Recht en ICT

Recente ontwikkelingen in het privacyrecht: 2010-2013

Jos DUMORTIER
gewoon hoogleraar ICRI KU Leuven, advocaat time.lex Brussel

Yung Shin VAN DER SYPE
wetenschappelijk medewerker ICRI KU Leuven

I. Inleiding

Privacy is actueel. Nooit eerder was de media-aandacht voor de bescherming van de persoonlijke levenssfeer zo hoog. In de media werd uitgebreid gerapporteerd over klokkenluiders[1], informatielekken en overheidsspionage-schandalen. De laatste jaren werd het recht op respect voor privacy steeds vaker aangewend en aangepast, toegepast en toegelicht vanuit juridisch perspectief. Zo werd bijvoorbeeld de cookie-wetgeving gewijzigd (door de wet van 10 juli 2012) en de omzetting van de zogenaamde 'dataretentierichtlijn' afgerond (door de wet van 30 juli 2013).
De ontwikkelingen zijn amper bij te houden. Niettemin trachten we in deze bijdrage toch ten minste de meest opvallende ontwikkelingen te schetsen. Daarbij maken we een onderscheid tussen drie aspecten van privacy- en gegevensbescherming:

1. de algemene regels tot bescherming van de persoonlijke levenssfeer, zoals die onder meer te vinden zijn in artikel 22 van de Belgische Grondwet, artikel 7 en 8 van het EU-Handvest en artikel 8 van het Europees Verdrag van de Rechten van de Mens (afdeling II);
2. de specifieke regels tot bescherming van het individu ten aanzien van de verwerking van zijn persoonsgegevens, zoals beschermd door de Europese Richtlijn 95/46/EG en de Belgische omzetting daarvan in de wet van 8 december 1992 (afdeling III);
3. de specifieke regels tot bescherming van het individu in het domein van zijn (private) elektronische communicatie, zoals geregeld door de Europese Richtlijn 2002/58/EG en de Belgische omzetting daarvan in de wet van 13 juni 2005 (afdeling IV).

Hoewel de keuze van de hieronder besproken *capita selecta* sterk vanuit Belgisch perspectief werd geïnspireerd, kan een bespreking van een aantal belangrijke Europese ontwikkelingen niet achterwege worden gelaten.

II. Bescherming van de persoonlijke levenssfeer

§1. Artikel 8 Europees Verdrag van Rechten van de Mens

De hoeksteen van de bescherming van de persoonlijke levenssfeer in Europa blijft nog steeds artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM). Artikel 8 EVRM luidt als volgt:

> *'1. Eenieder heeft het recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*

[1] Zie hierover o.m. ook Advies nr. 35/2011 van 21 december 2011, www.privacycommission.be.

2. Geen inmenging van openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid en het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.'

Deze bepaling kan niet alleen worden ingeroepen bij inmengingen vanwege de overheid, zoals uit de tweede alinea van artikel 8 ten onrechte zou kunnen worden afgeleid. Het kan ook toegepast worden op betrekkingen tussen particulieren.[2]

Uit de toepassing van artikel 8 EVRM door het Europees Hof van de Rechten van de Mens kan men interessante preciseringen halen over het begrip 'persoonlijke levenssfeer'. Zo weet men nu, nog duidelijker dan voorheen, dat bij de interpretatie ervan moet worden rekening gehouden met de betrokken persoon en met plaats en tijd. De persoonlijke levenssfeer van een magistraat of een overheidsambtenaar vraagt bijzondere zorg en bescherming omdat dit zo belangrijk is voor het vertrouwen van het publiek.[3] Omgekeerd is de persoonlijke levenssfeer van publieke personen, bijvoorbeeld uit de amusementssector of de koninklijke families, enger dan voor een doodgewone Jan met de pet.[4]

Naast deze elasticiteit heeft het begrip 'persoonlijke levenssfeer' ook een verschillende betekenis naargelang het slaat op de integriteit van de eigen lichamelijkheid of op de relaties met anderen. In het eerste geval gaat het over de vraag in hoeverre een persoon over zijn eigen lichaam mag beschikken.[5] In het tweede geval gaat het over de wijze waarop de persoon de relaties met zijn onmiddellijke omgeving organiseert en zijn recht op bescherming van de correspondentie uitoefent.[6] Daarenboven heeft het begrip 'persoonlijke levenssfeer' ook te maken met het zelfbeschikkingsrecht op de informatie over zich-

---

2 Zie bv. EHRM 15 januari 2009, *Reklos en Davourlis t. Griekenland*, http://hudoc.ehcr.coe.int, waar het gaat over een klacht van ouders tegen een ziekenhuisfotograaf die zonder hun toestemming een foto van hun pasgeboren baby had gemaakt. De ouders stapten naar het Griekse gerecht maar kregen geen voldoening. Daarop dienden zij een klacht in tegen de Griekse Staat. Op die manier komt een conflict tussen particulieren toch bij het Hof in Straatsburg.

3 Zie o.m. EHRM 11 maart 2003, *Lesnik t. Slovakije*, http://hudoc.echr.coe.int; EHRM 14 januari 2014, *Lavric t. Roemenië*, http://hudoc.echr.coe.int.

4 O.m. EHRM 24 juni 2004 en EHRM 7 februari 2012, *Von Hannover t. Duitsland*, http://hudoc.ehcr.coe.int.

5 Zie bijvoorbeeld de discussies over de bloedproef bij verkeerscontroles, de verplichting tot het dragen van een veiligheidshelm of autogordel, maar ook: het verbod om de as van een overledene in diens eigen tuin te verstrooien, en de discussies over de toepassing van artikel 8 EVRM op verbodsbepalingen inzake onder meer homoseksualiteit, geslachtsverandering of abortus.

6 Zie bv. in dit verband EHRM 13 mei 2008, *N.N. en T.A. t. België*, http://hudoc.ehcr.coe.int; EHRM 4 december 2012, *Lenev t. Bulgarije*, http://hudoc.ehcr.coe.int, over de strijdigheid van de Bulgaarse afluisterwetgeving met artikel 8 EVRM; EHRM 8 januari 2013, *Bucur en Toma t. Roemenië*, http://hudoc.echr.coe.int; EHRM 9 januari 2013, *Volkov t. Oekraine*, http://hudoc.echr.coe.int.

zelf. In die zin bevat artikel 8 in zekere zin ook een recht op bescherming van eer en reputatie.[7]
De toepassing van het tweede lid van artikel 8 EVRM is meestal een kwestie van afweging en van zoeken naar een evenwicht tussen de bescherming van het individu en de noden van de overheid. Hiervoor wordt telkens nagegaan of argumenten als openbare orde en veiligheid, misdaadpreventie, enz. opwegen tegen het fundamentele recht dat door artikel 8 wordt gegarandeerd.[8] Zo oordeelde het Hof bijvoorbeeld dat de oprichting van databanken met gegevens over DNA en vingerafdrukken strijdig is met artikel 8 van het EVRM indien het over onschuldige burgers gaat;[9] maar dat bedrijven door de fiscus wel kunnen bevolen worden om een kopie van een gedeelde computerserver ter beschikking te stellen ten behoeve van de inspectie indien voldoende effectieve en adequate waarborgen tegen misbruik zijn voorzien.[10]
Naast de verplichting voor de Belgische overheid om zich van ongeoorloofde inmenging te onthouden, kan artikel 8 EVRM in bepaalde gevallen voor de overheid positieve verplichtingen in het leven roepen.[11] Zoals het Europees Hof meermaals heeft opgemerkt, zijn de grenzen van de positieve en negatieve verplichtingen niet precies aangegeven. In beide gevallen moet een '*fair*' evenwicht worden gevonden tussen de strijdende belangen van het individu en die van de samenleving.[12]

§2. Artikelen 7 en 8 van het EU-Handvest

Artikel 7 van het Handvest van de grondrechten van de Europese Unie (hierna: EU-Handvest) luidt als volgt: 'eenieder heeft recht op eerbiediging van zijn

7 Zie o.m. EHRM 14 oktober 2008, *Petrina t. Roemenië*, http://hudoc.echr.coe.int; EHRM 6 januari 2009, *Pfeiffer t. Oostenrijk*, http://hudoc.echr.coe.int; EHRM 9 april 2009, A. t. Noorwegen, http://hudoc.echr.coe.int; EHRM 18 januari 2011, *Mikolajova t. Slovakije*, http://hudoc.echr.coe.int.

8 O.m. EHRM 6 december 2012, *Michaud t. Frankrijk*, http://hudoc.echr.coe.int, in verband met huiszoeking in een advocatenkantoor. Het Hof oordeelde dat de beide voorwaarden van artikel 8, tweede lid EVRM – maatregel voorzien bij de wet en noodzakelijkheid in een democratische samenleving – *in casu* zijn vervuld.

9 EHRM 4 december 2008*, S. & Marper t. Verenigd Koninkrijk*, http://hudoc.echr.coe.int.

10 Zie o.m. EHRM 14 maart 2013, *Bernh Larsen Holding AS e.a. t. Noorwegen*, http://hudoc.echr.coe.int.

11 EHRM 13 juni 1979, *Marckx t. België*, http://hudoc.echr.coe.int; EHRM 19 februari 1998, *Guerra e.a. t. Italië*, http://hudoc.echr.coe.int; zie ook *Rev. trim. D.H.* 1998, 808, noot P. FRUMER; EHRM 30 juli 1998, *Sheffield en Horsham t. Verenigd Koninkrijk*, http://hudoc.echr.coe.int.

12 EHRM 17 juli 2008, *Leschiutta en Fraccaro t. België*, http://hudoc.echr.coe.int; EHRM 17 oktober 2008, *I. t. Finland*, http://hudoc.echr.coe.int: 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'.

privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie'. Dit artikel stemt dus overeen met artikel 8, eerste lid EVRM.
Daarnaast bepaalt artikel 8, eerste lid van het Handvest dat '[e]enieder recht [heeft] op bescherming van de hem betreffende persoonsgegevens'. Naast het recht op bescherming van de persoonlijke levenssfeer erkent het EU-Handvest dus een afzonderlijk recht op gegevensbescherming. Het recht op bescherming van persoonsgegevens heeft, zoals het recht op privacybescherming, geen absolute gelding, maar moet in relatie tot de functie ervan in de maatschappij worden beschouwd.[13] Artikel 8, tweede lid van het Handvest laat bijgevolg onder bepaalde voorwaarden de verwerking van persoonsgegevens toe. In dat verband is vereist dat de persoonsgegevens 'eerlijk [moeten] worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet'.
In artikel 52, eerste lid van het Handvest wordt algemeen erkend dat aan de uitoefening van rechten zoals die welke in de artikelen 7 en 8 van het Handvest zijn erkend, beperkingen kunnen worden gesteld, voor zover deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten en vrijheden eerbiedigen, en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.
Uit artikel 52, derde lid van het Handvest volgt dat voor zover in het Handvest rechten zijn opgenomen die corresponderen met rechten welke zijn gegarandeerd door het EVRM, de inhoud en reikwijdte ervan dezelfde zijn als die welke er door genoemd verdrag aan worden toegekend. Met het oog daarop voegt artikel 53 van het Handvest hieraan toe dat geen van haar bepalingen mag worden uitgelegd als zou zij een beperking vormen van of afbreuk doen aan de rechten die met name door het EVRM worden erkend. In deze omstandigheden dient enerzijds te worden vastgesteld dat de eerbiediging van het in de artikelen 7 en 8 van het Handvest erkende recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens gelijk welke informatie betreft aangaande een geïdentificeerde of identificeerbare natuurlijke persoon.[14] Anderzijds dient te worden opgemerkt dat de beperkingen die mogen worden gesteld aan het recht op bescherming van de persoonsgegevens, overeenkomen met deze die worden toegelaten in het kader van artikel 8 EVRM.[15] Uit de toenemende rechtspraak van het Europese Hof van Justitie volgt o.m. nog dat een arbeidstijdregister dat voor elke werknemer het begin en het einde van de arbeidstijd alsook de bijhorende onderbrekingen of pauzes, onder het begrip 'persoonsgegevens' in de zin van het Handvest valt[16]; en dat het afnemen van vingerafdrukken zowel als de bewaring ervan in het paspoort, gerechtvaardig-

13 Zie HvJ C-112/00, S*chmidberger*, 2003, en de daarin aangehaalde rechtspraak, http://curia.europa.eu; HvJ C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito*, 2011, http://curia.europa.eu.
14 Zie met EHRM 16 februari 2000, *Amann t. Zwitserland*; EHRM 4 mei 2000, *Rotaru t. Roemenië*, http://hudoc.echr.coe.int.
15 HvJ C-92/09 en C-93/09, *Volker en Markus Schecke en Eifert*, 2010, http://curia.europa.eu; zie ook *CML Rev.* 2011, afl. 6, 2005, noot M. BOBEK.
16 HvJ C-342/12, *Worten*, 2013, http://curia.europa.eu.

de maatregelen kunnen zijn om frauduleus gebruik van paspoorten te voorkomen.[17]

§3. Artikel 22 van de Grondwet

Op nationaal niveau geniet de persoonlijke levenssfeer ook een grondwettelijke bescherming. Artikel 22 van de Belgische Grondwet luidt als volgt:

> *'Ieder heeft het recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht.'*

Recentelijk werden enkele wetswijzigingen voor het Grondwettelijk Hof aangevochten op grond van een vermeende schending van artikel 22 van de Grondwet. Een eerste voorbeeld betreft de veel besproken fiscale uitzonderingsmaatregelen waardoor het fiscaal bankgeheim (gedeeltelijk) werd opgeheven.[18] Begin 2013 boog het Grondwettelijk Hof zich tot tweemaal toe over deze materie.[19] In beide zaken ging het Hof na of de nieuwe maatregel een schending uitmaakte van artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 EVRM, in zoverre zij de belastingadministratie toeliet elke bank-, wissel-, krediet-, of spaarinstelling ertoe te verplichten aan haar gegevens mee te delen die de instelling bezit met betrekking tot een belastingplichtige ten aanzien van wie de administratie beschikt over aanwijzingen van fraude of wanneer zij zich voorneemt een beroep te doen op artikel 341 van het WIB 1992. Om de geoorloofdheid van de inmenging te beoordelen onderwierp het Grondwettelijk Hof de onderzoeksmethode aan een proportionaliteitstoets. Tweemaal werd een schending afgewezen. Het Hof was de mening toegedaan dat de bestreden maatregel een doelstelling van algemeen belang nastreeft, in zoverre de correcte vestiging van de belasting nodig is ter verzekering van het economisch welzijn van het land. Bovendien, vervolgde het Hof, was de regeling gestoeld op een voldoende duidelijke en voorzienbare grondslag, zodat elk individu in de gegeven omstandigheden in redelijke mate de gevolgen van een bepaalde handeling kon voorzien. Alsook werden daarbij voldoende waarborgen voorzien tegen willekeurige inmengingen van het privéleven van de belas-

17 HvJ C-291/12, *Schwarz*, 2013, http://curia.europa.eu.

18 Artikel 55 en 56 van de wet van 14 april 2011 houdende diverse bepalingen wijzigden artikel 322 WIB 1992 en voegden aldaar een artikel 333/1 in, *BS* 6 mei 2011; Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr. 12/2010 van 31 maart 2010; Advies nr. 13/2010 van 31 maart 2010 en Advies nr. 36 van 21 december 2011.

19 Gw Hof 14 februari 2013, nr. 6/2013; Gw Hof 14 maart 2013, nr. 39/2013, *T.F.R.* 2013, 498, noot J. BOSSUYT en F. DEBELVA. In de '*De Gucht*'-zaak werd op 17 december 2013 door het Hof van Beroep te Gent geoordeeld dat de fiscus niet over voldoende aanwijzingen van belastingontduiking beschikte. De machtiging om de rekeningen van het echtpaar De Gucht in te kijken werd vernietigd en aldus kunnen de daaruit verkregen gegevens niet door de fiscus worden gebruikt.

tingplichtige en van de personen met wie hij financiële verrichtingen heeft gedaan.

Een tweede voorbeeld van hoe het privacy-debat tot in het Grondwettelijk Hof werd gebracht betrof de discussie rond het boerka-verbod.[20] Met de wet van 1 juni 2011 werd een artikel 563*bis* in het Strafwetboek ingevoegd dat het dragen van kleding die het gezicht volledig dan wel grotendeels verbergt verbiedt. Een aantal burgers vochten deze wet aan op grond van verschillende grondwetsbepalingen. Naast de individuele vrijheid (art. 12 Gw.), de godsdienstvrijheid (art. 19 Gw.), en het recht van eenieder op een menswaardig leven (art. 23 Gw.), kreeg de discussie ook een privacy-rechtelijke insteek door de toetsing ervan aan artikel 22 van de Grondwet. Zoals steeds, bestaat de grondwettigheidstoets van het Hof erin om na te gaan of de inmenging wordt voorzien door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte, en evenredig is met de nagestreefde wettige doelstelling. Het Hof oordeelde dat de wet voldoende duidelijk is om eenieder toe te laten om, op het ogenblik dat een bepaald gedrag wordt aangemeten, te weten of dat gedrag al dan niet onder het toepassingsgebied van de wet valt en bijgevolg al dan niet strafrechtelijk kan worden bestraft. Bovendien beantwoordt de wet, aldus het Hof, ook aan een dwingende maatschappelijke behoefte, doordat een verbod op het dragen van gezichtsverhullende kledij onder meer is ingegeven door redenen van openbare veiligheid.

III. Bescherming van persoonsgegevens

§1. Inleiding

Aan de algemene Europese en nationale regels over de bescherming van de persoonlijke levenssfeer, is sinds de tweede helft van vorige eeuw specifieke wetgeving toegevoegd over de bescherming van het individu bij de verwerking van persoonsgegevens. Momenteel wordt dit hoofdstuk nog beheerst door de Europese Richtlijn 95/46/EG die in 1998 in België werd omgezet met een grondige aanpassing van de wet van 8 december 1992.[21] Dit landschap zou echter drastisch kunnen veranderen indien het voorstel van de Europese Commissie tot invoering van een verordening betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens, aanvaard zou worden.[22]
In België is de bescherming van de persoonlijke levenssfeer grotendeels een federale materie. Niettemin is aanvaard dat ook de gemeenschappen en gewesten beperkingen op het recht op privacybescherming kunnen aanbrengen voor zover deze kaderen binnen de regeling van een aangelegenheid die tot hun be-

20 Gw Hof 6 december 2012, nr. 145/2012 waarin het Grondwettelijk Hof de beroepen tot vernietiging van de wet van 1 juni 2011 verwerpt.

21 Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

22 COM (2012)11 final; voor meer informatie, zie: http://ec.europa.eu/justice/ newsroom/data-protection/news/120125_en.htm.

voegdheid behoort en voor zover daarbij de federale basisnormen en internationaalrechtelijke bepalingen niet worden aangetast.[23] Dit komt erop neer dat de decreetgever strengere voorwaarden dan de federale regelgeving mag voorzien, maar het federale beschermingsniveau niet mag verlagen.

§2. Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (WVP)

A. Toepassingsgebied

1. Persoonsgegevens

'Persoonsgegevens' worden in de wet gedefinieerd als 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit' (art. 1, §1 WVP).
Het gaat om een zeer ruim begrip dat alle mogelijke vormen van informatie kan omvatten. De enige harde beperking in de wet is dat de informatie moet toelaten om een natuurlijke persoon te identificeren. Dit criterium van identificeerbaarheid moet objectief beoordeeld worden.[24] Persoonsgegevens worden als dusdanig aangemerkt zolang *iemand* nog in staat is om, met welk redelijkerwijs inzetbaar middel ook, te achterhalen op welk individu de informatie betrekking heeft. Om een gegeven als persoonsgegeven te bestempelen is het bijgevolg voldoende dat ook enig ander persoon dan de verantwoordelijke voor de verwerking redelijkerwijs een middel kan inzetten om een natuurlijke persoon te identificeren. Om die reden worden identificatienummers, zoals bijvoorbeeld het IP-adres van een met het Internet verbonden computer, in principe als persoonsgegevens aangemerkt.[25]

2. Verwerking

'Verwerking' wordt in de wet gedefinieerd als 'elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, als-

23 Gw Hof 19 januari 2005, nr. 16/2005, www.grondwettelijkhof.be; RvS 28 mei 2004, nr. 37.288/3, http://jsp.vlaamsparlement.be/docs/stukken/2005-2006/ g531-1.pdf.

24 Artikel 29 Werkgroep, opinie 04/2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007.

25 Zie: *Parl.St.* Kamer 1997-98, nr. 1566/1, 12.

mede het afschermen, uitwissen of vernietigen van persoonsgegevens' (art. 1, § 2). Een verwerking omvat dus elke handeling die men op persoonsgegevens kan uitvoeren.
Nochtans vallen niet alle mogelijke verwerkingen onder het toepassingsgebied van de Wet Verwerking Persoonsgegevens. Artikel 3 verduidelijkt dat de wet van toepassing is op elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Het al dan niet geautomatiseerde karakter van de verwerking wordt bepaald door de hulpmiddelen die worden ingezet.[26] De niet-geautomatiseerde verwerking van persoonsgegevens valt enkel onder de bepalingen van de Wet Verwerking Persoonsgegevens wanneer de persoonsgegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen. Zo zal het houden van papieren fiches in een klasseersysteem bijvoorbeeld wel een verwerking zijn die onder de wet valt, ondanks het ontbreken van een elektronische component.
Verder worden de verwerkingen met uitsluitend persoonlijke of huishoudelijke doeleinden uit het toepassingsgebied van de wet uitgesloten (art. 3 §2 WVP). Deze uitzondering moet strikt geïnterpreteerd worden en kan men bijvoorbeeld niet spreken van 'uitsluitend persoonlijke doeleinden' indien persoonsgegevens in de vorm van tekst op een publieke internetpagina worden geplaatst.[27] Daarnaast bevat artikel 3 nog gedeeltelijke uitzonderingen voor verwerkingen 'voor uitsluitend journalistieke, artistieke of literaire doeleinden' en voor verwerkingen door de inlichtingen- en veiligheidsdiensten, de politie en Child Focus.

3. Territoriaal toepassingsgebied

Het criterium waarmee wordt bepaald of de Belgische wet al dan niet van toepassing is, gaat uit van de plaats van de vestiging van de verantwoordelijke van de verwerking (art. 3*bis* WVP).[28] Het is zeer goed mogelijk dat de verwerking in België wordt verricht doch plaatsvindt in het kader van de activiteiten van een vestiging van de verantwoordelijke in een andere lidstaat. In dat geval is de wetgeving van die andere lidstaat van toepassing.
Naast de vraag naar het toepasselijke recht, moet ook nagegaan worden wie de verantwoordelijke voor de verwerking is in deze situatie. Het antwoord op die vraag is onder meer van belang omdat de verantwoordelijke die een vestiging heeft op het grondgebied van verschillende lidstaten, de nodige maatregelen moet treffen om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving.[29] Wanneer een en dezelfde verantwoordelijke op het grondgebied van

26 J. DUMORTIER, 'Bestand of dossier', noot bij het arrest van het Hof van Cassatie, 16 mei 1997, *Computerr.* 4, 1997, p.161-163.
27 HvJ C-101/01, *Lindqvist*, 2003, http://curia.europa.eu, concl. A. TIZZANO; ook in *NJW* 2004, afl. 66, 405, met noot E. BREMS.
28 *Parl. St.* Kamer, 1997-1998, 1566/1, p. 26-28.
29 In overweging 19 van de richtlijn kan men lezen dat vestiging op het grondgebied van een lidstaat het effectief en daadwerkelijk uitoefenen van activiteiten door een vaste vestiging veronderstelt. Verder wordt in dezelfde overweging vermeld dat de rechtsvorm van een dergelijke vestiging, of het nu gaat om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid, hier niet doorslaggevend is.

verschillende lidstaten gevestigd is, moet hij in elk van de vestigingen voldoen aan de verplichtingen van de toepasselijke wetgeving. Om te beletten dat een persoon in de Europese Unie geen bescherming zou genieten bij de verwerking van persoonsgegevens omdat de verantwoordelijke voor de verwerking geen vestiging heeft in een lidstaat van de Europese Unie, wordt voor dit geval een ander criterium gehanteerd voor de aanduiding van het toepasselijke recht. Bepalend in dit laatste geval is in welke lidstaat de middelen zich bevinden waarmee de verwerking van persoonsgegevens wordt uitgevoerd. Indien de verantwoordelijke een vestiging heeft op Belgisch grondgebied en in het kader van de activiteiten van deze vestiging persoonsgegevens verwerkt in een land buiten de Europese Unie, is op die verwerking de Belgische wet van toepassing.

B. Actoren bij de verwerking van persoonsgegevens

De toekenning van rechten en plichten in de Wet Verwerking Persoonsgegevens is gebaseerd op een indeling in specifieke rollen van de personen die betrokken zijn bij de verwerking van persoonsgegevens. In de praktijk is het niet altijd evident om te bepalen welk profiel bij welke persoon past, en welke rechten en plichten men dus draagt.

1. Betrokkene

De 'betrokkene' is de geïdentificeerde of identificeerbare natuurlijke persoon van wie de persoonsgegevens worden verwerkt (art. 1, § 1). Los van het hierboven besproken probleem in verband met de identificeerbaarheid, levert deze definitie weinig problemen op in de praktijk.
De rol van betrokkene is vooral van belang als aanknooppunt voor sommige verplichtingen van de verantwoordelijke voor de verwerking, en omdat de betrokkene bepaalde rechten kan uitoefenen ten aanzien van zijn persoonsgegevens, die hieronder verder zullen worden besproken.

2. Verantwoordelijke voor de verwerking

De rol van 'verantwoordelijke' is complexer omdat er vaak discussies zijn over de vraag wie feitelijke en juridische zeggenschap heeft over een bepaalde verwerking van persoonsgegevens.[30]
De verantwoordelijke voor de verwerking wordt in artikel 1, § 4 WVP gedefinieerd als de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt.
In veel gevallen zal de verantwoordelijke voor de verwerking een rechtspersoon zijn die bepaalde persoonsgegevens moet verwerken om een specifieke

30 Voor de interpretatie van de begrippen 'verantwoordelijke' en 'verwerker' kan o.m. verwezen worden naar het Advies 1/2010 van de Artikel 29 Werkgroep d.d. 16 februari 2010, http://ec.europa.eu/justice.

dienst te kunnen leveren. Een bedrijf dat bijvoorbeeld een klantenbestand bewaart zal daarbij als verantwoordelijke voor de verwerking handelen. Het bedrijf bepaalt immers zowel het doel (klantenadministratie) als de middelen (bijvoorbeeld een bepaalde databank, de inzet van bepaald personeel, bepaalde financiële middelen enzovoort). Voor publieke dienstverlening zal meestal een administratief lichaam verantwoordelijk zijn: de Belgische staat, een Gemeenschap of Gewest, provincie, stad, gemeente, … Ten slotte is het niet uitgesloten dat een natuurlijke persoon als verantwoordelijke optreedt, wat vooral het geval kan zijn bij professionele dienstverleners die als zelfstandige natuurlijke personen actief zijn (bijvoorbeeld tandartsen, loodgieters, winkeliers, …). Belangrijk om voor ogen te houden is dat de hoedanigheid van verantwoordelijke betrekking heeft op een verwerking, en niet noodzakelijk op een relatie. Bovendien is het mogelijk dat één handeling resulteert in een verwerking waarbij meerdere partijen verantwoordelijk zijn voor verschillende aspecten. Ten slotte is het eveneens niet ondenkbaar dat er meerdere entiteiten samen het doel en de middelen van een verwerking bepalen (bijvoorbeeld een gezamenlijke publiciteitscampagne). In dit geval zullen zij gezamenlijk als verantwoordelijken optreden.[31] Het spreekt voor zich dat de toekenning van een bepaalde rol volledig afhangt van de toepasselijkheid van de wettelijk vastgestelde criteria. Het is dus niet mogelijk om contractueel een partij als verantwoordelijke voor de verwerking aan te duiden wanneer dit niet met de realiteit overeenstemt.

Het belang van het onderscheid tussen de verantwoordelijke en een loutere verwerker van persoonsgegevens (zie hierna) ligt in de grotere plichten die de verantwoordelijke draagt. Zo dient hij de toelaatbaarheid van de verwerking te verzekeren, moet hij de betrokkene informeren over alle relevante aspecten van de verwerking, fungeert hij als aanspreekpunt voor de betrokkene die zijn rechten wenst uit te oefenen, en moet hij de nodige afspraken maken met de eventuele verwerker met betrekking tot de veiligheid en vertrouwelijkheid van de persoonsgegevens. Dit impliceert onder meer dat de verantwoordelijke moet waken over de kwaliteit van de verwerkte gegevens; een gepast rechtenbeheer; de betrokkenheid van voldoende gekwalificeerd en geïnformeerd personeel; en de veiligheid van de persoonsgegevens. De wet vereist dat de maatregelen een 'passend' beveiligingsniveau verzekeren, rekening houdend met de stand van de techniek en de kosten voor het toepassen van de maatregelen, en met de aard van de te beveiligen gegevens en de potentiële risico's. De wetgever heeft er dus terdege rekening mee gehouden dat niet elke verwerking even privacygevoelig is, en dat de (kosten van de) maatregelen in redelijke verhouding moeten staan met het reële risico in geval van incidenten.[32]

31 Zie hierover B. VAN ALSENOY, 'Allocating responsibility among controllers, processors, and everything in between: the definition of actors and roles in Directive 95/46/EC', *CLSR* 2012, vol. 28, p. 25-43.

32 Zie Privacycommissie, Aanbeveling nr. 01/2013 van 21 januari 2013, http://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_01_2013.pdf.

3. Verwerker

In tegenstelling tot de verantwoordelijke heeft de 'verwerker' per definitie geen invloed op het doel en de middelen van de verwerking, maar speelt hij een uitvoerende rol. Artikel 1, § 5 WVP omschrijft de verwerker dan ook als de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt, met uitsluiting van de personen die onder rechtstreeks gezag van de verantwoordelijke voor de verwerking gemachtigd zijn om de gegevens te verwerken.
Het inzetten van een verwerker vereist dat er een schriftelijke overeenkomst wordt gesloten tussen de verantwoordelijke en de verwerker waarin onder meer de specifieke doeleinden van de verwerking en de aansprakelijkheid van de verwerker worden vastgelegd, en waarin de nodige technische en organisatorische maatregelen moeten worden opgenomen om de veiligheid en de vertrouwelijkheid van de persoonsgegevens te waarborgen conform de algemene verplichtingen van de verantwoordelijke (art. 16 WVP).

4. Andere actoren

Ten slotte definieert de wet nog de rollen van 'derde' en 'ontvanger' (art. 1 §6 WVP):
- een 'derde' is de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur, anders dan de betrokkene, de verantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verantwoordelijke of de verwerker gemachtigd is om de gegevens te verwerken;
- een 'ontvanger' is de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur, aan wie de gegevens worden meegedeeld, ongeacht of het al dan niet een derde betreft. Administratieve of gerechtelijke instanties aan wie gegevens kunnen worden meegedeeld in het kader van een bijzondere onderzoeksprocedure worden evenwel niet beschouwd als ontvangers.

Het belang van deze rollen ligt vooral in de afbakening van de rechten en plichten van de verantwoordelijke. Zo zal de verantwoordelijke in de aangifte van de verwerking bij de Privacycommissie moeten aangeven welke categorieën van ontvangers in aanraking zullen komen met de persoonsgegevens.

C. Rechtmatigheid en toelaatbaarheid

Eén van de basisbeginselen van de Wet Verwerking Persoonsgegevens is dat persoonsgegevens enkel verwerkt mogen worden op een eerlijke en rechtmatige wijze, en wanneer aan een bepaalde toelaatbaarheidsdrempel is voldaan. De rechtmatigheid van de verwerking is een overkoepelend vereiste, waarmee in algemene zin wordt uitgedrukt dat de verwerking enkel mag geschieden conform de toepasselijke wettelijke bepalingen. De rechtmatigheid vereist dus ook

dat alle bepalingen van de Wet Verwerking Persoonsgegevens werden gerespecteerd, en in die zin is de toelaatbaarheid van de verwerking een klein deelaspect van de rechtmatigheid, die daarnaast ook het respect voor alle andere hieronder besproken criteria impliceert.
Het toelaatbaarheidscriterium impliceert dat er een voldoende grondslag moet zijn voor de verwerking, m.a.w. een omstandigheid die het bestaan van een verwerking legitimeert.[33] De mogelijke voorwaarden voor toelaatbaarheid worden opgesomd in artikel 5, en omvatten verwerkingen:
a) wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend. Deze toestemming moet vrij, specifiek en geïnformeerd zijn. Hoewel stilzwijgende of impliciete toestemming dus tot de mogelijkheden behoort, wordt echter wel vereist dat de betrokkene zijn keuze maakt zonder enige dwang, met betrekking tot een voldoende nauwkeurig afgelijnde verwerking, en op basis van juiste en afdoende informatie over de omvang en doeleinden van de verwerking.
b) wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen. In dit geval is er als het ware sprake van een impliciete toestemming van de betrokkene, die immers zijn instemming met de overeenkomst heeft gegeven of zijn intentie daartoe heeft te kennen gegeven. Er wordt wel vereist dat de maatregelen voorafgaand aan een contract op verzoek van de betrokkene zijn genomen; louter publicitaire verwerkingen met het oog op de creatie van een intentie tot het sluiten van een overeenkomst vallen dus niet onder deze bepaling.[34]
c) wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verantwoordelijke voor de verwerking is onderworpen door of krachtens een wet, een decreet of een ordonnantie. De wetgever kan m.a.w. een expliciete of impliciete toelaatbaarheidsgrond voor de verwerking van persoonsgegevens creëren door het opleggen van verplichtingen (bijvoorbeeld met betrekking tot sociale zekerheid, fiscaliteit, welzijn van de werknemers, …) die de verwerking van persoonsgegevens noodzakelijkerwijs impliceren.
d) wanneer de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene. Dit zal bijvoorbeeld het geval zijn wanneer aan een betrokkene dringend medische hulp moet worden verstrekt, terwijl hij het bewustzijn heeft verloren of om andere redenen niet in staat is om zijn rechtsgeldige toestemming voor de verwerking van zijn persoonsgegevens uit te drukken.
e) wanneer de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang of die deel uitmaakt van de uitoefening van het openbaar gezag, die is opgedragen aan de verantwoordelijke voor de verwerking of aan de derde aan wie de gegevens worden verstrekt. Deze toelaatbaarheidsgrond volstaat m.a.w. voor de meeste taken die werden toevertrouwd aan administratieve organen of uitoefenaars van de openbare macht.

---

33 Luik 19 november 2009, *Computerr*. 2010, afl. 4, 196, met noot G. VANDENDRIESSCHE. Het Hof besliste *in casu* dat het verwerken van persoonsgegevens verworven via 'virale marketing' niet gesteund was op één van de rechtvaardigingsgronden van artikel 5 WVP.

34 Belangrijk in deze context is uiteraard het begrip 'noodzakelijk'. Zie hierover HvJ C-524/06, *Heinz Huber t. Bondsrepubliek Duitsland,* 2008, http://curia.europa.eu.

f) wanneer de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke voor de verwerking of van de derde aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming uit hoofde van deze wet, niet zwaarder doorwegen. Deze laatste toelaatbaarheidsgrond is de meest delicate, omdat zij de verantwoordelijke voor de verwerking toelaat om een eventueel gebrek aan rechtsgeldige toestemming van de betrokkene naast zich neer te leggen, indien zij over een legitiem belang beschikt dat zwaarder zou wegen dan de inbreuk op de persoonlijke levenssfeer van de betrokkene. Het probleem hierbij is vooral dat deze afweging in principe gebeurt door de verantwoordelijke zelf, en dat de betrokkenen veelal pas achteraf het bestaan van zulks zwaarwegend belang van de verantwoordelijke kunnen betwisten, namelijk wanneer de verwerkingen reeds voltrokken zijn.[35]
Zoals hierboven al werd aangehaald gelden verstrengde voorwaarden voor bepaalde categorieën van persoonsgegevens, zoals bijvoorbeeld gezondheidsgegevens. In algemene zin kan men stellen dat voor deze categorieën een explicietere en bij voorkeur schriftelijke toestemming van de betrokkene zal worden geëist, of dat de verantwoordelijke voor de verwerking kan verwijzen naar een bepaalde wettelijke grondslag of naar een bepaalde functie van openbaar nut die een verwerking van deze gegevens zonder toestemming van de betrokkene kan verantwoorden.

D. Doelgebondenheid en proportionaliteit

Naast de noodzaak om zich te vergewissen van de toelaatbaarheid van de verwerking, vereist de rechtmatigheid van de verwerking eveneens dat de verantwoordelijke zich houdt aan de finaliteit van de verwerking. Ruw geschetst houdt dit beginsel in dat de verantwoordelijke voor de verwerking zich dient te beperken tot verwerkingen die overeenstemmen met de doeleinden die werden overeengekomen met de betrokkene of die aan hem werden gecommuniceerd, of waarvoor er op een andere basis een rechtsgrond bestaat. De toelaatbaarheid van de verwerking is dus altijd gebonden aan een bepaalde finaliteit, en de verantwoordelijke mag deze niet negeren of overschrijden.[36]
In de Wet Verwerking Persoonsgegevens werd het finaliteitsbeginsel opgenomen in artikel 4 §1, 2°-5°, waarin telkens een ander aspect van dit beginsel werd toegelicht. Het uitgangspunt daarbij (art. 4 §1, 2°) is de doelgebondenheid van de inzameling en verwerking van persoonsgegevens: de gegevens dienen 'voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en re-

35 Niettemin kan deze toelaatbaarheidsgrond nooit *a priori*, bv. via een wettelijke maatregel, worden uitgesloten en mag de sub (f) voorgestelde afweging niet worden beperkt. Zie HvJ C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito*, 2011, http://curia.europa.eu.

36 Zie o.m. over de installatie van een gps-systeem in het bedrijfsvoertuig van een werknemer Arbh. Gent (8ste kamer) 14 oktober 2011, nr. 2010/AG/291, *J.T.T.* 2012, afl. 1126, 190.

glementaire bepalingen, onverenigbaar is met die doeleinden'. Met andere woorden, bij de verkrijging van de persoonsgegevens dient de verantwoordelijke voor de verwerking reeds een duidelijk afgelijnd en legitiem doel voor ogen te hebben en te communiceren, en hij dient zich bij latere verwerkingen aan dit doel te houden.
Dit impliceert niet dat elke verwerking strikt moet overeenstemmen met dit doel, maar enkel dat de verdere verwerking (m.a.w. volgend op de verkrijging van de persoonsgegevens) niet 'onverenigbaar' mag zijn met dit vastgestelde en bekendgemaakte doel. De precieze interpretatie van deze term is voor discussie vatbaar, maar uit de formulering van artikel 4 kan worden afgeleid dat de verwachtingen van een redelijke betrokkene een centrale rol spelen als maatstaf. M.a.w., met betrekking tot de doelgebondenheid is de redelijke voorzienbaarheid van de verdere verwerking voor de betrokkene een belangrijk criterium: kon de betrokkene die op de hoogte was van het doel redelijkerwijs voorzien dat zijn persoonsgegevens op een bepaalde manier werden verwerkt?
Een logisch corollarium van de doelmatigheidsbeperking is de proportionaliteitsregel (art. 4 §1, 3°): de verwerking van persoonsgegevens dient 'toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt'. Dit proportionaliteitsprincipe speelt een rol in elke verwerking. Bij de inzameling van persoonsgegevens impliceert dit bijvoorbeeld dat men niet meer gegevens opvraagt dan men nodig heeft voor het beoogde doel. Ook de principiële verplichting om persoonsgegevens niet langer bij te houden dan nodig is voor de verwezenlijking van het beoogde doel (art. 4 §1, 5°) is een toepassing hiervan. Ten slotte impliceert de finaliteitsregel ook een bepaalde verplichting om te waken over de kwaliteit van de betrokken persoonsgegevens (art. 4 §1, 4°). Ook op dit vlak rust aldus een plicht op de verantwoordelijke om een werkwijze vast te leggen waarmee eventuele onjuiste, onvolledige of gedateerde informatie kan worden gecontroleerd en gecorrigeerd of verwijderd.

E. De rechten van de betrokkene

1. Overzicht

Eén van de grote verdiensten van de Wet Verwerking Persoonsgegevens – en van de Europese bescherming van de persoonlijke levenssfeer in het algemeen – is dat een centrale rol aan de rechten van de betrokkene wordt toegekend. Elke betrokkene waarvan de persoonsgegevens worden verwerkt kan immers aanspraak maken op de eerbiediging van een aantal basisrechten, die hij kan uitoefenen ten aanzien van de verantwoordelijke, of die de verantwoordelijke voor de verwerking spontaan in acht moet nemen.

2. Recht op informatie

Een eerste recht van de betrokkene wordt in artikel 9 van de Wet Verwerking Persoonsgegevens geformuleerd als een verplichting van de verantwoordelijke om de betrokkene bepaalde informatie te verstrekken over de geplande ver-

werking. Het artikel maakt een onderscheid tussen twee hypotheses, naar gelang de bron van de persoonsgegevens.
Wanneer de gegevens rechtstreeks bij de betrokkene worden verkregen, bijvoorbeeld via een inschrijvingsformulier, een enquête of een interview, dan is artikel 9 §1 van toepassing. In dit geval moet de verantwoordelijke ten laatste op het moment van de verkrijging zelf de nodige informatie aan de betrokkene verstrekken, tenzij de betrokkene op dat moment al over deze informatie beschikt. Op die manier zal hij een geïnformeerde beslissing kunnen nemen. Uit een recent arrest van het Hof van Justitie volgt dat deze bepaling onverkort van toepassing is op Belgische privédetectives daar zij niet uitdrukkelijk bij wet van deze informatieverplichting werden ontslagen.[37]
Vanzelfsprekend kan een verantwoordelijke voor de verwerking ook op andere manieren in het bezit komen van de persoonsgegevens van de betrokkene, bijvoorbeeld omdat hij een databank met gegevens ontvangt van een klant waarvoor hij een dienst moet leveren, of omdat de betrokkene een derde heeft geïnstrueerd om zijn persoonsgegevens door te geven. In dit geval zal de verantwoordelijke vaak in de onmogelijkheid verkeren om de betrokkene bepaalde informatie te bezorgen, bijvoorbeeld omdat hij niet beschikt over de nodige contactgegevens (een absolute onmogelijkheid) of omdat het contacteren van de betrokkenen disproportionele investeringen zou kosten (een relatieve onmogelijkheid, bijvoorbeeld bij de aankoop van een databank met contactgegevens van honderdduizenden personen).
Bij verkrijging van persoonsgegevens van derden is artikel 9 §2 van de wet van toepassing, en schrijft de wet voor dat de nodige gegevens aan de betrokkene moeten worden bezorgd op het moment van de registratie van de gegevens of wanneer mededeling van de gegevens aan een derde wordt overwogen, uiterlijk op het moment van de eerste mededeling van de gegevens. De lijst van te bezorgen informatie loopt grotendeels gelijk met de opsomming in §1.

3. Recht op inzicht en inzage, verbetering en verhaal

Naast het recht op informatie op het moment van de verkrijging van de persoonsgegevens, beschikt de betrokkene ook over een reeks andere rechten die hij op elk moment kan uitoefenen ten aanzien van de verantwoordelijke, en die worden vastgelegd in de artikelen 10 en 12 van de Wet Verwerking Persoonsgegevens.
Een eerste recht dat de wet waarborgt is het zogenaamde mededelingsrecht (art. 10 WVP). Dit recht impliceert dat een betrokkene die zijn identiteit bewijst mag verzoeken om mededeling van de persoonsgegevens die op hem betrekking hebben waarover een verantwoordelijke beschikt, evenals de bron van deze gegevens, de doeleinden waarvoor de persoonsgegevens worden verwerkt, en de logica die aan een geautomatiseerde verwerking ten grondslag ligt wanneer dit resulteert in een automatisch besluit waaraan voor een persoon rechtsgevolgen verbonden zijn of dat hem in aanmerkelijke mate treft. In algemene zin komt dit recht erop neer dat de betrokkene mag vragen om inzage te krijgen in de gegevens die een verantwoordelijke verwerkt (zowel de abstracte gegevenscategorieën als de concrete gegevens zelf voor zover die op

37 HvJ C-473/12, *Englebert*, 2013, http://curia.europa.eu.

hem betrekking hebben), en om inzicht te verschaffen in de motivatie achter de verwerking (inclusief de bronnen van de gegevens en de doeleinden van de verwerking). De verantwoordelijke voor de verwerking moet het nodige doen om aan die vraag te beantwoorden, wat o.m. inhoudt dat hij met het oog daarop de te verstrekken gegevens zal moeten bewaren.[38]
Naast het mededelingsrecht heeft de betrokkene eveneens het recht om alle onjuiste persoonsgegevens die op hem betrekking hebben kosteloos te doen verbeteren (art. 12, eerste lid WVP). Het spreekt voor zich dat dit recht enkel mag worden gebruikt om objectieve onjuistheden te corrigeren. Het betreft geen censuurrecht dat de betrokkene kan misbruiken om ongewenste informatie aan te passen.
Ten slotte beschikt de betrokkene onder bepaalde omstandigheden ook over een principieel verzetsrecht (art. 12, tweede lid e.v. WVP). Wanneer de persoonsgegevens worden verkregen met het oog op *direct marketing* mag de betrokkene zich kosteloos en zonder enige motivering tegen de voorgenomen verwerking van zijn persoonsgegevens verzetten.[39] In andere gevallen kan de betrokkene zich enkel verzetten wanneer hij over zwaarwegende en gerechtvaardigde redenen beschikt, en op voorwaarde dat de rechtmatigheid van de verwerking niet gesteund is op een contractuele verplichting van de betrokkene of op de wet. De betrokkene kan zijn verzetsrecht ook op een meer gerichte manier uitoefenen. De wet laat namelijk toe dat hij om de verwijdering van zijn persoonsgegevens vraagt of dat hij eist dat deze niet meer zullen worden verwerkt, wanneer ze gelet op het doel van de verwerking onvolledig of irrelevant zijn, of wanneer de registratie, de mededeling of de bewaring ervan verboden zijn, of wanneer ze na verloop van de toegestane duur zijn bewaard. De betrokkene kan met andere woorden de naleving van het hierboven besproken proportionaliteitsbeginsel afdwingen.

4. Bescherming tegen geautomatiseerde beslissingsvorming

Artikel 12*bis* WVP beschermt personen tegen geautomatiseerde beslissingen. Het stipuleert dat een besluit waaraan voor een persoon rechtsgevolgen verbonden zijn of dat hem in aanmerkelijke mate treft niet louter mag worden genomen op grond van een geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren.
Vanzelfsprekend mag aan deze regel geen absolute interpretatie worden gegeven die de rol van informatiesystemen volledig zou uitsluiten. In de praktijk is het gebruik van deze systemen immers onmisbaar voor complexe beslissingen, zoals bijvoorbeeld de berekening van belastingen, waarbij met vele honderden factoren rekening moet worden gehouden voor elk van de miljoenen belastingplichtige natuurlijke en rechtspersonen. Er wordt enkel vereist dat dergelijke beslissingen niet louter het gevolg zijn van een geautomatiseerde verwerking, waarbij zelfs een beperkte menselijke tussenkomst (zoals bijvoorbeeld een

38 HvJ C-553/07, *College van burgemeesters en wethouders van Rotterdam t. M. Rijkeboer*, 2009, http://curia.europa.eu.
39 Zie hierover: Aanbeveling nr. 02/2013 van 30 januari 2013, www.privacycommission.be.

prima facie menselijke controle van de juistheid van de uitkomst) dus volstaat om aan de regel te voldoen.
Bovendien matigt artikel 12*bis*, tweede lid dit principe, door het verbod te herroepen wanneer het besluit wordt genomen in het kader van een overeenkomst of wanneer het zijn grondslag vindt in een bepaling voorgeschreven door of krachtens een wet, decreet of ordonnantie. De overeenkomst of de bepaling moet dan wel voorzien in passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene, wat minstens inhoudt dat hij de mogelijkheid krijgt om op nuttige wijze zijn standpunt naar voor te brengen. Het artikel viseert aldus niet zozeer de eliminatie van geautomatiseerde besluitvorming, doch eerder de eliminatie van elke menselijke betrokkenheid in dit proces.

F. Doorgifte van persoonsgegevens naar het buitenland

1. Principe

Binnen het Europese Economische Gebied gelden er geen bijzondere beperkingen voor de grensoverschrijdende overdracht van persoonsgegevens.[40] Echter, de Wet Verwerking Persoonsgegevens voorziet in een bijzondere regel voor de overdracht naar landen buiten deze zone.
Artikel 21 WVP stelt als principe voorop dat in dit geval de persoonsgegevens slechts mogen worden doorgegeven naar een dergelijk land 'indien dat land een passend beschermingsniveau waarborgt en de andere bepalingen van deze wet en de uitvoeringsbesluiten ervan worden nageleefd'. In principe is de overdracht dus verboden, tenzij in het land van bestemming een regelgevend kader werd ingericht dat een passend beschermingsniveau biedt. De beslissingen over een al dan niet passend beschermingsniveau worden in de praktijk genomen door de Europese Commissie, die de toepasselijke regelgeving in specifieke landen onderzoekt en nagaat of ze voldoet aan de Europese normen.[41]

2. Verenigde Staten: Safe Harbor

De Verenigde Staten nemen daarbij een bijzondere positie in. Voor dit land werd gekozen voor een tussenweg, onderhandeld tussen de Europese Commis-

40 De Wet Verwerking Persoonsgegevens is de omzetting is van de Europese richtlijn die, zoals hierboven al aangehaald, van toepassing is in het Europese Economische Gebied (m.a.w. de 28 lidstaten van de Europese Unie, samen met IJsland, Liechtenstein en Noorwegen). Deze landen beschikken dus over een regelgeving die min of meer gelijkloopt met de Belgische Wet Verwerking Persoonsgegevens, en die vergelijkbare garanties biedt bij de verwerking van persoonsgegevens.

41 Tot op heden heeft de Europese Commissie echter nog maar voor een tiental landen een positieve beslissing in dit verband gepubliceerd, waaronder Zwitserland, Argentinië, Canada, Israël en Australië. Verder prijken op de lijst ook een aantal kleinere staten zoals Andorra, de Farao Eilanden, het Eiland Man, Guernsey en Jersey. Zie http://ec.europa.eu/justice, onder 'gegevensbescherming'.

sie en het *U.S. Department of Commerce*, over de zogenaamde *Safe Harbor Principles*.[42] De *Safe Harbor Principles* zijn een korte lijst met beginselen die het *Department of Commerce* op 21 juli 2000 heeft uitgevaardigd, en waarin aan Amerikaanse ondernemingen wordt uiteengezet aan welke verplichtingen zij zouden moeten voldoen om Europese persoonsgegevens te mogen verwerken. de lijst heeft geen bindend karakter en het staat Amerikaanse ondernemingen vrij om te beslissen al dan niet tot de *Safe Harbor* toe te treden door de nodige procedures te implementeren in hun organisatie en door hun naleving van de *Principles* te registreren bij het *Department of Commerce*.[43] Het gevolg van toetreding tot de *Safe Harbor* is echter dat de betrokken onderneming beschouwd wordt als een organisatie die beschikt over een passend beschermingsniveau. Met andere woorden, ondernemingen die een deel uitmaken van de *Safe Harbor* mogen Europese persoonsgegevens ontvangen en verder verwerken. De namen van deze ondernemingen worden online gepubliceerd.[44]

3. Uitzonderingen

Bovendien voorziet artikel 22 WVP in een aantal uitzonderingen. Zo is een overdracht van persoonsgegevens onder meer toegelaten wanneer de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft, ongeacht het al dan niet passende beschermingsniveau van het land van bestemming. De doorgifte kan ook worden verantwoord op basis van noodzaak, bijvoorbeeld voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke of ter vrijwaring van het vitaal belang van de betrokkene.

4. Modelovereenkomsten en bindende ondernemingsregels

Artikel 22 *in fine* laat toe om overeenkomsten op te stellen waarbij de verantwoordelijke voor de verwerking en de ontvanger van de gegevens voldoende waarborgen bieden ten aanzien van de bescherming van de persoonlijke levenssfeer, de fundamentele rechten en vrijheden van personen, en de uitoefening van de daaraan verbonden rechten. Deze overeenkomsten moeten in principe voor advies worden voorgelegd aan de Privacycommissie. De standaardovereenkomsten werden opgesteld, goedgekeurd en gepubliceerd door de Europese Commissie[45], en beschikken op basis daarvan over een zekere legitimiteit. Hoewel het voorleggen van het gebruik van deze modellen aan de Privacycommissie in België verplicht is, wordt de goedkeuring ervan bij koninklijk besluit in de praktijk niet vereist[46], tenminste wanneer zij integraal worden

42 Zie http://www.export.gov/safeharbor.

43 Voor een beschrijving van de procedure, zie http://ita-web.ita.doc.gov /SafeHarbor /shreg.nsf/login?openform; laatst bezocht op1 april 2013.

44 Zie de *Safe Harbor List*: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages /safe+harbor+list; laatst bezocht op 17 januari 2013.

45 Zie http://ec.europa.eu/justice.

46 Bron: http://www.privacycommission.be.

overgenomen. Hun legitimiteit wordt in dit geval immers reeds afdoende gedekt door de beschikkingen van de Europese Commissie.[47]
Naast deze standaardovereenkomsten is er nog een tweede alternatief dat in de praktijk wordt gebruikt door internationaal vertakte ondernemingen die persoonsgegevens tussen hun verschillende vestigingen moeten kunnen uitwisselen, waarbij sommige van die branches gevestigd zijn in landen zonder een gepast beschermingsniveau. Zij kunnen daarbij gebruik maken van een soort gebundelde exportlicentie, in de vorm van zogenaamde bindende ondernemingsregels (*Binding Corporate Rules*). De bindende ondernemingsregels zijn niet geharmoniseerd door de Europese Commissie. Hierdoor beschikken ondernemingen over meer vrijheid om de inhoud van deze overeenkomsten in te vullen.[48] De keerzijde van de medaille is dat deze overeenkomsten niet enkel moeten worden voorgelegd voor advies aan de Privacycommissie,[49] maar in principe door een koninklijk besluit moeten worden bekrachtigd.[50] De Privacycommissie zal voor de goedkeuring van het ontwerp van gedragscode bovendien contact opnemen met de andere nationale privacycommissies om de goedkeuring van de *Binding Corporate Rules* in alle betrokken Europese landen te kunnen bekomen.[51] Op die manier poogt men om een schaalbaar alternatief aan te bieden aan verantwoordelijken voor de verwerking die op internationaal vlak persoonsgegevens moeten kunnen uitwisselen, ook buiten het Europees grondgebied.

G. Aangifteverplichting

Artikel 17 verplicht de verantwoordelijke voor de verwerking om zijn geplande verwerkingen vooraf aan te geven bij de Privacycommissie. De informatie

47 Beschikking 2001/497/EG van de Commissie van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG, *Publ. L.* 181 van 4 juli 2001; zoals aangevuld door Beschikking 2004/5271/EG van de Commissie van 27 december 2004 tot wijziging van Beschikking 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen, *Publ. L.* 385/74 van 29 december 2004; http://ec.europa.eu/justice.

48 Niettemin zijn er door de Artikel 29 Werkgroep een ganse reeks hulpmiddelen ontwikkeld, in de vorm van templates en '*Frequently Asked Questions*'. Zie http://ec.europa.eu/justice.

49 Zie bij wijze van voorbeeld het Advies 19/2012 van 4 juli 2012 van de Privacycommissie met betrekking tot *Binding Corporate Rules* voor de internationale overdracht van persoonsgegevens door de onderneming Hewlett Packard Company, en Advies nr. 39/2013 van 17 juli 2013 met betrekking tot de onderneming Intel, http://www.privacycommission.be.

50 Zie bij wijze van voorbeeld het Advies 13/2007 van 21 maart 2007 van de Privacycommissie met betrekking tot een ontwerp van KB voor de machtiging van bepaalde *Binding Corporate Rules* voor de internationale overdracht van persoonsgegevens door General Electric; zie Advies 13/2007, http://www.privacycommission.be. Inmiddels is echter tussen de FOD Justitie en de Privacycommissie in een protocol een verkorte procedure afgesproken voor de uitvaardiging van deze Koninklijke besluiten.

51 De procedure hiervoor werd aanzienlijk vereenvoudigd. Zie voor de laatste stand van zaken http://ec.europa.eu/justice.

in deze aangifte wordt opgenomen in het openbaar register, dat via het Internet kan worden geraadpleegd. De bedoeling van dit register is om het publiek toe te laten na te gaan wie hun gegevens verwerkt, en voor welk doeleinde. De aangifte (en de informatie in het register) bevat vanzelfsprekend alleen informatie over de verwerking als dusdanig, en niet de te verwerken persoonsgegevens zelf.[52]
Niet alle verwerkingen moeten worden aangegeven. Louter manuele verwerkingen worden volledig vrijgesteld van aangifte (m.a.w. alleen volledig of gedeeltelijk geautomatiseerde verwerkingen moeten worden aangegeven), evenals verwerkingen die alleen tot doel hebben een register bij te houden dat door of krachtens een wet, een decreet of een ordonnantie bedoeld is om het publiek voor te lichten en dat door iedere belanghebbende kan worden geraadpleegd. In dit laatste geval is de transparantie immers reeds voldoende gewaarborgd. Daarnaast voorziet ook het Koninklijk besluit tot uitvoering van de wet in de artikelen 51 tot 62 in een aantal vrijstellingen van de aangifteplicht. Het gaat voornamelijk over een aantal courante en evidente verwerkingen die doorgaans weinig risico voor de persoonlijke levenssfeer impliceren, waaronder personeelsbeheer, loonbeheer, boekhouding, klanten- en leveranciersbeheer.

§3. Europese ontwikkelingen – voorstel nieuw Europees kader

Op 25 januari 2012 publiceerde de Europese Commissie een voorstel voor een vernieuwd juridisch kader voor gegevensbescherming in de Europese Unie. De geplande beschermingsregeling bestaat uit twee teksten:
- een voorstel van Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens (hierna 'het ontwerp van Verordening') en,
- een voorstel van Richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens door de bevoegde overheden met het oog op preventie en opsporing, onderzoek en vervolging van strafrechtelijke inbreuken, of uitvoering van strafbepalingen en het vrije verkeer van deze gegevens ('het voorstel van Richtlijn').

Een eerste belangrijke wijziging, naast het feit dat het om een Verordening en dus om eengemaakte regels gaat voor het ganse grondgebied van de Unie, is de uitbreiding van het territoriale toepassingsgebied. In de toekomst zouden de Europese regels ook van toepassing zijn wanneer de verantwoordelijke van de verwerking geen zetel heeft in de EU, maar toch persoonsgegevens verwerkt van EU-onderdanen, tenminste wanneer de verwerking verbonden is aan het aanbieden van goederen of diensten aan deze personen of wordt gedaan met het doel om hun gedrag te monitoren. Met de invoering van een eengemaakt, uniform Europees regelgevend kader, zou het voor internationale ondernemingen een stuk eenvoudiger worden om te voldoen aan de regels. Deze admini-

52 Voor meer informatie over de procedure van aangifte, zie http://www.privacycommission.be/nl/de-aangifteprocedure.

stratieve vereenvoudiging wordt versterkt door het schrappen van de verplichting tot aangifte van de verwerking van persoonsgegevens. Er zullen daarentegen specifieke regels voorzien worden voor het monitoren van verwerkingen van persoonsgegevens die een hoog risico inhouden voor de betrokkenen omwille van hun aard, omvang of doel (bijvoorbeeld in geval van het verzamelen van heel gevoelige gegevens). Of dit risico aanwezig is, zal bepaald worden aan de hand van een evaluatie die de verantwoordelijke van de verwerking en de verwerker van de persoonsgegevens zal moeten uitvoeren m.b.t. de maatregelen en veiligheidsmechanismen die voorzien zijn voor de bescherming van de gegevens. Voortaan zullen ondernemingen ook slechts onderworpen zijn aan één enkele privacy autoriteit, namelijk diegene van het land waar hun zetel gevestigd is. De keerzijde van de medaille is dat de aansprakelijkheid van de ondernemingen wordt verhoogd. Zij moeten een hoog beschermingsniveau van de verzamelde gegevens kunnen garanderen en bij incidenten (bv. datalekken) zijn zij verplicht om de autoriteiten binnen de 24 uur te verwittigen. Er wordt ook een effectiever sanctiemechanisme ingevoerd met boetes die, naar het voorbeeld van de boetes bij inbreuken tegen het mededingingsrecht, zeer hoog kunnen oplopen. Ten slotte zullen ondernemingen met meer dan 250 werknemers, verplicht worden om een gegevensverantwoordelijke aan te stellen, die erop zal moeten toezien dat de verwerking van persoonsgegevens volgens de regels gebeurt.

Voor de individuen van wie persoonsgegevens worden onderworpen aan verwerking, zijn er een aantal nieuwe, bijkomende garanties ingevoerd die de bescherming van deze persoonsgegevens zouden moeten verhogen. De belangrijkste is de verscherpte definitie van het begrip 'toestemming'. Zo moet de toestemming die de betrokkene dient te geven voor de verwerking van zijn persoonsgegevens voortaan expliciet zijn en niet langer gewoon 'ondubbelzinnig'. De betrokkene zou verder, naast de klassieke rechten op toegang tot de gegevens, kopie, verbetering en het recht om zich te verzette, ook het recht krijgen om zijn gegevens over te dragen van de ene naar een andere dienstverlener (bijvoorbeeld van het ene sociale netwerk naar het andere). Ook wordt in een 'recht om vergeten te worden' voorzien. Dit houdt in dat een individu op elk ogenblik kan beslissen om zijn toestemming te herroepen in bepaalde gevallen en zijn gegevens dus te laten doorhalen. Wanneer een individu dit recht uitoefent, moet de verantwoordelijke van de verwerking van de persoonsgegevens onmiddellijk alle nodige (technische) stappen ondernemen om de gegevens te verwijderen. Indien hij deze zelf heeft doorgegeven aan derden, is hij er bovendien ook verantwoordelijk voor om deze derden in te lichten van het verzoek tot doorhaling van elke link naar of kopie van deze gegevens. Dit recht weegt echter niet op tegen het recht op vrije meningsuiting en de persvrijheid. Het wissen van gegevens is evenmin gerechtvaardigd wanneer zij noodzakelijk zijn voor historische, statistische en wetenschappelijke onderzoeksdoeleinden. Ten slotte zouden bedrijven voortaan rekening moeten houden met het principe '*privacy by default*', dat betekent dat de standaard instel-

lingen die zij moeten hanteren, diegene zijn die de betrokkene het meeste bescherming geven.[53]

IV. Bescherming van private communicatie

§1. Inleiding

Een belangrijk aspect van de privacy is het vertrouwelijke karakter van privécommunicatie. Zo wordt het briefgeheim sinds lang beschermd door artikel 29 van de Grondwet[54] en door artikel 8.1 van het EVRM.[55] Daarnaast is het in België strafrechtelijk verboden een aan de post toevertrouwde brief weg te maken, te openen, en het bestaan en de inhoud ervan bekend te maken.[56]
Op dit moment wordt de vertrouwelijkheid van elektronische communicatie in België echter vooral beschermd in het Strafwetboek en in de wet van 13 juni 2005 betreffende de elektronische communicatie (hierna: Wet Elektronische Communicatie of WEC).[57] Artikelen 259*bis* en 314*bis* van het Strafwetboek beschermen de inhoud van elektronische communicatie, en bestraffen bijvoorbeeld het afluisteren van een gesprek over de telefoon. Artikel 124 van de Wet Elektronische Communicatie heeft een veel breder toepassingsgebied en bestraft ook het kennis nemen van het bestaan van met elektronische communicatie overgebrachte gegevens, bv. de naam van correspondenten, het tijdstip of de duur van een gesprek.

---

53 Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 35/2012 van 21 november 2012 uit eigen beweging over het ontwerp van Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen ten opzichte van de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens, http://www.privacycommission.be/sites /privacy commission/files/documents /advies_35_2012_0.pdf.

54 'Het briefgeheim is onschendbaar. De wet bepaalt welke agenten verantwoordelijk zijn voor de schending van het geheim der aan de post toevertrouwde brieven.'

55 'Eenieder heeft recht op eerbiediging van zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling.'

56 Art. 151, 460 en 460*bis* Sw. en art. 2, 28 en 29 van de Wet van 26 december 1956 op de postdienst, *BS* 30 december 1956. Zie verder J. LEBOUTTE, 'De wettelijke bescherming van het briefgeheim', *De Gem*. 1988, p. 369-371; verder ook Corr. Brussel, 18 april 1986, *R.W.* 1987-88, 60, noot L. HUYBRECHTS (m.b.t. de vraag of een onrechtmatig geopende brief als bewijs kan aanvaard worden). Het briefgeheim is echter niet absoluut. Zie o.m. Cass. 18 juni 1962, *R.W.* 1962-63, 957. Het Hof besliste dat, wanneer de beambte van de posterijen een onbestelbare brief openmaakt en aldus incidenteel kennis krijgt van een wanbedrijf, het bestuur der posterijen hiervan dadelijk bericht moet geven aan het O.M. Dit bekend maken van de inhoud van de brief is niet strafbaar.

57 Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005, 28070.

§2. Elektronische communicatiewet

A. Uitzonderingen op het communicatiegeheim

Artikel 125, § 1 van de Wet Elektroniche Communicatie bevat zes uitzonderingen op het communicatiegeheim. De bepalingen van artikel 124 van de wet en van de artikelen 259*bis* en 314*bis* van het Strafwetboek zijn, volgens dit artikel, niet van toepassing:

- wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt;
- wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische-communicatiedienst te garanderen;[58]
- wanneer de handelingen worden gesteld om de interventie van hulp- en nooddiensten mogelijk te maken die antwoorden op aan hen gerichte verzoeken om hulp;
- wanneer de handelingen door het BIPT (Belgisch Instituut voor Post en Telecommunicatie) worden gesteld in het kader van zijn algemene opdracht inzake toezicht en controle;
- wanneer de handelingen door de ombudsdienst voor telecommunicatie, door de ambtenaren die zijn gemachtigd door de minister die de economie (economische inspectie) of door de Ethische Commissie voor de telecommunicatie of zijn secretariaat, of op verzoek van deze instellingen, worden gesteld in het kader van hun wettelijke onderzoeksopdrachten en niet het afluisteren van communicaties betreffen;
- wanneer de handelingen worden gesteld met als enig doel de eindgebruiker diensten aan te bieden die erin bestaan het ontvangen van ongewenste elektronische communicatie te verhinderen, mits hiertoe de nodige toestemming werd verkregen van de eindgebruiker.

Bij de eerste uitzondering wordt in de eerste plaats aan de wettelijke regelingen gedacht die aan het parket of de onderzoeksrechter toelaten om het telecommunicatiegeheim te doorbreken in het kader van een gerechtelijk onderzoek of vooronderzoek. De laatste uitzondering moet netwerkbeheerders de mogelijkheid geven om o.m. '*spam*' weg te filteren uit het e-mailverkeer.

B. Verkeersgegevens

Artikel 128 van de Wet Elektronische Communicatie bepaalt dat de registratie van elektronische communicatie en de daarmee verband houdende verkeersgegevens 'uitgevoerd in het legale zakelijke verkeer ten bewijze van een com-

58 Daarbij wordt gedacht aan personeel van operatoren en internet service providers maar ook aan netwerkbeheerders in bedrijven of administraties. Om de continuïteit van de telecommunicatiedienst te verzorgen, mogen zij dus het principe van het telecommunicatiegeheim overtreden met inachtneming van het proportionaliteitsprincipe. Slechts wanneer en in zoverre het nodig is om de dienst te verzorgen, mag bijvoorbeeld de netwerkbeheerder kennis nemen van het bestaan of de inhoud van telecommunicatieberichten. Tot de verzorging van de dienst behoren ook preventieve maatregelen (bv. back-up).

merciële transactie of van een andere zakelijke communicatie' is toegestaan. Voorwaarde is echter dat alle bij de communicatie betrokken partijen vóór de registratie op de hoogte gebracht worden van de registratie, de precieze doeleinden ervan en de duur van de opslag van de registratie. De bedoelde gegevens moeten worden gewist uiterlijk op het einde van de periode waarbinnen de transactie in rechte kan worden aangevochten.
Met betrekking tot verkeersgegevens oordeelde het Europees Hof van Justitie recentelijk dat aanbieders van openbare communicatienetwerken en openbaar beschikbare elektronische communicatiediensten verkeersgegevens mogen doorzenden aan de cessionaris van hun vorderingen betreffende verstrekking van telecommunicatiediensten met het oog op de inning daarvan. Bovendien is het de cessionaris toegelaten deze gegevens op zijn beurt te verwerken op voorwaarde dat hij handelt onder het gezag van de dienstenaanbieder voor de verwerking van die gegevens, en enkel de verkeersgegevens verwerkt die noodzakelijk zijn voor de inning van de gecedeerde vorderingen.[59]

C. 'Cookies'

Het gebruik van '*cookies*' en andere technieken waarbij, vooral via het internet, van op afstand wordt ingegrepen in de eindapparatuur van de gebruiker en meestal ook informatie wordt geplaatst op die apparatuur, slechts toegestaan op voorwaarde dat de abonnee of eindgebruiker hiervoor zijn geïnformeerde en expliciete toestemming heeft gegeven (art. 129 WEC).
Over de toepassing van deze bepaling wordt intensief gedebatteerd. In elk geval gaat het om de omzetting van een Europeesrechtelijke regel die dan ook op Europees niveau, op dezelfde manier in alle lidstaten, uitgelegd moet worden. Het uitgangspunt is dat voor *cookies* de expliciete toepassing van de abonnee of de eindgebruiker nodig is. Deze toestemming is evenwel niet altijd vereist voor alle informatie die wordt opgeslagen of geconsulteerd op de eindapparatuur van de gebruiker (of abonnee). Artikel 5.3. van de Richtlijn 2002/58/EG laat een uitzondering toe indien het gaat om een van de volgende criteria: (1) indien er sprake is van 'enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk' of (2) 'indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.'
Volgens de Privacycommissie zijn de *cookies* die zijn vrijgesteld van de toestemmingsplicht vooral bepaalde '*first party cookies*' en dan nog voornamelijk van het type '*user input session cookies*', dus *cookies* die door de gebruiker zelf geplaatst zijn en die taalinstellingen en persoonlijke voorkeuren onthouden bij een webwinkel (zoals klantidentificatie en virtueel winkelwagentje).[60] Anderzijds vallen bepaalde *cookies* duidelijk niet onder de vrijstelling op de informatieplicht. In de literatuur verwijst men naar de meest intrusieve en nieuwste cookievormen via diverse benamingen die soms door elkaar worden gebruikt zoals '*persistent cookies*', '*flash cookies*', '*super cookies*' en '*ever*

59 HvJ C-119/12, *Probst*, 2012, http://curia.europa.eu.
60 Zie Advies 10/2012 van 21 maart 2012, http://www.privacycommission.be.

cookies'.[61] Deze *cookies*, die worden gebruikt voor diverse of onbepaalde doeleinden, zijn niet duidelijk op expliciet verzoek van de eindgebruiker gevraagd, en blijven soms zelfs na een wis-actie op het eindapparaat van de gebruiker actief. Vaak gaat het hierbij om '*third party cookies*' waarover zeer weinig of niet door de diverse verantwoordelijken wordt geïnformeerd, en waarvoor bijzondere expertise en software vereist is om ze te verwijderen.

D. Het gebruik van cryptografie

Zowel voor spraaktelefonie als voor communicatie via het Internet worden meer en meer middelen aangeboden die de gebruikers toelaten om hun boodschappen te versleutelen en zodoende onleesbaar te maken voor derden. Overeenkomstig artikel 48 van de Wet Elektronische Communicatie is het gebruik van versleuteling in België vrij. De wet waarborgt de vrijheid van versleuteling zonder enige beperking op de complexiteit van encryptie en zonder enig systeem van neerleggen van sleutels. Bij koninklijk besluit kunnen sommige diensten met betrekking tot encryptie worden onderworpen aan een notificatieplicht bij het BIPT.[62] Op dit ogenblik is er nog geen koninklijk besluit in die zin uitgevaardigd.
Artikel 127, § 2, van de Wet Elektronische Communicatie verbiedt 'de levering of het gebruik van een dienst of van apparatuur die de toepassing van de regels over het opvragen van verkeers- of identificatiegegevens van eindgebruikers of het registreren van de inhoud van elektronische communicatie door de gerechtelijke autoriteiten bemoeilijkt of verhindert'.[63] Een uitzondering wordt echter gemaakt voor 'encryptiesystemen die kunnen worden gebruikt om de vertrouwelijkheid van de communicatie en de veiligheid van betalingen te garanderen'. Al bij al is deze regeling uiterst dubbelzinnig. In de praktijk wordt in België onbeperkt van encryptie gebruik gemaakt en wordt er voorlopig nog niet aan gedacht om daartegen op te treden met het oog op het vergemakkelijken van de activiteiten van gerechtelijke autoriteiten of inlichtingen- en veiligheidsdiensten.[64]

---

61 De Privacycommissie verwijst hier naar de studie van ENISA, van 2 februari 2011, *Bittersweet cookies. Some security and privacy considerations*, gepubliceerd op http://www.enisa.europa.eu.

62 'Het gebruik van versleuteling is vrij. De terbeschikkingstelling aan het publiek van versleutelingsdiensten aangewezen door de Koning, na advies van het Instituut, is onderworpen aan een voorafgaande kennisgeving aan het Instituut. De Koning legt na advies van het Instituut de inhoud en de vorm van die kennisgeving vast.'

63 Eigenaardig genoeg vermeldt artikel 127, § 2 geen encryptiesoftware (enkel 'diensten' en 'apparatuur'). Initiatieven zoals TOR (www.torproject.org) zouden evenwel bij KB in België verboden kunnen worden omdat ze als 'dienst' aangemerkt kunnen worden.

64 Voor bepaalde encryptieproducten (hardware of software) gelden weliswaar exportbeperkingen of is voor export een licentie nodig in het kader van de internationale en Europese reglementering inzake goederen voor dubbel gebruik (zogenaamde '*dual use*' goederen). Alle informatie hieromtrent kan men vinden op de

E. Andere telefoondiensten

De Wet Elektronische Communicatie regelt ook enkele privacyaspecten van klassieke telefoniediensten. Voor de weergave van de identificatie van het oproepende nummer (*call-ID*) bepaalt artikel 130 dat zowel de oproepende eindgebruiker als de abonnee zich kosteloos en op eenvoudige aanvraag moeten kunnen verzetten tegen het gebruik van deze dienst.
Voor wat betreft de automatische doorschakeling van oproepen door een derde naar het eindtoestel van de abonnee (*call forwarding*), bepaalt artikel 131 dat de abonnee deze functie moet kunnen stopzetten voor zover dit technisch en operationeel mogelijk is voor de operator.
De opname in de telefoongids of in de telefooninlichtingendienst mag enkel nadat de abonnee hiervoor zijn geïnformeerde toestemming heeft gegeven en voor zover dat zijn rechten zoals voorzien door de Wet Verwerking Persoonsgegevens (inzonderheid inzage-, correctie- en verzetsrecht) worden gewaarborgd.

F. Controle van communicatie in de onderneming

In de Belgische wetgeving is voor de werkgever, behalve de wettelijke uitzondering voor de registratie van 'zakelijke communicatie' (art. 128 WEC) nergens expliciet in een uitzondering op het principe van het telecommunicatiegeheim voorzien. Omdat de uitvoering van een arbeidsovereenkomst echter gezagsuitoefening en toezicht van de werkgever impliceert, wordt algemeen aangenomen dat de werkgever binnen bepaalde grenzen het gebruik van communicatiemiddelen in het bedrijf mag controleren.[65]
In de eerste plaats beslist de werkgever natuurlijk zelf welke communicatiemiddelen hij ter beschikking stelt aan zijn werknemers en waarvoor deze middelen gebruikt mogen worden. Uit de rechtspraak kan men echter opmaken dat de werkgever bij de uitoefening van dit recht rekening moet houden met het feit dat de werknemer ook op de werkplaats een recht op privécommunicatie behoudt. Hij mag het gebruik van communicatiemiddelen dus niet zodanig beperken dat alle mogelijkheden voor privécommunicatie voor de werknemer worden afgesloten.
In de tweede plaats moet de werkgever ervoor zorgen dat de controle van de communicatiemiddelen op een transparante manier gebeurt. Het arbeidsrecht schrijft voor dat de ondernemingsraad geïnformeerd moet worden over de installatie en het gebruik van middelen die de werkgever toelaten om telefoongesprekken, elektronische post, e.a. te controleren. Indien deze controle gericht is op communicatie van individuele werknemers, is er ook sprake van een verwerking van persoonsgegevens. Alle regels van de wetgeving in dat verband,

---

websites van de Europese Commissie: http://ec.europa.eu /trade/creating-opportunities/trade-topics/dual-use/. Voor Vlaanderen worden de licenties afgeleverd door de Dienst Controle Strategische Goederen (CSG). Zie daarvoor http://www.vlaanderen.be/nl/economie-en-werk/buitenlands-beleid/vergunning-voor-uit-en-doorvoer-van-strategische-goederen.

65 Zie hierover: Aanbeveling nr. 8/2012 van 2 mei 2012, www.privacycommission.be.

o.m. met betrekking tot het verstrekken van informatie aan de betrokkenen, moeten dan ook correct worden toegepast.
In de derde plaats mag de werkgever bij de uitoefening van zijn controlerecht niet verder gaan dan noodzakelijk in het kader van een normale bedrijfsvoering.
Wat dit in de praktijk betekent, is verder uitgewerkt in een collectieve arbeidsovereenkomst die over dit onderwerp in de schoot van de Nationale Arbeidsraad werd gesloten (CAO nr. 81).[66] De CAO gaat uit van het principe dat de controle op de elektronische onlinecommunicatiemiddelen van de werknemers slechts is toegestaan indien minstens een van de volgende doelstellingen wordt nagestreefd:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;

- de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken;

- de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming;

- het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën.

Individualisering is zonder meer mogelijk voor de eerste drie doelstellingen. Voor de vierde doelstelling voorziet de CAO in een alarmbelprocedure. Indien uit de resultaten van de algemene supervisie van het netwerk blijkt dat een werknemer de terzake geldende regels in het bedrijf niet heeft gerespecteerd, dient hij te worden verwittigd. Pas in een tweede stadium mag tot individualisering van de communicatiegegevens worden overgegaan. De 'in de onderneming geldende beginselen en regels voor het gebruik van online technologieën' worden bij voorkeur expliciet vastgelegd in een document op ondernemingsvlak.[67]

66 Collectieve Arbeidsovereenkomst nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens, zie www.nar-cnt.be.

67 Zie hierover: Aanbeveling nr. 8/2012 van 2 mei 2012, http://www.privacycommission.be/nl/cybersurveillance; en ook Advies nr. 18/2013 van 5 juni 2013 naar aanleiding van een klacht tegen de installatie van een kwaliteitsgarantieplatform om telefoongesprekken tussen werknemers en potentiële klanten van de werkgever op te nemen.

G. Ongevraagde elektronische communicatie

Ongewenste boodschappen worden vaak als zeer hinderlijk ervaren. Het probleem is vooral in de actualiteit gekomen in de context van de elektronische post ('*spam*'). In België is de regelgeving over ongewenste communicatie vrij ingewikkeld. Men moet namelijk rekening houden met vier verschillende wetten.[68]

In de eerste plaats is de wet van 8 december 1992 over de verwerking van persoonsgegevens van toepassing. Het is het duidelijk dat iemand die een boodschap wil verzenden, daarvoor ook meestal de contactgegevens van de geadresseerde zal verwerken.[69] Bovendien geeft de wet aan iedereen over wie persoonsgegevens worden verwerkt, een recht van verzet tegen het gebruik van die gegevens voor '*direct marketing*'.

In de tweede plaats wordt het probleem geregeld door de wetgeving over de marktpraktijken en de bescherming van de consument. Artikel 100 van de Wet Marktpraktijken vereist dat aan consumenten slechts een aanbod kan worden verstuurd via oproepautomaat of telefax nadat hij hier zijn voorafgaande toestemming voor heeft gegeven ('*opt-in*'). Voor andere communicatietechnieken (bijvoorbeeld gewone, niet-geautomatiseerde telefoonoproepen) moet de consument duidelijke en verstaanbaar worden geïnformeerd over het recht zich te verzetten tegen het ontvangen van reclame in de toekomst. Met het oog op de bescherming tegen *direct marketing* via telefonische oproepen zijn in de artikelen 100/1 tot en met 100/7 van de Wet Marktpraktijken sinds 2012 gedetailleerde regels uitgevaardigd. Daarbij wordt aan de abonnees o.m. de mogelijkheid gegeven om hun nummer te laten opnemen op een specifieke 'Robinsonlijst' (zie: www.robinsonlijst.be). Elke telefoonoproep voor *direct marketing* naar een nummer dat in dit bestand is opgenomen, wordt verboden, tenzij de abonnee uitdrukkelijk heeft toegestemd (zie art. 100/2).

In de derde plaats wordt het vraagstuk van de ongewenste elektronische communicatie geregeld door de Wet Elektronische Handel.[70] Artikel 13 van de wet somt de voorwaarden op waaraan reclame die deel uitmaakt van een dienst van de informatiemaatschappij, of een dergelijke dienst vormt, moet voldoen. Voorts bepaalt artikel 14 § 1 dat het gebruik van elektronische post voor reclame verboden is zonder voorafgaande, vrije, specifieke en geïnformeerde toestemming van de geadresseerde van de boodschappen.[71] De bewijslast hiervan ligt bij de dienstverlener die moet kunnen aantonen dat daadwerkelijk om reclame via elektronische weg werd verzocht.

Tot slot, in de vierde plaats, legt artikel 114 van de Wet Elektronische Communicatie aan de leveranciers van elektronische-communicatiediensten en de leveranciers van software voor elektronische communicatie de verplichting op

68 Zie hierover: Aanbeveling 02/2013 van 20 januari 2013, www.privacycommission.be.

69 Zie o.m.: Brussel (11de kamer) 17 maart 2010, *R.D.T.I.* 2011, afl. 42, 51, noot F. COPPENS.

70 Wet van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, *BS* 17 maart 2003.

71 De regeling in de artikel 14 §1 werd verder uitgewerkt door het Koninklijk Besluit van 4 april 2003 tot reglementering van het verzenden van reclame per elektronische post, *BS* 28 mei 2003.

hun abonnees kosteloos, rekening houdend met de stand van de techniek, de gepaste veilige diensten aan te bieden die de eindgebruikers in staat stellen ongewenste elektronische communicatie in alle vormen te verhinderen. Bij de afdwingbaarheid van de door dit artikel opgelegde verplichting kunnen echter vragen worden gesteld.[72]

H. Omzetting van de Dataretentierichtlijn

Met de wet van 30 juli 2013, waarin een aantal bepalingen van de wet elektronische communicatie en het wetboek van strafvordering werden aangepast, werd de implementatie van de Europese Dataretentierichtlijn (Richtlijn 2006/24/EG) volledig afgerond.[73]

De wet bepaalt dat internetproviders en operatoren van vaste en mobiele telefonie de verkeersgegevens, locatiegegevens en identificatiegegevens van hun gebruikers gedurende twaalf maanden moeten bewaren.

Het begrip aanbieders wordt in dit kader ruim begrepen; de wet bepaalt dat ook doorverkopers in eigen naam en voor eigen rekening hieronder moeten worden verstaan. Voor wat betreft de gegevens die moeten worden bewaard, bepaalt de wet dat ook de gegevens betreffende een oproeping zonder resultaat moeten worden bijgehouden voor zover zij werden geregistreerd en opgeslagen/gelogd door de operator. Uitgesloten voor bewaring zijn de gegevens waaruit de inhoud van de communicatie kan worden opgemaakt.[74]

§3. Europese ontwikkelingen op het vlak van private communicatie

Voor wat betreft Europese ontwikkelingen is de Verordening van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van de e-Privacy richtlijn (Richtlijn 2002/58/EG) meest markant.[75]

De nieuwe verordening bepaalt de nieuwe geharmoniseerde regels voor alle aanmeldingen van inbreuken in verband met persoonsgegevens door aanbieders van elektronische communicatiediensten. De verordening bepaalt de re-

72 J. DUMORTIER, *ICT-recht*, Leuven, ACCO, 2013, p. 310.

73 Wet van 30 juli 2013 houdende de wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het wetboek van strafvordering, *BS* 23 augustus 2013, Memorie van Toelichting, *Parl. St.* Kamer 2012-2013, nr. 2921/1, www.dekamer.be.

74 Het uitvoeringsbesluit verduidelijkt welke telecomgegevens door de operatoren moeten worden bewaard; KB 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005, *BS* 8 oktober 2013.

75 EU Verordening Nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement betreffende privacy en elektronische communicatie, *Pb.L.* 26 juni 2013.

gels voor de notificaties waaraan telecomoperatoren en internettoegangsleveranciers zich moeten houden met betrekking tot alle inbreuken op de beveiliging die resulteren in een vernietiging, wijziging, niet-geautomatiseerde vrijgave van of toegang tot persoonsgegevens. Zo wordt onder meer bepaald dat de bevoegde nationale autoriteit uiterlijk 24 uur na de opsporing van de inbreuk hierover minstens een voorlopige kennisgeving ontvangt en dat de niet-naleving van de notificatieverplichting door een nationale sanctieregeling moet worden bestraft.