Advies nr 10/2012 van 21 maart 2012

Betreft: wetsontwerp houdende diverse bepalingen inzake elektronische communicatie (CO-A-2012-009)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verzoek om advies van de Vice-Eerste Minister, Minister van Economie, Consumenten en Noordzee ontvangen op 27/02/2012;

Gelet op het verslag van de Voorzitter;

Brengt op 21 maart 2012 het volgend advies uit:

I. ONDERWERP VAN DE ADVIESAANVRAAG

---

1. De Vice-Eerste Minister, Minister van Economie, Consumenten en Noordzee verzocht de Commissie op 27 februari 2012 om advies te verlenen over een wetsontwerp houdende diverse bepalingen inzake elektronische communicatie (hierna het "wetsontwerp").

2. De Commissie ontving eveneens bij de aanvraag een wetsontwerp houdende wijzigingen aan de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post– en telecommunicatiesector. De Commissie stelt vast dat in deze tekst geen verwerking van persoonsgegevens voorkomt die aanleiding dient te geven tot een advies van de Commissie Bescherming Persoonlijke Levenssfeer, zodat zij dit wetsontwerp verder niet bespreekt.

3. Het wetsontwerp beoogt de omzetting naar het nationaal recht van onder meer de Richtlijn 2009/136/EG[1], onderdeel van het nieuwe EU-telecompakket van 2009. Deze richtlijn bevat een wijziging van (onder meer) de Richtlijn 2002/58/EG met betrekking tot de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

4. De Commissie wordt geraadpleegd voor die aspecten van het wetsontwerp die de bescherming van persoonsgegevens aangaan. Zij wijst er pro memorie op dat zij voor een aantal verbandhoudende thema's reeds relevante opinies heeft geformuleerd zoals inzake dataretentie[2], en aangaande de problematiek van cybersurveillance of werkgeverscontrole op internet- en e-mailgebruik van werknemers[3].

---

[1] Richtlijn tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming

[2] Advies 20/2009 van 1 juli 2009 inzake het voorontwerp van wet en het ontwerp van koninklijk besluit inzake dataretentie, en het ontwerp van koninklijk besluit inzake de medewerkingsplicht, gepubliceerd op http://www.privacycommission.be/nl/docs/Commission/2009/advies_20_2009.pdf

[3] Zie de verkennende nota en aanbevelingen raadpleegbaar op www.privacycommission.be

II. TOEPASSELIJKE WETGEVING

---

5. Het voorliggend advies onderzoekt de artikelen van het wetsontwerp die betrekking hebben op de bescherming van de persoonlijke levenssfeer.

6. Deze artikelen worden getoetst aan de beginselen van de WVP, de beginselen van de Richtlijn 2002/58/EG en de standpunten van de Europese Gegevensbeschermingsautoriteiten aangaande de omzetting van de Richtlijnen 2002/58/EG en 2009/136/EG, en de diverse thema's die verband houden met privacy en elektronische communicatie.

7. De Commissie verwijst derhalve hierna herhaaldelijk naar de standpunten van
   - de Werkgroep artikel 29 (hierna "de Groep 29"[4])
   - de Internationale werkgroep voor gegevensbescherming in de telecommunicatiesector (hierna "de Groep van Berlijn"[5])
   - de Europese toezichthouder van Gegevensbescherming (hierna "EDPS"[6])

III. ALGEMEEN ONDERZOEK VAN HET WETSONTWERP

3.1. Overzicht aspecten bescherming persoonlijke levenssfeer

8. Het wetsontwerp gaat in op de verschillende aspecten van bescherming van de persoonlijke levenssfeer bij elektronische communicatie. De volgende thema's en artikelen in het wetsontwerp blijken relevant voor de bescherming van de persoonlijke levenssfeer :

   - Locatiegegevens tbv nooddiensten (artikel 64 wetsontwerp);
   - Toegang tot de telefoongegevens op de gedetailleerde factuur voor de betrokkene die niet de abonnee is (artikel 67 wetsontwerp) ;
   - Complementaire bevoegdheid BIPT aangaande de beveiliging van netwerken en diensten (artikelen 74-76 wetsontwerp) en aangaande de bevoegdheid om kennis te

---

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm. Zie vnl. Advies 1/2009 over de voorstellen tot wijziging van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-privacyrichtlijn), gepubliceerd op http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_nl.pdf en het advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising') http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_nl.pdf

[5] http://www.privacycommission.be/nl/international/berlin-telecom/

[6] http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=nl

nemen van interne procedures operatoren voor verzoeken om toegang tot persoonsgegevens (artikel 87);

- De meldplicht van een inbreuk op de veiligheid van een openbaar elektronische-communicatiedienst in verband met persoonsgegevens (artikel 77 wetsontwerp), hierna "smalle meldplicht" – definitie van inbreuk op de veiligheid van een openbaar elektronische-communicatiedienst in verband met persoonsgegevens (artikel 14, 25° wetsontwerp);
- Bijkomende uitzonderingen op het geheim van privécommunicatie en –telecommunicatie (artikelen 86 en 87 wetsontwerp);
- regeling van cookies en andere bestanden of spionage software (opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker) via de vereiste van toestemming (artikel 88 wetsontwerp), hierna de "cookie consent";
- De voorwaarden voor het verzamelen en publiceren in telefoongidsen van gegevens van de abonnees (artikelen 65 en 115 wetsontwerp) ;
- De bescherming van de gebruiker tegen ongewenste communicatie (artikel 123 wetsontwerp)

3.2. Algemene opmerkingen :

3.2.1 principe van complementariteit van de Wet van 13 juni 2005 tov de WVP – wettelijke verankering samenwerking BIPT en Commissie

9. De Commissie wijst op de mogelijkheid dat een aantal bepalingen van het wetsontwerp inzake beveiliging overlappen met de WVP die de Richtlijn 95/46 EG omzet[7]. Zij wijst op de intentie van de Europese wetgever om met de Richtlijn 2002/58/EG de Richtlijn 95/46/EG aan te vullen[8]. De bepalingen van de Wet van 13 juni 2005 en de WVP kunnen elkaar derhalve overlappen, doch dienen eerder als complementair te worden beschouwd dan als afbreuk doende aan de WVP.

10. Concreet betekent dit bijvoorbeeld dat in de gevallen waar geen toestemming vereist is voor het gebruik van bepaalde cookies, de betrokkene toch steeds zal moeten worden geïnformeerd op basis van de WVP door de betrokken websitehouder of derde (zie verder bij de bespreking van de uitzonderingen in artikel 88 van het wetsontwerp en de algemene informatieplicht onder artikel 9 §§1 en 2 WVP). Dit betekent bvb ook dat klanten of betrokkenen ten aanzien van wie elektronische communicatie wordt gebruikt via een of

[7] Sinds de inwerkingtreding op 1 december 2010 van de wet van 11 december 1998.
[8] Zie overweging 10 en de diverse bepalingen in de Richtlijn 2002/58/EG "onverminderd" in artikel 2 van deze Richtlijn

andere techniek (e-mail, fax, telefoon, cookies,..) steeds hun recht van verzet tegen alle verwerkingen met het oog op direct marketing behouden (bvb ook als er geen reclame zou zijn, als het gaat op communicaties voor niet-commerciële doeleinden…) (artikel 12 WVP).

11. De Commissie adviseert om, naar Nederlands voorbeeld[9], in de memorie van toelichting opnieuw duidelijk te herinneren aan deze complementariteit van de wet van 13 juni 2005 ten opzichte van de WVP, en om de diverse voorbeelden dienaangaande in dit advies te hernemen (zie ook hierna).

12. Anderzijds wenst de Commissie dat de wetgever een nauwere samenwerking tussen de Commissie en het BIPT[10] betreffende onderwerpen waar de wederzijdse toezichtsbevoegdheden elkaar raken expliciet zou vastleggen in de wet van 13 juni 2005 . Dit o.m. gelet op de wettelijke vertrouwelijkheidsverplichting in artikel 33 WVP.

3.2.2. netneutraliteit en deep packet inspection

13. De Commissie wenst tenslotte een ander aspect onder de aandacht te brengen, hoewel dit strikt genomen niet te maken heeft met de omzetting van de Richtlijn 2009/136/EG.

14. Zij is van oordeel dat de wetgever ook het nieuwe Europese beginsel van netneutraliteit[11] zou dienen wettelijk te verankeren in de wet van 13 juni 2005. Dit opdat de meest privacyintrusieve vormen van deep packet inspection[12] door Belgische ISPs en andere marktpartijen tijdig aan banden zou worden gelegd.

15. Zij verwijst naar het standpunt van de EDPS[13] dienaangaande en zal aangaande deze thema's een aparte aanbeveling formuleren.

---

[9] Zie pagina 14 van het rapport TNO-IViR, gepubliceerd op http://www.tno.nl/downloads/rapport_opta_35473.pdf

[10] Zie het Nederlandse voorbeeld uit 2009 http://www.cbpweb.nl/downloads_pb/pb_20090915_samenwerkingsovereenkomst_at-cbp.pdf

[11] Het begrip netneutraliteit *"komt voort uit de visie dat informatie op internet onpartijdig moet worden doorgegeven, ongeacht de inhoud, bestemming of bron, en dat de gebruikers moeten kunnen beslissen welke toepassingen, diensten en apparatuur zij willen gebruiken. Dit betekent dat ISP's niet naar eigen goeddunken de toegang tot bepaalde toepassingen, zoals peer-to-peer („P2P") en dergelijke, voorrang kunnen geven of mogen vertragen*

[12] DPI is in feite een al geruime tijd gekende techniek waarbij men in (quasi) real time bepaalde datapakketten in netwerkverkeer automatisch inspecteert. Als de techniek van DPI aan de hand van het normale klassieke postverkeer zou worden uitgelegd zou dit betekenen dat (minstens) de naam van de verzender, de ontvanger, het type envelope of bericht en dergelijke meer wordt verwerkt door de postdienst voor diverse doeleinden alvorens de brief zou worden bezorgd. Kennisname van de inhoud van de communicatie is niet altijd bij elke vorm van DPI aanwezig, maar is wel een technische (zij het illegale) mogelijkheid

[13] Advies van 7 oktober 2011 van de Europese toezichthouder voor gegevensbescherming over netneutraliteit, beheer van verkeersstromen en bescherming van de persoonlijke levenssfeer en persoonsgegevens, PB, C34/1, 8 februari 2012, gepubliceerd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0001:0017:NL:PDF

IV. ONDERZOEK VAN DE ARTIKELEN VAN HET WETSONTWERP

4.1. locatiegegevens tbv nooddiensten (artikel 64 wetsontwerp)

16. Artikel 64 van het wetsontwerp wijzigt artikel 107 van de wet van 13 juni 2005. Een §1/1 wordt in dat laatste artikel toegevoegd die toelaat aan de operatoren om samen te werken met ondernemingen die openbare elektronische communicatienetwerken leveren opdat de localisatie van de gebruikers die bellen naar de nooddiensten mogelijk zou worden gemaakt, zelfs indien ze bellen met een nomaden VoIP dienst[14], dit wil zeggen een dienst die ontkoppeld is van het originele netwerk en die niet wordt geassocieerd met een bepaald netwerk (bvb skype).

17. Het nieuwe wetsontwerp laat het BIPT toe om de wijze te bepalen waarop deze toegang zal worden verschaft. Het is mogelijk dat de VoIP operator wordt verplicht om informatie over haar klanten te verzamelen, met name over hun exacte locatiegegevens teneinde aan hun verplichtingen te kunnen voldoen.

18. De Commissie wijst op de plicht van de VoIP operator om onder deze informatieverzameling over de eindgebruikers de informatieplicht van artikel 9 WVP te respecteren. Deze informatieverzameling dient als enige doelstelling te hebben om de localisatie ten behoeve van de nooddiensten te verrichten, en niet ten behoeve van andere doeleinden (bvb commerciële diensten)

4.2. Toegang tot de telefoongegevens op de gedetailleerde factuur voor de betrokkene die niet de abonnee is (artikel 67 wetsontwerp en artikel 10 WVP)

19. Op het gebied van de gespecifieerde versies van basisfacturen vraagt de Commissie zich af of de abonnee die niet (altijd) de eindgebruiker is ook een gedetailleerde factuur kan vragen zonder akkoord van of informatie aan de eindgebruiker. De Commissie wijst op het raakvlak met het recht van toegang van de betrokkene (artikel 10 WVP) en denkt bijvoorbeeld aan de vaak voorkomende hypothese van een werkgever die de facturen betaalt en die het detail van deze facturen vraagt. De rechtspraak die dateert van voor de wet van 13 juni 2005 aanvaardde vaak de productie van dergelijke facturen.

---

[14] Met nomadiciteit wordt bedoeld: « eigenschap van een elektronische communicatiedienst waardoor deze dienst gebruikt kan worden vanuit potentieel om het even welke aansluiting op een elektronische-communicatienetwerk » (artikel 1, 14° koninklijk besluit van 27 april 2007). Zie Mededeling betreffende de interpretatie van het begrip « specifiek met het oog op nomadisch gebruik bij het Instituut gereserveerde geografische nationale E.164 nummers » bedoeld in artikel 43, vierde lid, van het koninklijk besluit van 27 april 2007 betreffende het beheer van de nationale nummeringsruimte en de toekenning en intrekking van gebruiksrechten voor nummers, B.S., 5 december 2007.

20. Wellicht kan de wetgever in de memorie van toelichting verduidelijken in welke gevallen de wet de abonnee die niet de eindgebruiker is toelaat om kennis te nemen van het detail van de facturen, en om in voorkomend geval de eindgebruiker toe te laten om ook kennis te nemen van het detail van de facturen die hij indirect heeft gegenereerd maar waarvoor hij niet heeft betaald.

21. Tenslotte zou het interessant zijn om in de aanhef van artikel 110 § 1 van de wet van 13 juni 2005 toe te voegen "Onverminderd de toepassing van artikel 10 Wet 8 december 1992 (…)", waardoor ook duidelijk is dat de betrokkene steeds toegang kan krijgen tot zijn telefoongegevens bij de operator, zelfs indien hij niet de abonnee is.

4.3. Complementaire bevoegdheid BIPT aangaande beveiliging van netwerken en diensten (artikelen 74-76) en aangaande de bevoegdheid om kennis te nemen van interne procedures operatoren voor verzoeken om toegang tot persoonsgegevens (artikel 87)

22. De artikelen 74 tot en met 76 betreffen de veiligheidsmaatregelen die de ondernemingen die openbare elektronische communicatienetwerken aanbieden en de ondernemingen die openbare elektronische communicatiediensten verstrekken dienen te nemen.

23. Meerdere bevoegdheden worden aan het BIPT gegeven om de te geven informatie te bepalen, om de te nemen veiligheidsmaatregelen te bepalen of om toezicht te houden op de acties van de verschillende actoren. Zoals reeds vermeld in voormeld punt 3.2.2. (complementariteit) is het duidelijk dat bepaalde bevoegdheden van het BIPT onder het wetsontwerp kunnen samenvallen met de bevoegdheden van de Commissie onder de WVP, vanuit het opzicht dat beide aspecten betrekking hebben op de beveiliging van persoonsgegevens.

24. Zo laat het nieuwe artikel 113 § 6 2° toe aan het BIPT om informatie te verschaffen in een gestandaardiseerde vorm via de ondernemingen aangaande de *"beschermingsmaatregelen tegen gevaren voor de persoonlijke veiligheid, de persoonlijke levenssfeer en persoonsgegevens bij het gebruik van elektronische communicatiediensten."*

25. Het nieuwe artikel 113/1 alinea 2 geeft het BIPT de bevoegdheid om toezicht te houden *"op het opsporen, het observeren en het analyseren van de veiligheidsproblemen"* en om *"informatie daarover aan de gebruikers te verstrekken."*

26. Artikel 114 § 2 laatste alinea voorziet dat het BIPT de door de ondernemingen genomen maatregelen kan controleren en aanbevelingen kan *"formuleren over de beste praktijken betreffende het veiligheidspeil dat met deze maatregelen moet worden gehaald".* Er wordt bepaald dat dit geldt "*Onverminderd de wet van 8 december 1992* (…)".

27. Naast de tussenkomst van het BIPT in geval van inbreuken op de veiligheid van een openbaar elektronische-communicatiedienst in verband met persoonsgegevens (zie hierna), laat het nieuwe artikel 114/1 § 4 aan het BIPT toe om richtsnoeren aan te nemen en instructies uit te vaardigen over de omstandigheden waarin de ondernemingen die openbare elektronische communicatiediensten aanbieden verplicht zijn om kennisgeving te verrichten van een inbreuk in verband met persoonsgegevens. Ook het toepasselijke formaat en de manier waarop de kennisgeving geschiedt kunnen hierbij worden bepaald.

28. Artikel 87 van het wetsontwerp verleent het BIPT de bevoegdheid om kennis te nemen van de interne procedures van de operatoren aangaande verzoeken toegang tot persoonsgegevens (nieuw artikel 127 § 6 van de wet van 13 juni 2005).

29. Gelet op de complementariteit van de Wet van 13 juni 2005 en de WVP is de Commissie van oordeel dat alle bevoegdheden en standpunten van het BIPT aangaande de beveiliging van persoonsgegevens (artikel 16 WVP) en het uitoefenen van het recht van toegang tot persoonsgegevens (artikel 10 WVP) rekening zouden dienen te houden met de standpunten van de Commissie, de Groep 29 en de EDPS in deze materie.

30. Zoals eerder vermeld dringt een nauwere samenwerking tussen Commissie en het BIPT zich op. Dit zou door het wetsontwerp kunnen worden aangemoedigd, door het voorafgaand advies van de Commissie meer systematisch in het wetsontwerp te voorzien in geval het BIPT een van voormelde regelgevende bevoegdheden (van het type gestandaardiseerde informatie, richtsnoeren, instructies) uitoefent, onverminderd de mogelijkheid om de samenwerking te formaliseren via een samenwerkingsprotocol voor de overige aspecten.

31. De Commissie gaat hierna verder in op het verschil met de "brede meldplicht" die een melding ten aanzien van alle privacycommissies zal instellen voor inbreuken op de veiligheid in verband met persoonsgegevens, ook indien die niet betrekking hebben op een openbare elektronische-communicatiedienst.

4.4. De meldplicht van inbreuk op de veiligheid van een openbaar elektronische-communicatiedienst in verband met persoonsgegevens (artikel 77 § 3 wetsontwerp), hierna "smalle meldplicht" – definitie van inbreuk op de veiligheid van een openbaar elektronische-communicatiedienst in verband met persoonsgegevens (artikel 14, 25°)

32. Artikel 77 § 3 van het wetsontwerp bepaalt dat *"In geval van een inbreuk op de veiligheid van een openbaar elektronische communciatiedienst in verband met persoonsgegevens"*, de *"onderneming die openbare elektronische communciatiediensten aanbiedt"* het BIPT *"onverwijld in kennis" stelt "van de inbreuk in verband met persoonsgegevens."*

33. Artikel 77 § 3 van het wetsontwerp introduceert wat men in de literatuur een "smalle meldplicht" pleegt te noemen. Dit in aanvulling van een reeds bestaande informatieverplichting aan abonnees van "bijzondere risico's van inbreuken op de beveiliging van het netwerk"[15]. De term "smalle meldplicht" wijst vooral op de beperking van de meldplicht, met name de beperkte toepassing in de telecomsector (enkel de veiligheid van openbare elektronische communicatiediensten is voorwerp van de meldplicht).

34. De Commissie stelt vast dat de wetgever kiest voor de mogelijkheid om het BIPT in plaats van de Commissie aan te duiden als instantie aan wie dient te worden gemeld. Zij acht dit een logische opportuniteitsafweging gelet op de bestaande expertise van het BIPT los van de mogelijkheid onder de Richtlijn 2009/136/EG om een privacycommissie aan te duiden als "de bevoegde nationale instantie", hetgeen reeds het geval was in bepaalde lidstaten[16].

35. De Commissie verzoekt de wetgever wel om aandacht te hebben voor twee problemen die de keuze voor het BIPT met zich mee zal brengen.

36. Gelet op de complementariteit van de WVP met de wet van 13 juni 2005 inzake beveiliging van persoonsgegevens (zie hiervoor) bestaat er vandaag reeds het risico van discordantie bij tussenkomst van twee instanties in dezelfde materie (beveiliging van persoonsgegevens). Om tegenspraak in de standpunten te vermijden zal, zoals reeds gezegd, meer samenwerking met het BIPT vereist zijn.

---

[15] artikel 114 van de wet van 13 juni 2005 (artikel 4.1 Richtlijn 2002/58/EG)

[16] Zie bvb Frankrijk, waar dient te worden gemeld aan de CNIL. http://www.cnil.fr/la-cnil/actualite/article/article/transposition-du-paquet-telecom-renforcement-des-droits-des-internautes-et-signalement-des-fail/

37. Anderzijds zal sowieso op langere termijn rekening moeten worden gehouden met de lopende Europese discussie over de brede meldplicht[17] aan de privacycommissies. In de Richtlijn 2009/136/EG verklaarde de Europese Commissie reeds dat de introductie van een brede meldplicht (dwz toepasselijk op alle sectoren) als een prioriteit dient te worden beschouwd.[18] Ook de groep 29[19] sprak zich voor een brede meldplicht uit.

38. De Commissie verzoekt de wetgever reeds oog te hebben voor de mogelijke problemen die de parallelle handhaving van smalle en brede meldplicht op termijn kunnen stellen. Hoewel de Commissie de mogelijkheid verkiest om de smalle en brede meldplicht naast elkaar te introduceren, zal de wetgever dienen erover te waken dat dit op gecoördineerde wijze gebeurt (analoge modaliteiten van de meldplicht). Ook vraagt de Commissie dat nauwere samenwerking tussen het BIPT en de Commissie reeds expliciet door de wetgever wordt ondersteund in de Wet van 13 juni 2005.

39. De Commissie vindt de modaliteiten van de smalle meldplicht in artikel 77 § 3 nog onvoldoende duidelijk. In elk geval zullen de te melden risico's beter in kaart moeten worden gebracht. Alles melden en verwerken is immers geen optie; een totale formalisering van het notificatieproces nastreven werkt contraproductief. De Commissie is derhalve voorstander voor verduidelijkende uitvoeringsbepalingen. De Koning zou, na advies van de Commissie, kunnen bepalen wat de modaliteiten van de meldplicht zijn.

40. De Commissie wijst op een aantal positieve elementen in de omzetting van artikel 2 4 c) Richtlijn 2009/136/EG. Zo wordt het advies van de Groep 29 op een punt gevolgd. Waar de groep 29 pleitte voor een onmiddellijke melding[20], werd dit opgevolgd via het woord "onverwijld".

---

[17] Zie artikel 31 van het voorstel van Europese dataprotectieverordening van de Europese Commissie van 25 januari 2012, gepubliceerd op http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[18] Overweging 59 Richtlijn 2009/136/EG : "*De melding van beveiligingsinbreuken betreft evenwel het algemene belang van het feit dat burgers ingelicht worden over beveiligingstekortkomingen die kunnen resulteren in het verlies of de compromittering van hun persoonsgegevens, alsook over beschikbare of aan te raden voorzorgen die zij kunnen nemen om de eventuele economische verliezen of sociale schade als gevolg van dergelijke tekortkomingen tot een minimum te beperken. Het belang van gebruikers om te worden ingelicht is duidelijk niet beperkt tot de sector elektronische communicatie, en bijgevolg moeten op Gemeenschapsniveau prioritair expliciete, verplichte meldingseisen worden ingevoerd die in alle sectoren gelden. In afwachting van een door de Commissie uit te voeren evalutatie van alle relevante Gemeenschapswetgeving op dit gebied moet de Commissie, in overleg met de Europese Toezichthouder voor gegevensbescherming, onverwijld passende maatregelen nemen ter bevordering van de beginselen inzake melding van inbreuken betreffende gegevens uit Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie), ongeacht de sector of het soort gegevens.*"

[19] Pagina 5 opinie http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_nl.pdf

[20] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_nl.pdf

41. Verder stelt zij zich vragen over de interpretatie van de "technische uitzondering "op de meldplicht in artikel 77 § 3[21]. Deze uitzondering komt erop neer dat indien de persoonsgegevens worden gecodeerd, er geen nood zou zijn aan een meldplicht.

42. De Commissie treedt hier het standpunt van de groep 29 bij, die zich uitsprak tegen deze uitzondering[22] in artikel 4 c) Richtlijn 2009/136/EG die de opzet van de meldingsplicht totaal mist. Het al dan niet beschermen van persoonsgegevens met behulp van encryptie of andere middelen is slechts een modaliteit. De hoofddoelstelling van de meldingsplicht is juist om de getroffen persoon op kwalitatieve en nuttige wijze te kunnen informeren als er een afdoende hoog risico is voor deze burgers. Veronderstellen dat er geen risico is als gecodeerde persoonsgegevens worden gecompromitteerd, is een onjuiste veronderstelling en zou eerder andere vragen moeten oproepen zoals naar de wijze van codering (al dan niet end to end), of het al dan niet gaat om gevoelige persoonsgegevens in de zin van de WVP,….

43. Hoewel artikel 77 § 3 van het wetsontwerp een letterlijke omzetting is van artikel 4 c) Richtlijn 2009/136/EG is de Commissie derhalve voorstander van een meer risicogebaseerd kennisgevingsmodel.

4.5 Bijkomende uitzonderingen op geheim van privécommunicatie en –telecommunicatie (artikelen 86 en 87)

44. Het wetsontwerp voorziet in artikel 125 § 1 Wet 13 juni 2005 twee bijkomende uitzonderingen op het verbod om elektronische communicatie te onderscheppen. In de lijst van diensten waarvoor de bepalingen van artikel 124 van de wet van 13 juni 2005 en de artikelen 259*bis* en 314*bis* van het Strafwetboek niet van toepassing zijn worden toegevoegd :

    - bijkomende uitzondering voor de ambtenaren die zijn gemachtigd door de Minister die de economie tot zijn bevoegdheid heeft (In het kader van hun wettelijke bevoegdheden tot opsporing); en

---

[21] *"Inkennisstelling van een betrokken abonnee of individuele persoon van een inbreuk in verband met persoonsgegevens is niet vereist wanneer de onderneming die openbare elektronische-communicatiediensten aanbiedt tot voldoening van het Instituut heeft aangetoond dat zij de gepaste technologische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft."*

[22] Pagina 7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_nl.pdf : *"een dergelijke bepaling zou de kwaliteit en het nut van de aan de getroffen personen verstrekte informatie aanzienlijk beperken. Getroffen gebruikers kunnen wellicht alleen passende stappen nemen om de risico's te verminderen waarmee zij te maken krijgen, wanneer zij toereikend zijn geïnformeerd. Derhalve benadrukt de Groep het belang van het kennisgevingsmodel en hecht zij eraan dat er een risicobeoordeling wordt verricht om vast te stellen of burgers in kennis moeten worden gesteld, ongeacht de technische maatregelen die getroffen werden ter bescherming van hun gegevens."*

- bijkomende uitzondering voor de handelingen van de ethische commissie en haar secretariaat (in het kader van hun wettelijke onderzoeksopdrachten[23])

45. De Commissie heeft geen bijzondere opmerkingen op deze bijkomende uitzonderingen, voor zover zij gegrond zijn op een duidelijke wettelijke basis en worden aangewend voor een specifieke onderzoeksopdracht (artikel 22 Grondwet en 8 EVRM).

46. De Commissie stelt vast dat de huidige uitzondering ten behoeve van het BIPT wordt aangepast in volgende zin : *"4° wanneer de handelingen door het Instituut worden gesteld op bevel van de onderzoeksrechter en/of in het kader van zijn algemene opdracht inzake toezicht en controle".* Diverse vragen kunnen worden gesteld over het nut van deze aanpassing. Hoewel de tussenkomst van een onderzoeksrechter zeker kan gezien worden als een versterkte bescherming van de persoonlijke levenssfeer van de betrokkenen, stelt de Commissie zich toch vragen bij de onduidelijke bewoordingen (de "en/of" laat uitschijnen dat het bevel van de onderzoeksrechter niet nodig is indien het BIPT onder haar algemene opdracht optreedt). De reden waarom gelijkaardige voorwaarde ("op bevel van de onderzoeksrechter") niet wordt opgelegd aan pakweg de ombudsdienst voor telecommunicatie (artikel 125 § 1, 5°) roept vragen op naar de logica. De memorie van toelichting bevat dienaangaande geen uitleg. Verder zijn de modaliteiten van een samenwerking tussen het BIPT en de onderzoeksrechters onduidelijk, en creëert deze bepaling een verschil in de diverse administratieve procedures.

47. De Commissie verzoekt dan ook de bijkomende voorwaarde te schrappen uit artikel 88 van het wetsontwerp.

4.6 (uitzondering op) toestemmingsvereiste, diverse soorten cookies en andere vormen van opslag of consultatie van informatie (artikel 88 wetsontwerp)

48. Software om heimelijk de handelingen van de gebruiker te monitoren of de werking van de eindapparatuur van de gebruiker ten bate van derden te beïnvloeden („spyware") vormt, evenals virussen, een ernstige bedreiging voor de privacy van de gebruiker[24]. Het gewijzigde artikel 5.3. van de Richtlijn 2002/58/EG heeft daarom de bescherming van de gebruikers van elektronische netwerken versterkt door de toestemming te vereisen voordat informatie zoals cookies wordt opgeslagen op of wordt geconsulteerd op de gebruiker (of abonnee) zijn eindapparatuur.

---

[23] Zie de artikelen 134 en 134/1 van de wet van 13 juni 2005. De overige reglementering van de ethische commissie is te raadplegen op haar website http://www.telethicom.be (officiële publicaties > wetgeving)
[24] Overweging 65 Richtlijn 2009/136/EG

49. Deze toestemming is evenwel niet altijd vereist voor alle informatie die wordt opgeslagen op of wordt geconsulteerd op de gebruiker (of abonnee) zijn eindapparatuur. 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) het tweede criterium is "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."

50. De cookies die al dan niet aan een van beide criteria beantwoorden zouden beter dienen te worden omschreven door de wetgever (bvb in de memorie van toelichting). Voorbereidend werk in de schoot van de groep 29 aangaande een standpunt over cookies en een Nederlandse survey in opdracht van OPTA[25] in een rapport van TNO-IViR wijst alvast uit dat de lijst van cookies waarvoor geen toestemming vereist is en waarmee weinig privacy- en dataprotectieproblemen gemoeid zijn vrij beperkt is.

51. De cookies die zijn vrijgesteld van de toestemmingsplicht zijn vnl. bepaalde "first party" cookies[26] en dan nog vnl. van het type "user input session cookies", dwz cookies die door de gebruiker zelf geplaatst zijn en die taalinstellingen en persoonlijke voorkeuren onthouden bij een webwinkel (bvb klantidentificatie en virtueel winkelwagentje).

52. 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 "persistente cookies", "flash cookies", "supercookies" en "evercookies"[27]. De kenmerken van dergelijke cookies zijn verregaand. Het gaat hierbij om cookies die duidelijk niet op expliciet verzoek van de gebruiker worden gevraagd, die op het eindapparaat blijven soms na een wisactie (zgn. respawning[28]), en worden gebruikt voor diverse of onbepaalde doeleinden. 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.

---

[25] http://www.tno.nl/downloads/rapport_opta_35473.pdf

[26] Indien de websiteuitgever zelf cookies plaatst, wordt deze first party cooky genoemd. Zie pagina 16 van het hiervoor vermelde TNO-IViR rapport

[27] Een goede uitleg hierover is te vinden op pagina 8 van het rapport van ENISA van 2 februari 2011, Bittersweet cookies. Some security and privacy considerations, gepubliceerd op http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies

[28] Volgens pagina 3 van het TNO-IViR rapport wordt hierbij een verwijderde (http) cookie hersteld door een andere (flash) cookie.

53. De Commissie stelt net als andere gegevensbeschermingsautoriteiten in deze het gebrek aan duidelijkheid vast in het gewijzigde artikel 5.3. van de Richtlijn 2002/58/EG, dat in zeer abstracte en technische termen is opgesteld, zodat de buitenstaander moeilijk de impact van deze bepalingen kan inschatten. Volgens voormelde studie van TNO-IViR blijken zeer weinig gebruikers afdoende kennis te hebben om zich afdoende te kunnen beschermen. Hoewel de term cookies wel bekend is, worden cookies niet vanzelfsprekend gekoppeld aan online reclame op basis van surfgedrag ("online behavioural advertising" of "OBA"), en is het maken van een onderscheid tussen de diverse types cookies en hun mogelijk gebruik voor de meeste gebruikers een brug te ver. Informatie over geavanceerde cookies en het opstellen van profielen bleek in de meerderheid van de gevallen niet voorhanden. Doorsnee gebruikers hebben ook beperkte vaardigheden. Zo is het blokkeren van flash cookies voor "jan modaal" totaal onhaalbaar[29].

54. Het wetsontwerp en de memorie van toelichting nemen deze onduidelijkheid over door nergens te verduidelijken waarover het concreet gaat.

55. De Commissie is van oordeel dat artikel 88 van het wetsontwerp een loutere technische omzetting is van het beginsel van "cookie consent", die zij op zichzelf genomen onvoldoende acht als wettelijke bepaling om alle types en vormen van (inmengingen via) cookies afdoende af te bakenen en te legitimeren, en om de betrokkenen afdoende te beschermen.

56. De Commissie verzoekt de aandacht van de wetgever voor diverse problemen die aantonen dat dergelijke technische omzetting totaal onvoldoende is om de europese doelstelling van bescherming van de betrokkenen te behalen.

Probleem 1 : terminologie

57. De Commissie stelt vast dat aangaande de terminologie een nog lopende Europese discussie bestaat over de interpretatie van begrippen zoals "eindapparatuur", "cookies", de uitzonderingen op de vereiste van toestemming naargelang het type cookie en gebruiksdoeleinden van de cookie, de wijze waarop de toestemming kan worden verleend en de andere technieken voor opslag en consultatie van informatie. De wetgever dient derhalve minstens deze discussie op te volgen teneinde een duidelijker wettelijker omkadering te geven voor de diverse vormen van "consultatie van informatie" en het begrip "eindapparatuur"

[29] Zie pagina 3 van voormelde studie TNO-IViR

58. Een bijzonder terminologisch probleem is dat artikel 88 van het wetsontwerp enkel spreekt van "abonnee of eindgebruiker", terwijl de WVP het steeds heeft over het ruimere begrip "betrokkene". De Commissie verwijst opnieuw naar haar opmerking aangaande complementariteit (zie punt 3.2.2. hiervoor). Dit betekent dat als de abonnee niet de gebruiker is (bijvoorbeeld werkgever als abonnee), de betrokkene (dus de gebruiker) steeds dient te worden geïnformeerd, eventueel naast de abonnee (op basis van de gezamenlijke toepassing van artikel 10 WVP en de Wet van 13 juni 2005).

Probleem 2 : onjuiste veronderstellingen : browserinstelling is niet werkbaar als toestemming, niet voor elke cookie is een toestemming met hinderlijke pop-up en meer opslag van persoonsgegevens vereist

59. Probleem is ook dat al te vaak nog door de vertegenwoordigers van de belanghebbende ondernemingen wordt uitgegaan van verkeerde veronderstellingen en onjuiste argumenten in de debatten zoals de zogezegde oplossing "de browserinstelling van de gebruiker bepalend te laten zijn voor de vraag of de gebruiker de vereiste toestemming voor het plaatsen en lezen van cookies heeft gegeven"[30]. Marktpartijen kunnen echter ongestoord cookies blijven plaatsen omdat de drie belangrijkste browsers (Microsoft's Internet Explorer, Mozilla's Firefox en Google's Chrome) als standaardinstelling hebben dat ze alle cookies automatisch accepteren[31]. Ook wordt ten onrechte het beeld geschetst door de belanghebbende ondernemingen dat voor elke cookie apart toestemming zou moeten worden gevraagd, wat een uiterst hinderlijk pop-up scherm tot gevolg zou hebben. Dit valse argument overtuigde nochtans de Nederlandse wetgever die stelde in de memorie van toelichting bij de Nederlandse telecomwet : *"De consequentie hiervan is volgens de ingezonden reacties dat het gebruik van het internet gebruiksonvriendelijk wordt, dat in de praktijk de gebruiker steeds toestemming zal verlenen zonder zich te realiseren waarvoor en dat er juist meer persoonsgegevens geregistreerd moeten worden door degene die verantwoordelijk is voor de cookies".* Ook dat is een onjuiste voorstelling van de zaken, nu de Richtlijn en artikel 88 van het wetontwerp uitzonderingen toevoegen waarvoor de toestemming niet vereist is, waardoor de toestemming dus beperkt blijft tot de meest intrusieve toepassingen via cookies (vnl. de cookies van derde partijen) en bij normale toepassing van het Europese recht het aantal hinderlijke pop-ups over de tijd zal afnemen[32] (zgn. "leerproces" op basis van eerder gegeven toestemming, uiteraard voor zover vereist).

---

[30] Zie parlementaire voorbereiding Nederlandse telecomwet.

[31] Zie pagina 2 van het schrijven dd. 14 maart 2011 waarin de voorzitter van het Nederlandse College Bescherming Persoonsgegevens, tevens voorzitter van de Groep 29, reageert tegen deze argumenten. Zie http://www.cbpweb.nl/downloads_med/med_20110422_cookies_brief.pdf

[32] Zie pagina 3 van het schrijven van de Groep 29 van augustus 2011, gepubliceerd op http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf

Probleem 3 : buitenlandse studies wijzen op collectief verzuim van de informatieplicht door de sector, en er worden geen of nepoplossingen voorgesteld die geen toestemming inhouden

60. Uit onderzoek in Nederland[33] en Engeland[34] blijkt dat bedrijven die cookies plaatsen de gewone informatieplicht collectief verzuimen (artikel 9 WVP). De Nederlandse voorzitter van het College Bescherming Persoonsgegevens reageerde aldus ten aanzien van de Tweede Kamer : *"De belanghebbende bedrijven hebben de afgelopen jaren geen initiatieven ondernomen om mensen te informeren en keuzes te bieden via "best practises" of andere vormen van zelfregulering".*

61. Ook de volgende stap, op voorafgaande informatie gebaseerde toestemming ("informed consent") wordt derhalve niet door de bedrijven aangeboden. In dezelfde reactie stelt de Nederlandse voorzitter dat de betrokken bedrijven menen te kunnen volstaan met "opt-out constructies"[35] en een gemeenschappelijk ikoontje als invulling van de informatieplicht. Dit blijkt een Europees probleem. Er is sprake van een aanhoudende discussie tussen de Europese gegevensbeschermingsautoriteiten[36] enerzijds en vertegenwoordigers van de online advertentieindustrie[37] (IAB Europe en EASA) anderzijds aangaande de tot nu uitgewerkte "oplossingen" via zelfregulering aangaande het gebruik van cookies voor online reclame op basis van surfgedrag ("online behavioural advertising" of "OBA"). De Groep 29 benadrukte hierbij de vereiste van een concrete wilsuiting van de betrokkenen. Uiteraard is het niet zo dat alle cookies worden gebruikt ten behoeve van OBA. Maar OBA roept diverse vragen op omdat hierbij verschillende partijen betrokken kunnen zijn[38], er sprake is van verregaande profilering[39] van de gebruikers, hetgeen een efficiënte aanpak van dit type gebruik van cookies nog meer prioritair maakt.

---

[33] Zie pagina 5 punt 5 van voormelde studie TNO-IViR (http://www.tno.nl/downloads/rapport_opta_35473.pdf) : "Meer dan de helft van de partijen uit de survey blijkt de gebruiker niet te informeren".
[34] Zie het rapport van ENISA van 2 februari 2011, Bittersweet cookies. Some security and privacy considerations, gepubliceerd op http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies

[35] Gedoeld wordt op het "IAB Europe OBA Framework". Zie http://www.iabeurope.eu/news/self-regulation-framework.aspx
[36] Zie het advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising') http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_nl.pdf
[37] Zie de brieven van de Groep 29 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20111215_letter_oba_industry_en.pdf betreffende onder meer de IAB "i" icon oplossing
[38] Websiteuitgevers, adverteerders, advertentienetwerk, statistiekenleveranciers,…. Zie de Nederlandse survey gepubliceerd op http://www.tno.nl/downloads/rapport_opta_35473.pdf
[39] Zie Aanbeveling CM/Rec(2010)13 van 23 november 2010 van de Raad van Ministers over de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van profilering, gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864 en de explanatory memorandum gepubliceerd op https://wcd.coe.int/wcd/ViewDoc.jsp?id=1693029&Site=CM

Probleem 4 : toerekenbaarheid van de informatieplicht bij OBA

62. Gelet op het groot aantal partijen[40] dat betrokken kan zijn bij het gebruik van bepaalde "third party" cookies zoals in geval van OBA, dient de wetgever heel duidelijk af te bakenen op wie de informatieplicht weegt. Er dient (bvb in het online privacybeleid op basis van artikel 9 WVP) meer transparantie over de samenwerkingsvoorwaarden tussen deze partijen aan de gebruikers te worden gegeven, op basis waarvan de (mede)verantwoordelijkheid van elk van de betrokken partijen kan worden bepaald ten aanzien van de betrokkene toe.

63. Op basis van voormelde redenen en argumentatie schaart de Commissie zich achter de oproep van haar Nederlandse collega's om in artikel 88 van het wetsontwerp de ***ondubbelzinnige*** toestemming van de gebruikers en abonnees te vereisen voor de meest privacyinvasieve cookies (voor alle duidelijkheid dus niet voor de cookies waarvoor de voormelde vrijstelling op de toestemming geldt).

64. De Commissie roept de wetgever ook op om bijkomende toelichting mogelijk te maken door

- Te verwijzen naar de mogelijkheid voor het BIPT[41] of de Koning om, na voorafgaand advies van de Commissie, een besluit te nemen over welk type cookies met welk doel (gebruikstelling) kunnen vallen onder de uitzonderingen, dit aan de hand van de aanvullende verduidelijking die de Commissie verwacht vanuit Europa op dit punt[42], of de FAQ lijsten[43] die elders worden opgesteld door de bevoegde nationale instantie;
- Op gelijkaardige wijze de mogelijkheid voorzien om te bepalen voor welk type cookies de toestemming vereist is;
- de bijkomende informatieplicht te voorzien ten aanzien van de gebruiker en abonnee die, gelet specifieke aard van de verwerking, noodzakelijk is om de betrokken afdoende te beschermen (artikel 9 § 1 d) in fine WVP), zoals duidelijke informatie over welk types cookies worden gebruikt met welke doeleinden, en hoe men vnl. de cookies van derde partijen kan schrappen of blokkeren,… via de browser of op andere wijze

---

[40] Zie pagina 12 van het advies 02/2010 van de Groep 29 over online reclame op basis van surfgedrag, aangehaald op pagina 15 van voormelde studie ("normadressanten"), gepubliceerd op http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_nl.pdf. De groep 29 onderscheidt advertentienetwerken, adverteerders, mediabureaus en webstatistieken

[41] Zie de analoge bevoegdheid van het BIPT om de nummerreeksen inzake telefonie en SMS verkeer te bepalen

[42] De Commissie verwacht dat de groep 29 in 2012 een aanvullende opinie zal publiceren die meer duidelijkheid geeft over het type cookies dat kan vallen onder de uitzondering op de vereiste van toestemming.

[43] Zie bijvoorbeeld de FAQ lijst van de CNIL, en dan vnl. de vraag nr. 4 ("4. Tous les cookies sont-ils concernés , gepubliceerd » op http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/ce-que-le-paquet-telecom-change-pour-les-cookies/)

.

65. De memorie van toelichting bij artikel 88 van het wetsontwerp zou iets meer praktische verduidelijking kunnen bieden door te bepalen dat het gaat om de reglementering van het gebruik van (onder meer) cookies op de PC's, en dat de standaardinstellingen van de belangrijkste browsers vandaag geen toestemming kunnen inhouden, tenzij zij standaard third party cookies zouden weigeren en weggooien, dat de gebruiker per derde partij de keuze heeft om cookies te accepteren, ook op mobiele apparatuur,…

4.7. De voorwaarden voor het verzamelen en publiceren in telefoongidsen van gegevens van de abonnees (artikelen 65 en 115 van het wetsontwerp) ;

66. Namen, adressen en telefoonnummers van natuurlijke personen zijn persoonsgegevens in de zin van de WVP. Hun publicatie in een gids op het Internet vormt een verwerking, waardoor de WVP van toepassing is.

67. Onder het stelsel van de WVP is een verwerking enkel in een aantal gevallen toegelaten. Één van deze gevallen wordt in art. 5 c beschreven: *"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".* Een dergelijke wettelijke basis kan gevonden worden in art. 45, § 2 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Deze bepaling voorziet er onder meer in dat *"de personen die openbare telefoondiensten aanbieden aan abonnees […] de noodzakelijke abonneegegevens ter beschikking [stellen] van de personen die een aangifte [bij Het Belgisch Instituut voor postdiensten en telecommunicatie] hebben gedaan […]",* en dit met het op de levering van een telefoongids.

68. Gebruikers moeten volgens de Richtlijn 2009/136/EG *"op de hoogte worden gebracht van hun rechten met betrekking tot het gebruik van hun persoonlijke informatie in abonneegidsen, met name van het doel of de doelen van deze gidsen, alsmede van hun recht om kosteloos niet in een openbare abonneegids te worden opgenomen, overeenkomstig Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie). Waar systemen bestaan waarbij informatie in de gegevensbank van de abonneegids mag worden opgenomen maar niet toegankelijk voor de gebruikers van de gidsdiensten mag worden gemaakt, moeten de klanten ook over deze systemen worden geïnformeerd."*[44] Deze bepaling heeft betrekking op artikel 12 Richtlijn 2002/58/EG.

69. Verder bepaalt de wet betreffende de elektronische communicatie ook het volgende: "Zonder kosten voor de abonnees, houden de personen die aan abonnees openbare

[44] Overweging 33 Richtlijn 2009/136/EG

telefoondiensten aanbieden de gegevens apart met betrekking tot de abonnees die gevraagd hebben niet te worden opgenomen in een telefoongids, zodat die abonnees de telefoongids kunnen ontvangen zonder dat hun gegevens daarin vermeld staan" (art. 45, § 3).

70. De Commissie is van oordeel dat het schrappingsrecht in artikel 12.2 Richtlijn 2002/58/EG[45] vandaag nog niet volledig in Belgisch recht is omgezet.

71. Volgens de wet van 13 juni 2005 moest een specifieke regelgeving de voorwaarden voorzien om de gegevens uit de telefoongids te wissen. Het koninklijk besluit dat deze voorwaarden zou moeten bepalen in uitvoering van artikel 133 § 2[46] van de wet van 13 juni 2005, is echter nog niet genomen zodat de Belgische reglementering vandaag nog geen rekening houdt met de Richtlijn 2009/136/EG. De actuele bewoording van artikel 133 § 2 is ook onnodig formalistisch (KB, advies Commissie en BIPT) en stelt actueel de betrokkenen en de Commissie voor problemen in diverse dossiers, doordat bepaalde uitgevers van telefoongidsen in België actueel menen geen gevolg te moeten geven aan verzoeken tot schrapping. Operatoren verwijzen naar de verplichting opgelegd door artikel 45 § 2 van de wet van 13 juni 2005[47].

72. De Commissie verzoekt de Belgische wetgever om van het bepalen van de voorwaarden om de gegevens uit de telefoongids te wissen een prioriteit te maken. Concreet verzoekt zij de wetgever om artikel 133 § 2 van de wet van 13 juni 2005 laatste lid zo aan te passen dat de bepaling "volgens de procedures en onder de voorwaarden bepaald door de Koning, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut" wordt vervangen door "volgens de procedure voorzien in artikel 12 § 1 laatste lid van de wet van 8 december 1992".

---

[45] *"2. De lidstaten zorgen ervoor dat de abonnees de gelegenheid krijgen zelf te bepalen of, en zo ja welke, persoonsgegevens in een openbare abonneelijst worden opgenomen, voorzover die gegevens relevant zijn voor de doeleinden van de abonneelijst zoals bepaald door de aanbieder ervan, en om de gegevens daarin te verifiëren, te corrigeren of te laten verwijderen. Het niet opgenomen zijn in een openbare abonneelijst of de verificatie, correctie of verwijdering van persoonsgegevens van dergelijke lijsten brengt geen kosten met zich."*

[46] Art. 133 § 2 Wet 13 juni 2005. *"Iedere abonnee is gerechtigd de persoonsgegevens die op hem betrekking hebben in te zien overeenkomstig de voorwaarden bepaald door of krachtens de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.*

Iedere abonnee is bovendien gerechtigd om kosteloos, volgens de procedures en onder de voorwaarden bepaald door de Koning, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de persoonsgegevens die op hem betrekking hebben te laten verbeteren of te laten verwijderen uit de telefoongids of de telefooninlichtingendienst."

[47] Art. 45 § 2 Wet 13 juni 2005 *"De personen die openbare telefoondiensten aanbieden aan abonnees stellen de noodzakelijke abonneegegevens ter beschikking van de personen die een aangifte hebben gedaan in de zin van § 1, onder billijke, redelijke en niet- discriminerende, technische, financiële en commerciële voorwaarden."*

4.8. Bescherming van de gebruiker tegen ongewenste communicatie (artikel 123 van het wetsontwerp)

73. Het wetsontwerp wijzigt artikel 100 van de Wet van 6 april 2010 betreffende marktpraktijken en consumentenbescherming. Bedoeling is om artikel 2 Richtlijn 2009/136/EG om te zetten die artikel 13 Richtlijn 2002/58/EG ("ongewenste communicatie") wijzigde.

74. Volgens het nieuwe artikel 13 Richtlijn 2002/58/EG moet de nationale wetgever o.m. duidelijk voor de abonnees of gebruikers de keuzemogelijkheden (met name inzake opt-out) opsommen tussen toestemming en het recht van verzet die van toepassing zijn bij gevallen die niet onder het eerste en tweede lid van artikel 13 vallen. In de praktijk gaat het vooral om het aanpakken van telemarketing (zgn "cold calling")[48], voor zover de betrokkene geen klant is.

75. De Commissie is van oordeel dat artikel 123 van het wetsontwerp deze opdracht onvoldoende duidelijk tot uitvoering brengt.

76. Ten eerste dient de wetgever duidelijker een gemotiveerde keuze te maken tussen het beginsel van voorafgaande toestemming ("opt-in") of verzet in geval van telemarketing ("opt-out"). Indien de wetgever vervolgens voor opt-out kiest, dient hij deze keuze te motiveren. Een mogelijkheid is dat de memorie van toelichting zou verwijzen naar de verwachte evolutie in het Europese gegevensbeschermingsrecht[49] om de keuze voor opt-out te verdedigen. Een andere mogelijkheid is dat de wetgever verwijst naar het beperkte aantal lidstaten[50] die een keuze voor opt-in maakten inzake telemarketing.

77. Indien de wetgever voor opt-out kiest dient hij ook meer nadruk te leggen op de kwaliteit van informatie over de reeds bestaande verzetsmogelijkheden voor de abonnees en gebruikers vandaag. Een probleem dat blijkt uit de vragen en klachten die de Commissie vandaag ontvangt over dit thema is niet het gebrek aan bestaan van technieken om het recht van verzet uit te oefenen, maar het gebrek aan duidelijke communicatie over de verschillende mogelijke vormen van verzet aan de betrokkenen door de verwerkers (het callcenter of de telemarketeer) en de verantwoordelijke voor de verwerking namens wie de communicatie wordt overgebracht (de adverteerder/opdrachtgever).

---

[48] In geval van gebruik van andere middelen dan automatische oproepsystemen, elektronische berichten of faxberichten

[49] Artikel 19 van het voorstel van Europese Dataprotectieverordening van de Europese Commissie van 25 januari 2012, gepubliceerd op http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[50] In Italië besliste de Italiaanse privacycommissie voor de invoering van een opt-in beginsel. In Duitsland, Oostenrijk, Portugal (voor telemarketing aan consumenten), Spanje en Letland geldt ook de vereiste van toestemming voor telemarketing.

78. Hoewel in het wetsontwerp geen melding wordt gemaakt van de situatie waarbij betrokkene wel klant is van de afzender, geldt hierbij het basisregime inzake gegevensbescherming, met name het recht van verzet ten opzichte van alle verwerkingen met het oog op direct marketing (artikel 12 § 1 derde lid WVP[51]). Wellicht kan de memorie van toelichting bij artikel 123 van het wetsontwerp dit voor de volledigheid toelichten.

79. Artikel 123 van het wetsontwerp laat ook een aantal vormen van verzet compleet onbesproken:

- artikel 123 van het wetsontwerp verwijst niet naar artikel 12 WVP. Artikel 14 (b) Richtlijn 95/46/EG waarop dit artikel gebaseerd is bevat nochtans de algemene rechtsbasis in België voor het recht van verzet tegen alle verwerkingen met het oog op direct marketing, ook voor elektronische communicatie[52]. Belangrijk is dat de vorm en de techniek van het recht van verzet hierbij onbepaald is gelaten, en dat de lidstaten ervoor moeten zorgen dat de betrokkenen op de hoogte worden gebracht over het bestaan van dit recht;
- het recht om niet in de telefoongidsen te worden opgenomen (zie hiervoor). Betrokkenen richten zich vandaag vaak tot de uitgevers van telefoongidsen, waarbij de Commissie de betrokkenen vaak dient door te verwijzen naar de operatoren bij gebrek aan medewerking door de uitgevers van telefoongidsen;
- de mogelijkheid om zich te laten inschrijven op tal van private wegduwbestanden en "do not call me" registers waaronder de Robinson Phone van de Belgische direct marketingvereniging (hierna "BDMA") wellicht het meest gekende register is;
- de mogelijkheid voor de betrokkenen om zich in te schrijven op andere lijsten dan deze van BDMA (bvb buitenlandse verenigingen, wegduwbestanden van ondernemingen,…) ;
- het (niet in Belgisch recht omgezette) schrappingsrecht van de betrokkenen uit de gidsen (gelet op het gegeven dat de telefoongidsen vaak worden gebruikt voor telemarketingdoeleinden).

80. Daarnaast roept de inrichting van dit wegduwbestand of "blokkaderegister" ook tal van onbeantwoorde vragen op zoals

- Voert de wetgever een wettelijke verplichting in voor callcenters, telemarketeers, adverteerders en hun opdrachtgevers om gebruik te maken van dit register alvorens

[51] Artikel 12 § 1. (…)
Indien de persoonsgegevens verkregen worden met het oog op direct marketing mag de betrokkene zich kosteloos en zonder enige motivering tegen de voorgenomen verwerking van hem betreffende persoonsgegevens verzetten.
(…)
[52] Zie overwegingen 10 en volgende Richtlijn 2002/58/EG

telemarketingacties op te zetten? Actueel is gebruik van de robinson phone lijst niet verplicht in België (geldt enkel voor de leden van het BDMA), terwijl een belangrijk aantal landen[53] dit reeds wel voorziet. Verplicht gebruik van dit register voor het opzetten van telemarketingactie kan een zware garantie betekenen in geval van klacht van de betrokkene, indien professionelen een belangrijke deel van de bewijslast krijgen omdat zij moeten kunnen aantonen dat zij bij hun marketingacties gebruik maken van het wegduwbestand.

- welke zijn de garanties op een neutraal beheer van het "do not call me register" ? Het is geen toeval dat in tal van lidstaten dit register onder onafhankelijk beheer[54] of zelfs overheidsbeheer[55] wordt geplaatst, waarbij de kosten dienen te worden gedragen door de professionele gebruikers (callcenters of de telemarketeers, adverteerders/opdrachtgevers) via een licentiesysteem[56]. De vraag is of de wetgever eerst deze opties heeft overwogen, zoals de plaatsing van dit register bij het BIPT, de ombudsman telecom of een VZW onder onafhankelijk overheidstoezicht. Structurele onafhankelijkheid ten opzichte van de direct marketingsector biedt ongetwijfeld voordelen qua onafhankelijk beheer en correcte communicatie naar alle verzetsmogelijkheden en hun rechtsbasis (artikel 12 WVP).
- Vraag in geval van privaat beheer door een belangenvereniging van de direct marketing sector is of er een afzonderlijk intern beheer is bij deze organisatie (zgn. "chinese walls") of dat integendeel het register wordt beheerd door personen met een vaste dagtaak in de direct marketing sector. De vraag is ook of de communicatie naar de betrokkenen toe duidelijk of omslachtig is, neutraal of gekleurd, of er een duidelijke aparte website is voor het register,……).
- Hoe zit het met de ingezette middelen en datakwaliteit ? is de beheersdienst enkel elektronisch bereikbaar, of ook via andere kanalen ?
- zal dit nieuwe do not call me register simpelweg overname zijn van het bestaande register "robinson phone", beheerd door de BDMA of wordt er een nieuw bestand gecreëerd met dezelfde of nieuwe kenmerken en beperkingen, is er een overgangsregeling edm..?

---

[53] Denemarken, UK, Hongarije, Noorwegen, Oostenrijk, Zweden, Ierland. Ook in de Angelsaksische landen is dit een gevestigde verplichting voor communicaties aan consumenten (Australië, Canada, Nieuw-Zeeland en Verenigde Staten). Bron : http://ddma.nl/wp-content/uploads/2011/04/TMBlokkaderegisters09.pdf

[54] In Nederland is de stichting Infofilter (www.infofilter.nl) de aangewezen wettelijke beheerder van het bel-meniet-register

[55] In Italië werd het verzetsregister voor telemarketing (http://www.registrodelleopposizioni.it) opgericht door de "*Fondazione Ugo Bordoni*", een instelling die onder het toezicht staat van het Ministerie van Economische ontwikkeling.
In Ijsland beheert het Statistisch Bureau van Ijsland volgens artikel 28(2) van de Ijslandse privacywet dit register. In Denemarken kunnen burgers hun voorkeuren mbt direct marketing officieel laten registreren bij de gemeente in het burgerlijk registratiesysteem (zie sectie 29 punt 3 van de Deense wet inzake het burgerlijk registratiesysteem, te raadplegen op http://www.cpr.dk/cpr/site.aspx?p=194&ArticleID=4326) . Andere landen (bvb Portugal) hebben dan weer een "robinsonlijst" georganiseerd door een belangenvereniging van de direct marketing sector.

[56] Zie de uitleg mbt de tarieven en voorwaarden op https://www.bel-me-niet.nl/faq/3

- welke kenmerken en beperkingen zal dit register hebben? Is er een beperking in de duur qua inschrijving[57] of is de inschrijving "evergreen" ? In het buitenland werd ervoor gekozen om een aantal beperkingen in te bouwen. In het Nederlandse "bel-me-niet-register" geldt de beperking tot bescherming tot marketing tav consumenten (geen "b2b" marketing), en is er een "à la carte" systeem of "deelblokkadesysteem" waarbij consumenten bepaalde opties kunnen aan- of uitvinken volgens hun voorkeur. Dit zoals wanneer men wel nog wil gebeld worden met commerciële, ideële of charitatieve proposities, in plaats van een algehele telefonische blokkade voor dergelijke oproepen laten instellen of deelblokkades voor bepaalde soorten ongevraagde communicatie.
- geldt er een meldingsplicht in geval van een beveiligingsinbreuk op het niveau van dit register ? Indien ja, aan welke instantie (FOD Economie, BIPT, Commissie,…) ?
- welke zijn de maatregelen qua consistentie met andere bronnen op nationaal, europees en internationaal vlak, rekening houdend met het feit dat de wijze van naleving van het recht van verzet in de lidstaten sterk kan verschillen. Wordt de betrokkene doorverwezen naar de opname van zijn gegevens in gelijkaardige bronnen (reactief model waarbij de dienstverlening van de beheerder minimaal is) of neemt de verantwoordelijke professionele beheerder hier zelf initiatief voor (proactief model waarbij de beheerder de betrokkene helpt en eventueel bemiddelt) ?

81. De Commissie wenst zich niet a priori uit te spreken voor of tegen het plaatsen van een "do not call me register" in handen van een private of publiekrechtelijke organisatie (bvb bij BDMA of bij het BIPT), daar zij dit een opportuniteitskeuze acht. Zij acht het wel raadzamer dat de wetgever eerst en vooral aandacht geeft aan de afdoende garanties die elk als officieel erkend verzetsregister dient te bieden inzake neutraal beheer en communicatie, naast vele gelijkaardige alternatieven in binnen- en buitenland voor de betrokkenen.

82. De Commissie verzoekt derhalve om artikel 123 van het wetontwerp (passage mbt de wijziging van artikel 100 § 3 van de wet van 6 april 2010) te herschrijven. Zij verzoekt dat de bepaling *"een register bijgehouden door de Belgian Direct Marketing Association wiens ondernemingsnummer 0452.664.950 is."* wordt geschrapt. Zij verzoekt dat de bepaling wordt aangevuld met "De Koning bepaalt bij besluit, na overleg in de ministerraad en advies van de Commissie, de identiteit van de beheerder, de vereisten en kenmerken voor het beheer van het register, de toegang tot het register, de uitzonderingen op het verplicht gebruik van het register, het bestuur, de middelen en werking van het register, en de maatregelen om de transparantie van het register naar de gebruikers toe te verzekeren. Het register verwerkt de gegevens in conformiteit met de vereisten van de wet van 8 december 1992 en de beheerder rapporteert jaarlijks over haar werking."

[57] Voorheen gold een beperking van drie jaar bij de Robinson Phone list. Deze beperking zou inmiddels zijn afgeschaft.

V. BESLUIT

Het wetsontwerp en het Belgische recht blijven op enkele punten nog achterwege om het Europse dataprotectierecht inzake elektronische communicatie op technisch correcte wijze om te zetten (schrappingsrecht uit telefoongidsen, diverse opties inzake telemarketing, …).

Vooral de complexiteit van de wetgeving inzake elektronische communicatie en de complexe achterliggende techniek vallen op, evenals de complexiteit veroorzaakt door de complementariteit van de WVP ten opzichte van de Wet van 2005 (terminologie en raakvlak in de bevoegdheden van het BIPT en de Commissie inzake beveiliging, meldplicht voor beveiligingsinbreuken en recht van toegang).

Deze complexiteit is van aard om het uitoefenen van de rechten van de betrokkenen te bemoeilijken. Voor de meeste gebruikers is de internetinfrastructuur en zijn de gegevensstromen inzake direct marketing en telefoongidsen grotendeels onzichtbaar. De gebruikerservaring is vaak beperkt en begint en eindigt vaak op het eindpunt (bij de eindapparatuur of het krijgen van een commerciële telefoon). Nochtans zitten de meeste risico's betreffende persoonsgegevens in technologie en infrastructuur en in het gebruiken achter de schermen van de eindapparatuur of in de gebruiken van de professionele wereld.

Het gebrek aan duidelijke en concrete communicatie door de private marktpartijen conform het Europese recht over de gebruikte technieken, de doelstellingen en de mogelijkheden voor de betrokkene verhindert een goed begrip van de meeste gebruikers over de werking en impact van meer complexe gebruiksvormen van verschillende soorten cookies, deep packet inspection, online reclame op basis van surfgedrag, …. Onderzoeken wijzen uit dat respect voor de informatieplicht vandaag collectief wordt verzuimd, terwijl met behulp van deze technieken er vaak sprake is van intensief volgen van surfgedrag over meerdere websites en automatische profilering van gebruikers in bepaalde categorieën door een onbekend aantal partijen. Automatische beslissingen op basis van dergelijke veronderstelde belangstellingen en vermeend gedrag kunnen ertoe leiden dat gebruikers in of buiten het handelsverkeer anders worden behandeld dan anderen of zelfs worden uitgesloten van producten of diensten, terwijl de sector in gebreke blijft om werk te maken van duidelijker basisinformatie en effectieve omzetting van de toestemmingsvereiste.

Duidelijker communicatie over deze complexe elementen aan de betrokkenen, effectieve waarborgen (ondubbelzinnige toestemming voor de meest privacyinvasieve cookies die browsers omzeilen, een kwalitatief opt-out register dat verplicht moet worden gebruikt bij telemarketing,…) en het streven naar meer samenwerking tussen Commissie en BIPT en consistentie in de toepassing

van de WVP en de Wet van 2005 dienen derhalve een duidelijke prioriteit te krijgen in het wetsontwerp en de memorie van toelichting.

OM DEZE REDENEN,

De Commissie voor de bescherming van de persoonlijke levenssfeer brengt een gunstig advies uit over het wetsontwerp, onder voorbehoud van de naleving van de opmerkingen vermeld in dit advies en het besluit.

Gelet op de complexe materie en het belang ervan, blijft de Commissie zich ter beschikking houden bij eventueel verder overleg, herziening en/of uitvoering van de bepalingen van het wetsontwerp.

De Wnd. Administrateur, De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere