Privacyrecht

Recente ontwikkelingen in het privacyrecht 2008-2009

Jos DUMORTIER
gewoon hoogleraar ICRI K.U.Leuven

1. Deze bijdrage bevat een overzicht van de belangrijkste ontwikkelingen op het gebied van de privacyreglementering in Europa en België. Eerst bekijken we wat in de besproken periode in dit domein gebeurde op Europees niveau.

I. Europa

2. Bij de bespreking van de opmerkelijkste trends op Europees niveau maken we een onderscheid tussen wetgeving, rechtspraak en de activiteiten van de toezichthouders in de zogenaamde artikel 29 werkgroep .

§1. Nieuwe wetgeving

3. Op wetgevend vlak moet uiteraard in de eerste plaats de aanpassing van de Europese richtlijnen over privacy en elektronische communicatie vermeld worden. Deze aanpassing kwam eind 2009 tot stand na lange en moeizame onderhandelingen over het zogenaamde "telecom(municatie)pakket".[1]

A. Aanpassing aan de telecommunicatie-kaderrichtlijn

4. Tijdens de onderhandelingen was in het Europees Parlement beroering ontstaan over het Franse "hadopi" wetsontwerp. In dat wetsontwerp werd aan een administratieve autoriteit de mogelijkheid gegeven om internetgebruikers de toegang tot het internet te ontzeggen wanneer zij schuldig werden bevonden aan het illegaal downloaden van auteursrechtlijk beschermde werken.[2] Als reactie daartegen werd op Europees niveau een amendement voorgesteld dat het voor Lid-Staten onmogelijk moest maken de toegang tot het internet te ontzeggen zonder tussenkomst van een rechter. Uiteindelijk werd een compromis aanvaard en een lid toegevoegd aan artikel 1 van de kaderrichtlijn[3] dat als volgt luidt:
" *Maatregelen van de lidstaten betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken eerbiedigen de fundamentele rechten en vrijheden van natuurlijke personen zoals die door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht worden gewaarborgd.*
Maatregelen betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken die die fundamentele rechten en vrijheden kunnen beperken, mogen alleen worden opgelegd indien zij passend, evenredig en noodzakelijk zijn in een democratische samenleving, en zij worden uitgevoerd met inachtneming van adequate procedurele waarborgen overeenkomstig het Europees Verdrag tot bescherming van

1 Publicatieblad van de Europese Unie, L337 van 18 december 2009.
2 Uiteindelijk is dit ontwerp, in gewijzigde vorm, toch goedgekeurd en als wet uitgevaardigd.
3 Ibidem, p. 46

de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht, waaronder doeltreffende rechtsbescherming en eerlijke rechtsbedeling. Deze maatregelen mogen derhalve alleen worden genomen met inachtneming van het beginsel van het vermoeden van onschuld en het recht op een persoonlijke levenssfeer. Een voorafgaande, eerlijke en onpartijdige procedure wordt gegarandeerd, inclusief het recht van de betrokkene of betrokkenen om te worden gehoord, met dien verstande dat voor naar behoren gestaafde spoedeisende gevallen geëigende voorwaarden en procedurele regelingen gelden overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Het recht op een daadwerkelijke en tijdige beroepsmogelijkheid bij een rechterlijke instantie is gegarandeerd.".

B. Aanpassing van de richtlijn over privacy en elektronische communicatie

5. De belangrijkste wijziging in de richtlijn 2002/58/EG is de invoering van de meldingsplicht voor beveiligingsinbreuken. Vooraf moet duidelijk gesteld worden dat richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie) uitsluitend betrekking heeft op openbare elektronischecommunicatienetwerken en –diensten en zij niet van toepassing is op besloten gebruikersgroepen en bedrijfsnetwerken.

1. Meldingsplicht voor beveiligingsinbreuken

6. Aan artikel 3 wordt een derde lid toegevoegd met de volgende tekst:
"*In geval van een inbreuk in verband met persoonsgegevens stelt de aanbieder van openbare elektronischecommunicatiediensten de bevoegde nationale instantiezonder onnodige vertraging in kennis van de inbreuk inverband met persoonsgegevens.*
Indien de inbreuk in verband met persoonsgegevenswaarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens en persoonlijke levenssfeer van een abonnee of een individuele persoon stelt de aanbieder ook de abonnee of de individuele persoon in kwestie onverwijld van de inbreuk in kennis.
In kennisstelling van een betrokken abonnee of individuele persoon van een inbreuk op persoonsgegevens is niet vereist wanneer de aanbieder tot voldoening van de bevoegde instantie heeft aangetoond dat hij de gepaste technische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.
Onverminderd de verplichting van de aanbieder om de betrokken abonnees en de individuele personen in kwestie in kennis te stellen, indien de aanbieder de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan de bevoegde nationale instantie hem, na te hebben bezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk op persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten. De kennisgeving aan de bevoegde nationale instantie bevat bovendien een omschrijving van de gevolgen van de inbreuken van de door de aanbieder voorgestelde of getroffenmaatregelen om de inbreuk in verband met persoonsgegevens aan te pakken.

Afhankelijk van eventuele technische tenuitvoerleggingsmaatregelen overeenkomstig lid 5 kunnen de bevoegde nationale instanties richtsnoeren en, waar nodig, instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreukin verband met persoonsgegevens door aanbieders noodzakelijk is, het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt. Tevens kunnen zij bijhouden of aanbieders aan hun kennisgevingsverplichtingen overeenkomstigdit lid hebben voldaan en, zo niet, dan leggen zij sancties op.

Aanbieders houden een zodanige inventaris bij vaninbreuken op persoonsgegevens, o.m. de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, dat de bevoegde nationale instanties kunnen nagaan of de bepalingen van lid 3 worden nageleefd. De inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

Teneinde een samenhangende tenuitvoerlegging van de in de leden 2, 3 en 4 bedoelde maatregelen te waarborgen, kan de Commissie, na raadpleging van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), de bij artikel 29 van Richtlijn95/46/EG ingestelde werkgroep voor de bescherming van personen in verband met de verwerking van persoonsgegevens en de Europese Toezichthouder voor gegevensbescherming, technische uitvoeringsmaatregelen aannemen in verband met, onder meer, de omstandigheden, het formaat en de procedures die gelden voor de in dit artikel bedoelde informatieverstrekkings- en kennisgevingseisen. DeCommissie betrekt bij het aannemen van die maatregelen alle relevante belanghebbenden, met name om informatie in te winnen over de beste technische eneconomische methoden die beschikbaar zijn voor de tenuitvoerlegging van dit artikel.

Deze maatregelen, die niet-essentiële onderdelen van deze richtlijn beogen te wijzigen door haar aan te vullen, worden vastgesteld volgens de in artikel 14 bis, lid 2, bedoelde regelgevingsprocedure met toetsing."

Ter verduidelijking van wat onder een "inbreuk in verband van persoonsgegevens" moet worden verstaan, wordt van dat begrip de volgende definitie in artikel 2 ingelast: "een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronischecommunicatiedienst inde Gemeenschap". In overweging 61 kan men daarnaast ook lezen dat een inbreuk als schadelijk voor de persoonsgegevens of het privéleven van een abonnee of persoon moet worden beschouwd, wanneer er bijvoorbeeld identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering of aantasting van de reputatie, met betrekking tot de levering van openbare communicatiediensten in de Gemeenschap het gevolg ervan kan zijn. De kennisgeving moet informatie bevatten over de door de aanbieder van de dienst genomen maatregelen om de inbreuk aan te pakken, evenals aanbevelingen voor de be-

trokken abonnee of persoon. Verder wordt in de overwegingen ook vermeld dat "bij de vaststelling van gedetailleerde regels betreffende het formaat en de procedures voor het melden van inbreuken in verband met persoonsgegevens de nodige aandacht moet worden besteed aan de omstandigheden van de inbreuk, onder meer aan de vraag of de persoonsgegevens al dan niet met behulp van adequate technische beschermingsmaatregelen waren beschermd zodat de waarschijnlijkheid van identiteitsfraude of andere vormen van misbreuk in de praktijk kon worden beperkt. Bovendien moet bij dergelijke regels en procedures rekening worden gehouden met de rechtmatige belangen van de rechtshandhavingsautoriteiten in gevallen waarin vroegtijdige melding van incidenten nodeloos het onderzoek naar de omstandigheden van een inbreuk zou hinderen".
Tenslotte wordt in de overwegingen nog eens beklemtoond dat de meldingseisen beperkt zijn tot beveiligingsinbreuken die zich in de sector van de elektronische communicatie voordoen. Er is vooralsnog dus nog een meldingsplicht voor andere sectoren (bijv. banken, overheid, e.a.). Wel wordt door de Europese wetgever de wenselijkheid van een veralgemeende toepassing uitgedrukt en de Commissie wordt opgeroepen om in die richting onderzoek te verrichten.

2. Cookies

7. Een tweede belangrijke wijziging betreft het derde lid van artikel 5 betreffende o.m. het installeren van cookies op de eindapparatuur van elektronischecommunicatiegebruikers. Het nieuwe lid 3 luidt voortaan als volgt: "*De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleindenvan de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van eenuitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert*."
Nieuw in deze bepaling is dat o.m. voor de opslag van cookies de betrokken abonnee of gebruiker toestemming moet verlenen. Tot nu toe was het enkel verplicht de abonnee of gebruiker te informeren en hem het recht te geven om te weigeren dat o.m. een cookie zou worden geïnstalleerd. Betekent dit nu dat in de toekomst voor elke installatie van een cookie de gebruiker in staat moet gesteld worden om expliciet (bijv. door te klikken) daartoe eerst toestemming te verlenen? Uit overweging 66 lijkt men te kunnen afleiden dat dit niet de bedoeling is. In deze overweging wordt namelijk het volgende gesteld: "Het is mogelijk dat derden informatie op de apparatuur van een gebruiker willen installeren of toegang tot reeds opgeslagen informatie willen krijgen, dit om tal van redenen, gaande van wettige handelingen (b.v. bepaalde types cookies) tot ongeoorloofde indringing in de privésfeer (b.v. spyware of virussen). Daarom is het van kapitaal belang dat gebruikers duidelijke en omvattende informatie krijgen wanneer zij een handeling stellen die kan resulteren in een dergelijke

opslag of toegang. De wijze waarop informatie wordt gegeven en een recht van weigering wordt aangeboden moet zo gebruikersvriendelijk mogelijk zijn. Uitzonderingen op de verplichting om informatie te geven en een recht van weigering aan te bieden moeten worden beperkt tot situaties waarbij de technische opslag of toegang strikt noodzakelijk is voor het wettige doel of om het gebruik mogelijk te maken van een specifieke dienst waarom de abonnee of gebruiker heeft verzocht. Wanneer dit technisch mogelijk en doeltreffend is, kan, overeenkomstig de desbetreffende bepalingen van Richtlijn 95/46/EG, de toestemming van de gebruiker met verwerking worden uitgedrukt door gebruik te maken van de desbetreffende instellingen van een browser of een andere toepassing. Deze bepalingen moeten doeltreffender worden afgedwongen via uitgebreide bevoegdheden die aan de desbetreffende nationale instanties worden verleend."
De huidige praktijk, waarbij gebruikers via de instellingen van hun browser ervoor kunnen zorgen dat cookies worden geweigerd, lijkt dus nog steeds in overeenstemming met de nieuwe tekst.

3. Andere wijzigingen en preciseringen

8. Andere wijzigingen in de richtlijn hebben een meer beperkte draagwijdte of bevatten vooral preciseringen die nuttig kunnen zijn voor de interpretatie en de toepassing van de richtlijn.

E-mail marketing

9. Zo wordt in overweging 67 nu uitdrukkelijk bevestigd dat de regels over ongewenste direct marketing via e-mail ook van toepassing zijn op SMS, MMS en andere soortgelijke toepassingen. Ook wordt in de overwegingen uitdrukkelijk gesteld dat internet service providers over de mogelijkheid moeten beschikken om een rechtsvordering in te leiden tegen spammers en zo de belangen van hun klanten als onderdeel van hun eigen rechtmatige ondernemingsbelangen, moeten kunnen verdedigen. Tenslotte zijn er kleine tekstaanpassingen waardoor bijvoorbeeld verduidelijkt wordt dat de toestemming of het verzet van gebruikers met betrekking tot het ontvangen van direct marketing via e-mail steeds kosteloos moeten zijn, of dat de eisen inzake commerciële communicatie die door de richtlijn 2000/31/EG over de elektronische handel worden opgelegd (bijv. duidelijke vermelding dat het om een marketingbericht gaat, duidelijke identificatie van degene namens wie het bericht wordt verstuurd, e.a.), ook gelden voor direct marketing via e-mail. Helaas blijven een aantal discussiepunten, bijv. met betrekking tot de reikwijdte van het begrip "direct marketing" in deze context, onopgelost.[4]

4 Zie hierover H. GRAUX & J. DUMORTIER, Privacywetgeving in de praktijk, Kortrijk, UGA, 2009, p. 342, in het bijzonder voetnoot 492.

RFID

10. Lange tijd was sprake om in de richtlijn een bepaling in te voeren over het gebruik van RFID. Uiteindelijk heeft de Europese wetgever zich beperkt tot enkele kleine tekstaanpassingen die ervoor moeten zorgen dat, wanneer RFID wordt gebruikt om persoonsgegevens te verzamelen die vervolgens worden verstuurd via openbare communicatienetwerken (het internet bijvoorbeeld) of verwerkt in het kader van elektronische-communicatiediensten, de bepalingen van de richtlijn op het gehele proces van toepassing zijn. Overweging 56 zegt hierover het volgende: "De technologische vooruitgang maakt de ontwikkeling mogelijk van nieuwe toepassingen die zijn gebaseerd op systemen voor gegevensverzameling en identificatie, zoals contactloze radiofrequentiesystemen. RFID-systemen (Radio Frequency Identification Devices) bijvoorbeeld maken gebruik van radiofrequenties om gegevens op te vangen van op unieke wijze geïdentificeerde RFI-chips, gegevens die vervolgens kunnen worden verstuurd over bestaande communicatienetwerken. Een breed gebruik van dergelijke technologieën kan aanzienlijke economische en maatschappelijke baten opleveren en kan dus een krachtige bijdrage leveren voor de interne markt, op voorwaarde dat hun gebruik aanvaardbaar is voor de burger. Om dat doel te bewerkstelligen, is het noodzakelijk al de fundamentele rechten van het individu, inclusief het recht op privacy en gegevensbescherming, te waarborgen. Wanneer dergelijke systemen aan openbare elektronische communicatienetwerken worden gekoppeld of gebruik maken van elektronische-communicatiediensten als basisinfrastructuur gelden de relevante bepalingen van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), inclusief die in verband met veiligheids-, verkeers- en locatiegegevens en vertrouwelijkheid".

§2. Andere nieuwe Europese regelgeving

11. Van de andere Europese wetgeving die in de periode 2008-2009 werd uitgevaardigd, moet vooral het kaderbesluit over de verwerking van persoonsgegevens in het kader van politiële en justitiële samenwerking in strafzakenvermeld worden. Daarnaast werden ook belangrijke verdragen met de Verenigde S taten over de verstrekking van persoonsgegevens in het kader van o.m. de strijd tegen het terrorisme.

A. Kaderbesluit over verwerking van persoonsgegevens bij politiële en justitiële samenwerking

12. Dit kaderbesluit[5] is het eerste horizontale regelgevend instrument over de verwerking van persoonsgegevens door politie en gerechtelijke autoriteiten.

5 Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, Pb. EU L350 van 30 december 2008.

13. Het kende een lange voorgeschiedenis vooraleer het uiteindelijk werd aanvaard. Een aantal amendementen die in het Europees Parlement waren voorgesteld, zoals verwijzingen naar het Verdrag 108 van de Raad van Europa, het verbreden van het toepassingsgebied tot verwerkingen binnen de grenzen van een Lid-Staat of de oprichting van een werkgroep (naar het voorbeeld van de artikel 29 werkgroep), warden uiteindelijk niet aanvaard.
Het kaderbesluit is dus enkel toepasselijk op grensoverschrijdende uitwisselingen van persoonsgegevens in het kader van politiële en gerechtelijke samenwerking. Het bevat ook bepalingen over de transfer van persoonsgegevens naar derde landen en naar private partijen in de Lid-Staten.
Het kaderbesluitmoet worden omgezet door de Lid-Staten tegen 27 november 2010. Daarbij moet in elke Lid-Staat ook een autoriteit aangeduid worden die verantwoordelijk zal zijn voor de opvolging en het toezicht.

B. SIS-besluit

14. De Raad van de Europese Unie nam op 23 juni 2008 immers het zogenaamde SIS-besluit[6], dat gelijklopende bepalingen integreert in de EU-regelgeving als deel van de Europese politiële en justitiële samenwerking in strafzaken (de zogenaamde derde pijler van het EU-Verdrag).
De lidstaten worden door dit besluit verplicht om op nationaal niveau een databank te creëren van DNA-profielen voor bepaalde types van misdrijven[7]. Wanneer zij grensoverschrijdend vergelijkend onderzoek willen verrichten zullen zij een DNA-profiel verzenden naar het VIS, dat naar gelijkenissen zal zoeken in de deelnemende landen. Ingeval van een positief resultaat kunnen de gegevens van het gelijkende profiel worden opgevraagd met behulp van nog op te richten nationale contactpunten. Ook gegevens over vingerafdrukken en kentekenregistratie zullen uitwisselbaar worden, zoals dit momenteel ook al mogelijk is voor asielzoekers via het zogenaamde Eurodac-systeem8.

---

6 Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit, *Publ.L.* 210/1, 6 augustus 2008.

7 Indien dit in het finale kaderbesluit zo blijkt, dan staat dit op gespannen voet met het beschikbaarheidsbeginsel, dat immers enkel de uitwisseling van reeds beschikbare gegevens viseert, en dat niet zou mogen impliceren dat nieuwe gegevensverzamelingen moeten worden aangelegd.

8 Het Eurodac-systeem bestaat uiot een geautomatiseerde centrale gegevensbank en elektronische middelen voor de overdracht van gegevens tussen de lidstaten en de centrale gegevensbank, waarin de lidstaten vingerafdrukken opslaan van asielzoekers die aan de grenzen van de EU worden tegengehouden. Met behulp van deze vingerafdrukken kunnen de lidstaten dubbele asielaanvragen onder een valse identiteit opsporen, en gemakkelijker het land bepalen dat bevoegd is voor het afhandelen van de asielaanvraag. De juridische basis voor Eurodac is Verordening (EG) nr. 2725/2000 van de Raad van 11 december 2000 betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van de Overeenkomst van Dublin, *Publ. L.* 316 van 15 december 2000, blz. 1–10; zie ook http://europa.eu/scadplus/leg/nl/lvb/l33081.htm;

C. Overdracht van persoonsgegevens aan de Verenigde Staten

15. Op 30 november 2009 werd door de Europese Raad van Justitieministers een overeenkomst gesloten met de regering van de Verenigde Staten over de overdracht van bankgegevens in het kader van het Amerikaanse "Terrorist Finance Tracking Program (TFTP).[9] Als gevolg van deze overeenkomst kan de Amerikaanse regering gegevens over betalingsberichten opvragen voor het traceren van terrorismefinanciering. De gegevens worden door de Amerikaanse regering aangevraagd bij de centrale autoriteit van de Lid-Staat waar de beoogde operator gevestigd is die de de gevraagde gegevens kan verstrekken. Het kan daarbij ook gaan over betalingsberichten binnen de grenzen van één Lid-Staat.
Eerder was Europees protest gerezen tegen het feit dat de Amerikaanse regering gegevens over betalingsberichten had opgevraagd aan SWIFT. De gegevens hadden betrekking op Europese burgers maar werden door SWIFT in de Verenigde Staten verwerkt. Door de overeenkomst van 30 november 2009 is de discussie over de SWIFT-zaak grotendeels achterhaald.
Bezorgdheid is recent ook ontstaan over de toepassing van een andere overeenkomst tussen Europa en de Verenigde Staten, namelijk over de overdracht van passagiersgegevens. Deze overeenkomst dateert al van februari 2007 maar werd in juli 2008 herzien en geactualiseerd.[10] Ze werd in België geratificeerd bij wet van 30 november 2009.[11]

D. Modelclausules en Binding Corporate Rules

16. Overeenkomstig artikel 26, lid 2 van de Europese dataprotectierichtlijn 95/46/EG kunnen Lid-Staten de overdracht van persoonsgegevens naar derde landen buiten de Europese Unie, niettegenstaande het feit dat het derde land geen passend beschermingsniveau waarborgt op het gebied van de bescherming van persoonsgegevens, toch toelaten wanneer de verantwoordelijke voor de verwerking zelf voor voldoende waarborgen zorgt. In het bijzonder (maar niet uitsluitend) kunnen deze waarborgen resulteren uit aangepaste contractuele clausules. Met het oog op dat laatste kan de Europese Commissie in een be-

9 Besluit 2010/16/GBVB/JBZ van de Raad van 30 november 2009 houdende ondertekening, namens de Europese Unie, van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het betalingsberichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering, Publ. L8 van 13 januari 2010.

10 Zie verder http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp151_nl.pdf

11 Wet van 30 november 2009 houdende instemming met de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het Ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika (PNR-Overeenkomst 2007), gedaan te Brussel op 23 juli 2007 en te Washington op 26 juli 2007, B.S., 29/12/2009.

sluit modelclausules vaststellen die volgens haar voldoende waarborgen bieden. In dat geval moeten de Lid-Staten deze clausules aanvaarden.
De Europese Commissie heeft tot dusver modelclausules uitgevaardigd voor de transfers van persoonsgegevens tussen twee (of meer) verantwoordelijken en voor transfers tussen één of meer verantwoordelijken en één of meer verwerkers.[12] Deze laatste modelclausules zijn al sinds enige tijd het voorwerp van kritiek omdat ze geen adequate oplossing zouden bieden voor gevallen waarin gegevens worden geëxporteerd naar een verwerker die ze vervolgens op zijn beurt weer overdraagt naar één of meer sub-verwerkers. De Europese Commissie heeft een voorstel tot amendering van de modelclausules uitgewerkt om aan dergelijke situaties het hoofd te bieden maar tot dusver zijn deze wijzigingen nog niet uitgevaardigd.
Naast contractuele clausules kunnen Lidstaten, ingevolge artikel 26, lid 2, ook andere waarborgen aanvaarden om transfers naar derde landen zonder passend beschermingsniveau toe te laten. Eén van de mogelijkheden bestaat in het opstellen en aanvaarden van zogenaamde "binding corporate rules".[13] Vooral voor internationale bedrijven die in Europa gevestigd zijn en naar verschillende landen buiten Europa gegevens over personeel of klanten willen kunnen doorsturen, kunnen dergelijke "binding corporate rules" een oplossing bieden. Er wordt dan één document opgesteld waarin passende waarborgen worden aangegeven voor export naar derde landen. Vervolgens wordt dit document door alle vestigingen ondertekend.
In sommige Lid-Staten kunnen dergelijke documenten voorgelegd worden aan de nationale privacycommissie en volstaat goedkeuring van deze laatste om ze voor deze Lid-Staat in werking te doen treden. In België is dat helaas niet het geval omdat volgens de wet van 8 december 1992 "passende waarborgen" enkel via een koninklijk besluit aanvaard kunnen worden.
De laatste jaren zijn in de schoot van de artikel 29 werkgroep belangrijke inspanningen geleverd om de goedkeuring van "binding corporate rules" vlotter te doen verlopen. Vooral voor ondernemingen die in talrijke Lid-Staten gevestigd zijn, is het een hele klus om de goedkeuring voor hun document te verkrijgen in al die Lid-Staten. Daaraan is ten dele verholpen via een dubbele weg. Aan de ene kant is binnen de artikel 29 werkgroep aan een consensus gewerkt over hoe dergelijke "binding corporate rules" er moeten uitzien. Aan de andere kant wordt gestreefd naar een systeem van wederzijdse erkenning: wanneer goedkeuring voor de voorgestelde "binding corporate rules" wordt verkregen in één Lid-Staat zou dan die goedkeuring automatisch ook gelden voor andere Lid-Staten. Uiteraard kan dergelijk systeem van wederzijdse erkenning enkel werken tussen Lid-Staten waar de privacycommissie over de nodige bevoegdheden beschikt om "binding corporate rules" goed te keuren. Tot dusver zijn een twaalftal Lid-Staten tot het systeem van wederzijdse erkenning toegetreden. Voor België is toetreding, zoals reeds vermeld, helaas onmogelijk.
Vaak worden "binding corporate rules" ten onrechte aanzien als een soort privacygedragscode voor multinationale ondernemingen. Bij aanvaarding van deze regels zouden deze ondernemingen dan kunnen volstaan met de correcte

12 Zie http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm
13 Zie o.m. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf

toepassing ervan om in regel te zijn met de Europese en nationale privacywetgeving. Dat berust echter op een misverstand. De goedkeuring van "binding corporate rules" door privacycommissies van de verschillende Lid-Staten waarin de internationale onderneming is gevestigd, levert eigenlijk niet meer op dan een bundel van exportlicenties. Voor elk van de betrokken Lid-Staten wordt een toelating afgeleverd om een set van transfers naar één of meer derde landen door te voeren.

§3. Rechtspraak

17. Bij het overzicht van de belangrijkste Europese rechtspraak worden hierna achtereenvolgens het Europese Hof van de Rechten van de Mens en het Hof van Justitie van de Europese Unie bekeken.

A. Europees Hof van de Rechten van de Mens

18. Drie arresten die door het Europese Hof van de Rechten van de Mens in de hier behandelde periode 2008-2009 werden geveld, herinneren ons eraan dat bij de verwerking van persoonsgegevens niet enkel de bepalingen van de dataprotectiewetgeving nageleefd moeten worden maar deze verwerking ook getoetst moet worden aan artikel 8 van het EVRM.

1. I v. Finland: verplichte registratie en bewaring van toegangsgegevens

19. Het Europese Hof van de Rechten van de Mens (EHRM) in Straatsburg heeft op 17 juli 2008 een arrest geveld dat belangrijke gevolgen heeft voor organisaties die gevoelige persoonsgegevens verwerken.[14] De zaak ging over een verpleegster die in een polykliniek in Finland werkte. In dezelfde kliniek was zij voordien ook als patient geweest en daarbij was vastgesteld dat zij een HIV- besmetting had opgelopen.
Na verloop van tijd merkte de verpleegster dat haar collega's blijkbaar op de hoogte waren van haar ziekte. Dat was niet abnormaal omdat op dat ogenblik al het verzorgend personeel in de kliniek toegang had tot het patientenregister. In dat register stond o.m. informatie over de vastgestelde diagnose en over de behandelende geneesheer. Toen de verpleegster haar vermoeden meedeelde aan haar arts, werd het systeem veranderd en werd toegang beperkt tot de gegevens over patienten die men zelf verzorgde. De verpleegster zelf werd onder een valse naam geregistreerd en zij kreeg ook een nieuw sociaal zekerheidsnummer. Haar contract als verpleegster werd echter door de kliniek niet hernieuwd.
Na het einde van haar tewerkstelling legde zij klacht neer bij het bevoegde bestuur met het verzoek na te gaan wie haar vertrouwelijke patientengegevens in het register had geconsulteerd. De directeur van de kliniek werd opgeroepen maar die verklaarde dat het niet mogelijk was om dat te achterhalen. Enkel de

14 http://www.cl.cam.ac.uk/~rja14/Papers/echr-finland.pdf

laatste vijf consultaties van het patientendossier bleven in het archief bewaard. Bovendien stonden die consultaties geregistreerd op de naam van de dienst en niet op naam van de persoon die in die dienst werkte. Deze informatie werd overigens niet bewaard bij de archivering van het dossier.
Als gevolg daarvan bleef de klacht van de verpleegster zonder gevolg. De bevoegde administratie stelde vast dat de personen die de vertrouwelijke informatie hadden ingekeken en verspreid, niet geïdentificeerd konden worden. De administratie was echter van mening dat de kliniek in de toekomst elke consultatie van een patientendossier zou moeten registreren. De registratie zou bovendien op naam van de persoon vastgelegd moeten worden om individuele verantwoording mogelijk te maken. De kliniek ging op deze aanbevelingen in maar voor de betrokken verpleegster kwam deze maatregel natuurlijk te laat.
Daarom stapte de verpleegster naar de rechtbank. Zowel in eerste aanleg als in hoger beroep kreeg zij echter ongelijk. De rechters geloofden haar weliswaar wanneer zij vertelde hoe haar collega's via allerlei hints en opmerkingen duidelijk maakten dat zij op de hoogte waren van haar infectie. Zij vonden echter helaas geen sterke bewijzen dat iemand onrechtmatig het patientendossier had geconsulteerd.
Uiteindelijk werd de zaak dus voorgelegd aan het Europees Hof van de Rechten van de Mens. De verpleegster dagvaardde haar land – Finland – wegens schending van het recht op respect voor haar privacy. De kliniek waar zij gewerkt had was immers een publieke instelling, indirect onder de verantwoordelijkheid van de Finse Staat.
In haar arrest beklemtoont het Europees Hof dat het recht op privacy niet enkel betekent dat de Staat zich niet onrechtmatig mag mengen in het privéleven van haar burgers. Het houdt ook in dat de Staat positieve maatregelen moet nemen om ervoor te zorgen dat burgers elkaars privacy respecteren. De klacht van de verpleegster kwam er eigenlijk op neer dat de Staat hiervoor onvoldoende maatregelen had genomen.
De verpleegster haalde finaal toch nog haar slag thuis. Volgens het Hof kon zij onmogelijk aantonen dat iemand onrechtmatig haar dossier had geconsulteerd. Daarvoor ontbraken de nodige bewijzen. Het was echter de verantwoordelijkheid van de kliniek ervoor te zorgen dat deze bewijzen voorhanden waren. Vermits deze gegevens niet werden gelogd, was het patientendossier ontoereikend beschermd. Het Europees Hof veroordeelde daarom Finland omdat het onvoldoende de privacy van één van haar burgers had beschermd.
De belangrijkste passage van het arrest is deze waar het Hof opmerkt dat het louter voorzien in een wettelijke mogelijkheid om schadevergoeding te bekomen bij een onrechtmatige lek van persoonsgegevens, niet genoeg is. "Wat in dit verband wordt vereist is praktische en effectieve bescherming om elke mogelijkheid tot ongerechtvaardigde toegang uit te sluiten".
De draagwijdte van deze beslissing reikt ongetwijfeld verder dan de medische sector. Ook voor andere vertrouwelijke persoonsgegevens lijkt het voortaan noodzakelijk om van elke individuele toegang tot de databank een spoor te bewaren.

2. Marper v. Verenigd Koninkrijk: grenzen aan veralgemeende opslag van vingerafdrukken

20. In een interessant arrest van 4 december 2008 heeft het Europees Hof van de Rechten van de Mens zich uitgesproken over de oprichten van databanken met gegevens over DNA en vingerafdrukken van onschuldige burgers. Het Hof oordeelde dat dergelijke oprichting strijdig is met artikel 8 van het EVRM. [15]
De beslissing handelt over twee databanken met DNA-gegevens en vingerafdrukken die in het Verenigd Koninkrijk gebruikt worden in het kader van de misdaadbestrijding. In het specifieke geval ging het over twee personen (Michael Marper en een tweede persoon die enkel aangeduid is als S.) die in 2001 waren gearresteerd in afzonderlijke incidenten en vervolgens werden geregistreerd in de betrokken databanken. De zaak van Marper werd echter geseponeerd en S. werd vrijgesproken. Toch werden hun gegevens in de databanken bewaard met het oog op onderzoek naar eventuele toekomstige misdrijven. Volgens the Times bevatten de databanken gegevens over 5, 1 personen waarvan naar schatting 800.000 nooit werden veroordeeld.
Databanken met DNA-gegevens en vingerafdrukken bestaan in vrijwel alle Lid-Staten (ook in België) maar de Europese rechters merkten op dat "*the United Kingdom is the only member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued*."
Het Hof oordeelde dat de willekeurige registratie van DNA profielen en vingerafdrukken van personen die zijn vrijgesproken van misdrijven of waarvan de aanklachten zijn geseponeerd, een schending uitmaakt van hun fundamenteel recht op respect voor de persoonlijke levenssfeer. Meer restrictieve oplossingen daarentegen, zoals in Schotland waar DNA-profielen van niet-veroordeelde personen enkel worden bijgehouden indien het gaat over volwassenen die werden beschuldigd van geweld of sexuele misdrijven en dan nog beperkt tot een periode van drie jaar, werden niet a priori onrechtmatig bevonden.

3. Reklos en Davourlis v. Griekenland: geen babyfoto's zonder toestemming van ouders

21. Een derde beslissing die in dit kader vermeld moet worden, werd in januari 2009 door het Europees Hof van de Rechten van de Mens geveld in een zaak over babyfoto's.16 Het Hof diende te oordelen over een klacht van de ouders van een Griekse baby, Anastasios, die kort na zijn geboorte om gezondheidsredenen in een steriele omgeving was geplaatst, met uitsluitend toegang voor de zorgverstrekkende geneesheren en verpleegkundigen. Enige tijd later ontdekten de ouders echter dat een commerciële fotograaf eveneens toegang had gekregen tot de eenheid om foto's te maken van het kind met de bedoeling die

15 Zaak Marper & S. v. Verenigd Koninkrijk, Verzoeken 30562/04 e, 30566/04.
16 EHRM, Arrest van 15 januari 2009 in de zaak Reklos en Davourlis tegen Griekenland. (enkel in het Engels);

nadien aan de ouders te koop aan te bieden. In het betrokken ziekenhuis was deze praktijk gebruikelijk.
De ouders tekenden verzet aan tegen het louter om commerciële motieven toelaten van een vreemde persoon in de steriele omgeving waar hun kind vertoefde. Zij eisten de negatieven van de genomen foto's maar dat werd hen geweigerd. Daarop stapten zijn naar de Griekse rechtbank maar kregen daarvan ongelijk. Dit bracht hen uiteindelijk bij het Europees Hof in Straatsburg.
Het Hof ging akkoord met de stelling van de ouders dat het fundamenteel recht op respect voor de persoonlijke levenssfeer ook geldt voor een pasgeborene. De Europese rechters beklemtonen in hun beslissing dat het recht op identiteit een kernonderdeel vormt van de persoonlijke levenssfeer en dat een foto een belangrijk element vormt van de persoonlijkheid. Volgens het Hof had, vooraleer foto's te mogen nemen van het kind, vooraf minstens de toestemming van de ouders gevraagd moeten worden, ook al was er geen sprake van publicatie van de foto's of enig ander gebruik.

B. Hof van Justitie van de Europese Gemeenschap

1. Huber: wanneer is een verwerking "noodzakelijk"?

22. In een arrest van 16 december 2008 oordeelde het Europese Hof van Justitie over het Duitse "Ausländerzentralregister" (AZR).[17] In dat register worden persoonsgegevens opgenomen over o.m. personen van buitenlandse nationaliteit die minimaal drie maanden in Duitsland verblijven. De gegevens zijn vrij gedetailleerd en bevatten naast de gewone identificatiegegevens ook informatie over inkomende en uitgaande reizen naar en van het Duitse grondgebied, eventuele gegevens van de arbeidsbemiddelingsdiensten over onderzoeken in verband met arbeidsvergunningen, verblijfsadressen in het land van oorsprong, e.d. De oprichting en de werking van het register zijn geregeld in een federale wet (AZRG) van 1994.
Huber, een Oostenrijker die zich in Duitsland had gevestigd als zelfstandig verzekeringsagent, voelde zich door dit systeem gediscrimineerd. Als onderdaan van een Europese Lid-Staat had hij bezwaar tegen het feit dat gegevens over hem werden geregistreerd terwijl dat niet het geval was voor personen van Duitse nationaliteit.
Het Duitse gerechtshof dat over deze betwisting moest oordelen, legde een aantal prejudiciële vragen voor aan het Europese Hof van Justitie. Eén van die vragen handelde over de interpretatie van artikel 7 e) van de Europese dataprotectierichtlijn 95/46/EG. Daarin wordt, als één van de mogelijke rechtvaardigingsgronden voor een verwerking van persoonsgegevens, het geval vermeld waarbij "de verwerking noodzakelijk is voor de uitvoering van een taak van openbaar belang of de uitoefening van een functie van het openbaar gezag in hoofde van de verantwoordelijke of een derde persoon aan wie de gegevens worden meegedeeld". In het bijzonder vroegen de Duitse rechters zich af of van de verwerking van persoonsgegevens in het kader van het "Ausländerzentralregister" gezegd kon worden dat deze verwerking "noodzakelijk" was.

17 Zaak 524/06, Heinz Huber t. Bondsrepubliek Duitsland, zie ook http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm onder "case law"

In haar arrest stelt het Europese Hof dat de notie "noodzakelijkheid" in alle Lid-Staten op dezelfde manier uitgelegd moet worden omdat anders de harmoniseringsobjectieven van de dataprotectierichtlijn in het gedrang zouden komen. Het betreft dus een Europeesrechtelijk begrip dat in de context van de Europese richtlijn moet geïnterpreteerd worden.
Het Hof oordeelt in de eerste plaats dat het betrokken register als dusdanig niet onwettig is. Lid-Staten hebben, ondanks het vrij verkeer van personen, nog altijd specifieke regels voor onderdanen van andere Lid-Staten o.m. in het kader van hun bevoegdheden inzake bevolkingsadministratie, en voor de handhaving van deze specifieke regelgeving kan het verantwoord zijn om specifieke gegevens te verwerken over deze personen. Telkens moet men echter kijken welke gegevens voor die specifieke regelgeving nodig zijn.
Het Hof zegt verder dat de gegevens die in dit geval in het Duitse Ausländerzentralregister" worden verwerkt niet "noodzakelijk" zijn indien bepaalde gegevens worden opgeslagen die niet nodig zijn voor de toepassing van de wetgeving over de bevolkingsadministratie en de centrale opslag van die gegevens niet toelaat om deze wetgeving efficiënter toe te passen. Het is aan de nationale rechters om te oordelen of dat al dan niet het geval is.

2. Satamedia: hoever reiken uitzonderingen voor journalistieke doeleinden?

23. In Finland worden gegevens over inkomstenbelastingen van burgers (boven een bepaalde drempel) als publieke gegevens beschouw. Het mediabedrijf Markkinapörssi verzamelt deze publieke gegevens van de Finse belastingsdienst en publiceert ze jaarlijks in de regionale edities van het door haar uitgegeven dagblad Veropörssi. De informatie in deze publicaties bevat naam en voornaam van ongeveer 1,2 miljoen natuurlijke personen van wie het inkomen een bepaald plafond overstijgt, met daarbij telkens het bedrag van hun gedeclareerde inkomsten en details over het bedrag van door hen betaalde luxetaksen. Alles wordt gepresenteerd in een alfabetische lijst en geordend volgens gemeente en inkomenscategorie. In het dagblad wordt een bericht opgenomen dat iedereen die niet wil dat zijn of haar persoonsgegevens worden gepubliceerd, kan vragen op van de lijst weggelaten te worden.
Het mediabedrijf besloot nu om de informatie over de inkomstenbelastingen zoals die jaarlijks gepubliceerd werd in haar dagblad, ook over te dragen aan Satamedia, één van de andere bedrijven van dezelfde groep. In samenwerking met een mobiele telefoonoperator lanceerde dit bedrijf een SMS-dienst waarbij gebruikers de informatie over de inkomstenbelastingen via SMS op hun mobiele telefoon kunnen opvragen aan 2 euro per bericht. Ook hier werd een bericht meegestuurd dat wie niet wilde dat zijn of haar gegevens via dit systeem zouden worden verspreid, op verzoek uit het bestand zou worden weggelaten.
In verband met deze laatste dienst werd een geding ingespannen voor de Finse rechtbank op grond van de privacywetgeving. De Finse rechter besloot echter een aantal prejudiciële vragen voor te leggen aan het Europese Hof van Justitie. Eén van die vragen betrof de reikwijdte van het begrip "journalistieke doeleinden" in artikel 9 van de Europese dataprotectierichtlijn 95/46. Volgens dat artikel kunnen Lid-Staten een reeks uitzonderingen op de normale verplichten van verantwoordelijken van de verwerking van persoonsgegevens in hun

wetgeving opnemen, teneinde de bescherming van de privacy te verzoenen met de vrijheid van meningsuiting. De vraag was dus of deze uitzonderingen (in België opgenomen in artikel 3 van de Privacywet) ook konden gelden voor een dienst zoals hierboven beschreven.
In een interessant arrest van 18 december 2008[18] oordeelde het Europese Hof van Justitie dat de uitzonderingen waarin voorzien in artikel 9 niet enkel gelden voor mediabedrijven maar voor elke persoon die journalistiek bedrijft. Verder preciseerde het Hof ook dat het feit dat publicatie van informatie die tot het publiek domein behoort, ook als dit gebeurt met winstoogmerk, niets afdoet van het feit dat het om "journalistieke doeleinden" kan gaan. De Europese rechters merkten zelfs op dat commerciële bedoelingen zelfs tot de essentie behoren van het journalistieke bedrijf. Tenslotte oordeelde het Hof ook dat het medium dat gebruikt wordt om de informatie te verspreiden, of dat nu van traditionele aard is zoals papier of radio, of daarentegen elektronisch zoals het internet, niet relevant is voor de vraag of een activiteit "uitsluitend voor journalistieke doeleinden" wordt verricht.
Het Hof besluit dat activiteiten zoals de publicatie in een dagblad of het leveren van een interactieve SMS-dienst, waarbij gegevens van documenten die volgens het nationale recht tot het publiek domein behoren, beschouwd moeten worden als verwerking van persoonsgegevens die uitsluitend voor journalistieke doeleinden wordt verricht, indien het enige objectief van deze activiteiten erin bestaat informatie, opinies of ideeën te openbaren aan het publiek.

3. Rijkeboer: hoe lang moeten toegangsloggings worden bewaard?

24. Tenslotte bekijken we ook nog een arrest van het Europees Hof van Justitie van 7 mei 2009[19] omdat het belangrijke gevolgen heeft voor de vraag hoe lang toegangslogs bewaard moeten worden wanneer een toepassing toegang geeft tot persoonsgegevens.
Artikel 12 van de Europese dataprotectierichtlijn handelt over het inzagerecht en bepaalt dat elke betrokkene, van wie persoonsgegevens worden verwerkt, het recht heeft om van de verantwoorlijke zonder moeite, met redelijke tussenpozen en zonder overdreven wachttijden of kosten, bevestiging te krijgen dat gegevens over hem worden verwerkt, informatie over het doel van de verwerking "*en over de ontvangers of categorieën van ontvangers aan wie de gegevens werden meegedeeld*". In de Belgische Privacywet is deze bepaling min of meer letterlijk omgezet in artikel 10.
Eén van de praktische gevolgen van het inzagerecht voor betrokkenen is de eventuele verplichting, voor de verantwoordelijke, om logbestanden bij te houden. Anders is hij namelijk vaak niet in staat om aan de betrokkene een lijst te geven van de personen die toegang tot de gegevens hebben gehad. Een belangrijke vraag is nu hoever terug in de tijd een betrokkene deze informatie kan opvragen en dus, hoever in de tijd de logbestanden moeten teruggaan.

---

18 Zaak 73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy, zie ook http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm onder "case law"

19 Zaak C-553/07: http://tinyurl.com/njzppx

Mijnheer Rijkeboer oefende zijn inzagerecht uit bij de gemeente Rotterdam en vroeg aan de lokale administratie informatie over alle gevallen waarin personen toegang hadden gekregen tot zijn adresgegevens tijdens de laatste twee jaar voorafgaand aan zijn verzoek. Helaas schreef de Nederlandse GBA-wet voor dat deze gegevens door de gemeente maar één jaar moesten bijgehouden worden.
Rijkeboer protesteerde en de zaak kwam uiteindelijk voor de Raad van State die een prejudiciële vraag stelde aan het Europese Hof van Justitie. In haar arrest zegt dat Hof vooreerst dat een betrokkene in staat moet zijn om te controleren of zijn gegevens enkel werden meegedeeld aan geautoriseerde ontvangers. Het Hof merkt ook op dat de Europese richtlijn geen vermelding maakt over hoever deze controle terug in de tijd moet kunnen gaan.
Uiteraard, zo zegt het Hof, moet het in elk geval hierbij gaan over informatie over het verleden. Anders kan de betrokkene niet nagaan of fouten werden gemaakt en of hij eventueel schadevergoeding kan bekomen. Een mogelijke parameter om te bepalen hoever in het verleden de betrokkene moet kunnen teruggaan, is de duurtijd van bewaring van de gegevens zelf. Dat geldt echter niet absoluut. Het kan zijn dat deze duurtijd zeer lang is en het belang van de betrokkene om zoveel jaren terug te gaan sterk vermindert. Het is ook mogelijk dat het aantal mogelijke ontvangers zo groot is dat opslag van al deze data onredelijk zou zijn. In elk geval moet men aan de hand van een reeks parameters proberen vast te stellen hoe lang redelijkerwijze de loggegevens dienen bijgehouden te worden.
In het specifieke geval van Rijkeboer oordeelt het Europese Hof van de automatische uitwissing van de loggegevens na één jaar, terwijl de adresgegevens zelf veel langer worden bewaard, niet berust op een evenwichtige afweging van de belangen in deze context, tenzij aangetoond zou worden dat langere bewaring een onredelijke last zou opleggen aan de verantwoordelijke.

C. Artikel 29 werkgroep

25. Meer en meer wordt voor de interpretatie van wetgeving over de verwerking van persoonsgegevens verwezen naar de opinies van de artikel 29 werkgroep. In het verleden leverde die werkgroep al interessante opinies of werkdocumenten af over o.m. de reikwijdte van het begrip "persoonsgegevens", over nieuwe technologieën zoals RFID of biometrie, of over privacybescherming op de werkvloer of in de context van digitaal rechtenbeheer (DRM), het elektronisch patiëntendossier. Ook in de periode 2008-2009 zijn er uit de werkgroep enkele documenten voortgekomen die het vermelden waard zijn. Zo werden o.m. bruikbare aanbevelingen geformuleerd over privacybescherming op school (over foto's, websites, gebruik van CCTV en RFID, leerlingenkaarten, etc.), over zoekmachines (met o.m. de discussie over de bewaringstermijn van zoekgegevens), over de bekende "whereabouts" in het kader van dopingcontrole voor sportlui, enz.

II. België

§1. Nieuwe wetgeving

26. Van de nieuwe wetgeving die in de periode 2008-2009 in verband met privacybescherming in België is uitgevaardigd, onthouden we, op federaal vlak, de wet van 21 augustus 2008 tot oprichting van het eHealth-platform. Voor de volledigheid vermelden we ook het koninklijk besluit over de verwerking van persoonsgegevens door de CBFA. Op Vlaams niveau dient vooral melding gemaakt van het decreet betreffende het bestuurlijke elektronische gegevensverkeer.

A. eHealth-platform

27. Hoewel het principe van elektronische informatieuitwisseling in de gezondheidssector reeds in 2004 door de Ministerraad werd aanvaard, heeft het nog enkele jaren geduurd voor tot reële uitvoering hiervan werd overgegaan. De oprichting van de beheersinstelling BeHealth werd in 2006 aangekondigd in de wet van 27 december houdende diverse bepalingen[20] maar leidde niet onmiddellijk tot concrete gevolgen.
In de wet van 27 december 2006 werd de beheersinstelling BeHealth opgericht als een afzonderlijke dienst met afzonderlijk beheer binnen de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu. De taak werd opgeschreven als het beheer van een elektronisch dienstenplatform waarop gezondheidsgegevens zouden kunnen worden uitgewisseld tussen de actoren in de gezondheidszorg. Dit moest worden gerealiseerd door het verbinden van de netwerken van Fedict, het extranet van de Sociale Zekerheid en Carenet. BeHealth had zeker niet de bedoeling om een centrale databank met gezondheidsdgegevens te worden, maar kreeg de functie van een uitwisselingsplatform bestaande uit een backoffice, een portaal en een reeks basisdiensten zoals authenticatie en beveiliging.
Deze gedachtengang is overgenomen in de wet van 21 augustus 2008 over het eHealth-platform. [21] De "B" is weggevallen om aan te duiden dat het platform niet enkel beperkt is tot het federale niveau. Het wordt omschreven als een "beveiligd elektronisch uitwisselingsplatform waarop zorgverleners, zorginstellingen, ziekenfondsen, overheidsdiensten en patiënten in alle vertrouwen en met respect voor de persoonlijke levenssfeer, gegevens kunnen uitwisselen". Om alle betrokkenen zo veel mogelijk gerust te stellen wordt in artikel 6 bepaalt dat de wet op geen enkele wijze afbreuk doet aan de Privacywet, de wet betreffende de patiëntenrechten en de wettelijke en reglementaire bepalingen met betrekking tot de uitoefening van de geneeskunde. In geval van conflict hebben deze wettelijke en zelfs reglementaire bepalingen dus voorrang.

---

20 Wet houdende diverse bepalingen (I), 27 december 2006, *B.S.* 28 december 2006, art. 4.

21 Voor meer uitgebreide en actuele informatie verwijzen we naar de website van het eHealth-platform: http://www.behealth.be

Het eHealth-platform wordt opgericht als een openbare instelling van sociale zekerheid.[22] Het krijgt een Beheerscomité van 31 leden dat is samengesteld uit vertegenwoordigers van de zorgverstrekkers, de zorginstellingen, de mutualiteiten en de overheid. De administrateur-generaal van de Kruispuntbank van de Sociale Zekerheid wordt belast met het dagelijks beheer van het eHealth-platform. De Kruispuntbank van de Sociale Zekerheid stelt, tegen betaling, de diensten, het personeel, de uitrusting en de inrichtingen die nodig zijn voor de werking van het eHealth-platform te zijner beschikking. De concrete uitvoering van wettelijke opdrachten van het platform wordt geregeld in een beheersovereenkomst met de Staat. Binnen het platform wordt een Overlegcomité met de gebruikers ervan opgericht. Het Overlegcomité staat het Beheerscomité bij in de vervulling van zijn opdrachten.
De bedoeling is niet het gebruik van het platform te verplichten. In principe is is het gebruik van het eHealth-platform facultatief. Een belangrijke taak van het platform bestaat in het leveren van basisdiensten. Typische basisdiensten omvatten encryptie van gegevens tussen afzender en geadresseerde, een systeem voor gebruikers- en toegangsbeheer,een beveiligde elektronische brievenbus voor elke actor in de gezondheidszorg, een systeem voor elektronische datering, een systeem voor codering en anonimisering van informatie en een verwijzingsrepertorium. In het verwijzingsrepertorium wordt, na akkoord van de betrokken patiënten, aangeduid bij welke actoren in de gezondheidszorg welke types van gegevens worden bewaard met betrekking tot welke patiënten. Het verwijzingsrepertorium bevat zelf geen gezondheidsgegevens maar enkel verwijzingen naar plaatsen waar bepaalde types van gezondheidsgegevens te vinden zijn. Een patiënt moet ook eerst zijn – wellicht schriftelijke – toestemming geven vooraleer deze verwijzingsgegevens in het repertorium worden opgenomen. De implementatie van het verwijzingsrepertorium kan slechts geschieden na advies van het sectoraal comité.
Voor de identificatie van de patiënt moet bij uitwisseling via het eHealth-platform verplicht gebruik gemaakt worden van het identificatienummer van de sociale zekerheid – voor de meeste patiënten dus het Rijksregisternummer. Er is dus afgestapt van de gedachte om voor de gezondheidssector een apart persoonlijk gezondheidsidentificatienummer in te voeren. In haar advies van 2 april 2008 schrijft de Privacycommissie dat een algemeen sectoraal gezondheidsnummer door zoveel mensen zou worden gebruikt dat het toch geen effectieve, merkbaar betere persoonsbescherming zou bieden. “Gelet op het feit dat een correcte identificatie van primordiaal belang is enerzijds en er thans, in de huidige stand van zaken, geen afdoende argumenten voorhanden zijn die daartegen opwegen en anderzijds, het aangewezen is de optie voor een sterke identificator zoals het Rijksregisternummer en het identificatienummer van de sociale zekerheid te ondersteunen.”[23]

---

22 Art. 2 verwijst naar het koninklijk besluit van 3 april 1997 houdende maatregelen met het oog op de responsabilisering van de openbare instellingen van sociale zekerheid, met toepassing van artikel 47 van de wet van 26 juli 1996 tot modernisering van de sociale zekerheid en tot vrijwaring van de leefbaarheid van de wettelijke pensioenstelsels.

23 Advies nr. 14/2008, website van de Privacycommissie; zie http://www.privacycommission.be

Het eHealth-platform krijgt toegang tot het Rijksregister en heeft eveneens een machtiging om het Rijksregisternummer te gebruiken. Authenticatie kan op verschillende wijzen, o.m. – maar niet uitsluitend - door gebruik van de elektronische identiteitskaart. Voor de authenticatie van zorgverstrekkers wordt zoveel mogelijk gebruik gemaakt van authentieke bronnen, bijv. om na te gaan of iemand geregistreerd is als beroepbeoefenaar in de gezondheidszorg.
Elke mededeling van persoonsgegevens door of aan het eHealth-platform vereist een principiële machtiging van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid. Uitzonderingen blijven mogelijk maar daarvoor is in de meeste gevallen een Koninklijk besluit nodig met advies van de Privacycommissie.
De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, na advies van het Beheerscomité en na advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, bepalen welke gegevens door welke overheidsinstellingen aan het eHealth-platform verplicht en elektronisch worden meegedeeld voor de uitvoering van zijn opdrachten, en welke gegevens het *eHealth*-platform aan welke overheidsinstellingen verplicht en elektronisch meedeelt voor de uitvoering van hun opdrachten.

B. KB over de verwerking van persoonsgegevens door de CBFA

28. Om openbare overheden in staat te stellen hun opdrachten van bestuurlijke politie efficiënt uit te voeren, heeft de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens de Koning gemachtigd om die overheden vrij te stellen van bepaalde verplichtingen waarvan sprake in die wet, meer bepaald:
i) de verplichting om bepaalde informatie te verstrekken aan de natuurlijke personen van wie de gegevens worden verwerkt (art. 9, §§ 1 en 2, van die wet),
ii) de verplichting om die personen toegang te verlenen tot hun gegevens (art. 10 van die wet), en
iii) de verplichting om die personen in staat te stellen onjuiste gegevens te doen verbeteren of onrechtmatig opgenomen gegevens te doen verwijderen (art. 12 van die wet).

Doelstelling van het koninklijk besluit van 29 april 2009[24] is de Commissie voor het Bank-, Financie- en Assurantiewezen (CBFA) in bepaalde omstandigheden vrij te stellen van die verplichtingen.

24 Koninklijk besluit van 29 april 2009 tot uitvoering van artikel 3, § 5, 3°, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens met betrekking tot de Commissie voor het Bank-, Financie- en Assurantiewezen, BS 13 mei 2009.

§2. Rechtspraak

A. Grondwettelijk Hof: toestemming patiënt voor elektronisch patiëntendossier

29. Elektronische patiëntendossiers bieden de mogelijkheid tot consultatie en bijwerking door verschillende beroepsbeoefenaars in de gezondheidszorg vanuit verschillende plaatsen. Elke zorgverstrekker die de nodige autorisaties heeft, kan online toegang krijgen tot de gegevens met betrekking tot de patiënt. In principe kunnen echter geen patiëntengegevens gedeeld worden zonder toestemming van de patiënt. De Privacycommissie maakt een onderscheid tussen uitwisseling van gegevens tussen leden van eenzelfde behandelingsteam en uitwissseling tussen verschillende behandelingsteams. Uitwisseling binnen eenzelfde team behoort volgens de Commissie tot de normale verwachtingen van de patiënt. De toestemming hoeft dan ook niet expliciet te zijn. Indien de gegevens echter gedeeld worden met iemand uit een ander behandelingsteam, dan is het volgens de Commissie niet meer vanzelfsprekend om de toestemming te veronderstellen. "Gelet op de snelle, eenvoudige consulteerbaarheid van elektronische dossiers dient elke vorm van impliciete, stilzwijgende toestemming uitdrukkelijk te worden uitgesloten".[25] De toestemming moet dus in dat geval schriftelijk zijn.
Discussie is ontstaan over de vraag of het aanleggen van een elektronisch patientendossier niet eenvoudig te rechtvaardigen is op grond van de uitzondering waarin de Privacywet in artikel 7, §2, j) voorziet voor "verwerkingen die noodzakelijk zijn voor doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen aan de betrokkene of een verwant, of het beheer van gezondheidsdiensten handelend in het belang van de betrokkene". Die discussie laaide opnieuw op naar aanleiding van het Vlaams decreet betreffende het gezondheidsinformatiesysteem.[26] Artikel 19, § 1 van dat decreet bepaalt: "Mits toestemming van de zorggebruiker of, als de zorggebruiker jonger is dan 14 jaar, van zijn ouders, zendt de verantwoordelijke voor het individuele gezondheidsdossier of de gegevenscoördinator aan de zorgverstrekkers en organisaties met terreinwerking die n het operationele informatiesysteem participeren en die eron verzoeken, de gegevens uit het individuele gezondheidsdossier of de elektronische registratie over die noodzakelijk zijn om de continuïteit en de kwaliteit van de zorgverlening te verzekeren (...)". In artikel 19, § 4 wordt daaraan toegevoegd: "In afwijking van § 1 en voor zover de zorggebruiker zich niet tegen het overzenden van de gegevens verzet, wordt de toestemming verondersteld stilzwijgend verkregen te zijn als de overzending van de gegevens gebeurt: 1° naar aanleiding van een verwijzing die deel uitmaakt van de lopende zorgverlening, 2° in het kader van samenhangende activiteiten van de zorgverlening, 3° in het kader van samenhangende activiteiten van een preventieprogramma.". Deze bepaling werd voorge-

25 Advies nr. 05/2004 van 10 mei 2004 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, http://www.privacycommission.be

26 Decreet van 16 juni 2006 betreffende het gezondheidsinformatiesysteem, B.S. 7 september 2006

legd aan het Grondwettelijk Hof omdat ze strijdig zou zijn met artikel 7 van de Privacywet.
In haar arrest van 14 februari 2008[27] oordeelt het Grondwettelijk Hof dat de in artikel 7, § 2, van de wet van 8 december 1992 vermelde uitzonderingen op het verbod van de verwerking van persoonsgegevens in verband met de gezondheid, beperkend dienen te worden geïnterpreteerd. "De voorwaarde in artikel 4 van het decreet van 16 juni 2006 dat de gegevensuitwisseling noodzakelijk moet zijn om de continuïteit en de kwaliteit van de zorgverlening te verzekeren, is dermate ruim dat zij onvermijdelijk ook gegevensuitwisselingen zal betreffen die niet onder de in artikel 7, § 2, van de wet van 8 december 1992 vermelde uitzonderingen ressorteren, zodat hiervoor de schriftelijke toestemming van de betrokken persoon is vereist. Door de algemene bewoordingen waarin het is gesteld, doet artikel 19, § 1, van het bestreden decreet afbreuk aan de bescherming waarin artikel 7, § 2, a), van de wet van 8 december 1992 voorziet door het vereiste van een schriftelijke toestemming van de zorggebruiker. (...) Artikel 19, § 1, dient te worden vernietigd in zoverre het niet voorziet in de schriftelijke toestemming van de zorggebruiker".
Het Hof preciseert verder ook nog "dat de toestemming van de zorggebruiker wordt geacht stilzwijgend te zijn verkregen, als de overzending van gegevens gebeurt naar aanleiding van een verwijzing die deel uitmaakt van de lopende zorgverlening, maakt op zich een inbreuk op het vereiste van een schriftelijke toestemming van de zorggebruiker uit, die evenwel kan worden aanvaard vanwege het wezen zelf van de verwijzing van de patiënt. De toestemming kan evenwel slechts worden geacht stilzwijgend te zijn verkregen indien het gaat om de uitwisseling van de noodzakelijke gegevens binnen het behandelingsteam waarin de beroepsbeoefenaars zijn opgenomen met instemming van de zorggebruiker in diens overtuiging dat zorgcontinuïteit moet worden gewaarborgd. Elke uitwisseling die zulks miskent, bijvoorbeeld omdat de zorggebruiker een tweede mening wenst, die hij niet beïnvloed wenst te zien door de resultaten die in de vroegere zorgfasen werden vastgesteld, zou strijdig zijn met artikel 7 van de wet van 8 december 1992".
Volgens het Grondwettelijk Hof is dus de schriftelijke toestemming van de patiënt vereist voor elke doorgifte van gezondheidsgegevens uit een elektronisch patiëntendossier, tenzij het een uitwisseling betreft binnen het behandelingsteam dat de zorgen verstrekt waarbij uitwisseling kan steunen op de initiële toestemming die de patiënt heeft gegeven aan de beroepsbeoefenaar die tot dat behandelingsteam behoort.
Voor het overige is slechts één geval denkbaar waarin voor het delen van een elektronisch patiëntendossier geen schriftelijke toestemming vereist is, nl. de verwerking die noodzakelijk is voor de verdediging van de vitale belangen van de betrokkene of van een ander persoon, indien de betrokkene fysiek of juridisch niet in staat is om zijn toestemming te geven. Een gelijkaardige bepaling vindt men overigens ook in de wet betreffende de patiëntenrechten (art. 8, § 5). Deze wet stelt dat wanneer er in een spoedgeval geen duidelijkheid is omtrent de al dan niet voorafgaande wilsuitdrukking van de patiënt of zijn vertegenwoordiger, iedere noodzakelijke tussenkomst van de beroepsbeoefenaar onmiddellijk gebeurt in het belang van de gezondheid van de patiënt.

27 http://www.arbitrage.be/public/n/2008/2008-015n.pdf

B. Diverse andere rechtspraak

30. Het Arbeidshof te Brussel[28] boog zich over het geval van iemand die, na het oplopen van een arbeidsongeval een medisch dossier had lopen bij de werkgever. Hij verzocht herhaalde malen om inzage te krijgen in het dossier van de controlegeneeskundige, maar dat werd hem geweigerd. Het Hof kende betrokkene recht op inzage toe op grond van art. 9 par. 2 van de wet van 22 augustus 2002 betreffende de rechten van de patient en art. 10 par. 2 van de wet verwerking persoonsgegevens.
In een arrest van het Hof van beroep te Gent[29] ging het over de vermelding van faillissementen van andere vennootschappen waarin een mandaat werd bekleed door bestuurders van de vennootschap waarover handelsinformatie wordt verstrekt. Volgens het Hof is dit is wel degelijk informatie over natuurlijke personen die valt onder de wet verwerking persoonsgegevens. Gegevens omtrent alle eerdere bestuursmandaten zijn echter nuttig en relevant. Het selectief verwijderen van dergelijke gegevens, zelfs al zouden zij als negatieve informatie worden ervaren zou een onvolledige weergave van de werkelijke toestand van de vennootschap en zijn bestuurders tot gevolg hebben. Daarom werd de vermelding van deze gegevens als rechtmatig aanzien.
Interessant is ook een arrest van het Arbeidshof te Bergen[30] in een zaak tussen de NMBS en één van haar agenten. Het schaduwen door een privé-detective ingesteld door de werkgever teneinde controle en toezicht uit te oefenen op de activiteit van een werknemer werd als een onwettig bewijs beschouwd omdat dit een inbreuk is op diens privé-leven die niet kan worden gerechtvaardigd door de wettige belangen van de werkgever gelet op het buitensporig karakter van de maatregel. De inmenging in het privé-leven is slechts toegestaan indien de beginselen van wettigheid, doelgerichtheid en proportionaliteit in acht worden genomen. (Art. 22 G.W. en art. 8 EVRM). De bekentenis afgedwongen door het gebruik van onwettige bewijsmiddelen kan niet als bewijs worden weerhouden. (Art. 12 arbeidsovereenkomstenwet).
Het Hof overweegt dat de schending van het recht op eerbiediging van het privéleven, of ze nu strafrechtelijk gesanctioneerd wordt of niet, een burgerrechtelijke fout uitmaakt waarvan de constitutieve bestanddelen gevormd worden door de interpretatie die gegeven wordt aan de definitie van de fout volgens het burgerlijk aansprakelijkheidsrecht en in het licht van art. 8 EVRM. De fout gepleegd door de NMBS is voldoende bewezen door de onwettelijke onderzoeksdaden van haar inspectiedienst. Deze daden hebben een ontoelaatbare inmenging veroorzaakt in het privéleven van de betrokken statutaire agent. Het is evident dat de onwettige daden van de NMBS de geldigheid en bewijskracht van de vaststellingen aantasten die op deze basis tot stand zijn gekomen. Bijgevolg is het van geen belang te onderzoeken, om de omvang van de geleden schade vast te stellen, of de NMBS zich niet bovendien schuldig heeft gemaakt aan de schending van de wet verwerking persoonsgegevens of nog van de wet 19 juli 1991 tot regeling van het beroep van privé-detective.

---

28 Arbh. Brussel (7e k.) 5 maart 2009, Computerr. (NL) 2009, afl. 6, 260, noot Griet Verhenneman

29 Gent (1e k.) 6 januari 2008, TGR-TWVR 2008, afl. 2, 92,

30 Arbh. Bergen (2e k.) nr. 20380, 18 februari 2008, RDTI 2008, afl. 31, 229, noot ROSIER, K., GILSON, S;, RGCF 2008, afl. 6, 463

In de Juristenkrant werd verder ook melding gemaakt van een vonnis van de correctionele rechtbank te Hasselt[31] in de zaak van de bekende plastische chirurg Hoeyberghs. Betrokkene verweet het zijn tuchtrechtelijke overheid ook informatie over zijn dossiers te hebben opgevraagd bij de beide Limburgse parketten. Dat zou, zo hield hij voor, enerzijds een - in dagvaarding niet nader gespecifieerde - inbreuk uitmaken op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, en anderzijds in strijd zijn met het beroepsgeheim en een inbreuk vormen op artikel 458 Strafwetboek.
In klare bewoordingen stelt de rechtbank dat het uitsluitend opvragen van gegevens geen dergelijke inbreuken kunnen uitmaken. Door het opvragen van gegevens bij het parket kan men niet beschouwd worden als een persoon die persoonsgegevens verwerkt.
Ook nog vermeldenswaard is een beschikking van de voorzitter van de rechtbank van koophandel te Hoei in een geschil betreffende "virale marketing". Daarbij worden gebruikers van een website uitgenodigd om e-mailadressen van vrienden en kennissen in te tikken, meestal tegen beloning. Volgens de voorzitter schendt de techniek van virale marketing die wordt gebruikt door de uitgever van een site art. 94/3 WHPC. De uitgever van de site moet worden beschouwd als de verantwoordelijke voor de verwerking van persoonsgegevens in de zin van art. 1, par. 4 wet verwerking persoonsgegevens. De verwerking van de betrokken gegevens is niet gerechtvaardigd in de zin van art. 5, f van voormelde wet. Het is onaanvaardbaar dat het e-mailadres van de kennissen van de leden van de site tegen beloning wordt verzameld door een commerciële site, zonder dat de aandacht van het lid van de site waarvan men het adresboek vraagt op enig ogenblik wordt gevestigd op het feit dat een reclameboodschap zal worden verstuurd naar de correspondenten waarvan hij de adressen heeft overgemaakt en op de noodzaak om, bijvoorbeeld, de verzending naar minderjarigen te vermijden. Het feit dat de bestemmeling de garantie heeft dat, indien hij niet antwoordt, zijn adres binnen de vijftien dagen wordt gewist van de site die hem lastigvalt, is onvoldoende. De houder van een e-mailadres heeft een fundamenteel recht om, zonder zijn voorafgaande toestemming, niet de belaging te moeten ondergaan van sites die e-mailadressen verzamelen bij hun leden door hen voordelen en beloningen voor te spiegelen of door ze zonder meer op sleeptouw te nemen met een slimme commerciële promotiecampagne.
Tenslotte vermelden we ook nog een vonnis van de vrederechter te Waver[32] over de frequent gestelde vraag of een syndicus aan een eigenaar van een appartement de namen en adressen mag doorgeven van de andere mede-eigenaars van het flatgebouw. Volgens de recher is het de taak van de syndicus om aan een mede-eigenaar, die daarom vraagt, de persoonsgegevens van de andere mede-eigenaars mee te delen, op grond van de bevoegdheden die hem door de wet zijn toegekend. Dergelijke communicatie loopt in de pas met het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer[33], voor zover de mede-eigenaar, die daarom verzoekt, deze gegevens gebruikt voor een doel dat verenigbaar is met de wezenlijke, expliciete en legitieme fi-

31 Corr. Hasselt, 14 maart 2008, onuitg.
32 Vred. Waver (2) nr. 08A689, 16 september 2008, T.App. 2009, afl. 1, 40
33 Het betreft hier het advies 2008/22 van de Privacycommissie, http://www.privacycommission.be/nl/docs/Commission/2008/advies_22_2008.pdf

naliteit van de gegevensverzameling, namelijk gerelateerd aan de wettelijke bepalingen die de vereniging van mede-eigenaars beheersen.

C. Privacycommissie

31. Van de adviezen en aanbevelingen van de privacycommissie tijdens de periode 2008-2009 onthouden we vooral de zeer praktische aanbevelingen over het opvragen van adressen aan lokale bevolkingsadministraties of aan het Rijksregister (bijv. om het huidige adres van VRG-alumni te achterhalen).[34] Andere belangrijke documenten zijn het advies van april 2008 over biometrie[35] en de aanbeveling over direct marketing die in oktober 2008 werd gepubliceerd. [36] Tenslotte heeft de Privacycommissie zich in de beschouwde periode in een hele reeks adviezen duidelijk uitgesproken over de Belgische aanpak inzake bestuurlijk elektronisch gegevensverkeer, het gebruik van het Rijksregisternummer en van de elektronische identiteitskaart, de rol van integratoren, e.a. Best kan daarvoor verwezen worden naar de website van de Privacycommsie.

34 Aanbeveling 02/2009, zie www.privacycommission.be

35 Advies nr. 17/2008 van 9 april 2008; zie verder ook E. KINDT en J. DUMORTIER, "Biometrie als herkennings- of identificatiemiddel? Enkele juridische beschouwingen", *Computerr.* 2008/5

36 Aanbeveling nr 04/2009 van 14 oktober 2009, zie www.privacy.commission.be