

**PRINCIPIEEL STANDPUNT VAN DE LIGA VOOR MENSENRECHTEN INZAKE EEN ALGEMENE
BEWAARPLICHT.**

HOORZITTING KAMERCOMMISSIE JUSTITIE 02/01/2010

1. Inleiding

De algemene bewaarplicht van telecommunicatiegegevens vloeit voort uit een Europese richtlijn die de Belgische regering moest omzetten naar nationaal recht tegen 15 maart 2009. Het gaat om 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*”, alias de ‘databewaringsrichtlijn’¹.

Deze richtlijn werd in het leven geroepen om telecomoperatoren en internetproviders te verplichten bepaalde gegevens die door hen gegenereerd of verwerkt worden te bewaren. Op deze manier willen de Europese Commissie en de Raad van de Europese Unie garanderen dat dergelijke gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ‘ernstige criminaliteit’, zonder evenwel de draagwijdte van dit begrip nauwkeurig te omschrijven.

Het gaat meer bepaald om alle gegevens betreffende de betrokken personen, de datum, het tijdstip, de duur en de omvang van een telefoongesprek, een SMS-, of e-mailbericht, alsook de gebruikte technologie en de locatie ervan. Men wil met andere woorden weten wie met wie, wanneer, voor hoe lang, en van waar gebeld, geSMSt, of ge-e-mailed heeft. Daarnaast moeten ook de gegevens inzake de toegang tot het internet worden bewaard; bijvoorbeeld wanneer en van op welke computer (en dus vanuit welke plaats) u in- of uitlogde op het internet. Een belangrijke beperking is dat gegevens waaruit de inhoud van de communicatie kan worden achterhaald niet mogen worden bewaard. Niettemin is het best mogelijk om via de stelselmatige kennisname van verkeers- en locatiegegevens een min of meer volledig beeld te krijgen van bepaalde aspecten van iemands leven. Bijgevolg verdienen deze gegevens een afdoende beschermingsniveau.

Een algemene bewaarplicht van telecommunicatiegegevens zal fundamentele rechten van burgers (zoals het recht op privacy en het vermoeden van onschuld) op een significante wijze inperken. Bovendien stellen experts de meerwaarde van deze maatregel in vraag aangezien de bewaarplicht in de praktijk niet alleen ongeschikt blijkt, maar ook voor alle betrokken partijen een onredelijke financiële en praktische belasting betekent.

De Liga voor Mensenrechten doet dan ook een oproep aan de Belgische wetgever om de databewaringsrichtlijn niet om te zetten naar Belgisch recht en om de regering opdracht te geven initiatieven te nemen om deze Europese richtlijn op Europees niveau ongedaan te maken of minstens grondig bij te sturen. We staan met deze eis niet alleen, ook in andere Europese lidstaten is dit een expliciete

¹ Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG [Officieel Publicatieblad L 105 van 13/04/2006 blz. 54-63].

vraag². In totaal subsidiaire orde wenst de Liga nog te beklemtonen dat ook de reglementerende vorm waarin de bewaarplicht zou worden ingevoerd voor grondige kritiek vatbaar is. U vindt hierover meer informatie in de artikelgewijze bespreking van het voorontwerp van wet en ontwerp van KB van 27 augustus 2009.

2. Een algemene bewaarplicht schendt het recht op privacy.

De Liga voor Mensenrechten is geen voorstander van een algemene bewaarplicht -in eender welke vorm- aangezien het een serieuze schending inhoudt van het recht op privacy en vertrekt van de idee dat elke burger potentieel gevaarlijk is. Ieder van ons wordt op die manier immers als een potentiële verdachte aan het preventieve toezicht van de overheid onderworpen. De Liga begrijpt dat het opvragen van verkeers- en locatiegegevens in bepaalde gevallen zinvol en gerechtvaardigd kan zijn, maar is niet overtuigd van de noodzaak van een algemene bewaarplicht en van het feit dat minder ingrijpende maatregelen, zoals ‘*data preservation*’ niet langer volstaan.

De Liga pleit dan ook om het huidige systeem van ‘*data preservation*’ te bewaren zoals het werd gedefinieerd op een G8-top van Ministers van Justitie en Binnenlandse Zaken in Moskou in oktober 1999. De definitie luidt als volgt: “*the term “Preservation” shall mean that (a) upon lawful request by a competent authority, (b) based on the facts of a specific case, (c) specific historical data can be preserved to prevent its deletion, (d) pending issuance of a lawful demand from a competent authority to disclose the data. “Preservation” does not include prospective collection of data and does not obligate a service provider to generate data not already in existence*”³. M.a.w., naar aanleiding van een rechtmatig verzoek door een bevoegde autoriteit en gebaseerd op de feiten van een specifieke zaak kunnen welbepaalde historische gegevens worden bewaard om te vermijden dat zij vernietigd zouden worden in afwachting van een rechtmatig verzoek door een bevoegde autoriteit, zijnde een machtiging van een onafhankelijke rechter, om deze gegevens kenbaar te maken. ‘*Data preservation*’ betekent dus in essentie een bevel tot het “*niet-vernietigen*” van gegevens die reeds bestaan; gegevens die m.a.w. reeds worden bewaard door telecomoperatoren en internetproviders in de context van hun eigen dienstverlening.

De hele argumentatie van de regering in de Memorie van Toelichting bij het voorontwerp van wet en ontwerp van KB van 27 augustus 2009 is dan ook flagrant onjuist, en op zijn minst dubbelzinnig te noemen, wanneer men stelt dat de algemene bewaarplicht, zoals die voortvloeit uit de Europese databewaringsrichtlijn, “*niets nieuws*” brengt. Enerzijds argumenteert men immers dat er niets verandert met de databewaringsrichtlijn (en dat er bijgevolg geen (bijkomende) schending is van fundamentele rechten, zoals het recht op privacy) en anderzijds beklemtoont men nadrukkelijk de noodzaak om deze richtlijn dringend om te zetten. Aangezien men bij het omzetten van de databewaringsrichtlijn afstapt van het ‘*data preservation*’ principe mag het wel duidelijk wezen dat dit een serieuze omslag betekent.

² Zie infra punt 5.

³ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20DataPreservationChecklists_en.pdf.

Het is zo dat telecomoperatoren en internetproviders op basis van de wet op de elektronische communicatie van 2005 reeds bepaalde gegevens bewaren in het kader van hun dienstverlening, maar dit gaat om veel minder gegevens en om een veel kortere bewaarperiode (bijvoorbeeld tot het einde van de periode waarop klanten hun factuur bij hun operator of provider kunnen betwisten) dan het huidige voorontwerp van wet en ontwerp van Koninklijk Besluit vereisen. Deze bewaarde gegevens mogen volgens de wet van 2005 enkel worden geraadpleegd door de klant zelf of door de betrokken provider of operator indien dit noodzakelijk is voor hun dienstverlening. Het bewuste artikel 126 uit de wet op de elektronische communicatie van 2005 is immers nooit in werking getreden.

Aan deze wet op de elektronische communicatie is wel een Koninklijk Besluit verbonden dat het kader vastlegt waarbinnen politie of justitie dergelijke gegevens mogen opvragen en de wijze waarop operatoren en providers verplicht zijn hun medewerking hieraan te verlenen. Het gaat meer bepaald om specifieke procedures die zijn vastgelegd in de artikelen 46bis en 88bis van het Wetboek van Strafvordering. Deze procedures passen, ondanks hun brede toepassingsgrond, wel in het principe van '*data preservation*'. De regering bevestigt dat deze procedures zouden blijven gelden bij de algemene bewaarplicht en argumenteert op deze manier dat er derhalve geen bijkomend gevaar is voor het recht op privacy of het beroeps- en bronnengeheim. Deze redenering klopt echter niet om 3 redenen.

Vooreerst worden operatoren en providers op basis van het voorontwerp van wet en ontwerp van Koninklijk Besluit van 27 augustus 2009 verplicht om veel meer gegevens te bewaren dan zij nu reeds doen. Meer zelfs, internetproviders klagen aan dat zij technisch niet in staat zullen zijn om bepaalde gegevens uit het ontwerp van Koninklijk Besluit te bewaren. Het gaat dan om gegevens die door operatoren en providers niet geregistreerd worden bij de dienstverlening, maar die justitie of politie zouden kunnen gebruiken vanuit strafrechtelijk oogpunt.

Ten tweede klopt ook de redenering niet dat de schending van de privacy niet groter wordt met de 'loutere' aanpassing van de huidige bewaarplicht op basis van de elektronische communicatiewet van 2005. Ook al bestond er in 2005 een politiek akkoord over de wijze waarop politie en justitie in welbepaalde gevallen gegevens kon opvragen van telecomoperatoren en internetproviders wil dit niet zeggen dat dit automatisch ook opgaat voor onze huidige samenleving waarbij onze wijze van communicatie sterk veranderd is en het gebruik van telecommunicatie steeds meer centraal is komen te staan. Het gevaar op een schending van de privacy evolueert uiteraard mee en het is dus zeker niet zo dat er met een algemene bewaarplicht niets zou veranderen. De vraag is wat de gevolgen zullen zijn voor een samenleving die niet meer buiten telecommunicatie kan, zelfs voor discrete en vertrouwelijke zaken, wanneer dit voortaan allemaal in kaart wordt gebracht. Kan een werkelijk democratische samenleving zoals wij die momenteel kennen overleven wanneer het telecommunicatiegeheim op dergelijke schaal wordt prijsgegeven? Wat met het bronnengeheim van journalisten? Wat met het beroepsgeheim van advocaten, artsen en geestelijken? Wat met activiteiten van zakenlui en politici die discretie vereisen?

Ten derde, zelfs wanneer de procedures waarbij politie en justitie gegevens kunnen opvragen (cf. art 46bis en 88bis Sv.) hetzelfde blijven, gaat het Belgische project verder dan wat de Europese richtlijn beoogde. Het Europese Parlement heeft bij de

stemming van deze richtlijn namelijk benadrukt dat deze gegevens enkel door politie en justitie gebruikt mochten worden in de strijd tegen terrorisme en ernstige criminaliteit. Hoewel het te betreuren valt dat de Europese richtlijn voor een definitie van 'ernstige criminaliteit' verwijst naar de nationale wetgeving mogen we toch oordelen dat de artikelen 46bis en 88bis van het Belgische Wetboek van Strafvordering de drempel een flink stuk lager leggen: gegevens mogen hierbij worden opgevraagd voor praktisch alle misdrijven (meer bepaald voor wanbedrijven en misdaden in tegenstelling tot de door de richtlijn beoogde 'ernstige criminaliteit' zoals terrorisme en georganiseerde misdaad) en zelfs de beteugeling van kwaadwillige oproepen naar de nooddiensten, of het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk of -dienst komen in aanmerking! Ook is het momenteel onduidelijk in welke mate veiligheids- en inlichtingendiensten toegang zullen krijgen tot deze gegevens in het kader van de 'specifieke procedures' van de nieuwe BIM-wet. Het voorontwerp van wet en ontwerp van KB van 27 augustus 2009 ter omzetting van de databewaringsrichtlijn zeggen hier alleszins niets over.

De Liga voor Mensenrechten wil er dan ook op aandringen dat wanneer het parlement binnenkort debatteert over het feit of een algemene bewaarplicht nuttig dan wel noodzakelijk is, zij ook nagaat of de bestaande bewaarplicht op basis van de wet op de elektronische communicatie van 2005 nog wel aanvaardbaar is in een samenleving waarin telecommunicatie zo centraal is komen te staan en waarbij de kans op een eventuele schending van de privacy disproportioneel is toegenomen.

De algemene bewaarplicht wordt verder ook vaak gelegitimeerd door het feit dat opslag en gebruik ervan apart wordt geregeld; alsof met andere woorden de loutere opslag van dergelijke gegevens geen schending inhoudt van het recht op privacy en dat die schending pas optreedt met het gebruik ervan. Uiteraard is de wijze waarop men later gebruik kan maken van deze gegevens cruciaal, vandaar dat de Liga het ook onaanvaardbaar vindt dat dit niet limitatief in de wet zelf wordt ingeschreven, maar ook de loutere registratie en opslag van deze gegevens houdt reeds een inbreuk in op het recht op privacy. Zo oordeelde het Europese Hof voor de rechten van de Mens recent nog in de zaak Marper t. het Verenigd Koninkrijk dat de loutere registratie en opslag van persoonsgegevens door publieke autoriteiten een inbreuk vormen op het recht op privacy, ongeacht hoe deze gegevens verder worden gebruikt⁴. Het feit dat dergelijke gegevens via een omweg door private telecomoperatoren en internetproviders worden verzameld, verandert hieraan niets aangezien zij dit in opdracht van de overheid doen.

De reden hiervoor is duidelijk, aangezien de loutere opslag van gegevens een risico vormt op eventueel misbruik later. Dit kan gaan van oneigenlijk gebruik van persoonsgegevens door politie en justitie (hierbij kunnen we verwijzen naar de recente zaak van Yasmine⁵ en natuurlijk de herhaalde kritieken in de jaarrapporten

⁴ 4 DECEMBER 2008 - Europees Hof voor de Rechten van de Mens, S. en Marper t. het Verenigd Koninkrijk (appl. no. 30562/04 and 30566/04): http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/CASE_OF_S._AND_MARPER_v._THE_UNITED_KINGDOM.pdf.

⁵ <http://www.zdnet.be/news/107840/politiemensen-neuzen-massaal-in-gegevens-yasmine/> en <http://www.standaard.be/Artikel/Detail.aspx?artikelId=KR2FDEOQ&subsection=3>.

van het Comité P⁶) tot misbruik door derden (bijvoorbeeld de hacker Vendetta die persoonsgegevens van klanten van Belgacom openbaar maakte⁷). Niet alleen is het beangstigend om vast te stellen wat er nu reeds misloopt, nog erger zou het zijn met een algemene bewaarplicht die van elke burger vastlegt met wie hij of zij in interactie treedt. Internetproviders geven ter zake ook aan dat zij vrezen niet in staat te zullen zijn om de integriteit en de veiligheid van al deze gegevens te garanderen tegen crimineel en commercieel misbruik⁸!

Dat we dit arrest in de zaak Marper t. het Verenigd Koninkrijk mogen extrapoleren naar de context van verkeers- en locatiegegevens, ondanks de mening van de regering dat dergelijke gegevens weinig privacyschendend zijn, lijkt gerechtvaardigd gezien de eerdere arresten⁹ van ditzelfde Europese Hof waarin zij herhaaldelijk stelt dat het gebruik van verkeersgegevens een inbreuk kan opleveren van het recht op privacy, zoals gewaarborgd in artikel 8 EVRM, en dat die verkeersgegevens een integraal onderdeel uitmaken van de communicatie. We kunnen er van uit gaan dat deze inbreuk alleen maar groter wordt door de evolutie in moderne communicatietechnologieën waarbij het onderscheid tussen verkeersgegevens enerzijds en het eigenlijke onderscheppen van de inhoud van de communicatie anderzijds alleen maar kleiner wordt (zie punt 4).

Dat de algemene bewaarplicht een inbreuk vormt op het recht op privacy staat dus onomwonden vast. Het recht op privacy is echter niet absoluut en artikel 8 EVRM voorziet in enkele uitzonderingen indien deze ‘absoluut noodzakelijk’ zijn in een democratische samenleving en minder ingrijpende maatregelen niet langer volstaan. De vraag is dan ook niet zozeer of de Liga voor Mensenrechten het gevaar reëel acht dat we door het steeds meer uithollen van het recht op privacy binnen afzienbare tijd verglijden naar een autoritaire samenleving, maar of de overheid kan bewijzen dat een algemene bewaarplicht ‘absoluut noodzakelijk’ en ‘proportioneel’ is in onze huidige Belgische samenleving en dat minder ingrijpende maatregelen niet langer volstaan. Dit laatste is echter noch op Europees noch op Belgisch niveau voldoende aangetoond (zie punt 3). De Europese richtlijn werd destijds immers bijzonder snel aangenomen zonder de nodige reflectie en overleg en wordt dan ook sterk bekritiseerd doorheen heel de Europese Unie (zie punt 6) en niet alleen in België. Wanneer de Belgische regering bovendien wenst om de lijst van de te bewaren gegevens uit te breiden met informatie over bankgegevens, moet ook hier de ‘absolute noodzaak’ ervan worden

⁶ “Wij blijven vaststellen dat het gebruik van politionele gegevens door sommige politiemensen problematisch blijft. Wij blijven ervoor pleiten dat men strikt optreedt (op straf- en/of tuchtrechtelijk vlak) tegen het opvragen van gegevens zonder dat men hiervoor een concreet belang heeft [...] en dus buiten het kader van hun opdrachten van gerechtelijke en bestuurlijke politie of andere administratieve taken.” Comité P, jaarverslagen 2005, 2006, 2007 & 2008 onder ‘informatiebeheer’ (<http://www.comitep.be/nl/nl.html>)

⁷ <http://bewaarjeprivacy.be/nl/content/persberichten>.

⁸ EUROISPA and US ISPA, ‘Position paper on the impact of data retention laws on the fight against cybercrime’, 30/09/2002, p. 2.

⁹ Zie hiervoor onder meer: 6 SEPTEMBER 1978 - Europees Hof voor de Rechten van de Mens, Klass e.a. t. Duitsland, §49-50 (appl. no. 5029/71); 2 AUGUSTUS 1984 - Europees Hof voor de Rechten van de Mens, Malone t. het Verenigd Koninkrijk, §84 (appl. no. 8691/79); 2 AUGUSTUS 1984 - Europees Hof voor de Rechten van de Mens, Malone t. het Verenigd Koninkrijk, §84 (appl. no. 8691/79); 16 FEBRUARI 2000 - Europees Hof voor de Rechten van de Mens, Amann t. Zwitserland (appl. no. 27798/95); 25 SEPTEMBER 2001 - Europees Hof voor de Rechten van de Mens, P.G. en J.H. t. het Verenigd Koninkrijk, §42 (appl. no. 44787/98); 4 DECEMBER 2008 - Europees Hof voor de Rechten van de Mens, S. en Marper t. het Verenigd Koninkrijk (appl. no. 30562/04 and 30566/04).

aangetoond op basis van concreet cijfermateriaal en mag men ‘noodzakelijkheid’ niet verwarren met wat ‘bruikbaar’ of ‘wenselijk’ zou kunnen zijn voor politie en justitie. Het naar voren geschoven cijfermateriaal en de willekeurige voorbeelden die worden aangehaald in de bijlage van de Memorie van Toelichting bij het voorontwerp van wet van 27 augustus 2009 voldoen dan ook absoluut niet!

Kortom, het preventief bewaren van éénieders verkeers- en locatiegegevens is een nooit eerder geziene inbreuk op het recht op privacy. Vele mensen zijn misschien bereid dit recht op privacy in te ruilen voor andere behoeften, zoals de behoefte aan een veilige samenleving, omdat zij niet meteen zien wat dit recht op privacy hen biedt of wat dit recht precies moet veilig stellen. Het recht op privacy is waarschijnlijk één van de meest abstracte fundamentele mensenrechten, maar er schuilt een groot gevaar in het ondergeschikt stellen van dit recht aan andere verzuchtingen. Het recht op privacy moet namelijk de realisatie van andere fundamentele mensenrechten mogelijk maken en is met andere woorden een noodzakelijke voorwaarde voor het vrijwaren van een democratische rechtstaat. Zonder de garantie op privacy zullen mensen bijvoorbeeld minder snel geneigd zijn om kritische stellingen te verdedigen en te verspreiden en tegen de dominante tijdsgeest in te gaan. Zodra de dominante ideologie in een samenleving niet langer in vraag wordt gesteld, verglijdt men langzaam naar een autoritaire staatsvorm. Dat niet alleen de Liga voor Mensenrechten het recht op privacy als zeer belangrijk beschouwt, bewijst de verdragsrechtelijke en grondwettelijke verankering van het recht op privacy. Niet toevallig ook is de evolutie van het (steeds meer) erkennen van een recht op privacy gelijklopend met bepaalde breukmomenten in de geschiedenis, zoals het ontstaan van het EVRM na het fascisme van WO II.

Het preventief registreren van éénieders verkeers- en locatiegegevens leidt er bovendien toe dat er definitief afstand wordt gedaan van een belangrijk rechtsprincipe dat mensen als onschuldig behandelt tot het tegendeel is bewezen. Hierdoor komen we terecht in een samenleving die haar eigen burgers wantrouwt in plaats van ze te beschermen. Het beweerde bestaan van een terreurdreiging is geen vrijgeleide om de fundamentele beginselen van de rechtstaat buitenspel te zetten. Communicatiegegevens zijn immers veel meer dan een eenvoudige weergave van wie met wie wanneer belt. Verkeersgegevens worden nu gebruikt om associaties tussen mensen in kaart te brengen en, belangrijker nog, om activiteiten en voornemens van mensen af te leiden. Wanneer men dit in de bredere context plaatst van de stijgende tendens om enorme nationale databanken op te richten met interoperabiliteit op Europees niveau en een uitgebreide toegang voor politionele doeleinden, wordt een algemene bewaarplicht van telecommunicatiegegevens des te beangstigender. Gegevens die oorspronkelijk enkel verzameld werden voor de vereisten van een bepaalde dienstverlening worden dan ingezet voor het toezicht op burgers en sociale controle, en in het ergste geval voor inlichtingendoeleinden. Deze maatregel is dan ook een zoveelste uiting van een ‘cultuur van controle’ die de laatste decennia in onze West-Europese samenleving steeds meer genormaliseerd wordt en die in algemene zin meer gericht is op uitsluiting dan op solidariteit, meer op sociale controle dan op sociale voorzieningen, en meer op particuliere vrijheid van de markt dan op publieke vrijheden van universeel burgerschap. Dit is uiteraard onaanvaardbaar in een democratische samenleving die naam waardig!

Het kabinet van Justitie rechtvaardigt een algemene bewaarplicht -ondanks het

erkennen van enkele fundamentele kritieken- ook steeds vanuit het dogma dat “*iets doen nog altijd beter is dan niets doen*”. Niet alleen is dit een slechte motivatie om wetgeving te introduceren, het is ook een gevaarlijke stelling die weinig kritiek toelaat. Men moet afstappen van de idee dat alles in onze samenleving beheersbaar en controleerbaar kan, en moet, zijn. Het verleden leert ons dat de neveneffecten van een doorgedreven sociale controle op burgers vaak nefaster zijn dan de betwistbare voordelen. Ondanks het ‘*war on terror*’ discours dat hard zijn best doet om ons te overtuigen van het feit dat de wereld (plots) een onveilige plek is geworden, is terreur helaas een fenomeen van alle tijden en daarom is het belangrijkste middel in de bestrijding ervan net het behoud van fundamentele mensenrechten! Dergelijke uitzonderingsmaatregelen verglijden in de praktijk immers al snel naar een breder en algemeen toepassingsgebied, want “*als je niet te verbergen hebt, heb je toch niets te vrezen?*” Men zou echter ook kunnen oordelen dat een ‘recht op veiligheid’ impliceert dat een zekere marge van vrijheid behouden blijft.

3. De noodzaak van een algemene bewaarplicht werd niet bewezen.

Autoriteiten ter bescherming van persoonsgegevens (*Data Protection Authorities* of DPA’s), internationale burgerrechtenorganisaties en internetproviders argumenteren dat de overheid onvoldoende heeft aangetoond dat een algemene bewaarplicht noodzakelijk is voor de veiligheid van de samenleving en dat bestaande, minder ingrijpende maatregelen (cf. het concept van ‘*data preservation*’) niet langer volstaan. Zo stelde de Artikel 29 Werkgroep¹⁰ in een aanbeveling van 1999 dat “*binnen de juridische context [van de Europese verdragsteksten en de communautaire wetgeving] de verkennende of algemene bewaking van telecommunicatieverkeer op grote schaal moet worden verboden. [...] De inachtneming van [...] [he]t specificiteitsbeginsel, een logisch gevolg van het verbod van elke verkennende of algemene bewaking, impliceert [...] met betrekking tot verkeersgegevens dat de overheid slechts van geval tot geval, en niet op algemene en proactieve wijze, toegang tot deze gegevens kan krijgen*”¹¹.

En in een advies van 2001, n.a.v. de terreuraanslagen in New York, beklemtoont de Artikel 29 Werkgroep nogmaals de behoefte aan een evenwichtige aanpak in de strijd tegen terrorisme. De Artikel 29 Werkgroep is 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. Er moet volgens hen gestreefd worden naar een evenwichtige aanpak om te voorkomen dat we het soort samenleving dat we net proberen te beschermen, niet gaan ondermijnen. “*De Groep onderstreept in het bijzonder de noodzaak om rekening te houden met het langetermijneffect van urgente beleidsmaatregelen die momenteel snel worden toegepast of gepland. Deze reflectie op lange termijn is des te*

¹⁰ De artikel 29-Werkgroep (zij ontleent haar naam aan artikel 29 van de privacy-richtlijn 95/46/EG) overkoepelt alle nationale toezichthoudende autoriteiten en heeft een onafhankelijk en raadgevend karakter. De belangrijkste taak van deze werkgroep is het bevorderen van een uniforme toepassing in alle lidstaten van de principes ter bescherming van de persoonsgegevens uit richtlijn 95/46/EG.

¹¹ HUSTINX, P., *Aanbeveling 2/99 betreffende de bescherming van de persoonlijke levenssfeer in het kader van de interceptie van telecommunicatieverkeer*, (Artikel 29 Werkgroep), 3 mei 1999, p. 5, 9: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp19nl.pdf.

noodzakelijker vanwege het feit dat terrorisme geen nieuw verschijnsel is en niet als een tijdelijk verschijnsel kan worden aangemerkt. [...] 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 [waaronder het recht op de bescherming van persoonsgegevens].”¹².

Bovenstaande argumenten vormen een extra waarschuwing bij het omzetten van de databewaringsrichtlijn. Dit betekent dat het des te belangrijker is dat de overheid op basis van concrete gegevens aantoont waarom zij oordeelt dat een algemene bewaarplicht ‘absoluut noodzakelijk’ is, ondanks de hoger vermelde tegenargumenten. Het tot nu toe naar voren geschoven cijfermateriaal en de willekeurige voorbeelden die worden aangehaald in de bijlage van de Memorie van Toelichting bij het voorontwerp van wet van 27 augustus 2009 voldoen hiertoe absoluut niet! Wat immers opvalt is dat de Memorie van Toelichting steeds verwijst naar wat nuttig is voor, of de behoeften zijn van, politie en justitie, maar nooit het bewijs levert m.b.t. waarom de algemene bewaarplicht ‘absoluut noodzakelijk is in onze democratische samenleving’. Wanneer men dit zou willen aantonen, moet men dit doen op basis van bijkomend cijfermateriaal.

Hierbij denken we in eerste instantie aan cijfermateriaal dat het voorkomen van ernstige criminaliteit, zoals terreur en georganiseerde misdaad, in België in kaart brengt en op basis waarvan een algemene bewaarplicht gelegitimeerd zou kunnen worden. Daarnaast is het ook essentieel om inzage te hebben in de statistische gegevens die duiding kunnen brengen inzake de mate waarin, alsook welke, telecommunicatiegegevens door politie en justitie worden opgevraagd bij het oplossen van deze ernstige strafzaken en het al of niet kunnen beantwoorden van deze vraag door de verschillende telecomoperatoren en internetproviders. Ten slotte is het ook heel belangrijk om zicht te krijgen op het aantal ernstige misdaaddossiers (dus weer uitgesplitst naar type misdrijf) die onopgelost bleven wegens een gebrek aan verkeers- en locatiegegevens en in welke mate een omzetting van de databewaringsrichtlijn dit zou kunnen voorkomen. Deze gegevens zijn des te belangrijker wanneer een overheid opteert voor een maximale omzetting van richtlijn 2006/24/EG, namelijk de keuze om meer gegevens, langer te bewaren dan hetgeen vereist wordt.

Een bewaartermijn van 12 maanden moet bijgevolg geconfronteerd worden met cijfers uit de praktijk. Wanneer politie en justitie gegevens opvragen gaat het volgens ISPA (de *Internet Service Providers Association*) in 69,3% van de gevallen om gegevens van 0-3 maanden oud, in 22,7% van de gevallen om gegevens van 3-6 maanden oud, in 4,1% van de gevallen om gegevens van 6-9 maanden oud, en in slechts 4% van de gevallen om gegevens van 9 maanden oud of ouder (gegevens afkomstig van Belgacom, Telenet & Mobistar eind 2008).

Ook de noodzaak om de lijst van de te bewaren gegevens uit te breiden, moet aangetoond worden en hierbij mag men ‘noodzakelijkheid’ niet verwarren met wat ‘bruikbaar’ of ‘wenselijk’ zou kunnen zijn. Beschikt het kabinet van Justitie over cijfermateriaal op basis waarvan een vergelijking gemaakt zou kunnen worden tussen het aantal ernstige strafzaken die niet konden worden opgelost omwille van het

¹² 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.

ontbreken van bepaalde telecommunicatiegegevens -die men nu wil bewaren door de introductie van een algemene bewaarplicht- ten opzichte van het aantal ernstige strafzaken die wel succesvol konden worden afgerond op basis van de beschikbare telecommunicatiegegevens?

Op basis van dergelijke concrete gegevens kan men pas werkelijk oordelen of een algemene bewaarplicht nuttig dan wel noodzakelijk is, en, indien een algemene bewaarplicht als noodzakelijk zou worden beschouwd, oordelen over de wijze waarop die bewaarplicht vorm moet worden gegeven. Op dit moment wordt men echter gedwongen om appels met peren te vergelijken op basis van de onvolledige en vaak anekdotische gegevens in de bijlage bij de Memorie van Toelichting bij het voorontwerp van wet van 27 augustus 2009. De Liga begrijpt dat dergelijk statistisch cijfermateriaal niet aanwezig is wegens een gebrekkige informatisering van justitie, maar dat kan in een democratische rechtstaat niet volstaan als argument om fundamentele burgerrechten in te perken op basis van het fingerspitzengefühl van politie en parket!

Bovendien mag men in deze belangrijke afweging het langetermijneffect van een algemene bewaarplicht nooit uit het oog verliezen. Om de proportionaliteit van een bepaalde maatregel te evalueren volstaat het immers niet om alleen een afweging te maken van de te verwachten voordelen, maar men moet tevens de mogelijke negatieve effecten, m.a.w. de nefaste gevolgen voor fundamentele burgerrechten, in rekening brengen. In dit kader is het opvallend vast te stellen dat tal van experts het nut van een algemene bewaarplicht als garantie tegen terreur of criminaliteit in twijfel trekken.

4. Een algemene bewaarplicht is inefficiënt.
--

In de strijd tegen ernstige criminaliteit en terreur kan het opvragen van bepaalde telecommunicatiegegevens in bepaalde gevallen zinvol en gerechtvaardigd zijn, maar verschillende experts zijn van oordeel dat de algemene bewaarplicht, zoals ze geïntroduceerd werd door richtlijn 2006/24/EG, hiertoe geen effectief instrument is.

- Vooreerst wil men zoveel gegevens bijhouden voor een dermate lange periode dat het zeer moeilijk zal zijn om de juiste informatie terug te vinden in de enorme databanken waar de gegevens in zullen worden opgeslagen. Het bewaren van zoveel gegevens brengt bovendien een enorm veiligheidsrisico met zich mee. Internetproviders vrezen dat zij niet in staat zullen zijn om de integriteit en de veiligheid van al deze gegevens te garanderen tegen crimineel en commercieel misbruik¹³.
- Vaak ook zal de verzamelde informatie niet of moeilijk kunnen worden teruggekoppeld naar de uiteindelijke gebruiker. De persoon die op een bepaald moment gebruik maakt van een telecommunicatiedienst is immers lang niet altijd de abonnee of de geregistreerde gebruiker. Voornamelijk op het vlak van moderne communicatiesystemen, zoals communicatie over het internet, doen zich problemen voor. Zo kan men aan de hand van verkeersgegevens achterhalen van welke webserver een machine iets opvraagt, maar niet of de

¹³ EUROISPA and US ISPA, Position paper on the impact of data retention laws on the fight against cybercrime, 30/09/2002, p. 2.

eindgebruiker het zelf onder ogen heeft gekregen, of welke webpagina op die server het betreft¹⁴.

- Verkeers- en locatiegegevens kunnen ook op eenvoudige wijze vervalst en gemanipuleerd worden. Internetproviders wijzen er op dat mensen met een basiskennis van de werking van het internet er gemakkelijk voor kunnen zorgen dat ze onopgemerkt blijven op basis van de verzamelde gegevens in het kader van de algemene bewaarplicht. Aangezien de Europese richtlijn bedoeld is om ernstige vormen van criminaliteit op te sporen en te vervolgen, en verondersteld kan worden dat net dergelijke daders er wel voor zullen zorgen dat ze onopgemerkt blijven, dringt de vraag zich op of de algemene bewaarplicht wel zinvol is.

Zo zal een terrorist geen GSM-abonnement nemen op zijn werkelijke naam, maar eerder gebruik maken van anonieme prepaid-kaarten of, nog erger, van gestolen GSM's. Evenmin zal een terrorist e-mails versturen vanuit een account met zijn werkelijke identiteit en persoonsgegevens, maar eerder vanuit een account dat hij heeft gecreëerd op basis van een valse naam en adres. Een valse identiteit die misschien ontnomen werd aan een onschuldige burger die hierdoor in de problemen kan komen. Met andere woorden, de echte criminelen hebben niets te vrezen van deze nieuwe maatregel aangezien er voldoende trucs bestaan om anoniem te blijven. Daartegenover, zullen onschuldige burgers eventueel in de problemen kunnen komen indien hun naam werd gebruikt bij een e-mailaccount dat het hunne niet is, indien hun GSM werd gestolen, indien hun draadloos netwerk niet of onvoldoende beveiligd was, etc...! In dergelijke gevallen zullen burgers geconfronteerd worden met een omkering van de bewijslast. Zij zullen immers de moeilijke taak toebedeeld krijgen om het aldus verkregen bewijsmateriaal te weerleggen want "technologie liegt toch niet"? Het wordt intussen wel duidelijk dat men niet lichtzinnig over de vraag kan heengaan of een algemene bewaarplicht wel zinvol -laat staan noodzakelijk- en proportioneel is.

'*Data preservation*', het bewaren van specifieke, historische gegevens naar aanleiding van concrete vermoedens en mits de toestemming van een onafhankelijke rechter, lijkt dan een meer geschikt instrument om hetzelfde doel te bereiken. Bovendien wordt bij '*data preservation*' het recht op privacy en het vermoeden van onschuld van iedere burger niet miskend¹⁵.

Ten slotte moeten we ook vaststellen dat de bestaande wetsontwerpen ter realisatie van een algemene bewaarplicht van verkeers- en locatiegegevens technisch ondoordacht zijn en in de praktijk vaak onuitvoerbaar blijken.

- Internetproviders handelen het verkeer van hun klanten via heel veel verschillende servers af waardoor de complete verkeers- en locatiegegevens van een klant alleen zouden kunnen worden bemachtigd door een volledige tap op elke klant te zetten, dus inclusief op de inhoud. Hieruit zou de internetprovider vervolgens de gevraagde verkeers- en locatiegegevens moeten distilleren. Niet alleen gaat dit in tegen het expliciete verbod van de richtlijn, maar zal dit in de praktijk ook aanzetten tot misbruik van deze gegevens.
- De verplichting om mislukte oproepen, en in het geval van e-mail ook spam-

¹⁴ "Verslag van een mondeling overleg", *Eerste Kamer der Staten-Generaal*, 6 september 2005, <http://europapoort.eerstekamer.nl/9345000/1/j9vvgv6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

¹⁵ "Common Position of Principle on the Matter of Data Retention", juni 2008, p. 17.

mail, te bewaren lijkt een ondoordachte keuze. Communicatie van spam versturende servers wordt vaak afgeblokt alvorens het zijn bestemming heeft bereikt. In bepaalde gevallen zijn zowel afzender en ontvanger nog onbekend op het moment van het afbreken van de communicatie. Indien ook bij spam-mail verkeers- en locatiegegevens bewaard moeten worden, betekent dit dat bepaalde anti-spam technieken niet langer gebruikt kunnen worden en dit heeft allerlei vervelende consequenties, zoals meer spam in de inbox, veel hogere kosten verbonden aan de bewaarplicht, etc.

- Er zijn vele voorbeelden op te sommen waarbij de toegang tot het internet niet kan worden opgespoord: publieke plaatsen die een anonieme toegang tot het internet bieden, Internetcafé's die de identiteit van de individuele gebruikers niet controleren, voorafbetaalde accounts uit het buitenland, de individuele toegang in een netwerk van draadloos internet en een gedeelde verbinding.

Daarnaast zijn de bestaande wetsontwerpen ter realisatie van een algemene bewaarplicht van verkeers- en locatiegegevens in de praktijk vaak onuitvoerbaar.

- Zo wordt er geen rekening gehouden met de immense datastroom die plaatsvindt bij moderne telecommunicatiesystemen, zeker op het vlak van internet. Experts zijn van oordeel dat het onmogelijk is om uit al deze gegevens de gevraagde verkeers- en locatiegegevens te filteren¹⁶.
 - De verkeers- en locatiegegevens bij 'Voice over IP' (VoIP), een vorm van telefonie over het internet, kunnen enkel worden geregistreerd en bewaard wanneer de VoIP-'vertaling' uitgaat van dezelfde internetprovider als degene die de internetverbinding levert. Zelfs indien de aanbieders van VoIP-diensten zelf ook verplicht worden identificatiegegevens bij te houden, zal dit enkel effectief zijn voor diensten waarbij de verbinding tot stand wordt gebracht via een centrale server.
 - Een service provider zal enkel over gegevens beschikken die gegenereerd worden naar aanleiding van het gebruik van zijn 'dienst' maar niet over gegevens die voortkomen uit het gebruik van andere 'diensten' en zo worden deze ook bewaard.
 - Op dit moment bestaat er geen algemeen kader om internetgegevens (cf. relationele databases met een datamining-technologie) te verwerken. Het grote probleem daarbij is het 'voor-verwerken' van de gegevens. Er moeten standaard procedures komen om gebruikersgegevens te koppelen aan administratieve gegevens, maar dat kan zeer complex zijn. Indien op voorhand niet algemeen wordt vastgelegd hoe gegevens moeten worden bewaard kan men uit de verkregen data geen bruikbare informatie halen.
 - Er zullen zich in de toekomst bijkomende moeilijkheden stellen bij een algemene bewaarplicht:
1. Nieuwe telecommunicatiediensten gaan steeds meer op zoek naar beveiligingstechnieken, zoals versleuteling, waardoor de verkregen gegevens geen zinvolle informatie opleveren. Wanneer steganografie wordt gebruikt kan de encryptie zelfs niet worden opgemerkt. Software voor encryptie is in ruime mate beschikbaar en internetproviders verwachten dat VoIP ook versleuteld zal worden.
 2. Telefonie met Skype (VoIP) en internet gebaseerde VPN's (Virtual Private Networks) zijn vandaag de dag praktisch onopspoorbaar in een

¹⁶ "Verslag van een mondeling overleg", *Eerste Kamer der Staten-Generaal*, 6 september 2005, <http://europapoort.eerstekamer.nl/9345000/1/j9vvgv6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

publiek netwerk. Om te weten of een bepaald netwerkpakket een VoIP-pakket is, moet men aan ‘*deep packet inspection*’ doen en zelfs dan is het betwistbaar of men alle VoIP traffic kan onderscheppen. Bovendien bevindt men zich dan op een dubieuze scheidingslijn en kan men zich afvragen of men zo niet reeds de inhoud van communicatie gaat controleren. In het geval van een VPN-verbinding kan niets onderschept worden omdat alles geëncrypteerd wordt tussen de individuele gebruiker en de VPN-server.

3. Ontwikkelingen op het vlak van telecommunicatie gebeuren vaak door gebruikers en netwerkproviders hebben hier geen controle op.

Bovenstaande argumenten tonen aan dat de informatie die men zou verkrijgen op basis van een algemene bewaarplicht niet steeds eenduidig interpreteerbare of waterdichte bewijslast opleveren op basis waarvan men terroristische aanslagen of ernstige criminaliteit kan opsporen en voorkomen en de algemene bewaarplicht op die manier haar doel eigenlijk voorbijschiet.

5. Een algemene bewaarplicht schendt het beroeps- en bronnengeheim.

Naast bovenvermelde pijnpunten verstoort een algemene bewaarplicht bovendien het beroepsgeheim van artsen, advocaten, journalisten en geestelijken, evenals politieke en zakelijke activiteiten die vertrouwelijkheid vereisen. Zonder de garantie op privacy zullen mensen minder snel geneigd zijn om met hun problemen een beroep te doen op vertrouwenspersonen. 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 gebruiken¹⁷. Ook informanten van journalisten zullen bij een algemene bewaarplicht aarzelen om gevoelige informatie door te spelen via telecommunicatie¹⁸.

Het beroepsgeheim en het bronnengeheim zijn nochtans fundamentele en grondwettelijk beschermde rechten die van zeer groot belang zijn bij het vrijwaren van onze democratische rechtstaat. Daaruit vloeit voort dat een inbreuk op deze rechten enkel aanvaardbaar is in zeer uitzonderlijke omstandigheden, wanneer noodzaak en hoogdringendheid kunnen worden aangetoond en indien er strenge procedurele waarborgen worden gevolgd. Zo heeft het Belgische Grondwettelijk Hof in een recent vonnis van 23 januari 2008 verduidelijkt dat “*de strijd tegen witwaspraktijken en het financieren van terrorisme onder geen enkel beding een onconditionele en onbeperkte inbreuk op het beroepsgeheim kan rechtvaardigen*”¹⁹.

¹⁷ <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/>.

18

‘Deutsche Telekom verdacht van afluisteren journalisten’, De Standaard, 24 mei 2008, http://www.standaard.be/Artikel/Detail.aspx?artikelId=DMF24052008_046 en BRAUCK, M., ROSENBACH, M. en VERBEET, M., ‘Big Brother Eyes German Journalists’, Der Spiegel, 11 januari 2007: <http://www.spiegel.de/international/germany/0,1518,514872-2,00.html>.

¹⁹ Grondwettelijk Hof Nr: 10/2008, 23 januari 2008, www.const-court.be.

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.

6. Europa & de algemene bewaarplicht.

De Europese databewaringsrichtlijn werd op 21 februari 2006 aangenomen door de Raad in de onmiddellijke nasleep van de terreuraanslag die in Londen op 7 juli 2005 plaatsvond in een aantal metrostations en bussen. Deze verregaande richtlijn werd publiek dan ook gerechtvaardigd vanuit een strijd tegen het terreur, maar de vraag naar één of andere vorm van bewaarplicht bestond al veel langer. Zo circuleerden er al sinds het einde van de jaren 1990 wensenlijstjes van politiediensten over de omvang en inhoud van een gewenste bewaarplicht. Besluitvorming terzake bleef lange tijd uit gezien de mensenrechtelijke impact, maar het wetgevend proces kwam in een stroomversnelling door de publieke verontwaardiging over de verschillende recente terreuraanslagen op Westerse bodem in New York, Madrid en Londen.

De databewaringsrichtlijn werd bijgevolg bijzonder snel aangenomen, maar zonder de nodige reflectie en overleg. Dit leidde tot felle kritieken en weerstand doorheen heel de Europese Unie; ook op beleidsniveau. Zo spraken Viviane Reding, destijds Europees Commissaris voor Informatiemaatschappij en Media, de Commissie voor Industrie, onderzoek en energie van het Europese Parlement, en de Raad van ministers inzake Telecommunicatie zich onder meer uit tegen de databewaringsrichtlijn²⁰. Ook de Commissie voor Burgerlijke vrijheden, Justitie en Binnenlandse Zaken van het Europese Parlement nam op 24 november 2005 het rapport Alvaro aan waarbij gepleit werd voor een beperktere reikwijdte van de bewaarplicht en meer waarborgen gevraagd werden tegen eventueel misbruik²¹. Verder uitten de Europese Toezichthouder voor Gegevensbescherming en de Artikel 29 Werkgroep hun opmerkingen en aanbevelingen bij dit voorstel voor een richtlijn²². Tijdens de Raad voor Justitie en Binnenlandse Zaken van 1 en 2 december 2005 werd een deel van de voorgestelde wijzigingen doorgevoerd, waarna dit herwerkte voorstel als een compromis werd voorgelegd aan de Commissie en het Europees Parlement. Hierbij werd onder meer geopteerd voor een bewaartermijn van zes tot vierentwintig maanden en de reikwijdte van de richtlijn werd lichtjes ingeperkt. Desondanks raakte

²⁰ Viviane Reding, momenteel Europees commissaris voor Justitie, grondrechten en burgerschap, bevestigde deze gang van zaken recent nog tijdens de hoorzitting met de LIBE-commissie op 19/01/2010:

<http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm;jsessionid=151A805A1AD9823CDDDBCE0A7FFB013A1?language=NL>.

²¹ <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2005-0365&language=NL>.

²² Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een Richtlijn van het Europees Parlement en de Raad over de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische-communicatiediensten en houdende wijziging van Richtlijn 2002/58/EG (COM(2005) 438 def.) [Officieel Publicatieblad C 298 van 29/11/2005 blz. 0001 - 0012].

Advies 3/2006 van 25 maart 2006 inzake Richtlijn 2006/24/EG van het Europees Parlement en de Raad betreffende de bewaring van gegevens die worden gegenereerd of verwerkt in verband met het aanbieden van openbare elektronische-communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_nl.pdf.

men niet aan de kern van de punten die ter discussie werden gesteld door tal van actoren, zoals het Europese Parlement en de toezichhouders voor gegevensbescherming.

De herwerkte tekst werd echter doorgedrukt door de Raad van ministers inzake Justitie en Binnenlandse Zaken²³ en helaas stemde het Europese Parlement reeds op 14 december 2005 in een eerste lezing in met het door de Raad voorgestelde compromis. De eerdere standpunten van het Europese Parlement, zoals vastgelegd in het rapport Alvaro, én de burgerrechten van de Europese bevolking werden hierdoor volledig miskend. Niet iedereen binnen het Europese Parlement was dan ook gelukkig met deze uitkomst. Zo heeft rapporteur Alexander Nuno Alvaro²⁴ uit onvrede met de uiteindelijke beslissing zijn naam van het rapport laten schrappen. Daarnaast had ook een deel van de Europese Parlementsleden zich verzet tegen dit compromis door amendementen voor te stellen. Zo werd bijvoorbeeld de reikwijdte van de richtlijn beperkt tot “*ernstige misdaad zoals gedefinieerd in de nationale wetgevingen van de lidstaten*”. De meest fundamentele amendementen hebben het echter niet gehaald doordat op voorhand geheime voorakkoorden werden gesloten tussen de meerderheidspartijen van het Europese Parlement en de Raad²⁵. De ontstaansgeschiedenis van deze richtlijn is dan ook een zoveelste voorbeeld van de weinig democratische werking van Europa.

Er kwam dan ook al snel uit verschillende hoeken verzet tegen deze richtlijn; zij het om verschillende redenen en met verschillende oogmerken. Zo diende Ierland op 11 juli 2006, later bijgetreden door Slovenië, een verzoek tot vernietiging van richtlijn 2006/24/EG in bij het Europese Hof van Justitie (zaak C-301/06)²⁶. Ierland was niet zozeer gekant tegen het principe van een algemene bewaarplicht, maar was van oordeel dat de bewaarplicht op een foutieve rechtsgrond stelde. Zo oordeelde de Ierse regering dat een bewaarplicht door middel van een kaderbesluit had moeten worden aangenomen binnen het beleidsdomein Justitie en Binnenlandse Zaken, de zogenaamde derde pijler, aangezien de richtlijn tot doel heeft ernstige criminaliteit te bestrijden. Een van de argumenten van Ierland was de redenering dat vele landen aanvankelijk geen databewaringsregime kenden en dat “*geen enkele kwestie gerelateerd aan de interne markt kon rechtvaardigen dat een lidstaat verplicht werd telecomoperatoren gegevens te laten bijhouden [...] indien dergelijke verplichtingen voorheen nog niet bestonden onder de wetgeving van de lidstaat in kwestie*”²⁷. Ierland riep echter geen mensenrechtelijke bezwaren in tegen deze richtlijn bij haar procedure voor het Europese Hof van Justitie.

Vandaar dat op 8 april 2008 een grote en diverse groep van organisaties (waaronder burgerrechtenorganisaties, beroepsverenigingen, internetproviders, ...) zich als

²³ Viviane Reding, momenteel Europees commissaris voor Justitie, grondrechten en burgerschap, bevestigde deze gang van zaken recent nog tijdens de hoorzitting met de LIBE-commissie op 19/01/2010:

<http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm;jsessionid=151A805A1AD9823CDDDBCE0A7FFB013A1?language=NL>.

²⁴ Van de fractie ‘Alliantie van Liberalen en Democraten voor Europa’ (ALDE).

²⁵ December 2005, Statewatch Analysis, “*The European Parliament and data retention: Chronicle of a ‘sell-out’ foretold?*”, http://www.statewatch.org/news/2005/dec/sp_dataret_dec05.pdf.

²⁶ http://www.vorratsdatenspeicherung.de/images/ireland_2006-07-11.pdf.

²⁷ http://www.vorratsdatenspeicherung.de/images/ireland_2006-07-11.pdf.

'friends of the Court' schaarde achter het Ierse verzoek tot vernietiging door bijkomende mensenrechtelijke argumenten in te roepen²⁸. Zij oordeelden immers dat naast de discussie of de databewaringsrichtlijn wel op basis van de juiste rechtsgrond was aangenomen, het Hof zich ook best zou uitspreken over een veel belangrijker aspect, namelijk of de databewaringsrichtlijn al dan niet in strijd was met het Europees Verdrag voor de Rechten van de Mens, en meer bepaald met artikel 8 dat het recht op privacy moet vrijwaren.

In haar arrest van 10 februari 2009 oordeelde het Europese Hof van Justitie echter dat de databewaringsrichtlijn wel degelijk binnen de eerste pijler moest worden aangenomen aangezien de richtlijn de verplichtingen ten aanzien van telecomoperatoren en internetproviders regelt en niet zozeer het gebruik van deze gegevens door politie en justitie. Bovendien stelde het Hof dat aangezien de richtlijn terecht binnen de eerste pijler (m.b.t. harmonisatie van de interne markt) was aangenomen en nagenoeg geen bepalingen invoerde ten aanzien van de toegang tot, en het gebruik van, deze gegevens door politie en justitie, men ook geen uitspraak moest doen over het feit of deze richtlijn al dan niet in strijd is met het recht op privacy. Dit was natuurlijk zeer jammer aangezien het een uitgelezen kans was voor het Europese Hof van Justitie om uitspraak te doen over het aspect privacy en de proportionaliteit van de algemene bewaarplicht. Op basis van verschillende rechtszaken op nationaal niveau kan het echter best dat het Europese Hof van Justitie in de toekomst alsnog geïnterpelleerd zal worden om zich uit te spreken over de grond van de zaak, met name de schending van fundamentele mensenrechten, op basis van een prejudiciële vraag van een nationaal Grondwettelijk Hof. Momenteel zijn er twee zulke verzoeken ingediend, één bij het Duitse Grondwettelijke Hof door het Arbeitskreis Vorratsdatenspeicherung en één bij het Ierse Grondwettelijke Hof door Digital Rights Ireland.

Intussen hebben nationale gerechtshoven in verschillende Europese lidstaten zich reeds moeten uitspreken, of zullen dat in de nabije toekomst moeten doen, over de omzetting van de databewaringsrichtlijn na klachten van burgers, burgerrechtenorganisaties en telecomoperatoren die aanvoeren dat de willekeurige opslag van communicatiegegevens een schending uitmaakt van het fundamentele recht op privacy. Zo is er het voorlopige arrest van 11 maart 2008, herbevestigd op 28 oktober 2008, van het Federale Grondwettelijk Hof van Duitsland waarbij het Hof de Duitse omzetting van de databewaringsrichtlijn gedeeltelijk opschortte wegens een vermoedelijke onverenigbaarheid met de Duitse grondwet. Het Hof verbood daarbij niet het verzamelen van internet- en telefoniegegevens op zich, maar beperkte wel het gebruik van die gegevens in afwachting van een uitspraak ten gronde. Dat dit een relatief voorzichtig arrest betreft, moet gerelativeerd worden aangezien het Federale Grondwettelijk Hof van Duitsland traditioneel nogal bescheiden optreedt wanneer het een voorlopig arrest uitspreekt. Op 15 december 2009 organiseerde het Duitse Hof tevens hoorzittingen in verband met de klachten van 34.000 Duitse burgers²⁹. De rechters stelden zich daarbij zeer kritisch op naar de regeringsverantwoordelijken die de Duitse bewaarplicht moesten komen verdedigen. Momenteel is het wachten op het arrest ten gronde. We kunnen alleen maar hopen dat het Duitse Hof even kritisch zal

²⁸ http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/8-04-08_Brief_ngos_aan_ECJ.pdf

²⁹ <http://www.bverfg.de/pressemitteilungen/bvg08-037en.html> (1 BvR 256/08) en <http://www.bverfg.de/pressemitteilungen/bvg08-092en.html>. Zie ook <http://www.vorratsdatenspeicherung.de/content/view/301/79/lang.en/>.

zijn als de Grondwettelijke Hoven van Roemenië en Bulgarije die reeds oordeelden dat hun respectievelijke nationale wetgeving inzake de algemene bewaarplicht ongrondwettelijk is³⁰. Ten slotte werd er ook in Ierland en de Tsjechische Republiek een rechtszaak opgestart³¹ en bestaat er hevig protest tegen een nakende omzetting van de databewaringsrichtlijn in Oostenrijk³².

Enkele opmerkelijke uitspraken in het arrest van het Roemeense Grondwettelijke Hof zijn o.m.³³:

“The obligation to retain the data, established by Law 298/2008 [de Roemeense databewaringswet], as an exception or a derogation from the principle of personal data protection and their confidentiality, empties, through its nature, length and application domain, the content of this principle, as it was guaranteed by law [...]. Or, it is unanimously recognized in the ECHR jurisprudence [...] that the signatory member states of the Convention for the protection of human rights and fundamental freedoms have assumed obligations to ensure that the rights guaranteed by the Convention are concrete and effective, not theoretical and illusory, the adopted legal norms following the effective protection of rights. The legal obligation that foresees the continuous retention of personal data transforms though the exception from the principle of effective protection of privacy right and freedom of expression, into an absolute rule. The right appears as being regulated in a negative manner, its positive role losing its prevailing role. [...] The regulation of a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear by removing the safeguards regarding its execution. The physical and legal persons, mass users of the public electronic communication services or networks, are permanent subjects to this intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays.”

En verder: *“[...] Law 298/2008 imposes the obligation of a continuous retention of traffic data, from the moment of its entry into force and its application without considering the necessity for the cessation of the limitation once the determinant cause has disappeared. The intrusion into the free exercise of the right takes place continuously and independently of the occurrence of a justifying fact, of a determinant cause and only for the scope of criminal prevention and the discovery – after their perpetration – of serious crimes. [...] The Constitutional Court underlines that the justified use, under the conditions regulated by law 298/2008, is not the one that in itself harms in an unacceptable way the exercise of the right to privacy or the*

³⁰ <http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention> en http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.

³¹ http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/14-09-06_Digital_Rights_Ireland_Limited_vs_Ierland.pdf.

³² <http://futurezone.orf.at/stories/1636361/>.

³³ 8 OKTOBER 2009 - Grondwettelijk Hof, zaak no. 1258 (originele Roemeense versie): http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf en (niet originele versie, onofficiële vertaling naar het Engels): http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

freedom of expression, but rather the legal obligation with a continuous character, generally applicable, of data retention. This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. Law 298/2008, even though it uses notions and procedures specific to the penal law, has a large applicability – practically to all physical and legal persons users of electronic communication services or public communication networks - so, it can't be considered to be in agreement with the provisions in the Constitution and Convention for the defence of human rights and fundamental freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression.”

“The Constitutional Court observes that, even though Law 298/2008 refers to data with a predominantly technical character, these are retained with the scope of providing information regarding a person and its private life. [The retained data] as well as other „related data” - not defined in the law – are likely to prejudice, to inhibit the free usage of the right to communication or to expression. The retaining of these data, in a continuous way, in relation to every user of electronic communication services or public communication networks, regulated as an obligation of the providers they may not divert from without being subject to sanctions [...] is sufficient to generate in the mind of the persons the legitimate suspicion regarding the respect of their privacy and the perpetration of abuses. The legal safeguards on the concrete use of the retained data [...] are not sufficient and appropriate to dismiss the fear that the personal intimate rights are not breached, so that their manifestation can take place in an acceptable manner.”

“[...] The Constitutional Court does not deny the purpose considered by the legislator as such at the adoption of law 298/2008, in the sense that there is an urgent need to ensure adequate and efficient legal tools, compatible with the continuous process of modernization and technical upgrading of the communication means, so that the crime phenomenon can be controlled and fought against. [...] The limitation of the exercise of certain personal rights by considering collective rights and public interests [...] has always been a sensitive operation from the regulation point of view, so that a fair balance may be achieved between individual rights and interests, on the one hand, and the rights and interests of society, on the other hand. It is also true [...] that taking surveillance measures without adequate and sufficient safeguards can lead to “destroying democracy on the ground of defending it.” [...] In conclusion [...] the Constitutional Court observes, for the reason shown above, that the examined law is unconstitutional in its entirety [...]”

In België bleef het lang stil rond de databewaringsrichtlijn, maar recent besliste de regering om toch vooruit te gaan met de omzetting van deze richtlijn naar intern recht. De regering geeft aan dat dit dossier veel commotie heeft veroorzaakt in de verschillende Europese lidstaten, maar trekt hier geen conclusies uit voor de binnenlandse aanpak. Integendeel, de minister van Justitie pleit voor een snelle omzetting met een absolute deadline van juni 2010. De regering neemt immers in de tweede helft van 2010 (juli-december 2010) het voorzitterschap van de Europese Unie op zich en zij wil vermijden dat ze een mal figuur slaat doordat ze de richtlijn tegen

dan nog niet zou hebben omgezet terwijl ze op dat moment de evaluatie van dit belangrijke dossier op Europees niveau zou moeten leiden³⁴. Niet alleen is dit een flauw argument om fundamentele mensenrechten te negeren, maar dit klopt ook niet.

Enerzijds gaf Cecilia Malmström tijdens de hoorzitting in de LIBE-commissie van het Europese Parlement op dinsdagvoormiddag 19/01/2010 aan dat een grondige evaluatie van de databewaringsrichtlijn op zijn deugdelijkheid m.b.t. proportionaliteit, gegevensbescherming en kosten pas zou plaatsvinden begin 2011³⁵. Anderzijds is het helemaal niet zeker dat alle Europese lidstaten dezelfde mening zullen zijn toegedaan m.b.t. de deugdelijkheid van deze richtlijn. Zo werden de regeringen in Roemenië, Bulgarije en Duitsland gedwongen om hun nationale databewaringswetgeving aan te passen en is de Duitse liberale partij, die recent deel uitmaakt van de nieuwe Duitse regering, sterk gekant tegen de algemene bewaarplicht. Ook Zweden heeft ondanks aanmaningen van de Europese Commissie de databewaringsrichtlijn nog steeds niet omgezet naar nationaal recht³⁶. In plaats van de implementatieprocedure overhaast te doorlopen zoals de Belgische regering doet, zien een aantal politici dit als een kans om de databewaringsrichtlijn te evalueren op basis van haar consistentie met het Europees Verdrag voor de Rechten van de Mens. België zou hier beter lessen uit trekken en zich dus evenzeer kunnen opwerpen als een principiële tegenstander van de algemene bewaarplicht en op deze wijze de debatten op Europees niveau leiden. De verdediging van fundamentele mensenrechten op Europees niveau kan immers nooit een beschamende rol zijn! In die zin hebben burgerrechtenorganisaties EDRi (European Digital Rights) en de Duitse werkgroep inzake databewaring (AK Vorratsdatenspeicherung) de Europese Commissie reeds op 30 september 2009 gevraagd om de omstreden databewaringsrichtlijn van 2006 in te trekken. Indien de richtlijn niet wordt ingetrokken, eisen zij dat de richtlijn zodanig wordt aangepast dat er in een opt out clause wordt voorzien die toelaat dat lidstaten zelf kunnen beslissen of zij een algemene bewaarplicht nodig hebben.

Viviane Reding, momenteel ondervoorzitter van de Europese Commissie en commissaris voor Justitie, grondrechten en burgerschap - m.a.w. een zeer belangrijke figuur binnen de Commissie, benadrukte tijdens haar hoorzitting met de LIBE-commissie van het Europese Parlement op dinsdagvoormiddag 19/01/2010³⁷ dat zij met de aanneming van het Verdrag van Lissabon op 1 december 2009 en de inwerkingtreding van het Handvest van de Grondrechten van de Europese Unie een nieuwe koers wil varen op Europees niveau. Fundamentele mensenrechten en bescherming van persoonsgegevens worden voor haar topprioriteiten tijdens haar beleidsperiode, en deze beleidsverklaring wordt gedeeld door haar collega Cecilia Malmström, Commissaris voor Binnenlandse Zaken. Wanneer men deze uitspraak van Reding bekijkt in het licht van haar eerdere weerstand tegen de databewaringsrichtlijn dan mag men redelijkerwijze verwachten dat de evaluatie van de databewaringsrichtlijn niet unilateraal positief zal zijn en misschien zelfs wordt ingetrokken. België kan in die zin dan ook een positieve rol spelen tijdens haar

³⁴ zie 'debatnota inzake dataretentie' van de minister van Justitie Stefaan De Clerck.

³⁵ <http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm;jsessionid=151A805A1AD9823CDDDBCE0A7FFB013A1?language=NL>.

³⁶ RICKNAS, M., 'Sweden challenges EU data retention directive', Computerworld, 27 mei 2009: http://www.computerworld.com/s/article/9133566/Sweden_challenges_EU_data_retention_directive.

³⁷ <http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm;jsessionid=151A805A1AD9823CDDDBCE0A7FFB013A1?language=NL>.

komende voorzitterschap van de Europese Unie door zich op te werpen als een pionier die invasieve maatregelen niet zomaar omzet naar intern recht vanuit een terechte bekommernis om fundamentele mensenrechten. Wanneer de Belgische regering deze beslissing op dergelijke wijze motiveert aan de Europese Commissie moet er gezien de recente machtswissel in deze Commissie wel begrip voor bestaan, willen zij hun recente beleidsverklaringen alle eer aandoen...

7. Een algemene bewaarplicht brengt enorme kosten met zich mee die hoe dan ook voor rekening van de gewone burger zullen zijn.
--

Ten slotte zal een algemene bewaarplicht ook onvermijdelijk leiden tot zware financiële inspanningen voor telecomoperatoren en internetproviders³⁸. Indien zij hiervoor geen compensaties ontvangen van de overheid zullen zij deze kosten ongetwijfeld doorrekenen aan de consumenten door middel van een forse stijging in de abonnementsgelden. Sommigen spreken zelfs van een 25% verhoging van de abonnementsgelden voor telefonie en internet³⁹. Dit laatste zou de digitale kloof tussen burgers alleen maar vergroten in een tijdperk waarin telecommunicatie centraal staat. Indien de overheid er toch voor kiest om de kosten van de telecomoperatoren en de internetproviders te vergoeden, zijn het in feite de belastingbetalers die de rekening moeten betalen. Aangezien het departement Justitie, zoals recent bekend raakte, in totaal zo'n 25 miljoen euro moet besparen, ook op gerechtskosten, en dit departement reeds jarenlang een ondermaatse financiering kent met desastreuze gevolgen zoals een gebrekkige en verouderde infrastructuur, zou ze haar beperkte middelen beter inzetten op andere vlakken dan het vergoeden van de kosten verbonden aan een algemene bewaarplicht. Of het nu de consumenten of de belastingbetalers zijn die moeten opdraaien voor de hoge kosten van de algemene bewaarplicht, in de praktijk zou het betekenen dat iedere burger de kosten betaalt van het toezicht op zijn persoon.

³⁸ Voor meer informatie over het kostenaspect van de bewaarplicht zie bijvoorbeeld de KPMG-studie van november 2004 en "Common Position of Principle on the Matter of Data Retention", juni 2008, p. 17.

³⁹ TIBEAU, F., 'Telefonie en internet straks 25 procent duurder?', Datanews, 9 mei 2008: <http://datanews.rnews.be/nl/news/90-12-18142/telefonie-en-internet-straks-25-procent-duurder-.html>.

**Artikelgewijze bespreking van het voorontwerp van wet en ontwerp van KB van
27 augustus 2009**

Zoals hierboven reeds uiteengezet is de Liga voor Mensenrechten geen voorstander van een algemene bewaarplicht -in eender welke vorm- aangezien het een serieuze schending inhoudt van het recht op privacy en vertrekt van de idee dat elke burger potentieel gevaarlijk is. Bovendien stellen experts de meerwaarde van deze maatregel in vraag aangezien de bewaarplicht in de praktijk niet alleen ongeschikt blijkt, maar ook voor alle betrokken partijen een onredelijke financiële en praktische belasting betekent. De Liga voor Mensenrechten doet dan ook een oproep aan de Belgische wetgever om de databewaringsrichtlijn niet om te zetten naar Belgisch recht en om de regering opdracht te geven initiatieven te nemen om deze Europese richtlijn op Europees niveau ongedaan te maken of minstens grondig bij te sturen.

In totaal subsidiaire orde wenst de Liga nog te beklemtonen dat ook de reglementerende vorm waarin de bewaarplicht zou worden ingevoerd voor grondige kritiek vatbaar is. U vindt hieronder dan ook een artikelgewijze bespreking van het Voorontwerp van Wet van 27 augustus 2009 en het ontwerp van Koninklijk Besluit van 14 augustus 2009.

1. Wijze van omzetting:

Artikelen:

Memorie van Toelichting: p. 1, laatste alinea; p. 4, 2^e en 5^e alinea.

Bijlage bij MvT: p. 18, onderaan, en verder op p. 19.

Voorontwerp van Wet: art. 3, §1, 3^e lid.

Knelpunten:

De Memorie van Toelichting en artikel 3, §1, 3^e lid, van het Voorontwerp van Wet stipuleren dat de lijst van te bewaren gegevens en de bewaringsvoorwaarden 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, en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut”*. 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. Zo stelt de MvT op p. 4, 5^e alinea immers: *“Een Koninklijk Besluit laat dan ook een snelle update van het wettelijke kader toe”*. De Liga voor Mensenrechten is van oordeel dat deze materie te ingrijpend is om niet langs parlementaire weg te behandelen.

Dit betreft niet alleen een fundamentele kwestie, maar is zelfs de enige mogelijke optie aangezien artikel 22 van de Belgische Grondwet -dat het recht op eerbiediging van het privéleven en het gezinsleven waarborgt- enkel uitzonderingen op dit recht toelaat indien deze worden vastgelegd per wet. Het Grondwettelijk Hof heeft herhaaldelijk in haar arresten beklemtoond dat dit enkel een ‘wet’ in de formele betekenis van het woord kan zijn en dat deze verplichting voortvloeit uit art. 53 van

het EVRM⁴⁰. De mensenrechtencommissaris, Thomas Hammarberg, van de Raad van Europa heeft op 4 december 2008 nogmaals gewezen op welke elementen allemaal aanwezig moeten zijn in een dergelijke wet⁴¹. Een vage en algemene wettelijke basis voor het verzamelen, opslaan, gebruiken, analyseren en delen van persoonlijke gegevens voor strafrechtelijke doeleinden kan volgens hem in geen geval volstaan.

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 en de bewaringsvoorwaarden, te reguleren via een wet in plaats van een Koninklijk Besluit.

2. Bewaringstermijn:

A. Artikelen:

Memorie van Toelichting: p.6, 5^e alinea; p. 19, laatste alinea, p. 20, 1^e alinea en p. 23, 3^e alinea.

Bijlage bij MvT: p. 19, onderaan, en verder.

Voorontwerp van Wet: art. 3, §1,4^e lid.

Verslag aan de Koning: p. 4, 3^e en 4^e alinea.

Ontwerp van Koninklijk Besluit: art. 2, §3, 1^e en 2^e lid; art. 3, §3, 1^e en 2^e lid; art.4, §3, 1^e en 2^e lid; art. 5, §3, 1^e en 2^e lid; en art. 7, 4e lid.

Knelpunten:

Artikel 3, §1, 4^e lid van het Voorontwerp van Wet stelt dat de bewaringstermijn 12 maanden bedraagt en dat na afloop van deze termijn de gegevens onverwijld worden vernietigd, tenzij voor de normale bedrijfsvoering overige wettelijke termijnen van toepassing zijn. Dit betekent dat de te bewaren gegevens langer zullen worden bewaard dan de Europese richtlijn minimaal vereist. Het éézijdige argument om verkeers- en locatiegegevens zo lang mogelijk te bewaren om tegemoet te kunnen komen aan eventuele, toekomstige onderzoeksvragen heeft echter een belangrijke keerzijde. Hoe langer de bewaarperiode zal zijn, hoe groter de privacy-schending 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... Bovendien moet de noodzakelijkheid van een bewaartermijn van 12 maanden worden aangetoond met cijfers uit de praktijk en rekening houdende met eventuele neveneffecten op lange termijn.

Een ander knelpunt is de vraag wat er met de bewaarde gegevens gebeurt zodra zij rechtmatig opgevraagd worden door gerechtelijke autoriteiten. Het Voorontwerp van Wet en ontwerp van KB zeggen hierover niets. Worden zij dan opgeslagen in de A.N.G.? En zo ja, voor welke periode, wie heeft er toegang toe en voor welke doeleinden? De Liga wil er graag aan herinneren dat het informatiebeheer bij de politie al ruim 10 jaar zonder duidelijke, wettelijke regels functioneert. Na de terechte publieke commotie over het ontwerp van KB van 8 juli 2008 ‘*tot bepaling van de*

⁴⁰ Grondwettelijk Hof, Arrest nr. 202/2004 van 21 december 2004, B.5.4 en Arrest nr. 151/2006 van 18 oktober 2006, B.5.6. en volgende.

⁴¹

<https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679>

modaliteiten voor de verwerking van de persoonsgegevens en de informatie van de geïntegreerde politie, gestructureerd op twee niveaus in het raam van de algemene nationale gegevensbank’ dat veel te vaag bleef en teveel autonomie gaf aan de politiediensten, werden geen wettelijke initiatieven genomen tot een betere en transparantere regulering van het informatiebeheer bij de politie. In die zin kan het dan ook niet dat het huidige Voorontwerp van Wet stilzwijgend blijft over deze materie.

Aanbeveling:

De Liga is van oordeel dat een maximale bewaarperiode van 6 maanden essentieel is om de schending van het recht op privacy te beperken. Het tot nu toe naar voren geschoven cijfermateriaal en de willekeurige voorbeelden die worden aangehaald in de bijlage van de Memorie van Toelichting bij het Voorontwerp van Wet van 27 augustus 2009 voldoen absoluut niet om een bewaartermijn van 12 maanden te rechtvaardigen⁴². Het Voorontwerp van Wet moet ook duidelijkheid verschaffen over de opslag en bewaartermijn van de door politie en justitie opgevraagde gegevens, alsook het verdere beheer van deze gegevens (cf. regeling inzake toegang).

B. Artikelen:

Memorie van Toelichting: p.6, 6^e alinea (verder op p.7).

Bijlage bij de MvT: p. 23, 4-6^e alinea.

Voorontwerp van Wet: art. 3, §2.

Knelpunten:

Artikel 3, §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 bewaringstermijn voor de gegevens vast te leggen die langer is dan 12 maanden. In het Voorontwerp van Wet wordt echter niet nader verklaard wanneer er sprake is van “*uitzonderlijke omstandigheden*”. Om deze bepaling te preciseren verwijst men in de Memorie van Toelichting op p. 7, 1^e alinea, naar artikel 4, §1 van de Wet op de elektronische communicatie van 13 juni 2005, met name: “*wanneer de openbare veiligheid, de volksgezondheid, de openbare orde of de verdediging van het Rijk dit eisen [...]*”. Deze bepaling blijft echter nog dermate 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 burgerrechten⁴³.

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 zelf. Daarnaast moet ook bij wet worden vastgelegd met hoeveel maanden de maximale bewaartermijn van 12 maanden bij “*uitzonderlijke omstandigheden*” maximaal kan worden verlengd.

⁴² Zie eerder, punt 3: ‘De noodzaak van een algemene bewaarplicht werd niet bewezen’.

⁴³ Europees Hof voor de Rechten van de Mens, zaak van Silver en anderen versus het Verenigd Koninkrijk, 25 maart 1983, lijn 87 e.v.

3. Te bewaren gegevens

Artikelen:

Memorie van Toelichting: p. 1, laatste alinea; p. 4, 2^e en 5^e alinea.

Bijlage bij de MvT: p. 23, onderaan en verder.

Voorontwerp van Wet: art. 3, §1, 1^e en 3^e lid.

Verslag aan de Koning: p. 1, 3^e en 5^e alinea (verder p. 2); p. 2, 2^e en laatste alinea (verder p. 3); p. 3-7.

Ontwerp van Koninklijk Besluit: art. 1, 6^e en 7^e lid; art. 2, §1-2; art. 3, §1-2; art. 4, §1-2; art. 5, §1-2; en art. 6, 1^e lid.

Knelpunten:

Artikel 3, §1, 1^e lid van het Voorontwerp van Wet 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 3, §1, 3^e lid van het Voorontwerp van Wet stelt vervolgens dat de werkelijke lijst van de te bewaren gegevens zal bepaald worden door middel van een Koninklijk Besluit. De Memorie van Toelichting verduidelijkt op p. 4, 5^e 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 privacy-schending wordt, hoe hoger de gerelateerde kosten worden, 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 dus niet over de noodzakelijke democratische inslag om een dergelijke, fundamentele beslissing te nemen.

Bovendien laat het Verslag aan de Koning op p. 1, laatste 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 wensenlijstjes 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].*”⁴⁴. Ook het Europees Hof voor de Rechten van de Mens stelde in het arrest van Klass dat autoriteiten geen onbeperkte appreciatieruimte genieten ten aanzien van het in art. 8 EVRM gewaarborgde recht op privacy in de strijd tegen spionage en terreur⁴⁵.

De bijlage bij de Memorie van Toelichting (op p. 23 en verder) spreekt over een ‘beperkte’ uitbreiding van de lijst van te bewaren gegevens die door de Europese richtlijn werd bepaald. Zo ‘beperkt’ zijn deze gegevens echter niet. Enerzijds gaat het niet ‘alleen’ om gegevens die betrekking hebben op de gebruiker zoals op p. 27 van de bijlage bij de Memorie van Toelichting wordt beweerd, maar ook om verkeers- en locatiegegevens. Ook is het onduidelijk waarom de regering ervan zou uitgaan dat gegevens in verband met de gebruiker minder invasief zouden zijn? Het gaat bijvoorbeeld om informatie inzake de wijze van betalen, het leverings- en facturatieadres, de bijbehorende diensten waarop een abonnee geregistreerd is, de datum en plaats van registratie bij de dienst, de locatie van het netwerkaansluitpunt bij het einde van elke verbinding, het IP-adres dat gediend heeft voor het nemen van het abonnement of voor de registratie van de gebruiker, het volume van gegevens die tijdens de sessie of gevraagde tijdseenheid geüpload en gedownload werden, etc.

Aan de hand van een stelselmatige kennisname van bovenstaande gegevens, in combinatie met de gegevens die men in overeenstemming met richtlijn 2006/24/EG wil bewaren, kan men reeds een min of meer volledig beeld krijgen van bepaalde aspecten van iemands leven. Zo bieden dergelijke gegevens 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; hoe, waar en wanneer wordt er betaald voor deze diensten; welke diensten worden gebruikt; ...) 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. Men kan het bewaren van verkeers- en locatiegegevens dan ook bezwaarlijk als minder ingrijpend beschouwen dan het af luisteren van de inhoud van communicatie. Bijgevolg verdient het een afdoende beschermingsniveau.

Het klopt dat richtlijn 2006/24/EG het bewuste artikel 15 van richtlijn 2002/58/EG niet vervangt, maar dit maakt een uitbreiding van de lijst met de te bewaren gegevens nog niet legaal zonder de ‘absolute noodzakelijkheid’ ervan in een democratische

⁴⁴ 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.

⁴⁵ 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](http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Klass&sessionid=15331040&skin=hudoc-en).

samenleving op afdoende wijze aan te tonen! Ten slotte gaat het schamele argument van de regering niet op waarin gesteld wordt dat de bijkomende gegevens “*mee kunnen uitsluiten dat slachtoffers van identiteitsfraude onterecht worden betrokken als dader in een gerechtelijk dossier waar zij geen uitstaans mee hebben*”⁴⁶. Zoals eerder uitgelegd onder punt 4 (‘Een algemene bewaarplicht is inefficiënt’) is het risico veel groter dat een algemene bewaarplicht net zorgt voor foutieve incriminaties, zoals onder meer de Nederlandse Renate Tromp aan den lijve mocht ondervinden⁴⁷, en misbruiken allerhande⁴⁸.

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 maximaal beperkt moet blijven tot die gegevens die vereist worden door richtlijn 2006/24/EG. Het tot nu toe naar voren geschoven cijfermateriaal en de willekeurige voorbeelden die worden aangehaald in de bijlage van de Memorie van Toelichting bij het Voorontwerp van Wet van 27 augustus 2009 voldoen echter absoluut niet om de ‘absolute noodzaak’ van een algemene bewaarplicht, laat staan een uitbreiding van de lijst met de te bewaren gegevens, aan te tonen⁴⁹.

4. *Doeleinden van het bewaren en raadplegen van gegevens.*

Artikelen:

Memorie van Toelichting: p. 1, 2^e alinea; p. 6, 4^e alinea.

Bijlage bij de MvT: p. 13, punt 3; p. 14, punt 5; p. 17, punt 8.

Voorontwerp van Wet: art. 3, §1.

□ Knelpunten:

Artikel 3, §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 3, §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 opsporing en de vervolging van strafbare feiten, zoals vastgelegd in de artikelen 46bis en 88bis van het Wetboek van*

⁴⁶ Bijlage bij de MvT: p. 27, 3^e alinea.

⁴⁷ <http://www.intermediair.nl/artikel/weekblad-archief/57049/de-overheid-ziet-alles-en-wij-vinden-het-best.html>, http://cgi.omroep.nl/cgi-bin/streams?id/NCRV/serie/NCRV_1239778/NCRV_1246780/bb.20070430.asf?start=00:17:11&end=00:30:00 en [http://pauwenwitteman.vara.nl/Archief-detail.113.0.html?&tx_ttnews\[pointer\]=34&tx_ttnews\[tt_news\]=1064&tx_ttnews\[backPid\]=111&cHash=48ebce6893](http://pauwenwitteman.vara.nl/Archief-detail.113.0.html?&tx_ttnews[pointer]=34&tx_ttnews[tt_news]=1064&tx_ttnews[backPid]=111&cHash=48ebce6893).

⁴⁸ ‘Deutsche Telekom verdacht van afluisteren journalisten’, De Standaard, 24 mei 2008, http://www.standaard.be/Artikel/Detail.aspx?artikelId=DMF24052008_046 en BRAUCK, M., ROSENBAACH, M. en VERBEET, M., ‘Big Brother Eyes German Journalists’, Der Spiegel, 11 januari 2007: <http://www.spiegel.de/international/germany/0,1518,514872-2,00.html>.

⁴⁹ Zie eerder, punt 3: ‘De noodzaak van een algemene bewaarplicht werd niet bewezen’.

- Strafvordering*”;
- *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*’.

Aangezien het verzamelen en bewaren van de verkeers- en locatiegegevens reeds een enorme privacyschending met zich meebrengt, moeten de doeleinden waarvoor dit toegelaten is beperkt blijven tot het “*onderzoeken, opsporen en vervolgen van ernstige criminaliteit*” zoals vastgelegd door richtlijn 2006/24/EG. Bovenstaande 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 subsidiariteit⁵⁰.

Deze richtlijn stipuleert bovendien dat deze “*ernstige vormen van criminaliteit*” moeten worden gedefinieerd in nationale wetgeving. Men mag aan deze verplichting niet verzaken door simpelweg te verwijzen naar de vigerende wetgeving (cf. art. 46bis & 88bis Sv.) die de toegang tot deze gegevens regelen. Zoals eerder uiteengezet betekent de loutere opslag van persoonsgerelateerde gegevens reeds een aanzienlijke inbreuk op het recht op privacy. Het opsplitsen van regels die de bewaring van gegevens regelen en deze die de toegang ertoe regelen is dan ook onaanvaardbaar in een democratische samenleving aangezien niemand dan nog een overzicht behoudt van het geheel, uitbreiding van de toegang ertoe op een weinig transparante wijze kan plaatsvinden en tenslotte toezicht en controle zeer moeilijk worden gemaakt. Bovendien mogen we toch oordelen dat de artikelen 46bis en 88bis van het Belgische Wetboek van Strafvordering de drempel een flink stuk lager leggen dan de Europese richtlijn voor ogen had. Op basis van art. 46bis en 88bis Sv. mogen gegevens immers worden opgevraagd voor praktisch alle misdrijven (meer bepaald voor wanbedrijven en misdaden in tegenstelling tot de door de richtlijn beoogde ‘ernstige criminaliteit’ zoals terrorisme en georganiseerde misdaad). Andere misplaatste doeleinden die het Voorontwerp van Wet toelaat, zijn ‘de beteugeling van kwaadwillige oproepen naar de nooddiensten’ en ‘het onderzoek door de Ombudsdienst voor telecommunicatie naar de identiteit van elke persoon die kwaadwillig gebruik heeft gemaakt van een elektronisch communicatienetwerk of –dienst’. Ook is het momenteel onduidelijk in welke mate veiligheids- en inlichtingendiensten toegang zullen krijgen tot de te bewaren gegevens in het kader van de ‘specifieke procedures’ van de nieuwe BIM-wet. Het Voorontwerp van Wet van 27 augustus 2009 en het ontwerp van KB van 14 augustus 2009 ter omzetting van de databewaringsrichtlijn zeggen hier alleszins niets over. Is dit reeds een eerste voorbeeld van hoe de toegang tot deze gegevens op een weinig transparante wijze wordt uitgebreid?

⁵⁰ 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 bewaren van de verkeers- en locatiegegevens reeds een enorme privacyschending met zich meebrengt, moeten de doeleinden waarvoor dit toegelaten is beperkt blijven 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. Deze limitatieve lijst van ernstige criminaliteit moet rekening houden met de gestelde voorwaarden bij het verdragsrechtelijk en grondwettelijk beschermde recht op privacy (zie boven). Daarnaast moet het Voorontwerp van Wet ook limitatief opsommen wie beschouwd kan worden als een bevoegde autoriteit om, mits een rechtmatig bevel, gegevens op te vragen bij de Coördinatiecel Justitie. Men mag aan deze verplichting niet verzaken door simpelweg te verwijzen naar de vigerende wetgeving (cf. art. 46bis & 88bis Sv.) die de toegang tot deze gegevens regelen.

5. Voorwaarden voor het raadplegen van de bewaarde gegevens.

Artikelen:

Bijlage bij de MvT: p. 10, 4^e alinea; p. 13, punt 3; p. 14, punt 5; p. 17, punt 8; p. 31, punt 14.

Voorontwerp van Wet: art. 3, §1, 5^e lid.

Verslag aan de Koning: p. 8, 2^e alinea.

Ontwerp van Koninklijk Besluit: art. 7, 3^o en art. 8.

Knelpunten:

Artikel 3, §1, lid 5, 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 rechtszekerheid⁵¹. Op basis van art. 7, 3^o, in combinatie met art. 8 van het ontwerp van KB kunnen we vermoeden dat niemand rechtstreeks toegang heeft tot de te bewaren gegevens buiten de Coördinatiecel Justitie binnen elke operator. Dit is echter een dermate belangrijk principe dat het tevens in het Voorontwerp van Wet expliciet moet worden opgenomen. Bovendien zou ook het Voorontwerp van Wet moeten preciseren hoe de Coördinatiecel Justitie zal worden samengesteld en hoe een concrete overdracht van informatie van de Coördinatiecel Justitie naar een bevoegde autoriteit met een rechtmatig bevel in de praktijk zal plaatsvinden. Ook deze procedures zijn cruciaal en zouden geregeld moeten worden in het Voorontwerp van Wet en niet in een afzonderlijk KB inzake de medewerkingsplicht van operatoren.

De bewaarplicht vormt op zichzelf reeds een ernstige bedreiging voor het functioneren van beroepen die vertrouwelijkheid vereisen zoals in het geval van

⁵¹ 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=hbk&action=html&highlight=Silver&sessionid=15329098&skin=hudoc-en>.

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 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 gebruiken⁵².

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 onbeperkte inbreuk op het beroepsgeheim kan rechtvaardigen⁵³”. 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.

Een ander knelpunt is de vraag wat er met de bewaarde gegevens gebeurt zodra zij rechtmatig opgevraagd worden door politie en justitie. Het Voorontwerp van Wet en ontwerp van KB zeggen hierover niets, maar op p. 31, onder punt 14, van de bijlage bij de Memorie van Toelichting kan men lezen dat *“de geraadpleegde gegevens bewaard zullen worden door de bevoegde gerechtelijke autoriteiten en niet langer bewaard dienen te worden door de operatoren”*. Worden zij dan opgeslagen in de A.N.G.? En zo ja, voor welke periode, wie heeft er toegang toe en voor welke doeleinden? De Liga wil er graag aan herinneren dat het informatiebeheer bij de politie al ruim 10 jaar zonder duidelijke, wettelijke regels functioneert. Na de terechte publieke commotie over het ontwerp van KB van 8 juli 2008 *‘tot bepaling van de modaliteiten voor de verwerking van de persoonsgegevens en de informatie van de geïntegreerde politie, gestructureerd op twee niveaus in het raam van de algemene nationale gegevensbank’* dat veel te vaag bleef en teveel autonomie gaf aan de politiediensten, werden geen wettelijke initiatieven genomen tot een betere en transparantere regulering van het informatiebeheer bij de politie. In die zin kan het dan ook niet dat het huidige Voorontwerp van Wet stilzwijgend blijft over deze materie.

Aanbeveling:

⁵² <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/](http://www.vorratsdatenspeicherung.de/content/view/236/1/lang/en/).

⁵³ Grondwettelijk Hof Nr. 10/2008, 23 januari 2008, www.const-court.be.

De Liga voor Mensenrechten vindt het een onaanvaardbare schending van het recht op privacy om de verkeers- en locatiegegevens op een onbeperkte wijze toegankelijk te stellen. De Liga vraagt bijgevolg dat het Voorontwerp van Wet expliciet vermeldt dat niemand rechtstreeks toegang heeft tot de te bewaren gegevens buiten de Coördinatieceel Justitie binnen elke operator. Verder moet het Voorontwerp van Wet ook preciseren hoe de Coördinatieceel Justitie zal worden samengesteld en hoe deze niet alleen zijn onafhankelijkheid ten aanzien van de operator, maar ook ten aanzien van de gerechtelijke autoriteiten kan bewaren. Daarnaast moet het Voorontwerp van Wet ook preciseren hoe een concrete overdracht van informatie van de Coördinatieceel Justitie naar een bevoegde autoriteit met een rechtmatig bevel in de praktijk zal plaatsvinden. Ook deze procedures zijn cruciaal en zouden geregeld moeten worden in het Voorontwerp van Wet en niet in een afzonderlijk KB inzake de medewerkingsplicht van operatoren.

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 rechter⁵⁴. Daarnaast vraagt de Liga voor Mensenrechten ook dat elke toegang tot en raadpleging van de databank 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. Verder moet het Voorontwerp van Wet ook preciseren welke regels van kracht zijn nadat opgevraagde gegevens door de bevoegde gerechtelijke autoriteiten verder worden bewaard. Het is daarbij essentieel dat het doelbindingsprincipe wordt gevrijwaard, m.a.w. dat 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 Mensenrechten de nodige waarborgen om het beroeps- en bronnengeheim te vrijwaren bij het bewaren en raadplegen van verkeers- en localisatiegegevens⁵⁵.

6. Toezichthoudende instantie(s)

Artikelen:

Memorie van Toelichting: p. 2, laatste alinea (verder op p. 3); p. 3, 3^e en 4^e alinea.

Bijlage bij de MvT: p. 14, punt 4; p. 16, punt 6.

Voorontwerp van Wet: art. 3, §1.

Knelpunten:

De Memorie van Toelichting stelt op p. 2, onderaan, en verder op p. 3 dat individuen recht hebben op inzage in de over hem/haar bewaarde gegevens, alsook recht hebben op een rechtzetting bij eventuele fouten; dit alles onverminderd een klacht bij de

⁵⁴ 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.

⁵⁵ 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.

Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Verder stelt de Memorie van Toelichting op p. 3 dat het BIPT als (min of meer onafhankelijke) toezichthoudende instantie bevoegd is 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 kan leggen. Gezien de 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, zou het een logische en meer verantwoorde keuze zijn om (ook) de Commissie ter Bescherming van de Persoonlijke Levenssfeer bevoegd te maken voor een ambtshalve toezicht op de naleving van een algemene bewaarplicht en niet enkel voor individuele klachtenbehandeling.

De Memorie van Toelichting stelt op p. 3 onderaan dat het Voorontwerp van Wet een extra strafbepaling invoegt in het Strafwetboek betreffende externe en interne hacking waardoor ook de gerechtelijke autoriteiten toezicht kunnen houden op het goede verloop van de bewaring van gegevens. Dit is een positieve ontwikkeling, maar het Voorontwerp van Wet moet ook voorzien wie, op welke wijze en op basis van welke regels kan optreden als onafhankelijke autoriteit, dus niet de gerechtelijke diensten zelf, om ambtshalve toezicht te houden op het rechtmatige beheer van de te bewaren gegevens van zodra zij opgevraagd worden door politie of justitie. Opdat zij deze taak effectief zouden kunnen uitvoeren is het noodzakelijk dat het Voorontwerp van Wet, zoals reeds eerder opgemerkt onder punt 2 en 5, tevens preciseert welke regels van kracht zijn nadat opgevraagde gegevens door de bevoegde gerechtelijke autoriteiten verder worden bewaard.

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. Gezien de 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, zou het een logische en meer verantwoorde keuze zijn om (ook) de Commissie ter Bescherming van de Persoonlijke Levenssfeer bevoegd te maken voor een ambtshalve toezicht op de naleving van een algemene bewaarplicht en niet enkel voor individuele klachtenbehandeling. Ook moet worden nagegaan wie kan optreden als onafhankelijke autoriteit om ambtshalve toezicht te houden op het rechtmatige beheer van de te bewaren gegevens van zodra zij opgevraagd worden door politie of justitie. Hierbij is het tevens noodzakelijk dat het Voorontwerp van Wet, zoals reeds eerder opgemerkt onder punten 2 en 6, preciseert welke regels van kracht zijn nadat opgevraagde gegevens door de bevoegde gerechtelijke autoriteiten verder worden bewaard.

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 geregistreerde 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.

7. Sancties

Artikelen:

Memorie van Toelichting: p. 2, laatste alinea (verder op p. 3); p. 3, 2^e, 3^e en 4^e alinea; p. 8, 1^e-5^e alinea (verder op p. 9).

Bijlage bij de MvT: p.16, punt 6; p. 17, punt 7.

Voorontwerp van Wet: art. 3, §1; art. 4

Knelpunten:

De Memorie van Toelichting verwijst naar de heersende strafrechtelijke en administratieve sancties bij het niet naleven van de geldende regels door de aanbieders van elektronische communicatienetwerken en –diensten of derden.

- 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 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^o 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.
- Een strafrechtelijke sanctie is voorzien d.m.v. artikel 550bis, §1 van het Strafwetboek inzake externe hacking dat een persoon bestraft die zich toegang verleent tot het systeem zonder dat hij hiervoor gemachtigd is. Verzwarende omstandigheden ingeval van bezit, onthulling, verspreiding of gebruik van de gegevens worden bestraft overeenkomstig artikel 550bis, §§3 en 7.
- Een strafrechtelijke sanctie is voorzien d.m.v. artikel 550bis, §2 van het Strafwetboek inzake interne hacking dat een persoon bestraft die, hoewel gemachtigd om toegang te hebben tot het systeem, zijn toegangsbevoegdheid overschrijdt. Verzwarende omstandigheden ingeval van bezit, onthulling, verspreiding of gebruik van de gegevens worden bestraft overeenkomstig artikel 550bis, §§3 en 7.
- Een strafrechtelijke sanctie is voorzien d.m.v. artikel 550ter van het Strafwetboek inzake de persoon die, terwijl hij daartoe niet gerechtigd is, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist of met enig ander technologisch middel de normale aanwending van gegevens in een informaticasysteem verandert.

Het Voorontwerp van Wet voegt in art. 4 een aanvullende strafbepaling toe op de bestaande strafbepalingen betreffende externe en interne hacking.

- Een strafrechtelijke is voorzien door het in te voeren art. 145, §3ter van

de wet van 13 juni 2005 betreffende de elektronische communicatie. Dit artikel bestraft de persoon die naar aanleiding van de uitoefening van zijn bediening, maar buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft, met bedrieglijk opzet of met het oogmerk om te schaden, de gegevens bedoeld in art. 126 WEC op enige manier overneemt, onder zich houdt, of er enig gebruik van maakt, en de persoon die, terwijl hij weet dat de gegevens bekomen zijn door het plegen van dit misdrijf, deze gegevens onder zich houdt, aan een ander persoon onthult of verspreidt, of er enig gebruik van maakt.

Aanbeveling:

De Liga voor Mensenrechten is blij met de verduidelijking inzake de heersende strafrechtelijke en administratieve sancties, maar vraagt dat er naast de hoger vermelde sancties in het Voorontwerp van Wet ook bepalingen worden opgenomen met betrekking tot de geldende regels inzake het verdere informatiebeheer bij gerechtelijke autoriteiten na het opvragen van dergelijke gegevens (cf. punt 2, 5 en 6) alsook sancties vaststelt bij overtredingen hiervan. Deze sancties moeten effectief, evenredig en ontradend zijn conform art. 13 van richtlijn 2006/24/EG.

Ten slotte vraagt de Liga dat er voorzien wordt in een nietigheidssanctie voor het verkregen bewijs wanneer de te bewaren gegevens op basis van art. 126 WEC op een onrechtmatige wijze zijn verkregen. De bijlage bij de Memorie van Toelichting stelt op p. 17 onder punt 7 dat dit momenteel niet voorzien wordt door art. 46bis of 88bis Sv. en dat daardoor de Antigoonleer van het Hof van Cassatie van toepassing is. Aangezien de na te leven vormvoorschriften inzake telefoontap wel op straffe van nietigheid zijn voorgeschreven en verkeers- en locatiegegevens zoals eerder uitgelegd op p. 25, voorlaatste alinea, ook een gelijkwaardig beschermingsniveau verdienen, vraagt de Liga om de nietigheidssanctie uit te breiden naar de toepassing van art. 126 WEC. Dit is tevens een extra argument om de regels inzake het bewaren van gegevens en de regels die de toegang tot deze gegevens bepalen niet op te splitsen (zie punt 4).

<i>8. Evaluaties & rapportage</i>

Artikelen:

Memorie van Toelichting: p. 7, 2^e alinea en p. 9, 2^e alinea.

Voorontwerp van Wet: art. 3, §3-4 en art. 5.

Verslag aan de Koning: p. 8, laatste alinea (verder op p. 9)

Ontwerp van Koninklijk Besluit: art. 12.

Knelpunten:

Artikel 3, §3 en 4, van het Voorontwerp van Wet voorziet in een tweevoudige evaluatie van de algemene bewaarplicht zoals vastgelegd in art. 126 WEC en het bijbehorende KB. Zo stelt de Memorie van Toelichting op p.7, 2^e alinea dat “[...] er twee jaar na de inwerkingtreding van het Koninklijk Besluit een grote eenmalige evaluatie [moet] komen waarbij de verantwoordelijke ministers verslag uitbrengen aan het Parlement over de toepassing van de wet en van het Koninklijk Besluit, en waarbij eventueel inhoudelijke aanbevelingen gedaan kunnen worden omtrent bewaartermijnen, inhoud van de bewaarde gegevens, praktische toepassing, etc. Deze

evaluatie kan in voorkomend geval tot passende initiatieven leiden. Anderzijds voorziet het Voorontwerp van Wet ook in een jaarlijkse rapportage aan het parlement. Het betreft een statistische rapportering zoals die voor een aantal onderzoeksmaatregelen ook is opgenomen in artikel 90decies Sv.” De Liga is zeer tevreden met dit initiatief maar wil er wel op wijzen dat er meer informatie nodig zal zijn dan nu wordt voorzien in art. 3, §3-4, van het Voorontwerp van Wet om een werkelijke evaluatie uit te voeren inzake de deugdelijkheid van de algemene bewaarplicht. Artikel 3, §3, van het Voorontwerp van Wet somt volgende gegevenscategorieën op:

- de gevallen waarin overeenkomstig de toepasselijke wettelijke bepalingen gegevens zijn verstrekt aan de bevoegde autoriteiten;
- de tijd die is verstreken tussen de datum waarop de gegevens zijn bewaard en de datum waarop de bevoegde autoriteiten om de overdracht ervan verzochten;
- de gevallen waarin verzoeken niet konden worden ingewilligd.

Bovenstaande informatiecategorieën peilen echter enkel naar een eventuele noodzaak om de algemene bewaarplicht uit te breiden, maar maken een reële evaluatie van de noodzaak van een algemene bewaarplicht moeilijk. Daartoe zou men immers ook gegevens moeten verzamelen inzake het algemene voorkomen van ernstige criminaliteit in België, uitgesplitst naar type misdrijf, en de oplossingsgraad ervan procentueel vergelijken met de oplossingsgraad van dergelijke misdrijven in de periode voor de introductie van een algemene bewaarplicht. Daarnaast is het ook interessant om, voor zover mogelijk, zicht te hebben op de mate waarin, alsook welke, gegevens die worden bewaard overeenkomstig art. 126 WEC noodzakelijk waren als enigste aanknopingspunt bij het oplossen van ernstige strafzaken. Ten slotte zouden ook misbruiken en, indien bekend de gevolgen ervan, moeten worden gerapporteerd aan het parlement. Eventuele neveneffecten van een algemene bewaarplicht vormen immers ook cruciale informatie bij het evalueren van de maatregel op zijn deugdelijkheid.

Aanbeveling:

De Liga voor Mensenrechten is zeer tevreden met de keuze van een jaarlijkse rapportage van de Minister van justitie aan het parlement alsook met de keuze van een uitgebreide evaluatie twee jaar na de inwerkingtreding van de algemene bewaarplicht. De Liga vreest echter dat een reële evaluatie van de noodzaak van een algemene bewaarplicht moeilijk zal zijn zonder de statistische informatie inzake bijkomende gegevenscategorieën. We denken hierbij o.m. aan:

- het algemene voorkomen van ernstige criminaliteit in België, uitgesplitst naar type misdrijf, waarvan de oplossingsgraad procentueel moet worden vergeleken met de oplossingsgraad van dergelijke misdrijven in de periode voor de introductie van een algemene bewaarplicht;
- de mate waarin, alsook welke, gegevens die worden bewaard overeenkomstig art. 126 WEC noodzakelijk waren als enigste aanknopingspunt bij het oplossen van ernstige strafzaken;
- eventuele misbruiken en, indien bekend, de gevolgen ervan.