LIGA VOOR MENSENRECHTEN

Omzetting Dataretentierichtlijn raakt aan de basis van het recht op privacy

(17 juli 2013)

Wat voorafging: **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]

Pertinente verdedigers van de fundamentele rechten en vrijheden van burgers, o.a de Liga's voor Mensenrechten en de Ordes van advocaten, verzetten zich tegen het wetsontwerp. De voornaamste argumenten tegen de omzetting van de richtlijn worden hier nog even op een rijtje gezet.

Privacy als afweerrecht

De voorgenomen omzetting van de Databewaringsrichtlijn won in 2010 nog de allereerste Big Brother Award van de Liga voor Mensenrechten. Geen symbolisch meer betekenisvol gebaar dat dataretentie knaagt aan de fundamenten van het recht op privacy.

Dat de algemene bewaarplicht een inbreuk vormt op het recht op privacy staat onomwonden vast. Dit 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 fundamentele vraag is dan ook 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.

Het debat omtrent databewaring brengt ons *in se* terug tot de vraag naar de betekenis en waarde van artikel 8 EVRM. Dit artikel is oorspronkelijk in het leven geroepen als een afweerrecht tegen buitensporige overheidsbemoeienis. Een overheid die zich in de persoonlijke levenssfeer van haar burgers wil mengen zal dit enkel op basis van gegronde redenen kunnen doen. Die uitzonderingen

[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].

zijn wat de naam aangeeft: slechts uitzonderingen. Overheidstransparantie is essentieel, transparant burgerschap slechts begeerd en daarenboven ondemocratisch. Er moet worden afgestapt van de balanstheorie die veiligheid tegenover vrijheid plaatst. Vrijheid behoort de basis te blijven. Dat recht op vrijheid houdt op zichzelf al voldoende beperkingen in, die garanties moet bieden tegen buitensporig gedrag. Men zou zelfs kunnen oordelen dat een 'recht op veiligheid' impliceert dat een zekere marge van vrijheid behouden blijft.

Verdacht wetgevend parcours

De snelheid waarmee het wetsontwerp door de Kamer wordt gejaagd wekt de indruk dat de regering, en de meeste parlementairen, de omstreden kwestie behandelen alsof het een alledaagse zaak is. Dit is te meer verontrustend in een regime waarin er sprake is – of zou moeten zijn - van parlementaire democratie en scheiding der machten. Dit is op twee vlakken problematisch vanuit het oogpunt van de democratie: enerzijds de verdachte spoed waarmee het wetsontwerp doorheen het wetgevend proces wordt gehaast, anderzijds de al even verdachte weg die hierbij wordt gevolgd, doorheen de Commissies voor Infrastructuur en Financiën.

Vooreerst de verdachte spoed. Op 3 juli is het wetsvoorstel ingediend in de Kamer; op 4 juli werd door Kamervoorzitter Flahaut de urgentie aanvaard; op 9 juli is het wetsontwerp vervolgens besproken in de Commissie Infrastructuur, Verkeer en Overheidsbedrijven. Het is geen geheim dat men de tekst nog graag voor het reces gestemd wil krijgen. De manoeuvres van de regering om een dergelijk belangrijke zaak op enkele dagen door het parlement te jagen tarten alle principes die in een parlementair regime zouden moeten gelden.

Er wordt urgentie gevraagd, hoewel de richtlijn al dateert van 2006 en er zeven jaar de tijd is geweest om de wet te maken. Hoe zwaar weegt het principe van urgentie als diegene die de urgentie vraagt zelf aan de basis ligt van de initiële vertraging? Bovendien wordt een ingrijpende privacybeperkende wet nog snel tijdens de vakantie gestemd, wanneer half (democratisch) België reeds elders vertoeft. Deze week stond hierover nog te lezen in Le Vif: "*Voter un loi si "privaticide" en trois semaines, pendant les vacances, c'est honteux. Démocratiquement, il y a un problème*". Le Vif citeert de woorden van een jurist die opereert in de marge van de Privacycommissie.

De urgentie wordt geargumenteerd met de dreiging van sancties door de E.U. via het Europees Hof van Justitie, in navolging van de Zweedse veroordeling op 30 mei 2013. Een zorgvuldige lezing van het arrest leert echter dat Zweden bij een eerder arrest van 4 februari 2010 door het Europees Hof van Justitie was aangemaand om binnen een bepaalde termijn de richtlijn om te zetten, maar heeft nagelaten dat tijdig te doen. Een dergelijk voorbereidend arrest bestaat er tegen België vooralsnog niet, dus lijkt het argument voor de hoogdringendheid geenszins valabel. Bovendien zou België zich beter afzetten tegen dergelijke vormen van chantage door de E.U. Elk land behoudt immers de soevereiniteit om te weigeren inbreuken op de fundamentele rechten in te voeren. België zou dus beter de houding van de EU aanklagen in plaats van zich er slaafs door te laten leiden. Des te meer omdat heel wat Europese landen, Duitsland voorop, nog steeds geen dergelijke wet hebben, om nagenoeg dezelfde redenen.

Elke mogelijkheid tot ernstig debat wordt als gevolg van de spoed uit de weg gegaan. De parlementairen hebben de tekst amper enkele dagen voor de bespreking in de Commissie gekregen en dit in een zaak die aan fundamentele rechten raakt, die historische bakens verzet op dat terrein,

waar tonnen papier over volgeschreven zijn, waar vier grondwettelijke hoven zich negatief over uitgelaten hebben… Begrijpe, wie begrijpen kan!

Vervolgens de verdachte weg. Het wetsontwerp wordt achtereenvolgens behandeld door de Commissie Infrastructuur en de Commissie Financiën. Niet door de Commissie Justitie of door de verzamelde Commissies, hoewel het wetsontwerp uitgaat van de ministers die voor beide Commissies verantwoordelijk zijn. Dit is onaanvaardbaar voor een materie die in essentie gaat over privacy van alle burgers en niet over de uitbreiding van de infrastructuur van de providers en telecommaatschappijen. Op de site van de Kamer staat als eerste *eurovoc descriptor* de "eerbiediging van het privéleven" aangeduid. Terecht, maar volkomen genegeerd door de regering. Onvermijdelijk rijst de vraag hoeveel parlementairen van de Commissie Infrastructuur een grondige kennis hebben van deze kwestie, van de vernietigingen van de nationale wetten door diverse Europese grondwettelijke hoven, alsook van de standpunten van o.a de Ordes van advocaten en van de Liga's voor Mensenrechten.

<u>Gaat België verder dan nodig?</u>

De richtlijn van 2006 bepaalt dat harmonisatie in de EU wordt nagestreefd op het vlak van "het onderzoeken, opsporen en vervolgen van ernstige criminaliteit" (artikel 1.1 Richtlijn). Er wordt dus niet gesproken over de Staatsveiligheid. Toch maakt België een wetsontwerp dat ook voor de Staatsveiligheid geldt. Maar er zijn meerdere principiële en praktische punten het voorwerp van discussie waard. In 2008 formuleerde de Privacycommissie een ongunstig advies over het toenmalige wetsontwerp tot omzetting, dat voorlag. De tekst vereiste een wijziging op een aanzienlijk aantal punten. Een vergelijking van het huidige wetsontwerp met de adviestekst van 2008 onthult dat niet alle aanpassingen werden doorgevoerd:

- **Gelet op het legaliteitsbeginsel, dienen essentiële elementen inzake de bewaring van gegevens (m.n. de te bewaren gegevens en de bewaarduur) in het voorontwerp te worden bepaald.** De te bewaren gegevens per type dienst en de uitzonderingen betreffende de bewaarduur moeten nog steeds bij KB worden bepaald.
- **Het voorontwerp moet de "zware criminele feiten" verduidelijken waarvoor de bewaarde gegevens kunnen worden gebruikt.** In het wetsontwerp had een limitatieve lijst van misdrijven, in het kader waarvan de data kunnen opgevraagd worden, opgenomen moeten zijn om zo het gebruik te beperken tot ' zware criminaliteit'. Aan deze aanbeveling werd niet voldaan.
- **De toepassing van het voorontwerp en ontwerp KB op de "aanbieders en doorverkopers" dient te worden herbekeken en eventueel moet voor deze categorie in een aparte regeling worden voorzien.** Er bestond in 2008 een akkoord hierover om dit te schrappen maar deze categorie blijkt nu toch te zijn weerhouden in het huidige wetsontwerp.
- **Het bewaren van de gegevens voor "kwaadwillige oproepen naar de nooddiensten en ombudsdienst voor telecommunicatie" moet uit de toepassing van het voorontwerp van wet worden gehaald en in een aparte regeling worden gegoten.** Aan deze aanbeveling werd niet voldaan. Er wordt geargumenteerd dat het bestaan van drie verschillende reglementeringen te complex zou zijn. Dus werd één regeling voor de drie categorieën weerhouden.

- **De toezichthoudende autoriteiten en hun bevoegdheden moeten expliciet worden aangeduid in het voorontwerp.** Aan deze aanbeveling werd niet voldaan.

Er wordt nu geschemerd met het gegeven dat er jaarlijks een rapport zal worden voorgelegd aan het parlement. Dit gaat echter enkel over statistische gegevens en de ervaring met dit soort evaluaties is dat het zuivere *windowdressing* is. Als het parlement nu al niet alert is, boezemt dit weinig vertrouwen in over de kwaliteit van die jaarlijkse rapporten.

Advies van de Raad van State

Ook de Raad van State boog zich over de ontwerptekst en formuleerde haar bedenkingen bij de poging van de regering om de Staatsveiligheid te betrekken in de omzetting van richtlijn 2006/24/EG (richtlijn gegevensbewaring), terwijl het voor de Raad duidelijk is dat de mogelijkheid om gegevensbewaring te regelen in het kader van de nationale veiligheid, landsverdediging of de openbare veiligheid te waarborgen een materie is die wordt geregeld door richtlijn 2002/58/EG (e-privacyrichtlijn). De raad bevestigt dat het oogmerk waarmee zowel krachtens het huidige artikel 126 van de wet van 13 juni 2005 als krachtens het ontworpen artikel 126 gegevens worden bewaard, beduidend verder reikt dan de doelstellingen bepaald in richtlijn 2006/24/EG, te weten “het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten”. De Raad vraagt zich af, gelet op het Europees recht in navolging van het standpunt Europese Commissie hieromtrent, of de beste oplossing om te garanderen dat het Europees recht wordt nageleefd er niet in bestaat twee naast elkaar bestaande regelingen op te zetten: een regeling die richtlijn 2006/24/EG omzet en een andere regeling die op richtlijn 2002/58/EG steunt. Het wetsontwerp negeert ‘om praktische redenen’ deze fundamentele aanbeveling.

Voorts merkt de Raad m.b.t. de overdracht van gegevens krachtens het ontworpen artikel 126 op dat in de ontworpen tekst en de wetsbepalingen niets wordt gezegd over de overheidsinstanties en de precieze regels voor het aanvragen en overdragen van de gegevens. Aangezien het een regeling betreft die strijdig kan zijn met een grondrecht, m.n. de bescherming van de persoonlijke levenssfeer, moet de wetgever zelf de kernpunten van de regeling inzake de overdracht vastleggen.

Fundamentele bezwaren

Ook experts stellen 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.

1. **Een algemene bewaarplicht schendt het recht op privacy**

De algemene bewaarplicht schendt 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 mogelijke verdachte aan het preventieve toezicht van de overheid onderworpen. 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 – het wettelijk vermoeden van onschuld - 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 nochtans geen vrijgeleide om de fundamentele beginselen van de rechtstaat

buitenspel te zetten. Het opvragen van verkeers-en locatiegegevens kan in bepaalde gevallen en in specifieke dossiers zinvol en gerechtvaardigd zijn wanneer het gefocust gebeurt, maar de noodzaak van een algemene bewaarplicht lijkt geenszins bewezen.

Justitie en staatsveiligheid beschikken al over een uitgebreid arsenaal methoden om criminaliteit en bedreigingen voor de staat op te sporen. Deze 'conventionele' methoden laten toe om het gros van de uitdagingen op die terreinen efficiënt te beantwoorden. Het is dus niet zo dat die diensten met lege handen staan. Deze conventionele methoden, gefocust gebruikt op uitgetekende dadergroepen, zijn bij een goed gebruik ervan veel efficiënter dan een massale screening van de bevolking.

Het is nu al 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 (enkel telefoongegevens) en om een veel kortere bewaarperiode (bijvoorbeeld tot het einde van de periode waarop klanten hun factuur bij hun operator of provider kunnen betwisten). De geplande databewaringswet breidt de te bewaren gegevens uit met internetcommunicatie. De inbreuk op onze privacy wordt dus aanzienlijk groter. In onze huidige samenleving is onze wijze van communicatie sterk veranderd en is het gebruik van telecommunicatie steeds meer centraal komen te staan. Het gevaar op een schending van de privacy evolueert uiteraard mee.

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?

De algemene bewaarplicht wordt 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, maar ook de loutere registratie en opslag van deze gegevens houdt reeds een inbreuk in van het recht op privacy en een risico op eventueel misbruik later. Ondertussen voert de Europese Unie immers reeds uitgebreid onderzoek naar de mogelijkheden van "*datamining*".

2. 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.

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 groep 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.

Bovenstaande argumenten vormen een extra waarschuwing bij het omzetten van de databewaringsrichtlijn. Dit betekent dat het des te belangrijker is dat de overheid op basis van concrete gegevens aantoont waarom zij oordeelt dat een algemene bewaarplicht 'absoluut noodzakelijk' is. 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. Indien nog geen nieuw cijfermateriaal voorhanden 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.

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 hulp van dataretentie.

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 die onopgelost bleven wegens een gebrek aan verkeers-en locatiegegevens en in welke mate een omzetting van de databewaringsrichtlijn dit zou kunnen voorkomen.

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).

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

4. De specifieke gevolgen voor het optreden van de staatsveiligheid en de veiligheid van het leger

Het wetsontwerp voorziet dat ook de veiligheidsdiensten de bewaarde data zullen kunnen opvragen. Dit kan voor wat de staatsveiligheid betreft op eenvoudige vraag van het diensthoofd, dit is de adminstrateur-generaal, en dus zonder tussenkomst van de bestuurlijke commissie van magistraten.

Het werkterrein van de staatsveiligheid (artikel 8 van de wet van 30 november 1998) betreft elke individuele of collectieve activiteit ontplooid in het land of vanuit het buiteland die verband kan houden met spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties. Onder extremisme wordt begrepen racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat.

Zonder de noodzaak van de taken van de staatsveiligheid in vraag te stellen wordt opgemerkt dat dit ruime werkterrein, wanneer de data ook door de staatsveiligheid kunnen opgevraagd worden, kan leiden tot een te verregaande controle op de maatschappelijke, sociale, politieke of syndicale bewegingen die zich kritisch opstellen tegenover het beleid. De ruime schaal van controle door buitenlandse veiligheidsdiensten zoals onlangs aan de oppervlakte kwam maakt dat alertheid op dit punt op haar plaats is.

5. De algemene bewaarplicht stuit op veel kritiek binnen Europa

De databewaringsrichtlijn werd destijds bijzonder snel aangenomen, maar zonder de nodige reflectie en overleg. Dit leidde tot felle kritieken en weerstand doorheen heel de Europese Unie.

5.1. Procedures voor het Hof van Justitie en de Grondwettelijke hoven

Het Europese Hof van Justitie werd geïnterpelleerd 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 het Grondwettelijk Hof van Ierland. 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. De zaak werd op 9 juli 2013 voor het Hof gepleit. Een uitspraak wordt ten vroegste eind dit jaar verwacht. België zou er goed aan doen deze uitspraak af te wachten alvorens halsoverkop de richtlijn om te zetten.

Intussen hebben nationale gerechtshoven in verschillende Europese lidstaten zich reeds moeten uitspreken 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. 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. Ten slotte bestaat er hevig protest tegen de omzetting van de databewaringsrichtlijn in Oostenrijk.

5.2. Herziening door de Europese Commissie van de Richtlijn 2006/24/EG

De Europese Commissie heeft op 18 april 2011 haar evaluatie van de databewaringsrichtlijn gepubliceerd. 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 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. Terecht rijst de vraag waarom België in allerijl een richtlijn moet omzetten die volgend jaar (2014) wordt herzien door de Europese Unie.

5.3. Kritieken van de burgerrechtenorganisatie European Digital Rights

Burgerrechtenorganisatie EDRi (European Digital Rights) heeft op 17 april 2011 een schaduwrapport gepubliceerd over de databewaringsrichtlijn. 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 E.U. 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 de 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 ontkend.

Bovenstaande argumenten wijzen op het belang van een fundamenteel debat over de noodzaak en de gevolgen van doorgedreven dataretentie. Met de recente schandalen in de V.S., Frankrijk en nu ook Luxemburg zou bijkomende alertheid van de volksvertegenwoordigers op zijn plaats zijn, maar helaas. Alleen Ecolo en Groen leken kort aan de alarmbel te hebben getrokken. Ook de andere fracties dienen de waarde van het recht op privacy te onderschrijven en te verdedigen. We hoeven ons niet zonder meer neer te leggen bij de evidentie dat databewaring gebeurt. We moeten terug naar de basis: de Staat heeft niet het recht om iedereen voortdurend te controleren, zonder concrete aanleiding. Dataretentie doet net dat!

Indien u graag meer informatie wenst, gelieve contact op te nemen met Caroline De Geest, Beleidsmedewerker Liga voor Mensenrechten, 09/223.07.38 - Caroline@mensenrechten.be of Raf Jespers, lid Liga voor Mensenrechten, advocaat Progress Lawyers Network, auteur 'Big Brother in Europa', 0478/22.71.27 - Raf.jespers@progresslaw.net

"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