

**PRINCIPIEEL STANDPUNT VAN DE LIGA VOOR MENSENRECHTEN INZAKE
EEN ALGEMENE BEWAARPLICHT.
GESPREK KABINET JUSTITIE DO. 6/11/2008**

1. 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. De Liga begrijpt dat het bewaren van verkeers- en locatiegegevens in bepaalde gevallen noodzakelijk kan zijn, maar is niet overtuigd van de noodzaak van een algemene bewaarplicht en het feit dat minder ingrijpende maatregelen, zoals *data preservation* (het bewaren van telecommunicatiegegevens bij bepaalde misdrijven, indien er concrete verdenkingen bestaan en er een machtiging van een onafhankelijke rechter is), niet langer volstaan.

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 langzaamaan naar een autoritaire staatsvorm. Dat niet alleen de Liga voor Mensenrechten het recht op privacy als zeer belangrijk beschouwd, bewijst de verdragsrechtelijke en grondwettelijke verankering van het recht op privacy in artikel 8 van het Europees Verdrag van de Rechten van de Mens, artikels 7 en 8 van het Handvest van de Grondrechten van de Europese Unie en artikel 22 van onze Belgische Grondwet. 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.

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 noodzakelijk en proportioneel is in onze huidige Belgische samenleving en dat minder ingrijpende maatregelen niet langer volstaan.

2. Een algemene bewaarplicht leidt tot de omkering van een belangrijk algemeen rechtsbeginsel, namelijk het vermoeden van onschuld.

Een algemene bewaarplicht maakt van ruim 10 miljoen Belgische inwoners potentiële verdachten. Het preventief registreren van éénieders verkeers- en locatiegegevens leidt ertoe 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. 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.

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

Een algemene bewaarplicht verstoort 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 gebruiken¹. Ook informanten van journalisten zullen bij een algemene bewaarplicht aarzelen om gevoelige informatie door te spelen via telecommunicatie.

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 onbepaalde inbreuk op het beroepsgeheim kan rechtvaardigen²”. 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.

¹ <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/>.

² Grondwettelijk Hof Nr: 10/2008, 23 januari 2008, www.const-court.be.

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

Gegevensbeschermingsautoriteiten (*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 Werkgroep 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*”³.

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 misdaadbesteding 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. [...] 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]*.”⁴.

Concreet verwacht de Liga voor Mensenrechten dat de overheid op basis van concrete gegevens aantoont waarom zij oordeelt dat een algemene bewaarplicht noodzakelijk is, ondanks de hoger vermelde tegenargumenten. Hierbij denken we in eerste instantie aan cijfermateriaal dat het voorkomen van ernstige criminaliteit in België in kaart brengt en op basis waarvan een algemene bewaarplicht gelegitimeerd zou kunnen worden. Daarnaast zouden we ook graag de statistische gegevens ontvangen inzake de mate waarin, en welke, telecommunicatiegegevens door politie en justitie worden opgevraagd bij het oplossen van strafzaken en het al of niet kunnen beantwoorden van deze vraag door de verschillende telecomoperatoren. 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.

³ 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.

⁴ 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.

Een bewaartermijn van 24 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).

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 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 deze belangrijke afweging mag men het langetermijneffect van een algemene bewaarplicht echter nooit uit het oog te verliezen.

| |
|--|
| 5. Een algemene bewaarplicht is inefficiënt. |
|--|

De strijd tegen ernstige criminaliteit kan het bewaren van telecommunicatiegegevens in bepaalde gevallen noodzakelijk maken, 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 misbruik⁵.
- 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

⁵ 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 betreft⁶.

- 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. *Data preservation*, het bewaren van specifieke 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 miskend⁷.

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 expliciete uitbreiding om de algemene bewaarplicht naast openbare elektronische communicatiediensten en -netwerken, ook toe te passen op private elektronische communicatiediensten en -netwerken, zou een enorme administratieve en technische last met zich meebrengen voor bedrijven en publieke instellingen, en mogelijk ook voor vele private burgers. Bovendien zou het een efficiënte en alomvattende controle op aanbieders van elektronische communicatiediensten en -netwerken onmogelijk maken gezien de proliferatie van private elektronische communicatiediensten en -netwerken in onze huidige digitale samenleving en het feit dat deze zich niet moeten laten registreren bij het BIPT.
- 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.

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

⁷ “Common Position of Principle on the Matter of Data Retention”, juni 2008, p. 17.

- 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 filteren⁸.
- 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 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

⁸ "Verslag van een mondeling overleg", *Eerste Kamer der Staten-Generaal*, 6 september 2005, <http://europapooort.eerstekamer.nl/9345000/1/j9vvgv6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

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.

| |
|--|
| 6. Een algemene bewaarplicht brengt enorme kosten met zich mee die hoe dan ook voor rekening van de gewone burger zullen zijn. |
|--|

Een algemene bewaarplicht zal onvermijdelijk leiden tot zware financiële inspanningen voor telecomoperatoren en internetproviders⁹. 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. 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. 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.

⁹ 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.