Advies nr. 24 /2008 van 2 juli 2008

Betreft: Advies betreffende het voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 *betreffende de elektronische communicatie*, en betreffende het ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van bewaring van de gegevens (A/08/024)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna "WVP"), inzonderheid artikel 29;

Gelet op het verzoek om advies van de Minister voor Ondernemen en Vereenvoudigen ontvangen op 23/05/2008;

Gelet op het verslag van mevrouw Anne Vander Donckt;

Brengt op 02/07/2008 het volgend advies uit:

A. INLEIDING

1. Op 23 mei 2008 heeft de Minister voor Ondernemen en Vereenvoudigen de Commissie verzocht om advies uit te brengen inzake het de voorstellen tot omzetting van de Europese 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*.

2. Het betreft meer bepaald een voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 *betreffende de elektronische communicatie* (hierna 'het voorontwerp van wet'), en een ontwerp van koninklijk besluit tot vaststelling van de te bewaren gegevens overeenkomstig artikel 126 van de wet van 13 juni 2005, alsook de voorwaarden en de duur van de bewaring van die gegevens (hierna 'het ontwerp kb'). De Commissie zal hiernavolgend dan ook advies uitbrengen inzake deze ontwerpen, rekening houdend met de informatie waarover ze beschikt.

B. TOEPASSELIJKE WETGEVING

3. Vooreerst kan worden verwezen naar de Richtlijn 2006/24/EG. Aangezien er persoonsgegevens worden verwerkt is verder de WVP van toepassing, evenals de wet van 13 juni 2005 *betreffende de elektronische communicatie* (hierna 'WEC'). Tenslotte dient het koninklijk besluit vermeld van 9 januari 2003 *tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid, en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109ter, E, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven* (hierna 'het kb van 9 januari 2003').

C. VOORGESCHIEDENIS

4. Diverse Europese lidstaten hebben in het verleden wetgeving aangenomen op het gebied van het bewaren van gegevens door aanbieders van diensten ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Deze nationale bepalingen vertonen onderling aanzienlijke verschillen. De juridische en technische verschillen tussen de nationale bepalingen op het gebied van het bewaren van gegevens ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten belemmeren de werking van de interne markt voor elektronische communicatie. De aanbieders van diensten immers worden geconfronteerd met uiteenlopende voorschriften wat betreft de categorieën te bewaren verkeers- en locatiegegevens, de bewaringsvoorwaarden en bewaringstermijnen.

5. In de conclusies van de Europese Raad justitie en binnenlandse zaken van 19 december 2002 wordt benadrukt dat wegens de opmerkelijke toename van de mogelijkheden van elektronische communicatie, gegevens betreffende het gebruik daarvan van bijzonder belang zijn en een waardevol instrument bij het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, met name in de strijd tegen de georganiseerde misdaad. In zijn verklaring betreffende de bestrijding van terrorisme van 25 maart 2004 heeft de Europese Raad aan de Raad justitie en binnenlandse zaken opdracht gegeven maatregelen te bestuderen met het oog op het vaststellen van regels voor het bewaren van verkeersgegevens door telecommunicatieaanbieders. In de verklaring ter veroordeling van de terroristische aanslagen op Londen die is aangenomen door de bijzondere vergadering van de Europese Raad van 13 juli 2005 wordt nogmaals nadrukkelijk gewezen op de noodzaak om zo spoedig mogelijk gemeenschappelijke maatregelen aan te nemen in verband met het bewaren van verkeersgegevens van elektronische communicatie.

6. **De doelstellingen van de Richtlijn 2006/24/EG bestaan derhalve in het harmoniseren van de aan aanbieders opgelegde verplichtingen inzake het bewaren van sommige gegevens en het waarborgen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.**

7. De Groep 29[1] heeft in haar advies 3/2006 inzake de Richtlijn 2006/24 erop gewezen dat de lidstaten om de bepalingen van de richtlijn op uniforme wijze om te zetten en de bepalingen van artikel 8 van het EVRM in acht te nemen, afdoende specifieke garanties moeten invoeren, welke minstens het volgende zouden moeten omvatten :

- specificatie van het doel : duidelijke definitie en afbakening van 'ernstige strafbare feiten';
- beperking van de toegang : de gegevens mogen alleen beschikbaar zijn voor uitdrukkelijk aangewezen wetshandhavingautoriteiten;
- gegevensminimalisering;
- geen datamining;
- onafhankelijke controle van machtiging tot toegang;
- scheiding van systemen;
- veiligheidsmaatregelen;
- doel van bewaring van gegevens door aanbieders.

D. ONDERZOEK VAN DE ADVIESAANVRAAG

D.1.VERGELIJKING HUIDIGE ARTIKEL 126 WEC MET HET NIEUWE VOORONTWERP

8. Artikel 126 WEC luidt momenteel als volgt : ' *§ 1. Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de Minister van Justitie en van de minister en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de voorwaarden vast waaronder de operatoren de verkeersgegevens en de identificatiegegevens van eindgebruikers, registreren en bewaren, met het oog op het opsporen en de beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek door de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst.*
§ 2. De gegevens die moeten worden bewaard en de duur van de bewaring, die wat de openbare telefoniedienst betreft niet minder dan twaalf en niet meer dan zesendertig maanden mag zijn, worden door de Koning bepaald in een besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut.

[1] Deze werkgroep werd in het leven geroepen door artikel 29 van de Richtlijn 95/46/EG, en is een onafhankelijk adviserend orgaan met betrekking tot de bescherming van persoonsgegevens. Haar taken zijn beschreven in artikel 30 van de Richtlijn 95/46/EG en in artikel 15 van de Richtlijn 2002/58/EG.

De operatoren zorgen ervoor dat de in § 1 vermelde gegevens onbeperkt toegankelijk zijn vanuit België.'

9. Het kb waarvan sprake in §2 is er nooit gekomen. Het huidige artikel 126 WEC is van toepassing op de operatoren, en niet op de aanbieders en doorverkopers voorzien in artikel 9, §§5 en 6 WEC. Hiermee worden bijvoorbeeld[2] bedoeld de netwerken of diensten bestemd voor gebruik door leden van een groep van ondernemingen, een netwerk van een universiteit, een bank en haar agenten, … . In het voorontwerp van wet worden de aanbieders en doorverkopers wél opgenomen in artikel 126 WEC. Het voorontwerp van wet voegt ook de locatiegegevens toe aan het huidige artikel 126 WEC.

10. In haar advies 08/2004[3] heeft de Commissie over het huidige artikel 126 WEC onder meer verklaard :

'De Commissie herinnert aan de opmerkingen die zij formuleerde in haar advies 33/99 van 13 december 1999 en die op Europees niveau door de groep van Europese functionarissen voor gegevensbescherming meerdere keren werd herhaald en die het a priori vasthouden van communicatiegegevens en de verenigbaarheid hiervan met de fundamentele beginselen van bescherming van persoonsgegevens, betreffen[4].' Zo had de Commissie eraan herinnerd dat *'noch de internationale teksten (…) noch de wet van 8 december 1992 (beginselen van proportionaliteit, beperkte bewaartijd,…) algemene toezichtsmethodes toestaan die los staan van een onderzoek naar specifieke misdrijven (uitgezonderd het zeer specifieke geval van de proactieve recherche, die strikt omkaderd is).'* De Commissie refereert ook nog aan de jurisprudentie van het Europees Hof van de Rechten van de Mens[5] *'die leidt tot het verbieden van de op grote schaal gehanteerde verkennende en algemene toezichtsmethodes op telecommunicatiediensten. Aldus zou een access provider niet verplicht kunnen worden om systematisch alle oproepen uitgaande van zijn klanten te registreren, maar alleen wanneer een onderzoek wordt ingesteld naar een specifieke persoon. Hij zou ook niet*

---

[2] Zie Belgische Kamer van Volksvertegenwoordigers, verantwoording bij de amendementen bij het wetsontwerp houdende diverse bepalingen, Doc 51, 2873/002.

[3] Advies nr. 08/2004 van 14 juni 2004 betreffende het voorontwerp van wet betreffende de elektronische communicatie.

[4] Aanbeveling nr. 3/99 van 7 september 1999 over de bewaring van verkeersgegevens door Internetdienstenaanbieders voor wetshandhavingsdoeleinden ; Advies 5/2002 van 11 oktober 2002 over de verklaring van de Europese functionarissen voor gegevensbescherming tijdens de internationale conferentie van Cardiff (9-11 september 2002) over het verplicht systematisch bewaren van telecommunicatiegegevens : "Indien verkeersgegevens in specifieke gevallen moeten worden bewaard, moet de noodzaak daarvoor duidelijk worden aangetoond, moet de bewaarperiode zo kort mogelijk zijn en moet de desbetreffende praktijk duidelijk bij de wet zijn geregeld, op zodanige wijze dat voldoende waarborgen worden geboden tegen onrechtmatige toegang en andere misbruiken. Het systematisch bewaren van alle soorten verkeersgegevens voor een periode van een jaar of meer zou zeker in strijd zijn met het evenredigheidsbeginsel en derhalve in ieder geval onaanvaardbaar zijn."

[5] Arresten Klass en Malone.

mogen gedwongen worden om een logboek bij te houden van de toegangen die het onderzoek zouden kunnen sterken '.

D.2. PRAKTISCHE IMPLICATIES

11. De voorliggende bepalingen zullen een niet geringe impact hebben op de bedrijfsvoering, niet enkel van de grote gekende operatoren zoals bijvoorbeeld Belgacom, Mobistar, Telenet, maar eveneens binnen een onderneming of KMO, die internettoegang en emailverkeer voorzien voor hun werknemers. Onder de huidige versie van het ontwerp lijkt zelfs een thuisnetwerk niet uitgesloten, indien men dit bijvoorbeeld beschikbaar stelt voor gasten. Zij zullen in de toekomst gehouden zijn om de gevraagde gegevens te bewaren en op te slaan gedurende 24 maanden, of langer. Tevens dienen zij te voldoen aan stringente veiligheidsmaatregelen, waaronder de creatie van een 'Coördinatiecel Justitie' en de nominatie van aangestelden voor de bescherming van persoonsgegevens. Daarnaast moeten zij de bewaarde gegevens onverwijld ter beschikking kunnen stellen van de aanvragers. Één en ander lijkt in de praktijk moeilijk uitvoerbaar te zijn, temeer daar de netwerken geviseerd door artikel 9, §§5 en 6 WEC geen aangifte bij het BIPT dienen te doen, en er derhalve moeilijk een controle kan gebeuren naar bijvoorbeeld de naleving door deze netwerken van de noodzakelijke veiligheidsmaatregelen. Zij dienen ook rekening te houden met de bestaande privacyreglementeringen, zoals bijvoorbeeld de CAO nr. 81 van 26 april 2002 inzake de controle op het gebruik van internet en email op de werkvloer. Deze reglementeringen staan haaks op hetgeen door het voorontwerp van wet wordt voorzien voor de aanbieders bedoeld in artikel 9, §§5 en 6 WEC. Tenslotte dient er in dit verband op gewezen dat de Richtlijn 2006/24 enkel de **openbare** elektronische communicatiediensten of -netwerken viseert, en dus niet de aanbieders bedoeld in artikel 9, §§5 en 6 WEC.

12. Daarnaast dient opgemerkt dat de bepalingen van de richtlijn zijn opgesteld onder meer rekening houdende met de opmerkingen van de telecomoperatoren inzake de technische en praktische modaliteiten van opslag, zoals de te bewaren gegevens. De Commissie stelt zich dan ook de vraag in hoeverre het ontwerp kb met de technische mogelijkheden van de operatoren rekening houdt, zeker wat betreft de te bewaren gegevens buiten hetgeen wordt voorzien door de richtlijn. De recent afgesloten raadpleging van de sector door het BIPT[6] zal hierover waarschijnlijk meer duidelijkheid kunnen verschaffen.

[6] Raadpleging door de Raad van het BIPT op verzoek van de Minister voor Ondernemen en administratieve Vereenvoudiging van 27 mei 2008 betreffende de omzetting van Richtlijn 2006/24, antwoordtermijn t.e.m 16 juni 2008.

D.3. HUIDIGE PRAKTIJK

13. Er bestaat vandaag reeds een uitvoerige regeling betreffende de identificatie van telefoonnummers (art. 46bis wetboek van strafvordering, hierna 'Sv.') en het opsporen of lokaliseren van privé (tele)communicaties (art. 88bis Sv.).

14. Art. 46bis Sv. verleent aan de procureur des Konings de bevoegdheid de identificatiegegevens op te vorderen met betrekking tot de telecommunicatiediensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk gebruikt worden. Zo kan nagegaan worden welke telefoonnummers gekoppeld zijn aan een bepaalde persoon. Omgekeerd kan ook, vertrekkend van het telefoonnummer dat men ergens heeft aangetroffen, opgevraagd worden welke abonnee of gewoonlijke gebruiker daaraan gekoppeld is.[7] Artikel 46bis, §2 Sv. bepaalt dat iedere operator van wie gevorderd wordt de in §1 bedoelde gegevens mee te delen, deze verstrekt aan de procureur des Konings binnen een termijn te bepalen door de Koning. Het kb van 9 januari 2003 heeft hieraan uitvoering gegeven.

15. Voor het opsporen of lokaliseren is een bevel van de onderzoeksrechter vereist. Het betreft (1) de opsporing van oproepgegevens van de telecommunicatiemiddelen van waaruit of waarnaar bepaalde oproepen worden of werden gedaan en (2) de lokalisering van oorsprong of bestemming van telecommunicatie. Hierdoor kunnen deelnemers aan een per GSM gevoerd gesprek worden gelokaliseerd, onder meer via satellietverbindingen en zendmastbepaling.[8] Artikel 88bis, §2 Sv. bepaalt dat iedere operator de gegevens waarom verzocht werd meedeelt binnen een termijn te bepalen door de Koning. De modaliteiten van de technische medewerking worden eveneens vastgesteld door de Koning. Het kb van 9 januari 2003 heeft hieraan uitvoering gegeven.

16. Het is niet duidelijk waarom voormelde artikelen, en het kb van 9 januari 2003 dat ze uitvoert, niet zouden volstaan voor het opsporingsonderzoek en het gerechtelijk onderzoek. Wat is de noodzaak van een bewaarplicht zoals voorzien door het voorontwerp van wet ? Wat is de impact van het voorontwerp van wet en ontwerp kb op de voormelde artikelen 46 bis en 88bis Sv., en het kb van 9 januari 2003 ? De ontwerpteksten geven hieromtrent geen uitsluitsel.

---

[7] VAN DEN WYNGAERT, C., Strafrecht, strafprocesrecht en internationaal strafrecht, in hoofdlijnen, Maklu, 2006, p. 979.

[8] VAN DEN WYNGAERT, C., o.c., p. 979-980.

D.4. ARTIKELSGEWIJZE BESPREKING VOORONTWERP VAN WET

Artikel 2

17. Artikel 2 vervangt het huidige artikel 126 WEC. §1 van artikel 2 van het voorontwerp van wet luidt als volgt :

'*Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bewaren de operatoren, alsook de aanbieders en doorverkopers bedoeld in artikel 9, §§5 en 6, de verkeers –en locatiegegevens en de gegevens voor identificatie van de eindgebruikers die door hen worden gegenereerd of verwerkt bij het aanbieden van elektronische communicatienetwerken –en diensten, met het oog op :*

a) het onderzoek, de vervolging en de beteugeling van strafbare feiten;
b) de beteugeling van kwaadwillige oproepen naar de nooddiensten;
c) het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk –of dienst.

18. Zoals reeds gesteld onder punt 9 supra, vermeldt artikel 2 van het voorontwerp van wet niet enkel de operatoren, maar eveneens de aanbieders en doorverkopers bedoeld in artikel 9, §§5 en 6 WEC. Hierdoor worden de entiteiten die voordien in de WEC door twee aparte bepalingen inzake de bewaring van gegevens werden geviseerd, in éénzelfde bepaling (het nieuwe artikel 126) gegroepeerd.

19. In het vroegere artikel 126 WEC was het voorgaande reeds voorzien voor een operator, nu komen er ook de aanbieders en doorverkopers bij die worden vermeld in artikel 9, §§5 en 6 WEC. Artikel 9, §7 voorzag dat zij eveneens gegevens moeten bewaren voor de doeleinden a) en b), doch niet voor het doeleinde c). Dit wordt nu wel voorzien. Onder aanbieders en doorverkopers moet bijvoorbeeld worden begrepen het interne netwerk van een bedrijvengroep. Deze worden evenwel niet geviseerd door de richtlijn 2006/24/EG, welke overeenkomstig artikel 3 enkel en alleen van toepassing is op aanbieders van openbare elektronische communicatiediensten of een openbaar communicatienetwerk bij het leveren van de betreffende communicatiediensten.

20. De reden voor het niet vermelden van de aanbieders en doorverkopers onder het huidige artikel 126 WEC, maar wel in artikel 9, §7 WEC kan worden teruggevonden in de verantwoording gegeven bij één van de amendementen[9] bij het wetsontwerp diverse bepalingen met betrekking tot de §§§ 5,6 en 7 : '*anderzijds blijft de nood om te voorzien in een samenwerking met de gerechtelijke autoriteiten. De samenwerkingsverplichting zoals die voorzien is voor de operatoren (met onder andere de verplichting om een contactpersoon voor de gerechtelijke autoriteiten aan te duiden die 7 dagen op 7 en 24 uur op 24 beschikbaar is) is in deze evenwel niet geschikt en daarom wordt de mogelijkheid gecreëerd om de nadere regels inzake het bewaren van gegevens en de samenwerking met de gerechtelijke autoriteiten in een uitvoeringsbesluit te omschrijven.'* Voormelde passage toont aan dat men de aanbieders en doorverkopers waarvan sprake in artikel 9, §§ 5 en 6 WEC niet zomaar kan gelijkstellen met een operator in de zin van artikel 2, 11° WEC. Zeker de zware procedure van samenwerking met de gerechtelijke autoriteiten zoals voorzien in het kb van 9 januari 2003 wilde men niet op éénzelfde wijze van toepassing verklaren op de aanbieders en doorverkopers. Het is dan ook vreemd dat zulks nu net wel gebeurt, door artikel 126 WEC (via het voorliggend artikel 2 van het voorontwerp van wet) niet enkel op de operatoren, doch eveneens op de aanbieders en doorverkopers van toepassing te maken. **Gezien het feit dat deze niet werden geviseerd door de Richtlijn 2006/24, de praktische implicaties vermeld onder punt 11, en gezien voormelde passage uit de verantwoording bij de wet van 20 juli 2006 houdende diverse bepalingen, lijkt het de Commissie aangewezen om de aanbieders en doorverkopers uit de toepassing van artikel 2 van het voorontwerp van wet te lichten, en in een andere bepaling onder te brengen. In het algemeen, met betrekking tot de voorliggende ontwerpen, dient opgemerkt dat men probeert onder het mom van de omzetting van de richtlijn veel meer op te leggen dan in de Richtlijn, bedoeld als maximumkader, wordt voorzien (zoals bijvoorbeeld naast de openbare ook de private netwerken te viseren, het opnemen van bijkomende gegevens, ...).**

21. De Commissie merkt verder op dat een operator die gegevens verwerkt voor rekening van de Staat, zoals voor punt a) van artikel 2 van het voorontwerp van wet het geval is, handelt als zijn verwerker, zoals gedefinieerd in artikel 1, §5 WVP. De Staat zou in casu dan ook kunnen worden beschouwd als verantwoordelijke voor de verwerking. Het verdient hier dan ook aanbeveling om expliciet in artikel 2 te verduidelijken dat de operatoren als verantwoordelijke voor de verwerking in de zin van de WVP worden beschouwd.

---

[9] Zie Wetsontwerp houdende diverse bepalingen, 9 juni 2006, doc 51, 2518/007, p. 4.

22. De memorie van toelichting en het voorontwerp van wet verduidelijken dat het nieuwe artikel 126 van toepassing is onverminderd de bepalingen van de WVP. Daarom zijn de operatoren voortaan uitdrukkelijk verplicht (wat voorheen trouwens ook reeds het geval was) het geheel van de bepalingen van de WVP en haar uitvoeringsbesluit van 13 februari 2001 na te leven. Dit stemt overeen met de bepalingen van de richtlijn, die eveneens voorziet in een toepassing van de richtlijn 95/46/EG op de operatoren[10].

23. De memorie van toelichting stelt dat de operatoren en aanbieders de WVP moeten naleven, onder meer inzake de rechten van de betrokkenen : *'de persoon dient zijn gegevens te kunnen inzien en, indien nodig, deze te laten rechtzetten of verwijderen'* . Het recht op inzage zoals voorzien door artikel 10 WVP en het recht op verbetering (artikel 12) worden onverkort van toepassing geacht. Aanbieders of operatoren zouden desgevraagd een volledig overzicht moeten verstrekken van de bewaarde gegevens. Hieromtrent dient opgemerkt dat de abonnee van een aansluiting via het inzagerecht inzicht zou 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 memorie van toelichting gaat ten onrechte aan deze problematiek voorbij. Bij vaste en mobiele telefonie zijn er oplossingen om de privacy te beschermen zoals het afschermen van nummers. Dit geldt echter niet voor internet. Voor het afleveren van e-mails worden immers geen gespecificeerde rekeningen verstrekt, en lijken er dus ook geen oplossingen voorhanden om de adresgegevens af te schermen.

24. Artikel 2 voorziet in de punten a), b) en c) de bijzondere finaliteiten waarvoor de verkeers, locatiegegevens en identificatiegegevens van de gebruikers kunnen worden aangewend. Hieromtrent kunnen de volgende bemerkingen gemaakt :

25. Het doeleinde voorzien onder punt a) : *onderzoek, vervolging en beteugeling van strafbare feiten* maakt een omzetting uit van de Richtlijn 2006/24, waarvan het doel het onderzoek, opsporen en vervolgen van **zware criminaliteit** betreft. Het voorontwerp van wet verwijst echter enkel naar strafbare feiten, hetgeen de facto inhoudt dat de bewaarde gegevens voor om het even welke strafbare inbreuk kunnen worden aangewend, zelfs overtredingen. Dit is niet bepaald in lijn met het uitgangspunt van de richtlijn en het principe van proportionaliteit, welke voorzien in de bewaring van bepaalde gegevens voor de strijd tegen de georganiseerde misdaad en het terrorisme, dus niet voor om het even welk misdrijf (cfr. supra, nrs. 4-6).

---

[10] Zie de overwegingen 15 en 16.

26. Naar analogie met bijvoorbeeld de BOM-wet[11] of artikel 90 ter Sv. inzake het aftappen van privé-communicatie, zou de wetgever in het huidige voorontwerp van wet kunnen voorzien in een strikte opsomming van de zware misdrijven voor het onderzoek, vervolging en beteugeling van dewelke de bewaarde gegevens kunnen worden aangewend. Minstens dient rekening te worden gehouden met de artikelen 46 bis en 88 bis Sv., welke momenteel respectievelijk voorzien in het opvragen door de procureur des Konings van identificatiegegevens met betrekking tot een telecommunicatiedienst en het opvragen door de onderzoeksrechter van locatiegegevens van een telecommunicatie. Op die manier zou tevens duidelijkheid worden verschaft over wie toegang heeft tot de bewaarde gegevens, voor de finaliteiten vermeld onder a). Hieromtrent voorzien de ontwerpen niets, behoudens voor de interne toegang bij de operatoren (Coördinatiecel Justitie). De Richtlijn bepaalt in artikel 4 inzake de toegang tot de gegevens dat de lidstaten bepalingen moeten aannemen om te waarborgen dat de gegevens alleen in welbepaalde gevallen, en in overeenstemming met de nationale wetgeving aan de bevoegde nationale autoriteiten worden verstrekt.

27. **Daarenboven zou elk ander gebruik van deze gegevens strafbaar moeten worden gesteld, en dient er tevens een nietigheidssanctie aan verbonden te worden.** Zie hieromtrent hetgeen wordt bepaald door artikel 13, 2. van de richtlijn : *'elke lidstaat neemt in het bijzonder de noodzakelijke maatregelen om ervoor te zorgen dat elke opzettelijke toegang tot of overbrenging van gegevens die overeenkomstig deze richtlijn worden bewaard die niet is toegestaan uit hoofde van krachtens deze richtlijn vastgestelde nationale uitvoeringsbepalingen, strafbaar is met sancties, met inbegrip van administratieve of strafrechtelijke sancties, die effectief, evenredig en afschrikkend zijn*.' Aangezien het BIPT bevoegd[12] is voor de controle op de naleving van de wet van 13 juni 2005 betreffende de elektronische communicatie en de bijbehorende uitvoeringsbesluiten, is voorzien in de mogelijkheid van alternatieve sancties, met name administratieve geldboetes, welke het IBPT overeenkomstig artikel 21 van de wet van 17 januari 2003 kan opleggen. De ontwerpen bepalen evenwel niet expliciet welke overheidsinstantie toezicht houdt op de veiligheid van de bewaarde gegevens, hetgeen nochtans wordt voorzien door artikel 9 van de Richtlijn. **Het verdient aanbeveling om de toezichthoudende autoriteiten op te nemen in het voorontwerp van wet evenals hun bevoegdheden en sancties, en er niet enkel naar te verwijzen in de memorie van toelichting.**

---

[11] Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere opsporingsmethoden.

[12] Zie artikel 14, wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post –en telecommunicatiesector.

28. Wat met het bewijs bekomen in strijd met de bepalingen van deze wet, bijvoorbeeld door personen die onbevoegd zijn om over deze informatie te beschikken ? Indien men zulk een bewijsmiddel wenst uit te sluiten, verdient het aanbeveling om zulks expliciet te voorzien in het voorontwerp van wet, en de **nietigheid van dergelijk bewijs op te leggen**. De Antigoonleer[13] van het Hof van Cassatie sluit onrechtmatig bekomen bewijs immers niet ipso facto uit.

29. Punt b) van artikel 2 van het voorontwerp van wet vermeldt 'de beteugeling van kwaadwillige oproepen naar de nooddiensten'. Punt c) voorziet in het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van personen die kwaadwillig gebruik hebben gemaakt van een elektronisch communicatienetwerk of –dienst. Deze punten vloeien niet voort uit de omzetting van de Richtlijn 2006/24, maar zijn voorzien in specifieke bepalingen. Overeenkomstig artikel 43bis § 3 7° van de wet van 21 maart 1991[14], is de ombudsdienst ermee belast van elke persoon die beweert het slachtoffer te zijn van kwaadwillig gebruik van een elektronische-communicatienetwerk of –dienst, het verzoek te onderzoeken om inlichtingen te krijgen over de identiteit en het adres van de gebruikers van elektronische-communicatienetwerken of –diensten die deze persoon hebben lastiggevallen, voorzover die gegevens beschikbaar zijn.

30. **De punten b) en c) maken geen deel uit van de omzetting van de richtlijn 2006/24. Aangezien de doeleinden van deze punten geen uitstaans hebben met 'ernstige criminaliteit', kan men zich de vraag stellen naar de opname in hetzelfde artikel, en de gelijkbehandeling van de punten a), b) en c) in het voorontwerp van wet en het ontwerp kb.** Er wordt namelijk geen enkel onderscheid voorzien naar de bewaarde gegevens waarop een beroep kan worden gedaan, noch naar de gebruiksduur van deze gegevens. Voor punt b) bijvoorbeeld lijkt toegang tot gegevens inzake emaildiensten niet noodzakelijk te zijn. Er wordt evenmin aangetoond waarom deze gegevens gedurende 24 maanden voor dit doeleinde zouden moeten toegankelijk zijn. **Omwille van het proportionaliteitsbeginsel en finaliteitsbeginsel, opgenomen in artikel 4 van de WVP, zou het voorontwerp van wet of minstens het ontwerp kb in een onderscheid tussen de voormelde punten moeten voorzien. Idealiter dienen de punten b) en c) in separate wetgeving te worden geregeld.**

---

[13] Zie hieromtrent onder meer het arrest Cass. 14 oktober 2003, T. Strafr. 2004, 129 met noot Ph. TRAEST.

[14] Wet betreffende de hervorming van sommige economische overheidsbedrijven.

31. Artikel 2, § 1 van het voorontwerp van wet voorziet verder : '*De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van justitie en van de minister, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de krachtens het eerste lid te bewaren gegevens alsook de voorwaarden en termijn van bewaring van deze gegevens.'*

32. **De Commissie merkt op dat de keuze om de soorten gegevens niet in de wettekst zelf, maar in een koninklijk besluit op te nemen, moeilijk verenigbaar is met de keuze die in de richtlijn 2006/24 is gemaakt over de te bewaren gegevens.** Aanvankelijk was door de Europese Commissie namelijk voorgesteld om een lijst gegevens als bijlage bij de richtlijn te voegen, waarbij een versnelde besluitvormingsprocedure zou gelden voor aanpassingen aan die lijst. Het Europees Parlement heeft evenwel met grote meerderheid een amendement aangenomen van de rapporteur Alvaro, om de gegevens in de tekst van de richtlijn zelf op te nemen. Zo is tevens gekozen voor een zwaardere procedure van aanpassing van de soorten te bewaren gegevens, met volledig instemmingsrecht van het Europees Parlement. **Eenzelfde opmerking dient gemaakt voor wat betreft de termijn van bewaring van de gegevens, cfr. infra, nrs. 33 en volgenden**. Het voorgaande gaat des te meer op gezien het feit dat in de memorie van toelichting wordt verklaard dat het kader voor de bewaring van gegevens, zoals voorzien door de richtlijn, niet noodzakelijk aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voldoet. Vandaar dat men in het ontwerp kb bijkomende gegevens wenst op te nemen, welke niet worden voorzien door de richtlijn, zoals bankgegevens.

33. Omtrent de bewaarduur voorziet artikel 2, §1 van het voorontwerp van wet : '*De bewaringstermijn voor de gegevens bedoeld in het eerste lid mag niet korter zijn dan 6 maanden en niet langer dan 24 maanden.'* Artikel 6 van de richtlijn bepaalt dat de gegevens minimum 6 maanden en maximum 24 maanden kunnen worden bewaard, vanaf de datum van de communicatie. Voor wat de duur betreft, wordt in het ontwerp kb gekozen voor de door de richtlijn voorziene maximumduur van 24 maanden. Het verslag aan de Koning motiveert deze keuze summier door te stellen dat '*op basis van de praktijk die is waargenomen bij de verschillende gedecentraliseerde politiediensten of bij het federale parket inzake verzoeken om inlichtingen aan de operatoren en aan de aanbieders van netwerken of diensten voor elektronische communicatie, mag worden aangenomen dat een uniforme termijn van vierentwintig maanden voor de bewaring van de verschillende, in*

artikel 126 van de wet bedoelde soorten gegevens, het meest geschikte mechanisme vormt."[15]

34. De Richtlijn 2006/24 biedt in artikel 6 een bewaartermijn van ten minste 6 maanden en ten hoogste 2 jaar aan. De groep 29 heeft 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[16]. 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 voor zover 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-operatoren.

35. De Commissie stelt vast dat het verslag aan de Koning nauwelijks uitlegt hoe de maximumtermijn van 24 maanden is bepaald. Men verwijst naar de praktijk bij de diverse politiediensten. De Commissie vraagt om de noodzaak van deze bewaartermijn duidelijker te rechtvaardigen en te onderbouwen. In navolging van de recente adviezen van de Groep 29 over dit onderwerp adviseert de Commissie 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."*[17]

---

[15] Verslag aan de Koning, p. 1-2.

[16] Zie: advies 4/2001 over de ontwerp overeenkomst van de Raad van Europa inzake computercriminaliteit, 10/2001 over een evenwichtige benadering in de strijd tegen het terrorisme, 4/2005 over het voorstel van richtlijn en advies 3/2006 inzake richtlijn 2006/24/EG.

[17] Groep 29, advies 4/2005, p. 8.

36. Verder merkt de Commissie op dat de belangrijkste grondslag voor de Richtlijn, verwoord in artikel 1, het harmoniseren is 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. Gezien de implementaties en voorstellen in andere EU lidstaten waarvan de Commissie kennis heeft, stelt ze vast dat van enige harmonisatie van de bewaartermijn vooralsnog weinig sprake is. Duitsland lijkt te kiezen voor een bewaartermijn van 6 maanden, net als Finland en Tsjechië. Ook Zweden, één van de vier initiatiefnemers van de totstandkoming van een Europese bewaarplicht, lijkt voor een minimumimplementatie te kiezen. Andere landen als Frankrijk, Denemarken en Spanje kiezen voor een bewaartermijn van 12 maanden. Nederland lijkt eveneens voor een termijn van 12 maanden te kiezen. Voor zover bekend opteert enkel Italië voor een bewaarduur van 24 maanden, en dan nog enkel voor telefoongegevens, de opslag van internetgegevens zou 6 maanden bedragen.

37. **Gelet op het voorgaande, meent de Commissie dat de actueel voorziene bewaarduur van 24 maanden verder onderbouwd dient te worden met meer overtuigende argumenten. Bij afwezigheid van zulk een rechtvaardiging, dient desgevallend een aanpassing van de voorziene termijn overwogen, zeker gelet op de gangbare bewaartermijnen in de meeste andere Europese landen, welke momenteel 6 tot 12 maanden bedragen.**

38. Artikel 2, §2 van het voorontwerp van wet voorziet dat de Koning, indien *uitzonderlijke omstandigheden* dat rechtvaardigen, na advies van het Instituut en van de Commissie voor de bescherming van de persoonlijke levenssfeer, voor een *onbeperkte periode,* een bewaringstermijn voor de gegevens kan vastleggen die langer is dan 24 maanden.

39. Vooreerst merkt de Commissie op dat de Nederlandse en Franse versie van het ontwerp kb verschillen, namelijk met betrekking tot de periode, welke in de Franse versie 'une période *limitée*' betreft, en in de Nederlandse 'een *onbeperkte* periode'. Overeenkomstig artikel 12 van de richtlijn dient deze verlenging in de tijd beperkt te zijn, en moet de Nederlandse versie dienovereenkomstig worden aangepast.

40. De Koning krijgt hierbij dus de mogelijkheid om een langere termijn dan het wettelijke maximum van 24 maanden te bepalen, *in uitzonderlijke omstandigheden*. Artikel 12 van de richtlijn verwoordt dit als volgt : '*Lidstaten met specifieke omstandigheden die een in de tijd beperkte verlenging van de in artikel 6 bedoelde bewaringsperiode rechtvaardigen, kunnen de noodzakelijke maatregelen treffen.'* Indien het gaat om een uitzondering, is het volgens de Commissie op zijn minst nodig om het basisprincipe van deze uitzondering formeel in de wet te regelen. Deze algemene regel kan nadien verder uitgewerkt worden in een koninklijk besluit, maar de grondslag zou in de wet moeten verankerd worden, wat hier niet het geval is : **de term 'uitzonderlijke omstandigheden' biedt niet voldoende rechtszekerheid, is uitermate vaag en is hierdoor te ruim interpreteerbaar.**

D.5. ANALYSE ONTWERP KB

D.5.1. Algemene bespreking ontwerp kb

41. De Commissie verwijst inzake de in het ontwerp kb voorziene bewaartermijn van 24 maanden naar de opmerkingen gedaan onder de nrs. 33 en volgenden. Zij herhaalt tevens dat de bewaarduur en soorten bewaarde gegevens bij voorkeur in de wet zouden moeten worden bepaald, en niet in het ontwerp kb, cfr. supra nr. 32.

42. De bewaarduur wordt in het ontwerp kb verschillend behandeld naargelang de aard van de gegevens : gegevens voor de identificatie van de abonnee en de gebruikte dienst worden bewaard gedurende de hele duur van het abonnement en voor een periode van 24 maanden vanaf de dag waarop het abonnement verstrijkt. De verkeers -en locatiegegevens, worden bewaard voor een periode van 24 maanden vanaf de dag waarop ze door de dienstenaanbieder zijn gegenereerd of verwerkt. Het voorgaande lijkt in te gaan tegen de tekst van de richtlijn, waar de bewaarduur ingaat vanaf de datum van de communicatie.

43. De memorie van toelichting[18] stelt dat de richtlijn een minimaal kader voorziet voor de bewaring van gegevens op het vlak van elektronische communicatie, hetwelk niet noodzakelijk voldoet aan de behoeften van de politiediensten en gerechtelijke autoriteiten voor het onderzoek, de vervolging en de beteugeling van strafbare feiten. Zo ontbreken volgens de memorie van toelichting in de door de richtlijn opgestelde lijst bepaalde gegevens die onmisbaar zijn voor identificatie van personen betrokken bij een relevante communicatie in het kader van een strafrechtelijk onderzoek, zoals bankgegevens. Merk op

[18] Mvt, p. 1-2.

dat de memorie stelt bijkomende gegevens nodig te hebben voor het strafrechtelijk onderzoek, maar deze gegevens eveneens openbaar maakt, of alleszins niet afsluit, voor onderzoeken door de Ombudsman of in het kader van de beteugeling van kwaadwillige oproepen naar de nooddiensten. Zoals hierboven onder de nrs. 22 en 23 reeds opgemerkt, dient verduidelijkt wie toegang heeft tot welke gegevens. In het licht van het proportionaliteitsbeginsel, kan men namelijk maar toegang hebben tot de gegevens welke men daadwerkelijk nodig heeft. In elk geval kan de Commissie zich niet vinden in de overweging van de memorie als zou de richtlijn een minimum kader voorzien : de richtlijn schrijft in artikel 5 gedetailleerd voor welke categorieën gegevens bewaard moeten worden. In overweging 21 bepaalt de richtlijn dat haar doel het onderzoeken, opsporen en vervolgen van zware criminaliteit uitmaakt, en zij niet verder gaat dan nodig is om deze doelstellingen te verwezenlijken. Volgens overweging 12 van de richtlijn moet de lijst van 'categorieën gegevens' als een maximum kader worden opgevat. Voor het bewaren van andere gegevens kunnen de lidstaten een beroep doen op artikel 15, eerste lid van richtlijn 2002/25/EG. **Wetgeving die op grond van dat artikel wordt uitgevaardigd, dient afzonderlijk te voldoen aan het vereiste van artikel 8 EVRM, namelijk dat ze in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.** De Commissie heeft een lijst opgevraagd bij de opstellers van het ontwerp met de extra –namelijk buiten hetgeen wordt voorzien door de richtlijn- te bewaren gegevens. Zulk een lijst kon haar vooralsnog evenwel niet worden overgemaakt, zodat de Commissie hiernavolgend -onder voorbehoud van misinterpretatie- zelf tracht na te gaan wat correspondeert met de richtlijn, en wat er buiten gaat. De Commissie heeft hierbij opgemerkt dat er voor elke categorie van gegevens in het ontwerp kb klaarblijkelijk meer wordt bewaard dan voorzien door de richtlijn, al dan niet met een motivering daaromtrent. De Commissie zal hiernavolgend in de artikelsgewijze bespreking hierop nader ingaan.

D.5.2. Artikelsgewijze bespreking van het ontwerp kb

ARTIKEL 1

44. Dit artikel definieert een aantal begrippen, waaronder 'Persoonsgegevens' : hieronder worden begrepen de naam en voornaam, het facturatie en het contactadres van de abonnee of de gebruiker. Er dient opgemerkt dat deze definitie niet overeenkomt met de definitie van 'persoonsgegeven' in artikel 1, §1 van de WVP, welke veel ruimer is. De Commissie gaat er dan ook vanuit dat het hier niet de bedoeling is om dezelfde definitie te hanteren als voorzien door de WVP.

45.

ARTIKEL 2

45. Artikel 2 betreft de gegevens die de operatoren voor vaste telefonie moeten bewaren, i.e. zij die een openbare vaste-telefoniedienst aanbieden. Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie op het ogenblik van een communicatie.

46. De eerste categorie bevat voornamelijk de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. **De Commissie merkt op dat enkel de elementen 1° en 2° (het aan de abonnee toegewezen nummer, en de persoonsgegevens van de abonnee) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 8°.** Deze uitbreiding wordt niet gemotiveerd, tenzij door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. Over element 6° stelt het verslag aan de koning dat *'deze gegevens kunnen uiterst belangrijk blijken te zijn om te bepalen tot welke operator de gerechtelijke autoriteiten zich eventueel moeten wenden om de inlichtingen te verkrijgen van voor of na een bepaalde periode*.' Voor wat punt 7, de bankgegevens, betreft, merkt de Commissie op dat deze gegevens door de onderzoekers bij de banken kunnen worden bekomen, aangezien de onderzoekers over de identiteitsgegevens beschikken. In hoeverre is het dan proportioneel om deze gegevens hier op te nemen ?

47. De verzameling van de elementen 3° tot en met 8° gaat verder dan de lijst zoals voorzien in artikel 5 van de richtlijn. Zoals hierboven reeds aangehaald, moet volgens overweging 12 van de richtlijn deze lijst als een maximum kader worden opgevat. Voor het bewaren van andere gegevens kunnen de lidstaten een beroep doen op artikel 15, eerste lid van richtlijn 2002/25/EG. Wetgeving die op grond van dat artikel wordt uitgevaardigd, dient afzonderlijk te voldoen aan het vereiste van artikel 8 EVRM, namelijk dat ze in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Het ontwerp kb voldoet hieraan vooralsnog niet.

48. De tweede categorie van gegevens zijn gegevens gegenereerd tijdens een communicatie. Hieromtrent heeft de Commissie geen opmerkingen.

ARTIKEL 3

49. Dit artikel betreft de gegevens die de operatoren voor mobiele telefonie moeten bewaren, i.e. de operatoren die een openbare mobiele telefonie dienst aanbieden. Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie op het ogenblik van een communicatie.

50. De eerste categorie bevat voornamelijk de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. **De Commissie merkt op dat enkel de elementen 1° en 2° (het aan de abonnee toegewezen nummer, en de persoonsgegevens van de abonnee) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 10°.** Deze uitbreiding wordt summier gemotiveerd, vooreerst door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. Over elementen 3° en 4° stelt het verslag aan de koning dat *'weten wanneer de kaart is gekocht en wanneer deze voor de eerste keer is gebruikt kan kostbare informatie opleveren voor de rechercheurs. … Door de inlichtingen over het opladen van krediet op een voorafbetaalde kaart te bewaren is het mogelijk de gebruikscapaciteit te kennen waarover de gebruiker beschikt, de wijze waarop hij heeft opgeladen, of de plaats waar de oplaadbeurt heeft plaatsgevonden. Dergelijke informatie valt buiten het bestek van de gegevens die normaal door de richtlijn worden beoogd, maar is werkelijk van belang in het kader van een onderzoek, waar dat kleine stukje informatie vaak de enige piste is waarover*

de politiediensten beschikken om een verdachte te proberen identificeren.' De Commissie volgt deze uitleg, maar meent omwille van de reeds onder de nrs. 43 en 47 genoemde opmerkingen dat zulks niet volstaat om verder te gaan dan hetgeen wordt voorzien door de richtlijn.

51. De tweede categorie van gegevens zijn gegevens gegenereerd tijdens een communicatie. Hieromtrent heeft de Commissie geen opmerkingen.

ARTIKEL 4

52. Dit artikel heeft betrekking op de aanbieders van internettoegang. Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie.

53. De eerste categorie bevat voornamelijk de gegevens die door de abonnee worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt. **De Commissie merkt op dat enkel de elementen 1° en 2° (de identificatiecode van de abonnee, en de persoonsgegevens van de abonnee) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 8°.** Deze uitbreiding wordt summier gemotiveerd, door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. De Commissie neemt nota van deze uitleg, maar meent omwille van de reeds onder de nrs. 43 en 47 genoemde opmerkingen dat zulks niet volstaat om verder te gaan dan hetgeen wordt voorzien door de richtlijn.

54. De tweede categorie van gegevens zijn gegevens inzake het verkeer en de locatie. **De Commissie merkt op dat enkel de elementen 1° tot en met 4°, en 6° (maar volgens de richtlijn enkel bij de aanvang, niet bij het einde) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 5° en 7°.** Deze uitbreiding wordt niet gemotiveerd, en kan gelet op de hierboven reeds gemaakte opmerkingen dan ook niet worden gevolgd.

ARTIKEL 5

55. Artikel 5 heeft betrekking op de gegevens die moeten worden bewaard door de aanbieders van emaildiensten en door de aanbieders van internet telefoniediensten. Met de aanbieders van emaildiensten worden zowel SMTP mail bedoeld als webmail, zoals Hotmail, Yahoo, Gmail, ... Die gegevens worden opgedeeld in twee categorieën : enerzijds gegevens met betrekking tot de identificatie van de abonnee, of de gebruikte dienst, anderzijds gegevens in verband met het verkeer en de locatie.

56. Voor wat betreft de webmail diensten zoals Hotmail en Gmail is het niet duidelijk op welke grond zij aan de bewaarplicht zijn onderworpen. De memorie van toelichting, noch het verslag aan de koning verschaft hier duidelijkheid over.

57. De eerste categorie bevat voornamelijk de gegevens die door de abonnee of gebruiker worden verstrekt wanneer hij een abonnement aangaat of wanneer het abonnement loopt, of wanneer hij van de aangeboden diensten gebruik maakt. **De Commissie merkt op dat enkel de elementen 1° en 2° (de identificatiecode van de abonnee of van de gebruiker, en de persoonsgegevens van de abonnee of de gebruiker) zijn voorzien door artikel 5 van de richtlijn, maar blijkbaar niet 3° tot en met 6°.** Deze uitbreiding wordt summier gemotiveerd, door de memorie van toelichting welke stelt dat het kader van de richtlijn niet noodzakelijk voldoet aan de behoeften van de politiediensten en de gerechtelijke autoriteiten voor het onderzoek, de vervolgingen de beteugeling van strafbare feiten. De Commissie neemt nota van deze uitleg, maar meent omwille van de reeds onder de nrs. 43 en 47 genoemde opmerkingen dat zulks niet volstaat om verder te gaan dan hetgeen wordt voorzien door de richtlijn.

58. De tweede categorie van gegevens zijn gegevens gegenereerd tijdens een communicatie. Hieromtrent heeft de Commissie geen opmerkingen, behoudens aangaande punt 7 (wat betreft punt 7, voorziet de richtlijn enkel de opslag van de locatie bij de aanvang).

ARTIKEL 6

59. Het eerste lid van artikel 6 slaat op de operatoren die verschillende gecombineerde diensten aanbieden, zoals bijvoorbeeld het verzenden van mails via een gsm. De gegevens die zij in voormeld geval zullen moeten bewaren moeten overeenstemmen met zowel hetgeen werd voorzien door artikel 3 (mobiele telefonie) als artikel 5 (email) van het ontwerp kb. **De Commissie verwijst naar de hierboven gemaakte opmerkingen bij de artikelen 2 tot en met 5, welke *mutatis mutandis* op artikel 6 van toepassing zijn.**

60. Het tweede en derde lid betreft bepalingen inzake de tijdsaanduidingen, welke werden overgenomen uit het koninklijk besluit van 9 januari 2003. De Commissie heeft hieromtrent geen opmerkingen.

ARTIKEL 7

61. Artikel 7 stelt volgens het verslag aan de koning een aantal voorwaarden inzake bewaring vast die bedoeld zijn om de veiligheid van de gegevens te garanderen en ervoor te zorgen dat ze op gepaste wijze worden verwerkt door personeel dat daarvoor bevoegd is. De elementen 1°, 2°, en 4° werden rechtstreeks overgenomen uit de richtlijn 2006/24, artikel 7. Punt 1 voorziet in een gescheiden opslag voor de te bewaren gegevens, hetgeen overeenstemt met de aanbevelingen van de groep 29, welke voorzien in een decentrale, logisch gescheiden opslag van de specifiek voor opsporingsdoeleinden te bewaren gegevens. Er dient vanuit privacyoogpunt een duidelijke scheiding te zijn tussen de gegevens welke door de operatoren worden bewaard voor bedrijfsdoeleinden, en deze bewaard uit hoofde van de voorliggende ontwerpen. Het ontwerp kb blijft verder onder element 2° nogal vaag, door enkel te verwijzen naar 'passende technische en organisatorische maatregelen' en deze niet verder uit te werken. Hieromtrent verwijst de Commissie ter informatie naar de door haar opgestelde referentiemaatregelen welke volgens de Commissie, naargelang van geval tot geval, toepasbaar dienen te zijn op een verwerking van persoonsgegevens[19].

62. Element 3° legt de operator op om te garanderen dat enkel de Coördinatiecel Justitie bedoeld in artikel 2 van het koninklijk besluit van 9 januari 2003 toegang heeft tot de gegevens.

---

[19] Zie hieromtrent het document 'Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens' vanwege de Commissie voor de bescherming van de persoonlijke levenssfeer, te consulteren op haar website http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

63. **De Commissie merkt hieromtrent vooreerst op dat hierdoor enkel de toegang tot de gegevens bij de operatoren zelf wordt geregeld, i.e. intern, doch niet aan wie deze gegevens extern kunnen worden overgemaakt.** De coördinatiecel justitie is overeenkomstig artikel 2, §1 van voormeld kb : '*...Om aan de medewerkingsplicht te voldoen zoals opgelegd door artikel 46bis, §2, 88bis, §2 en 90quater, §2 van het wetboek van strafvordering, wordt er door iedere operator van een telecommunicatienetwerk en iedere verstrekker van een telecommunicatiedienst één of meerdere personen bij name aangeduid en belast met de taken die uit de medewerkingsplicht voortvloeien, hierna genoemd de 'Coördinatiecel Justitie'.* Zoals reeds aangegeven supra onder punten 26, 29 en 30, zou er duidelijk moeten worden voorzien aan wie welke gegevens kunnen worden overgemaakt door de Coördinatiecel Justitie. Overeenkomstig artikel 2, §1, c) van het voorontwerp van wet zou bijvoorbeeld ook de Ombudsman voor de telecommunicatie inzage moeten kunnen krijgen, hetgeen nu niet expliciet is voorzien. **Er dient duidelijk en limitatief te worden bepaald, bij voorkeur in het voorontwerp van wet, wie toegang heeft tot de bewaarde gegevens, tot welke gegevens in het bijzonder, en voor welke specifieke doeleinden.**

64. **Daarnaast dient herhaald dat deze Coördinatiecel door het kb van 9 januari 2003 enkel werd geïnstalleerd bij de operatoren, en niet bij de aanbieders en doorverkopers vermeld in artikel 9, §§5 en 6 WEC.** Is het de bedoeling dat de aanbieders en doorverkopers ook een dergelijke coördinatiecel in het leven roepen, die aan dezelfde bepalingen moet voldoen inzake 24/7 beschikbaarheid en dergelijke ? Zoals reeds opgemerkt supra onder punt 16 heeft de wetgever vroeger deze gelijkbehandeling van operatoren enerzijds en aanbieders en doorverkopers anderzijds uitgesloten door niet naar hen te verwijzen in de huidige versie van artikel 126 WEC, doch wel in artikel 9, §7 WEC, welke in een aparte regeling voor deze categorie zou voorzien.

65. **Verder is 'de garantie' van de operator dat enkel de coördinatiecel justitie toegang heeft niet voldoende, de niet-naleving van deze interne toegangsregel zou strafrechtelijk moeten worden gesanctioneerd.** Zie hieromtrent hetgeen wordt bepaald door artikel 13, 2. van de richtlijn : *'elke lidstaat neemt in het bijzonder de noodzakelijke maatregelen om ervoor te zorgen dat elke opzettelijke toegang tot of overbrenging van gegevens die overeenkomstig deze richtlijn worden bewaard die niet is toegestaan uit hoofde van krachtens deze richtlijn vastgestelde nationale uitvoeringsbepalingen, strafbaar is met sancties, met inbegrip van administratieve of strafrechtelijke sancties, die effectief, evenredig en afschrikkend zijn*.'

66. Tenslotte moet elke operator ervoor zorgen dat de gegevens aan het einde van de bewaringstermijn worden vernietigd, met uitzondering van de geraadpleegde en vastgelegde gegevens. Omtrent deze laatste gegevens wordt geen bewaarduur voorzien. Het zou evenwel logisch lijken dat indien de gegevens werden geraadpleegd in het kader van een gerechtelijk onderzoek, deze verder worden bewaard door de verantwoordelijke diensten voor zolang als nodig voor hun onderzoek, en kunnen worden vernietigd bij de operator. Indien de onderzoeksinstanties evenwel van oordeel waren dat de gegevens niet nuttig waren voor het onderzoek, is er geen noodzaak om de gegevens nog langer te laten bewaren door de operator na de voorziene bewaartermijn.

ARTIKELEN 8 EN 9

67. Hieromtrent heeft de commissie geen opmerkingen.

ARTIKEL 10

68. Dit artikel bepaalt dat het ontwerp kb ook van toepassing is op mislukte oproeppogingen. De richtlijn 2006/24 bepaalt in artikel 3, 2. dat zij geen vereisten bevat betreffende de bewaring van gegevens in verband met niet tot stand gekomen verbindingen, maar wel betreffende oproeppogingen zonder resultaat, hetgeen volgens de richtlijn een communicatie uitmaakt waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord[20].

69. De verwoording in artikel 10 sluit hier niet helemaal bij aan, waar zij stelt dat het besluit ook van toepassing is op oproepen die niet terechtgekomen zijn wegens een interventie van de netwerkbeheerder. Het ware aangewezen dit te herschrijven, bijvoorbeeld '*...ook van toepassing op oproepen die door het netwerkbeheer werden beantwoord*'.

[20] Zie artikel 2, f) Richtlijn 2006/24/EG.

ARTIKEL 11

70. Volgens het verslag aan de koning wijst artikel 11 binnen elke coördinatiecel Justitie een aangestelde voor de gegevensverwerking aan, zoals dat wordt toegestaan door artikel 17bis, tweede en derde lid, van de WVP. Artikel 11, derde lid is erop gericht de onafhankelijkheid van de aangestelde in zijn functie te garanderen.

71. De Commissie onderstreept dat de Koning het statuut van de aangestelden voor de gegevensbescherming nog niet heeft vastgesteld in toepassing van artikel 17bis van de WVP. Het zou dus voorbarig zijn vooruit te lopen op toekomstige bepalingen. Alle definities van controlefuncties, hetzij intern of niet, zouden dus rekening moeten houden met de Richtlijn 95/46/EG (overweging (49) en artikel 18). De hier bedoelde aangestelden voor de gegevensbescherming zouden in de praktijk een bevoorrechte gesprekspartner moeten zijn van de Commissie, hetgeen in het ontwerp kb wordt gestimuleerd door op te leggen om hun identificatie –en contactgegevens mee te delen aan de Commissie. Het is tevens aangewezen dat het ontwerp kb een grote zichtbaarheid verzekert voor hun adviezen en rapporten. In dit opzicht beveelt de Commissie aan dat het ontwerp kb zou aangepast worden opdat deze rapporten eveneens systematisch aan haar zouden meegedeeld worden.

72. De onafhankelijkheid van de aangestelden voor de gegevensbescherming is primordiaal. Het is evenwel belangrijk dat deze verzekerd wordt door gepaste maatregelen. De volgende maatregelen kunnen in het ontwerp kb aangenomen worden, bovenop deze die reeds vermeld zijn in artikel 11:

• Kennisgeving aan de Commissie van de aard van juridische band tussen deze aangestelden en de dienst waar zij hun functie van aangestelde zullen uitoefenen, alle elementen met betrekking tot de beroepskwalificaties in verband met de functie van aangestelde, maatregelen genomen door de verantwoordelijke voor de verwerking in functie van de door de aangestelde voor de bescherming van gegevens uit te voeren opdrachten;

• Verplichting om de aangestelden op een dusdanig niveau in de hiërarchie te plaatsen zodat zij over de mogelijkheid beschikken om rechtstreeks met het management/directiecomité te communiceren en hun opdracht rechtstreeks uit te oefenen bij de verantwoordelijke voor de verwerking;

73. Tenslotte dient nogmaals herhaald dat artikel 11, §2, 3° moet worden verduidelijkt, cfr. supra nr. 63, aangezien het ontwerp kb noch het voorontwerp van wet duidelijk stellen wie extern bij de coördinatiecel justitie toegang heeft tot de bewaarde gegevens.

ARTIKEL 12

74. Artikel 12 legt de betrokken operatoren de verplichting op om het instituut jaarlijks een aantal statistische inlichtingen mee te delen die bestemd zijn voor de EG Commissie. Vreemd genoeg legt artikel 12 dit enkel op aan de 'operator die een openbare telefoniedienst verstrekt'. Indien men ervoor kiest om het voorontwerp van wet en het ontwerp kb eveneens van toepassing te verklaren op de aanbieders en doorverkopers bedoeld in artikel 9, §§5 en 6 WEC, dienen zij eveneens in dit artikel te worden meegenomen. Het betreft overeenkomstig artikel 10 van de richtlijn ook niet enkel een 'telefoniedienst', doch wel een elektronische communicatiedienst of communicatienetwerk.

ARTIKELEN 13 EN 14

75. Hieromtrent heeft de commissie geen opmerkingen.

OM DEZE REDENEN,

Is de Commissie van oordeel dat

- gelet op het legaliteitsbeginsel, de essentiële elementen inzake de bewaring van gegevens in het voorontwerp van wet duidelijker dienen te worden bepaald. In dit opzicht zou de bewaarduur in het voorontwerp van wet moeten worden bepaald, en eveneens de te bewaren gegevens.
- de noodzaak voor het bewaren van bepaalde gegevens, die niet voorzien zijn in de richtlijn, dient gerechtvaardigd overeenkomstig de principes van artikel 8 EVRM.
- het voorontwerp van wet zou dienen te verduidelijken voor het onderzoek, de vervolging en de beteugeling van welke (zware) criminele feiten de bewaarde gegevens kunnen worden gebruikt.
- de bewaarduur van 24 maanden meer dient te worden gefundeerd en gerechtvaardigd, en desgevallend heroverwogen met het oog op de voorziene bewaartermijnen in de meeste andere Europese landen.

- de toepassing van het voorontwerp van wet en ontwerp kb op de aanbieders en doorverkopers voorzien in artikel 9, §§ 5 en 6 dient te worden herbekeken, en voor hen eventueel in een andere bepaling te voorzien.
- Het bewaren van de gegevens voor de doeleinden voorzien in artikel 2, §1, b) en c) (de kwaadwillige oproepen naar de nooddiensten en de ombudsdienst voor telecommunicatie) uit de toepassing van het voorontwerp van wet dienen gehaald, en hieromtrent in een separate regelgeving moet worden voorzien.
- uitzonderingen niet kunnen worden geregeld via een koninklijk besluit, doch dat minstens het basisprincipe van de uitzondering in de wet dient te worden geregeld. Het begrip 'uitzonderlijke omstandigheden' in artikel 2, §2 van het voorontwerp van wet is te vaag.
- de toewijzing van de personen of instanties die toegang hebben tot de bewaarde gegevens via de coördinatiecel justitie expliciet moet gebeuren in het voorontwerp van wet , waarbij tevens dient aangegeven wie toegang heeft tot welke gegevens.
- de niet naleving van de vereisten inzake toegang en gebruik van de verzamelde gegevens strafbaar dient gesteld.
- de toezichthoudende autoriteiten expliciet moeten worden aangeduid in het voorontwerp van wet , evenals hun bevoegdheden en sancties terzake.

Gelet op de in dit advies vermelde opmerkingen, brengt de Commissie voor de bescherming van de persoonlijke levenssfeer een *ongunstig* advies uit over de actuele inhoud van het voorontwerp van wet en ontwerp van koninklijk besluit.

Voor de Administrateur m.v.,
Het Afdelingshoofd ORM,

De Voorzitter,

(get.) Patrick Van Wouwe

(get.) Willem Debeuckelaere