Recht en ICT

Recente ontwikkelingen in de toepassing van de privacywetgeving

Jos DUMORTIER
Gewoon hoogleraar K.U.Leuven

In deze bijdrage overlopen we enkele belangrijke recente ontwikkelingen op het gebied van de privacywetgeving in Europa en België over de periode 2006-2007. Daarbij maken we een onderscheid tussen: 1) nieuwe uitgevaardigde en voorstelde regelgeving, 2) belangrijke ontwikkelingen op Europees niveau en 3) enkele markante beslissingen van de Commissie voor de bescherming van de persoonlijke levenssfeer.

I. Overzicht van uitgevaardigde en voorgestelde regelgeving

In de periode 2006-2007 werd in het domein van de privacybescherming een aantal belangrijke nieuwe normatieve teksten geproduceerd. De ontbinding van het federale Parlement in de lente van 2007 heeft ervoor gezorgd dat de meeste van deze teksten (nog) niet definitief zijn goedgekeurd en uitgevaardigd. Hierna overlopen we kort de wetten en decreten betreffende de bewakingscamera's en het hergebruik van overheidsinformatie en de ontwerpen over de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën, de verplichting tot dataretentie voor operatoren van publieke communicatienetwerken en communicatiediensten. Tenslotte bespreken we ook kort de bevoegdheidskwestie in deze materie naar aanleiding van de voorbereiding van het Vlaams decreet over het elektronische bestuurlijke gegevensverkeer (e-government).

§ 1. Camerabewaking

De wet van 21 maart 2007 over de plaatsing en het gebruik van bewakingscamera's verscheen in het Staatsblad van 31 mei en is sinds 10 juni effectief in werking.[1] Voordien werd het gebruik van bewakingscamera's uitsluitend geregeld door de algemene principes van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens (hierna: "de privacywet"). Enkel voor camera's op de werkplaats bestond een specifieke regeling, in de vorm van een collectieve arbeidsovereenkomst (CAO nr. 68). Daarnaast heeft de zogenaamde voetbalwet ook camera's die opgesteld worden bij voetbalwedstrijden aan speciale regels onderworpen.

De nieuwe wet geldt voor *alle andere* bewakingscamera's, waarvoor tot nu toe nog geen specifieke regels bestaan. Het toepassingsgebied is bovendien beperkt tot vaste of mobiele camerasystemen met een bewakingsfunctie. Camera's voor andere doeleinden vallen dus niet onder de regeling. Een voorbeeld is een webcam die via Internet in realtime de weersituatie in een kustgemeente wil laten zien.

In de nieuwe wet wordt een onderscheid gemaakt tussen drie soorten plaatsen waar bewakingscamera's opgesteld kunnen worden: 1) niet-besloten plaatsen zoals straten, pleinen of niet afgesloten parken; 2) besloten plaatsen die toegankelijk zijn voor het publiek, zoals winkelgalerijen, grootwarenhuizen, dancings of

[1] http://www.privacycommission.be/nl/static/pdf/wetgeving/camerawet_21_03_2007.pdf

cafés; 3) besloten plaatsen die niet toegankelijk zijn voor het publiek zoals appartementsgebouwen, kantoorgebouwen of fabrieksterreinen.

In elk van die drie situaties moet de verantwoordelijke die bewakingscamera's wil installeren, eerst een aangifteformulier invullen. Gelukkig kan dat online, via de website van de Privacycommissie: www.privacycommission.be. Via een zestal schermen waarop een reeks inlichtingen over het geplande camerasysteem moeten ingevuld worden, wordt een document gegenereerd dat onmiddellijk op de server van de Privacycommissie wordt opgeslagen. Daarnaast moet een verkorte verklaring met de hand of elektronisch worden ondertekend en opgestuurd. De website van de Privacycommissie bevat ook een overzicht van de wettelijke bepalingen.

Voor het plaatsen van bewakingscamera's op niet-besloten plaatsen moeten eerst ook nog positieve adviezen verkregen worden van de gemeenteraad en van de korpschef van de politiezone. Voor bewakingscamera's op besloten plaatsen, al dan niet toegankelijk voor het publiek, is dat niet nodig. Via de aangifte aan de Privacycommissie wordt echter automatisch een bericht doorgestuurd naar de korpschef van de politiezone.

De wet bevat verder een reeks voorwaarden voor het plaatsen en gebruik van bewakingscamera's en voor het bekijken en gebruiken van de beelden. Daarenboven blijven de basisprincipes van de privacywet gelden. Er geldt ook een maximum bewaringstermijn die nooit langer is dan één maand.

Een aantal praktische details van de wet moet nog verder uitgewerkt worden in een Koninklijk besluit. Daarin zal bijvoorbeeld geregeld worden hoe het pictogram er moet uitzien dat standaard in elke zone met bewakingscamera's zal aangebracht moeten worden. Zolang dat besluit nog niet is verschenen, moet het publiek verwittigd worden volgens de gewone regels van de privacywet. Dat kan bijvoorbeeld via een bordje waarop de naam van het bedrijf, de melding dat permanent wordt gefilmd en een telefoonnummer vermeld wordt.

Voor reeds geïnstalleerde bewakingscamera's voorziet de nieuwe wet in een overgangsperiode van drie jaar. Op dat moment moeten alle bewakingscamera's die onder de wet vallen, bij de Privacycommissie geregistreerd zijn.

De belangrijkste kritiek op de wet komt erop neer dat de gelijktijdige toepassing van de algemene bepalingen van de privacywet en de specifieke bepalingen van de camerawet tot moeilijke complicaties zal leiden. Sommigen vrezen ook dat de nieuwe wet het plaatsen van bewakingscamera's op plaatsen waar dit niet strikt noodzakelijk is, zal stimuleren.

§ 2. Hergebruik van overheidsinformatie

Een Europese richtlijn van 17 november 2003[2] regelt het hergebruik van overheidsinformatie. Het uitgangspunt van de richtlijn is dat de overheid een breed scala aan informatie produceert, verzamelt en verspreidt i.v.m. de meest uiteenlopende domeinen waarop zij actief is (op sociaal en economisch vlak, toerisme, bedrijven, milieu-informatie, de onderwijs, geografie, …). Al deze overheidsinformatie kan een belangrijke grondstof zijn voor allerhande digitale informatieproducten en -diensten. Nieuwe informatie- en communicatietechnologieën zorgen ervoor dat niet alleen de toegankelijkheid van overheidsinformatie aanzienlijk wordt verbeterd maar bieden ook totaal nieuwe vormen en mogelijkheden van hergebruik van overheidsinformatie. Best zouden die mogelijkheden optimaal benut moeten worden. In de richtlijn worden een aantal regels opgelegd die bij het hergebruik van overheidsinformatie moeten worden nageleefd. Die regels hebben onder meer betrekking op het verbod tot discriminatie tussen private en publieke sector, de verplichting tot transparantie, de prijs die de overheid aan kandidaat-hergebruikers mag aanrekenen, enz.

De richtlijn moest door de lidstaten tegen 1 juli 2005 in het nationale recht zijn omgezet. Op het moment van dit schrijven (januari 2007) hebben alle lidstaten, behalve België, aan deze verplichting voldaan.[3] Dat komt omdat de richtlijn in België niet enkel door de federale staat maar ook door de gewesten en de gemeenschappen omgezet moet worden. Dat is momenteel nog niet door het Brussels Gewest gebeurd.

Bij de omzetting van de richtlijn heeft de federale wetgever rekening gehouden met het zeer strikte standpunt van de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna: "de privacycommissie"). Terecht heeft de Commissie erop gewezen dat elke vorm van hergebruik moet worden beschouwd als een verwerking in de zin van de wet van 8 december 1992 voor zover het gaat om de verwerking van persoonsgegevens. Dat staat met zoveel woorden in overweging 21: "De uitvoering en toepassing van deze richtlijn geschiedt in volledige overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen i.v.m. de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens". Bovendien bepaalt artikel 1.4 uitdrukkelijk: "*Deze richtlijn laat het niveau van de bescherming van individuen met betrekking tot het verwerken van persoonsgegevens krachtens de bepalingen van het Gemeenschapsrecht en de nationale wetgeving intact en heeft daar geen enkele invloed op, en houdt met name geen wijziging in van de verplichtingen en rechten in Richtlijn 95/46/EG*".

De Belgische privacycommissie heeft hieruit – volgens ons ten onrechte – afgeleid dat vooraleer persoonsgegevens voor hergebruik ter beschikking worden

---

2 Richtlijn 2003/98/EG van 17 november 2003 inzake het hergebruik van overheidsinformatie,

3 http://ec.europa.eu/information_society/policy/psi/actions_ms/implementation/index_en.htm

gesteld, ze eerst volledig anoniem gemaakt moeten worden.[4] In de wet van 7 maart 2007 die voor de omzetting van de richtlijn op federaal niveau zorgde[5], is dit advies opgevolgd. Artikel 4 van de wet luidt als volgt: "Bestuursdocumenten die persoonsgegevens bevatten, komen pas in aanmerking voor hergebruik, nadat de betrokken overheid de nodige voorzorgsmaatregelen heeft genomen om de identiteit te verbergen van de personen op wie de persoonsgegevens betrekking hebben, inzonderheid door de informatie die de bestuursdocumenten bevatten te anonimiseren overeenkomstig de definitie voorzien in artikel 1, 5°, van het koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens".

Tijdens de parlementaire discussie over deze bepaling werd de vraag gesteld of deze verplichting ook toepasselijk is op de gegevens die opgenomen zijn in de Kruispuntbank van Ondernemingen (KBO). Zeer veel ondernemingen dragen de naam van de natuurlijke persoon die de vennootschap heeft opgericht. Indien deze naam anoniem gemaakt moet worden, zou de bedrijfsinformatie onbruikbaar worden voor allerlei doeleinden waarvoor ze nu wordt aangewend. Nochtans bepaalt artikel 20 van de wet van 16 januari 2003 (de KBO-wet) uitdrukkelijk dat de publieke gegevens uit de KBO mogen worden gecommercialiseerd volgens de voorwaarden die de Koning bepaalt. De Staatssecretaris sloot deze discussie af met de stelling dat de wet op het hergebruik een algemene strekking heeft en daarom "geenszins afwijkt af van de bijzondere bepalingen van de wet van 16 januari 2003 betreffende de Kruispuntbank van Ondernemingen, die onverkort van toepassing blijven".[6]

Op Vlaams niveau hield men zich, naar het voorbeeld van de meeste EU-lidstaten in deze discussie gelukkig op de vlakte. Anonimisering van persoonsgegevens wordt niet als voorwaarde voor hergebruik opgelegd. Het decreet rond hergebruik van overheidsinformatie werd samen met de uitvoeringsbesluiten van 19 juli 2007 gepubliceerd in het Belgisch Staatsblad van 5 november 2007. Een ministerieel besluit van 8 oktober 2007 legt een modellicentie vast voor het hergebruik.

§ 3. Wetsontwerp Financiën

In de Kamer van Volksvertegenwoordigers is door de vorige regering een wetsontwerp ingediend over de bescherming van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën.[7] Als gevolg van het wetontwerp zou de uitwisseling van persoonsgegevens binnen de FOD Financiën aan controleprocedures worden onderworpen. Naar het voor-

---

4 Advies nr. 04/2006 van 8 februari 2006, p. 4: "ofwel neemt de betrokken overheid de nodige voorzorgsmaatregelen voor een volledige anonimisering, ofwel is er geen hergebruik mogelijk van de bewuste bestuursdocumenten".
Zie http://www.privacycommission.be/nl/docs/Commission/2006/advies_04_2006.pdf

5 Wet tot omzetting van de richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie, *B.S.,* 19 april 2007.

6 Zie het Commissieverslag van 22 januari 2007, Doc. Kamer, 51ste zitting, 2634/002.

7 http://www.dekamer.be/FLWB/PDF/51/3064/51K3064001.pdf

beeld van wat nu reeds het geval is voor gegevens uit het Rijksregister of uit de Kruispuntbank voor de Sociale Zekerheid zou een machtiging nodig zijn om gegevens van de FOD Financiën te verkrijgen voor andere doeleinden, bijvoorbeeld om de hoogte van het inkomen na te gaan met het oog op het verlenen van studiebeurzen of andere voordelen.

Het wetsontwerp heeft tevens tot doel om de verschillende moderniseringsprojecten die momenteel binnen de FOD Financiën op stapel staan, in overeenstemming te brengen met de privacywetgeving. Er worden bijvoorbeeld bepaalde voorwaarden opgelegd voor het aanleggen van het "uniek dossier" over een belastingsplichtige of over het gebruik van het geplande "datawarehouse" dat de FOD moet ondersteunen om op een meer gerichte manier de fiscale controles te organiseren.

Door de ontbinding van het federale Parlement is het wetsontwerp vervallen maar het zal, al dan niet in gewijzigde vorm, zeker opnieuw door de huidige of volgende regering worden ingediend.

§ 4. Dataretentie

Een Europese richtlijn van 15 maart 2006 verplicht de lidstaten om in hun wetgeving aan operatoren van elektronische publieke communicatienetwerken en aanbieders van publieke communicatiediensten een verplichting tot dataretentie op te leggen.[8] Onder dataretentie wordt het bewaren van verkeersgegevens, locatiegegevens en gegevens over abonnees en gebruikers verstaan, gedurende een bepaalde tijd en met het doel ze beschikbaar te stellen wanneer nodig voor gerechtelijke autoriteiten bij een onderzoek naar ernstige misdrijven. Deze richtlijn moest door de lidstaten worden omgezet tegen 15 september 2007 voor vaste en mobiele telefonie. Voor internetverkeer krijgen de lidstaten tijd tot 15 maart 2009.

In België werden met dat oogmerk door de vorige regering voorontwerpen van wet en koninklijk besluit goedgekeurd. Door de ontbinding van het federale parlement laat de goedkeuring en uitvaardiging van deze teksten voorlopig nog op zich wachten. In een voorontwerp van wet wordt een wijziging van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie voorgesteld. Dat artikel bevat momenteel reeds het principe van dataretentie maar werd nog niet verder uitgevoerd in een Koninklijk besluit. De voorgestelde wetswijziging moet het artikel in overeenstemming brengen met de Europese richtlijn, o.m. door de toevoeging van de dataretentieverplichting voor locatiegegevens en het aanpassen van de bewaringstermijn (zes maanden tot twee jaar). Het BIPT krijgt bovendien de mogelijkheid om de termijn in uitzonderlijke omstandigheden te verlengen. In de voorontwerpen van uitvoeringsbesluiten worden deze principes verder uitgewerkt, voorlopig enkel in het domein van de vaste en mobiele telefonie.

8 http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

§ 5. Privacybescherming in Gewesten en Gemeenschappen

Over de bevoegdheid van de Gewesten en Gemeenschappen inzake de bescherming van de persoonlijke levenssfeer is wat meer duidelijkheid gekomen door het advies van de Raad van State in Advies 37.288/3 over het voorontwerp van decreet betreffende het gezondheidsinformatiesysteem.[9] Volgens de Raad van State mogen de gemeenschappen en gewesten ook beperkingen op dit recht aanbrengen voor zover deze kaderen binnen de regeling van een aangelegenheid die tot hun bevoegdheid behoort en voor zover daarbij de federale basisnormen en internationaalrechtelijke bepalingen niet worden aangetast. Dit komt er op neer dat de decreetgever strengere voorwaarden dan de federale regelgeving mag voorzien, maar het federale beschermingsniveau niet mag verlagen. Dit strookt met het standpunt ingenomen door het Grondwettelijk Hof in zijn arrest van 19 januari 2005 dat de Vlaamse decreetgever gehouden is door de federale wetgeving die als minimumregeling geldt in welke aangelegenheid dan ook. In dit arrest heeft het Hof beslist dat de bekendmaking van persoonsgegevens, in casu publicatie van disciplinaire schorsingen van meerderjarige sportbeoefenaars op een website van de Vlaamse regering, een inmenging inhoudt van het recht op eerbiediging van het privé-leven zoals gewaarborgd bij artikel 22 van de Grondwet en een schending van het proportionaliteitsbeginsel uit de WVP. [10]

Met die principes voor ogen, wordt momenteel een ontwerp van decreet over het elektronische bestuurlijke gegevensverkeer – maar meestal aangeduid als het "e-governmentdecreet"" voorbereid. De belangrijkste doelstelling van het ontwerp bestaat erin een oplossing aan te bieden voor het uitwisselen van persoonsgegevens tussen de verschillende Vlaamse administraties of tussen deze Vlaamse administraties en de federale of andere regionale overheden.

II. Belangrijke ontwikkelingen op Europees niveau

§ 1. Algemeen

Wellicht de belangrijkste evolutie op Europees vlak in het hier besproken domein is het Verdrag van Lissabon.[11] Dat maakt een einde aan de kunstmatige verdeling in pijlers, hoewel de specificiteit van het buitenlands en veiligheidsbeleid onderlijnd blijft. Omdat privacybescherming zo sterk verbonden is met de discussie over het veiligheidsbeleid, bestaat vandaag voortdurend discussie over de mogelijkheden om in dit domein op Europees vlak regelgeving te ontwikkelen.

De bedoeling is dat het nieuwe Verdrag nog vóór de verkiezingen van het Europees Parlement van 2009 in werking treedt. Elke lidstaat heeft zijn eigen interne procedures om dit verdrag te ratificeren. Voorlopig heeft enkel Ierland

9 Advies 37.288/3.
Zie http://jsp.vlaamsparlement.be/docs/stukken/2005-2006/g531-1.pdf, vanaf p. 179

10 Arrest nr. 16/2005 van 19 januari 2005, http://www.grondwettelijkhof.be

11 Pb. EG 17/12/2007.
http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:NL:HTML

beslist om een referendum te organiseren. België zal het verdrag door middel van een parlementaire procedure ratificeren. Het Verdrag van Lissabon moet zowel door het federale Parlement als door de parlementen van de Gewesten en Gemeenschappen goedgekeurd worden.

§ 2. Toepassing van de Europese richtlijnen

Op Europees vlak werd in de periode 2006-2007 verder gewerkt aan de opvolging van het eerste rapport van de Europese Commissie over de toepassing van de dataprotectierichtlijn 95/46/EG. In dat rapport, dat al dateert van 2003[12], concludeerde de Commissie dat er geen wijzigingen van de wetgeving nodig zijn, maar dat er inspanningen dienen te worden geleverd om de toepassing van de richtlijn te verbeteren. In het verslag was een *Werkprogramma voor een betere toepassing van de Richtlijn gegevensbescherming* opgenomen. Daarin werden tien actiereinen voorgesteld, bijvoorbeeld op het vlak van meer harmonisatie, betere afdwingbaarheid, stimulering van privacyvriendelijke technologie, enz. In een mededeling van 7 maart 2007[13] heeft de Commissie een balans opgemaakt over de stand van zaken met betrekking tot de uitvoering van dat werkprogramma.

Eén van de actiepunten die in het werkprogramma werden aangekondigd, is de publicatie van interpretatienota's over de toepassing van de dataprotectierichtlijn. Die nota's moeten een remedie vormen tegen de grote diversiteit bij de interpretatie van de richtlijn in de verschillende lidstaten. Mede als gevolg daarvan is de Artikel 29 groep van de privacycommissarissen gestart met het uitwerken van een reeks adviezen en werkdocumenten over de klassieke interpretatieverschillen bij de toepassing van de richtlijn, zoals de definitie van het concept "persoonsgegevens"[14] of de verwerking van gezondheidsgegevens.[15]

§ 3. Export van persoonsgegevens

De problematiek van de doorgifte van persoonsgegevens naar landen buiten de Europese Unie wordt geregeld door de artikelen 25 en 26 van Richtlijn 95/46/EG. De export naar een derde land dat geen passend beschermingsniveau biedt kan slechts gebeuren mits toepassing van een van de bij artikel 26 voorziene uitzonderingen. Naast de ondubbelzinnige toestemming van de betrokkene, de noodzaak voor het sluiten of uitvoeren van een contract, een belangrijk algemeen belang, de vitale belangen van de betrokkene of de export – onder bepaalde voorwaarden – vanuit publieke registers, kan een verantwoordelijke ook overeenkomsten sluiten. Die overeenkomsten kunnen worden aangegaan met een andere verantwoordelijke voor de verwerking of met een verwerker naar wie de gegevens buiten de Europese Gemeenschap worden geëxporteerd. Ze moeten degene die de gegevens in een land zonder passend beschermingsniveau buiten de Europese Unie ontvangt, verplichten om bij de verwerking van de gegevens de Europese spelregels

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:NL:PDF
13 http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_nl.pdf
14 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_nl.pdf
15 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_nl.pdf

te volgen. Wie op grond van dergelijke overeenkomsten persoonsgegevens wil exporteren, moet daarvoor modelcontracten gebruiken die door de Europese Commissie ter beschikking worden gesteld.[16]

Voor internationale ondernemingen met vestigingen in talrijke landen vormen de modelcontracten geen ideale oplossing. Voor deze situatie wordt op Europees niveau de toepassing van "binding corporate rules" gepromoot. Dat zijn interne regels die binnen de internationale onderneming worden overeengekomen en vervolgens moeten goedgekeurd worden door de privacycommissarissen van alle landen waarin ze moeten worden toegepast. In de praktijk leidt dat laatste echter tot een eindeloze lijdensweg.

In België, bijvoorbeeld, voorziet de wet enkel in de mogelijkheid voor de Koning om, na advies van de Commissie, een doorgifte toe te laten indien de verantwoordelijke voor de verwerking voldoende waarborgen biedt. In de huidige stand van de wetgeving heeft dit als gevolg dat niet met "binding corporate rules" kan worden gewerkt zonder de uitvaardiging van een Koninklijk besluit daarover. Omdat een dergelijk besluit dat in het algemeen export op grond van dergelijke "binding corporate rules" toelaat, voorlopig ontbreekt, is voor General Electric, die van deze techniek gebruik wilde maken, ad-hoc een ontwerp van besluit opgesteld.[17]

§ 4. Doorgifte van persoonsgegevens naar de US

Voor de export van persoonsgegevens naar de Verenigde Staten geldt nog steeds de overeenkomst over de zogenaamde "safe harbor".[17] In de hier besproken periode is echter vooral discussie ontstaan rond de uitvoer van passagiersgegevens en uiteraard over de zaak "SWIFT".

Als gevolg van de aanslagen van 11 september 2001 werd in de Verenigde Staten de Aviation and Transportation Security Act uitgevaardigd. Die wet verplicht buitenlandse luchtvaartmaatschappijen aan de Amerikaanse overheid inzage in de gegevens van passagiers naar de Verenigde Staten te geven voor hun vertrek. Het gaat daarbij over gegevens uit het reserveringssysteem (PNR: Passenger Name Record). Daarin worden naast identificatiegegevens zoals naam en adres ook kredietkaartnummer, voedselvoorkeur, eventuele gezondheidsproblemen, vroegere reisboekingen en andere data opgeslagen.

De Amerikaanse eis plaatste de Europese luchtvaartmaatschappijen voor een moeilijk dilemma. Aan de ene kant riskeerden ze forse boetes die konden oplopen tot 3000 dollar per passagier. Aan de andere kant realiseerden ze zich dat de doorgifte van de passagiersgegevens naar de Verenigde Staten regelrecht indruist tegen de Europese privacywetgeving. In Europa mogen de reizigersdata uit een reserveringssysteem niet zomaar door de overheid worden gebruikt voor allerlei andere

16 http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm

17 Zie hierover het advies van de Privacycommissie van 21 maart 2007: http://www.privacycommission.be/nl/docs/Commission/2007/advies_13_2007.pdf

18 http://www.export.gov/safeharbor/

doeleinden. Export van persoonsgegevens buiten de Europese Unie is daarnaast enkel toegelaten naar landen die zelf ook een adequaat beschermingsregime bieden voor deze gegevens. De VS behoort alvast niet tot deze categorie. Daarom worden voor doorgifte van gegevens naar Amerika altijd strenge voorwaarden opgelegd.

De Europese Commissie kwam met een oplossing voor de dag door in onderhandelingen te treden met het Amerikaanse Homeland Security Departement. Dat leidde in 2004 tot een compromis. Zo werd het aantal datavelden waartoe de VS toegang krijgen, gereduceerd van 60 tot 34. In plaats van een "pull" systeem werd een "push" regeling uitgewerkt. De Amerikanen kunnen dus zelf niet rechtstreeks inloggen in het reserveringssysteem maar krijgen de data toegestuurd. De bewaringstermijn werd teruggebracht van 50 (!) naar 3,5 jaar. Tenslotte werden beperkingen opgelegd aan de Amerikaanse overheid voor het verdere gebruik van de passagiersgegevens (enkel voor bestrijding van criminaliteit en terrorisme).

Het compromis stootte op felle kritiek. Op het Internet werd de Europese Commissie door allerlei organisaties verweten dat ze de privacy van de Europese burgers aan de Amerikanen had verkocht. Ook het Europese Parlement vond dat het akkoord onvoldoende bescherming bood voor de Europese burgers. Volgens haar had de Commissie bovendien de verkeerde bevoegdheid aangewend om dit dossier te regelen.

Doorgifte van persoonsgegevens buiten de EU is, zoals al vermeld, alleen mogelijk naar landen die een adequaat beschermingsniveau hebben en de Commissie heeft de bevoegdheid hierover te beslissen. Volgens het Parlement mocht de Commissie die bevoegdheid echter niet gebruiken om met de Amerikanen een akkoord te sluiten over de strijd tegen terrorisme.

Het Europese Parlement heeft uiteindelijk via een arrest van het Europese Hof van Justitie van 30 mei 2006[19] gelijk gekregen met deze laatste stelling. Daarom is in juli 2007 een nieuw akkoord gesloten dat aan de kritiek van het Hof van Justitie tegemoetkomt. Inhoudelijk is dit nieuwe akkoord door de Europese privacycommissarissen echter onmiddellijk streng bekritiseerd.[20]

Op 19 juli 2006 ontving de Privacycommissie van het College voor Inlichtingen en Veiligheid een verzoek om een advies uit te brengen over "de vraag of er in het kader van het dossier "SWIFT" sprake is van een schending van de Belgische wetgeving, meer specifiek van de WVP". De Commissie verwoordde haar standpunt op deze vraag in een *advies nr. 37/2006 van 27 september 2006*.[21] De Commissie ontving vervolgens op 3 november 2006 het verzoek van de eerste minister om een advies uit te brengen over de inhoud en de vorm van een eventuele overeenkomst met de VS. In een tweede *advies van 20 december 2006* ver-

19 http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-317/04

20 http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_17_08_07_en.pdf

21 http://www.privacycommission.be/nl/docs/Commission/2006/advies_37_2006.pdf

leende de Commissie derhalve advies aan de Belgische Regering over deze aangelegenheid.[22] Dit advies herinnerde ook aan de mogelijke acties door de Belgische Regering en de Europese context voor de transfer van persoonsgegevens aan de UST. In een *advies van 22 november 2006* volgden de Europese privacycommissarissen (de Artikel 29 werkgroep) de bevindingen van het eerste "SWIFT advies" van de Belgische privacycommissie. In dit advies benadrukte de Artikel 29 werkgroep dat, zelfs in de strijd tegen het terrorisme, de fundamentele rechten dienen te worden gewaarborgd.[23]

Na de twee adviezen van de Commissie aan vertegenwoordigers van de Regering en de oproep van de Artikel 29 werkgroep ging de Privacycommissie begin 2007 van start met een bemiddeling ten aanzien van de betrokken financiële instellingen in België en SWIFT.[24] De Commissie onderzoekt sinds begin 2007 ook de wijze waarop de Belgische financiële instellingen hun klanten informeerden over het gebruik van het SWIFT netwerk en de doorgifte van persoonsgegevens door SWIFT aan de US autoriteiten.

§ 5. Communicatie van IP-adressen aan auteursrechthebbenden

Op 29 januari 2008 velde het Europese Hof van Justitie een arrest in de zaak Promusicae/ Telefónica.[25] Promusicae is een Spaanse vereniging waarvan de leden producenten en uitgevers van muzikale en audiovisuele opnamen zijn. Zij heeft de Spaanse rechterlijke instanties verzocht om Telefónica te gelasten, de identiteit en het adres te verstrekken van bepaalde personen aan wie zij internettoegang verschaft en van wie het „IP-adres" en de datum en het uur waarop zij met internet verbonden zijn geweest, bekend is. Volgens Promusicae gebruiken deze personen zogenaamde „peer-to-peer"netwerken om onder elkaar muziek of videobestanden uit te wisselen zonder rekening te houden met het auteursrecht.

Telefónica voerde aan dat volgens de Spaanse wet de door Promusicae gevraagde gegevens slechts mogen worden verstrekt in het kader van een strafrechtelijk onderzoek of wanneer dit nodig is ter waarborging van de openbare veiligheid en de landsverdediging. De Spaanse rechter wenste van het Hof van Justitie van de Europese Gemeenschappen te vernemen of de lidstaten volgens het gemeenschapsrecht ter verzekering van de doeltreffende bescherming van het auteursrecht de verplichting moeten opleggen om in het kader van een civiele procedure persoonsgegevens mee te delen.

Het Hof merkt in haar arrest op dat de richtlijnen betreffende de bescherming van persoonsgegevens onder meer een uitzondering maken voor de maatregelen die

---

22 http://www.privacycommission.be/nl/docs/Commission/2006/advies_47_2006.pdf

23 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_nl.pdf

24 Zie o.m. het "technisch dossier" dat door de Privacycommissie hierover is gepubliceerd: http://www.privacycommission.be/nl/static/pdf/cbpl-documents/technisch_dossier_swift.pdf

25 Zaak C-207/06. http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=NL&Submit=rechercher&numaff=C-275/06

nodig zijn voor de bescherming van andermans rechten en vrijheden. Aangezien de richtlijn betreffende privacy en elektronische communicatie niet preciseert om welke rechten en vrijheden het gaat, moet deze richtlijn aldus worden uitgelegd dat hieruit de wil van de wetgever blijkt om noch de bescherming van het eigendomsrecht, noch gevallen waarin de houders van auteursrechten ter bescherming van dit eigendomsrecht een civiele procedure instellen, van de werkingssfeer ervan uit te sluiten. Deze richtlijn sluit dus niet uit dat de lidstaten de verplichting opleggen om in het kader van een civiele procedure persoonsgegevens mee te delen. Zij dwingt de lidstaten evenwel evenmin om een dergelijke verplichting op te leggen.

Wat de richtlijnen betreffende de intellectuele eigendom betreft, stelt het Hof vast dat deze evenmin vereisen dat de lidstaten ter verzekering van de doeltreffende bescherming van het auteursrecht de verplichting opleggen om in het kader van een civiele procedure persoonsgegevens mee te delen.

Het Hof beklemtoont vervolgens dat het verzoek om een prejudiciële beslissing de vraag opwerpt hoe de vereisten inzake de bescherming van verschillende grondrechten, namelijk enerzijds het recht op eerbiediging van de persoonlijke levenssfeer en anderzijds het recht op bescherming van de eigendom en het recht op een doeltreffend beroep, met elkaar kunnen worden verzoend.

Op dit punt komt het Hof tot de conclusie dat de lidstaten zich bij de omzetting van de richtlijnen betreffende de intellectuele eigendom en de bescherming van persoonsgegevens moeten baseren op een uitlegging daarvan die het mogelijk maakt een juist evenwicht tussen de verschillende door de communautaire rechtsorde beschermde grondrechten te verzekeren. Bij de tenuitvoerlegging van de maatregelen ter omzetting van deze richtlijnen moeten de autoriteiten en de rechterlijke instanties van de lidstaten vervolgens niet alleen hun nationale recht conform deze richtlijnen uitleggen, maar er ook voor zorgen dat zij zich niet baseren op een uitlegging van deze richtlijnen die in conflict zou komen met deze grondrechten of de andere algemene beginselen van gemeenschapsrecht, zoals het evenredigheidsbeginsel.

III. Enkele markante beslissingen van de Belgische Privacycommissie

In een korte bijdrage kan geen exhaustief overzicht gegeven worden van de "rechtspraak" van de Privacycommissie in de afgelopen twee jaren. Hieronder wordt enkele markante aanbevelingen en adviezen geselecteerd waarin de Commissie haar – zeer brede – interpretatie van het begrip "persoonsgegevens" of sommige "moeilijke" regels uit de privacywet heeft gepreciseerd.

§ 1. Klasfoto's en ander beeldmateriaal

Op 28 november 2007 publiceerde de Commissie een aanbeveling over de toepassing van de privacywet op het nemen en publiceren van foto –en videomateriaal.[26] De beoogde situaties betreffen enkel deze waarin beelden worden geregistreerd (foto's, filmpjes, ...) van gebeurtenissen in 'besloten kring' (school, sportclub, vereniging, ...) via fototoestel, camera, gsm, … voor verspreiding op papier, het internet, via email, gsm, … . De aanbeveling maakt een onderscheid naargelang het beeldopnamen van minderjarigen of meerderjarigen betreft.

Ingevolge het recht op afbeelding dat aan elke persoon wordt toegekend, komt het in beginsel alleen aan de betrokken persoon toe te beslissen over de vervaardiging en het gebruik van de afbeelding van zijn beeltenis. Zowel het nemen van de foto, als de publicatie ervan zijn dus onderworpen aan de toestemming van de persoon die men wenst te fotograferen en wiens foto men wenst te publiceren. Volgens de privacywet moet die toestemming "ondubbelzinnig" maar niet noodzakelijk schriftelijk of uitdrukkelijk zijn. Stilzwijgende toestemming is voldoende en zou kunnen worden afgeleid uit het feit dat een persoon zich laat fotograferen tijdens een activiteit van een vereniging, en er zich bewust van is of behoorde te zijn dat de foto in het verenigingsblad kan worden gepubliceerd. Dit valt binnen het normaal verwachtingspatroon van de betrokkenen. Het gebruiken van deze foto om publiciteit voor de school of de vereniging te voeren, valt hier evenwel buiten.

Omwille van bewijsredenen is het, volgens de privacycommissie in de meeste gevallen echter aangewezen om één en ander schriftelijk vast te leggen. Dit kan praktisch gebeuren door ingeval van aansluiting bij een verenigingeen specifiek formulier aan de betrokkene voor te leggenover de vervaardiging en het gebruik van zijn afbeelding. "Hier kan men vervolgens een onderscheid maken naargelang de foto's (gericht of niet gericht). Voor de niet-gerichte foto's (bijvoorbeeld klas – of groepsfoto's) volstaat het om de betrokkenen te informeren dat zulke foto's worden genomen, voor welk doel en welke publicatie. Een toestemming is hier dus niet vereist. Voor de gerichte foto's (bijvoorbeeld een individuele foto) moet op een nauwkeurige wijze worden verwezen naar de soort(en) te nemen foto's/filmpjes, de verspreidingsvorm (intern of extern, via krantje, internet)."

Wat de toestemming van minderjarigen betreft, wordt meer en meer aanvaard dat een minderjarige met onderscheidingsvermogen zelf zijn toestemming kan geven. Dit begrip wordt door de huidige rechtspraak beoordeeld volgens de concrete, feitelijke omstandigheden van de zaak, maar dikwijls ligt de leeftijdsgrens in de buurt van 12 à 14 jaar. Indien het een minderjarige met onderscheidingsvermogen betreft,, meent de Commissie dat er van een samenwerkingssysteem dient te worden uitgegaan, waarbij de toestemming niet enkel door de wettelijke vertegenwoordigers wordt gegeven, doch tevens door de minderjarige.

De Commissie verwijst verder naar haar advies nr. 34/1999 van 13 december 1999, waarin ze stelde: 'Het begrip 'verwerking van beelden' strekt zich in het

[26] http://www.privacycommission.be/nl/docs/Commission/2007/aanbeveling_02_2007.pdf

kader van voorliggend advies uit tot elk opnamesysteem, analoog of numeriek, al dan niet onderbroken, met of zonder bewaring van deze opnames, op welke drager dan ook." Het fotograferen of filmen, al dan niet numeriek, is dus een geautomatiseerde verwerking uitmaken in de zin van de privacywet.

Verder wijst de Commissie op de uitzondering voor persoonlijke of huishoudelijke doeleinden (artikel 3, §2 van de privacywet). Dit is bijvoorbeeld het geval bij privé-opnamen van familiefeesten of sportmanifestaties. De uitzondering betreft een gebruik voor een duidelijk bepaalbare groep van personen: de toegang tot de gegevens dient beperkt te zijn tot een benoembare groep familieleden, kennissen of vrienden. Men kan hier als voorbeeld verwijzen naar foto's van een familiefeest die per email aan de aanwezigen worden gestuurd, of die op een beveiligde website worden geplaatst, die enkel toegankelijk is voor de betrokken familieleden, en waarvan de pagina's met persoonsgegevens zijn afgeschermd van zoekmachines. Indien deze gegevens evenwel worden verstrekt aan een onbepaald aantal personen, bijvoorbeeld via een vrij toegankelijke website, kan er op deze uitzondering geen beroep meer worden gedaan, en is de privacywet onverkort van toepassing.

In verband met de uitzondering voor journalistieke doeleinden (artikel 3, § 3 van de wet) schrijft de Privacycommissie dat deze uitzondering verbonden is met de uitoefening door journalisten van hun democratisch controlerecht, met name de zogenaamde "waakhondfunctie" van de pers in een democratische samenleving. "Het gaat dan ook over een uitzondering waarop in de naam van de persvrijheid een beroep kan worden gedaan, met name door een geaccrediteerde journalist in de zin van de wet van 30 december 1963 betreffende de erkenning en de bescherming van de beroepsjournalist12, of door éénieder die zulk een rol vervult. Een ledenblad van een vereniging of een schoolkrant vallen derhalve niet onder deze uitzondering."

Gelet op het feit dat het nemen en/ of het publiceren van een foto een (volledig of gedeeltelijk)

geautomatiseerde verwerking uitmaakt, dient de verantwoordelijke voor de verwerking in principe hiervan aangifte te doen bij de Privacycommissie overeenkomstig artikel 17 van de privacywet.

§ 2. Camera's in kinderdagverblijven

In een advies van 12 april 2006[27] bracht de Commissie advies uit over de installatie van camera's in kinderdagverblijven. De camera's ("webcams") bieden aan de ouders de mogelijkheid om op door de directie van het kinderdagverblijf vastgestelde tijdstippen via het Internet het gedrag van hun kind te observeren. Tegelijk krijgen zij echter ongewild eveneens de mogelijkheid om de andere kinderen en het personeel van het kinderdagverblijf te observeren, alsook externe partijen (sociale werkers, inspecteurs, animatoren,….).

[27] http://www.privacycommission.be/nl/docs/Commission/2006/advies_08_2006.pdf

Volgens de Commissie houdt de verspreidingsvorm via internet verder het risico in dat de beelden door derden op een al dan niet illegale wijze kunnen worden onderschept. Tevens kunnen de beelden worden hergebruikt door de ouders of derden voor andere doeleinden dan deze dewelke initieel door het kinderdagverblijf werden beoogd.

De kinderen zijn in dit geval, gezien hun leeftijd van 0-3 jaar, uiteraard niet bekwaam om hun toestemming te geven voor de geplande verwerking, aangezien zij minderjarig zijn en niet kunnen geacht worden over het noodzakelijke onderscheidingsvermogen te beschikken. Derhalve zal in dit geval de mogelijkheid om al dan niet toestemming te geven voor de geplande verwerking overgaan op de ouders, als wettelijke vertegenwoordigers van hun kind en als bestanddeel van hun ouderlijk gezag. De eventuele toestemming door de ouders zal dienen te zijn ingegeven door het belang van het kind. Het ouderlijk gezag is namelijk een geheel van doelgerichte bevoegdheden die uitsluitend in het belang van de minderjarige gegeven zijn.

Interessant in dit advies is vooral de passage waarin de Commissie toelicht dat het in de gegeven omstandigheden geen echte "vrije" toestemming betreft. Vooreerst heeft het kinderdagverblijf de toestemming van alle betrokken ouders nodig. Indien één van de betrokkenen zijn of haar toestemming weigert, kan het kinderdagverblijf derhalve niet overgaan tot het filmen van de aanwezige kinderen. Hier kunnen zich diverse praktijkproblemen stellen: wat bijvoorbeeld als de ouders het onderling niet eens zijn? Verder lijkt het waarschijnlijk dat het kinderdagverblijf bij het aanvaarden van nieuwe kinderen eerder deze zal weerhouden waarvan de ouders positief staan ten aanzien van een dergelijk webcamsysteem. Dit kan derhalve tot gevolg hebben dat de ouders, mede gelet op het tekort aan kinderopvang in de praktijk, niet volledig vrij zijn om hun toestemming te geven voor het webcamtoezicht.

Tenslotte moet de toestemming van de ouders op elk moment kunnen worden ingetrokken. Men kan zich de vraag stellen of zulk een intrekking werkelijk mogelijk is, gelet op de eventuele negatieve consequenties ervan voor het kind (bijvoorbeeld ontslag uit het kinderdagverblijf).

Omdat het webcamtoezicht niet kan gerechtvaardigd worden op grond van de ondubbelzinnige toestemming van de ouders (artikel 5 a) van de privacywet), onderzoekt de Privacycommissie vervolgens of geen beroep kan gedaan worden op artikel 5 f) van de wet. Op grond van die bepaling is een verwerking van persoonsgegevens gerechtvaardigd wanneer ze noodzakelijk is voor de behartiging van een rechtmatig belang van de verantwoordelijke mits het privacybelang van de betrokkene niet zwaarder doorweegt.

Volgens de Privacycommissie overweegt echter in dit geval het privacybelang. "Voor een jong kind zou de evolutie naar autonomie weer op losse schroeven kunnen gezet worden door de "virtuele" inmenging van ouders die het alledaagse leven van hun kind wensen te zien: "wanneer een ouder 's avonds het kind opvangt en vertelt dat hij het heeft zien spelen met een bepaald vriendje of een

bepaald stuk speelgoed, is de ouder niet langer de volwassene waarop men kan steunen maar een alwetende god die alles ziet en alles weet. Het kind zou aldus een vals veiligheidsgevoel kunnen hebben en de indruk krijgen dat zijn ouder over hem waakt, ook al is hij niet fysiek aanwezig".

Daarom acht de Commissie de installatie van webcams dan ook als disproportioneel in de zin van artikel 5, f) te kunnen worden beschouwd. In casu dient het belang van het kind te prevaleren op het belang van de verantwoordelijke voor de verwerking.

§ 3. Luchtfoto's en satellietbeelden

In een advies van 12 juli 2006[28] heeft de Privacycommissie zich uitgesproken over het gebruik van satellietbeelden voor het vaststellen van bouwovertredingen. De satellietbeelden betreffen beelden van percelen welke mogelijks toebehoren aan natuurlijke personen. De dienst stedenbouw kan vervolgens de eigenaar(s) van een bepaald perceel identificeren. De Commissie besluit dan ook dat de geautomatiseerde verwerking van satellietbeelden van eigendommen van natuurlijke personen, door de dienst stedenbouw, als een verwerking van persoonsgegevens dient te worden beschouwd." Derhalve zal de privacywet erop van toepassing zal zijn. Deze conclusie is zeer verregaand en voor discussie vatbaar. Ze leidt ertoe dat ook het fotograferen van een huis, een voertuig, een meubel of een paraplu als een verwerking van persoonsgegevens kan worden beschouwd, op voorwaarde tenminste dat de eigenaar van die goederen een identificeerbare natuurlijke persoon is. De toepassing van de privacywet wordt hiermee op slag aanzienlijk verbreed.

Gelet op voormelde strafsancties inzake bouwovertredingen maakt de verwerking van satellietfoto's door middel waarvan bouwovertredingen worden vastgesteld, volgens de Privacycommissie, verder een verwerking van gerechtelijke gegevens uit in de zin van artikel 8 van de wet. In principe is een dergelijke verwerking overeenkomstig de privacywet verboden. Artikel 8, §2 voorziet evenwel in een aantal uitzonderingsgevallen, waarbij in casu punt a) van belang is: onder toezicht van een openbare overheid of van een ministeriële ambtenaar in de zin van het gerechtelijk wetboek, indien de verwerking noodzakelijk is voor de uitoefening van hun taken; evenals punt b): door andere personen, indien de verwerking noodzakelijk is voor de verwezenlijking van doeleinden die door of krachtens een wet, een decreet of een ordonnantie zijn vastgesteld.

Rond dezelfde periode publiceerde de Privacycommissie ook een advies over het publiceren van luchtfoto's en plannen van onbebouwde percelen op het Internet.[29] Het doel van een dergelijke publicatie bestaat erin een actieve openbaarheid te garanderen van de potentiële reserves van gronden in elke gemeente. Daarom wordt de lijst van bouwkavels die opgenomen zijn in het ROP (Register onbebouwde percelen) publiek ter beschikking gesteld via een "atlas van de woonge-

[28] http://www.privacycommission.be/nl/docs/Commission/2006/advies_26_2006.pdf
[29] http://www.privacycommission.be/nl/docs/Commission/2006/advies_40_2006.pdf

bieden". Bedoeling van deze atlas is om diegenen die in een gemeente op zoek zijn naar een bouwgrond, kosteloos kennis te laten nemen van wat er bestaat aan mogelijke bouwpercelen.

Opnieuw stelt de Privacycommissie dat de publicatie op het Internet van de foto's en plannen van de onbebouwde percelen onvermijdelijk de identificatie van hun eigenaars meebrengt. "Inderdaad, de bedoelde percelen kunnen herkend worden aan de hand van hun situatie, door zich ter plaatse te begeven of door ze te koppelen aan een plan met de huisnummers. Nadat een potentiële gegadigde aldus in het bezit gekomen is van het adres van het perceel zal hij vrij gemakkelijk via de diensten van het kadaster de eigenaar kunnen identificeren".

In hetzelfde advies is de Commissie ook opnieuw ingegaan op de relatie tussen privacy en openbaarheid van bestuur. Het advies bevestigt de rechtspraak van de Commissie inzake openbare registers, zoals o.m. samengevat in het advies van 10 september 2001 betreffende de organisatie van de openbaarheid van het kadaster. Voor de Commissie is het essentieel dat "de mededeling aan derden van gegevens uit de openbare of semi-openbare registers een vorm van extern gebruik moet zijn waarbij wordt getracht het wettelijk en gewettigd doel te verwezenlijken dat de grondslag van de verwerking vormt in dit geval het openbaar of semi-openbaar register".

Zoals door de Commissie werd herinnerd in haar adviezen nr. 26/97, 28/97 en 21/2005, wordt het conflict tussen twee fundamentele rechten, zoals het recht op de eerbiediging van het privéleven en het recht op informatie, geval per geval opgelost door de methode van afweging van de concurrerende belangen; de individuele beslissingen tot machtiging of weigering zouden idealiter door een onafhankelijke instantie moeten worden genomen. Het is, volgens de Privacycommissie, bovendien slechts indien de mededeling van persoonsgegevens aan een derde de bovenhand krijgt op de rechten en belangen van de betrokkene, dat deze mededeling mogelijk wordt. Bovendien moet, gelet op de risico's verbonden aan de ontwikkeling van de informatie- en communicatietechnologie, deze afweging van concurrerende belangen met grote zorgvuldigheid gebeuren.

In casu stelt de Commissie zich vragen bij het gewettigd karakter van een dergelijke openbaarheid en de impact die deze zou hebben inzake bescherming van de persoonlijke levenssfeer. Dit soort openbaarheid lijkt niet verenigbaar met het doeleinde bij de oprichting van de registers van onbebouwde percelen. Deze registers zijn in de eerste plaats een instrument voor het grondbeleid dat aan de gemeenten toelaat studies te verrichten over de woningnood met het oog op het eventueel uitbreiden van de woonzone. Het vergemakkelijken van immobiliënreclame voor onbebouwde percelen kadert apriori niet in hun opdrachten van algemeen belang inzake grondbeleid en is onevenredig in die mate dat iedere eigenaar die zijn onbebouwd perceel wenst te verkopen, zelf maatregelen neemt om deze verkoop openbaar te maken.

De organisatie van een actieve openbaarheid van het grondbeleid via het Internet moet verenigbaar zijn met het doeleinde van het bijhouden van een register van

onbebouwde percelen en zodanig zou worden georganiseerd dat er geen risico bestaat op aantasting van de rechten op bescherming van het privéleven. De perceeleigenaars lopen inderdaad het risico op ongepaste ogenblikken lastig gevallen te worden indien de gezuiverde plannen van de percelen of luchtfoto's in een schaal kleiner dan 1/50.000 op het Internet zouden gepubliceerd worden. Volgens de Privacycommissie is de realisatie van deze openbaarheid aan de hand van een luchtfoto van het grondgebied van de volledige gemeente op een schaal 1/50.000, zoals gevoegd bij de aanvraag, zonder mogelijkheid van enige geïnformatiseerde selectie, het verst dat men in deze situatie kan gaan.

§ 4. Uitwisseling van gegevens door fiscale administraties

In een advies van 19 september 2007[30] heeft de Privacycommissie geoordeeld dat fiscale administraties onderling gegevens mogen uitwisselen, voorzover ze binnen hun wettelijke bevoegdheden blijven. De discussie over dit onderwerp startte in de zomer van 2004. Het Europees Hof van Justitie velde toen een arrest waarin de Belgische beurstaks niet verenigbaar werd geacht met de Europese richtlijn. Beleggers kregen daarop de mogelijkheid om de ten onrechte betaalde beurstaks terug te vragen. De overheid kreeg maar liefst 426.000 aanvragen tot terugbetaling binnen. Tot op heden zijn alle dossiers nog altijd niet afgewerkt. In totaal werd al meer dan 120 miljoen euro aan de beleggers terugbetaald.

De administratie van de inkomstenbelastingen selecteerde uit de aanvragen tot terugbetaling 29.000 dossiers. Ze deed dat op basis van de hoogte van het teruggevraagde bedrag en het beroep van de belegger (bedrijfsleider of zelfstandige). Bedoeling was te onderzoeken of de inlichtingen die hun collega's hadden verkregen via de aanvragen tot terugbetaling, verenigbaar waren met de aangiften die voor de inkomstenbelastingen waren ingediend.

Die uitwisseling van gegevens tussen fiscale administraties leidde tot een discussie over een mogelijke schending van de privacywet. Eerder waren al gelijkaardige twijfels gerezen toen de fiscus gegevens over het koopgedrag van belastingsplichtigen opvroeg bij de grootwarenhuizen. De privacywet verbiedt namelijk dat persoonsgegevens die in een bepaalde context worden verzameld, hergebruikt worden voor andere doeleinden die daarmee niet verenigbaar zijn. Wie zijn wekelijkse aankopen doet in een grootwarenhuis en daarbij een klantenkaart gebruikt, verwacht niet direct dat zijn aankoopgegevens aan de fiscus zullen doorgegeven worden. Daarom is die praktijk ook niet verzoenbaar met de genoemde regel uit de privacywet.

Om een einde te stellen aan de twijfels over de actie van de fiscus tegen de beleggers die hun beurstaks terugvroegen, legde de Staatssecretaris voor modernisering van de financiën de kwestie voor aan de Privacycommissie. In het advies van 19 september stelde deze laatste vast dat de wet in dit geval zelf bepaalt welke gegevens door administraties gebruikt mogen worden. Inderdaad bepaalt artikel 336

[30] http://www.privacycommission.be/nl/docs/Commission/2007/advies_27_2007.pdf

van het Wetboek Inkomstenbelastingen dat elke inlichting die een ambtenaar van een fiscaal staatsbestuur in het uitoefenen van zijn functie ontdekt, door de Staat kan worden ingeroepen voor het opsporen van belastingsschulden. Op grond van dat artikel konden de inlichtingen verkregen door de ene fiscale administratie (AKRED: administratie van het kadaster, registratie en domeinen), hergebruikt worden door een andere fiscale administratie (AOIF: administratie van de ondernemings – en inkomstenfiscaliteit).

Het advies van de Privacycommissie ligt in de lijn van eerdere uitspraken van het Hof van Cassatie en van de Europese Commissie voor de Rechten van de Mens. Het Hof van Cassatie velde in 1981 een uitspraak over een belastingsplichtige die onroerende goederen had verkocht voor ruim 6 miljoen frank. Ondervraagd door de fiscus n.a.v. een controle, kon hij geen aanvaardbare uitleg geven over hoe hij de opbrengst had besteed. Daarop werd hij ambtshalve belast: de fiscus ging ervan uit dat het bedrag werd belegd met een belastbare jaarlijkse intrest van 5 procent. De belastingsplichtige verzette zich op grond van de schending van het respect voor de privacy. Volgens hem kon hij niet verplicht worden om aan de fiscus een lijst voor te leggen van zijn privé-uitgaven om te bewijzen hoe hij de 6 miljoen uit de verkoop van onroerend goed had besteed. Het Hof van Cassatie gaf de fiscus echter gelijk en stelde dat inmengingen van de overheid in het privéleven van de burgers toegelaten zijn voor het economisch welzijn van het land. Dit oordeel werd op Europees niveau nadien bevestigd.

In principe schrijft de privacywet ook voor dat de betrokkene geïnformeerd moet worden indien persoonsgegevens worden verwerkt. De vraag was dus ook of de aanvragers voor terugbetaling van de beurstaks niet verwittigd hadden moeten worden dat de informatie ook voor fiscale controle gebruikt kon worden. De Privacycommissie heeft ook op dit punt de fiscus gelijk gegeven. Bij hergebruik van gegevens moet de betrokkene niet worden geïnformeerd indien dit hergebruik voorgeschreven wordt door een wettelijke of reglementaire bepaling.

§ 5. Klokkenluiders

Op 29 november 2006) publiceerde de Commissie voor de bescherming van de persoonlijke levenssfeer een aanbeveling over *klokkenluiden*. ("whistleblowing").[31]

Klokkenluiders zijn werknemers, medewerkers of leden van een organisatie die rapporteren over misbruiken in hun organisatie. Een bekend voorbeeld is dat van de Amerikaan Jeffrey Wigand, een werknemer van een bekend internationaal bedrijf in de tabaksector, die aan het licht bracht dat de bedrijfsleiding schadelijke stoffen in sigaretten mengde om het verslavend karakter ervan te verhogen. In sommige landen, o.m. het Verenigd Koninkrijk bestaat over klokkenluiden in deze betekenis sinds enkele jaren specifieke wetgeving. In ons land voorlopig nog niet.

[31] http://www.privacycommission.be/nl/docs/Commission/2006/-aanbeveling_01_2006.pdf

Steeds meer bedrijven leggen aan hun werknemers op om misbruiken die zij vaststellen, onmiddellijk aan de directie te melden. Dikwijls worden daarvoor webformulieren op de bedrijfssite geplaatst.

Sinds enige tijd legt men ook een verband tussen deze regels en de toepassing van bijvoorbeeld de Sarbanes-Oxley wetgeving. Sectie 301(4) van deze wet bepaalt dat werknemers van een onderneming hun bezorgdheid moeten kunnen uiten bij het auditcomité over twijfelachtige boekhoudkundige kwesties. Daarbij moet het bedrijf aan die werknemers garanties bieden van anonimiteit en vertrouwelijkheid.

De Privacycommissie heeft onderzocht aan welke voorwaarden klokkenluidersystemen moeten voldoen om verenigbaar te zijn met de privacywetgeving. Eerder er ook al een advies hierover van de Artikel 29 werkgroep.[32]

In het algemeen maant de Commissie aan tot voorzichtigheid. Zo geldt de Amerikaanse SOX-wetgeving niet voor alle Belgische bedrijven. Bovendien geldt de meldingsplicht enkel voor boekhoudkundige en auditkwesties. Voor bedrijven die geen enkele band hebben met de Verenigde Staten en voor andere kwesties (bijv. pesterijen op het werk) zijn klokkenluidersystemen niet verboden maar moet men rekening houden met beperkingen.

Toezicht en controle in de onderneming moet normaal worden uitgeoefend via hiërarchische weg. Een intern meldsysteem mag enkel beschouwd worden als een specifiek subsidiair kanaal. Het kan enkel gaan om meldingen van problemen die gewoonlijk niet via de normale hiërarchische kunnen worden gedetecteerd (bijv. ongewenste intimiteiten).

De Commissie raadt in elk geval aan om over het systeem een duidelijke *policy* op te stellen. Daarin moeten de scope en de grenzen van het interne meldingssysteem goed omschreven worden. Ook een accurate beschrijving van de procedure voor indiening en behandeling van de meldingen is belangrijk. Er moet tevens aangeduid worden wat de gevolgen zijn van onterechte meldingen.

Uit de aanbeveling blijkt verder dat de Privacycommissie tegenstander is van verplichte meldingssystemen. Het systeem blijft best facultatief. Men moet ook geen meldingen aanmoedigen, bijvoorbeeld door de klokkenluider een beloning voor te spiegelen. Anonieme meldingen mogen absoluut een uitzondering blijven. Het meldsysteem mag zeker niet leiden tot een "klik"-cultuur in het bedrijf.

Meldingen worden, volgens de Commissie, best behandeld door een daartoe aangestelde klachtenbehandelaar. Deze laatste moet ervoor zorgen dat de meldingen discreet worden behandeld met respect voor de persoonlijke levenssfeer van de betrokkenen. Tot slot valt elk geautomatiseerd meldsysteem (bijv. via een website of e-mail) ook onder de aangifteplicht bij de Commissie.

---

32 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_nl.pdf