I

(Resoluties, aanbevelingen en adviezen)

ADVIEZEN

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING

Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van met name Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)

(2008/C 181/01)

DE EUROPESE TOEZICHTHOUDER VOOR GEGEVENSBESCHERMING,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, en met name op artikel 286,

Gelet op het Handvest van de grondrechten van de Europese Unie, en met name op artikel 8,

Gelet op Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([1]),

Gelet op Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ([2]),

Gelet op Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 inzake de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, en met name op artikel 41 ([3]),

Gezien het verzoek van de Europese Commissie om advies op grond van artikel 28, lid 2, van Verordening (EG) nr. 45/2001 dat op 16 november 2007 is ontvangen,

BRENGT HET VOLGENDE ADVIES UIT:

I. **INLEIDING**

1. De Commissie heeft op 13 november 2007 een voorstel aangenomen voor een richtlijn tot wijziging van met name Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (hierna te noemen „voorstel" of „voorgestelde wijzigingen"). Zoals gebruikelijk wordt Richtlijn 2002/58/EG ook in dit advies de „e-privacy-richtlijn" genoemd.

([1]) PB L 281 van 23.11.1995, blz. 31.
([2]) PB L 201 van 31.7.2002, blz. 37.
([3]) PB L 8 van 12.1.2001, blz. 1.

2. Het voorstel beoogt een versterking van de bescherming van de privacy en de persoonsgegevens van natuurlijke personen in de elektronische-communicatiesector. Dit wordt niet bewerkstelligd door een volledige herziening van de bestaande e-privacy-richtlijn, maar door een aantal ad hoc-wijzigingen van die richtlijn die hoofdzakelijk gericht zijn op de versterking van de beveiligingsvoorschriften en de invoering van betere handhavingsmechanismen.

3. Het voorstel maakt deel uit van een bredere hervorming van de vijf telecommunicatierichtlijnen van de EU (het „telecommunicatiepakket"). Naast de voorstellen tot herziening van het telecommunicatiepakket ([1]) heeft de Commissie tegelijkertijd ook een voorstel aangenomen voor een verordening tot oprichting van de Europese Autoriteit voor de elektronische-communicatiemarkt ([2]).

4. De opmerkingen in dit advies hebben alleen betrekking op de voorgestelde wijzigingen van de e-privacy-richtlijn, tenzij deze wijzigingen stoelen op begrippen of bepalingen uit voorstellen tot herziening van het telecommunicatiepakket. Daarnaast verwijst een aantal opmerkingen in dit advies naar bepalingen van de e-privacy-richtlijn die door het voorstel niet worden gewijzigd.

5. De volgende punten komen in het advies aan bod: *i)* de werkingssfeer van de e-privacy-richtlijn en in het bijzonder de „betrokken diensten" (voorgestelde wijziging van artikel 3, lid 1); *ii)* de kennisgeving van inbreuken op de beveiliging (voorgestelde wijziging waarbij de nieuwe leden 3 en 4 aan artikel 4 worden toegevoegd); *iii)* de bepalingen betreffende cookies, spyware en soortgelijke middelen (voorgestelde wijziging van artikel 5, lid 3); *iv)* gerechtelijke procedures ingeleid door aanbieders van elektronische-communicatiediensten en andere rechtspersonen (voorgestelde wijziging waarbij het nieuwe lid 6 aan artikel 13 wordt toegevoegd, en *v)* de verscherping van de handhavingsmechanismen (voorgestelde wijziging waarbij het nieuwe artikel 15 *bis* wordt ingevoegd).

Raadpleging van de EDPS en brede openbare raadpleging

6. Het voorstel werd op 16 november 2007 door de Commissie aan de EDPS toegezonden. De EDPS vat dit op als een verzoek om advies uit te brengen aan de communautaire instellingen en organen, overeenkomstig artikel 28, lid 2, van Verordening (EG) nr. 45/2001 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (hierna Verordening (EG) nr. 45/2001).

7. De EDPS stelt het op prijs dat de Commissie hem voor de aanneming van het voorstel informeel heeft geraadpleegd over het concept-voorstel omdat dit hem in staat heeft gesteld vooraf een aantal suggesties te doen. Het verheugt de EDPS dat een aantal daarvan in het voorstel zijn overgenomen.

8. De aanneming van dit voorstel werd voorafgegaan door een brede openbare raadpleging, een werkwijze die de EDPS waardeert. De Commissie heeft immers in juni 2006 een openbare raadpleging gelanceerd over haar mededeling betreffende de herziening van het telecommunicatiepakket, waarin zij haar kijk op de situatie uiteenzet en een aantal wijzigingsvoorstellen doet ([3]). De Groep van artikel 29 voor de bescherming van personen in verband met de verwerking van persoonsgegevens („Groep gegevensbescherming"), waarvan de EDPS lid is, heeft van deze gelegenheid gebruik gemaakt om in een op 26 september 2006 ([4]) aangenomen advies haar mening te uiten over deze wijzigingsvoorstellen.

([1]) De voorgestelde wijzigingen van de telecommunicatierichtlijn staan in de volgende voorstellen: *i)* voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van de Richtlijnen 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, 2002/19/EG inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten en 2002/20/EG betreffende de machtiging voor elektronische-communicatienetwerken en -diensten, 13 november 2007, COM(2007) 697 def.; *ii)* voorstel voor een richtlijn van het Europees Parlement en de Raad 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 met betrekking tot consumentenbescherming, 13 november 2007, COM(2007) 698 def.

([2]) Voorstel voor een verordening van het Europees Parlement en de Raad tot oprichting van de Europese Autoriteit voor de elektronische-communicatiemarkt, 13 november 2007, COM(2007) 699 def.

([3]) Mededeling over de herziening van het regelgevingskader van de EU voor elektronische-communicatienetwerken en -diensten (SEC(2006) 816) van 29 juni 2006. Bij deze mededeling gaat een werkdocument van de diensten van de Commissie (COM(2006) 334 def.).

([4]) Advies 8/2006 van 26 september 2006 over de evaluatie van het regelgevingskader voor elektronische communicatie en -diensten, met name de richtlijn e-privacy (WP 09).

Algemeen oordeel van de EDPS

9. In het algemeen genomen staat de EDPS positief tegenover het voorstel. Hij staat volledig achter de bedoeling van de Commissie om met haar voorstel de bescherming van de privacy en de persoonsgegevens van natuurlijke personen in de elektronische-communicatiesector te versterken. De EDPS is in het bijzonder ingenomen met de aanneming van een regeling van verplichte kennisgeving van inbreuken op de beveiliging (wijziging van artikel 4 van de e-privacy-richtlijn waarbij de nieuwe leden 3 en 4 worden toegevoegd). Indien zich beveiligingsinbreuken voordoen, heeft een meldplicht duidelijke voordelen. Zij versterkt de verantwoordingsplicht van organisaties, stimuleert ondernemingen om strenge beveiligingsmaatregelen te nemen en maakt het mogelijk te achterhalen wat de betrouwbaarste technieken voor informatiebescherming zijn. Bovendien geeft zij de betrokkenen de mogelijkheid stappen te ondernemen om zich te beschermen tegen identiteitsdiefstal of andere vormen van misbruik van persoonlijke informatie.

10. De EDPS is ingenomen met andere wijzigingsvoorstellen, zoals de mogelijkheid, voor rechtspersonen met een rechtmatig belang, om diegenen die sommige bepalingen van de e-privacy-richtlijn overtreden, voor de rechter te brengen (wijziging van artikel 13 waarbij het nieuwe lid 6 wordt toegevoegd). Een andere positief element is de versterking van de onderzoeksbevoegdheden van de nationale regelgevende instanties waardoor deze in staat gesteld worden om te toetsen of de gegevensverwerking strookt met de wet en om overtreders te identificeren (toevoeging van artikel 15 *bis*, lid 3. De mogelijkheid om een onwettige verwerking van persoonsgegevens en schendingen van de privacy zo spoedig mogelijk te doen ophouden, is een noodzakelijke maatregel met het oog op de bescherming van de rechten en vrijheden van natuurlijke personen. Het voorgestelde artikel 15 *bis*, lid 2, dat de nationale regelgevende instanties de bevoegdheid verleent om inbreuken te doen ophouden, is dan ook zeer welkom omdat deze instanties daardoor onmiddellijk een einde zullen kunnen maken aan ernstige gevallen van onrechtmatige gegevensverwerking.

11. De in het voorstel gehanteerde aanpak en de meeste wijzigingsvoorstellen stroken met de opvattingen over het toekomstige gegevensbeschermingsbeleid die te vinden zijn in eerdere EDPS-adviezen, zoals het advies over de toepassing van de richtlijn gegevensbescherming ([1]). De aanpak stoelt ondermeer op de overtuiging dat er geen behoefte is aan nieuwe beginselen inzake gegevensbescherming, maar aan specifiekere regels voor het oplossen van de gegevensbeschermingsproblemen die samenhangen met nieuwe technologieën, zoals internet, RFID, enz. Ook is behoefte aan instrumenten om de doeltreffendheid en de handhaving van de gegevensbeschermingswetgeving te verbeteren zodat rechtspersonen een beroep op de rechter kunnen doen voor inbreuken op de regels inzake de gegevensbescherming en de verantwoordelijken voor de verwerking verplicht worden inbreuken op de beveiliging te melden.

12. Hoewel de aanpak in het algemeen positief is, betreurt de EDPS dat het voorstel niet zo ambitieus is als had gekund. Sedert 2003 is uit de toepassing van de e-privacy-richtlijn en uit zorgvuldige analyses van dit vraagstuk namelijk gebleken dat sommige bepalingen verre van helder zijn, met rechtsonzekerheid en nalevingsproblemen als gevolg. Zo is het bijvoorbeeld niet duidelijk of semi-openbare aanbieders van elektronische-communicatiediensten onder de e-privacy-richtlijn vallen, terwijl toch mocht worden gehoopt dat de Commissie de herziening van het telecommunicatiepakket, en in het bijzonder van de e-privacy-richtlijn, aangegrepen zou hebben om een aantal knelpunten aan te pakken. Waar het nieuwe punten betreft, zoals de instelling van een meldplicht voor inbreuken op de beveiliging, beperkt het voorstel zich bovendien tot deeloplossingen. Zo behoren instanties die zeer gevoelige soorten gegevens verwerken, zoals onlinebanken en aanbieders van e-healthdiensten, niet tot de organisaties die verplicht zijn om inbreuken op de beveiliging te melden. De EDPS betreurt deze aanpak.

13. De EDPS hoopt dat de wetgever in de loop van de wetgevingsprocedure met betrekking tot dit voorstel rekening zal houden met de in dit advies vervatte opmerkingen en suggesties om de vraagstukken die de Commissie in haar voorstel over het hoofd heeft gezien, op te lossen.

([1]) Advies van de Europese Toezichthouder voor gegevensbescherming van 25 juli 2007 inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming (PB C 255 van 27.10.2007, blz. 1).

II. ANALYSE VAN HET VOORSTEL

II.1. Werkingssfeer van de e-privacy-richtlijn, in het bijzonder de betrokken diensten

14. Een problematisch aspect van de huidige e-privacy-richtlijn is de werkingssfeer ervan. Het voorstel bevat een aantal nuttige elementen, die hierna onder punt i), worden besproken, om de werkingssfeer van het voorstel, en met name de diensten die onder de richtlijn vallen („betrokken diensten"), te omschrijven en te verduidelijken. Het valt te betreuren dat de voorgestelde wijzigingen niet alle problemen oplossen. Zoals onder punt ii) hierna wordt uiteengezet, beogen de wijzigingen jammer genoeg niet de werkingssfeer van de richtlijn te verruimen tot de elektronische-communicatiediensten in private netwerken.

15. In artikel 3 van de e-privacy-richtlijn worden de betrokken diensten, met andere woorden de diensten waarop de in de richtlijn vervatte voorschriften van toepassing zijn, als volgt omschreven: „Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken".

16. In de e-privacy-richtlijn zijn de betrokken diensten dus de aanbieders van openbare elektronische-communicatiediensten over openbare netwerken („PPECSs"). De definitie van een PPECS staat in artikel 2, onder c), van de kaderrichtlijn ([1]). Openbare communicatienetwerken worden omschreven in artikel 2, punt d), van de kaderrichtlijn ([2]). Voorbeelden van activiteiten van PPECSs zijn de verstrekking van internettoegang, de transmissie van informatie via elektronische netwerken, mobiele en telefoonaansluitingen, enz.

i) *Voorgestelde wijzigingen van artikel 3 van de e-privacy-richtlijn: De „betrokken diensten" omvatten openbare communicatienetwerken die gegevensverzamelings- en identificatiesystemen ondersteunen*

17. In het voorstel wordt artikel 3 van de e-privacy-richtlijn gewijzigd door te verduidelijken dat openbare elektronische-communicatienetwerken *„openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen*" omvatten. In overweging 28 wordt verklaard dat de ontwikkeling van toepassingen waarvoor gegevens, inclusief persoonsgegevens, worden verzameld en waarbij gebruik wordt gemaakt van radiofrequenties, zoals RFID-systemen onder de e-privacy-richtlijn moeten vallen wanneer zij aan openbare elektronische-communicatienetwerken zijn gekoppeld of gebruik maken van elektronische-communicatiediensten als basisinfrastructuur.

18. De EDPS is van mening dat deze bepaling positief is omdat zij verduidelijkt dat een aantal RFID-toepassingen onder de e-privacy-richtlijn vallen, wat tevoren niet even duidelijk was, en zo misverstanden en onjuiste interpretaties van de wet definitief uit de wereld helpt.

19. Op basis van het huidige artikel 3 van de e-privacy-richtlijn vallen sommige RFID-toepassingen al onder de richtlijn. Dit heeft verschillende elkaar versterkende redenen. In de eerste plaats vallen RFID-toepassingen onder de definitie van elektronische-communicatiediensten. In de tweede plaats worden zij verstrekt via een elektronische-communicatienetwerk voor zover de toepassingen gebaseerd

([1]) Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (PB L 108 van 24.4.2002, blz. 33). Deze kaderrichtlijn omschrijft wat moet worden verstaan onder een elektronische-communicatiedienst, namelijk: i) „elektronische-communicatiedienst": een gewoonlijk tegen vergoeding aangeboden dienst die bestaat in het overbrengen van signalen via netwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken. ii) diensten die met behulp van elektronische-communicatienetwerken en -diensten overgebrachte inhoud leveren zijn uitgesloten van de definitie van elektronische-communicatiediensten. iii) het aanbieden van diensten: het bouwen, exploiteren, leiden of beschikbaar stellen van een netwerk. iv) elektronische-communicatiediensten omvatten niet de diensten van de informatiemaatschappij zoals omschreven in de richtlijn e-handel als dienst(en) die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten verleend worden.

([2]) „Openbaar communicatienetwerk": een elektronische-communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om openbare elektronische-communicatiediensten aan te bieden.

zijn op een transmissiesysteem dat draadloos signalen overbrengt. Tenslotte kan het netwerk openbaar of privaat zijn. Indien het openbaar is, worden de RFID-toepassingen beschouwd als „betrokken diensten" en vallen zij dus onder de e-privacy-richtlijn. De voorgestelde wijziging zal echter iedere resterende twijfel daarover wegnemen en dus meer rechtszekerheid bieden.

20. Zoals in een eerder advies van de EDPS over RFID ([1]) reeds is gesteld, sluit deze bepaling niet uit dat met betrekking tot RFID aanvullende wetgevingsinstrumenten vereist kunnen zijn. Deze maatregelen moeten echter in een ander kader en niet als onderdeel van dit voorstel worden genomen.

ii) *Opneming van elektronische-communicatiediensten in private en semi-private netwerken*

21. Hoewel de EDPS de bovenstaande verduidelijking toejuicht, betreurt hij dat de vervaging van de grenzen tussen openbare en private netwerken in het voorstel niet aan bod komt. Tevens betreurt hij dat de definitie van de „betrokken diensten" die onder de e-privacy-richtlijn vallen niet is verruimd tot private netwerken. In zijn huidige vorm is artikel 3, lid 1, van de e-privacy-richtlijn alleen van toepassing op *elektronische-communicatiediensten over openbare communicatienetwerken*.

22. De EDPS merkt op dat de diensten hoe langer hoe meer een mix van private en openbare diensten worden. Men denke bijvoorbeeld aan universiteiten die duizenden studenten toegang verlenen tot internet en e-mail. Het is duidelijk dat semi-openbare (of semi-private) netwerken de persoonlijke levenssfeer van natuurlijke personen kunnen schaden en zij moeten dan ook onderworpen zijn aan dezelfde regels als de zuiver openbare netwerken. Private netwerken, bijvoorbeeld van werkgevers die hun werknemers internettoegang verstrekken, hotel- of woningeigenaren die hun gasten, respectievelijk huurders, telefoon en e-mail ter beschikking stellen, en internetcafés hebben een invloed op de bescherming van de gegevens en de persoonlijke levenssfeer van de gebruikers en zouden dus onder de e-privacy-richtlijn moeten vallen.

23. In de jurisprudentie van een aantal lidstaten zijn aan in private netwerken verstrekte elektronische-communicatiediensten trouwens al dezelfde verplichtingen opgelegd als aan openbare netwerken ([2]). Ook de Duitse gegevensbeschermingsautoriteiten hebben geoordeeld dat het aanbieden van privé e-mailgebruik in een bedrijf volgens de Duitse wetgeving tot gevolg kan hebben dat het bedrijf wordt beschouwd als aanbieder van openbare telecommunicatiediensten en derhalve onder de e-privacy-richtlijn valt.

24. Kortom, het toenemende belang van de gemengde (privaat/openbaar) en private netwerken in het leven van alledag en het toenemende gevaar dat de persoonsgegevens en de privacy daardoor lopen, rechtvaardigt dat deze diensten aan dezelfde regels worden onderworpen als de openbare elektronische-communicatienetwerken. Daarom is de EDPS, evenals de Groep van artikel 29 ([3]), van mening dat de richtlijn moet worden gewijzigd opdat de werkingssfeer zodanig wordt verruimd dat ook deze private diensten ertoe behoren.

II.2. **Kennisgeving van inbreuken op de beveiliging: wijziging van artikel 4**

25. Artikel 4 van de e-privacy-richtlijn wordt gewijzigd door de toevoeging van twee nieuwe leden (3 en 4) waardoor de verplichting wordt opgelegd om inbreuken op de beveiliging te melden. Overeenkomstig artikel 4, lid 3, zijn PPECSs namelijk verplicht om de nationale regelgevende instantie onverwijld in kennis te stellen van iedere inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens, verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van openbare communicatiediensten (samen „de compromittering van gegevens"). Tevens zijn PPECSs verplicht hun abonnees in kennis te stellen.

([1]) Advies van 20 december 2007 over de Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende radiofrequentie-identificatie (RFID) in Europa: maatregelen met het oog op een beleidskader COM(2007) 96.

([2]) Zo heeft het hof van beroep van Parijs in haar arrest *BNP Paribas tegen World Press Online* van 4 februari 2005 geoordeeld dat er geen onderscheid is tussen aanbieders van internetdiensten die internettoegang verstrekken op commerciële basis en werkgevers die hun personeel toegang tot internet verlenen.

([3]) Advies 8/2006 van 26 september 2006 over de evaluatie van het regelgevingskader voor elektronische communicatie en -diensten, met name de richtlijn e-privacy (WP 09).

Voordelen van deze verplichting

26. De EDPS is ingenomen met de bepalingen (artikel 4, leden 3 en 4) waardoor een verplichte kennisgeving van inbreuken op de beveiliging wordt ingevoerd. De kennisgeving van beveiligingsinbreuken heeft positieve effecten voor de bescherming van persoonsgegevens en van de privacy, wat al is gebleken in de Verenigde Staten, waar op het niveau van de staten reeds een aantal jaren wetgeving ter zake bestaat.

27. In de eerste plaats verscherpt wetgeving inzake de kennisgeving van inbreuken op de beveiliging de aansprakelijkheid van de PPECSs voor de gecompromitteerde informatie. In het kader van het beleid inzake gegevensbescherming en bescherming van de privacy houdt de verantwoordingsplicht in dat alle organisaties verantwoordelijk zijn voor de informatie die aan hun zorg en controle is toevertrouwd. De verplichte kennisgeving komt neer op de bevestiging van het feit enerzijds dat de gecompromitteerde gegevens onder de verantwoordelijkheid van de betrokken organisatie vallen en anderzijds dat het aan deze organisatie is om ten aanzien van de gegevens het nodige te doen.

28. In de tweede plaats is gebleken dat de verplichte kennisgeving van beveiligingsinbreuken gegevensverwerkende organisaties ertoe beweegt om te investeren in beveiliging. Het loutere feit dat beveiligingsinbreuken bekend moeten worden gemaakt, motiveert organisaties om strengere beveiligingsnormen te hanteren om persoonsgegevens te beschermen en inbreuken te voorkomen. Voorts helpen de meldingen van beveiligingsinbreuken bij het onderkennen en uitvoeren van betrouwbare statistische analyses omtrent de doeltreffendste beveiligingsoplossingen en -systemen. Er is lang een gebrek geweest aan harde gegevens over inbreuken op de informatiebeveiliging en de beste technologieën voor informatiebescherming. De verplichte kennisgeving van inbreuken op de beveiliging zal dit probleem wellicht oplossen, zoals in de Verenigde Staten is gebeurd met de wettelijke meldplicht inzake beveiligingsinbreuken. Immers, de kennisgevingen verstrekken informatie over de technologieën die het gemakkelijkst aanleiding geven tot inbreuken ([1]).

29. Tenslotte maakt de kennisgeving van beveiligingsinbreuken mensen bewust van het gevaar dat zij lopen wanneer hun persoonsgegevens gecompromitteerd raken en stelt zij hen in staat de nodige maatregelen te nemen om het risico te beperken. Indien bankgegevens bijvoorbeeld gecompromitteerd zijn, kan de geïnformeerde klant besluiten de gegevens die toegang verlenen tot zijn bankrekening te wijzigen om te beletten dat iemand ze zich toeeigent en op een onwettige manier gebruikt (meestal „identiteitsdiefstal" genoemd). De kennisgevingsverplichting reduceert dus de kans dat iemand het slachtoffer van identiteitsdiefstal wordt en kan de slachtoffers ook helpen maatregelen te nemen om het probleem de wereld uit te helpen.

Leemten van de voorgestelde wijziging

30. Hoewel de EDPS ingenomen is met de in artikel 4, leden 3 en 4, vervatte regeling voor de kennisgeving van inbreuken, had hij graag een ruimere toepassingssfeer gezien waartoe ook de aanbieders van diensten van de informatiemaatschappij zouden behoren. Dit zou betekenen dat ook onlinebanken, onlinebedrijven en aanbieders van e-healthdiensten onder de wet zouden vallen ([2]).

31. De redenen die een meldplicht inzake beveiligingsinbreuken voor aanbieders van elektronischecommunicatiediensten (PPECSs) rechtvaardigen, gelden ook voor andere organisaties die enorme hoeveelheden persoonsgegevens verwerken waarvan de openbaarmaking bijzonder schadelijk kan zijn voor de betrokkenen. Het gaat ondermeer om onlinebanken, gegevensmakelaars en andere aanbieders van onlinediensten, bijvoorbeeld die welke gevoelige gegevens verwerken (zoals gezondheidsgegevens, politieke overtuigingen, enz.). De compromittering van door onlinebanken en onlinebedrijven beheerde informatie, die niet alleen rekeningnummers maar ook kredietkaartgegevens kan omvatten, kan aanleiding geven tot identiteitsdiefstal. In dat geval is het essentieel dat de betrokkenen worden ingelicht opdat zij de nodige maatregelen kunnen nemen. In het geval van e-healthdiensten zal de compromittering van gevoelige informatie de betrokkene zo niet financiële schade dan toch niet-economische schade toebrengen.

([1]) Zie het rapport „*Security Economics and the Internal Market*", dat in opdracht van ENISA is opgesteld door Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. Het rapport is te vinden op: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.

([2]) De aanbieders van diensten van de informatiemaatschappij zijn in de richtlijn e-handel gedefinieerd als dienst(en) die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten verleend worden.

32. Als de meldplicht ruimer wordt toegepast, zullen de bovengenoemde positieve effecten bovendien niet beperkt blijven tot een activiteitensector, namelijk die van de aanbieders van openbare elektronischecommunicatiediensten, maar voelbaar zijn voor de diensten van de informatiemaatschappij in het algemeen. Het opleggen van een meldplicht inzake beveiligingsinbreuken aan diensten van de informatiemaatschappij zoals onlinebanken, zal immers niet alleen de verantwoordingsplicht van deze diensten vergroten, maar deze ook motiveren om hun beveiligingsmaatregelen te verscherpen en aldus toekomstige inbreuken te voorkomen.

33. Er zijn al gevallen waarin de e-privacy-richtlijn van toepassing is op andere diensten dan PPECSs, zoals artikel 5 betreffende de vertrouwelijkheid van informatie en artikel 13 betreffende spam. Dit wijst erop dat de wetgever in het verleden al zeer terecht heeft beslist om de werkingssfeer van sommige bepalingen van de e-privacy-richtlijn uit te breiden omdat hij dit passend en nodig achtte. De EDPS hoopt dat de wetgever ook in het huidige geval niet zal aarzelen om even verstandig en flexibel te werk te gaan en de werkingssfeer van artikel 4 zal uitbreiden tot aanbieders van diensten van de informatiemaatschappij. Daartoe zou het volstaan in artikel 4, lid 3, de aanbieders van diensten van de informatiemaatschappij te vermelden: „In het geval van een inbreuk op de beveiliging die resulteert in een accidentele of (…) stelt de aanbieder van de openbare elektronische-communicatiediensten en de aanbieder van diensten van de informatiemaatschappij (…) de betrokken abonnee en de nationale regelgevende instantie daarvan onverwijld in kennis".

34. De EDPS ziet deze verplichting en het opleggen ervan aan de PPECSs en de aanbieders van diensten van de informatiemaatschappij als eerste stap in een ontwikkeling die er uiteindelijk toe kan leiden dat de verplichting aan alle verantwoordelijken voor de verwerking in het algemeen wordt opgelegd.

Vaststelling van het specifieke rechtskader voor inbreuken op de beveiliging via comitologie

35. Dit voorstel gaat niet in op een aantal vraagstukken in verband met de verplichte kennisgeving van inbreuken op de beveiliging, zoals de omstandigheden van de kennisgeving, het formaat en de procedures. In artikel 4, lid 4, van het voorstel wordt de vaststelling van maatregelen ter zake overgelaten aan een „comitologiecomité" ([1]), met name het Comité voor communicatie dat is ingesteld bij artikel 22 van de kaderrichtlijn, overeenkomstig het besluit van de Raad van 28 juni 1999. Meer bepaald worden deze maatregelen vastgesteld overeenkomstig artikel 5 van het besluit van de Raad van 28 juni 1999, dat regels bevat voor de regelgevingsprocedure met betrekking tot „maatregelen van algemene strekking die ten doel hebben essentiële onderdelen van een basisbesluit toe te passen".

36. De EDPS is niet gekant tegen de keuze om al deze kwesties in de uitvoeringwetgeving te regelen. De aanneming van wetgeving via de comitologieprocedure zal de wetgevingsprocedure wellicht verkorten. De comitologie zal ook de harmonisatie ten goede komen, wat zeker moet worden nagestreefd.

37. Gezien het grote aantal vraagstukken dat in de uitvoeringsmaatregelen moet worden geregeld en het belang ervan (zie hierna), lijkt het beter om al deze kwesties samen in een wetgevend instrument te regelen, dan ze gedeeltelijk in de e-privacy-richtlijn en gedeeltelijk in de uitvoeringsmaatregelen te behandelen. Daarom moet de keuze van de Commissie worden toegejuicht om deze aangelegenheden te regelen in de uitvoeringsmaatregelen, na raadpleging van de EDPS en hopelijk van andere belanghebbenden (zie hierna).

In de uitvoeringsmaatregelen te regelen vraagstukken

38. Het belang van de uitvoeringsmaatregelen blijkt duidelijk wanneer de vraagstukken die daarin moeten worden geregeld enigszins in detail worden bekeken. In de uitvoeringsmaatregelen kunnen immers de normen voor de kennisgeving worden vastgesteld. Zo zal daarin bijvoorbeeld worden bepaald wanneer sprake is van een inbreuk op de beveiliging, onder welke voorwaarden de kennisgeving aan de betrokkenen en aan de autoriteiten moet geschieden en wat de termijnen zijn voor het bericht en de kennisgeving.

([1]) De wetgevingsprocedures in de EG omvatten comités die zijn samengesteld uit vertegenwoordigers van de regeringen van de lidstaten op ambtenaren niveau.

39. De EDPS is van mening dat de e-privacy-richtlijn, en in het bijzonder artikel 4, geen uitzonderingen op de kennisgevingsverplichting mogen bevatten. Hij is dan ook ingenomen met de aanpak van de Commissie in artikel 4, waarbij een kennisgevingsplicht zonder enige uitzondering wordt ingesteld, maar wel de mogelijkheid wordt geboden dit en andere vraagstukken te regelen in de uitvoeringswetgeving. Hoewel de EDPS de argumenten kent die het toestaan van bepaalde uitzonderingen zouden kunnen rechtvaardigen, is hij er toch voorstander van dat deze en andere kwesties met zorg worden geregeld in de uitvoeringswetgeving, na een grondig en algemeen debat over alle problemen in dit verband. Zoals reeds is vermeld, vereist de complexiteit van de vraagstukken in verband met de verplichte kennisgeving van beveiligingsinbreuken, waaronder de vraag of het aangewezen is uitzonderingen toe te staan, dat deze op een uniforme wijze worden aangepakt, dat wil zeggen in een wetgevingsinstrument dat uitsluitend op dit onderwerp betrekking heeft.

Raadpleging van de EDPS en de noodzaak van een ruimere raadpleging

40. Gezien de grote invloed die de uitvoeringsmaatregelen zullen hebben op de bescherming van de persoonsgegevens van natuurlijke personen, is het belangrijk dat de Commissie, alvorens zij deze maatregelen aanneemt, een behoorlijke raadpleging organiseert. Daarom is de EDPS ingenomen met artikel 4, lid 4, van het voorstel, waarin uitdrukkelijk wordt bepaald dat de Commissie de uitvoeringsmaatregelen vaststelt na raadpleging van de Europese Toezichthouder voor gegevensbescherming. Deze maatregelen zullen niet alleen betrekking hebben op de bescherming van persoonsgegevens en privacy van natuurlijke personen, maar daarop ook een grote invloed uitoefenen. Daarom is het belangrijk dat de EDPS overeenkomstig artikel 41 van Verordening (EG) nr. 45/2001 om advies wordt verzocht.

41. Het kan wenselijk zijn, naast de raadpleging van de EDPS, ook te bepalen dat de concept-uitvoeringsmaatregelen het voorwerp moeten uitmaken van een openbare raadpleging die dient om advies in te winnen en de uitwisseling van ervaringen en beste praktijken te stimuleren. Dit zal niet alleen het bedrijfsleven maar ook andere belanghebbenden, inclusief de gegevensbeschermingsautoriteiten en de Groep van artikel 29, een geschikt kanaal bieden om hun mening kenbaar te maken. Een openbare raadpleging is des te noodzakelijker omdat het Europees Parlement in de procedure voor de aanneming van wetgeving via de comitologieprocedure een beperkte rol speelt.

42. De EDPS neemt er nota van dat de Commissie overeenkomstig artikel 4, lid 4, van het voorstel ook de Europese Autoriteit voor de elektronische-communicatiemarkt zal raadplegen voor zij uitvoeringsmaatregelen vaststelt. In dit verband waardeert de EDPS het beginsel dat de Europese Autoriteit voor de elektronische-communicatiemarkt wordt geraadpleegd als bewaarder van de ervaring en de kennis betreffende netwerk- en informatiebeveiliging van ENISA. Het lijkt wenselijk bij wijze van tussentijdse oplossing in de voorgestelde wijziging (artikel 4, lid 4) te bepalen dat ENISA wordt geraadpleegd totdat de Europese Autoriteit voor de elektronische-communicatiemarkt is opgericht.

II.3. **Bepaling betreffende cookies, spyware en soortgelijke software: wijziging van artikel 5, lid 3**

43. Artikel 5, lid 3, van de e-privacy-richtlijn heeft betrekking op technologieën die het mogelijk maken via elektronische-communciatienetwerken toegang te verkrijgen tot informatie en informatie op te slaan in de eindapparatuur van de gebruiker. Een voorbeeld van de toepassing van artikel 5, lid 3, is het gebruik van cookies ([1]). Andere voorbeelden zijn het gebruik van technologieën zoals spyware (verborgen spionageprogramma's) en Trojaanse paarden (programma's die verborgen zitten in berichten en andere onschuldig ogende software). Het doel van deze technieken is zeer uiteenlopend. Sommige zijn volmaakt onschuldig of zelfs nuttig voor de gebruiker, terwijl andere duidelijk zeer schadelijk en bedreigend zijn.

([1]) Cookies worden om diverse redenen door ISSPs (websites) op de eindapparatuur van de gebruiker geplaatst, ondermeer het herkennen van de bezoeker wanneer deze aanbieders van een website bezoekt. Concreet houdt dit in dat, wanneer een website een cookie naar een internetgebruiker stuurt, aan de computer van de betrokkene een uniek nummer wordt toegekend (de computer die cookies van website A ontvangt, wordt dan „de computer waarop cookie 111 staat"). De website houdt dit nummer bij als referentienummer. Indien de gebruiker van de computer waarop cookie 111 is geplaatst het cookiebestand niet verwijdert, zal de website zijn computer bij een volgend bezoek van de website identificeren als de computer waarop cookie 111 staat. De website leidt daaruit automatisch af dat deze computer de website herhaaldelijk heeft bezocht. Het mechanisme waardoor een website een bezoeker als terugkerende bezoeker kan herkennen is eenvoudig. Wanneer een computer met cookies, zoals cookie 111, een website bezoekt die bij een vorig bezoek een cookie heeft achtergelaten, zoekt deze website de harde schijf van de gebruiker af naar het nummer van het cookiebestand. Indien de browser van de gebruiker een cookiebestand vindt dat overeenkomt met het door de website bijgehouden referentienummer, informeert deze de website dat cookie 111 op de computer staat.

44. Artikel 5, lid 3, van de e-privacy-richtlijn bevat de voorwaarden voor het verkrijgen van toegang tot en het opslaan van informatie, op de eindapparatuur van de gebruiker, met name door middel van de bovengenoemde technologieën. Meer bepaald moeten internetgebruikers overeenkomstig artikel 5, lid 3, *i)* worden voorzien van duidelijke en volledige informatie, onder andere over de doeleinden van de verwerking, overeenkomstig Richtlijn 95/46/EG, en *ii)* het recht aangeboden krijgen om een dergelijke verwerking te weigeren, d.w.z. om af te zien van de verwerking van informatie die van hun eindapparatuur is gehaald.

Voordelen van de voorgestelde wijziging

45. De werkingssfeer van het huidige artikel 5, lid 3, van de e-privacy-richtlijn is beperkt tot situaties waarin de toegang tot informatie en de opslag van informatie op de eindapparatuur van de gebruiker door middel van *elektronische-communciatienetwerken* geschiedt. Dit omvat het bovengenoemde geval van gebruik van cookies en andere technologieën zoals spyware die via elektronische-communicatienetwerken worden geplaatst. Het is echter helemaal niet duidelijk of artikel 5, lid 3, van toepassing is in situaties waarin dergelijke technologieën (cookies/spyware en dergelijke) via software op externe dataopslagmedia of via downloads op de eindapparatuur van de gebruiker terechtkomen. Aangezien er, ongeacht het communicatiekanaal, een gevaar voor de privacy bestaat, valt het te betreuren dat artikel 5, lid 3, op slechts een communicatiekanaal van toepassing is.

46. De EDPS is dan ook ingenomen met de wijziging van artikel 5, lid 3, die de werkingssfeer ervan *de facto* verruimt door de vermelding van „elektronische-communicatienetwerken" te schrappen. Het gewijzigde artikel 5, lid 3, omvat immers zowel de gevallen van toegang tot en opslag van informatie op de eindapparatuur van de gebruiker via elektronische-communicatienetwerken als via andere externe media voor gegevensopslag, zoals CD's, CD-ROM's of USB-sticks.

Technische opslag ter vergemakkelijking van de verzending

47. Het wijzigingsvoorstel laat de laatste zin van artikel 5, lid 3, van de e-privacy-richtlijn ongewijzigd. Daarin wordt bepaald dat de voorschriften van de eerste zin van artikel 5, lid 3, „geen beletsel [vormen] voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering of vergemakkelijking van de verzending van een communicatie over een elektronische-communicatienetwerk, of, indien strikt noodzakelijk, voor de levering van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij (…)". De dwingende voorschriften van de eerste zin van artikel 5, lid 3, (de verplichting om informatie te verstrekken en het recht te bieden om te weigeren) zijn niet van toepassing wanneer de toegang tot de eindapparatuur van de gebruiker of de opslag van de informatie uitsluitend gericht is op de *vergemakkelijking* van de verzending van een communicatie of strikt noodzakelijk is voor de levering van een door de gebruiker gevraagde dienst van de informatiemaatschappij.

48. In de richtlijn wordt niet gedefinieerd wanneer toegang tot of opslag van informatie uitsluitend ten doel heeft de verzending te vergemakkelijken of informatie te verstrekken. Een situatie die zeker onder deze uitzondering valt, is de totstandbrenging van een internetverbinding omdat een internetverbinding nodig is om een IP-adres ([1]) te verkrijgen. De computer van de eindgebruiker wordt verzocht aan de aanbieder van internettoegang bepaalde gegevens over zichzelf te verstrekken en krijgt dan van de aanbieder een IP-adres. In dit geval wordt informatie die in de eindapparatuur van de eindgebruiker is opgeslagen, doorgegeven aan de aanbieder van internettoegang om de gebruiker toegang te verlenen tot internet. Omdat deze informatie nodig is om de dienst te verlenen, is de aanbieder van internettoegang vrijgesteld van zowel de verplichting om mee te delen dat de informatie wordt verzameld als van de verplichting om het recht aan te bieden om te weigeren.

49. Indien een op het internet aangesloten gebruiker een bepaalde website wenst te bezoeken, moet hij een verzoek richten tot de server die de website host. De server reageert als hij weet waarheen hij de informatie moet sturen, dat wil zeggen als hij het IP-adres kent. Gezien de wijze waarop dit adres is opgeslagen, moet de website die de internetgebruiker wenst te bezoeken toegang hebben tot informatie die zich op zijn eindapparatuur bevindt. Deze toegang valt duidelijk ook onder de uitzondering. Het lijkt inderdaad passend dat de voorschriften van artikel 5, lid 3, niet van toepassing zijn op deze gevallen.

([1]) Een IP-adres (*Internet Protocol address*) is een uniek adres dat sommige elektronische apparaten gebruiken om elkaar te identificeren en met elkaar te communiceren in een computernetwerk dat gebruik maakt van de „*Internet Protocol standard*" (IP), of, eenvoudig gezegd, een computeradres. Alle apparaten die deel uitmaken van een netwerk, waaronder routers, switchen, computers, infrastructuurservers (bv. NTP, DNS, DHCP, SNMP, enz.), printers, internet-faxapparatuur en sommige telefoons, kunnen hun eigen adres hebben dat uniek is binnen dat specifieke netwerk. Sommige IP-adressen zijn bedoeld om uniek te zijn in het wereldwijde internet, terwijl andere alleen uniek moeten zijn binnen een bedrijf.

50. De EDPS acht het passend dat aanbieders in situaties zoals de bovenstaande, waarin de technische opslag of de toegang tot de eindapparatuur van de gebruiker *noodzakelijk* is voor het uitsluitende doel de verzending van een communicatie over een elektronische-communicatienetwerk uit te voeren, worden vrijgesteld van de informatieplicht en het aanbieden van het weigeringsrecht. Hetzelfde geldt wanneer de technische opslag of de toegang strikt noodzakelijk is voor de levering van een dienst van de informatiemaatschappij. Indien de technische opslag of de toegang louter ten doel heeft de verzending van een communicatie te *vergemakkelijken*, acht de EDPS het echter niet nodig vrijstelling van de informatieplicht en het verplichte aanbieden van het weigeringsrecht te verlenen. Op basis van de laatste zin van het artikel zou de betrokkene bijvoorbeeld geen informatie krijgen en geen weigeringsrecht hebben wanneer een cookie zijn voorkeurtaal of locatie (bv. België, China) registreert omdat dit type cookies kan worden voorgesteld als een manier om de verzending van een communicatie te vergemakkelijken. Het is de EDPS bekend dat het voor de betrokkenen in de praktijk mogelijk is de opslag van cookies op het niveau van de software te weigeren of te beperken. Dit is echter niet duidelijk genoeg vastgelegd in een wettelijke bepaling die de betrokkene in de bovengenoemde situatie formeel in staat stelt zijn rechten te verdedigen.

51. Daarom stelt de EDPS een kleine wijziging van het laatste gedeelte van artikel 5, lid 3, voor, namelijk de schrapping van het woord „vergemakkelijking" in de laatste zin: „Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering of vergemakkelijking van de verzending van een communicatie over een elektronische-communicatienetwerk, of, indien strikt noodzakelijk, voor de levering van een (…) dienst van de informatiemaatschappij".

II.4. **Gerechtelijke procedures ingeleid door PPECSs en rechtspersonen: aanvulling van artikel 13, lid 6**

52. Artikel 13, lid 6, van het voorstel voorziet in civielrechtelijke rechtsmiddelen voor natuurlijke of rechtspersonen die een rechtmatig belang hebben, en in het bijzonder de aanbieders van elektronische-communicatiediensten die een rechtmatig ondernemingsbelang hebben bij de bestrijding van inbreuken op artikel 13 van de e-privacy-richtlijn. Dit artikel heeft betrekking op ongevraagde commerciële communicatie.

53. De voorgestelde wijziging zal aanbieders van internettoegang bijvoorbeeld in staat stellen om spammers aan te pakken wegens misbruik van hun netwerk en degenen die zenderadressen vervalsen of servers kraken om ze als „*spam relay*" te gebruiken, enz., voor de rechter te brengen.

54. In de e-privacy-richtlijn was het niet duidelijk of PPECSs het recht hadden om een rechtsvordering in te stellen tegen spammers, en PPECSs hebben maar uiterst zelden een zaak aangespannen wegens inbreuk op artikel 13, zoals omgezet in de nationale wetgeving ([1]). Door aanbieders van elektronische-communicatiediensten het recht te verlenen hun ondernemingsbelangen te verdedigen, bevestigt het voorstel dat de e-privacy-richtlijn ten doel heeft niet alleen de individuele abonnees maar ook de aanbieders van elektronische-communicatiediensten te beschermen.

55. De EDPS is tevreden dat het voorstel aanbieders van elektronische-communicatiediensten met een rechtmatig ondernemingsbelang de mogelijkheid biedt een vordering in te stellen tegen spammers. Behalve in uitzonderlijke omstandigheden hebben individuele abonnees noch het geld noch voldoende reden om dit soort rechtszaken te beginnen. Aanbieders van internettoegang en andere PPECSs daarentegen beschikken over de financiële draagkracht en de technologische capaciteit om spamcampagnes te onderzoeken en de daders te identificeren en het lijkt dan ook niet meer dan billijk dat zij het recht hebben om gerechtelijke stappen te ondernemen tegen spammers.

56. De EDPS waardeert de voorgestelde wijziging in het bijzonder omdat zij het mogelijk maakt dat ook consumentenverenigingen en vakbonden die de belangen van „gespamde" consumenten vertegenwoordigen in hun naam de zaak voor de rechter brengen. Zoals reeds gezegd, volstaat de schade die individuele betrokkenen ten gevolge van spam ondervinden meestal niet om hen ertoe te bewegen een rechtszaak te beginnen. De EDPS heeft deze maatregel in verband met inbreuken op de privacy en de gegevensbescherming in het algemeen al voorgesteld in zijn advies inzake de follow-up van het

([1]) Zie bijvoorbeeld de zaak Microsoft corporation vs Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming ([1]). De EDPS is van mening dat het voorstel verder had kunnen gaan en collectieve processen („class actions") had kunnen voorstellen, zodat groepen burgers in gegevensbeschermingszaken gezamenlijk kunnen procederen. In het geval van spam, waarbij een grote groep personen spam ontvangt, bestaat de mogelijkheid dat groepen personen de handen in elkaar slaan en gezamenlijk een collectief proces aanspannen tegen de spammers.

57. De EDPS betreurt in het bijzonder dat het voorstel rechtspersonen in hun mogelijkheid beperkt om gerechtelijke stappen te ondernemen bij overtreding van artikel 13 van de richtlijn, dat wil zeggen wanneer een inbreuk wordt gepleegd op de bepaling inzake ongevraagde elektronische communicatie. Op grond van de voorgestelde wijziging kunnen rechtspersonen niet naar de rechter stappen voor inbreuken op de andere bepalingen van de e-privacy-richtlijn. De huidige bepaling laat bijvoorbeeld niet toe dat een rechtspersoon zoals een consumentenvereniging gerechtelijke stappen onderneemt tegen een aanbieder van internettoegang die persoonsgegevens van miljoenen gebruikers heeft bekendgemaakt. De handhaving van de e-privacy-richtlijn in haar geheel (dus niet alleen van een specifiek artikel) zou er sterk op vooruitgaan als artikel 13, lid 6, algemener werd geformuleerd om rechtspersonen in staat te stellen inbreuken op om het even welke bepaling van de e-privacy-richtlijn bij de rechter aanhangig te maken.

58. Daartoe stelt de EDPS voor artikel 13, lid 6, om te vormen tot een afzonderlijk artikel (artikel 14). Tevens dient de formulering van artikel 13, lid 6, enigszins te worden gewijzigd in die zin dat „overeenkomstig dit artikel" wordt vervangen door „overeenkomstig deze richtlijn".

II.5. **Versterking van de handhavingsmechanismen: toevoeging van artikel 15 *bis***

59. De e-privacy-richtlijn bevat geen uitdrukkelijke handhavingsmechanismen. In plaats daarvan wordt verwezen naar het handhavingsgedeelte van de richtlijn gegevensbescherming ([2]). De EDPS is ingenomen met het voorgestelde nieuwe artikel 15 *bis*, waarin uitdrukkelijk aandacht wordt besteed aan de handhavingsproblematiek in het kader van de richtlijn.

60. In de eerste plaats merkt de EDPS op dat een effectief handhavingsbeleid op dit gebied veronderstelt, zoals wordt bepaald in het nieuwe artikel 15 *bis*, lid 3, dat de nationale instanties over onderzoeksbevoegdheden beschikken om de nodige informatie te verzamelen. Het bewijs van een overtreding van de e-privacy-richtlijn zal vaak in elektronische vorm zijn en kan opgeslagen zijn op verschillende computers en apparaten of netwerken. In dit verband is het belangrijk dat de handhavingsinstanties een huiszoekingsbevel kunnen verkrijgen dat hun de bevoegdheid verleent tot het betreden en doorzoeken van plaatsen en het in beslag nemen van voorwerpen.

61. In de tweede plaats is de EDPS bijzonder ingenomen met de voorgestelde wijziging, te weten artikel 15 *bis*, lid 2, waarin wordt bepaald dat de nationale regelgevende instanties de bevoegdheid moeten hebben inbreuken te doen ophouden en over de nodige onderzoeksbevoegdheden en -middelen moeten beschikken. De nationale regelgevende instanties, inclusief de nationale autoriteiten voor gegevensbescherming, dienen over de bevoegdheid te beschikken om overtreders te bevelen een einde te maken aan een activiteit die in strijd is met de e-privacy-richtlijn. Een bevel of bevoegdheid om een inbreuk te doen ophouden is een nuttig instrument wanneer de handelingen waardoor de rechten van personen worden geschonden, gaande zijn. Bevelen zullen zeer nuttig zijn om de inbreuken op de e-privacy-richtlijn te doen ophouden, zoals bijvoorbeeld de overtreding van artikel 13 betreffende ongevraagde elektronische communicatie die in se een aanhoudende gedraging is.

62. Ten derde stelt het voorstel de Commissie in staat om technische uitvoeringsmaatregelen te nemen met het oog op een doeltreffende grensoverschrijdende samenwerking bij de handhaving van nationale wetgeving (voorgestelde wijziging van artikel 15 *bis*, lid 4). De samenwerkingservaring omvat tot nog toe de overeenkomst op initiatief van de Commissie inzake gemeenschappelijke procedures voor de behandeling van grensoverschrijdende klachten inzake spam.

([1]) Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming (PB C 255 van 27.10.2007, blz. 1).

([2]) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

63. De EDPS is van mening dat, indien de wetgeving de regulerende instanties helpt om hun ambtsgenoten in andere landen bij te staan, dit zeker zal bijdragen tot grensoverschrijdende wetshandhaving. Daarom is het goed dat het voorstel de Commissie in staat stelt te zorgen voor grensoverschrijdende samenwerking, inclusief procedures voor informatie-uitwisseling.

III. **CONCLUSIES EN AANBEVELINGEN**

64. De EDPS juicht het voorstel ten zeerste toe. De wijzigingsvoorstellen versterken de bescherming van de persoonlijke levenssfeer en de persoonsgegevens van natuurlijke personen in de elektronische-communicatiesector door middel van een zachte aanpak die organisaties niet op onverantwoorde en onnodige wijze belast. Meer bepaald is de EDPS van mening dat de voorgestelde wijzigingen voor het merendeel ongewijzigd moeten blijven omdat ze goed beantwoorden aan het gestelde doel. De wijzigingsvoorstellen waarvan de EDPS hoopt dat ze ongewijzigd zullen blijven, staan vermeld in punt 69.

65. Ondanks dit overwegend positieve oordeel, vindt de EDPS dat sommige wijzigingsvoorstellen moeten worden verbeterd om ervoor de zorgen dat ze werkelijk een goede bescherming van persoonsgegevens en de privacy van natuurlijke personen bieden. Dit geldt in het bijzonder voor de bepalingen inzake de kennisgeving van inbreuken op de beveiliging en inzake de gerechtelijke procedures ingeleid door aanbieders van elektronische-communicatiediensten wegens overtreding van de bepalingen betreffende spam. Voorts betreurt de EDPS dat een aantal zaken die in de huidige e-privacy-richtlijn niet naar behoren geregeld zijn, in het voorstel niet worden aangepakt en dat dus de kans is gemist om de herziening aan te grijpen om knelpunten op te lossen.

66. Om deze twee gebreken van het voorstel (slecht of niet opgeloste problemen) te verhelpen, wordt in dit advies een aantal redactievoorstellen gedaan. De punten 67 en 68 bevatten een overzicht van de problemen en specifieke suggesties. De EDPS verzoekt de wetgever er in de loop van het wetgevingsproces met betrekking tot dit voorstel rekening mee te houden.

67. De wijzigingsvoorstellen in het voorstel die de EDPS zeer graag gewijzigd zou zien, omvatten:

i) **kennisgeving van inbreuken op de beveiliging**: Zoals reeds gezegd, is de voorgestelde wijziging waarbij *artikel 4, lid 4*, wordt toegevoegd, van toepassing op aanbieders van openbare elektronische-communicatiediensten over openbare netwerken (ISPs, netwerkexploitanten) die verplicht zijn de nationale regelgevende instanties en hun abonnees in kennis te stellen van inbreuken op de beveiliging. De EDPS steunt deze verplichting ten volle. De EDPS is echter van mening dat de verplichting ook moet gelden voor aanbieders van diensten van de informatiemaatschappij die vaak gevoelige informatie verwerken zoals onlinebanken en -verzekeraars, e-healthdiensten en alle andere onlinebedrijven.

Daartoe stelt de EDPS voor de aanbieders van diensten van de informatiemaatschappij op de volgende wijze in artikel 4, lid 3, te vermelden: „In het geval van een inbreuk op de beveiliging (…) stelt de aanbieder van de openbare elektronische-communicatiediensten *en de aanbieder van diensten van de informatiemaatschappij* (…) de betrokken abonnee en de nationale regelgevende instantie daarvan onverwijld in kennis";

ii) **gerechtelijke procedures ingeleid door aanbieders van openbare elektronische-communicatiediensten over openbare netwerken**: In haar huidige vorm voorziet de voorgestelde wijziging van artikel 13, lid 6, in civielrechtelijke rechtsmiddelen voor natuurlijke of rechtspersonen, in het bijzonder aanbieders van elektronische-communicatiediensten, om inbreuken op artikel 13 van de e-privacy-richtlijn betreffende spam te bestrijden. De EDPS is tevreden met deze bepaling. Hij ziet echter niet in waarom deze nieuwe bevoegdheid beperkt zou moeten blijven tot artikel 13 en stelt voor rechtspersonen in staat te stellen om voor overtredingen van om het even welke bepaling van de e-privacy-richtlijn een gerechtelijke procedure in te leiden.

De EDPS stelt voor het huidige artikel 13, lid 6, daartoe om te vormen tot een afzonderlijk artikel 14. Tevens dient de formulering van artikel 13, lid 6, enigszins te worden gewijzigd in die zin dat „overeenkomstig dit artikel" wordt vervangen door „overeenkomstig deze richtlijn".

68. De werkingssfeer van de e-privacy-richtlijn, die momenteel beperkt is tot aanbieders in openbare elektronische-communicatienetwerken, is een van de zorgwekkendste vraagstukken die in het voorstel over het hoofd zijn gezien. De EDPS is van mening dat de richtlijn moet worden gewijzigd om de werkingssfeer uit te breiden tot aanbieders van elektronische-communicatiediensten in gemengde (privaat/openbaar) en private netwerken.

69. De wijzigingsvoorstellen die volgens de EDPS zeker ongewijzigd moeten blijven, zijn:

i) **RFID**: De voorgestelde wijziging van *artikel 3* waarin wordt bepaald dat de elektronische-communicatienetwerken „openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen" omvatten, is geheel bevredigend. Deze bepaling is zeer positief omdat zij verduidelijkt dat een aantal RFID-toepassingen aan de e-privacy-richtlijn moet voldoen, zodat de bestaande rechtsonzekerheid op dit punt wordt weggenomen;

ii) **cookies/spyware**: De voorgestelde wijziging van *artikel 5, lid 3*, is verheugend omdat zij inhoudt dat de informatieplicht en het verplichte aanbieden van het recht om te weigeren dat cookies/spyware op de eindapparatuur van de gebruiker worden opgeslagen nu ook zullen gelden voor externe gegevensopslagmedia zoals CD-ROM's en USB-sticks. De EDPS suggereert echter een kleine wijziging van het laatste gedeelte van artikel 5, lid 3, namelijk de schrapping van het woord „vergemakkelijking" in de laatste zin;

iii) **keuze van de comitologie met raadpleging van de EDPS en voorwaarden/beperkingen van de meldplicht**: De voorgestelde wijziging waarbij artikel 4, lid 4, betreffende de kennisgeving van inbreuken op de beveiliging, wordt toegevoegd, laat het aan de comitologie over om, na raadpleging van de EDPS, een besluit te nemen over complexe aangelegenheden in verband met de omstandigheden, de vorm en de procedures van de regeling voor het melden van inbreuken op de beveiliging. De EDPS steunt deze uniforme aanpak volledig. Wetgeving inzake de kennisgeving van inbreuken op de beveiliging is een afzonderlijk thema dat een zorgvuldige bespreking en analyse vergt.

Het verzoek van sommige belanghebbenden om te voorzien in uitzonderingen op de meldplicht inzake beveiliginginbreuken van artikel 4, lid 4, hangt hiermee samen. De EDPS is daar sterk tegen. Hij geeft er de voorkeur aan dat het vraagstuk van de kennisgeving, de wijze waarop wordt gemeld en de gevallen waarin een melding kan worden ingekort of op enige wijze beperkt, in zijn geheel wordt geanalyseerd nadat hierover een echt debat is gehouden;

iv) **handhaving**: De voorgestelde wijziging waarbij *artikel 15 bis* wordt toegevoegd, bevat vele nuttige elementen die bewaard moeten blijven en die zullen bijdragen tot de effectieve handhaving, zoals de versterking van de onderzoeksbevoegdheden van de nationale regelgevende instanties (artikel 15 *bis*, lid 3) en het aan de nationale regelgevende instanties verlenen van de bevoegdheid om de inbreuken te doen ophouden.

Gedaan te Brussel, 10 april 2008.

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming