

I. ALGEMEEN

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^{1,2}”.

Deze richtlijn werd in het leven geroepen om telecomoperatoren en internet providers 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.

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.

II. CONCREET

Deze richtlijn heeft betrekking op de verkeers- en locatiegegevens van natuurlijke personen en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. **Alle gegevens betreffende de betrokken personen, het tijdstip, de locatie, de duur, de omvang en de modaliteit van een telefoongesprek, SMS of e-mailbericht moeten worden bewaard**³. Belangrijke beperking is dat gegevens waaruit de inhoud van de communicatie kan worden achterhaald niet mogen worden bewaard.

De richtlijn laat een keuzevrijheid aan de lidstaten voor de termijn waarbinnen verkeers- en locatiegegevens moeten worden bewaard. De minimale bewaartijd is zes maanden, te rekenen vanaf de datum van de communicatie. Langer dan twee jaar kan bewaring van het telecommunicatieverkeer niet verplicht worden tenzij lidstaten een (in de tijd begrensde) verlenging van de bewaringsperiode kunnen rechtvaardigen, en de Commissie en de overige lidstaten hiervan onverwijld in kennis stellen. De bewaarde gegevens worden aan het einde van de bewaarperiode vernietigd, met uitzondering van geraadpleegde gegevens.

¹ Richtlijn 2002/58/EG “betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie”.

² Deze richtlijn (COD/2005/0182) is sinds 03/05/2006 van kracht. Zie hiervoor: <http://www.europarl.europa.eu/oeil/file.jsp?id=5275032>.

³ Zie hiervoor Richtlijn 2006/24/EG, Artikel 5: ‘Te bewaren categorieën gegevens’, <http://www.europarl.europa.eu/oeil/file.jsp?id=5275032>.

De lidstaten moeten de extra kosten die telecomoperatoren en internet providers maken voor het bewaren, opslaan en doorzenden van gegevens niet vergoeden. Nochtans kunnen de bewaarkosten hoog oplopen. De lidstaten moeten er tevens voor zorgen dat de telecomoperatoren en internet providers een aantal beginselen van gegevensbeveiliging respecteren. **Zo moeten de lidstaten waarborgen inbouwen die garanderen dat de bewaarde gegevens alleen in ‘welbepaalde gevallen’, en in overeenstemming met de nationale wetgeving, aan de ‘bevoegde’ nationale autoriteiten worden verstrekt.** Los van deze (veel te) vage omschrijving, moet de toekomst uitwijzen of de databanken waarin de gegevens worden opgeslagen ook voldoende technisch beveiligd zullen zijn.

In ieder geval **moet elke lidstaat er voor zorgen dat één of meer overheidsinstanties verantwoordelijk worden gesteld voor het monitoren van de veiligheid van de bewaarde gegevens.** Deze instanties moeten **volledig onafhankelijk** werken. **De niet toegestane toegang of overbrenging van gegevens moet beteugeld worden met administratieve of strafrechtelijke sancties die ‘effectief’, ‘evenredig’ en ‘afschrikkend’ zijn.** Het wordt afwachten hoe de Belgische overheid deze sancties concreet invult.

III. KNELPUNTEN

Efficiëntie van de maatregel⁴

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 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 is⁵.

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 Providers⁶, zullen criminele

⁴ 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/j9vvy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

⁵ http://www.ispa.be/files/data_retention_positionpaper.pdf.

⁶ *Ibid*, http://www.euroispa.org/docs/020930eurousispa_dretent.pdf.

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.

Reikwijdte van de maatregel⁷

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**⁸.

Schending van het recht op privacy⁹

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 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 vergroten¹⁰. 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

⁷ Naar: VAN DOOREN, (06-09-2005), 'Verslag van een mondeling overleg' in Eerste Kamer der Staten-Generaal [WWW]:

<http://europapoort.eerstekamer.nl/9345000/1/j9vvygy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

⁸ http://www.euroispa.org/docs/020930eurosispa_dretent.pdf,

http://www.euroispa.org/docs/020930eurosispa_dretent.pdf.

⁹ Naar: VAN DOOREN, (06-09-2005), 'Verslag van een mondeling overleg' in Eerste Kamer der Staten-Generaal [WWW]:

<http://europapoort.eerstekamer.nl/9345000/1/j9vvygy6i0ydh7th/vgbwr4k8ocw2/f=/vh24j3sk6zu8.pdf>.

¹⁰ http://www.ispa.be/files/data_retention_positionpaper.pdf,

http://www.euroispa.org/docs/020930eurosispa_dretent.pdf.

samenleving (finaliteitsbeginsel) en dat bestaande, minder ingrijpende maatregelen, niet langer volstaan (subsidiariteitsbeginsel)¹¹.

België wil nog verder...

In ons land blijft de Europese richtlijn vooralsnog dode letter, omdat ze nog niet is omgezet in een Belgische wet¹². Het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) werkt momenteel aan een wetsontwerp om de richtlijn te implementeren in de Belgische wetgeving. De tekst wordt verwacht tegen eind maart of april 2008, maar de onderhandelingen zijn tot dan geheim. Op sommige vlakken zou men echter verder willen gaan dan de Europese richtlijn vereist. **Naast verkeers- en locatiegegevens van het telefonisch en e-mailverkeer, wordt ook overwogen om het surfgedrag van iedereen te registreren.** Het omzetten van de Europese richtlijn wordt zo echter misbruikt om lang gevraagde, maar disproportionele en onaanvaardbare maatregelen in te voeren.

Het registreren van éénieders surfgedrag kan immers verregaande gevolgen hebben en gebruiksmogelijkheden creëren die veel verder gaan dan het oorspronkelijke doel. Het gevaar bestaat dat **een weinig privacy-vriendelijk wetsontwerp misbruikt wordt om kritische stemmen in de samenleving nauwlettend in het oog te houden en desgevallend monddood te maken.** Op deze manier evolueren we langzaam naar een politiestaat waarbij alle fundamentele verworvenheden van onze parlementaire democratie worden opgeofferd in de strijd tegen zware criminaliteit en terrorisme, die nu net hetzelfde oogmerk hebben...

En er is al zoveel...

De opvattingen over privacy zijn sinds de aanslagen van 11 september 2001 flink veranderd. **Algemeen is er een klimaat ontstaan waarbij het recht op privacy ondergeschikt wordt verklaard aan het streven naar veiligheid.** Vaak gebeurt dit onder de slogan “wie niets te verbergen heeft, heeft niets te vrezen”. **Vele mensen zien hier geen problemen in omdat ze vaak niet weten wat er kan gebeuren, en reeds gebeurt, met hun gegevens.**

De laatste jaren zijn er **tal van nieuwe maatregelen** ingevoerd in de strijd tegen zware criminaliteit, terreur en illegale migratie. Zo is er de introductie van ondermeer RFID-chips in bankbiljetten, het Europese biometrische paspoort met een nationale en op termijn een centrale Europese database, de verschillende veiligheids- en informatiesystemen (zoals SIS I en II, VIS, Eurodac, API en de meer recente plannen zoals PNR en het entry/exit systeem), alsook een explosie van het aantal geplaatste bewakingscamera's. **Vermits men de respectievelijke gegevens die hierbij worden verzameld steeds meer aan elkaar gaat koppelen, komt de bescherming van de persoonlijke levenssfeer alsmaar meer in het gevaar.** De European Data Protection Supervisor is naar aanleiding van de laatste plannen van Frattini dan ook van oordeel dat men beter een evaluatie zou maken van de reeds genomen initiatieven vooraleer men steeds nieuwe maatregelen invoert. Op deze manier

¹¹ (cf. het principe van ‘data preservatie’) http://www.euroispa.org/docs/020930euroispa_dretent.pdf.

¹² 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.

slaagt niemand er immers nog in een overzicht te behouden van alle getroffen maatregelen en is het voor burgers bijzonder moeilijk om zicht te krijgen op het feit of en wanneer ze door deze maatregelen in hun rechten geschonden worden¹³.

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 ordehandhavingdiensten kunnen naar believen grasduinen in deze databanken. Dat we hierbij **niet steeds kunnen vertrouwen op de professionaliteit van deze diensten**, blijkt ondermeer uit de herhaaldelijke vaststellingen van het Comité P. Uit hun onderzoek blijkt namelijk dat politieagenten de politionele of externe gegevensbanken vaak oneigenlijk bevragen¹⁴. Een substantieel deel van de politieagenten kan geen verantwoording geven voor het opzoeken van private personen in dergelijke databanken en vaak is er sprake van een oneigenlijk gebruik van de databanken om private redenen. Wanneer iedere agent toegang zou krijgen tot de verkeers- en locatiegegevens van telecomoperatoren en internet providers, alsook tot de gegevens van éénieters surfgedrag, kunnen dergelijke praktijken reusachtige dimensies aannemen. Zo zou men kunnen nagaan welke websites de buurman, waar men al jaren mee in de clinch ligt, de laatste maanden bezocht heeft; of je schoonbroer een buitenechtelijke relatie heeft op basis van zijn telefoon-, e-mail- en SMS-verkeer; of je ex-partner reeds deelneemt aan datingprogramma's op basis van zijn/haar surfgedrag; of ...?

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 beschikken¹⁵. Daarnaast ijveren deze laatsten ook voor de mogelijkheid om een computer te kunnen 'hacken'. Gegevens die op een computer opgeslagen zijn, mogen voorlopig immers alleen onderschept worden tijdens de verzending 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 veiligheidsbelangen¹⁶. **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 Federal Computer Crime Unit (FCCU) en de betrokken administraties. Men stelt de eis om steeds meer privacy op te offeren in het streven naar meer veiligheid niet ter discussie, maar onderzoekt daarentegen of

13

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2008/EDPS-2008-01-EN_Border%20package.pdf

¹⁴ Jaarrapport Comité P 2005: <http://www.comitep.be/nl/nl.html>.

¹⁵ 05-03-2008, 'Gedachtewisseling over het Nationaal Veiligheidsplan 2008-2011', p.25.

¹⁶ http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

men de weigering om al die internet- en telecomgegevens te bewaren, strafbaar kan stellen, en of het BIPT een gelimiteerde lijst mag opstellen van erkende 'onderaannemers' die de gegevensbewaring voor de telecomoperatoren en internet providers mogen verzorgen. Dit laatste zou immers in strijd kunnen zijn met de Europese regels voor de vrijmaking van de dienstensector.

IV. BESLUIT

De Europese richtlijn vormt reeds een fundamentele aantasting van de privacy waarvan finaliteit, proportionaliteit en subsidiariteit niet zijn aangetoond, en die bovendien gebruiksmogelijkheden creëert die veel verder gaan dan het oorspronkelijke doel. De hoop dat de Belgische wetgever deze richtlijn op een zo privacy-vriendelijke wijze zou implementeren, wordt in de praktijk voorlopig niet gerealiseerd. 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.

Zelfs al dicteert Europa een aantal maatregelen, dan nog is er ruimte voor de lidstaten om die uit te voeren met een zo groot mogelijk respect voor de burgerlijke vrijheden. **Concreet vragen wij 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 toezichthoudende overheidsinstantie(s).** Ten slotte is het belangrijk dat de Belgische wetgever de reikwijdte van de Europese richtlijn niet uitbreidt door internet providers te verplichten ook het surfgedrag te registreren. Er komt in het nationale parlement bijgevolg nog een belangrijke 'tweede ronde' om de Europese richtlijn vorm te geven.

Indien u vragen of bedenkingen heeft, kan u steeds contact opnemen met Maartje De Schutter, beleidsmedewerker Liga voor Mensenrechten, via tel.: 09/223.07.38 of e-mail: maartje@mensenrechten.be.

