtlijn verschilt enerzijds van de hierboven geciteerde situatie vanwege het stellen van een grens aan de lengte van het bewaren van de gegevens, ook al bestaat voor lidstaten altijd de mogelijkheid om de bewaartermijn te verlengen via art. 12 dataretentierichtlijn. Anderzijds betreft dataretentie van telecommunicatiegegevens niet alleen personen die ooit in aanraking kwamen met politie of justitie, maar alle gebruikers van telecommunicatie. Toch zijn de overeenkomsten het meest opvallend: ongeacht een verdenking, de leeftijd, crimineel verleden of aard van het misdrijf waarop opsporingsonderzoek zich richt worden telecommunicatiegegevens bewaard – terwijl het vrijwel onmogelijk is voor normale burgers om onder de bewaarplicht uit te komen en het nog maar de vraag is of er toereikende, onafhankelijk toezichtmechanismes van kracht zijn op de dataretentieverplichtingen (zie par. 3.2.3. en par. 3.3.2.5., waar besproken wordt dat dit in gelijke zin geldt voor de uitoefening van vorderingsbevoegdheden door opsporingsinstanties). Negatieve effecten op de persoonlijke- en culturele vorming van minderjarigen vormden voor het EHRM in de *S. and Marper* uitspraak gronden om een schending van art. 8 EVRM aan te nemen,[308] en zijn bij dataretentie eveneens aan de orde (zie par. 3.2.2.).

Van meer fundamentele aard is de observatie van het EHRM, dat de bescherming van art. 8 EVRM "unacceptably weakened" geraakt met het zonder meer – "at any cost" – aanwenden van moderne technologieën voor de retentie van persoonsgegevens ten dienste van de opsporing.[309] Met de onderhavige database was in de ogen van het EHRM duidelijk de grens bereikt. Waar technologie nieuwe mogelijkheden voor de opsporing faciliteert is dit slechts toegestaan na een nauwkeurige belangenafweging van de mogelijke implicaties van dergelijke maatregelen. Dataretentie is als zodanig nooit onderworpen aan een nauwkeurige belangenafweging en zou, evenals de retentie van biometrische gegevens, een onacceptabele afzwakking van de bescherming van het recht op privacy zoals neergelegd in art. 8 EVRM kunnen behelzen. Met deze uitspraak van december 2008 lijkt het EHRM de opvatting te zijn toegedaan, dat zodra wij als maatschappij dergelijke maatregelen laten

[306] Aangezien telecommunicatiegegevens meer inzicht gegeven in de persoonlijke levenssfeer van gebruikers dan vingerafdrukken (zie par. 3.2.1.), gelden de overwegingen uit EHRM S. and Marper v. The United Kingdom ook voor telecommunicatiegegevens.
[307] EHRM S. and Marper v. The United Kingdom, nr. 119. De eerste woorden 'in this respect' slaan op de toetsing van de proportionaliteit.
[308] EHRM S. and Marper v. The United Kingdom, nr. 124.
[309] EHRM S. and Marper v. The United Kingdom, nr. 112.

bestaan, de persoonlijke levenssfeer dusdanig uitgehold wordt dat er überhaupt nauwelijks meer sprake kan zijn van een recht op privacy.[310]

Het BVerfG past in de eerder besproken zaak in 2008 grote terughoudendheid toe in de toetsing van de implementatiewet aan de Duitse grondwet omdat het geen constitutionele crisis wil ontketenen, nu de implementatie wordt voorgeschreven door gemeenschapsrecht.[311] Daarom wordt het bewaren voorlopig toegestaan, terwijl de toegang voorlopig wordt beperkt (zie par. 3.3.2.). Het Kabinet ziet zich met deze uitspraak onterecht gesterkt in zijn opvatting dat de beperking van de persoonlijke levenssfeer niet zozeer op de bewaarplicht zelf maar pas op het gebruik van de gegevens door opsporingsdiensten slaat.[312] Het BVerfG oordeelt namelijk dat er aan de bewaarplicht nog niet dermate "besonderes schwerweigender und irreparabler Nachteil" verbonden is, dat het BVerfG niet het risico moet lopen de "größter Zurückhalltung" inzake zijn "Entscheidungskompetenz" in dit vraagstuk te buiten te gaan.[313]

Zodra het Europees Hof van Justitie in Luxemburg zich zal uitspreken over de verenigbaarheid van de dataretentierichtlijn dan wel het wetsvoorstel met art. 8 EVRM, is er geen sprake van een terughoudende toetsing of een competentievraagstuk, nu de maatregel in de vorm van een richtlijn – een Eerste pijler maatregel – vorm heeft gekregen.[314] Ongeacht het Kabinetsstandpunt heeft het HvJEG, dat zich in de komende jaren hoogstwaarschijnlijk zal uitspreken over dit vraagstuk,[315] sterke rationele argumenten tot zijn beschikking om de noodzakelijkheid en de proportionaliteit van dataretentie in twijfel te trekken en op basis daarvan te oordelen dat dataretentie onverenigbaar is met art. 8 EVRM.

### 3.3.2. Toegang en de hernieuwde verhouding met beschikbaarheid

Vanwege de constatering dat er sterke rationele argumenten bestaan om de inbreuk van dataretentie an sich niet te rechtvaardigen, zal de verenigbaarheid van het samenspel tussen nationale implementaties en de toegang tot de verplicht bewaarde telecommunicatiegegevens in die lidstaten met art. 8 EVRM nog problematischer zijn.

Het BVerfG komt in de reeds aangehaalde voorlopige voorziening tot de conclusie dat het de toegang tot verplicht bewaarde gegevens moet beperken totdat de verenigbaarheid van de maatregel met de Duitse grondwet aan toetsing is onderworpen, en gebiedt daartoe onder meer een grondige (privacy) impact assessment door de overheid.[316] Volgens BVerfG weegt het nadeel dat het publieke opsporingsbelang hiervan ondervindt aanmerkelijk minder zwaar dan het nadeel voor de grondrechten van burgers. Mutatis mutandis dienen de gevolgen voor de persoonlijke levenssfeer van burgers eerst inzichtelijk gemaakt te worden door een grondige, onafhankelijke en wetenschappelijk gedegen analyse, voordat het wetsvoorstel in werking kan treden. Problematisch daarbij is de implementatieplicht die op de wetgever rust.

---

[310] Breyer wijst dan ook terecht op het ontbreken van wetenschappelijke kennis over zowel de positieve als negatieve gevolgen van dataretentie, en dat onomkeerbare maatregelen die indruisen tegen grondrechten van burgers op dat moment nog niet geoorloofd zouden moeten worden, Breyer 2005, p.371; Amici Curiae 2008, p.7.
[311] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 127.
[312] *Kamerstukken II*, 2008-2009, 331 145, nr. C, p.26.
[313] Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 140, 148, 150.
[314] Zie par. 1.4.
[315] Van Hoboken 2009.
[316] Bundesverfassungsgericht 11 maart 2008, 1 BVerfG 256/08, par. 160.

Breyer wijst terecht op het ontbreken van wetenschappelijke kennis over zowel de positieve als negatieve gevolgen van dataretentie, en dat onomkeerbare maatregelen die indruisen tegen grondrechten van burgers op dat moment nog niet geoorloofd zouden moeten worden.[317] In het verlengde hiervan is een eventuele margin of appreciation van lidstaten niet ter sprake, nu de impact van dataretentie niet met zekerheid is vast te stellen.

Deze scriptie doet desalniettemin een bescheiden eerste poging tot zo'n analyse, om de noodzaak van vervolgonderzoek te onderstrepen. Omdat dit onderzoek niet kan ingaan op alle aan telecommunicatiegegevens gerelateerde vorderingsgrondslagen in het wetsvoorstel en het Wetboek van Strafvordering, wordt hier specifiek ingegaan op de rechtvaardiging van de vijf ontwikkelingen die aan het einde van par. 3.2.3. werden opgesomd en grotendeels ook al in hoofdstuk 2 ter sprake kwamen.

#### *3.3.2.1. Bewaartermijn twaalf maanden: art. 13.2a lid 3 jo. 13.4 lid 3 Tw (nieuw)*

Bij de behandeling in de Eerste Kamer vormen noodzaak en proportionaliteit van de in de Tweede Kamer uiteindelijk overeengekomen bewaartermijn van twaalf maanden belangrijke discussiepunten. De Minister brengt steeds naar voren dat twaalf maanden wat hem betreft gezien moet worden als een minimum en openbaart zelfs de mogelijkheid de termijn bij een van de evaluatiemomenten omhoog bij te stellen.[318] Hij onderbouwt het nut en de noodzaak van zijn zienswijze niet met harde cijfers, omdat het "niet alleen een kwantitatieve maar ook om een kwalitatieve vraag gaat."[319] De adviezen van behoeftestellers en allerlei voorbeelden vormen de kern van de onderbouwing het Kabinet om een langere termijn dan zes maanden te hanteren. Zo vergt de opsporing van specifieke complexe vormen van veelal georganiseerde misdaad een lange termijn. Daarnaast komt de "behoefte"[320] voor een lange termijn voort uit opsporingsonderzoek waarbij internationale samenwerking nodig is en de zogenaamde cold cases. Voorts bestaat de mogelijkheid dat later in het onderzoek onbekende telefoons worden aangetroffen of dat het onderzoek überhaupt pas later op gang komt. Verbazingwekkend genoeg stelt de Minister dat een langere bewaarplicht gunstig kan zijn voor verdachten en burgers, omdat zij hun onschuld kunnen bewijzen en de gegevens bij een langere termijn minder vaak gevorderd zullen worden door opsporingsdiensten, omdat de vrees niet bestaat dat zij niet meer beschikbaar zijn.[321]

Voor de voorbeelden van de Minister is niet alleen steeds een tegenargument te verzinnen,[322] bovendien zijn zij te scharen onder het aangeven van het "nut" of de "behoefte" van een langere termijn

[317] Breyer 2005, p.371; Amici Curiae 2008, p.7.
[318] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.3/7; nr. C, p.20.
[319] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.4.
[320] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.7.
[321] Te vinden in: *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.4-7; *Kamerstukken II*, 2007-2008, 31 145, nr. 9, p.14-15.
[322] De georganiseerde misdaad zal de bewaarplicht juist kunnen omzeilen door veel modernere vormen van telecommunicatie te gebruiken, zoals in par. 3.3.1.2. werd besproken. Dat er later in het onderzoek sprake kan zijn van nieuwe ontwikkelingen, is altijd het geval en vormt op zich geen argument voor het verlengen van een termijn: er zal immers altijd sprake kunnen zijn van bepaalde omstandigheden die het opsporingsonderzoek in de weg zitten. Nu telecommunicatiegegevens een steeds centraler onderdeel van het opsporingsonderzoek vormen, zal de situatie dat de met betrekking tot de verdachte gegenereerde telecommunicatiegegevens nog niet zijn ingezien door behoeftestellers zelden of nooit voorkomen. Als uit die gegevens blijkt dat een verdenking op onjuiste gegevens gebaseerd is, wordt de aandacht van het opsporingsonderzoek verplaatst naar andere verdachten. Bovendien wordt de notificatieplicht veronachtzaamd door het OM, waardoor de verdachte, nog voordat hij verdacht wordt, vaak niet eens weet of zijn

dan de minimumtermijn, overigens duidingen die de Minister zelf bezigt.[323] Ongetwijfeld is de opsporing gebaat bij een langere bewaartermijn, en zijn daar enkele concrete situaties te bedenken die dit aantonen. Maar volgens vaste jurisprudentie van het EHRM is nut nog geen noodzaak. De noodzaak van een langere termijn is met de genoemde voorbeelden van de Minister niet hard gemaakt. Leidt het ontbreken van verplicht bewaarde telecommunicatiegegevens tot het niet kunnen oplossen van een significant deel van de in Nederland gepleegde ernstige misdrijven of terroristische aanslagen? De harde cijfers (zie par. 3.3.1.) en de bevindingen van het Stratix onderzoek uit 2003, dat concludeerde dat aanbieders in de praktijk aan vrijwel alle toegangsverzoeken van opsporingsinstanties kunnen voldoen (zie par. 2.2.1.), weerspreken een bevestigend antwoord op deze vraag.

De al besproken rationele argumenten in het kader van het ontbreken van de noodzaak van een bewaarplicht, gelden evenzeer bij een bespreking van de rechtvaardiging van de lengte van de termijn. Evenals bij de totstandkoming van de dataretentierichtlijn (zie par.1.6.), was het recht op privacy voor de Minister nooit maatgevend: "de consequenties van de wettelijke bewaarplicht voor de bescherming van de persoonlijke levenssfeer mogen naar mijn mening niet worden overtrokken."[324] In par. 3.2.2. bleek al het gebrekkige redenering van de Minister met het oog op de inbreuk die alleen al het opslaan van gegevens maakt. De aard van de inbreuk is veel zwaarder dan de Minister doet voorkomen, dientengevolge moet de rechtvaardiging onder lid 2 aan strengere eisen voldoen. In dit verband verdient de vage grens tussen toegang en gebruik, zoals in par. 2.1. al werd besproken, vermelding. Eenmaal opgevraagd, belanden telecommunicatiegegevens in het gebruiksregime van onder meer de Wet politiegegevens. Na bevraging van de gegevens worden bewaartermijnen de facto verlengd met minimaal één jaar oplopend tot vijf jaar op grond van art. 8 jo. art. 9 jo. art. 10 Wet politiegegevens.

Een rationele analyse van de noodzaak en proportionaliteit van de maatregel kunnen een bewaarplicht op zichzelf (zie par. 3.3.1.), laat staan een langere termijn dan de minimale van zes maanden, moeilijk rechtvaardigen. De art. 29 WG adviseert telecommunicatiegegevens zo kort mogelijk te bewaren, om verenigbaarheid met art. 8 EVRM niet te riskeren.[325] Het verdient aanbeveling om de bewaartermijn zoveel mogelijk te beperken, aangezien een ruimere termijn verenigbaarheid met art. 8 EVRM in de problemen kan brengen.

#### *3.3.2.2. Kwalificatie 'ernstige misdrijven': aansluiting bij art. 67 lid 1 Sv*

De verwijzing naar het merkwaardige art. 67 lid 1 Sv (zie par. 2.3.3. en par. 3.2.3.) strookt niet met de door de Minister gegeven doel van de dataretentiemaatregel.[326] De maatregel zou nodig zijn bij bepaalde categorieën ernstige misdrijven en de gevallen waarin misdaad doorgaans een grensoverschrijdend karakter heeft, maar de reikwijdte van de toegangsbevoegdheden wordt niet tot deze categorieën delicten begrensd. De indruk ontstaat, dat nut prevaleert boven de 'pressing social need'. Er is derhalve geen sprake van beperking van de inbreuk op art. 8 lid 1 EVRM. Mogelijk versterkt dit chilling effecten, nu bij burgers de indruk kan ontstaan dat opsporingsdiensten in vrijwel alle

---

gegevens worden ingezien (zie par. 3.3.2.5.), Deze theoretische constructies vormen nog geen sluitend bewijs om het recht op privacy dusdanig in te perken.

[323] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.3.

[324] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.8.

[325] Art. 29 WP Opinion 3/2006, 25 mrt. 2006, p.3.

[326] *Kamerstukken I*, 2008-2009, 31 145, nr. F, p.4-7; *Kamerstukken II*, 2007-2008, 31 145, nr. 9, p.14-15.

gevallen toegang tot telecommunicatiegegevens kunnen afdwingen. De art. 29 WG adviseert de term 'serious crime' helder af te bakenen, omdat een te ruim begrip onverenigbaar is met art. 8 EVRM.[327] Deze alternatieve benadering is gekozen in bijvoorbeeld Denemarken, Spanje, Portugal en Finland.[328] De optelsom van deze constateringen is dat beoordelingsvrijheid bij de rechtvaardiging van de verwijzing naar art. 67 lid 1 Sv voor de kwalificatie van 'ernstige misdrijven' gering kan zijn, aangezien het doel van de maatregel, de aard van de inbreuk op de zelfontplooiing en consensus binnen andere lidstaten in deze belangrijke beoordelingscriteria zijn. Zoals Jacobs & White schrijven, is het moeilijk om vooraf vast te stellen hoe het EHRM hierover zal oordelen.[329] Rechtsvergelijkend onderzoek naar het bestaan van een consensus binnen afbakening van de term 'ernstige misdrijven' kan meer zekerheid geven.[330] Vooralsnog zijn de gronden voor de verwijzing naar art. 67 lid 1 Sv in ieder geval niet "relevant and sufficient." Mijns inziens is het vasthouden aan de verwijzing naar art. 67 lid 1 Sv moeilijk te rechtvaardigen onder art. 8 lid 2 EVRM.

#### *3.3.2.3. Vorderen verplicht bewaarde gebruiksgegevens door opsporingsambtenaren*

Een uitbreiding van de vorderingsbevoegdheid van actuele naar verplicht bewaarde gegevens strookt niet met het vereiste van een beperking van de inbreuk van dataretentie. De drempels voor de toegang tot gebruiksgegevens zijn al ruim: betrokkenheid bij de verdachte van 'een misdrijf' is voldoende. Deze drempel voor de toegang komt niet overeen met het doel van de dataretentiemaatregel, de bestijding van ernstige misdrijven. Eveneens ter sprake bij de weging van de proportionaliteit is het zwaarder worden van de test, naarmate het karakter van de inbreuk ernstiger is. Dit kan onderverdeeld worden in drie deelgebieden, volgt uit de uitspraak van het EHRM in de zaak *Vogt v. Germany*.[331] Alhoewel de data in kwestie (1) gebruiksgegevens betreffen, die minder inbreukmakend zijn dan verkeers- of locatiegegevens, is de reikwijdte (2) van de maatregel gigantisch: van alle gebruikers, ongeacht hun status (3), worden gebruiksgegevens bewaard die onder lage voorwaarden bij het CIOT opgevraagd zouden kunnen worden. Betrokkenheid bij de verdachte van een misdrijf is voldoende, de gebruiksgegevens van alle telecommunicatiegebruikers zijn beschikbaar.

De ernst van de potentiële inbreuk is gering qua soort gegevens, groot qua bereik – met name gezien het karakter van de bevoegdheid als eerste stap in het opsporingsonderzoek (zie par. 2.2.2.). De inbreuk wordt als deze kans zich concretiseert nauwelijks beperkt; onderwijl hoeven burgers niet op de hoogte gesteld te worden van de inzage door opsporingsinstanties in gebruiksgegevens op grond van art. 126bb Sv. De bevoegdheid wordt jaarlijks circa twee miljoen keer gebruikt, een uitbreiding van de bevoegdheid zal hoogstwaarschijnlijk leiden tot een scherpe toename – nog sterker dan de huidige jaarlijkse toename van 24,7% – van de uitoefening van de bevoegdheid. Deze vergaande gevolgen maken een margin of appreciation lastig voor te stellen, al is rechtsvergelijkend onderzoek naar het bestaan van een consensus binnen het vorderen van gebruiksgegevens in de lidstaten gewenst om deze

[327] Art. 29 WP Opinion 3/2006, 25 mrt. 2006, p.3.
[328] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.4/5.
[329] Jacobs & White 2006, p.233.
[330] In de zaak *S. and Marper v. The United Kingdom* was het bestaan van consensus over de bewaring van biometrische gegevens een eenvoudige grond om de veel verdergaande inbreuken in het Verenigd Koninkrijk te verwerpen, EHRM S. and Marper v. The United Kingdom, nr. 112.
[331] EHRM Vogt v. Germany, nr. 48; Daarnaast bijvoorbeeld in EHRM Silver a.o. v. The United Kingdom, nr. 88.

voorstelling zeker te stellen.[332] Al met al kan de inbreuk op de persoonlijke levenssfeer door het vorderen van verplicht bewaarde gebruiksgegevens door opsporingsambtenaren niet gerechtvaardigd worden door art. 8 lid 2 EVRM, en dient de overheid te garanderen dat het verplicht bewaarde telecommunicatiegegevens niet beschikbaar zal stellen voor de vorderingsgrondslag van art. 126na lid 1 Sv.

#### *3.3.2.4. Toegang tot locatiegegevens gedurende mobiele communicatie*

Dat het wetsvoorstel aanbieders verplicht locatiegegevens *tijdens* mobiele telefonie te bewaren, is een problematisch gegeven (zie par. 2.3.2.). Niet zozeer omdat de bijlage hiermee verder gaat dan de richtlijn, maar het is juist deze categorie telecommunicatiegegevens die na aandringen van het Europees Parlement niet werd opgenomen in art. 5 dataretentierichtlijn vanwege een te vergaande inbreuk op de persoonlijke levenssfeer van gebruikers. Alhoewel met betrekking tot deze categorie al de bijzondere bewaarplicht inzake mobiele communicatie van kracht is, vormt alleen al het gedurende twaalf maanden bewaren van deze gegevens volgens het CBP "een te indringende, alomvattende verborgen surveillance van de verplaatsingen van zeer grote aantallen onverdachte burgers."[333] De termijn van de bijzondere bewaarplicht wordt met het wetsvoorstel met negen maanden uitgebreid. Dat het bewaren van deze categorie telecommunicatiegegevens te ver gaat voor zowel de Europese wetgever als de nationale toezichthouder, toont aan dat het wél opnemen van deze gegevens in de bijlage bij het wetsvoorstel niet zonder controverse is.

Het EHRM heeft verdragspartijen in de zaak *Klass a.o. v. Germany* een ruime, maar niet ongelimiteerde beoordelingsvrijheid gegeven op het specifieke terrein van de nationale veiligheid.[334] Het zal de wetgever op basis van deze uitspraak kunnen worden toegestaan om de beschikbaarheid van deze categorie telecommunicatiegegevens voor de AIVD en de MIVD voor twaalf maanden te garanderen, mits de rechtvaardiging van deze beschikbaarheid "relevant and sufficient" is. De aangevoerde gronden zouden het EHRM moeten overtuigen dat er "exceptional cirumstances" aan de orde zijn, en dat er sprake is van "adequate and effective safeguards."[335] Het is overigens nog maar de vraag, of aan dit laatste kan worden voldaan (zie par. 3.3.2.5.).

Dat negen maanden extra locatiegegevens met het wetsvoorstel eveneens beschikbaar komen voor de opsporing, is een andere kwestie. De aard van juist deze inbreuk maakt onverenigbaarheid aannemelijk, aangezien hij gepaard gaat met omstandigheden als het niet strikt beperkt zijn van de toegang tot 'ernstige misdrijven', de gebrekkige controle op opsporingsdiensten en het laten vallen van de verdachte-eis in de Wet vorderen gegevens telecommunicatie. Het zal slechts in hoogst uitzonderlijke gevallen voorkomen dat opsporingsdiensten geconfronteerd worden met een strafbaar feit dat de nationale veiligheid in gevaar brengt. Opsporing an sich vormt juist een extra aanleiding voor het EHRM om verdragsstaten een striktere beoordelingsvrijheid op te leggen.[336] Dit is des te plausibeler, gezien het door de Europese wetgever en het CBP ingenomen standpunt. Bovendien is reeds betoogd

[332] EHRM S. and Marper v. The United Kingdom, nr. 112.
[333] CBP 2007, p.7.
[334] EHRM Klass a.o. v. Germany, nrs. 48-50.
[335] Jacobs & White 2006, p.237.
[336] EHRM S. and Marper v. The United Kingdom, nr. 103.

dat hier niet alleen de privacy van burgers, maar ook hun recht op vrije vergadering en vereniging aan de orde kan zijn (zie par. 3.2.2.). De toegang tot deze categorie telecommunicatiegegevens van de afgelopen twaalf maanden zal daarom beperkt moeten worden tot de AIVD en MIVD, om onverenigbaarheid met art. 8 EVRM niet te riskeren. Rechtsvergelijkend onderzoek naar de verplichte bewaring van deze categorie, en de daaraan gekoppelde toegangscriteria, kan wederom meer zekerheid bieden op dit punt.

#### *3.3.2.5. Het gebrek aan controle op de opsporingsdiensten*

Uit vaste jurisprudentie van het EHRM volgt dat het wetsvoorstel in overeenstemming dient te zijn met de algemene beginselen van de rechtsstaat, oftewel waarborgen tegen willekeur en misbruik moet bevatten.[337] Gezien de aard van de inbreuk van dataretentie, de toegang door opsporingsdiensten en de hiervoor besproken specifieke omstandigheden in de Nederlandse situatie die de inbreuk niet beperken maar verhevigen, heeft de wetgever een positieve verplichting deze waarborgen tegen willekeur en misbruik zeer nauwkeurig te verankeren.[338]

Juist omdat de burger in eerste instantie niets merkt van de op art. 8 lid 1 EVRM inbreukmakende toegang tot de hem betreffende telecommunicatiegegevens, en deze niet goed kan aanvechten, is deugdelijke controle van essentieel belang.[339] In de recente uitspraak *Liberty a.o. v. The United Kingdom* oordeelt het EHRM dat "the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge."[340] Deze verplichtingen gelden voor alle "general programs of surveillance."[341]

De term 'public scrutiny and knowledge' is mijns inziens te splitsen in twee deelgebieden. Allereerst het individuele perspectief, dat ook raakt aan het recht op een daadwerkelijk rechtsmiddel, zoals neergelegd in art. 13 EVRM. De Minister stelt dat er voor individuele burgers sprake is van voldoende mogelijkheden om te achterhalen of er met betrekking tot individuen opsporingshandelingen worden verricht, namelijk via de notificatieplicht van opsporingsinstanties en inzagerechten van de burger op grond van de Wbp en Wet politiegegevens.[342] Uit de eindevaluatie door het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie (WODC) van de Wet bijzondere opsporingsbevoegdheden blijkt echter dat de notificatieplicht in de praktijk massaal wordt genegeerd, omdat dit geen prioriteit heeft binnen het OM en er geen sanctie staat op het uitblijven van notificatie.[343] Deze ontwikkeling is terecht bekritiseerd door onder meer Chavannes.[344] Voor het uitblijven van notificatie bestaat geen rechtvaardiging, te meer daar het hier raakt aan essentiële en algemene beginselen van de rechtsstaat, te weten waarborgen tegen "abuse of power" en ook art. 13 EVRM waarin het recht op een daadwerkelijk rechtsmiddel is neergelegd.[345] Blijkbaar vormt

[337] EHRM P.G. and J.H. v. France, nr. 97; EHRM Huvig v. France, nr. 52.
[338] EHRM Vogt v. Germany, nr. 48; Daarnaast bijvoorbeeld in EHRM Silver a.o. v. The United Kingdom, nr. 88 en EHRM S. and Marper v. The United Kingdom, nr. 103.
[339] Chavannes 2008, p.245.
[340] EHRM Liberty a.o. v. The United Kingdom, nr. 67.
[341] EHRM Liberty a.o. v. The United Kingdom, nr. 62-63.
[342] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.23.
[343] *Kamerstukken II*, 2004-2005, 30 164, nr. 5, p.7. Zie tevens par. 2.2.2.
[344] Chavannes 2008.
[345] EHRM Liberty a.o. v. The United Kingdom, nr. 69.

de persoonlijke levenssfeer van burgers een ondergeschikt belang in de afweging van opsporingsdiensten om telecommunicatiegegevens wel of niet op te vragen. Dan wijst de Minister op de rechterlijke toetsing van de bevoegdheden ex post, dat wil zeggen in de rechtszaal.[346] Koops & Buruma relativeren deze toetsing, nu onrechtmatig verkregen bewijs in de praktijk vrijwel altijd door de rechter toegestaan wordt.[347] Uit deze overwegingen volgt de wenselijkheid van uitgebreidere notificatieplichten en de sanctionering van het achterwege laten van notificatie, omdat dergelijke maatregelen de inbreuk op art. 8 lid 1 EVRM, onder meer het chilling effect (zie par. 3.2.2.), beperken en concrete waarborgen voor het individu tegen willekeur en misbruik van bevoegdheden vormen.

Op de tweede plaats is er een gemeenschappelijk perspectief. Waar het Agentschap Telecom toezicht houdt op de aanbieders via art. 15.1 Tw (art. 9 dataretentierichtlijn), baart het ontbreken van toezicht op de opsporingsdiensten zorgen. Naast het ontbreken van direct, onafhankelijk toezicht op opsporingsdiensten,[348] vermeldt de transponeringstabel bij het wetsvoorstel dat art. 10 en art . 14 dataretentierichtlijn "geen implementatie behoeven."[349] De statistische verantwoordingsplicht die in deze artikelen wordt geregeld is echter de belangrijkste methode om te controleren in hoeverre behoeftestellers in kwantitatieve zin gebruik of misbruik maken van de toegangsbevoegdheden.[350] Het Kabinet heeft toegezegd hier in een AMvB op terug te komen en wijst daarnaast op de algemene taak van het CBP om toezicht uit te oefenen op de naleving van wettelijke voorschriften; de vraag is of het CBP geëquipeerd is om deze taak bovenop een uitgebreid takenpakket uit te voeren. Dat de Minister het gebruik van telecommunicatiegegevens door inlichtingen- en veiligheidsdiensten karakteriseert als "staatsgeheim",[351] en dus bij voorbaat al uitsluit van onderwerping aan statistische controle, geeft weinig vertrouwen in de totstandkoming van deze AMvB.[352] Het op deze wijze afdoen van de onafhankelijke controle op uitoefening van de bevoegdheden door behoeftestellers, doen Zwenne & Schmidt vermoeden dat de regering dergelijke informatie zoveel mogelijk geheim wil houden.[353] Na de plenaire behandeling in de Tweede Kamer en de stellingname daarin van de Minister dat er sprake is van voldoende toezicht, is dit overigens geen onderwerp van gesprek meer geweest in de behandeling van het wetsvoorstel.[354] Mijns inziens rechtvaardigt dit de conclusie van Zwenne & Schmidt dat het Kabinet en het parlement "grote risico's nemen met de rechtsstatelijkheid van ons bestel." [355]

Buiten het belang van controle op opsporingsinstanties vanuit rechtsstatelijk oogpunt, heeft transparantie volgens Solove een gunstige uitwerking op de effectiviteit van de opsporing.[356] Enerzijds kunnen maatregelen onderzocht en verbeterd worden, anderzijds kan blijken dat een controversiële maatregel als dataretentie of datamining blijkbaar toch noodzakelijk is in een democratische samenleving. In dat geval zou de overheid hard kunnen maken dat burgers bepaalde schendingen van de grondrechten dienen te accepteren, omdat daarmee de democratische samenleving waarvan zij deel

[346] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.23.
[347] Koops & Buruma 2007, p.86 en de omvangrijke verwijzing naar jurisprudentie van de HR aldaar.
[348] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.18.
[349] *Kamerstukken I*, 2008-2009, 31 145, nr. A, p.8.
[350] Zwenne & Schmidt 2008, p.285.
[351] *Kamerstukken II*, 2006-2007, 31 145, nr. 3, p.19.
[352] Zwenne & Schmidt 2008, p.285.
[353] Zwenne & Schmidt 2008, p.285. De parallel met het ontbreken van toezicht op de aftapbevoegdheden, en het gebrek aan verantwoording door behoefstellers, schept evenmin vertrouwen. Zie Chavannes 2008, p.245.
[354] Handelingen II, 2006-2007, nr.83, p.5836.
[355] Zwenne & Schmidt 2008, p.285.
[356] Solove 2008, p.361.

uitmaken gediend wordt.[357] In aanvulling op alle bezwaren uit het oogpunt van de persoonlijke levenssfeer en de rechtsstatelijkheid van ons bestel, is het precies dit pragmatisme van Solove dat het ontbreken van controle op opsporingsinstanties en de geheimzinnigheid van het Kabinet hierover zo onbegrijpelijk maken – juist vanuit het oogpunt van deze behoeftestellers. Effectieve en legitieme opsporing lijken toch op zijn minst nastrevenswaardige doelen voor opsporingsdiensten. De burger mag dan wel – overigens onterecht – vinden dat hij niets te verbergen heeft,[358] maar wat hebben behoeftestellers dan te verbergen? Met Chavannes deel ik de opvatting dat de overheid in ieder geval een serieuzere poging moet doen tot transparantie, om aan te tonen dat men de rechtsstatelijke waarborgen, die het fundament van een vrije en democratische samenleving vormen, zal respecteren – te meer daar de noodzaak van de maatregel nog niet is aangetoond. "Alleen zo'n overheid verdient het voordeel van de twijfel."[359]

De controle op de opsporingsdiensten, van essentieel belang in een democratische rechtsstaat, is gebrekkig terwijl het individu onvoldoende in staat wordt gesteld om zich van de uitoefening van de opsporingsbevoegdheden ten koste van zijn privacybelang te vergewissen. Er lijkt in ieder geval geen sprake te zijn van nauwkeurig geformuleerde waarborgen tegen willekeur en misbruik, zoals vereist door het EHRM. Een margin of appreciation op dit punt is in het werkterrein van de nationale veiligheid denkbaar, gezien jurisprudentie van het EHRM, maar om deze redenen voor het ontbreken van controle op de activiteiten van de opsporingsdiensten moeilijk voor te stellen. [360] De risico's van gebrekkige controle op de uitoefening van de toegangsbevoegdheden, zowel in individuele gevallen als vanuit gemeenschappelijk initiatief, versterken de inbreuk op art. 8 lid 1 EVRM en maken rechtvaardiging van het wetsvoorstel met art. 8 lid 2 EVRM problematisch.

## *3.4. Rechtvaardiging en de politieke arena*

Met een reden is rationaliteit in de laatste paragrafen benadrukt. Voor de behandeling van het wetsvoorstel schreef de art. 29 WG al dat de dataretentierichtlijn grote ruimte laat voor verschillende interpretatie en implementatie ervan in nationale lidstaten.[361] Groothuis voorzag daarom in 2006 dat belanghebbenden in het kader van het proportionaliteits- en noodzakelijkheidsvereiste over elke kwestie eens of oneens kunnen zijn, niet op basis van rationele overwegingen maar aangezien het een politieke kwestie betreft.[362] De Minister onderschrijft dit evenzeer in zijn memorie van antwoord aan de Eerste Kamer: "een zeker verschil van inzicht zal mogelijk blijven over de uitkomsten van de afweging. Dat is vrijwel inherent aan het politieke proces."[363] Ook Zwenne & Schmidt signaleren in hun eerste bespreking van de dataretentierichtlijn in 2005 al "hoe weinig betekenisvol het vereiste van

[357] Idem.
[358] D. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, San Diego Law Review, Vol. 44, 2007.
[359] Chavannes 2008, p.245.
[360] EHRM Vogt v. Germany, nr. 48; EHRM P.G. and J.H. v. France, nr. 97; EHRM Huvig v. France, nr. 52; EHRM Silver a.o. v. The United Kingdom, nr. 88.
[361] Art. 29 WP Opinion 3/2006, 25 mrt. 2006, p.2.
[362] Groothuis 2006, p.808.
[363] *Kamerstukken I*, 2008-2009, 31 145, nr. C, p.20.

proportionaliteit soms kan zijn bij politieke dilemma's die verdeeldheid veroorzaken."[364] Zij verwachtten niet dat de discussie over het implementatievoorstel enkel beslecht zal worden door rationele analyses of juridische expertise, maar dat ideologische voorkeuren een belangrijke plek in de motiveringen van partijen zullen spelen.

De genoemde commentatoren lijken gelijk te krijgen. De zere plek in de regulering van privacy ligt in de politieke arena: het politieke klimaat kan van grote invloed zijn op het onderkennen of juist miskennen van schendingen van het recht op privacy. De ambivalente Europese regulering van de beschikbaarheid, die in hoofdstuk 1 aan de orde is gekomen, lijkt hieraan bij te dragen. Alhoewel de rechtvaardigingen van het Kabinet op belangrijke punten niet volstaan in het licht van art. 8 lid 2 EVRM, kunnen diezelfde rechtvaardigingen in de smaak vallen in de politieke arena. "Rechtwetenschappelijk gestoelde misgivings winnen aan concrete urgentie",[365] schrijven Zwenne & Schmidt na de voltooiing van de behandeling van het wetsvoorstel in de Tweede Kamer.

In de Eerste Kamer viel een van de grootste tegenstanders van de bewaarplicht, de reeds genoemde CDA-senator Franken, van zijn voetstuk in de politieke arena van de plenaire behandeling. De senator is zelfs hoogleraar Informatierecht aan de Universiteit Leiden. Zijn bewoordingen tijdens het debat tonen aan dat rationaliteit met betrekking tot het dataretentievraagstuk in de politieke arena vooralsnog ver te zoeken is:

> "Op deze inhoudelijke kritiek, die mijn fractie nog steeds heeft, wil ik eerst – zij het kort – ingaan en constateren, dat ik het eens ben met de manifesten die mijn vakbroeders en -zusters respectievelijk in NRC Handelsblad van 2 april 2008 en in Trouw van 26 juni 2009 hebben gepubliceerd. Het zou voor een wetenschappelijk debat aardiger zijn geweest wanneer ik het niet eens was met mijn naaste collega's, maar – en daarmee kom ik op mijn tweede punt – we moeten hier vandaag een politieke beslissing nemen en dan kiest mijn fractie – onder een aantal hieronder te noemen voorwaarden – voor *een standpunt, waarin politieke opportuniteit zwaarder weegt dan wetenschappelijke rationaliteit*."[366]

## 3.5. Conclusie

Vanuit grondrechtelijk perspectief zijn de dataretentierichtlijn en het wetsvoorstel problematische wetgevingsmaatregelen. Telecommunicatiegegevens geven diepgaand inzicht in de handelingen van gebruikers, terwijl de techniek de door de Europese richtlijnen en het wetsvoorstel veronderstelde scheiding tussen inhoudsgegevens en transportgegevens nog niet kan garanderen. De overstap van verplichte anonimisering/verwijdering naar verplichte bewaring van alle telecommunicatiegegevens kan het vertrouwen van de burger in vrije, ongemonitorde communicatie ernstig beschadigen alsmede de sociale exclusie van verdachten bewerkstelligen. Nu de rol van elektronische telecommunicatie in onze dagelijkse activiteiten de afgelopen jaren sterk verandert, bedreigt dataretentie steeds nadrukkelijker de handelingsvrijheid, identiteitsvorming en persoonlijke ontwikkeling van het individu – kernwaarden van de persoonlijke levenssfeer die het EHRM expliciet onder de beschermingsomvang van art. 8 lid 1 EHRM schaart.

De inbreuk op art. 8 lid 1 EVRM wordt in individuele gevallen geconcretiseerd door de

[364] Zwenne & Schmidt 2005, p.302.
[365] Zwenne & Schmidt 2008, p.285.
[366] Zie het stenogram van de plenaire behandeling van wetsvoorstel 31 145 op 6 juli 2009, p.21 (eigen cursivering), te raadplegen via: <http://www.eerstekamer.nl/behandeling/20090706/stenogram/f=y.pdf> [geraadpleegd juli 2009].

vordering van opsporingsdiensten. De geleidelijk opgeheven toegangsbelemmeringen in Nederland verhevigen de inbreuk op art. 8 lid 1 EVRM verhevigen, terwijl het wegnemen van beschikbaarheidsbelemmeringen de toegang tot telecommunicatiegegevens juist tot een waardevoller opsporingsmiddel maken.[367] Dat de uitoefening van toegangsbevoegdheden in Nederland nauwelijks is onderworpen aan controle, speelt dit 'chilling effect' in de kaart.

Nu de bewijslast voor de rechtvaardiging van de inbreuk op de privacy is verschoven naar de lidstaten, stelt de gebrekkige rechtvaardiging van het Kabinet teleur. Dit sterkt de bestaande twijfels over het wel of niet bestaan van een 'pressing social need' en de effectiviteit van de maatregel; twijfels die het Kabinet niet op overtuigende wijze heeft weerlegd. De criminaliteit daalt zelfs op alle fronten consequent sinds 2002, terwijl het OM steeds beter in staat is om misdrijven op te lossen. Tegelijkertijd kan de bewaarplicht eenvoudig omzeild worden via allerlei veelgebruikte nieuwe vormen van telecommunicatie, zoals VoIP en social networking sites. Daarbij kan identiteitsfraude, bijvoorbeeld middels IP-spoofing, leiden tot onjuiste verdenkingen op basis van telecommunicatiegegevens. Waar ervaren criminelen precies weten hoe aan de bewaarplicht te ontkomen, worden juist de onschuldige burgers met het wetsvoorstel disproportioneel getroffen in hun persoonlijke levenssfeer.

Evenals in de Europese context,[368] kiest het Kabinet in het dataretentievraagstuk een eenzijdige invalshoek: het gezichtspunt van de behoeftestellers wordt vertegenwoordigd, maar aan de inbreuk op de grondrechten van burgers wordt nauwelijks belang gehecht, deze wordt af en toe zelfs gebagatelliseerd. Terrorismebestrijding en de opsporing van strafbare feiten zijn van evident belang in een democratische samenleving, maar de grondrechten van burgers staan nu juist aan de wieg van diezelfde samenleving. Het Kabinet lijkt het instrumentaliseren van alle telecommunicatiehandelingen van burgers te rechtvaardigen met de notie dat dit inzicht 'nuttig' kan zijn voor opsporingsdiensten, zonder oog te hebben voor deze grondrechten. Het EHRM oordeelde in de zaak *S. and Marper v. The United Kingdom* dat de bescherming van art. 8 EVRM onacceptabele schade oploopt als het zondermeer aanwenden van nieuwe technologieën voor de opsporing wordt toegestaan. In lijn met dit oordeel is de wetgever mijns inziens tekortgeschoten in de zeer nauwkeurige belangenafweging die art. 8 en het EHRM vereisen. Dit geeft het HvJEG voldoende grond aan de verenigbaarheid van het wetsvoorstel te twijfelen.

De structurele ontkenning van de interdependentie van beschikbaarheid en toegang is een belangrijke, zo niet de belangrijkste misvatting in de zienswijze van het Kabinet. Waar de gemeenschapswetgever vanwege het recht van de pijlers van de Europese Unie deze scheiding aanbracht in de dataretentierichtlijn, had de wetgever met het wetsvoorstel de kans moeten grijpen om de toegang tot de gegevens te beperken. De deconstructie van beschikbaarheidsbelemmeringen had gebalanceerd moeten worden met specifieke restricties voor de toegang, alsmede systematische transparantie en andere vormen van controle op de opsporingsdiensten. In de politieke arena kan de wetgever nog wegkomen met haar gebrekkige rekenschap van de vereisten van art. 8 EVRM en het prevaleren van opportuniteit boven rationaliteit, maar in de rechtszaal is dit onwaarschijnlijk. Het EHRM en het BVerfG hebben deze interdependentie van beschikbaarheid en toegang in eerdere uitspraken immers wel meegewogen, en dezelfde of gelijksoortige dataretentieverplichtingen in strijd met de grondrechten van burgers verklaard.

[367] Zie par. 2.5.
[368] Zie par. 1.6.

In een bescheiden poging de wetgever te overtuigen van deze interdependentie, zijn in deze scriptie vijf knelpunten in de Nederlandse wetgeving aan het licht gebracht. Omdat problemen ook vragen om een oplossing, biedt het navolgende hoofdstuk enkele effectieve alternatieven. Niet alleen om de scheefgegroeide driehoeksverhouding letterlijk 'recht' te zetten, maar vooral om de dringende noodzaak tot vervolgonderzoek betreffende het samenspel tussen het wetsvoorstel en het Wetboek van Strafvordering in het licht van verenigbaarheid met art. 8 EVRM te onderstrepen.

# 4. HET ALTERNATIEVE PERSPECTIEF

Op basis van de bevindingen in met name par. 3.3.2. van het grondwettelijke perspectief, worden hier enkele alternatieven geboden voor de aldaar gesignaleerde knelpunten. Er is getracht te komen tot realistische aanbevelingen, in lijn met de adviezen van art. 29 WG,[369] om bij te dragen aan verenigbaarheid met art. 8 EVRM. In de keuze voor de alternatieven zijn zowel het opsporingsbelang als de grondrechten van burgers verdisconteerd, om zo te streven naar een balans tussen de persoonlijke levenssfeer van art. 8 lid 1 EVRM en het legitieme belang van de opsporing van lid 2. Het moge duidelijk zijn dat opsporing op zichzelf een legitiem belang is, en dat een te verregaande restrictie van de toegang zowel onrealistisch als onwenselijk is. Onrealistisch gezien het politieke klimaat, onwenselijk omdat slechts sporadische toegang tot verplicht bewaarde gegevens de Wet bewaarplicht telecommunicatiegegevens in zichzelf disproportioneel maakt: de balans tussen de maatschappelijke last van dataretentie enerzijds, het opsporingsbelang anderzijds slaat ook dan te ver door. Op een bepaald moment is er een soort juridisch 'break even'.

Gezien de bevindingen van het vorige hoofdstuk, vormt een beperking van de inbreuk op de persoonlijke levenssfeer de rode draad in de aanbevelingen. De alternatieven zijn gebaseerd op de vijf case studies van par. 3.3.2. Andere alternatieven zullen op basis van vervolgonderzoek gevonden moeten worden. Er ligt een belangrijke taak voor de wetenschap om het gehele spectrum van het samenspel tussen dataretentie en de strafvorderlijke bevoegdheden in beeld te brengen. Mijn voorspelling is dat dit vervolgonderzoek veel tijd zal vergen, vanwege het algehele karakter van de bewaarplicht en het feit dat de regulering van beschikbaarheid voortaan beheerst wordt door het opsporingsbelang. In de komende jaren is kritische reflectie op evaluaties van bestaande dataretentiemaatregelen en initiatieven tot nieuwe bewaarplichten noodzakelijk. Deze kritische reflectie dient zich niet te beperken tot het rechtswetenschappelijke onderzoeksdomein, maar multidisciplinair inzicht is vereist in de cumulatieve effecten van maatregelen op bijvoorbeeld de handelingsvrijheid en identiteitsvorming.[370]

## *4.1. Bewaartermijn naar zes maanden*[371]

De inbreuk op art. 8 lid 1 EVRM wordt beperkt door te opteren voor de kortst mogelijke bewaartermijn van zes maanden, zoals de art. 29 WG en het CBP in gelijke zin hebben aanbevolen.[372] De Eerste Kamer kan tijdens het plenaire debat op 7 juli a.s. afdwingen de bewaartermijn van twaalf maanden ex art. 13.2a lid 3 jo. 13.4 lid 3 wetsvoorstel naar zes maanden terug te brengen. De Eerste Kamer heeft dit

[369] Art. 29 WP Opinion 3/2006, 25 mrt. 2006, p.3; art. 29 WP Opinion 4/2005, 21 okt. 2005, p.8/9.
[370] Een mooi voorbeeld van dergelijk multidisciplinair onderzoek is de studie *Internet & Privacy* van Irma van der Ploeg en Jos de Mul, in: S. Zouridis, P. Frissen, N. Kroon, J. De Mul en J. van Wamelen (red.), *Internet En Openbaar Bestuur*, Den Haag 2001. In te zien via: <http://www2.eur.nl/fw/hyper/Download/05_Priva.pdf> [geraadpleegd juli 2009].
[371] Inmiddels heeft de tijd deze korte paragraaf ingehaald. GroenLinks-senator Strik heeft getracht deze novelle via een motie af te dwingen; een nipte meerderheid van CDA, VVD, SGP en ChristenUnie heeft de motie echter niet gesteund. Zie *Kamerstukken I*, 2008-2009, 31 145, nr. L.
[372] Art. 29 WP Opinion 3/2006, 25 mrt. 2006, p.3. CBP 2007.

instrument onlangs nog toegepast bij de implementatie van richtlijn 2006/32/EG over de slimme energiemeters, waarbij de privacy van burgers evenmin gegarandeerd was.[373] Via een dergelijke novelle wordt de verenigbaarheid van het wetsvoorstel met art. 8 EVRM dichterbij gebracht. De eerste evaluatie van het wetsvoorstel ex art. 13.9 wetsvoorstel is een volgend moment om de bewaartermijn aan te passen.

## *4.2. Heldere afbakening van de term 'ernstige misdrijven'*

'Purpose specification' vormt een van de hoekstenen van de Europese privacyregulering en is verankerd in art. 6 lid 1 sub b van de privacyrichtlijn 95/46/EG. De ongedefinieerde, open benadering van 'ernstige misdrijven' die de wetgever hanteert druist in tegen dit elementaire principe van het gegevensbeschermingsrecht. Er is daarom geen margin of appreciation voor de wetgever te verwachten, de gronden voor het ontbreken van een heldere afbakening van de term 'ernstige misdrijven' zijn in ieder geval niet "relevant and sufficient" om een beoordelingsvrijheid te staven.[374]

De art. 29 WG adviseert om het begrip 'ernstige misdrijven' af te bakenen.[375] De afbakening van het begrip ernstige misdrijven vormt een belangrijke manier voor de wetgever om zich rekenschap te geven van het beperkingsvereiste onder art. 8 EVRM. Bovendien is het in lijn met het in art. 13.2a lid 2 wetsvoorstel en door de Minister beschreven doel, namelijk dat verplicht bewaarde telecommunicatiegegevens alleen voor de bestrijding van ernstige criminaliteit ingezien kunnen worden en daartoe alleen toegankelijk zijn voor speciaal daartoe bevoegde personen bij de aanbieders op grond van art. 13.5 lid 2 sub b wetsvoorstel.[376]

In Denemarken, Spanje, Portugal en Finland[377] is ervoor gekozen de categorieën ernstige misdrijven expliciet in het implementatiewetsvoorstel. Deze benadering zou de wetgever moeten overwegen. Daarmee wordt bovendien teruggegrepen op de in art. 13.2a lid 2 wetsvoorstel verwoorde doelstelling van de bewaarplicht. Het Europees Parlement heeft bij de totstandkoming van de dataretentierichtlijn art. 2 lid 2 van dit Aanhoudingsbevel genoemd, waarin 24 categorieën ernstige misdrijven staan opgesomd.[378] De concrete aanbeveling luidt dan ook om deze 24 categorieën ernstige misdrijven over te nemen in een catalogus van ernstige misdrijven. Dit is te realiseren via een wetswijziging van de Telecommunicatiewet, waarin de term 'ernstige misdrijven' opgenomen wordt in een nieuw art. 13.2a lid 1 sub c wetsvoorstel. Tegelijkertijd dient de wetgever de verwijzing in art. 126n lid 1 Sv naar art. 67 lid 1 Sv te veranderen naar dit nieuwe art. 13.2a lid 1 sub c.

Dit behelst een substantiële inperking van de toegangsbevoegdheden van de Officier van Justitie. Al is een begrenzing van de toegang wenselijk vanuit grondrechtelijk perspectief; het is zeer te betwijfelen of de wetgever de toegangsbevoegdheden van opsporingsdiensten tot beschikbare telecommunicatiegegevens ooit nog aan strengere criteria zal onderwerpen ten opzichte van een

[373] Wet implementatie EG-richtlijnen energie-efficiëntie, 31 320. Zie tevens: <http://webwereld.nl/nieuws/56719/senaat-schakelt-verplichte-energiemeter-uit.html> [geraadpleegd juli 2009].
[374] EHRM S. and Marper v. The United Kingdom, nr. 112.
[375] Art. 29 WP Opinion 3/2006, 25 mrt. 2006, p.3.
[376] De waarborgen tegen misbruik en toegang door onbevoegden bij de aanbieders en derde private partijen moeten overigens nog geregeld worden in een AMvB op grond van art. 13.5 lid 4 wetsvoorstel.
[377] Kamerstukken I, 2008-2009, 31 145, nr. C, p.4/5.
[378] Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002, PB EG L 190/01.

moment daarvoor. Een herinrichting van de verstrekking van aanbieders lijkt realistischer.[379] Bij de verplichte verstrekking door aanbieders op grond van art. 13.2a Tw jo. 13.4 Tw zou gedifferentieerd kunnen worden naar de ernst van het misdrijf. Een mogelijkheid is om niet alle verplicht bewaarde telecommunicatiegegevens, maar alleen van de afgelopen drie of zes maanden te verstrekken indien er sprake is van een verdenking ex art. 67 lid 1 sub b of sub c Sv. Betreft de verdenking een delict waarvoor een maximale gevangenisstraf van vier jaren of meer is gesteld ex art. 67 lid 1 Sv, dan worden alle gegevens vertrekt. Er zou aansluiting gezocht kunnen worden met de praktijk, oftewel in hoeverre welke soorten telecommunicatiegegevens vandaag de dag beschikbaar zijn. Aangezien hier nauwelijks tot geen gegevens over bekend zijn, kan over de uitvoering niet sluitend worden geadviseerd.

Het belangrijke punt is dat alle verplicht bewaarde telecommunicatiegegevens, die nu nog niet beschikbaar zijn voor de opsporing van ernstige strafbare feiten, straks alleen verstrekt worden als het een verdenking van een daadwerkelijk ernstig strafbaar feit betreft – en dat de Officier van Justitie niet alle verplicht bewaarde gegevens krijgt in te zien van de betrokkene bij de verdachte van een delict als de 'heling van een goed' (zie par. 2.2.2.). Zo wordt de balans tussen een beperking van de inbreuk op de persoonlijke levenssfeer van (betrokkenen bij) de verdachte en het opsporingsbelang verdisconteerd. Op termijn zou een dergelijke maatregel in een wet in formele zin moeten worden vastgelegd, maar op de korte termijn kan dit geregeld worden in een nieuwe AMvB, gebaseerd op art. 13.4 lid 4 wetsvoorstel, getiteld "Besluit verstrekking gegevens telecommunicatie". Een nieuw artikel 3 in het Besluit vorderen gegevens telecommunicatie[380] is een andere mogelijkheid.

## 4.3. Art. 126na lid 1 Sv: alleen toegang tot actuele gebruiksgegevens

Het CIOT werd, het zij nog maar eens herhaald, twee miljoen maal geraadpleegd in 2007, met een jaarlijkse stijging van 24,7% sinds 2003.[381] Met een aanpassing van een AMvB zou het CIOT de gebruiksgegevens kunnen gaan bewaren, zodat opsporingsambtenaren ieder moment van de dag inzage kunnen krijgen van de gebruiksgegevens over de afgelopen 12 maanden van (de betrokkene bij) de verdachte van een misdrijf. "Nu er toch een bewaarplicht telecommunicatiegegevens van kracht is...". Dit heeft ingrijpende gevolgen voor de persoonlijke levenssfeer van telecommunicatiegebruikers, te meer vanwege dit lage toegangscriterium van art. 126na lid 1 Sv. Een initiatief hiertoe heeft zich vooralsnog niet aangediend, maar op de mogelijkheid van precies deze bevoegdheidsuitbreiding dienen beide kamers bedacht te zijn, gezien de frequentie waarmee gebruiksgegevens door opsporingsambtenaren worden opgevraagd. Op grond van art. 13.4 lid 3 wetsvoorstel wordt een conceptwijziging overigens wel aan beide kamers overgelegd, voordat tot een wijziging van de AMvB overgegaan kan worden.

## 4.4. Toegang tot locatiegegevens tijdens mobiele communicatie beperken

De toegang van opsporingsinstanties, bijvoorbeeld door de Officier van Justitie op grond van art. 126n lid 1 Sv, tot locatiegegevens tijdens mobiele telecommunicatie die in de afgelopen twaalf maanden zijn

[379] *Stb.* 2004, 394.
[380] *Stb.* 2004, 394.
[381] Zie par. 2.3.3. en par. 3.3.2.3.

bewaard lijkt onverenigbaar met art. 8 EVRM. Deze categorie moet in de huidige situatie drie maanden bewaard worden in het kader van de bijzondere bewaarplicht mobiele communicatie (zie par. 2.2.1.).[382] Het inzicht van opsporingsinstanties in de locatiegegevens van burgers tijdens hun mobiele telefoongesprekken wordt middels het wetsvoorstel met negen maanden uitgebreid.

In par. 3.3.2.4. is uiteengezet dat de wetgever in dit vraagstuk een begrensde beoordelingsvrijheid kan verwachten. Het verdient aanbeveling om de inbreuk te beperken, een belangrijke stap om onverenigbaarheid te ondervangen. Tegelijkertijd zal het Kabinet de bestandsanalyse ex art. 5 Besluit bijzondere vergaring nummergegevens telecommunicatie, ter identificatie van prepaid bellers, willen blijven faciliteren.[383] Daarom zal gezocht moeten worden naar een realistisch alternatief dat de huidige status quo handhaaft.

In die lijn worden hier twee alternatieven geboden. De indirecte route gaat langs de heldere afbakening van de term 'ernstige misdrijven' (zie par. 4.3.) en het herstellen van deugdelijke controle op opsporingsdiensten (zie par. 4.5.). Beide maatregelen werken als stabiliserende factoren op de ernst van deze inbreuk, en passen binnen de vier factoren die het EHRM laat meewegen bij de toekenning van een margin of appreciation (zie par. 3.3.). Als directe route kan de gegevensverstrekking door aanbieders aan de Officier van Justitie beperkt worden tot de locatiegegevens die gedurende de afgelopen drie maanden gegenereerd zijn. Dit is mogelijk door aan art. 2 sub e Besluit vorderen gegevens telecommunicatie de hieronder gecursiveerde zinsnede toe te voegen, zodat lid 2 sub e in zijn geheel als volgt luidt:[384]

> "de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker ingeval van een verbinding of poging daartoe, *die in de afgelopen drie maanden door de aanbieder in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt*."

Hiermee wordt wederom niet de beschikbaarheid beperkt, maar de verstrekking door aanbieders aan opsporingsdiensten begrensd. De termijn van drie maanden is hier gekozen om aansluiting te zoeken bij de momenteel van kracht zijnde bijzondere bewaarplicht.

De combinatie van de twee alternatieven brengt verenigbaarheid met art. 8 EVRM in zicht, terwijl aan de mogelijkheden voor de opsporing niet getornd wordt en de gedurende twaalf maanden beschikbare locatiegegevens tijdens mobiele communicatie wel toegankelijk zijn met het oog op de nationale veiligheid.

## *4.5. Werken aan effectieve controle op opsporingsdiensten*

Het instellen van effectieve vormen van controle vormt een van de belangrijkste aanbevelingen van dit onderzoek, vanwege de positieve uitwerking op vele deelgebieden van het dataretentievraagstuk. De inbreuk op art. 8 lid 1 EVRM wordt beperkt, in het bijzonder nu de chilling effecten afnemen en het vertrouwen in de opsporing kan toenemen. De rechtvaardiging van de inbreuk ex art. 8 lid 2 EVRM wordt in lijn met de jurisprudentie van het EHRM gebracht, die een nauwkeurige formulering van waarborgen tegen misbruik en willekeur vereist. Individuele burgers worden beter in staat gesteld hun

[382] Zie Besluit bijzondere vergaring nummergegevens telecommunicatie, *Stb.* 2002, 31.
[383] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.9/10; nr. 9, p.22/23.
[384] *Stb.* 2004, 394.

inzagerechten uit te oefenen, zodra notificatieplichten beter worden nageleefd. Het kan leiden tot effectievere opsporing, nu de resultaten van de opsporing vrijkomen voor vervolgonderzoek door onder meer rechtswetenschappers en criminologen. Het geeft de wetgever een ruimere beoordelingsvrijheid inzake het installeren van afwijkende maatregelen die in de specifieke Nederlandse situatie blijken bij te dragen aan de opsporing. Bovendien kan transparantie dat deel van de samenleving dat zich ernstig zorgen maakt over de verregaande inbreuk op de persoonlijke levenssfeer overtuigen deze inbreuken te accepteren, nu de maatregelen daadwerkelijk resultaat oogsten. En zo zijn er nog veel meer redenen te bedenken waarom effectieve controle op de opsporingsdiensten niet alleen wenselijk, maar vanuit het oogpunt van het nastreven van een democratische rechtsstaat noodzakelijk is.

Een eerste alternatief is het garanderen van de naleving van notificatieplichten door de opsporingsinstanties, door de uitblijving ervan te sanctioneren. Daarbij kan gedacht worden aan tuchtrecht. Hoe deze sanctionering precies vormt dient te krijgen, is een belangrijk onderwerp voor vervolgonderzoek. Instructies, standaard-procesbeschrijvingen en audits hebben de situatie volgens de Minister verbeterd,[385] maar gezien het belang van de notificatieplicht is de zekerheid van een concrete regeling, alsmede onafhankelijk en effectief toezicht van elementair belang. Mijns inziens heeft de strakke naleving door opsporingsdiensten niet alleen een gunstige uitwerking op de rechten van de betrokkene, maar leidt het ook tot meer weloverwogen keuzes in het opsporingsonderzoek – en worden telecommunicatiegegevens alleen opgevraagd als dit noodzakelijk in plaats van nuttig is.

Een tweede alternatief is het alsnog implementeren van art. 10 jo. art. 14 dataretentierichtlijn in het wetsvoorstel, zodat de nu bij AMvB op te richten Commissie statistische gegevens in het vervolg op wettelijke grondslag gebaseerde toezichtsbevoegdheden heeft. Momenteel is nog onduidelijk welke bevoegdheden deze Commissie statistische gegevens precies zal krijgen.[386] Dat een en ander in deze ronde niet wettelijk is vastgelegd is een gemiste kans. Toch betekent dit niet dat daarmee niet meer tot wettelijke verankering van effectieve kwantitatieve controle op de uitoefening van opsporingsbevoegdheden gestreefd moet worden. Dit blijft de belangrijkste manier om opsporingsinstanties te controleren.[387]

De twee hier geopperde concrete alternatieven kunnen een aanzet geven, maar een daadwerkelijk transparante opsporing vereist op de eerste plaats – gezien het gebrek aan aandacht voor dit fenomeen – een cultuuromslag binnen de Nederlandse politiek. Met verbazing heb ik kennisgenomen van het feit dat de samenleving momenteel in het duister tast over de zowel de kwantitatieve als kwalitatieve uitoefening van de vorderingsbevoegdheid van de Officier van Justitie ex art. 126n lid 1 Sv.[388] In de komende jaren dient de wetgever op zijn minst een behoorlijke poging te doen de vereisten van een democratische rechtsstaat en de waarborgen gesteld door het EHRM serieus te nemen.[389]

---

[385] *Kamerstukken I*, 2006-2007, 30 164 en 30 327, nr. G, p.4.
[386] Zwenne & Schmidt 2008, p.285.
[387] Idem.
[388] *Kamerstukken II*, 2006-2007, 31 145, nr. 3 (MvT), p.18/19.
[389] Chavannes 2008.

# 5. ALLES ONDER CONTROLE?

## 5.1. Conclusie

In deze scriptie is vanuit verschillende perspectieven gekeken naar de regulering van telecommunicatiegegevens en de ontstane driehoeksverhouding tussen beschikbaarheid, toegang en privacy. Hiertoe is het samenspel van de Wet bewaarplicht telecommunicatiegegevens, de strafvorderlijke bevoegdheden uit met name de Wet vorderen gegevens telecommunicatie en art. 8 EVRM onderzocht. "Het is tijd, dat wij de draden, die wij sponnen, samenbinden."[390]

Het uitgangspunt bij de regulering van telecommunicatiegegevens was het begrenzen van de beschikbaarheid bij aanbieders, om de persoonlijke levenssfeer van de gebruiker te beschermen. Het historische perspectief bracht aan de oppervlakte dat dit uitgangspunt – via de ambivalente boodschap van art. 6 jo. art. 9 versus art. 15 lid 1 E-privacyrichtlijn – geleidelijk is vervangen door de inlijving van het opsporingsbelang in de regulering van deze beschikbaarheid; juist om via toegang een completer beeld te geven van de gebruiker: "gij zult anonimiseren" is stilaan vervangen door "gij zult bewaren voor de opsporing".

De door de dataretentierichtlijn gegarandeerde beschikbaarheid gaat echter niet gepaard met het beperken van de toegang tot die telecommunicatiegegevens. Dat dit in de dataretentierichtlijn niet is gebeurd, maakt verenigbaarheid met art. 8 EVRM gezien vaste jurisprudentie van het EHRM problematisch. De gemeenschapswetgever heeft de regulering van de toegang overgelaten aan de lidstaten, vervolgens heeft Het Hof van Justitie deze keuze van de gemeenschapswetgever bekrachtigd op Europees constitutioneelrechtelijke gronden. Maar de Pijlerstructuur van de Europese Unie komt te vervallen als het Verdrag van Lissabon wordt geratificeerd. De nu nog bestaande onduidelijkheid of de gemeenschapswetgever wel of niet regels kan stellen over de toegang is dan weggenomen.

Gelijktijdig met de totstandkoming van deze Europese beschikbaarheidsverplichting openbaarde het nationale perspectief een deconstructie van de feitelijke toegangsbelemmeringen in de Nederlandse strafvorderlijke bevoegdheden, met name sinds de inwerkingtreding van de Wet vorderen gegevens telecommunicatie. Daarnaast is de samenwerking tussen opsporingsinstanties en het bedrijfsleven drastisch toegenomen. Deze ontwikkelingen ondersteunen de bredere constatering dat zowel de regulering van beschikbaarheid als toegang zich in de afgelopen jaren kenmerken door een eenzijdige, dat wil zeggen door het opsporingsbelang beheerste invalshoek.

De privacy van de telecommunicatiegebruiker was derhalve bij de totstandkoming van zowel Europese als Nederlandse dataretentieverplichtingen onderbelicht. Grondige analyse van de aard van de privacyinbreuk van dataretentie op zichzelf, en in relatie met de strafvorderlijke bevoegdheden, leert dat de prijs die de burger moet betalen zeer hoog is, terwijl de effectiviteit en de 'pressing social need' van de maatregel niet overtuigend zijn aangetoond. Dientengevolge lijkt evenmin aan het proportionaliteitsvereiste van art. 8 lid 2 EVRM te kunnen worden voldaan. In dit licht, mede gezien de

[390] P. Scholten, 'De beslissing', in: *Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht,* 1931, Algemeen deel 1, § 28, p. 129.

recente uitspraak van het EHRM in de uitspraak *S. and Marper v. The United Kingdom*, is de ontstane driehoeksverhouding vanuit grondrechtelijk perspectief kwestieus.

Het fundamentele probleem in de driehoeksverhouding is dat beschikbaarheid en toegang formeel gescheiden zijn in de dataretentierichtlijn. Lidstaten moeten nu een bewaarplicht implementeren, terwijl de toegang door reeds bestaande nationale – en op Europees niveau sterk verschillende – wetgeving wordt beheerst. Maar waar beschikbaarheid en toegang in de privacyrichtlijn nog onderscheidenlijk van elkaar konden opereren, is via art. 15 lid 1 E-privacyrichtlijn met de dataretentierichtlijn een onafscheidelijke, wederzijdse beïnvloeding tussen de twee ontstaan. Het is voortaan van cruciaal belang om deze toenemende interdependentie van beschikbaarheid en toegang te onderkennen, om de privacy van burgers te respecteren.

Het ontbreken van een samenhangende visie over een adequate balans binnen de driehoeksverhouding vormt een risico voor nationale wetgeving in de lidstaten, een risico dat zich in de Nederlandse situatie heeft gemanifesteerd. Het Kabinet heeft zich in de politieke arena kunnen beroepen op deze scheiding van beschikbaarheid en toegang, zonder daarmee in strijd met de dataretentierichtlijn te handelen. Maar het achterwege blijven van beperkingen van de niet geringe inbreuk op art. 8 lid 1 EVRM, het ontbreken van overtuigend bewijs van de noodzakelijkheid en effectiviteit van de maatregel, de gebrekkige controle op opsporingsdiensten en het ontbreken van nauwkeurig geformuleerde waarborgen tegen misbruik door deze diensten zijn gewichtige factoren die bij elkaar opgeteld leiden tot de aanzienlijke mogelijkheid dat het wetsvoorstel een schending van art. 8 EVRM oplevert.

Geconcludeerd kan worden dat de wetgever zich te weinig rekenschap heeft gegeven van de beperkende werking van art. 8 EVRM op dataretentieverplichtingen, en dat de tekortkomingen van het Europees constitutionele recht zich volledig hebben laten gelden in de Wet bewaarplicht telecommunicatiegegevens. Vanwege het extrapoleren van de formele, volgens A-G Y. Bot "kunstmatige" scheiding van beschikbaarheid en toegang in de dataretentierichtlijn heeft de wetgever te weinig ondernomen om de inbreuk op de persoonlijke levenssfeer van telecommunicatiegebruikers, de facto alle burgers, te ondervangen. In de scriptie zijn daarom concrete alternatieven aangedragen, als aanzet op de noodzakelijke beperking van de inbreuk op art. 8 lid 1 EVRM die de wetgever achterwege heeft gelaten.

Nu het wetsvoorstel op 7 juli jl. is aangenomen in de Eerste Kamer, kennen ook de Nederlandse aanbieders binnen afzienbare tijd een bewaarplicht van telecommunicatiegegevens. Al is het wetsvoorstel goedgekeurd door de volksvertegenwoordiging, zet de scriptie een stap verder door op te roepen om de eenzijdige invalshoek in het wetsvoorstel los te laten, en tot een samenhangende visie te komen op de driehoeksverhouding tussen de Wet bewaarplicht telecommunicatiegegevens, de strafvorderlijke toegangsbevoegdheden van opsporingsdiensten en het recht op privacy van burgers. De titel van deze scriptie, "Alles onder controle?", lijkt in eerste instantie te duiden op de door de veertien hoogleraren geuite bezorgdheid voor de grondrechten van burgers. Maar de vraag is eveneens gericht tot de wetgever, die de implicaties van het wetsvoorstel tot nu toe onvoldoende in ogenschouw heeft genomen en het wetgevingsproces niet helemaal onder controle had.

## 5.2. Aanbevelingen aan Kamerleden

De alternatieven die in hoofdstuk 4 zijn geboden op de huidige regulering van beschikbaarheid van en toegang tot telecommunicatiegegevens worden hier kort weergegeven. Zij zien alle op een beperking van de inbreuk op art. 8 EVRM, een vereiste uit de vaste jurisprudentie van het EHRM. Voor een bespreking van de alternatieven wordt steeds verwezen naar afzonderlijke paragrafen.

De aanbevelingen dienen te worden gezien als een eerste aanzet om de gesignaleerde problematiek binnen de driehoeksverhouding tussen beschikbaarheid, toegang en de persoonlijke levenssfeer te ondervangen. Verder onderzoek is noodzakelijk, een indruk van daarvan wordt in de volgende paragraaf gegeven.

i. De bewaarplicht dient alsnog teruggebracht te worden tot zes maanden via een wetswijziging van art. 13.2a lid 3 jo. 13.4 lid 3 Tw. (par. 4.1.)

ii. De term 'ernstige misdrijven' uit art. 13.2a lid 2 wetsvoorstel dient helder afgebakend te worden via een nieuw in te voeren art. 13.2a lid 1 sub c, waarin voor de duiding 'ernstige misdrijven' bijvoorbeeld aangesloten wordt bij de 24 categorieën die in art. 2 lid 2 van het Europese Aanhoudingsbevel staan opgesomd.[391] (par. 4.2.)

iii. De verplichte verstrekking door aanbieders op grond van art. 13.2a Tw jo. 13.4 Tw moet gedifferentieerd worden naar de ernst van het misdrijf, om tot een proportionele verstrekking van telecommunicatiegegevens te komen. Ingeval van verdenking van de relatief lichtere vormen van criminaliteit uit art. 67 lid 1 sub b/c Sv, kan de verstrekking door aanbieders beperkt worden tot bijvoorbeeld drie of zes maanden voorafgaand aan het toegangsverzoek van opsporingsdiensten. (par. 4.2.)

iv. De vorderingsbevoegdheid van opsporingsambtenaren ex art. 126na lid 1 Sv kan via de wijziging van een AMvB uitgebreid worden van actuele tot verplicht bewaarde gebruiksgegevens. Beide Kamers dienen bedacht te zijn van deze mogelijkheid, die vanwege de lage toegangsdrempels in art. 126na lid 1 Sv en de frequentie waarmee van de bevoegdheid gebruik gemaakt wordt een enorme reikwijdte zal hebben en een ernstige inbreuk vormt op art. 8 lid 1 EVRM. (par. 4.3.)

v. Gezien de verplichte bewaring van locatiegegevens tijdens mobiele communicatie in de bijlage bij het wetsvoorstel, die daarmee een gevoelige categorie toevoegt ten opzicht van art. 5 dataretentierichtlijn, dient de gegevensverstrekking door aanbieders aan de Officier van Justitie beperkt te worden tot de locatiegegevens die gedurende de afgelopen drie maanden gegenereerd zijn. De huidige status quo van de bijzondere bewaarplicht krachtens art. 13.4 lid 2 Tw jo. art. 7 Besluit bijzondere vergaring nummergegevens telecommunicatie,[392] waarmee de identificatie van prepaid bellers gefaciliteerd wordt, is daarmee gehandhaafd, terwijl de

[391] Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002, PB EG L 190/01.
[392] *Stb.* 2002, 31.

beschikbaarheid in het kader van de nationale veiligheid voor de AIVD en MIVD is gegarandeerd. Hiertoe dient aan art. 2 sub e Besluit vorderen gegevens telecommunicatie de hieronder gecursiveerde zinsnede toegevoegd te worden:[393] (par. 4.4.)

> "de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker ingeval van een verbinding of poging daartoe, *die in de afgelopen drie maanden door de aanbieder in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt.*"

vi. De naleving van notificatieplichten door opsporingsdiensten dient te worden afgedwongen via een systeem van sanctionering, om het achterwege blijven van notificatie in de praktijk te ondervangen. Onafhankelijk toezicht door een specifiek op de uitoefening van de kwalitatieve bevoegdheden door opsporingsinstanties toegerust orgaan is daarbij vanuit rechtsstatelijk oogpunt zeer wenselijk. (par. 4.5.)

vii. Art. 10 jo. art. 14 dataretentierichtlijn dienen in het wetsvoorstel geïmplementeerd te worden, zodat de nu nog onduidelijke taakomschrijving en bevoegdheden van de aangekondigde Commissie statistische gegevens in het vervolg op wettelijke grondslag gebaseerd zijn. (par. 4.5.)

## 5.3. Agenda voor vervolgonderzoek

De aanbevelingen onderstrepen de noodzaak tot vervolgonderzoek, omdat zij slechts een gedeelte van het gehele spectrum van de driehoeksverhouding dekken. Hier ligt een belangrijke taak voor de wetenschap. De urgentie van een samenhangende visie met betrekking tot de regulering van de beschikbaarheid van en toegang tot telecommunicatiegegevens is hoog. Het instellen van een onafhankelijke commissie kan overwogen worden, waarin alle belanghebbenden vertegenwoordigd zijn – behoeftestellers, aanbieders, burgers en vooral ook de wetenschap om het geheel in een bredere context te kunnen bezien. De Adviescommissie Informatiestromen Veiligheid is een vrij recent voorbeeld, waarvan de activiteiten resulteerden in het rapport *Data voor Daadkracht*.[394]

Commissie of niet, de met dataretentie in het leven geroepen driehoeksverhouding tussen de regulering van beschikbaarheid, toegang en het recht op privacy dient aan kritische reflectie te worden onderworpen – gevrijwaard van het politieke klimaat van vandaag de dag, mogelijke politieke druk of Europees constitutioneelrechtelijke handicaps. Een onderzoek naar de cumulatieve effecten van verschillende wetgevingsmaatregelen neemt daarbij een belangrijke plaats in, zoals aanbevolen in de studie door het Rathenau Instituut en het Tilburg Institute for Law, Technology and Society (TILT). In het bijzonder dienen de cumulatieve effecten voor de persoonlijke levenssfeer van de Wet bewaarplicht

[393] *Stb.* 2004, 394.
[394] Adviescommissie Informatiestromen Veiligheid, *Data voor daadkracht, Gegevensbestanden voor veiligheid: observaties en analyse*, 1 sept. 2007. Her rapport onderzocht de systematiek van de regulering van informatiestromen uit (grote) gegevensbestanden in de publieke en private sector ten behoeve van de veiligheid. Te raadplegen via: <http://www.bzk.nl/aspx/download.aspx?file=/contents/pages/89605/datavoordaadkracht.pdf> [geraadpleegd juli 2009].

telecommunicatiegegevens en de Wet vorderen gegevens telecommunicatie uit 2006 inzichtelijk gemaakt te worden.

Deze scriptie heeft daarnaast enkele concrete punten voor vervolgonderzoek aan het licht gebracht, die hier ten behoeve van de helderheid zijn opgesomd met verwijzing naar de vindplaatsen in de scriptie:

- Het nut van de voorgestelde dataretentiemaatregelen voor de opsporing van strafbare feiten is evident, maar het Kabinet heeft de 'pressing social need' van de voorgestelde dataretentiemaatregelen nog niet overtuigend bewezen. Vervolgonderzoek dient het verband tussen het bestaan van de bewaarplicht en het oplossen van ernstige misdrijven aan de hand van concrete kwantitatieve analyse in kaart te brengen, alsmede de weerslag die dit heeft op de grondrechten van burgers. De studie zou inspiratie kunnen putten uit het omvangrijke onderzoek van het Max Planck Institut.[395] (par. 3.3.1.)

- In het verlengde hiervan is multidisciplinair onderzoek naar mogelijke chilling effecten van dataretentie en de impact van het wetsvoorstel op 'het reflexieve project van het zelf' van burgers vereist. De aard van telecommunicatie verandert en de invloed op identiteitsvorming en persoonlijke- en culturele ontwikkeling neemt daarbij toe. Blijkens kleinschalig onderzoek voelt de helft van de Duitsers zich door dataretentie belemmerd in het zich uiten via telecommunicatie.[396] In hoeverre sorteert dataretentie dezelfde effecten op Nederlanders? (par. 3.2.2.)

- Recente technologische ontwikkelingen, zoals IP-spoofing en nieuwe vormen van telecommunicatie, maken het trekken van conclusies op basis van telecommunicatiegegevens discutabel en het omzeilen van de bewaarplicht eenvoudig. Vervolgonderzoek dient in te gaan op deze bezwaren van de effectiviteit van de bewaarplicht, met name op het risico dat juist niet-verdachte burgers hierdoor disproportioneel in hun privacybelang kunnen worden getroffen. (par. 3.3.1.)

- Rechtsvergelijkend onderzoek naar de strafvorderlijke bevoegdheden, en het bestaan van een brede consensus daarin onder verdragspartijen bij het EVRM, geeft inzicht in een van de belangrijke factoren die de beoordelingsvrijheid van de wetgever bepalen. (par. 3.3.2.2.; par. 3.3.2.3.; par. 3.3.2.4.)

- De gebrekkige onafhankelijke controle op opsporingsdiensten is vanuit rechtsstatelijk en grondrechtelijk oogpunt onwenselijk. Verschillende vormen van toezicht op de opsporingsdiensten dienen geanalyseerd te worden op hun effectiviteit, uitvoerbaarheid en uitwerking op opsporingsactiviteiten. Tevens dient nader onderzoek opgezet te worden naar de

[395] H. Albrecht, C. Dorsch, C. Krüpe, *Rechtswirklichkeit der Auskunftserteilung über Telekommunikations-verbindungsdaten nach §§ 100g, 100h StPO*, Max Planck Institut, feb. 2008, zie: <http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf> [geraadpleegd juli 2009].
[396] Gesellschaft für Sozialforschung und Statistischen Analyse mbH, *Meinungen der Bundesbürger zur Vorratsdatenspeicherung*, 2 juni 2009, zie: <http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf> [geraadpleegd juli 2009].

sanctionering van niet-naleving door opsporingsdiensten van de notificatieplicht. (par. 3.3.2.5.; par. 4.5.)

- Voor de door het Europese constitutionele recht van de pijlers ingegeven scheiding van de regulering van beschikbaarheid (Eerste pijler) en toegang (Derde pijler), bestaat na de ratificatie van het Verdrag van Lissabon geen enkele reden meer. Dit maakt een nieuwe Europese wetgevingsmaatregel mogelijk, waarin de interdependentie van beschikbaarheid en toegang tot haar recht komt – een wens die ook door A-G Y. Bot in zaak C-301/06 is geuit. Vervolgonderzoek kan zich richten op de vormgeving van een dergelijke nieuwe maatregel. Tevens kan onderzocht worden, óf en hoe dit bij de evaluatie van de huidige dataretentierichtlijn verwezenlijkt kan worden. (par. 1.5.; par. 2.4.)

# EPILOOG: 'HEMEL EN HEL'

De afgelopen weken heb ik de werking van onze democratie van dichtbij gevolgd. De opzienbarende voorbereiding van de senatoren in de vaste commissie voor Justitie stemde mij hoopvol. Toen sommige leden van de "Chambre de Réflection"[397] op 6 en 7 juli jl. hun eerdere reflectie opeens vergeten leken te zijn, was ik een illusie armer en een ervaring rijker. Niet wetenschappelijke rationaliteit, maar politieke opportuniteit had het laatste woord. Mijn vertrouwen in de democratie heeft een fikse deuk opgelopen.

Eigenlijk zou ik de bewuste Kamerleden het schilderij van Escher willen tonen. Bij de eerste blik op het schilderij zie je een helder onderscheid tussen de engel, zeg Majoor Boshardt, en de duivel, Marc Dutroux. Maar als je het schilderij langer op je laat inwerken, verschuift je aandacht geleidelijk naar de rand. Het aantal engeltjes en duiveltjes neemt sterk toe, terwijl het onderscheid steeds troebeler wordt – om tenslotte te eindigen in een oneindig grijs gebied. Escher laat zien dat aan de dag des oordeels niet is te ontkomen: welke randgevallen mogen dan naar de hemel, en wie wordt vanuit het grijze gebied naar de hel verbannen? Zowel de heldere als de troebele afwegingen maken deel uit van dezelfde werkelijkheid, die door Escher treffend in één beeld wordt weergegeven. Verdieping in het schilderij stemt kritisch op teveel macht aan welke hogere instantie dan ook.

Zo is het ook met dataretentie: hoe langer ik het fenomeen bestudeerd heb, hoe kritischer ik ben geworden op de maatregel. Dit geldt ook voor de mensen uit mijn naaste omgeving. Zonder al te diep na te denken zijn zij in eerste instantie bereid een beetje privacy in te leveren om de volgende Dutroux achter slot en grendel te krijgen. Met dergelijke extreme gevallen wordt dataretentie dan ook steevast gerechtvaardigd door het Kabinet. Maar als ik de tijd neem om familie en vrienden, overigens vaak aan de hand van Escher, uit te leggen wat nu precies de implicaties zijn van dataretentie, dan verandert hun mening meestal vrij snel: gegevens van niet-verdachten, voor de opsporing van relatief lichte vormen van criminaliteit… Enfin, u kunt het in de scriptie lezen. Juist in deze randgevallen, die de overgrote meerderheid van de toegangsverzoeken door opsporingsdiensten betreffen, is de rechtvaardiging van de Minister kwestieus.

Vervolgens vertel ik mijn tante of buurman dat de nood hoog is. De dichotomie van privacy versus veiligheid is namelijk een misvatting.[398] Privacy omhelst veel meer dan de persoonlijke levenssfeer. Zonder privacy zijn tastbaardere waarden als vrijheid, autonomie en waardigheid waardeloos. Daarnaast dient het individuele perspectief losgelaten te worden, aangezien wij steeds vaker als groep of profiel in een bepaalde context getypeerd worden – denk maar aan datamining of een groep demonstranten. Nog fundamenteler is de notie dat onze gemeenschap niet kan functioneren zonder privacy, aangezien vrije verkiezingen, religieuze tolerantie of vrije vergadering niet mogelijk zijn. Zonder privacy geen democratische rechtstaat.[399] Om al deze redenen zou het een goede zaak zijn als wij, de senatoren incluis, nog eens diep nadenken over de samenleving waarin wij willen leven. Wij zijn gewaarschuwd: "Privacy is like oxygen. We really appreciate it only when it is gone."[400]

---

[397] <http://www.eerstekamer.nl/begrip/taken_en_positie_eerste_kamer> [geraadpleegd juli 2009].
[398] *Kamerstukken I*, 2007–2008, 31 200 VI, nr. F, pag.39. Aan het woord is hoogleraar Corien Prins.
[399] Idem, pag.40.
[400] C.J. Sykes, in: R. Whitaker, *The End of Privacy: How Total Surveillance Is Becoming a Reality*, New Press 1998, nr. 33.

# BIBLIOGRAFIE

## A. Jurisprudentie


***Hof van Justitie van de Europese Gemeenschappen***
HvJEG 29 januari 2008, nr. C-275/06, Promusicae v. Telefónica.
HvJEG 14 oktober 2008, nr. C-301/06, Conclusie A-G Y. Bot.
HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council.

***Europees Hof voor de Rechten van de Mens***
EHRM 13 mei 1976, appl. 6825/74, *(X v. Iceland).*
EHRM 7 december 1976, appl. 5493/72, *(Handyside v. The United Kingdom).*
EHRM 6 september 1978, appl. 5029/71, *(Klass a.o. v. Germany).*
EHRM 25 maart 1983, appl. 5947/72, *(Silver a.o. v. The United Kingdom).*
EHRM 2 augustus 1984, NJ 1988, 534 *(Malone)*.
EHRM 24 april 1990, appl. 11105/84, *(Huvig v. France)*.
EHRM 24 september 1992, appl. 10533/83, *(Herczegfalvy v. Austria).*
EHRM 26 september 1995, appl. 17851/91, (*Vogt v. Germany).*
EHRM 30 juli 1998, appl. 27671/95, *(Valenzuela Contreras v. Spain)*.
EHRM 16 februari 2000, appl. 27798/95, *(Amann v. Switzerland).*
EHRM 25 september 2001, NJ 2003, 670, *(P.G. and J.H. v. France)*.
EHRM 17 februari 2004, appl. 44158/98, *(Gorzelik and others v. Poland)*.
EHRM 24 januari 2006, appl. 62617/00, *(Copland v. The United Kingdom).*
EHRM 1 juli 2008, appl. 58243/00, *(Liberty a.o. v. The United Kingdom).*
EHRM 4 december 2008, appl. 30562/04, *(S. and Marper v. The United Kingdom)*.

***Duitse Constitutionele Hof***
Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08.

***Hoge Raad***
HR 25 november 2005, Mediaforum 2006-1, *(Lycos/Pessers)*, m.nt. A.H. Ekker.


## B. Literatuur


***Asscher & Koops 2003***
L.F. Asscher & E.J. Koops, Verkeersgegevens: een juridische en technische inventarisatie, Amsterdam: Otto Cramwinckel 2003.

***Amici Curiae 2008***
P. Breyer (on behalf of 43 European organizations), *Submission concerning the action brought on 6 July 2006 Ireland v Council of the European Union, European Parliament Case C-301/06*, 8 April 2008, zie: <http://www.vorratsdatenspeicherung.de/images/data_retention_brief_08-04-2008.pdf> [geraadpleegd maart 2009]

***Bignami 2007***
F. Bignami, *Privacy and law enforcement in the European Union: The Data Retention Directive*, Chicago Journal of International Law, Summer 2007, Vol. 8, no. 1, p. 233-255.

***Birnhack & Elkin-Koren 2005***

M.D. Birnhack & N. Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, Viriginia Journal of Law & Technology, Vol. 8, Oct. 2003. De update van oktober 2005 is in te zien via: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=381020> [geraadpleegd mei 2009].

***Blok 2002***

P.H. Blok, '*Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlands en Amerikaans recht'*, Den Haag: Boom 2002.

***Breyer 2005***

P. Breyer, *Telecommunications data retention and human rights: the compatability of blanket traffic data retention with the ECHR*, European Law Journal, Vol. 11, 2005, no. 3, p. 365-375.

***CBP 2007***

*Advies CBP Wetsontwerp implementatie Europese Richtlijn Dataretentie,* 22 jan. 2007. <www.cbpweb.nl/downloads_adv/z2006-01542_2.pdf> [geraadpleegd maart 2009].

***Chavannes 2008***

R.D. Chavannes, *Veel taps, weinig verantwoording*, Mediaforum (20), 2008, nr. 6, p.245.

***Commissie-Mevis 2001***

Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, *Gegevensvergaring in Strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, aangeboden mei 2001.

***Cooper 2003***

D. Cooper, *Memorandum of laws concering the legality of data retention with regard to the rights guaranteerd by the European Convention on Human Rights*, Covington & Burling for Privacy International, 10 okt. 2003, te raadplegen via:
<www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf>
[geraadpleegd april 2009].

***De Mul 2001***

J. de Mul (et al.), *ICT de baas?*, Onderzoeksprogramma Internet en Openbaar bestuur, 2001.

***De Mul & Frissen 2000***

J. de Mul & V. Frissen, *Under construction*, Infodrome 2000.

***Drijber 2009***

P.B. Drijber, *Noot bij HvJEG 10 februari 2009, nr. C-301/06, Ireland v.Parliament and Council*, Mediaforum (21), 2009, nr. 6, p.256-261.

***Van Dijk & Van Hoof 2006***

P. van Dijk, F. Van Hoof, A. van Rijn & L. Zwaak (eds.), *Theory and practice of the European Convention on human rights*, Antwerpen-Oxford: Intersentia 2006.

***Dommering 2000***

E.J. Dommering e.a., *Informatierecht*, Amsterdam: Otto Cramwinckel 2000.

***Dommering 2009***

E.J. Dommering, *Van 'Ja zuster, nee zuster' naar 'Discodans': de lange weg naar commerciële informationele privacy*, in: D. Visser, 'Bundel Portretrecht' (nog te publiceren).

***Ekker 2008***

A.H. Ekker, *Duitse kritiek op de Europese bewaarplicht van telecomgegevens*, Privacy & Iinformatie, november 2008, afl. 5, p. 231-236.

***Frissen 2008***

V. Frissen, *De digitale diaspora*, Rotterdam: Ger Guijs 2008.

***Groothuis 2006***

M. Groothuis, *De bewaarplicht van verkeersgegevens bij internet en telefonie en de verhouding tot het recht op eerbiediging van de persoonlijke levenssfeer*, NJCM-Bulletin (31), 2006, nr. 6, p. 792-811.

***Hijmans 2008***

H. Hijmans, *Over de verwachtingen van het Verdrag van Lissabon op het gebied van privacy en rechtshandhaving*, NJB (83), afl. 29, 2008, p. 1791-1795.

***Van Hoboken 2009***

J.V.J. van Hoboken**,** *Noot bij HvJEG 10 februari 2009, nr. C-301/06, Ireland v.Parliament and Council*, Privacy & Informatie (70) 2009, nr. 59, afl. 2, p. 86-88.

***Hofhuis 2006***

Y. Hofhuis, *Minimumharmonisatie in het Europees recht*, Deventer: Kluwer 2006.

***Jacobs & White 2006***

C. Ovey & R.C.A. White (4th edition), *The European Convention on human rights*, Oxford: Oxford University Press 2006.

***Kapteyn & Verloren van Themaat 2003***

P.J.G. Kapteyn & P. Verloren van Themaat, *Het recht van de Europese Unie en van de Europese Gemeenschappen*, Deventer: Kluwer 2003.

***Koops & Buruma 2007***

B.J. Koops & Y. Buruma, *Formeel strafrecht en ICT*, in: B.J. Koops, 'Strafrecht en ICT', Den Haag: Sdu 2007, p. 77-121.

***Mac Gillavry 2004***

E.C. Mac Gillavry, *Met wil en dank, een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven*, Nijmegen: Wolf legal publishers 2004.

***Mac Gillavry 2006***

E.C. Mac Gillavry, *Heeft u even voor de nieuwe Wet politiegegevens?*, in: 'Systeem in ontwikkeling: Liber Amicorum G. Knigge', Nijmegen: Wolf Legal Publishers 2005.

***Mol Lous 2006***

L.P. Mol Lous, *Een Europese bewaarplicht voor verkeersgegevens: de Commissie als bewaker van het opsporingsbelang*, SEW (54), nr. 89, oktober 2006, p.352-357.

***Prechal 2005***

S. Prechal, *Directives in EC law,* Oxford: Oxford University Press 2005.

***Rathenau/TILT 2007***

A. Vedder, B.J. Koops, P. de Hert, *Van privacyparadijs tot controlestaat: Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag: Rathenau/TILT 2007.

***Smits 2006***

A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, Nijmegen: Wolf legal publishers 2006.

***Solove 2004***

D.J. Solove, *The digital person: Technology and privacy in the information age*, New York: New York University Press 2004.

***Solove 2008***

D.J. Solove, *Data Mining and the Security-Liberty Debate*, University of Chicago Law Review (74), 2008, nr. 75, p. 343-362.

***Stevens, Koops & Wiemans 2004***

L. Stevens, B.J. Koops. & P. Wiemans, *Een strafvorderlijke gegevensvergaring nieuwe stijl*, NJb (79), 2004, nr. 32, p. 1680-1686.

***Stratix 2003***

Stratix Consulting Group B.V., *Onderzoek 'Bewaren Verkeersgegevens door Telecommunicatieaanbieders,* Eindrapport uitgebracht aan het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie, Schiphol: Stratix 2003.

***Teunissen 2009***

J.M.H.F. Teunissen**,** *Noot bij HvJEG 10 februari 2009, nr. C-301/06, Ireland v. Parliament and Council*, Jurisprudentie Bestuursrecht (70) 2009, nr. 10.

***Tufekci 2008***

Z. Tufekci, *Can you see me now?*, SAGE Bulletin of Science, Technology and Society, vol. 28, 2008, p.20-36. Zie [geraadpleegd februari 2009]:
<http://userpages.umbc.edu/~zeynep/papers/ZeynepCanYouSeeMeNowBSTS.pdf>

***Van Veen & Van Ginneken 2009***

C. van Veen & P.P.J. van Ginneken, *De Dataretentierichtlijn: speelbal tussen pijlers*, Mediaforum (21), 2009, nr. 1, p. 2-10.

***Wellman & Haythornthwaite 2002***

C. Haythornthwaite & B. Wellman, *The Internet in Everyday Life*, Oxford: Blackwell publishers 2002. Zie [geraadpleegd april 2009]:
<http://www.chass.utoronto.ca/~wellman/publications/everdayintro/Haythornthwaite_Wellman_intro.PDF>

***Zwenne & Schmidt 2005***

G.J. Zwenne & A. Schmidt, *Recht en risico, Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens*, Mediaforum (17), 2005, nr. 9, p. 292-302.

***Zwenne & Schmidt 2008***

G.J. Zwenne & A. Schmidt, *Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens*, Mediaforum (20), 2008, nr. 7/8, p. 278-285.