Advies College bescherming persoonsgegevens
Wetsontwerp implementatie Europese Richtlijn Dataretentie

Behorend bij de aanbiedingsbrief van 22 januari 2007

INHOUDSOPGAVE

1. Bewaartermijn van achttien maanden

Wetsvoorstel

Het wetsvoorstel schrijft een bewaartermijn voor van 18 maanden, voor zowel telefonie- als internetverkeersgegevens. In de Memorie van Toelichting (hierna: MvT) wordt de noodzaak voor deze termijn onderbouwd met een beroep op het rapport "Wie wat bewaart die heeft wat" van de Erasmus Universiteit uit 2005.[1] Dat rapport concludeert dat een bewaartermijn van twaalf maanden wenselijk is. Blijkens de MvT dient die termijn als minimum aangemerkt te worden. *De door de onderzoekers van de Erasmus Universiteit aanbevolen bewaartermijn moet vanuit het oogpunt van effectiviteit van de opsporing echter als een minimum worden beschouwd. Gelet op de bevindingen van de Erasmus Universiteit zal het minder veelvuldig voorkomen dat de bewaarde gegevens na twaalf maanden nog nodig blijken voor de opsporing van ernstig strafbare feiten maar strafrechtelijke onderzoeken mogen niet mislukken doordat die termijn is verlopen.*[2] Uit het wetsvoorstel blijkt voorts dat Nederland geen beroep doet op de mogelijkheid om een langere bewaartermijn te kiezen dan 24 maanden. In de MvT ontbreekt (nog) een invulling van de (beoogde) bewaartermijnen in overige lidstaten. Het betreffende hoofdstuk 6 is pro memorie gelaten.

Bepalingen in de Richtlijn

De Richtlijn dataretentie[3] biedt in artikel 6 een bandbreedte voor de bewaartermijn van ten minste zes maanden en ten hoogste twee jaar. Artikel 12 voegt daaraan toe dat lidstaten de in de Richtlijn bepaalde gegevens voor een langere, maar niet onbeperkte, termijn kunnen bewaren als specifieke omstandigheden dat rechtvaardigen.

[1] Wie wat bewaart die heeft wat. Onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens van telecommunicatieverkeer (juni 2005) Erasmus Universiteit Rotterdam, blz. 5.
[2] Concept Memorie van Toelichting 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), ongenummerde versie, zoals toegestuurd aan het CBP per brief van 11 december 2006, blz. 5.
[3] Richtlijn 2006/24/EG 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. Hierna: de Richtlijn.

1a Onderbouwing noodzaak achttien maanden

Het CBP en de Groep Gegevensbescherming Artikel 29 hebben zich steeds op het standpunt gesteld dat het invoeren van een bewaarplicht voor de historische verkeersgegevens van alle burgers een zeer ingrijpende maatregel is waarvan de noodzaak onweerlegbaar dient te worden aangetoond.[4] In artikel 8 EVRM is het fundamentele recht van burgers verankerd op eerbiediging van hun persoonlijke levenssfeer. De overheid mag bij wet alleen inbreuk maken op dat recht voorzover dat in een democratische samenleving *noodzakelijk* is. De noodzaak stelt hoge eisen aan de proportionaliteit van elke specifieke maatregel die de persoonlijke levenssfeer van burgers inperkt. De algemene bepalingen uit de Richtlijn laten onverlet dat elke nationale implementatie zelfstandig getoetst moet worden aan artikel 8 EVRM en de bijbehorende jurisprudentie van het EHRM. Dat geldt nadrukkelijk voor de noodzaak van een bewaartermijn die langer is dan de termijn die noodzakelijk is voor de bedrijfsvoering van de aanbieders.

Het CBP stelt vast dat de MvT nauwelijks uitlegt hoe de termijn van achttien maanden is bepaald. De MvT stelt enerzijds dat strafrechtelijke onderzoeken niet mogen mislukken doordat de termijn van twaalf maanden is verlopen, en doet anderzijds een beroep op de bewaartermijn in andere lidstaten. *Ook om te voorkomen dat een onevenwichtige verhouding in het rechthulpsverkeer tussen de lidstaten bij de verstrekking van bewaarde telecommunicatiegegevens zou ontstaan, verdient het aanbeveling om te kiezen voor enige verlenging van de door de Erasmus Universiteit aanbevolen bewaartermijn.*[5] Voordat het CBP ingaat op de Europese harmonisatie, wil het, in relatie tot de bescherming van de persoonlijke levenssfeer, ingaan op de onderbouwing van de specifieke noodzaak in Nederland van het bewaren van verkeersgegevens voor opsporingsdoeleinden.

Met het oog op de proportionaliteit van de inbreukmakende maatregel wijst het CBP erop dat naarmate de beschikbare gegevens een grotere periode beslaan, er door de opsporingsinstanties meer inzicht wordt verkregen in de handel en wandel van onschuldige personen.

In navolging van de recente adviezen van de Groep Gegevensbescherming Artikel 29 over dit onderwerp[6] adviseert het CBP daarom een geharmoniseerde minimale toepassing van de bepalingen van de Richtlijn, met een bewaartermijn die zo min mogelijk afwijkt van het oorspronkelijke doel waarvoor de gegevens door de aanbieders van communicatiediensten worden opgeslagen. Het is noodzakelijk om de lengte van een bewaarverplichting, die immers indruist tegen de algemene vernietigingsplicht uit Richtlijn 2002/58/EG, te onderbouwen met overtuigende argumenten. *"Zoals hierboven gezegd, moet de voor een algemene gegevensbewaarplicht aangevoerde rechtvaardigingsgrond met harde bewijzen aannemelijk kunnen worden gemaakt. Dat geldt ook voor de maximumtermijnen die in dat geval van toepassing zouden moeten zijn."*[7]

---

[4] Zie onder andere van de Groep Gegevensbescherming Artikel 29: Advies 4/2001 over de ontwerp-overeenkomst van de Raad van Europa inzake computercriminaliteit, 10/2001 over een evenwichtige benadering in de bestrijding van terrorisme, 5/2002 over het verplicht systematisch bewaren van telecommunicatieverkeers-gegevens, 9/2004 over het ontwerp-kaderbesluit [...], 4/2005 over het voorstel voor een Richtlijn [...] en Advies 3/2006 inzake Richtlijn 2006/24/EG. Het CBP heeft daarnaast 2 september 2002 een brief verstuurd aan de minister van Justitie over het voornemen om een bewaarplicht in te voeren, in september 2004 een uitgebreide bijdrage geleverd aan de consultatie van de Europese Commissie, een opinie-artikel voor NRC-Handelsblad dd 22 augustus 2005 en een bijdrage geleverd aan een hoorzitting van de Tweede Kamer op 28 september 2005.
[5] MvT, blz 5.
[6] Artikel 29, Advies 3/2006 en Advies 4/2005.
[7] Artikel 29, Advies 4/2005, blz. 8.

Voor die bewijzen leunt de MvT voornamelijk op het rapport van de Erasmus Universiteit. Het CBP meent echter dat dat onderzoek onvoldoende bewijs levert van de noodzaak van een langere bewaartermijn dan gehanteerd in de huidige praktijk waarin aanbieders verkeersgegevens voor hun eigen bedrijfsvoering bewaren.

De onderzoekers kregen 65 opsporingsdossiers tot hun beschikking waarin verkeersgegevens van vaste en mobiele telefonie een belangrijke rol speelden. Ze constateerden dat de verkeersgegevens in vrijwel al die gevallen beschikbaar waren bij de aanbieders. *"De door de opsporing gevraagde gegevens werden in nagenoeg alle onderzochte zaken geleverd."*[8]

De selectie bevatte geen dossiers waarin internetverkeersgegevens een rol speelden. De onderzoekers zijn daarop met vertegenwoordigers van politie en Justitie gaan praten over de wenselijkheid van een langere bewaartermijn. "*Nu op basis van het dossieronderzoek geen valide conclusies kunnen worden getrokken ten aanzien van nut en noodzaak van een (verruiming van de) bewaartermijn is besloten om door middel van interviews en een ronde tafel-gesprek meer inzicht te verkrijgen in de problemen die binnen de opsporing worden ondervonden ten aanzien van het verkrijgen van historische verkeersgegevens met betrekking tot communicatie via internet service providers."*[9]

Het is op basis van deze gesprekken, en niet op basis van het onderzoek naar het feitelijk gebruik van verkeersgegevens, dat de conclusie is getrokken dat een bewaartermijn van één jaar voor alle verkeersgegevens wenselijk is. Daarbij is al een aanzienlijke marge ingebouwd ten opzichte van de onderzochte praktijk.

Met de aldus tot stand gekomen conclusie dat een bewaarplicht van een jaar wenselijk zou zijn, is evenwel nog niet voldaan aan het noodzakelijkheidscriterium uit artikel 8 EVRM: *"(a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable […]."*[10] De door het EVRM vereiste onderbouwing van de proportionaliteit ontbreekt dus.

De thans beoogde bewaartermijn van achttien maanden staat verder in schril contrast met de herhaalde verzekeringen van de minister van Justitie aan de Kamer dat Nederland een bewaartermijn nastreefde van twaalf maanden voor telefoniedata en zes maanden voor internetdata. Minister Donner: *Ik heb aangegeven dat ik in ieder geval voor Nederland de ruimte wilde voor een bewaartermijn van een jaar, en voor internetgegevens voor een termijn van een half jaar. Dat is gerealiseerd; dat kan nu. Dat andere lidstaten in hun nationale wetgeving eventueel langere termijnen vaststellen, moeten zij weten.*[11] Tijdens dat debat nam een ruime Kamermeerderheid een motie aan ter afkeuring van de richtlijn, met name omdat er een langere bewaartermijn dan twaalf maanden mogelijk werd gemaakt.[12]

[8] Erasmus, blz. 23.
[9] Erasmus, blz. 23.
[10] EHRM 25 maart 1983, Silver and others v. United Kingdom, nr. 97.
[11] *Handelingen II* 2005-2006, blz. 3405.
[12] de motie-Dittrich c.s. (23490, nr. 407). "Gelet op het feit dat de Richtlijn van het Europese Parlement en de Raad betreffende de bewaring van gegevens (PE-CONS 3677/05) niet aan de voorwaarden van een bewaartermijn van maximaal 1 jaar, een adequate regeling voor de toegang tot opgeslagen gegevens en een compensatieregeling voor een level playing field voldoet; (...)"

Ten slotte maakt het CBP uit de MvT op dat de bewaartermijn kennelijk op het laatste moment is veranderd van twaalf in achttien maanden. Op drie plaatsen in de tekst is nog sprake van een bewaartermijn van twaalf maanden.[13]

1b Harmonisering in EU-verband

In de MvT wordt gewezen op het belang van een langere bewaartermijn dan de twaalf maanden die volgens het Erasmus rapport nodig zouden kunnen zijn in verband met rechtshulpverzoeken uit andere lidstaten. Daar is echter geen onderzoek naar gedaan.

Om de effectiviteit te vergroten van verzoeken ligt het niet voor de hand om te kijken naar een verlenging van de bewaartermijn. Veel eerder moet gekeken worden naar stroomlijning van de procedures en formaliteiten voor internationale rechtshulp. In langdurige internationale onderzoeken kan voorts bij herhaling worden verzocht om de bewaarde gegevens.

De belangrijkste grondslag voor de Richtlijn, verwoord in artikel 1, is het harmoniseren van de nationale bepalingen in de lidstaten over bewaarplichten, teneinde te garanderen dat de gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.

Het CBP heeft slechts beperkt inzicht in implementaties en voorstellen in andere EU lidstaten, maar stelt vast dat van enige harmonisatie van de bewaartermijn vooralsnog geen sprake is. Buurland Duitsland[14] kiest voor een bewaartermijn van zes maanden, net als Finland en Tsjechië[15]. Ook Zweden, één van de vier initiatiefnemers van de totstandkoming van een Europese bewaarplicht, lijkt voor een minimumimplementatie te kiezen. Andere landen als Frankrijk[16], Denemarken[17], Spanje[18] en België kiezen voor een bewaartermijn van twaalf maanden. Alleen Italië[19] en Ierland[20] kennen langere termijnen, van respectievelijk viereneenhalf en drie jaar.

---

[13] MvT blz. 10, blz. 20 en blz. 32. Blz. 10: (*...) negen maanden langer bewaard zal worden (dan het gemiddelde van drie maanden).* Blz. 20: *Met de in dit wetsvoorstel voorgestelde bewaarperiode wordt aangesloten bij de door de Erasmus Universiteit aanbevolen termijn. In het licht van de betrokken belangen is de voorgestelde termijn dan ook bezwaarlijk als disproportioneel aan te merken.*Blz. 32: *De verplichting tot vernietiging impliceert dat, zodra één jaar is verstreken sedert de datum van inwerkingtreding van dit wetsvoorstel, de bewaarde gegevens dagelijks worden vernietigd.*

14 Het Duitse wetsontwerp met bijbehorende memorie van toelichting is sinds 8 november 2006 in consultatie. URL wetsontwerp: http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/RefETeil1neu.pdf URL MvT: http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/RefETeil2neu.pdf

[15] Verordening van de Tjechische telecommunicatie autoriteit (CTÚ), medio december 2005. Het decreet schrijft bewaartermijnen van drie tot zes maanden voor. Engelstalige informatie: http://www.ctu.cz/main.php?pageid=178

[16] Frankrijk: Décret n° 2006-358 du 24 mars 2006 d'application de la loi sur la sécurité quotidienne (LSQ), relatif à la conservation des données de communication, URL: http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSD0630025D

[17] Denemarken: Executive Order (988/2006), URL: http://www.jm.dk/image.asp?page=image&objno=76136 en Guidelines (174/2006), URL: http://www.jm.dk/wimpdoc.asp?page=document&objno=76135, beiden van 28 september 2006. Ze treden beide in werking op 15 september 2007.

[18] Spanje kent raamwetgeving die een bewaarplicht voor internetdata van twaalf maanden mogelijk maakt, maar geen concrete delegatiebepalingen, evenmin als een bewaarplicht voor telefoniedata. Ley de Servicios de la Sociedad de la Información (LSSI), in werking sinds 12 oktober 2002, URL: http://www.lssi.es/

[19] Italië kende sinds 2003 via Decreet 259/2003, 'Codice delle comunicazioni elettroniche' een bewaarplicht voor telefoniedata van 30 maanden, met een verlengingsmogelijkheid van 24 maanden en voor internetdata een bewaarplicht van zes maanden, met een verlengingsmogelijkheid van zes maanden. Eind juli 2005 werd het besluit genomen (artikel 6) om alle verkeersgegevens, inclusief internetdata te bewaren tot 31 december 2007, Nuove norme per il contrasto del terrorismo internazionale e della criminalità, in werking sinds 1 augustus 2005, URL: http://www.interno.it/legislazione/pages/articolo.php?idarticolo=646

[20] Ierland heeft alleen een bewaarplicht voor telefonieverkeersgegevens. Irish Criminal Justice (Terrorist Offences) Act, 2005, Deel 6, paraaf 63, URL: http://www.irishstatutebook.ie/ZZA2Y2005S63.html

Het CBP weet niet of de Commissie reeds een oordeel heeft uitgesproken over de extra lange termijnen in deze drie landen, noch over de specifieke omstandigheden die deze langere bewaartermijnen zouden moeten rechtvaardigen.

In het Verenigd Koninkrijk ten slotte, de grote motor achter het invoeren van een Europese bewaarplicht verkeersgegevens, zeker na de aanslagen van 7 juli 2005, wordt vooralsnog volstaan met vrijwillige afspraken met een aantal grote operators. Tegen volledige kostenvergoeding verstrekken de aangesloten operators al enige tijd de gevraagde gegevens. Het Verenigd Koninkrijk kent sinds eind 2001 overigens wel de mogelijkheid om een wettelijke bewaarplicht in te voeren.[21]

Gegeven het belang van de bescherming van persoonsgegevens en de verplichte afweging tussen de rechten van burgers en de noodzaak van het belang van de staat om daar een inbreuk op te maken, hecht het CBP grote waarde aan de Duitse keuze voor een minimumimplementatie van de Richtlijn.

De Duitse keuze voor een minimale bewaartermijn is gemotiveerd door consequent verzet van het Parlement tegen de invoering van een bewaarplicht. Dat verzet is mede gebaseerd op onderzoek van branche-organisatie Bitkom naar het nut en de noodzaak van het bewaren van verkeersgegevens. Het onderzoek vergelijkt de wetgeving en het gebruik van historische verkeersgegevens in Oostenrijk, Frankrijk, Italië, Nederland, Zweden, Spanje, het Verenigd Koninkrijk en de Verenigde Staten. Ook uit dat rapport vloeide de conclusie voort dat een langere bewaartermijn dan (gemiddeld) drie maanden niet gerechtvaardigd kon worden.[22]

Samenvatting

Het CBP meent dat Nederland zou moeten volstaan met de minimaal verplichte bewaartermijn van zes maanden, die in veel gevallen al langer is dan de termijn waarvoor de gegevens noodzakelijk zijn voor de bedrijfsvoering. Voor een langere bewaartermijn zijn nut en noodzaak niet aangetoond. Ook een beroep op de noodzaak tot harmonisatie van de termijn faalt, gezien de grote verschillen in implementatie in de verschillende lidstaten.

[21] De mogelijkheid van het uitvaardigen van een bewaarplicht is vastgelegd in de Code of Practice on Data Retention die aangenomen is als deel 11 van de Anti-terrorism, Crime and Security Act. URL: http://security.homeoffice.gov.uk/ripa/communications-data/data-code-of-practice/ De bijbehorende, herziene, concept Code of Practice van 10 maart 2005 beschrijft geen bewaartermijn, alleen de toegangsmogelijkheden. URL: http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf?view=Standard&pubID=401821

[22] Samenvatting BITKOM onderzoek (Duitstalig, okttober 2004), URL: http://www.bitkom.org/files/documents/Zusammenfassung_Studie_VDS.pdf URL volledig rapport: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf

2. De keuze voor delegatiebepalingen

Wetsvoorstel
Bij het omzetten van de bepalingen uit de Richtlijn kiest het wetsvoorstel ervoor om vijf belangrijke beslissingen uit te stellen en te volstaan met open delegatiebepalingen, met name betreffende de soorten gegevens die bewaard dienen te worden; de keuze voor centrale of decentrale opslag en het bijhouden van statistieken over het gebruik van de gegevens. Daarnaast worden de voorgeschreven beveiligingsmaatregelen gedelegeerd naar een mogelijk op te stellen AmvB, evenals de invulling van de manier waarop en de snelheid waarmee aanbieders moeten kunnen voldoen aan een verzoek.

Bepalingen in de Richtlijn
De Richtlijn schrijft in artikel 5 gedetailleerd voor welke categorieën gegevens bewaard moeten worden. Blijkens overweging 12 van de Richtlijn moet deze lijst als maximum worden opgevat. Voor het bewaren van andere gegevens (zoals oproeppogingen zonder resultaat) kunnen de lidstaten een beroep doen op artikel 15 eerste lid van Richtlijn 2002/58/EG. Wetgeving die op grond van dat artikel wordt uitgevaardigd, dient afzonderlijk te voldoen aan het vereiste dat de wetgeving *in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in artikel 13, lid 1, van Richtlijn 95/46/EG.*[23]

Wat de keuze betreft tussen centrale en decentrale opslag schrijft overweging 13 van de Richtlijn voor dat voorkomen moet worden dat gegevens twee keer worden bewaard.

2a Soorten gegevens
De keuze om de soorten gegevens niet in de wetstekst zelf, maar in een AmvB op te nemen, strookt niet met de keuze die in de Richtlijn is gemaakt over de te bewaren gegevens. Aanvankelijk stelde de Europese Commissie voor om een lijst gegevens als bijlage bij de Richtlijn te voegen. Daarbij zou een aparte, versnelde besluitvormingsprocedure gelden (de zogenaamde 'comitologie') voor aanpassingen van de lijst. Het Europees Parlement heeft met grote meerderheid een amendement aangenomen van de liberale rapporteur Alexandre Alvaro om de gegevens in de tekst van de Richtlijn zelf op te nemen. Daarbij is ook expliciet gekozen voor een zwaardere procedure van aanpassing van de soorten te bewaren gegevens, met volledig instemmingsrecht van het Europees Parlement.

Uit de Aanwijzingen voor de regelgeving (Ar)[24], met name uit de toelichting bij Aanwijzing 22 Ar maakt het CBP op dat hoofdelementen van een richtlijn in de wet zelf dienen te worden opgenomen en dat "*ter zake van welke delegatie toelaatbaar is, steeds (dient) te worden onderzocht welke elementen van een regeling zo gewichtig zijn dat de volksvertegenwoordiging rechtstreeks bij de vaststelling moet worden betrokken.*" Het is evident dat de lijst te bewaren gegevens een hoofdelement is van de wetgeving

[23] Richtlijn 2002/58/EG, Artikel 15 eerste lid.
[24] Staatscourant 1996, blz. 177.

waarbij dus het primaat van de wetgever voorop dient te staan. Het CBP ziet in het Duitse wetsontwerp een goed model voor een dergelijke implementatie.[25]

Locatiegegevens gedurende de communicatie
Uit de MvT blijkt dat Nederland in de voorgenomen delegatiebepaling verder wil gaan dan de soorten gegevens die de Richtlijn voorschrijft. Aanbieders zouden ook de locatiegegevens (van mobiele telefoons en bijvoorbeeld laptops en pda's die gebruik maken van mobiele datacommunicatie) moeten bewaren die *gedurende de communicatie* ontstaan.[26] Dit zou volgens de MvT alleen een verlenging betekenen van de bestaande verplichtingen volgens het bestaande Besluit bijzondere vergaring nummergegevens. Het CBP is van mening dat dit een onjuiste lezing is van de verplichtingen in dat besluit. Het besluit is genomen met het oog op het achterhalen van de identiteit van een af te tappen houder van een prepaid mobiele telefoon. Justitie geeft in een dergelijk geval aan een aanbieder door op welke tijdstippen (ten minste twee) en vanaf welke locaties er met een toestel is gebeld. Alleen voorzover de operators de gevraagde gegevens verwerken, kunnen zij gevraagd worden de locatiegegevens achterhalen. Het besluit omvat nadrukkelijk geen vergaarplicht en schept dus geen verplichting om alle locatiegegevens gedurende de communicatie drie maanden te bewaren. In de praktijk hoeven aanbieders alleen de mastgegevens te bewaren van de mast waarop de communicatie is gestart.[27]

Het bewaren van locatiegegevens gedurende de communicatie is volgens het CBP bovenmatig aan de Richtlijn en als voorgenomen delegatiebepaling in strijd met Aanwijzing 337 AR. Dat bepaalt dat het niet is toegestaan om bij implementatie van een richtlijn andere regels op te nemen dan voor de implementatie noodzakelijk zijn.

Maar ook als deze extra categorie opgenomen zou worden in een apart wetsvoorstel, met een beroep op de uitzonderingsmogelijkheid van artikel 15 eerste lid 2002/58/EG, acht het CBP het bewaren van deze categorie gegevens disproportioneel. Deze categorie is met reden uitgesloten van het toepassingsgebied van de Richtlijn, omdat het neerkomt op een te indringende, alomvattende verborgen surveillance van de verplaatsingen van zeer grote aantallen onverdachte burgers. De Duitse memorie van toelichting verwijst expliciet naar het debat in het Europees Parlement over dit onderwerp en stelt vast dat de Richtlijn juist proportioneel is omdat deze gegevens niet bewaard hoeven te worden.[28]

---

[25] In het nieuwe artikel 110a TeleKommunikationsGesetz (TKG), "Speicherungspflichten für Verkehrsdaten" geeft het tweede lid een specificatie van de te bewaren verkeersgegevens van vaste, mobiele en internettelefoondiensten, het derde lid een specificatie van de e-mailverkeersgegevens en het vierde lid een specificatie van de verkeersgegevens met betrekking tot internettoegang.
[26] MvT blz 4: "*Voor de categorie locatiegegevens zal - in afwijking van de richtlijn- worden bepaald dat ook de locatiegegevens die worden gegenereerd na aanvang van de communicatie moeten worden bewaard.*" en blz 7: "*In het Besluit bijzondere vergaring nummergegevens (Stb. 2002, 31) is deze bestandsanalyse uitgewerkt. De aanbieder is gehouden om de voor de bestandsanalyse benodigde gegevens gedurende een periode van drie maanden te bewaren. Het betreft hier de gegevens betreffende de tijdstippen waarop telecommunicatie heeft plaatsgevonden, de met die tijdstippen en de desbetreffende telecommunicatie corresponderende nummers en de basisstations waarbij deze gegevens zijn binnengekomen.*" (...) *Dit impliceert dat de bewaartermijn van drie maanden voor de daarvoor benodigde gegevens wordt verhoogd naar achttien maanden.*"
[27] Overgenomen uit de Gezamenlijke reactie Aanbieders op consultatie Wetsvoorstel Dataretentie, blz. 5.
[28] Duitse Begründung, blz. 64: "*(...)insbesondere da besonders kostenträchtige Speicherungsvorgaben auf europäischer Ebene verhindert werden konnten (z.B. Speicherung ,,erfolgloser Anrufversuche", auch wenn diese von den Diensteanbietern bisher nicht gespeichert oder protokolliert werden; Speicherung van Standortdaten auch während und am Ende von Mobilfunkverbindungen).*"

2b Centrale of decentrale opslag

Overweging 13 van de Richtlijn schrijft voor dat de gegevens zodanig worden bewaard dat *voorkomen wordt dat gegevens twee keer worden bewaard*. Die overweging sluit uit dat lidstaten voor de bewaarplicht een model zouden kiezen als het CIOT in Nederland, het Centraal Informatiepunt Opsporing Telecommunicatie. Dat is een systeem waarbij telefoon- en internet aanbieders de naam, adres en woonplaatsgegevens van hun klanten kopiëren naar een aparte server die bevraagd kan worden via het CIOT. De bevoegde autoriteiten kunnen via het CIOT alle aanbieders gelijktijdig bevragen om de identiteit van de houder te achterhalen van een bepaald nummer, of omgekeerd, het nummer behorend bij een bepaalde identiteit. Tijdens debatten in de Tweede Kamer en in brieven heeft de Minister van Justitie herhaaldelijk aangegeven dat zijn voorkeur voor implementatie van de bewaarplicht uitging naar een CIOT-achtige oplossing.[29] Daarbij liet hij de mogelijkheid open of de gegevens verdubbeld moesten worden of onmiddellijk doorgeleid naar een centraal serverpark. Het CBP stelt vast dat er bij de keuze voor een CIOT-achtige oplossing altijd sprake is van verdubbeling van een bepaalde set gegevens, namelijk van de gegevens die nodig zijn voor de eigen bedrijfsvoering (drie tot zes maanden, afhankelijk van bijvoorbeeld de factuurtermijn). De verdubbeling van deze set gegevens is volgens het CBP in strijd met de Richtlijn.

Het CBP adviseert in navolging van de aanbevelingen van de Groep Gegevensbescherming Artikel 29 een *decentrale, logisch gescheiden* opslag van de specifiek voor opsporingsdoeleinden te bewaren verkeersgegevens. Voor de op grond van artikel 13.2a Tw te bewaren gegevens zullen hoe dan ook andere regels gelden voor bewaring, gebruik, verstrekking, beveiliging en vernietiging. Dat kan een aanbieder niet realiseren zonder die gegevens logisch te scheiden van de voor eigen bedrijfsdoeleinden verwerkte gegevens.

De MvT refereert voorts aan een apart onderzoek dat door Verdonck, Klooster & Associates BV is verricht. Dit rapport concludeert dat een centrale opslag van de gegevens de voorkeur geniet, vanuit kostenoverwegingen en omdat de gegevens makkelijker te beveiligen zouden zijn. De uitkomsten van dit onderzoek bieden echter nog onvoldoende houvast om een keuze te maken voor centrale of decentrale opslag, stelt de MvT. Uit de bijdrage aan de consultatie over het wetsontwerp van vrijwel alle telefoon- en internetaanbieders in Nederland[30], maakt het CBP op dat de aanbieders zich unaniem distantiëren van de conclusies van bovengenoemd onderzoek, met name ook als het gaat om een eventuele voorkeur voor een centrale opslag.

Het CBP vindt dat het rapport ten onrechte geen rekening houdt met de risico's die een centrale opslag met zich meebrengt, zoals thans nog niet voorzien nevengebruik. Naar de ervaring van het CBP schept ieder aanbod zijn eigen vraag.

Een decentrale opslag heeft aan de andere kant een belangrijk voordeel dat niet door de MvT is onderkend, namelijk dat de aanbieders een extra controle uitvoeren op de

[29] Bijvoorbeeld in de aanbiedingsbrief bij het Erasmus rapport, *Kamerstukken II* 2004-2005, 23 490, nr. 388, blz. 7: "*Het CIOT-model kent vele voordelen, waaronder de kosteneffectiviteit. Dit model is aanzienlijk goedkoper dan het model waarbij aanbieders afzonderlijk systemen moeten ontwikkelen om aan de bewaarplicht te voldoen. Voor de aanbieders is het voordeel van toepassing van het CIOT-model gelegen in het feit dat het bewaren, doorzoekbaar maken en zoeken van de gegevens wordt verricht door het CIOT.*"

[30] Gezamenlijke reactie Aanbieders op consultatie Wetsvoorstel Dataretentie, verstuurd aan het Ministerie van Economische Zaken op 18 januari 2007.

uitvoerbaarheid van een bevel. Ervaringen met het introduceren van nieuwe strafvorderlijke bevoegdheden in de telecomsector tonen aan dat er behoefte is aan veel overleg over de precieze vraagstelling en de mogelijke antwoorden. Het rapport van de Tilburgse universiteit over de evaluatie van zeven jaar aftapbeleid *"beveelt investeringen in kennis en kunde aan op de werkvloer (niet alleen maar wel met name bij de behoeftestellers"*[31] De ervaringen met aftappen nopen tot grote terughoudendheid bij het willen automatiseren van zoekvragen door de complexe databases met historische verkeersgegevens. Vaak is voor het leveren van een nauwkeurig antwoord een extra bewerking nodig. De expertise van de aanbieders kan daarbij niet steeds worden gemist.

2c Overige delegatiebepalingen
Het CBP begrijpt niet waarom de verplichting tot het bijhouden van statistieken, zoals de Richtlijn die voorschrijft in artikel 10, niet is omgezet in de wetstekst zelf. Het CBP gaat hier uitgebreider op in bij het bespreken van controlemiddelen op het rechtmatig gebruik van de gegevens.

Ten aanzien van de beveiligingsmaatregelen waartoe de Richtlijn verplicht, kan het CBP zich wel voorstellen dat delegatie nuttig is, omdat het gaat om gedetailleerde technische specificaties. Deze delegatie heeft geen facultatief karakter, en moet dus nader worden ingevuld in de MvT.

Ten slotte, als het gaat om de mogelijke delegatiebepaling over het invullen van het in de Richtlijn vervatte criterium 'onverwijld' voor het voldoen aan een vordering verkeersgegevens, verwijst de MvT naar de *thans geldende afspraken op operationeel niveau, die tussen de aanbieders en de behoeftestellende diensten zijn overeen gekomen*.[32] Het CBP acht het van belang dat in de MvT wordt vastgelegd dat die huidige afspraken een periode van één tot vijf werkdagen bestrijken, afhankelijk van de bewerkingen die een aanbieder moet doen om het gevraagde gegeven te produceren.
Een eventueel op te stellen AmvB met een nadere invulling van de termijnen zou in ieder geval een reflectie moeten zijn van de praktijk bij grote en bij kleine aanbieders, zonder een eventuele leversnelheid van één specifieke aanbieder dwingend op te leggen aan alle aanbieders.

Samenvatting
Het CBP acht de keuze om de soorten gegevens, de wijze van opslag en de verplichting tot het bijhouden van statistieken op te nemen in delegatiebepalingen onwenselijk en wetstechnisch onjuist. Bij het vaststellen van de soorten gegevens dient de wetstekst zich te beperken tot de gegevens die in de Richtlijn worden voorgeschreven. Het uitbreiden van de bewaarplicht naar gegevens die *gedurende de communicatie* worden gegenereerd kan alleen als zelfstandig wetsvoorstel worden ingediend na een eigen toetsing aan de vereisten van artikel 8 EVRM. Het voornemen om deze gewichtige elementen van de regeling vast te stellen in delegatiebepalingen is bovendien in strijd met Aanwijzing 22 Ar.
Het feit dat de MvT openlaat of er gekozen wordt voor centrale of decentrale opslag is in strijd met overweging 13 van de Richtlijn. Het CBP acht decentrale opslag, met een strikte *logische* scheiding van de operationele data, onontkoombaar.

[31] Koops, B., R. Bekkers, F. Bongers & M. Fijnvandraat. Evaluatie aftapbeleid, Een evaluatie van hoofdstuk 13 Telecommunicatiewet, Tilburg, november 2005, blz. 9.
[32] MvT, blz. 12.

3. Begrenzing van de toegang tot de bewaarde gegevens

Wetsvoorstel
Volgens de toelichting bij het wetsvoorstel beoogt de bewaarplicht te garanderen dat de te bewaren gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Wat de toegang tot de te bewaren gegevens betreft verbiedt het tweede lid van artikel 11.13 Tw aanbieders om de op grond van artikel 13.2a, tweede lid te bewaren gegevens voor andere doelen te verwerken. Volgens de toelichting is aldus verzekerd dat dat de op grond van hoofdstuk 13 Tw te bewaren gegevens uitsluitend worden bewaard ten behoeve van een van hoofdstuk 11 afwijkend doel, namelijk de beschikbaarheid voor de bestrijding van ernstige misdrijven.

De op grond van artikel 13.2a te bewaren gegevens kunnen door de aanbieder niet voor eigen bedrijfsdoeleinden worden verwerkt, tenzij het gegevens betreft die toch al overeenkomstig de artikelen 11.5 en 11.5a Tw kunnen worden verwerkt.

In de MvT wordt opgemerkt dat het de diverse toezichthouders vrij staat om de door hen benodigde gegevens op te vragen voor hun taken. Die mogelijkheid bestaat alleen voor de gegevens die de aanbieder conform de artikelen 11.5 een 11.5a Tw voor eigen bedrijfsdoeleinden bewaart.[33] De gegevens die worden bewaard op grond van hoofdstuk 13 zullen niet toegankelijk zijn voor bijvoorbeeld OPTA.[34]

De MvT geeft verder een overzicht van de huidige wetgeving voor de beschikbaarstelling voor de opsporing en vervolging van strafbare feiten. Het CIOT blijft aangewezen voor een vordering van actuele gebruikersgegevens.

Bepalingen in de Richtlijn
Uitgangspunt is dat de te bewaren gegevens beschikbaar zullen zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit, zoals gedefinieerd in de nationale wetgevingen van de lidstaten (artikel 1, eerste lid). De Richtlijn bepaalt in artikel 4 dat lidstaten moeten waarborgen dat de overeenkomstig de Richtlijn bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving, aan de bevoegde autoriteiten worden verstrekt. Wetgevingsmaatregelen die toegang tot en gebruik door nationale instanties regelen, vallen blijkens overweging 25 niet onder de reikwijdte van communautaire regelgeving.

Noodzaak van beperkingen aan de toegang
Het CBP en de Groep Gegevensbescherming Artikel 29 hebben consequent aangedrongen op specifieke waarborgen bij de implementatie van de Richtlijn in nationale rechtstelsels, teneinde te voldoen aan de vereisten die voortvloeien uit artikel 8 EVRM. Het afbakenen van de toegang is daarbij steeds een bron van zorg geweest. Telkens weer is gewezen op de noodzaak de toegang tot de te bewaren gegevens te beperken tot het opsporen, onderzoeken of vervolgen van *ernstige* criminaliteit. Verwerking voor andere doeleinden zou expliciet moeten worden

[33] MvT, blz. 10.
[34] Idem.

uitgesloten, evenals de mogelijkheid van datamining op de communicatie- en bewegingspatronen van onverdachte personen.[35]

Artikel 4 van de Richtlijn verplicht de lidstaten om de procedure en de te vervullen voorwaarden voor toegang tot gegevens die bewaard worden vast te stellen in nationale wetgeving, rekening houdend met de relevante bepalingen van de wetgeving van de Europese Unie of publiek internationaal recht, met name het EVRM, zoals geïnterpreteerd door het Europees Hof voor de Rechten van de Mens. Het feit dat de Richtlijn bij dit onderwerp expliciet voor de term wetgeving kiest, in relatie tot het EVRM, en niet voor de algemenere term 'bepaling', verplicht de lidstaten tot een zorgvuldige afbakening van de toegang in de wetstekst zelf.

Het wetsvoorstel komt slechts gedeeltelijk tegemoet aan deze eisen. Het verbod voor aanbieders om specifiek voor hoofdstuk 13 te bewaren gegevens voor eigen doeleinden te gebruiken, komt goed uit de verf. Het CBP mist echter een duidelijke beperking in de doeleinden waarvoor de te bewaren gegevens beschikbaar kunnen komen van de opsporingsinstanties en veiligheidsdiensten. In het voorgestelde artikel 13.2a is weliswaar het doel geformuleerd waarvoor aanbieders gegevens dienen te bewaren, te weten het onderzoeken, opsporen en vervolgen van ernstige misdrijven, maar die verplichting sluit alleen verdere verwerking uit voor eigen bedrijfsdoeleinden.

De voorgestelde bepaling van 11.13 Tw staat volgens het CBP op geen enkele wijze in de weg aan de uitoefening van bestaande bevoegdheden tot het vorderen van de gegevens, niet alleen van opsporingsinstanties maar ook van bestuursorganen. Het CBP gaat er voorts van uit dat met het wetsvoorstel niet is beoogd op enige wijze verandering te brengen in de mogelijkheden voor derden om langs civielrechtelijke weg de beschikking te krijgen over de op grond van artikel 13.2a te bewaren gegevens. De MvT concludeert daarmee volgens het CBP ten onrechte dat de Nederlandse wetgeving voorziet in adequate procedures en waarborgen voor de toegang tot de bewaarde gegevens door de bevoegde nationale autoriteiten.

3a Toegang voor strafvordering

Er is een opvallend verschil tussen de wetstekst en de MvT als het gaat om toegang voor de strafvordering. In het nieuwe eerste lid van artikel 13.4 Tw worden de artikelen 126n en 126u Sv en artikel 28 van de Wet Inlichtingen- en Veiligheidsdiensten genoemd als grondslag voor vorderingen waaraan de aanbieders moeten voldoen. Maar de MvT noemt daarnaast artikel 126na en 126ua Sv, alsmede de in de Wet terroristische misdrijven gegeven bevoegdheden van 126ii, 126hh en 126zh en 126 zi Sv.[36]

Het CBP meent dat de wet een limitatieve opsomming moet geven van strafvorderlijke toegangsmogelijkheden, zowel in de tekst van de wet als in de MvT. Bijzondere aandacht daarbij verdient het bestaande artikel 13.2b Tw, dat niet is gewijzigd in het wetsvoorstel. Het verdient naar de opvatting van het CBP de voorkeur de betreffende strafvorderlijke bevoegdheden aan te passen en vervolgens de spiegelbepalingen in de Tw (en dan met name 13.2b en het voorgestelde 13.4, eerste lid Tw) daarbij aan te laten sluiten.

[35] Artikel 29 WP, opinie 3/2006
[36] MvT, blz. 15.

In het licht van de (komende) bewaarplicht acht het CBP het noodzakelijk om het systeem van toepasselijke strafvorderlijke bevoegdheden kritisch te beoordelen. Het CBP ziet daarbij niet in wat nog de toegevoegde waarde is van het bevriezingsbevel van artikel 126ni Sv. In het Duitse implementatievoorstel is besloten om die bepaling uit het Cybercrime-verdrag niet in te voeren, omdat de bewaarplicht reeds voorziet in de mogelijkheid om verkeersgegevens beschikbaar te houden voor opsporingsdoeleinden.

3b Datamining
Artikel 126hh Sv geeft de bevoegdheid tot het vorderen van het bewaarde bestand of delen daarvan met het oog op de voorbereiding van de opsporing van terroristische misdrijven. Het CBP acht toepassing van deze bevoegdheid op de gegevens die onder de bewaarplicht vallen in strijd met artikel 4 van de Richtlijn. Dat artikel vereist de lidstaten bepalingen aannemen om te waarborgen dat gegevens alleen in welbepaalde gevallen worden verstrekt.

Het CBP wijst in dit verband op de uitspraak van het Duitse Bundesverfassungsgericht van 4 april 2006[37]. Het Hof concludeert dat preventieve 'Rasterfahndung' zonder dat er daadwerkelijke aanwijzingen zijn voor een dreigend gevaar een ontoelaatbare inbreuk met zich meebrengt voor de persoonlijke levenssfeer, terwijl datamining nu eenmaal ongeschikt moet worden geacht voor het afwenden van een dergelijk gevaar, alleen al omdat die methode veel tijd vergt. Het wetsvoorstel dient volgens het CBP dan ook uit te sluiten dat de bevoegdheid van artikel 126hh kan worden ingezet voor het verkrijgen van het (gedeeltelijke) bestand met bewaarde gegevens.

3c Toegang voor bestuursorganen en derden
De MvT maakt niet duidelijk of een aanbieder kan, dan wel zou moeten weigeren te voldoen aan een vordering van bestuursorganen, dan wel aan civiele vorderingen van derden tot verkrijging van de op grond van artikel 13.2a Tw bewaarde gegevens.

De MvT noemt specifiek de OPTA, die alleen de beschikking zou kunnen krijgen over de gegevens die de aanbieder in overeenstemming met artikel 11.5 en 11.5a Tw bewaart, maar andere bestuursorganen kunnen zich op eigen bevoegdheden gaan beroepen om toegang tot de gegevens te vorderen. Daarbij kunnen complexe vraagstukken ontstaan over de voorrang van tegenstrijdige wetten.

Het nieuwe artikel 11.13 Tw verbiedt aanbieders om de te bewaren gegevens voor andere doeleinden te verwerken dan de opsporing en vervolging van ernstige misdrijven. Te verwachten valt dat deze bepalingen in de praktijk gaan botsen met mogelijke vorderingen van bestuursorganen of een bevel van de rechter. Het is niet aan de aanbieder om daarin een weg te vinden, maar aan de wetgever. Het CBP meent dan ook dat in het wetsvoorstel alsnog expliciet zou moeten worden uitgesloten dat de te bewaren gegevens langs bestuursrechtelijke dan wel civielrechtelijke weg kunnen worden verkregen. Dat kan door aanpassing van de betreffende bevoegdheden, bijvoorbeeld in het geval van de OPTA via artikel 18.7 Tw.

[37] BvR 518/02, zie voor een bespreking ook Datenschutz und Datensicherheit 30 (2006) 11, blz. 685 e.v.

3d Informatierechten betrokkenen

De MvT gaat in het vijfde hoofdstuk, *Rechtsbescherming*, in op het inzage- en correctierecht van betrokkenen. Het recht op kennisneming als bedoeld in artikel 35 WBP wordt onverkort van toepassing geacht. Aanbieders zouden desgevraagd een volledig overzicht moeten verstrekken van de bewaarde gegevens, zonder zich te kunnen beroepen op de uitzonderingsgronden van artikel 43 onder a en b. Ook het correctierecht zoals bepaald in artikel 36 WBP zou van toepassing zijn.

Het CBP juicht elke expliciete erkenning van de informatierechten van betrokkenen toe, maar meent dat per geval een nadere afweging dient te worden gemaakt van de belangen van derden, zoals bepaald in artikel 43 onder e WBP. Bij verkeersgegevens over telecommunicatie zijn onvermijdelijk derden betrokken, de personen waarmee een betrokkene heeft gebeld of ge-e-maild. Het verstrekken van een uitgebreid overzicht (dat volgens het wetsontwerp tot achttien maanden terug in de tijd zou kunnen gaan), kan een inbreuk maken op de rechten en vrijheden van anderen dan de direct betrokkene. Ook zou de abonnee van een aansluiting via het inzagerecht inzicht kunnen krijgen in het communicatiegedrag of de locatiegegevens van alle gebruikers over een langere periode. Daarbij valt te denken aan werknemers of gezinsleden, waaronder minderjarigen. De MvT gaat ten onrechte aan deze problematiek voorbij.

Als de gekozen bewaartermijn gelijk was geweest aan de termijn waarbinnen gegevens noodzakelijk zijn voor de bedrijfsvoering, had dit probleem met het inzagerecht zich niet of nauwelijks voorgedaan. Zowel bij vaste als mobiele telefonie zijn er immers oplossingen om de privacy te beschermen als het afschermen van nummers. Dit geldt echter niet voor internet. Voor het afleveren van e-mails worden immers geen gespecificeerde rekeningen verstrekt, en zijn dus ook geen oplossingen voorhanden om de adresgegevens af te schermen.

Samenvatting

Het CBP is van mening dat de grenzen voor toegang tot de te bewaren gegevens onvoldoende scherp zijn getrokken. Daarmee is het wetsontwerp in strijd met artikel 4 van de Richtlijn. Het CBP vraagt zich af in hoeverre artikel 11.13 Tw de bestaande mogelijkheden beperkt voor derden om de beschikking te krijgen over de bewaarde gegevens. De bestaande wettelijke bevoegdheden voor het verkrijgen van de te bewaren gegevens dienen daarom alsnog nader te worden ingeperkt. Dat geldt zowel voor strafvorderlijke als voor bestuursrechtelijke en civielrechtelijke bevoegdheden.

Het CBP adviseert om in het wetsvoorstel uit te sluiten dat de bevoegdheid van artikel 126hh Sv kan worden ingezet voor het verkrijgen van het (gedeeltelijke) bestand van bewaarde gegevens (ten behoeve van datamining).

Het systeem van strafvorderlijke bevoegdheden op grond waarvan de opsporingsinstanties de beschikking kunnen krijgen over de te bewaren gegevens verdient kritische doordenking, met name waar het de relatie betreft tussen de bewaarplicht en de mogelijkheid verkeersgegevens te bevriezen (126ni Sv).

Ten aanzien van de informatierechten van betrokkenen adviseert het CBP een uitgebreide toelichting op te nemen in de MvT over de balans met rechten en vrijheden van anderen, in het bijzonder als het gaat om werknemers en gezinsleden.

4. Controlemiddelen op rechtmatig gebruik

Wetsvoorstel

Uit de transponeringstabel bij het wetsvoorstel blijkt dat artikel 10 van de Richtlijn, over het jaarlijks notificeren van de Europese Commissie van statistieken over opvragingen en gebruik, niet omgezet wordt. De MvT geeft aan dat aanbieders de statistieken moeten bijhouden.[38] Daarvan kan het Openbaar Ministerie een registratie bijhouden. *De registratie van deze gegevens zal kunnen worden gecoördineerd door een door de Minister van Justitie aan te wijzen orgaan. Daarvoor kan worden gedacht aan het Landelijk Parket van het Openbaar Ministerie.*[39] Het wetsontwerp gaat ervan uit dat de statistieken alleen justitiële bevragingen betreffen: *Voor wat betreft de gegevens die worden opgevraagd door de inlichtingen- en veiligheidsdiensten, geldt dat de informatie over de toepassing van deze bevoegdheden door de diensten staatsgeheim is*.[40]

Bepalingen in de Richtlijn

Artikel 10 van de Richtlijn schrijft voor dat de lidstaten jaarlijks statistieken moeten verstrekken aan de Europese Commissie over de aantallen en aard van de verstrekkingen, inclusief de gevallen waarin de verzoeken niet konden worden ingewilligd.

4a Statistieken

De verplichting tot het bijhouden van statistieken is opgenomen in de Richtlijn om na verloop van tijd te kunnen evalueren of de Richtlijn adequaat is, of bijstelling behoeft, zowel waar het de soorten gegevens betreft als de bewaartermijn. Het CBP meent dat uit de evaluatiebepalingen van de Richtlijn voortvloeit dat de statistieken in ieder geval deels openbaar worden gemaakt, wanneer de Europese Commissie op uiterlijk 15 september 2010 een openbaar evaluatieverslag presenteert aan het Europees Parlement en de Raad.[41] Gezien het grote maatschappelijke belang van de bewaarplicht meent het CBP dat de wetgever eveneens een eigen evaluatie moet doen van de gekozen implementatie. Die evaluatie is erbij gebaat als er openbare statistieken beschikbaar zijn over de aantallen bevragingen van historische verkeersgegevens. Door de bepalingen uit de Richtlijn over statistieken in de wet te verankeren, kan tevens worden voorzien in (een verplichting tot) het publiceren van statistieken over de aantallen taps, zoals toegezegd door de regering bij brief van 15 december 2006.[42] Een dergelijke verplichting tot het bijhouden van statistieken door het Landelijk Parket zou het model kunnen volgen van het Duitse implementatievoorstel in paragraaf 100g.[43] Daarbij zou de verplichting volgens het CBP op de behoeftestellers moeten rusten en niet op de aanbieders.

---

[38] MvT, blz 30. "*Deze gegevens zullen door de aanbieders moeten worden verzameld (...).*"
[39] MvT, blz. 31.
[40] Idem.
[41] Richtlijn, artikel 14 eerste lid.
[42] *Kamerstukken II* 2005/06, 30 517, nr 2, blz. 13: *"Het kabinet is wel bereid om de tapstatistieken bij te houden voor wat betreft de taps in het belang van de opsporing van strafbare feiten en daar politieke verantwoording over af te leggen."*
[43] SPO-E Wetboek van Strafvordering § 100g [Erhebung von Verkehrsdaten]
(4) Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:
1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;
2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;
3. die jeweils zugrunde liegende Anlassstraftat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;
4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

De MvT stelt dat er via het CIOT een registratie wordt bijgehouden van het opvragen van gebruikersgegevens, maar dat dat bij het uitoefenen van andere strafvorderlijke bevoegdheden thans niet het geval is. Over de bevragingen via het CIOT wil het CBP opmerken dat het om zeer grote aantallen gaat, en dat sinds de oprichting in 1999 audits naar de rechtmatigheid van de verstrekkingen, ondanks de verplichting hiertoe in het Besluit verstrekking gegevens telecommunicatie, niet hebben plaatsgevonden.

Ten slotte meent het CBP dat de Richtlijn ten aanzien van de te leveren statistieken geen onderscheid maakt tussen vorderingen door inlichtingendiensten en justitiële vorderingen. De Richtlijn spreekt van 'bevoegde autoriteiten'. Het CBP ziet niet in hoe het noemen van een getal (het aantal vorderingen door de inlichtingendiensten) een staatsgeheim in gevaar zou kunnen brengen.

4b Notificatieplicht

In het wetsontwerp wordt niets gezegd over de notificatieplicht bij de bevraging van andere dan identificerende gegevens. Het CBP denkt dat het naleven van de notificatieplicht en het bijhouden van statistieken over het aantal notificaties belangrijk is om controle mogelijk te maken op het rechtmatig gebruik van de gegevens. Bij de invoering van de Wet bevoegdheden vorderen gegevens werd deze notificatieplicht als belangrijke waarborg geïntroduceerd: *Deze waarborgen bevorderen de zorgvuldige toepassing van de bevoegdheden en zijn daarmee mede in het belang van de personen over wie in het belang van een opsporingsonderzoek gegevens gevorderd worden.*[44]

Tijdens het debat met de Eerste Kamer over deze wet haalden de leden een rapport aan van het WODC waaruit blijkt dat de notificatieplicht op grote schaal wordt geschonden. De minister gaf toen aan: *Omdat de notificatieplicht inderdaad een van de waarborgen is voor een zorgvuldige en controleerbare toepassing van de bijzondere opsporingsbevoegdheden, is een betere toepassing van deze verplichting van belang. Naar aanleiding van de evaluatie van de wet bijzondere opsporingsbevoegdheden is daarom aan het openbaar ministerie gevraagd een plan van aanpak op te stellen met maatregelen om tot een betere naleving van deze plicht te komen.*[45]

Een manier om een betere naleving van de notificatieplicht te bevorderen is het instellen van een verplichting om statistieken bij te houden van het verzenden van notificaties. Bij die statistieken horen ook de aantallen gevallen, met redenen omkleed, waarin bewust niet is genotificeerd. Ook hier biedt het Duitse implementatievoorstel volgens het CBP een relevant model.[46]

---

5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren

[44] *Kamerstukken I* 2004/05, 29 441, nr. C, blz. 12.

[45] *Kamerstukken I* 2004–2005, 29 441, nr. C, blz. 15.

[46] § 101 SPO [Allgemeine Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen]
Von den in Absatz 1 genannten Maßnahmen sind die nachfolgend bezeichneten Personen zu benachrichtigen, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 9 und die dafür vorgesehene Frist hinzuweisen. Zu benachrichtigen sind im Falle (... verschillende wetsartikelen)
6. des § 100g [Verkehrsdatenerhebung] die Beteiligten der betroffenen Telekommunikation
§ 100e [Berichtspflicht]
(1) Für die nach § 100c angeordneten Maßnahmen gilt § 100b Abs. 5 entsprechend. Die Bundesregierung berichtet dem Deutschen Bundestag jährlich über die im jeweils vorangegangenen Kalenderjahr nach § 100c angeordneten Maßnahmen
(2) 8. ob eine Benachrichtigung der Betroffenen (§ 101 Abs. 4 bis 7) erfolgt ist oder aus welchen Gründen von einer Benachrichtigung abgesehen worden ist.

Samenvatting

Het CBP beveelt aan dat de wetgever de verplichting tot het bijhouden van statistieken in de wetstekst zelf vastlegt, en zich daarbij verplicht tot openbaarmaking van de statistieken. Ook de aantallen bevragingen door inlichtingendiensten zouden hierin opgenomen moeten worden. Ter vergroting van de middelen om de rechtmatigheid van bevragingen te controleren, beveelt het CBP verder strikte naleving van de notificatieplicht na, gekoppeld aan een verplichting tot het bijhouden van statistieken over de naleven van die plicht.