

## ‘7 argumenten tegen de Belgische databewaringsplannen’.

De respectievelijke administraties van de Federale Overheidsdienst Binnenlandse Zaken en de Federale Overheidsdienst Justitie, de Federal Computer Crime Unit (FCCU) en het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) onderhandelen momenteel over een wetsontwerp om de Europese richtlijn inzake databewaring<sup>1</sup> om te zetten naar Belgische wetgeving<sup>2</sup>. De tekst wordt verwacht tegen eind maart of april 2008, maar de onderhandelingen zijn tot dan geheim.

Deze Europese richtlijn werd in het leven geroepen om telecomoperatoren en internet providers te verplichten bepaalde gegevens die door hen gegenereerd of verwerkt worden te bewaren. Concreet gaat het om alle gegevens betreffende de betrokken personen, het tijdstip, de locatie, de duur, de omvang en de modaliteit van een telefoongesprek, SMS of e-mailbericht. 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.

De Liga voor Mensenrechten en de Ligue des droits de l’Homme willen erop wijzen dat deze bewaarplicht het recht op privacy van burgers op een significante wijze inperkt. 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.

### 1. Efficiëntie van de maatregel<sup>3</sup>

Niemand zal betwisten dat de strijd tegen ernstige criminaliteit het bewaren van gegevens over het telecommunicatieverkeer noodzakelijk maakt, maar experts, zoals Prof. Hans Franken, zijn van oordeel dat deze richtlijn hiertoe geen effectief instrument is.

Vooreerst zijn er problemen met betrekking tot de bruikbaarheid van de te verzamelen gegevens. Zo zal het vaak voorkomen dat de uiteindelijke gebruiker van telecommunicatiediensten niet met de bewaarde gegevens kan worden geïdentificeerd. Men kan aan de hand van verkeersgegevens bijvoorbeeld achterhalen van welke webserver een machine iets opvraagt, maar niet of de eindgebruiker het zelf onder ogen heeft gekregen, of welke website op die server het betreft. Soms ook gaan meerdere gebruikers schuil achter één IP-adres, en in

---

<sup>1</sup> Op 21 februari 2006 stemde de Raad van de Europese Unie de richtlijn 2006/24/EG “betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG”. Deze richtlijn (COD/2005/0182) is sinds 03/05/2006 van kracht. Zie hiervoor: <http://www.europarl.europa.eu/oeil/file.jsp?id=5275032>.

<sup>2</sup> De richtlijn moest naar nationale wetgeving worden omgezet tegen 15/09/2007 m.b.t. de bewaring van communicatiegegevens inzake vaste en mobiele telefoonnetwerken. Elke lidstaat kan de implementatie van de richtlijn echter uitstellen tot 15/03/2009 m.b.t. de bewaring van communicatiegegevens inzake internet-toegang, internet-telefonie en internet-e-mail indien dit wordt gemeld aan de Raad en de Europese Commissie. Verschillende lidstaten hebben dit reeds (voor verschillende termijnen) gedaan: zo o.m. Nederland, Oostenrijk, het VK, Estland, Cyprus, Griekenland, Luxemburg, Slovenië, Zweden, Litouwen, Letland, Tsjechië, België, Polen, Finland en Duitsland.

<sup>3</sup> Naar: DEENE, J., ‘Bewaren van telecommunicatieverkeer verplicht vanaf juni 2007’, *De Juristenkrant*, nr 126, 22 maart 2006 en VAN DOOREN, (06-09-2005), ‘Verslag van een mondeling overleg’ in Eerste Kamer der Staten-Generaal [WWW]:

<http://europapoort.eerstekamer.nl/9345000/1/j9vvyg6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

de toekomst (met IPv6) zal het fenomeen van het eenmalige IP-adres voorgoed zijn ingang doen waardoor voor iedere verschillende e-mail en het bezoeken van websites automatisch een ander IP-adres wordt toegekend. Aangezien men bovendien een enorme hoeveelheid aan gegevens wenst te bewaren, zal de gezochte informatie in deze enorme databanken niet altijd terug te vinden zijn en dit wordt moeilijker naargelang de termijn waarin men de gegevens wenst te bewaren langer is<sup>4</sup>.

Anderzijds zijn de verkeersgegevens van het internetverkeer die wel zouden kunnen worden vastgelegd volgens Prof. Franken onbruikbaar als bewijsmateriaal omdat ze op eenvoudige wijze vervalst en gemanipuleerd kunnen worden. Volgens onafhankelijke experts, maar ook volgens verschillende verenigingen van Internet Service Providers<sup>5</sup>, zullen criminele individuen die kennis van informatica, of relaties hebben met informatici, de maatregel vrij gemakkelijk kunnen ontlopen. De burger zal er echter een zware prijs voor betalen.

### 2. Reikwijdte van de maatregel<sup>6</sup>

De Europese richtlijn blijft nogal vaag over welke gegevens nu precies bewaard moeten worden. Er mag dan al expliciet verboden worden om gegevens te bewaren waaruit de inhoud van de communicatie kan worden afgeleid, toch 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. Bovendien handelen de netwerken van providers het verkeer van klanten via heel veel verschillende servers af, waardoor de complete verkeersgegevens van een klant alleen kunnen worden bemachtigd door een volledige tap op elke klant te zetten, inclusief op de inhoud. Daaruit moet de provider vervolgens de verkeersgegevens distilleren. Niet alleen gaat dit in tegen het expliciete verbod van de richtlijn, maar zal dit in de praktijk vragen om misbruik. Internet Service Providers vrezen dat zij niet in staat zullen zijn om de integriteit en de veiligheid van al deze gegevens te garanderen<sup>7</sup>.

### 3. Schending van het recht op privacy<sup>8</sup>

Op deze manier is er bijgevolg ook sprake van een schending van het recht op privacy. Een inbreuk op de eerbiediging van de persoonlijke levenssfeer kan op grond van art. 8, tweede lid, van het EVRM enkel gerechtvaardigd zijn wanneer deze beperking bij wet is voorzien en dit 'in een democratische samenleving noodzakelijk' is. Dit noodzaakcriterium wordt in de rechtspraak van het Europees Hof in Straatsburg nader ingevuld aan de hand van de beginselen van proportionaliteit, finaliteit en subsidiariteit.

Prof. Hansen oordeelt terzake dat een redelijke verhouding tussen doel en middelen (proportionaliteitsbeginsel) ontbreekt, omdat de bewaarplicht niet alleen ongeschikt is, maar voor de betrokkenen tevens een onredelijke belasting betekent. Ook wanneer men een uitsplitsing van de opslag over een aantal diensten aanbieders zou realiseren, zal het aantal te

---

<sup>4</sup> [http://www.ispa.be/files/data\\_retention\\_positionpaper.pdf](http://www.ispa.be/files/data_retention_positionpaper.pdf).

<sup>5</sup> *Ibid*, [http://www.euroispa.org/docs/020930eurosispa\\_dretent.pdf](http://www.euroispa.org/docs/020930eurosispa_dretent.pdf).

<sup>6</sup> Naar: VAN DOOREN, (06-09-2005), 'Verslag van een mondeling overleg' in Eerste Kamer der Staten-Generaal [WWW]:

<http://europapoort.eerstekamer.nl/9345000/1/j9vvyg6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

<sup>7</sup> [http://www.euroispa.org/docs/020930eurosispa\\_dretent.pdf](http://www.euroispa.org/docs/020930eurosispa_dretent.pdf),

[http://www.euroispa.org/docs/020930eurosispa\\_dretent.pdf](http://www.euroispa.org/docs/020930eurosispa_dretent.pdf).

<sup>8</sup> Naar: VAN DOOREN, (06-09-2005), 'Verslag van een mondeling overleg' in Eerste Kamer der Staten-Generaal [WWW]:

<http://europapoort.eerstekamer.nl/9345000/1/j9vvyg6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

bewaren gegevens gigantisch blijven en de kosten zodanig toenemen, dat daarmee het criterium van proportionaliteit wordt geschonden. De directe kosten voor het internetgebruik, die natuurlijk aan de consument in rekening zullen worden gebracht, zullen hierdoor substantieel hoger worden, wat de digitale kloof in de samenleving alleen maar zal vergroten<sup>9</sup>. Zelfs al zou de overheid beslissen om een deel van de kosten op zich te nemen, betekent dit nog dat de burger zélf zal moeten betalen (via het belastinggeld) om zich te laten controleren.

Ten slotte argumenteren internet service providers dat de overheid onvoldoende heeft aangetoond dat een algemene bewaarplicht noodzakelijk is voor de veiligheid van de samenleving (finaliteitsbeginsel) en dat bestaande, minder ingrijpende maatregelen, niet langer volstaan (subsidiariteitsbeginsel)<sup>10</sup>.

#### 4. België wil nog verder...

Desalniettemin wordt in België overwogen om, naast de verkeers- en locatiegegevens van het telefonisch en e-mailverkeer, ook het surfgedrag op algemene wijze te registreren. Het omzetten van de Europese richtlijn wordt zo echter misbruikt om lang gevraagde, maar disproportionele en onaanvaardbare maatregelen in te voeren.

#### 5. En er is al zoveel...

Algemeen is er de laatste jaren een klimaat ontstaan waarbij het recht op privacy ondergeschikt wordt verklaard aan het streven naar veiligheid. Vele mensen zien hier geen problemen in omdat ze vaak niet weten wat er kan gebeuren, en reeds gebeurt, met hun gegevens. Zo zijn er recent tal van nieuwe maatregelen ingevoerd in de strijd tegen zware criminaliteit, terreur en illegale migratie. Vermits de respectievelijke gegevens die hierbij worden verzameld steeds meer aan elkaar worden gekoppeld, komt de bescherming van de persoonlijke levenssfeer alsmear meer in het gevaar.

#### 6. Vermoeden van onschuld

Bovenvermelde maatregelen zorgen er bovendien voor dat het democratische principe waarbij éénieder onschuldig wordt geacht tot het tegendeel is bewezen, wordt omgekeerd. De gegevens van iedereen worden immers zonder onderscheid bewaard en veiligheids- en ordehandhavingsdiensten kunnen naar believen grasduinen in deze databanken. Dat we hierbij niet steeds kunnen vertrouwen op de professionaliteit van deze diensten, blijkt ondermeer uit herhaaldelijke vaststellingen van het Comité P<sup>11</sup>.

#### 7. Gegevensbescherming

Dit brengt ons dan ook meteen tot de cruciale vraag welke nationale autoriteiten ‘bevoegd’ geacht worden om deze bewaarde gegevens te raadplegen én onder welke voorwaarden. De bijgehouden informatie is immers van een zeer gevoelig niveau en toegang ertoe moet strikt gereguleerd worden (bijvoorbeeld enkel in het kader van een gerechtelijk onderzoek, op bevel van de onderzoeksrechter). De minister van Binnenlandse Zaken, Patrick Dewael, meldt tijdens een bespreking van het Nationaal Veiligheidsplan 2008-2011 in het parlement echter dat de politiediensten ook pro-actief over dergelijke maatregelen willen beschikken<sup>12</sup>. Daarnaast ijveren deze laatsten ook voor de mogelijkheid om een computer te kunnen

<sup>9</sup> [http://www.ispa.be/files/data\\_retention\\_positionpaper.pdf](http://www.ispa.be/files/data_retention_positionpaper.pdf),  
[http://www.euroispa.org/docs/020930eurosispa\\_dretent.pdf](http://www.euroispa.org/docs/020930eurosispa_dretent.pdf).

<sup>10</sup> (cf. het principe van ‘data preservatie’) [http://www.euroispa.org/docs/020930eurosispa\\_dretent.pdf](http://www.euroispa.org/docs/020930eurosispa_dretent.pdf).

<sup>11</sup> Jaarrapport Comité P 2005: <http://www.comitep.be/nl/nl.html>.

<sup>12</sup> 05-03-2008, ‘Gedachtewisseling over het Nationaal Veiligheidsplan 2008-2011’, p.25.

'hacken'. Gegevens die op een computer opgeslagen zijn, mogen voorlopig immers alleen onderschept worden tijdens de overzending ervan. Evident zijn deze eisen echter niet. Recent vernietigde het hoogste Gerechtshof van Duitsland (het Bundesverfassungsgericht) immers nog een controversiële wet, die een geheime doorlichting van computers toeliet in het kader van de staatsveiligheid en de strijd tegen terreur, vanuit de terechte motivatie dat burgerrechten primeren op veiligheidsbelangen<sup>13</sup>. De opvatting dat de veiligheid zou zijn gediend met het prijsgeven van de privacy is dan ook een onzinnig en gevaarlijk dogma.

Deze fundamentele basisovertuiging vormt duidelijk niet de achterliggende filosofie van de huidige onderhandelingen tussen het BIPT, de FCCU en de betrokken administraties. Het wordt dan ook hoog tijd dat er een democratisch debat komt waarbij de huidige wanverhouding tussen burgerlijke vrijheden enerzijds en veiligheid en ordehandhaving anderzijds fundamenteel wordt besproken.

Concreet vragen de Liga voor Mensenrechten en de Ligue des droits de l'Homme dat het parlement enerzijds zeer strikt invult welke gegevens, door wie, bewaard mogen worden; wie toegang zal hebben tot al deze gegevens, en onder welke voorwaarden; en hoe lang de gegevens bewaard mogen worden. Anderzijds vragen wij 'effectieve', 'evenredige' en 'afschrikkende' sancties bij een overtreding hiervan en uitgebreide bevoegdheden voor de toezichhoudende overheidsinstantie(s). Ten slotte is het ook belangrijk dat de Belgische wetgever de reikwijdte van de Europese richtlijn niet uitbreidt door internet providers te verplichten ook het surfgedrag op algemene wijze te registreren. Er komt in het nationale parlement bijgevolg nog een belangrijke 'tweede ronde' om de Europese richtlijn vorm te geven.

Graag nodigen wij u uit om deze eisen te ondersteunen door het ondertekenen van de petitie die u terugvindt via onderstaande link:

<http://www.mensenrechten.be/main.php?action=start>

Voor bijkomende inlichtingen, kan u steeds contact opnemen met Maartje De Schutter, beleidsmedewerker Liga voor Mensenrechten, op tel.: 09/223.07.38 of per e-mail: [maartje@mensenrechten.be](mailto:maartje@mensenrechten.be).



<sup>13</sup> [http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227\\_1bvr037007.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html).