

Ministerie van Veiligheid en Justitie

Amsterdam
21 juni 2012

Geachte mevrouw Odinet en mevrouw De Jong,

Bits of Freedom dankt u hartelijk voor uw uitnodiging om haar visie ten aanzien van de belangrijke evaluatie van de Wet bewaarplicht telecommunicatiegegevens met u te delen.

Op grond van deze wet wordt het communicatiegedrag van nagenoeg alle zestien miljoen Nederlanders, verdacht en onverdacht, bewaard voor de duur van één jaar. In deze brief benadrukt Bits of Freedom welke essentiële aspecten van de bewaarplicht in de evaluatie uitgebreide aandacht behoeven.

Uitgangspunt van de evaluatie

1. Artikel 13.9 van de Telecommunicatiewet luidt:

Onze Minister van Veiligheid en Justitie zendt in overeenstemming met Onze Minister binnen drie jaar na de inwerkingtreding van deze wet en vervolgens telkens na drie jaar aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van de wijziging van de artikelen 13.2a, 13.4 en 13.5 in de praktijk, voor zover die wijzigingen betrekking hebben op de implementatie van Richtlijn nr 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie.

2. Het wetsartikel noemt twee aspecten die geëvalueerd dienen te worden.

- Het eerste aspect is doeltreffendheid. De doeltreffendheid zegt iets over de



mate waarin de beoogde doelstelling is behaald. Deze evaluatie zal dan ook de vraag moeten beantwoorden of en in welke mate is voldaan aan behalen van de doelstelling van de bewaarplicht.

- Het tweede aspect betreft de effecten van de implementatie van de richtlijn. Deze evaluatie zal de gevolgen voor de persoonlijke levenssfeer en de noodzakelijkheid, proportionaliteit, subsidiariteit en effectiviteit van de bewaarplicht kritisch moeten beoordelen.

Doeltreffendheid is niet aangetoond

3. Op nationaal niveau beoogt de bewaarplicht, waarbij aanbieders van elektronische communicatiediensten en -netwerken verplicht zijn tot het bewaren van bepaalde gegevens, te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.¹ Op Europees niveau heeft de richtlijn tot doel de nationale bepalingen van de lidstaten die betrekking hebben op het bewaren van deze gegevens, te harmoniseren.²

Om de doeltreffendheid van de wetgeving te kunnen beoordelen moet de mate waarin het beoogde doel is behaald worden bepaald. Het behalen van de doelstelling kan worden afgemeten aan een significante en herleidbare toename van de oplossingsgraad van zaken over ernstige criminaliteit. De evaluatie moet haar conclusie onderbouwen met kwalitatieve en kwantitatieve informatie.

4. Het is daarbij belangrijk onderscheid te maken naar de verschillende soorten gegevens. De aard van de gegevens zijn voor elk van de categoriën erg verschillend: het tijdstip van communicatie moet anders worden behandeld dan de geografische locaties van de betrokkenen ten tijde van die communicatie.
5. Het is daarbij ook belangrijk voor ogen te houden welke gegevens al voorhanden zijn, of kunnen zijn, op grond van andere regelgeving en welke gegevens alleen beschikbaar zijn op grond van de verplichting tot het bewaren van gegevens die voortvloeit uit de bewaarplicht.
6. Tot op heden heeft de Nederlandse regering, maar ook de Europese Commissie, niet kunnen aantonen dat het beoogde doel behaald is.

Evaluatie EC zegt niets over doeltreffendheid in Nederland

7. De evaluatie van de Europese Commissie bevat geen informatie die de vraag, of het beoogde doel van de Nederlandse Wet bewaarplicht telecommunicatie-gegevens is gerealiseerd, beantwoordt. Dat is niet verwonderlijk, aangezien de inbreng van de Nederlandse regering voor de evaluatie van de Europese Commissie irrelevant was.



In de brief van het ministerie van Justitie van 2 september 2010 aan de Europese Commissie³ blijven cruciale vragen van de Commissie⁴ onbeantwoord. Zo voorziet het ministerie niet in de gevraagde kwantitatieve informatie over o.a. veroordelingen die gebaseerd zijn op gegevens die bewaard worden op grond van de richtlijn.

De toenmalige minister stelde zonder enige onderbouwing dat gebruikers- en verkeersgegevens in 65% van alle opsporingsonderzoeken worden gebruikt. De voorbeelden van opsporingsonderzoeken waarin verkeersgegevens een rol hebben gespeeld, aangedragen door de Raad van Commissarissen, zijn echter zonder betekenis door een gebrek aan detail. Ook verwijst de minister naar 24 strafzaken die in 2010 voor de rechter zijn gebracht en waarin verkeers-gegevens een rol hebben gespeeld. Het merendeel van deze zaken werd onderzocht, en veelal zelfs voor het eerst voor de rechter gebracht, voordat de bewaarplicht van kracht werd. Daarmee werd aangetoond dat de gegevens al voorhanden waren voordat de bewaarplicht van kracht werd.

Dat de gegevens in onderzoeken worden gebruikt zegt daarnaast ook niets over de oorzaak van de beschikbaarheid van de gegevens. Het zegt ook niets over de rol die de gegevens in het onderzoek hebben gespeeld. Er is niet af te leiden of de beschikbaarheid van de gegevens van doorslaggevende betekenis is geweest voor het oplossen van de onderzoeken, of de gegevens niet ook op een andere manier beschikbaar waren of konden zijn en of de beschikbaarheid van de gegevens een significante bijdrage hebben geleverd aan de bestrijding van ernstige misdrijven.

Kwalitatieve en kwantitatieve informatie ontbreekt

8. Verder zijn er geen gedetailleerde cijfers bekend met betrekking tot de vorderingen van opsporings- en inlichtingendiensten bij telefonie- en internetaanbieders. In het jaarverslag over 2010 van het ministerie van Veiligheid en Justitie is het "aantal aanvragen op historische gegevens, zoals verkeers- en identificerende gegevens" opgenomen. Dit cijfer heeft echter alleen betrekking op de laatste zes maanden van dat jaar en er is geen nadere duiding beschikbaar.⁵
9. Andere en meer gedetailleerde gegevens worden niet geregistreerd of niet openbaar gemaakt. Bits of Freedom heeft in juli 2011 bij het KLPD een verzoek op grond van de Wet openbaarheid van bestuur gedaan. Het korps werd verzocht documenten openbaar te maken die iets zeggen over de vorderingen van zulke gegevens in bijvoorbeeld de eerste zes maanden van 2010 en over de vorderingen welke door de aanbieders zijn geweigerd. Dit verzoek is in eerste instantie geweigerd en op het aangetekende bezwaar moet nog altijd worden beslist.



10. Ook is er geen significante stijging te zien in het aantal zaken van ernstige criminaliteit dat door de opsporings- en inlichtingendiensten wordt opgelost. Er kan al helemaal niet worden geconcludeerd dat een eventuele stijging direct te relateren is aan de beschikbaarheid van de gegevens die bewaard worden op grond van de bewaarplicht. Uit onderzoek van het WODC blijkt zelfs dat in de periode van 2005 tot en met 2010 het percentage opgeloste zaken met één procent daalde (van 25% naar 24%).⁶
11. Op grond hiervan moet geconcludeerd worden dat tot op heden de Nederlandse regering op geen enkele wijze heeft kunnen onderbouwen dat de bewaarplicht een significante en herleidbare bijdrage levert aan de bestrijding van de ernstige criminaliteit. Wil deze evaluatie een betekenisvolle bijdrage leveren aan de beoordeling van de doeltreffendheid van de bewaarplicht, moet zij wél voorzien in de kwantitatieve en kwalitatieve informatie op grond waarvan iets gezegd kan worden over de doeltreffendheid van de bewaarplicht.

Grootste effect is een enorme inbreuk op de privacy van alle burgers

12. Het grootste effect van het grootschalig en ongericht bewaren van de gebruikers- en verkeersgegevens van alle Nederlanders is de gigantische inbreuk op de privacy van zestien miljoen verdachte én onverdachte burgers. De Europese Toezichthouder Gegevensbescherming noemde de Europese richtlijn "the most privacy invasive instrument ever adopted by the European Union."⁷

Op grond van de bewaarplicht worden gegevens bewaard waarin is vastgelegd wie wanneer met wie contact heeft gehad, hoe lang dat contact heeft geduurd en de geografische locatie van de beide gesprekspartners. De gegevens met betrekking tot het belgedrag worden voor de duur van één jaar bewaard. Daarmee kunnen aanbieders en opsporings- en inlichtingendiensten met grote precisie vaststellen waar iemand bijna een jaar geleden (bijvoorbeeld "13 juli 2011 om 14:11 uur") was, terwijl de betrokkene daarvan zelf geen weet meer heeft.⁸

Het bewaren van bovenstaande gegevens leidt uiteraard tot inbreuk op de persoonlijke levenssfeer. Die inbreuk wordt nog vergroot omdat uit de opgeslagen verkeersgegevens inzage geven in het sociale netwerk van betrokkenen. Daarnaast leidt het ongericht opslaan van verkeersgegevens tot het bewaren van de communicatie van personen met een beroepsmatig verschoningsrecht.

Noodzaak niet aangetoond

13. Op grond van artikel 8 van het Europees Verdrag van de Rechten van de Mens ("EVRM") heeft een ieder recht op eerbiediging van zijn privéleven, zijn familie-



en gezinsleven, zijn woning en zijn correspondentie. Het is het recht op de eerbiediging van de persoonlijke levenssfeer. De inbreuk die de bewaarplicht maakt op dit recht is ook door de regering onderkend bij het tot stand komen van de Wet bewaarplicht telecommunicatiegegevens.⁹ Het tweede lid van artikel 8 EVRM stelt voorwaarden aan inbreuken op dit recht door de overheid.

Eén van de voorwaarden is dat deze inbreuk in een democratische samenleving noodzakelijk is. De evaluatie moet antwoord geven of en in welke mate deze inbreuk inderdaad in een democratische samenleving noodzakelijk is.

14. Om vast te stellen of voldaan is aan de criteria van artikel 8 lid 2 EVRM moet de relevante jurisprudentie met betrekking tot dit artikel worden meegewogen.
- Het Europese Hof voor de Rechten van de Mens ("EHRM") oordeelde in 2008 dat alleen al het bewaren van persoonsgegevens als een inbreuk op de persoonlijke levenssfeer van de betrokkenen moet gezien worden, ongeacht de vraag of deze persoonsgegevens daadwerkelijk opgevraagd worden.¹⁰ Aangezien gebruikers- en verkeersgegevens van nagenoeg alle burgers voor de duur van twaalf maanden bewaard worden, staat vast dat de inbreuk op de persoonlijke levenssfeer per definitie enorm is.
 - Het EHRM stelt verder dat een inbreuk alleen als "noodzakelijk in een democratische samenleving" kan worden beschouwd i) als er sprake is van een dringende maatschappelijke noodzaak ("pressing social need"), ii) als de maatregel in verhouding staat tot het nagestreefde legitieme doel en iii) als de rechtvaardiging relevant en voldoende is.¹¹ Vervolgens oordeelt het EHRM dat een maatregel die tot de opslag van biometrische persoonsgegevens van alle burgers die ooit eens verdachte zijn geweest (ook die later zijn vrijgesproken) verplicht, een disproportionele maatregel betreft en daarmee in strijd is met artikel 8 EVRM. Volgens het Hof is er geen sprake van een evenwichtige afweging van het publieke belang enerzijds en het belang van de persoonlijke levenssfeer van betrokkenen anderzijds. De bewaarplicht gaat nog verder, omdat daar ook de gegevens van nagenoeg alle verdachte én onverdachte burgers worden opgeslagen.¹²

In het licht van deze uitspraken zal in het kader van de evaluatie moeten worden beoordeeld of er in Nederland sprake is van een dringende maatschappelijke noodzaak die het bewaren van de telecommunicatiegegevens van alle Nederlanders rechtvaardigt. Daarnaast moet de bewaarplicht in verhouding staan tot het beoogde doel (proportionaliteit) en tevens de rechtvaardiging relevant en voldoende zijn.

- Belangrijk is daarbij het oordeel van het Hof van Justitie van de Europese Unie ("HvJEU") dat inbreuken op de persoonlijke levenssfeer "binnen de grenzen van het *strikt* noodzakelijke moeten blijven".¹³ Een maatregel is enkel strikt noodzakelijk indien hetzelfde of een vergelijkbaar resultaat niet behaald kan worden op een andere manier, waarbij minder inbreuk wordt gemaakt op fundamentele rechten van burgers.



- Tot slot moet bij de beoordeling van noodzakelijkheid nog rekening gehouden worden met de uitspraak van het EHRM¹⁴ waarin is bepaald dat “strikt noodzakelijk” niet gelijk gesteld kan worden aan “onmisbaar”. Dat de langdurige beschikbaarheid van telecommunicatiegegevens mogelijk onmisbaar is voor het bereiken van een bepaald doel, maakt nog niet dat gesproken kan worden van “noodzakelijk in een democratische samenleving”.
15. In artikel 52 van het Handvest van de Grondrechten van de Europese Unie is opgenomen dat beperkingen op rechten en vrijheden uit het handvest, waaronder dat op de eerbiediging van de persoonlijke levenssfeer, de wezenlijke inhoud van die rechten en vrijheden moet eerbiedigen. Dat is ook meermaals door het EHRM vastgesteld. In 2002 stelt het EHRM¹⁵ dat “the limitations (thereby) introduced must not restrict or reduce the right in such a way or to such an extent that the very essence of the right is impaired.” Het Roemeense Constitutionele Hof heeft om precies deze reden geoordeeld dat de bewaarplicht onverenigbaar is met artikel 8 EVRM.¹⁶ Omdat de bewaarplicht een enorme inperking op de persoonlijke levenssfeer van alle Nederlanders met zich meebrengt, moet ook dit punt in de evaluatie worden meegenomen.
16. De evaluatie zal verder ook moeten uitwijzen of de huidige regels subsidiair zijn. Beoordeeld moet worden of, als de gegevens inderdaad noodzakelijk zijn, deze gegevens niet al op een andere wijze beschikbaar zijn of kunnen zijn. Op grond van het Wetboek van Strafvordering hebben opsporingsdiensten niet alleen de bevoegdheden tot het vorderen van gegevens, maar ook tot het vorderen van het bewaren en beschikbaar houden van bepaalde gegevens.
- Aangezien aanbieders gegevens over het communicatiegedrag van hun klanten reeds voor andere doelen opslaan, moet serieus onderzocht worden of het huidige regime van het Wetboek van de Strafvordering niet al volstaat, al dan niet met een verhoudingsgewijs kleine aanpassing.

Gegevens worden niet afdoende beschermd

17. Uit de regels die worden gesteld aan de verwerking van persoonsgegevens valt af te leiden dat dergelijke gegevens altijd afdoende beveiligd moeten worden en dat de gegevens niet langer bewaard worden dan strikt noodzakelijk. Dat blijkt echter niet het geval, zodat de verwerking op zich niet voldoet aan de eisen van een rechtmatige verwerking.
18. Uit het onderzoek van het Agentschap Telecom bleek dat 92 procent van de onderzochte internetaanbieders geen of slechts enkele maatregelen hadden genomen voor de beveiliging van de onderhavige gegevens. Slechts acht procent van de aanbieders voldeed aan alle gestelde normen om de gegevens te beschermen tegen onrechtmatige verwerkingen.¹⁷ Het zelfde onderzoek toonde aan dat slechts een kwart van de aanbieders de gegevens binnen acht



dagen na het aflopen van de bewaartermijn verwijderde. Bijna 40 procent van de aanbieders verwijderde de gegevens in zijn geheel niet.¹⁸ Hieruit moet geconcludeerd worden dat de bewaarplicht is omgeven met onveilige opslag van gegevens.

Betrokkenen krijgen geen inzage in bewaarde gegevens

19. Ook hebben burgers in de praktijk geen mogelijkheid om de persoonsgegevens die door telefonie- en internetaanbieders worden verwerkt, in te zien. Verzoeken tot inzage in persoonsgegevens worden namelijk niet of slechts gedeeltelijk gehonoreerd. De betrokkene kan daardoor niet controleren of de verwerking juist, volledig, relevant en rechtmatig is

Anders dan in de Memorie van Toelichting is gesuggereerd, is het belang van het inzagerecht voor de burger in de praktijk onverminderd groot.¹⁹ De stelling dat “de relevante gegevens over zijn belgedrag doorgaans reeds zijn af te leiden uit de gespecificeerde factuur” is onjuist. Op de factuur zijn normaliter alleen die gesprekken en berichten opgenomen waarvoor kosten gerekend worden. Inkomende gesprekken en berichten worden dan ook niet op de factuur getoond. Bovendien ontbreken de bijzonder gevoelige locatiegegevens op de factuur.

Het wringt daarom dat in de praktijk burgers praktisch gezien geen gebruik kunnen maken van hun recht op inzage in de gegevens die door de aanbieders op grond van de bewaarplicht worden bewaard. Aanbieders proberen op dat punt verzoeken zoveel mogelijk in algemene termen te beantwoorden.²⁰ Bij verzoeken waarin expliciet om de onderhavige gegevens gevraagd wordt, is het antwoord bij sommige aanbieders beperkt tot minder dan drie procent van de beschikbare gegevens.²¹

Opsporings- en inlichtingendiensten vorderen lichtzinnig

20. Naast de gebreken in de manier waarop telecommunicatiebedrijven gegevens verwerken, handelen ook opsporings- en inlichtingendiensten niet zorgvuldig in de omgang met de gegevens. Uit het onderzoek van het Agentschap Telecom blijkt dat minstens 20 procent van de onderzochte internetaanbieders vastgesteld heeft dat opsporings- en inlichtingendiensten op onzorgvuldige wijze vorderingen doen.²²
21. Dat beeld wordt bevestigd bij de vorderingen van opsporings- en inlichtingendiensten van niet-historische gebruikersgegevens. Uit interne onderzoeken van het ministerie blijkt dat opsporing- en inlichtingendiensten het CIOT zonder bevoegdheid raadplegen, de rechtmatigheid van de vorderingen niet controleren en dat het gehele proces onvoldoende wordt gedocumenteerd.²³ Ook de bevindingen van het College Bescherming Persoonsgegevens zijn vernietigend.



Bij politiekorps Haaglanden kon van zes uit elf onderzochte vorderingen de rechtmatigheid niet aangetoond worden²⁴. Bij de Dienst Nationale Recherche waren dat er zelfs negen uit elf.²⁵

Andere risico's: datalekken en gebruik voor andere doelen

22. De onzorgvuldige handelwijze van telecommunicatiebedrijven vormt op zichzelf al een risico voor de privacy van burgers. De risico's van grootschalige opslag zijn echter nog omvangrijker aangezien de gebrekkige beveiliging kan leiden tot toegang tot de persoonsgegevens door onbevoegde derden. Dit is geen onrealistisch scenario: eerder dit jaar vond er bij KPN een digitale inbraak plaats waarbij volledige toegang is verkregen tot honderden servers. Deze servers werden volgens het Openbaar Ministerie gebruikt voor internetdiensten én opslag van informatie van klanten.²⁶
23. Een ander gevaar van de grootschalige opslag van gegevens is dat deze gegevens vroeg of laat voor andere dan de oorspronkelijk beoogde doelen wordt gebruikt ("function creep"). Dat ook dat geen onrealistisch scenario is, wordt duidelijk uit een recente uitspraak van het EHvJ (Bonnier Audio).²⁷ Het Hof oordeelde dat de data retentie richtlijn er niet aan in de weg staat dat beschikbare identificerende gegevens worden gebruikt in een geschil over de handhaving van het auteursrecht, ongeacht of deze gegevens zijn opgeslagen op grond van de bewaarplicht. Deze vorm van verdere verwerking is onverenigbaar met het doel waarvoor de gegevens werden bewaard, zodat er inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkenen.

Aanvullingen op de startnotitie

24. Naast de hiervoor genoemde inhoudelijke punten wil Bits of Freedom nog een enkele suggesties doen voor het behandelen en specificeren van de startnotitie. In de lijst van deskundigen die geraadpleegd worden ontbreken academici. Bits of Freedom draagt als suggestie graag voor: A.M. Arnbak, B.J. Koops en G.J. Zwenne. Aan de zijde van aanbieders raadt Bits of Freedom u aan om ook te spreken met G. Wabeke, manager Lawful Intercept bij KPN, A. Blom, directeur van BudgetPhone en S. van Geffen, managing director van Greenhost. In de literatuurlijst ontbreken verschillende belangrijke documenten waaronder:
 - T. Spapens, M. Siesling, E. de Feijter, "Brandstof voor de opsporing, evaluatie Wet bevoegdheden vorderen gegevens", 2011²⁸
 - Gelekte interne notitie Europese Commissie, 15 december 2011²⁹
 - European Digital Rights, "Shadow evaluation report on the Data Retention Directive", 17 april 2011³⁰
 - A.M. Arnbak, "Alles onder controle?", juli 2009³¹



- K. de Vries, R. Bellanova, P. de Hert, S. Gutwirth. "The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)" Privacy and data protection : an element of choice (to be published). Ed. S. Gutwirth, Y. Poullet, P. De Hert & R. Leenes. Springer, 2011.³²
- H.J. Albrecht, e.a., "Schützlücken durch Wegfall der Vorratdatenspeicherung?", juli 2011³³

Samengevat: is bewaarplicht noodzakelijk, proportioneel, effectief en subsidiair?

25. Bits of Freedom vertrouwt er op dat het ministerie, gezien de grote belangen, een grondige en degelijke evaluatie maakt. Tot op heden hebben de Europese Commissie en de Nederlandse regering de noodzaak van het bewaren van gegevens over het communicatiegedrag van nagenoeg alle zestien miljoen Nederlandse burgers niet steekhoudend kunnen aantonen.

In de evaluatie moet aangetoond worden dat de beoogde doelstelling is behaald. Dat moet onderbouwd worden met kwalitatieve en kwantitatieve informatie. De evaluatie zal ook moeten ingaan op de enorme inbreuk die de bewaarplicht maakt op de persoonlijke levenssfeer. De belangrijkste vraag is of de bewaarplicht noodzakelijk, proportioneel, effectief en subsidiair is.

De evaluatie zal bovendien moeten onderzoeken of de beveiliging van de gegevens voldoende is, of onbevoegde toegang tot gegevens voorkomen wordt, of de gegevens ook weer tijdig verwijderd worden en of de vordering van deze gegevens door opsporings- en inlichtingendiensten altijd rechtmatig is.

De evaluatie zal ook aandacht moeten besteden aan het gebruik van de gegevens voor andere doelen dan de bestrijding van ernstige criminaliteit. Ook moeten de problemen die betrokkenen ondervinden bij het effectueren van hun recht tot inzage moeten worden onderzocht.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Rejo Zenger



- 1 Tweede Kamer, 2006-2007, 31 145, nr. 3, p. 1
- 2 Richtlijn 2006/24/EG van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, artikel 1(1).
- 3 <https://www.bof.nl/2010/12/16/waardeloze-inbreng-justitie-voor-europese-evaluatie-bewaarplicht/>
- 4 <http://wiki.vorratsdatenspeicherung.de/images/D11574.pdf>
- 5 Jaarverslag en slotwet Ministerie van Veiligheid en Justitie 2010
- 6 WODC, Criminaliteit en rechtshandhaving 2010
- 7 Peter Hustinx, The moment of truth for the Data Retention Directive, uitgesproken op de conferentie "Taking on the Data Retention Directive" van 3 december 2010
- 8 Zie ook Malte Spitz' infographic op <http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten>
- 9 Tweede Kamer, 2006-2007, 31 145, nr. 3, p. 25
- 10 EHRM, 4 december 2008, 30562/04, S and Marper v. The United Kingdom, par. 121
- 11 EHRM, 4 december 2008, 30562/04, S and Marper v. The United Kingdom, par. 101
- 12 EHRM, 4 december 2008, 30562/04, S and Marper v. The United Kingdom, par. 125
- 13 EHvJ, 9 november 2010, C-92/09 en C-93/09, Volker und Markus Schecke, par. 86
- 14 EHRM, 7 december 1976, 5493/72, Handyside v. The United Kingdom, par. 48. Zie ook EHRM, 25 maart 1983, 5947/72, Silver a.o v. The United Kingdom, par 97.
- 15 EHRM, 11 juli 2002, 28957/96, Goodwin v. The United Kingdom, par. 99
- 16 <http://www.edri.org/edriagram/number7.23/romania-decision-data-retention>
- 17 Agentschap Telecom, 3 mei 2010, Eindrapport nulmeting Wet bewaarplicht telecommunicatiegegevens, p. 14
- 18 Agentschap Telecom, 3 mei 2010, Eindrapport nulmeting Wet bewaarplicht telecommunicatiegegevens, p. 15
- 19 Tweede Kamer, 2006-2007, 31 145, nr. 3, p. 27
- 20 https://rejo.zenger.nl/files/20110616-reactie-op-inzageverzoek_redacted.pdf
- 21 https://rejo.zenger.nl/files/20110826-reactie-hernieuwd-inzageverzoek_redacted.pdf
- 22 Agentschap Telecom, 3 mei 2010, Eindrapport nulmeting Wet bewaarplicht telecommunicatiegegevens, p. 20
- 23 Ministerie van Justitie, 19 april 2010, Eindrapport Audit CIOT 2009
- 24 College Bescherming Persoonsgegevens, april 2011, Onderzoek CIOT-bevragingen Politiekorps Haaglanden
- 25 College Bescherming Persoonsgegevens, april 2011, Onderzoek CIOT-bevragingen Dienst Nationale Recherche
- 26 <http://www.om.nl/actueel-0/nieuws-persberichten/@158613/17-jarige-jongen/>
- 27 EHvJ, 19 april 2012, C-461/10
- 28 http://wodc.nl/images/volledige-tekst_tcm44-335387.pdf
- 29 http://quintessenz.at/doqs/0001000116/2011_12_15_Eu_Commission_data_retention_reform.pdf, zie ook <https://www.bof.nl/2012/01/10/europese-commissie-blind-voor-kritiek-bewaarplicht/>
- 30 http://www.edri.org/files/shadow_drd_report_110417.pdf
- 31 https://www.bof.nl/live/wp-content/uploads/2009/12/Alles_onder_controle_-_Masterscriptie_A.M._Arnbak_-_5749131-zonder-bijlage.pdf
- 32 http://works.bepress.com/serge_gutwirth/53/
- 33 http://vds.brauchts.net/MPI_VDS_Studie.pdf