

1. Wijze van omzetting

Artikelen:

*Memorie van Toelichting, p. 2, 4^e en laatste alinea (verder op p. 3).
Voorontwerp van Wet, Art. 1, §1, 2^e lid.*

Knelpunten:

De memorie van toelichting en artikel 1, §1, 2e lid, van het voorontwerp van wet stipuleren dat de lijst van te bewaren gegevens, de bewaringsvoorwaarden alsook de werkelijke bewaringstermijn zullen worden vastgelegd door de Koning via een Koninklijk Besluit. Dit zal gebeuren aan de hand van “*een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister [welke?], en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut [het BIPT?]*”. Op deze manier wordt een democratisch debat in het parlement over deze cruciale items onmogelijk gemaakt en kan men -zonder verantwoording te moeten afleggen ten opzichte van het parlement en de bevolking- verregaande beslissingen nemen die bovendien (te) gemakkelijk gewijzigd kunnen worden in de toekomst. De Liga voor Mensenrechten is van oordeel dat deze materie te ingrijpend is om niet langs parlementaire weg te behandelen.

Aanbeveling:

De Liga voor Mensenrechten pleit ervoor om de omzetting van Richtlijn 2006/24/EG, zeker wat betreft de kritieke punten, zoals de lijst van te bewaren gegevens, de bewaringsvoorwaarden en de werkelijke bewaringstermijn, te reguleren via een wet in plaats van een Koninklijk Besluit.

2. Bewaringstermijn

A. Artikelen:

*Memorie van Toelichting, p.3, 5^e en 6^e alinea.
Voorontwerp van Wet, Art. 2, §1, 2^e en 3^e lid.*

Knelpunten:

Artikel 2, §1, 3^e lid, stelt dat de bewaringstermijn niet korter mag zijn dan 6 maanden en niet langer dan 24 maanden. Artikel 2, §1, 2^e lid bepaalt echter dat de werkelijke bewaringstermijn zal bepaald worden in een Koninklijk Besluit. Het vastleggen van de werkelijke bewaringstermijn is echter geen detail bij het uitvoeren van de bewaarplicht, maar vormt een cruciaal element waarover gedebatteerd moet worden in het parlement op basis van concrete argumenten. Het éézijdige argument om verkeers- en locatiegegevens zo lang mogelijk te bewaren om tegemoet te kunnen komen aan eventuele, toekomstige onderzoeksvragen heeft immers een belangrijke keerzijde. Hoe langer de bewaarperiode zal zijn, hoe groter de privacyschending wordt, hoe hoger de gerelateerde kosten worden voor de samenleving, hoe moeilijker informatie terug te vinden zal zijn, hoe groter de foutenmarge wordt, hoe moeilijker het wordt deze gegevens te beveiligen en hoe groter het risico wordt op misbruik van deze gegevens... Een Koninklijk Besluit beschikt nu eenmaal niet over de noodzakelijke democratische inslag om een dergelijke, fundamentele beslissing te nemen.

Aanbeveling:

De Liga voor Mensenrechten pleit ervoor om de werkelijke bewaartermijn te reguleren door middel van een wet na een fundamenteel en uitgebreid parlementair debat. De Liga is van oordeel dat een maximale bewaarperiode van 6 maanden essentieel is om de schending van het recht op privacy te beperken. Bovendien zijn er geen enkele aanwijzingen die een langere

bewaartermijn in België kunnen rechtvaardigen, laat staan noodzakelijk maken. Zoniet is het aan de Belgische overheid om deze noodzaak aan te tonen op basis van concreet cijfermateriaal.

B. Artikelen:

Memorie van Toelichting, p.3, 5^e alinea.

Voorontwerp van Wet, Art. 2, §2.

Knelpunten:

Artikel 2, §2, van het voorontwerp van wet geeft de Koning bovendien de bevoegdheid (conform Richtlijn 2006/24/EG) om in uitzonderlijke omstandigheden, en voor een beperkte periode, een langere bewaartermijn dan het wettelijke maximum van 24 maanden te bepalen. Er wordt echter niet nader verklaard wanneer er sprake is van “*uitzonderlijke omstandigheden*”. Deze bepaling is dan ook zo vaag en algemeen dat het rechtsonzekerheid creëert en volgens de rechtspraak van het Europees Hof voor de Rechten van de Mens een schending uitmaakt van fundamentele burgerrechten¹.

Aanbeveling:

De Liga voor Mensenrechten vraagt dat België bij wet afstand doet van deze mogelijkheid tot verlenging van de maximale bewaartermijn. Minstens moet er een limitatieve lijst worden opgesteld van wat kan worden beschouwd als een “*uitzonderlijke omstandigheid*” en deze moet vervolgens worden opgenomen in het voorontwerp van wet. Daarnaast moet ook bij wet worden vastgelegd met hoeveel maanden de maximale bewaartermijn van 24 maanden bij “*uitzonderlijke omstandigheden*” maximaal kan worden verlengd.

<u>3. Te bewaren gegevens</u>

Artikelen:

Memorie van Toelichting, p. 2, voorlaatste alinea en p. 3, voorlaatste alinea.

Voorontwerp van Wet, Art. 2, §1, 1^e en 2^e lid.

Knelpunten:

Artikel 2, §1, 1^e lid, verplicht operatoren om de verkeers- en locatiegegevens en de gegevens voor identificatie van de eindgebruikers te bewaren die door hen worden gegenereerd of verwerkt bij het aanbieden van hun respectievelijke elektronische communicatienetwerken en -diensten. Artikel 2, §1, 2^e lid, stelt dat de werkelijke lijst van te bewaren gegevens echter zal bepaald worden door middel van een Koninklijk Besluit. De memorie van toelichting verduidelijkt op p. 2, laatste alinea, ook de keuze voor een KB aangezien “het een snelle update van het wettelijk kader toelaat”.

Het bepalen van de lijst van te bewaren gegevens is echter geen detail bij het uitvoeren van de bewaarplicht, maar vormt een cruciaal element waarover ook hier weer gedebatteerd moet worden in het parlement op basis van concrete argumenten. Het éézijdige argument om zoveel mogelijk gegevens te bewaren om tegemoet te kunnen komen aan eventuele, toekomstige onderzoeksvragen kent immers dezelfde belangrijke keerzijde. Hoe meer gegevens bewaard worden, hoe groter de privacyschending wordt, hoe hoger de gerelateerde kosten worden, hoe moeilijker informatie terug te vinden zal zijn, hoe groter de foutenmarge

¹ Europees Hof voor de Rechten van de Mens, zaak van Silver en anderen versus het Verenigd Koninkrijk, 25 maart 1983, lijn 87 e.v.,

<http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=Silver&sessionid=15329098&skin=hudoc-en>.

wordt, hoe moeilijker het wordt deze gegevens te beveiligen en hoe groter het risico wordt op misbruik van deze gegevens... Een Koninklijk Besluit beschikt dus niet over de noodzakelijke democratische inslag om een dergelijke, fundamentele beslissing te nemen.

Bovendien laat de memorie van toelichting op p. 3, voorlaatste alinea, uitschijnen dat men de lijst van te bewaren gegevens, zoals vastgelegd in Richtlijn 2006/24/EG, wenst uit te breiden louter op basis van wenselijkheidslijstjes van politiediensten. De memorie van toelichting gaat er echter van uit dat deze uitbreiding wordt gecompenseerd door de expliciete bepaling in het voorontwerp van wet dat de privacywet van 8 december 1992 van toepassing zal zijn op de bewaarplicht. Deze extra referentie verandert echter niets aan de praktijk aangezien aanbieders van openbare elektronische communicatiediensten en -netwerken uiteraard ook zonder deze expliciete referentie reeds gebonden waren door de bepalingen uit de privacywet van 8 december 1992. Er wordt door het voorontwerp van wet dan ook geen enkele sterke garantie ten aanzien van het recht op privacy geboden die de uitbreidingen op Richtlijn 2006/24/EG kunnen compenseren.

De Artikel 29 Werkgroep waarschuwde ons reeds in een advies van 2001, n.a.v. de terreuraanslagen in New York, voor dit soort disproportionele maatregelen die onze samenleving ondermijnen. Zo is de Artikel 29 Werkgroep van oordeel dat niet alles wat bruikbaar of wenselijk zou kunnen zijn voor de misdaadbestrijding ook als een noodzakelijke maatregel beschouwd kan worden in een democratische samenleving. Zeker niet wanneer dit leidt tot de systematische registratie van alle elektronische communicatie. *“Één van de kernelementen van terrorismebestrijding impliceert dat wij zorg dragen voor het behoud van fundamentele waarden die de grondslag van onze democratische maatschappijen vormen [zoals het recht op de bescherming van persoonsgegevens].”*². Ook het Europees Hof voor de Rechten van de Mens stelde in het arrest van ‘Klass en anderen’ dat autoriteiten geen onbeperkte appreciatieruimte genieten ten aanzien van het in art. 8 EVRM gewaarborgde recht op privacy in de strijd tegen spionage en terreur³.

Aanbeveling:

De Liga voor Mensenrechten pleit ervoor om de lijst van te bewaren gegevens te reguleren door middel van een wet na een fundamenteel en uitgebreid parlementair debat. De Liga is van oordeel dat de lijst van te bewaren gegevens op zijn minst beperkt moet blijven tot die gegevens die vereist worden door Richtlijn 2006/24/EG. Bovendien zijn er geen enkele aanwijzingen die een uitbreiding van deze lijst in België kunnen rechtvaardigen, laat staan noodzakelijk maken. Zoniet is het aan de Belgische overheid om deze noodzaak aan te tonen op basis van concreet cijfermateriaal.

4. *Verantwoordelijken voor het opslaan & bewaren van de gegevens*

Artikelen:

Memorie van Toelichting, p. 1, 1^e en 2^e alinea.

Voorontwerp van Wet, art. 2, §1.

² RODOTA, S., *Advies 10/2001 betreffende de behoefte aan een evenwichtige aanpak in de strijd tegen terrorisme*, (Artikel 29 Werkgroep), 14 december 2001, p. 3-4:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53nl.pdf.

³ EHRM, Klass e.a. versus Duitsland, 6 september 1978, regel 49-50:

<http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Klass&sessionId=15331040&skin=hudoc-en>.

Knelpunten:

Richtlijn 2006/24/EG geldt enkel ten aanzien van aanbieders van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken. De memorie van toelichting en art. 2, §1 van het voorontwerp van wet verwijzen niet langer naar het belangrijke adjectief ‘openbaar’ en breiden zo impliciet de verplichting uit naar alle aanbieders van elektronische communicatiediensten en -netwerken, ook ten aanzien van die aanbieders die geen deel uitmaken van het publieke domein. Bijgevolg zou de bewaarplicht ook van toepassing worden op interne webmail van bedrijven, universiteiten, alsook op private thuisnetwerken. Het toepassen van de bewaarplicht op private elektronische communicatiediensten en -netwerken zou een enorme administratieve en technische last met zich meebrengen voor bedrijven en publieke instellingen, en mogelijks ook voor vele private burgers.

Bovendien zou het een efficiënte en alomvattende controle op aanbieders van elektronische communicatiediensten en -netwerken onmogelijk maken gezien de proliferatie van private elektronische communicatiediensten en -netwerken in onze huidige digitale samenleving. Aangezien elektronische communicatiediensten of -netwerken die het openbare domein niet overschrijden zich volgens art. 9, §§5 en 6 van de wet van 13 juni 2005 betreffende de elektronische communicatie niet moeten laten registreren bij het BIPT of een andere officiële instelling, is het onduidelijk hoe een toezichhoudende instantie moet nagaan of de nodige veiligheidsmaatregelen en privacyprotocollen worden nageleefd door de aanbieders van zulke elektronische communicatiediensten of -netwerken.

Aanbeveling:

De Liga voor Mensenrechten pleit ervoor om de reikwijdte van het voorontwerp van wet te beperken tot die operatoren die expliciet door Richtlijn 2006/24/EG worden gevat, met name de aanbieders van openbaar beschikbare elektronische communicatiediensten of van openbaar beschikbare elektronische communicatienetwerken.

5. <u>Doeleinden van het bewaren en raadplegen van gegevens</u>

Artikelen:

Memorie van Toelichting, p. 1, 2^e alinea en p. 3, 4^e alinea.

Voorontwerp van Wet, Art. 2, §1.

Knelpunten:

Artikel 2, §1, van het voorontwerp van wet, alsook de memorie van toelichting, zorgen er voor dat het toepassingsgebied van Richtlijn 2006/24/EG flink wordt uitgebreid. Richtlijn 2006/24/EG legt aan aanbieders van openbare elektronische communicatiediensten of een openbaar elektronisch communicatienetwerk de verplichting op om bepaalde gegevens die door hen gegenereerd of door hen worden verwerkt, te bewaren teneinde te garanderen dat die gegevens beschikbaar zullen zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit. Artikel 2, §1, van het Belgische voorontwerp van wet laat echter toe dat de te bewaren gegevens in het kader van de bewaarplicht ook kunnen worden geraadpleegd bij:

- *“het onderzoek, de vervolging en de beteugeling van strafbare feiten;*
- *de beteugeling van kwaadwillige oproepen naar nooddiensten;*
- *het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronische communicatienetwerk of -dienst”.*

Richtlijn 2006/24/EG verwijst dus enkel naar “het onderzoeken, opsporen en vervolgen van ernstige criminaliteit” (zoals gedefinieerd in de nationale wetgevingen van de lidstaten) waarbij, bij de goedkeuring van deze richtlijn, destijds expliciet werd gerefereerd aan de strijd tegen terrorisme en kinderpornografie. Het Belgische voorontwerp van wet wil het gebruik van de te bewaren gegevens echter toelaten bij het “*onderzoeken, opsporen en beteugelen van elke strafbare daad*”, ongeacht de ernst ervan. Bovendien is de woordkeuze van “*beteugeling*” op zijn minst bizar te noemen. Waarom wijkt men af van de woordkeuze van de betrokken Richtlijn terzake, en wat houdt “beteugeling” precies in? Het Van Dale Woordenboek ‘Hedendaags Nederlands’ verklaart “beteugelen” als “*in zijn vrije uiting, loop of beweging bedwingen; inhouden, intomen*”. Omvat dit bijgevolg ook een “preventie”-aspect? Het Europees Parlement heeft bij de bespreking van Richtlijn 2006/24/EG immers expliciet het woord “preventie” laten schrappen aangezien ze het bewaren en raadplegen van verkeers- en locatiegegevens ter preventie van ernstige criminaliteit niet proportioneel achtte⁴.

Een tweede uitbreiding van de reikwijdte van Richtlijn 2006/24/EG in het Belgische voorontwerp van wet vormt de mogelijkheid om verkeers- en locatiegegevens te bewaren en te raadplegen bij “de beteugeling van kwaadwillige oproepen naar nooddiensten”. Op dit moment kunnen nooddiensten die problemen hebben met kwaadwillige oproepen klacht neerleggen bij het parket. Het parket zal de oproepen vervolgens onderzoeken op basis van de gegevens die zij kunnen opvragen bij telecomoperatoren. Er zijn bijgevolg geen bijkomende juridische mogelijkheden vereist. Ten slotte roept het Belgische voorontwerp van wet nog een derde uitbreiding van Richtlijn 2006/24/EG in het leven door de mogelijkheid om verkeers- en locatiegegevens te bewaren en te raadplegen bij “het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk of -dienst”. De Ombudsdienst voor telecommunicatie beschikt reeds over de mogelijkheid om personen die misbruik maken van een elektronisch communicatienetwerk of -dienst te identificeren en te onderzoeken op basis van artikel 43bis, §3, 7° van de wet van 21 maart 1991 inzake de hervorming van sommige economische overheidsbedrijven.

Beide bepalingen (in voorgaande alinea) moeten duidelijk worden onderscheiden van de bewaarplicht in het kader van Richtlijn 2006/24/EG die als doel heeft “het onderzoeken, opsporen en vervolgen van ernstige criminaliteit”. Het is dan ook onduidelijk waarom kwaadwillige oproepen naar nooddiensten en misbruik van elektronische communicatienetwerken en -diensten expliciet worden vermeld en opgenomen in het voorontwerp van wet ter omzetting van Richtlijn 2006/24/EG. Beide bepalingen beantwoorden immers niet aan de voorwaarden die het verdragsrechtelijk en grondwettelijk beschermde recht op privacy, alsook de vaste rechtspraak van het Europees Hof voor de Rechten van de Mens, stellen aan een toelaatbare inbreuk op dit recht op privacy. Een inbreuk op dit recht kan enkel gerechtvaardigd zijn wanneer deze beperking bij wet is voorzien en dit ‘in een democratische samenleving noodzakelijk’ is ter vrijwaring van de nationale veiligheid, de openbare veiligheid of het economische welzijn van de staat. Dit criterium van de noodzakelijkheid wordt in de rechtspraak van het Europees Hof te Straatsburg verder ingevuld aan de hand van de beginselen van proportionaliteit, finaliteit en subsidiariteit⁵.

⁴ Alexander Nuno Alvaro, *Verslag van het Europees Parlement (Commissie burgerlijke vrijheden, justitie en binnenlandse zaken) over het voorstel voor een richtlijn van het Europees Parlement en de Raad 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 (A6-0365/2005)*, 28/11/2005, p. 10 (Amendement 14).

⁵ Europees Hof voor de Rechten van de Mens, zaak van Silver en anderen versus het Verenigd Koninkrijk, 25 maart 1983, lijn 97, p. 33, <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=Silver%20%20et%20%20al.&sessionid=14625595&skin=hudoc-en>.

Aanbeveling:

Aangezien het verzamelen en raadplegen van de verkeers- en locatiegegevens een enorme privacyschending met zich meebrengt, moet het gebruik van deze gegevens beperkt worden tot het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals vastgelegd door Richtlijn 2006/24/EG. Deze Richtlijn stipuleert bovendien dat deze “ernstige vormen van criminaliteit” moeten worden gedefinieerd in nationale wetgeving. De Liga voor Mensenrechten vraagt dan ook om een limitatieve lijst van “ernstige vormen van criminaliteit” waarop de bewaarplicht, en dus het voorontwerp van wet, van toepassing zal zijn op te nemen in dit voorontwerp van wet. Deze limitatieve lijst van ernstige criminaliteit moet rekening houden met de gestelde voorwaarden bij het verdragsrechtelijk en grondwettelijk beschermde recht op privacy (zie boven).

<i>6. Voorwaarden voor het raadplegen van de bewaarde gegevens</i>
--

Artikelen:

Voorontwerp van Wet, Art. 2, §1, 4e lid.

Knelpunten:

Artikel 2, §1, lid 4, van het voorontwerp van wet stipuleert dat “*de operatoren [...] ervoor [zorgen] dat de gegevens opgenomen in het eerste lid [i.e. de verkeers- en locatiegegevens, alsook de gegevens voor identificatie van de eindgebruikers] onbeperkt toegankelijk zijn vanuit België*”. Deze bepaling is veel te algemeen en te vaag opdat burgers en operatoren zouden weten waaraan zij moeten voldoen en creëert dus een gebrek aan rechtszekerheid⁶.

De bewaarplicht vormt een ernstige bedreiging voor het recht op privacy. Het is dan ook ondenkbaar dat men deze gegevens zonder verdere voorwaarden ter beschikking zou stellen van politiediensten en gerechtelijke autoriteiten. Het bewaren van verkeers- en locatiegegevens is immers vaak even ingrijpend als het afluisteren van de inhoud van telecommunicatie. Via de stelselmatige kennisname van verkeers- en locatiegegevens kan men immers een min of meer volledig beeld krijgen van bepaalde aspecten van iemands leven. Zo bieden verkeers- en locatiegegevens niet alleen een gedetailleerd beeld van de gevoerde communicatie, maar ook van de sociale omgeving (met wie wordt er gebeld, geSMSt, ge-e-maild, ...) en de bewegingen (vanwaar wordt er gebeld, geSMSt, ge-e-maild, ...) van individuen. In die zin verkrijgt men min of meer dezelfde informatie als bij een observatie van individuen. Daarnaast kunnen dergelijke gegevens ook automatisch geanalyseerd worden, in samenhang met andere gegevens, op zoek naar specifieke patronen volgens welbepaalde criteria (dit noemt men ‘datamining’). Het bewaren van verkeers- en locatiegegevens opent dus perspectieven die niet mogelijk zijn bij het verwerken van de inhoud van communicatie. Het kan dan ook niet zijn dat het bewaren van verkeers- en locatiegegevens als minder ingrijpend wordt beschouwd dan het afluisteren van de inhoud van communicatie en bijgevolg een lager beschermingsniveau krijgt toebedeeld.

Daarnaast vormt de bewaarplicht ook een ernstige bedreiging voor het functioneren van beroepen die vertrouwelijkheid vereisen zoals in het geval van journalisten, artsen, advocaten en geestelijken. Informanten, patiënten, cliënten en andere gegevensleveranciers die normaal op anonimiteit kunnen rekenen op basis van het bronnen- of beroepsgeheim, zouden met de introductie van de bewaarplicht kunnen aarzelen om nog langer gebruik te

⁶ Europees Hof voor de Rechten van de Mens, zaak van Silver en anderen versus het Verenigd Koninkrijk, 25 maart 1983, lijn 87 e.v., <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=Silver&sessionid=15329098&skin=hudoc-en>.

maken van telecommunicatiemiddelen aangezien op die manier een relatie gebaseerd op vertrouwen onmogelijk wordt gemaakt. Een enquête die werd uitgevoerd onder de bevolking in Duitsland in mei 2008 door het onderzoeksbureau Forsa heeft de nefaste gevolgen van de bewaarplicht sinds de introductie ervan in Duitsland reeds aangetoond. 52% van de ondervraagden gaf hierbij aan niet langer telefoon of e-mail te gebruiken bij vertrouwelijke contacten en 11% van de ondervraagden zou zelfs hoegenaamd geen telecommunicatie meer gebruiken⁷.

Het respecteren van het beroeps- en bronnengeheim is nochtans een fundamenteel en grondwettelijk beschermd recht en bijgevolg van uiterst belang in het vrijwaren van onze democratische samenleving en onze rechtstaat. Een inbreuk op dit fundamentele recht is dan ook maar toelaatbaar in zeer uitzonderlijke omstandigheden, wanneer noodzaak en hoogdringendheid kan worden aangetoond en op voorwaarde dat er strenge procedurele waarborgen in acht worden genomen. Zo heeft het Belgische Grondwettelijk Hof in een recent vonnis van 23 januari 2008 herbevestigd dat *“het beroepsgeheim van advocaten een algemeen rechtsbeginsel is dat noodzakelijk is om de naleving van fundamentele rechten te verzekeren”*. In het bijzonder verduidelijkt het Grondwettelijk Hof dat de strijd tegen witwaspraktijken en het financieren van terrorisme onder geen enkel beding een onvoorwaardelijke en onbepaalde inbreuk op het beroepsgeheim kan rechtvaardigen⁸. De Liga voor Mensenrechten is ervan overtuigd dat deze waarschuwing van het Grondwettelijk Hof geïnterpreteerd kan worden als een algemene afwijzing van disproportionele inbreuken op het beroepsgeheim en het bronnengeheim.

Aanbeveling:

De Liga voor Mensenrechten vindt het een onaanvaardbare schending van het recht op privacy om de verkeers- en locatiegegevens op een onbepaalde wijze toegankelijk te stellen. De Liga vraagt bijgevolg dat het voorontwerp van wet algemene, maar strenge regels opstelt inzake de voorwaarden waaronder de te bewaren gegevens geraadpleegd mogen worden, alsook wie beschouwd moet worden als een bevoegde autoriteit. Op basis van de memorie van toelichting (p. 1, 6^e alinea) neemt de Liga aan dat veiligheids- en inlichtingendiensten onder geen enkele voorwaarden toegang krijgen tot de te bewaren gegevens. Dit moet ook expliciet opgenomen worden in het voorontwerp van wet.

In lijn met de aanbevelingen van de CCBE (*the Council of Bars and Law Societies of Europe*) vraagt de Liga voor Mensenrechten onder meer dat het voorontwerp van wet duidelijk vastlegt dat toegang tot de te bewaren gegevens door de bevoegde autoriteiten enkel mogelijk is na een expliciete en voorafgaande toestemming van een onafhankelijke rechter⁹. Daarnaast vraagt de Liga voor Mensenrechten ook dat elke toegang tot en raadpleging van de database met de te bewaren gegevens wordt geregistreerd en dat deze geregistreerde gegevens worden overgemaakt aan de toezichthoudende instantie(s), zoals bepaald in artikel 9 van Richtlijn 2006/24/EG. Bovendien moet het voorontwerp van wet beantwoorden aan artikel 6 van Richtlijn 95/46/EG en artikel 6, §1, van Richtlijn 2002/58/EG. Dit betekent dat eens de bevoegde autoriteiten de te bewaren gegevens hebben geraadpleegd, deze gegevens enkel verder gebruikt en opgeslagen mogen worden voor zover en zolang dit noodzakelijk is voor het doeleinde waarvoor zij origineel werden opgevraagd. Ten slotte vraagt de Liga voor

⁷ <http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/>; <http://www.vorratsdatenspeicherung.de/content/view/236/1/lang/en/>.

⁸ Grondwettelijk Hof Nr: 10/2008, 23 januari 2008, www.const-court.be.

⁹ X, ‘CCBE Recommendations for the implementation of the data retention Directive’, 15/09/2006, p. 3: http://www.ccbe.org/fileadmin/user_upload/NTCdocument/en_it_law_ccbe_recom1_1182246703.pdf.

Mensenrechten de nodige waarborgen om het beroeps- en bronnengeheim te vrijwaren bij het bewaren en raadplegen van verkeers- en locatiegegevens¹⁰.

7. Toezichthoudende instantie

Artikelen:

Memorie van Toelichting, p. 2, 3^e alinea.

Knelpunten:

Enkel in de memorie van toelichting wordt er impliciet verwezen naar het BIPT als (min of meer onafhankelijke) toezichthoudende instantie door de verwijzing naar de bevoegdheid van het BIPT om toe te zien op de naleving van de wet van 13 juni 2005 op de elektronische communicatie en desgevallend krachtens art. 21 van die wet een administratieve boete op te leggen. Noch in de memorie van toelichting, noch in het voorontwerp van wet wordt er verwezen naar de bevoegdheid terzake van de Commissie ter bescherming van de persoonlijke levenssfeer als toezichthoudende instantie. Dit zou echter een verantwoorde keuze zijn gezien haar reeds bestaande bevoegdheden onder de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, en bijgevolg haar expertise terzake. Ten slotte zijn er ook geen bepalingen in het voorontwerp van wet die verwijzen naar het toezicht op het correct en legaal gebruik van de te bewaren gegevens door de bevoegde autoriteiten.

Aanbeveling:

De Liga voor Mensenrechten wil duidelijke bepalingen in het voorontwerp van wet met betrekking tot wie zal optreden als onafhankelijke, toezichthoudende instantie(s) én wat hun concrete bevoegdheden terzake zullen zijn. Zoals hierboven reeds gesteld, vraagt de Liga dat elke toegang tot en raadpleging van de database met de te bewaren gegevens wordt geregistreerd en dat deze geregistreeerde gegevens worden overgemaakt aan de toezichthoudende instantie(s) ter controle. Dit is het absolute minimum om het recht op bescherming van de persoonlijke levenssfeer te vrijwaren. Maximale waarborgen moeten worden ingebouwd om te verzekeren dat de toezichthoudende instantie(s) werkelijk autonoom kan (kunnen) optreden.

8. Sancties

Artikelen:

Memorie van Toelichting, p. 2, 2^e en 3^e alinea.

Knelpunten:

Enkel in de memorie van toelichting bij het voorontwerp van wet wordt er impliciet verwezen naar de heersende strafrechtelijke en administratieve sancties bij niet naleving van de geldende regels door de aanbieders van elektronische communicatienetwerken en -diensten.

- Een strafrechtelijke sanctie is voorzien d.m.v. artikel 39 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Dit artikel kan een boete opleggen voor de verantwoordelijke voor verwerking (of de aangestelde of gevolmachtigde) die artikel 4 van de

¹⁰ Teneinde het beroeps- en bronnengeheim te vrijwaren mag er zeker geen afbreuk gedaan worden aan de Wet van 7 april 2005 tot bescherming van de journalistieke bronnen (meer specifiek art. 3, 4 en 5), aan het Koninklijk Besluit van 7 november 1967 betreffende de uitoefening van de gezondheidszorgberoepen, aan artikelen 55 tot en met 70 van de Code van geneeskundige plichtenleer, aan artikel 2.3 van de Gedragscode voor advocaten van de Europese Gemeenschap en ten slotte aan artikel 458 van het Strafwetboek.

voornoemde wet overtreedt, met name betreffende de kwaliteit van de gegevens (niet buitensporig veel gegevens, geen oneindige bewaringstermijn, geen oneigenlijk gebruik ten opzichte van de bepaalde doeleinden, enz.).

- Een administratieve sanctie is voorzien d.m.v. artikel 21 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Artikel 14, 3° van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector maakt het BIPT bevoegd voor de controle op de naleving van de wet van 13 juni 2005 betreffende de elektronische communicatie en de bijbehorende uitvoeringsbesluiten, en krachtens artikel 21 van diezelfde wet mag het BIPT een administratieve boete opleggen aan operatoren.

Aanbeveling:

De Liga voor Mensenrechten vraagt dat er in het voorontwerp van wet expliciet bepalingen worden opgenomen met betrekking tot de geldende strafrechtelijke en administratieve sancties. Deze sancties moeten van toepassing zijn bij onrechtmatige handelingen (verzamelen, raadplegen, verspreiden, ...) van zowel de aanbieders van openbare elektronische communicatienetwerken en -diensten die de gegevens moeten bewaren als de (al of niet bevoegde) autoriteiten die gebruik maken van de te bewaren gegevens. Ten slotte moeten deze sancties ook effectief, evenredig en ontradend zijn conform art. 13 van Richtlijn 2006/24/EG.