LIGA VOOR MENSENRECHTEN

Principieel Standpunt van de Liga voor Mensenrechten inzake een algemene bewaarplicht.

(Maart 2013)

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 openbare 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, ge-sms't, of ge-e-maild 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 afdoend 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.

[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].

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 bij de omzetting van de databewaringsrichtlijn naar Belgisch recht rekening te houden met de evaluaties van de Europese Commissie en burgerrechtenorganisatie European Digital Rights (EDRi) en met de uitspraken van enkele grondwettelijke hoven van lidstaten die de databewaringsrichtlijn ongrondwettig hebben verklaard.[2]

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.

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). 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. Artikel 126 uit de wet op de elektronische communicatie van 2005 stelt dat de telecomoperatoren en internetproviders de verkeersgegevens en identificatiegegevens van gebruikers registeren en

[2] Zie infra punt 6.

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

bewaren, met het oog op de opsporing en beteugeling van strafbare feiten, met het oog op de beteugeling van kwaadwillige oproepen naar de nooddiensten en met het oog op het onderzoek van de ombudsdienst voor telecommunicatie naar de identiteit van de personen die kwaadwillig gebruik hebben gemaakt van een elektronische communicatienetwerk of -dienst.

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*'. Op dit moment heeft de Liga nog geen inzage gehad in het nieuwe voorstel van omzetting van de databewaringsrichtlijn, maar in 2009 was de opvatting van de regering dat deze procedures zouden blijven gelden bij de algemene bewaarplicht en argumenteerde ze op deze manier dat er derhalve geen bijkomend gevaar zou zijn 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, 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 Belgisch 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 hoopt dat wanneer het parlement binnenkort opnieuw debatteert over het feit of een algemene bewaarplicht nuttig dan wel noodzakelijk is, er rekening wordt gehouden met deze opmerkingen en 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 onaanvaardbaar zou vinden mocht dit niet limitatief in de wet worden 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 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 gebruikt.[4] 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 zaak van zangeres Yasmine[5] en natuurlijk de herhaalde kritieken in de jaarrapporten van het Comité P[6]) tot misbruik door derden (bijvoorbeeld de hacker Vendetta die persoonsgegevens van klanten van Belgacom openbaar maakte[7]). Niet alleen is het beangstigend om vast te stellen wat er nu reeds misloopt, nog erger zou het zijn met een algemene

[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=KR2FDEQQ&subsection=3.

[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.

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 misbruik![8]

Dat we dit arrest in de zaak Marper t. het Verenigd Koninkrijk mogen extrapoleren naar de context van verkeers-en locatiegegevens, lijkt gerechtvaardigd gezien de eerdere arresten[9] 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. Op Europees niveau is door EDRi intussen reeds aangetoond dat de algemene bewaarplicht niet 'absoluut noodzakelijk' en niet 'proportioneel' is[10]. Op Belgisch niveau was dit in 2009 onvoldoende 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. In 2009 was het initieel de bedoeling van de Belgische regering om de lijst van de te bewaren gegevens uit te breiden met informatie over bankgegevens. Nu weten we echter niet wat het nieuwe voorstel voorziet aangezien we nog geen inzage hebben gehad in het nieuwe voorstel. Indien dit nog steeds de bedoeling is, moet ook hier de 'absolute noodzaak' ervan worden 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 werden aangehaald in de bijlage van de Memorie van Toelichting bij het voorontwerp van wet van 27 augustus 2009 voldeden dan ook absoluut niet!

[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 en 30566/04).

[10] Zie infra punt 6.

Kortom, het preventief bewaren van eenieders 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 langzaamaan 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 eenieders 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. Communicatiebeginselen 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 interoperationaliteit 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 inlichtingsdoeleinden. 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 rechtvaardigde destijds 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 niets 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 er onvoldoende werd 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 Werkgroep[11] 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 […] het 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*"[12].

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 noodzakelijker vanwege het feit dat terrorisme geen nieuw verschijnsel is en niet als een tijdelijk verschijnsel kan worden aangemerkt. […] Eén 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]"*[13].

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

[11] 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.

[12] 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.

[13] 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/fs/privacy/docs/wpdocs/2001/wp53nl.pdf.

concrete gegevens aantoont waarom zij oordeelt dat een algemene bewaarplicht 'absoluut noodzakelijk' is, ondanks de hoger vermelde tegenargumenten. Het cijfermateriaal en de willekeurige voorbeelden die werden aangehaald in de bijlage van de Memorie van Toelichting bij het voorontwerp van wet van 27 augustus 2009 voldeden hiertoe absoluut niet! Wat immers opvalt, is dat de Memorie van Toelichting steeds verwees naar wat nuttig is voor, of de behoeften zijn van, politie en justitie, maar nooit het bewijs leverde m.b.t. waarom de algemene bewaarplicht 'absoluut noodzakelijk is in onze democratische samenleving'. Het is van groot belang dat de Belgische regering dit kan aantonen want dit punt wordt beoordeeld door het Grondwettelijk Hof indien het ooit tot een procedure zou komen. Wanneer men dit zou willen aantonen, moet men dit doen op basis van bijkomend cijfermateriaal. Aangezien wij nog geen inzage hebben gehad in het nieuwe voorstel, vraagt de Liga of er sindsdien reeds nieuw cijfermateriaal voorhanden is. Indien dit niet het geval is, raden wij de Belgische overheid ten zeerste aan om rekening te houden met het cijfermateriaal uit de rapporten van de Europese Commissie en/of EDRi[14]. Het "Duitse Federale Agentschap voor Criminaliteit" publiceerde in 2011 een politiestudie. Deze studie toonde aan dat de bewaring van communicatiegegevens niet doeltreffend is voor de vervolging van ernstige criminaliteit. De cijfers toonden aan dat in 2009 meer criminele feiten werden geregistreerd door de politie dan in 2007 (16.814 tegenover 15.790). In 2009 werd, met het gebruik van dataretentie, slechts 83.5% van deze feiten opgehelderd tegenover 84.4% in 2007, zonder behulp van dataretentie. De Duitse protestbeweging AK Vorrat stelt dat de contraproductiviteit van de algemene bewaarplicht vooral te wijten is aan het feit dat gebruikers vermijdingsgedrag gaan stellen om te ontsnappen aan de nadelige gevolgen van dataretentie. Draadloos internet, internetcafés, prepaid-telefoonkaarten of publieke telefoons zijn maar enkele voorbeelden van hoe gebruikers anoniem kunnen surfen of bellen. Deze studie doorprikt dan ook de mythe dat dataretentie vooral het strafrechtelijk onderzoek ten goede komt[15]. Dit wordt eveneens geconcludeerd in een studie van het Duitse Max Planck-Instituut voor buitenlands en internationaal strafrecht. Ook hier wordt gesteld dat dataretentie niet leidt tot meer veiligheid voor burgers. De databewaringswetten van Duitsland en Zwitserland (in deze laatste is de wet al tien jaar van kracht) leiden niet tot meer opgeloste ernstige misdrijven.[16]

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, is hier zeker van belang. 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. In 2009 was er onvoldoende

[14] Zie infra punt 6.

[15] Arbeitskreis Vorratsdatenspeicherung, *Serious criminal offences, as defined in sect. 100a stop, in Germany according to police crime statistics*, p. 8: http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf.

[16] Arbeitskreis Vorratsdatenspeicherung, *Criminologists: No "security gap" without blanket communications data retention*, 8 februari 2012: http://www.vorratsdatenspeicherung.de/content/view/534/79/lang,en/.

cijfermateriaal aanwezig, maar ondertussen heeft het dossier lang stilgelegen. De Liga vraagt zich af of dit was om het vereiste cijfermateriaal te verzamelen of is er in die tussentijd niets gebeurd? In geval van dit laatste, zou de Belgische regering een richtlijn omzetten zonder voldoende kennis van zaken.

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 2009).

Indien zou worden beslist om de lijst van de te bewaren gegevens uit te breiden, moet de noodzaak hiervan 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 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. In 2009 werd men echter gedwongen om appelen 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 begreep dat dergelijk statistisch cijfermateriaal toen niet aanwezig was 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 misbruik[17].
- 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 eindgebruiker het zelf onder ogen heeft gekregen, of welke webpagina op die server het betreft.[18]
- 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 prepaidkaarten 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.

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

[18] "Verslag van een mondeling overleg", *Eerste Kamer der Staten-Generaal*, 6 september 2005, http://europapoort.eerstekamer.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf.

Bovendien wordt bij *'data preservation'* het recht op privacy en het vermoeden van onschuld van iedere burger niet miskend.[19]

Ten slotte moeten we ook vaststellen dat de wetsontwerpen die in 2009 werden opgesteld ter realisatie van een algemene bewaarplicht van verkeers- en locatiegegevens technisch ondoordacht waren en in de praktijk vaak onuitvoerbaar leken. De Liga hoopt dat er rekening wordt gehouden met onderstaande argumenten.

- 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 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, Internetcafés 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 waren de wetsontwerpen van 2009 ter realisatie van een algemene bewaarplicht van verkeers- en locatiegegevens in de praktijk vaak onuitvoerbaar. Ook hier hoopt de Liga dat er rekening werd/wordt gehouden met onderstaande argumenten in het nieuwe voorstel.

- 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 filteren.[20]
- 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.

[19] "Common Position of Principle on the Matter of Data Retention", juni 2008, p. 17.
[20] "Verslag van een mondeling overleg", Eerste Kamer der Staten-Generaal, 6 september 2005, http://europapoort.eerstekamer.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf.

- 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 standaardprocedures 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 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 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 trafiek 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 gebruiken.[21] Ook informanten van journalisten zullen bij een algemene bewaarplicht aarzelen om gevoelige informatie door te spelen via telecommunicatie[22].

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 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*".[23] 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 en 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 de 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 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 databewaringsrichtlijn.[24] 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

[21] Kreativrauschen, Data Retention Effectively Changes the Behavior of Citizens in Germany, 4 juni 2008: http://www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/; Arbeitskreis Vorratsdatenspeicherung, *Civil liberties campaigners: Communications Data Retention will be stopped*, 30 juni 2008: http://www.vorratsdatenspeicherung.de/content/view/236/1/lag/en.

[22] '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.

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

[24] Viviane Reding, momenteel Europees commissaris voor Justitie, grondrechten en burgerschap, bevestigde deze gang van zaken tijdens de hoorzitting met de LIBE-commissie op 19/01/2010: http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm;jsessionid=151A805A1AD9823CDDBCE0A7FFB013A1?language=NL.

tegen eventueel misbruik.[25] Verder uitten de Europese Toezichthouder voor Gegevensbescherming en de Artikel 29 Werkgroep hun opmerkingen en aanbevelingen bij dit voorstel voor een richtlijn[26]. 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 men niet aan de kern van de punten die ter discussie werden gesteld door tal van actoren, zoals het Europese Parlement en de toezichthouders voor gegevensbescherming.

De herwerkte tekst werd echter doorgedrukt door de Raad van ministers inzake Justitie en Binnenlandse Zaken[27] 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 Alvaro[28] 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 Raad.[29] 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 de richtlijn 2006/24/EG in bij het Europese Hof van Justitie (zaak C-301/06).[30] Ierland was niet zozeer gekant tegen het principe van een algemene bewaarplicht, maar was van oordeel dat de bewaarplicht op een foutieve rechtsgrond stoelde. Zo oordeelde de Ierse regering dat een bewaarplicht door middel van een kaderbesluit had moeten worden

---

[25] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A6-2005-0365&language=NL.

[26] 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 (COM52005) 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.

[27] Viviane Reding 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=151A805A1AD9823CDDBCE0A7FFB013A1?language=NL.

[28] Van de fractie 'Alliantie van Liberalen en Democraten voor Europa' (ALDE).

[29] 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.

[30] Arbeitskreis Vorratsdatenspeicherung, *Case C-301/06 Ireland v Council of the European Union, European Parliament*, 6 juli 2011: http://www.vorratsdatenspeicherung.de/images/ireland_2006-07-11.pdf.

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*".[31] Ierland riep toen echter geen mensenrechtelijke bezwaren in tegen deze richtlijn bij haar procedure voor het Europese Hof van Justitie. Door een uitspraak in 2010 van het Ierse Grondwettelijke Hof, zal Ierland dit keer wel mensenrechtelijke bezwaren inroepen (zie infra, p. 15).

Naar aanleiding van deze eerste procedure door Ierland voor het Europese Hof van Justitie, schaarde zich op 8 april 2008 een grote en diverse groep van organisaties (waaronder burgerrechtenorganisaties, beroepsverenigingen, internetproviders,…) als 'friends of the Court' achter dit Ierse verzoek tot vernietiging door bijkomende mensenrechtelijke argumenten in te roepen.[32] 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. Het kan echter best dat het Europese Hof van Justitie in de toekomst nogmaals 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 Grondwettelijk Hof van een lidstaat. In Ierland is dit reeds gebeurd. Het Ierse Grondwettelijk Hof stelde in haar arrest van 5 mei 2010 Digital Rights Ireland gelijk en in diezelfde maand werd door Ierland een prejudiciële vraag gesteld aan het Europese Hof van Justitie over de schending van de fundamentele mensenrechten door de databewaringsrichtlijn[33]. De uitspraak werd ten vroegste verwacht in mei 2012, maar tot op heden is dit nog niet gebeurd.[34]

---

[31] Arbeitskreis Vorratsdatenspeicherung, *Case C-301/06 Ireland v Council of the European Union, European Parliament*, 6 juli 2011: http://www.vorratsdatenspeicherung.de/images/ireland_2006-07-11.pdf.

[32] Bewaar je privacy, *Submission concerning the action brought on 6 July 2006, Ireland v Council of the European Union, European Parliament, Case C-301/06*: http://bewaarjeprivacy.be/sites/www.bewaarjeprivacy.be/files/8-04-08_Brief_ngos_aan_ECJ.pdf.

[33] Edri, *Irish Court allows Data Retention Law to be challenged in ECJ*, 19 mei 2010: http://www.edri.org/edrigram/number8.10/data-retention-ireland-ecj.

[34] EDWARD MCGARR, Digital Rights Ireland Data Retention Case, 10 mei 2010: http://www.mcgarrsolicitors.ie/2010/05/10/digital-rights-ireland-date-rention-case/.

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 arrest van 2 maart 2010 van het Federale Grondwettelijk Hof van Duitsland waarin wordt gesteld dat de algemene bewaarplicht voor beperkt gebruik dat gepaard gaat met hoge databeveiliging niet noodzakelijk de Duitse grondwet schendt[35]. Het Duitse Hof stelt wel dat de algemene bewaarplicht een grote beperking inhoudt van het recht op privacy en daarom enkel onder beperkte omstandigheden mag worden toegepast. Een databewaringsperiode van zes maanden is, volgens het Duitse Hof, de absolute bovengrens van wat als proportioneel kan worden beschouwd (paragraaf 215). Verder stelt het Duitse Hof dat data enkel mag worden opgevraagd indien er reeds een vermoeden was van een ernstig misdrijf of bewijs van een gevaar voor de openbare veiligheid. Ook moet het opvragen van data worden verboden in bepaalde gevallen (bijvoorbeeld data inzake emotionele of sociale zaken) die gebaseerd zijn op vertrouwelijkheid. Er moet een transparant overzicht plaatsvinden van gebruik van data. De Grondwettelijke Hoven van Roemenië, Bulgarije en de Tsjechische Republiek oordeelden dat hun respectievelijke nationale wetgeving inzake de algemene bewaarplicht ongrondwettelijk is.[36] Ten slotte bestaat er hevig protest tegen de omzetting van de databewaringsrichtlijn in Oostenrijk.[37]

Enkele opmerkelijke uitspraken in het arrest van het Roemeense Grondwettelijke Hof zijn o.m.:[38]

"*The obligation to retain the data, established by Law 298/2088 [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 through 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*

[35] Edri, German Federal Constitutional Court rejects data retention law, 10 maart 2010: http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional; Bundesverfassungsgericht, Leitsätze zum Urteil des Ersten Senats vom 2. März 2010: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (1BvR 256/08, para 1- 345)

[36] Edri, *Bulgarian Court annuls a vague article of the data retention law*, 17 december 2008 : http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention; Legile Internetului, *Decision no. 1258* from 8 October 2009: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf; Edri, *Czech Constitutional Court rejects data retention legislation*, 6 april 2011: http://www.edri.org/edrigram/number9.7/czech-data-retention-decision.

[37] Edri, *Thousands of Austrians standing up against data retention*, 25 april 2012: http://www.edri.org/edrigram/number10.8/data-retention-austria.

[38] 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.

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 tot 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 exclusing 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 had 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 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 tot 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 tot 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 defense of human rights and fundamental freedoms regarding the guaranteeing of the rights of 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 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. In 2009 gaf de regering aan dat dit dossier veel commotie veroorzaakte in de verschillende Europese lidstaten, maar trok hier toen geen conclusies uit voor de binnenlandse aanpak. De Liga hoopt dat de regering dit keer wel conclusies hieruit trekt.

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 2011.[39] Deze evaluatie werd inmiddels uitgevoerd en wordt kort toegelicht op p. 18-19. 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. Zweden heeft lange tijd geweigerd om de richtlijn om te zetten.[40] In plaats van de implementatieprocedure overhaast te doorlopen, zagen een aantal Zweedse politici de kans om de databewaringsrichtlijn te evalueren op basis van haar consistentie met het Europees Verdrag voor de Rechten van de Mens. Zweden werd door het Europese Hof van Justitie op de vingers getikt voor het niet tijdig omzetten van de richtlijn en het Hof heeft toen ook een dwangsom opgelegd.[41] België zou uit de Zweedse casus lessen kunnen trekken en zich dus evenzeer kunnen opwerpen als een principiële tegenstander van de algemene bewaarplicht. De verdediging van fundamentele mensenrechten op Europees niveau kan immers nooit een beschamende rol zijn! Vandaar dat de burgerrechtenorganisaties EDRi en de Duitse werkgroep inzake databewaring (AK Vorrat) de Europese Commissie reeds op 30 september 2009 hebben gevraagd om de omstreden databewaringsrichtlijn van 2006 in te trekken.

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 in de LIBE-commissie van het Europese Parlement op dinsdagvoormiddag 19/01/2010[42] dat zij met de aanname van het Verdrag van Lissabon op 1 december 2009 en de inwerkingtreding van het Handvest van de Grondrechten van de Europese

[39] http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm:jsessionid=151A805A1AD9823CDDBCE0A7FFB013A1?language=NL.
[40] Edri, Sweden argues that transposing data retention directive is unnecessary, 7 september 2011: http://www.edri.org/edrigram/number9.17/sweden-contests-data-retention-unnecessary.
[41] Europa, Data retention: Commission refers Sweden back to Court for failing to transpose EU legislation, 6 april 2011: http://europa.eu/rapid/press-release_IP-11-409_en.htm?locale=en.
[42] http://www.europarl.europa.eu/hearings//commissioners/getHomePage.htm:jsessionid=151A805A1AD9823CDDBCE0A7FFB013A1?language=NL.

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.

De Europese Commissie heeft op 18 april 2011 haar evaluatie van de databewaringsrichtlijn gepubliceerd[43]. Hierin worden enkele conclusies en aanbevelingen gemaakt waarop de herziening van de databewaringsrichtlijn, voorzien voor 2014, zou moeten steunen. Ten eerste stelt de Commissie dat 1) de algemene bewaarplicht een zeer belangrijke rol speelt in de preventie en vervolging van criminaliteit, 2) de industrie zeker kan zijn van een goed functionerende interne markt en 3) het recht op privacy en de bescherming van persoonlijke gegevens worden gerespecteerd. Ten tweede erkent de Commissie de problematische omzetting van de databewaringsrichtlijn binnen de verschillende lidstaten. Er zijn veel verschillen in de omzetting van de richtlijn tussen de verschillende lidstaten inzake de toegang tot data, de periode van bewaring, de bescherming en beveiliging van de data en statistieken. De Commissie zal de lidstaten blijven helpen bij de omzetting en indien nodig zal ze handhavend optreden. Ten derde erkent de Commissie dat de richtlijn zelf geen garantie stelt dat de bewaarde data worden opgeslagen, opgevraagd en gebruikt volledig volgens het recht op privacy en de bescherming van persoonlijke gegevens. Deze verantwoordelijkheid ligt namelijk bij de lidstaten zelf. Ten vierde erkent de Commissie dat er kosten verbonden zijn aan het in praktijk brengen van de databewaringsrichtlijn en overweegt dan ook verschillende manieren van terugbetaling van de kosten aan de operatoren.

Ten vijfde verzekert de Commissie dat de herziening van de databewaringsrichtlijn het proportionaliteitsprincipe zal nastreven. Uitzonderingen en limieten op de bescherming van persoonlijke gegevens zullen enkel gelden voor zover dit noodzakelijk is. Concreet zal bij de herziening worden nagegaan wat de implicaties voor de effectiviteit en efficiëntie zijn van het strafrechtssysteem en de handhaving, voor de privacy en kosten van operatoren en van een striktere regulering inzake opslag, toegang en gebruik van data. De Commissie stelt dat volgende zaken zullen worden onderzocht: 1) consistentie inzake het doel van de dataretentie en de types van misdrijven waarvoor men toegang krijgt tot de bewaarde data en het gebruik ervan, 2) meer harmonisatie, en indien mogelijk, een verkorting van de periode van databewaring in de verschillende lidstaten, 3) het instellen van een onafhankelijk toezichtsorgaan dat waakt over de verzoeken tot toegang tot de data, de databewaring zelf en de toegang tot de data binnen de verschillende lidstaten, 4) het beperken van het aantal autoriteiten die toegang krijgen tot de data, 5) de vermindering van categorieën van data die moeten worden bewaard, 6) een handleiding voor technische en organisatorische veiligheidsmaatregelen inzake de toegang, de overhandiging en het gebruik van data en 7) de ontwikkeling van een realiseerbaar meetsysteem en verslagprocedures om vergelijkingen van toepassingen en evaluaties te vergemakkelijken. De Commissie wil eveneens overwegen in welke mate '*data preservation'* de algemene bewaarplicht kan aanvullen.

In het licht van de evaluatie van de databewaringsrichtlijn zal de Commissie deze richtlijn herzien. Er zullen een aantal opties worden bedacht in samenwerking met politie en justitie, operatoren en consumentengroepen, databeschermingsautoriteiten en burgerrechtenorganisaties. De Commissie

[43] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC),* 18 April 2011.

zal verder onderzoek voeren naar publieke percepties inzake databewaring en de impact hiervan op het gedrag. De bevindingen die hieruit voortvloeien zullen dan de basis vormen voor het voorstel van de Commissie. De Liga stelt zich de vraag waarom België in allerijl een richtlijn moet omzetten die volgend jaar (2014) wordt herzien door de Europese Unie.

Burgerrechtenorganisatie EDRi (European Digital Rights) heeft op 17 april 2011 (één dag voor het evaluatierapport van de Commissie) een schaduwrapport gepubliceerd over de databewaringsrichtlijn[44]. In dit rapport wordt geconcludeerd dat zowel in dit rapport als in het evaluatierapport van de Commissie wordt aangetoond dat de databewaringsrichtlijn op elk gebied heeft gefaald. De richtlijn respecteert de fundamentele rechten van Europese burgers niet, is mislukt in de harmonisatie van de interne markt en heeft bewezen niet noodzakelijk te zijn in de strijd tegen ernstige criminaliteit. Ten eerste stelt EDRi dat de databewaringsrichtlijn het meeste privacy-schendend instrument is dat ooit werd aangenomen door de EU. EDRi verwijst ook naar verschillende nationale Grondwettelijke Hoven die de nationale databewaringswetten hebben vernietigd. Ten tweede stelt EDRi dat de statistieken van de lidstaten in het evaluatierapport van de Commissie de noodzakelijkheid van de algemene bewaarplicht niet bewijzen. Uit de statistieken blijk dat de algemene bewaarplicht geen effect heeft op de opsporing, het onderzoek en de vervolging van ernstige criminaliteit. In landen zonder een algemene bewaarplicht vindt noch een stijging van criminaliteit plaats, noch een daling in opgeloste zaken. Ook de inwerkingtreding van de algemene bewaarplicht heeft geen significant effect op criminaliteit of het aantal opgeloste zaken.

Ten derde is er geen harmonisatie van de interne markt gecreëerd door de richtlijn. De omzetting in nationale wetgeving verschilt namelijk tussen de meeste lidstaten. Ten vierde zorgen de kosten die de databewaringsrichtlijn met zich meebrengt voor een hindernis op het vrij verkeer van elektronische communicatiediensten en bemoeilijkt het concurrentie tussen de operatoren. Ten vijfde stelt EDRi dat lidstaten de veiligheidsmaatregelen die uit de richtlijn voortvloeien niet volledig respecteren. Een aantal lidstaten heeft geen procedure tot verwijdering van data na de bewaarperiode wat kan leiden tot misbruik van gegevens, wat door de Commissie overigens wordt ontkent.

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 internetproviders.[45] 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 voor telefonie en internet.[46] 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.

---

[44] European Digital Rights, *Shadow evaluation report on the Data Retention Directive (Directive 2006/24/EC),* 17 April 2011.

[45] 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.

[46] 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.

Aangezien het departement Justitie 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.[47]

"De Liga voor Mensenrechten strijdt tegen onrecht en discriminatie. Wij laten van ons horen als er in ons land mensenrechten geschonden worden. In gevangenissen, op het internet, op papier of in het dagelijks leven. De liga streeft naar een samenleving met vrije burgers die eerlijke en gelijke kansen krijgen. Want wij hebben recht op onze Rechten."

Contact: Gebroeders De Smetstraat 75, 9000 Gent – 09/223.07.38 – www.mensenrechten.be

[47] ISPA, Position Data Retention, November 2012, p. 2-4.