Tweede advies van de Europese toezichthouder voor gegevensbescherming over de herziening van 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)

(2009/C 128/04)

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,

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,

Gelet op Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 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, en met name op artikel 41,

BRENGT HET VOLGENDE ADVIES UIT:

I. INLEIDING

Achtergrond

1. De Europese Commissie heeft op 13 november 2007 een voorstel aangenomen tot wijziging van, onder andere, de richtlijn betreffende privacy en elektronische communicatie, meestal de e-privacyrichtlijn genoemd ([1]) (hierna „het voorstel" of „het Commissievoorstel"). De EDPS heeft hierover op 10 april 2008 een advies met verbeteringsaanbevelingen uitgebracht, met als doel ertoe bij te dragen dat de wijzigingsvoorstellen uitmonden in een richtlijn die de best mogelijke bescherming van de persoonlijke levenssfeer en de persoonsgegevens van natuurlijke personen biedt („eerste advies van de EDPS") ([2]).

2. De EDPS heeft in dit eerste advies zijn waardering uitgesproken voor het voorstel van de Commissie om een meldingsplicht in te voeren voor inbreuken op de beveiliging, waarbij ondernemingen verplicht worden natuurlijke personen in kennis te stellen van eventuele inbreuken in verband met hun persoonsgegevens. Voorts verklaart hij zich ingenomen met de nieuwe bepaling die, ter aanvulling op bestaande instrumenten voor het bestrijden van spam, rechtspersonen (bijv. consumentenorganisaties en internetdienstenaanbieders) de mogelijkheid biedt juridische actie te ondernemen tegen spammers.

3. Vervolgens heeft de EDPS tijdens de aan de eerste lezing voorafgaande bespreking in het Europees Parlement nader advies verstrekt in de vorm van opmerkingen over specifieke vraagstukken die de voor de herziening van de Universeledienstrichtlijn ([3]) en de e-privacyrichtlijn bevoegde commissies van het Europees Parlement in hun verslagen aan de orde hadden gesteld („Opmerkingen") ([4]). Deze opmerkingen hebben in hoofdzaak betrekking op vraagstukken in verband met de verwerking van verkeersgegevens en de bescherming van intellectuele-eigendomsrechten.

4. Op 24 september 2008 heeft het Europees Parlement („EP") een wetgevingsresolutie over de e-privacyrichtlijn aangenomen („eerste lezing") ([5]). Een groot aantal van de door het EP in aansluiting op het advies en de opmerkingen van de EDPS aangenomen amendementen is door de EDPS met instemming begroet. Eén van de belangrijke wijzigingen is dat de meldingsplicht voor inbreuken op de beveiliging ook zal gelden voor aanbieders van diensten van de informatiemaatschappij (d.w.z. ondernemingen die via het internet werken). De EDPS was ook

([1]) De herziening van de e-privacyrichtlijn maakt deel uit van een ruimer herzieningsproces, dat strekt tot de oprichting van een telecommunicatieautoriteit op EU-niveau en de herziening van de Richtlijnen 2002/21/EG, 2002/19/EG, 2002/20/EG, 2002/22/EG en 2002/58/EG, alsook van Verordening (EG) nr. 2006/2004 (hierna in zijn geheel „de herziening van het telecommunicatiepakket").

([2]) Advies van 10 april 2008 over het voorstel 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 (richtlijn betreffende privacy en elektronische communicatie), PB C 181 van 18.7.2008, blz. 1.

([3]) Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten (Universeledienstrichtlijn), PB L 108 van 24.4.2002, blz. 51.

([4]) Opmerkingen van de EDPS over specifieke vraagstukken die in het verslag van de IMCO over de herziening van Richtlijn 2002/22/EG (universeledienst) & Richtlijn 2002/58/EG (e-privacy) worden aangesneden, 2 september 2008. Beschikbaar op: www.edps.europa.eu

([5]) Wetgevingsresolutie van het Europees Parlement van 24 september 2008 over het 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 (COM(2007) 698 — C6-0420/2007 — 2007/0248(COD)).

ingenomen met het amendement dat natuurlijke en rechtspersonen de mogelijkheid biedt een inbreuk op enige bepaling van de e-privacyrichtlijn voor de rechter te brengen (en niet alleen inbreuken op de bepalingen betreffende spam, zoals de Commissie oorspronkelijk had voorgesteld). Aansluitend op de eerste lezing van het Parlement heeft de Commissie een gewijzigd voorstel betreffende de e-privacyrichtlijn aangenomen (hierna „het gewijzigd voorstel") ([6]).

5. Op 27 november 2008 heeft de Raad een politiek akkoord bereikt over een herziening van de regelgeving van het telecommunicatiepakket, waaronder de e-privacyrichtlijn, dat het gemeenschappelijk standpunt van de Raad zal worden („gemeenschappelijk standpunt") ([7]). Overeenkomstig artikel 251, lid 2, van het Verdrag tot oprichting van de Europese Gemeenschap zal het gemeenschappelijk standpunt worden meegedeeld aan het EP, dat eventueel amendementen kan voorstellen.

Algemene opmerkingen over het standpunt van de Raad

6. De Raad heeft het voorstel op een aantal essentiële punten gewijzigd en een groot aantal door het EP aangenomen amendementen niet geaccepteerd. Hoewel het gemeenschappelijk standpunt ontegenzeglijk positieve elementen bevat, is de EDPS over het geheel genomen bezorgd over de inhoud ervan, met name omdat een aantal van de positieve wijzigingen die waren voorgesteld in amendementen van het EP, het gewijzigd voorstel van de Commissie en de adviezen van de EDPS en de Europese gegevensbeschermingsautoriteiten (verstrekt via de Groep artikel 29) ([8]) niet in het gemeenschappelijk standpunt zijn overgenomen.

7. Integendeel: in niet weinig gevallen heeft de Raad de in het gewijzigd voorstel en de amendementen van het EP voorgestelde bepalingen die de burgers garanties hadden moeten bieden, geschrapt of fors afgezwakt, met als gevolg dat natuurlijke personen in het gemeenschappelijk standpunt een aanzienlijk lager niveau van bescherming wordt geboden. Daarom brengt de EDPS nu een tweede advies uit, in de hoop dat, naarmate de e-privacyrichtlijn in het wetgevingsproces vordert, nieuwe wijzigingen worden aangenomen waarbij deze waarborgen met betrekking tot gegevensbescherming worden hersteld.

8. Dit tweede advies is toegespitst op een aantal essentiële probleempunten, en komt niet *in extenso* terug op het eerste advies of de opmerkingen van de EDPS, die onverkort geldig blijven. Dit advies gaat met name in op de volgende elementen:

— de bepalingen betreffende de kennisgeving van inbreuken op de beveiliging;

— het toepassingsgebied van de e-privacyrichtlijn wat betreft particuliere en voor het publiek toegankelijke particuliere netwerken;

— het verwerken van verkeersgegevens voor beveiligingsdoeleinden;

— de mogelijkheid voor rechtspersonen om inbreuken op de e-privacyrichtlijn voor de rechter te brengen.

9. Doel van dit advies, is na te gaan hoe deze vraagstukken in het gemeenschappelijk standpunt van de Raad worden benaderd, en dit standpunt te vergelijken met de eerste lezing van het EP en het gewijzigd voorstel van de Commissie. De hier gedane aanbevelingen zijn bedoeld om de bepalingen van de e-privacyrichtlijn te stroomlijnen en ervoor te zorgen dat de richtlijn de geëigende bescherming blijft bieden met betrekking tot de persoonlijke levenssfeer en de persoonsgegevens van natuurlijke personen.

II. DE BEPALINGEN BETREFFENDE DE KENNISGEVING VAN INBREUKEN OP DE BEVEILIGING

10. De EDPS is voorstander van het aannemen van een regeling voor de kennisgeving van inbreuken op de beveiliging waarbij autoriteiten en natuurlijke personen op de hoogte worden gebracht ingeval hun persoonsgegevens zijn gecompromitteerd ([9]). Kennisgeving van inbreuken op de beveiliging kan natuurlijke personen helpen de nodige stappen te nemen om mogelijke schade als gevolg van de inbreuk te verlichten. Het verplicht maken van deze kennisgeving zal ondernemingen ertoe aanzetten gegevens beter te beveiligen en hun aansprakelijkheid met betrekking tot de persoonsgegevens waarvoor ze verantwoordelijk zijn, scherper stellen.

11. De meldingsplicht voor inbreuken op de beveiliging wordt in het gewijzigd voorstel van de Commissie, de eerste lezing van het Europees Parlement en het gemeenschappelijk standpunt van de Raad op drie verschillende manieren benaderd. Elk van die benaderingen heeft positieve kanten, maar de EDPS acht ze ook alle drie voor verbetering vatbaar, en adviseert om in de laatste fase in aanloop naar de aanname van een regeling betreffende inbreuken op de beveiliging rekening te houden met de onderstaande aanbevelingen.

([6]) Gewijzigd 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 elektronischecommunicatienetwerken 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, Brussel, 6.11.2008 COM(2008) 723 def.

([7]) Beschikbaar op de openbare website van de Raad.

([8]) Advies 2/2008 over de herziening van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-privacyrichtlijn), beschikbaar op de website van de Groep artikel 29.

([9]) In dit advies wordt het woord „gecompromitteerd" gebruikt voor inbreuken in verband met persoonsgegevens die het gevolg zijn van onbedoelde of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde mededeling van of toegang tot persoonsgegevens, die worden verstrekt, opgeslagen of anderszins verwerkt.

12. In de analyse van de drie benaderingen van de genoemde regeling moeten vijf kernpunten in ogenschouw worden genomen: *i)* de definitie van een inbreuk op de beveiliging; *ii)* de entiteiten die tot kennisgeving verplicht zijn („betrokken entiteiten"); *iii)* het criterium dat tot kennisgeving verplicht; *iv)* het aanwijzen van de entiteit die bepaalt wanneer een inbreuk op de beveiliging aan dit criterium voldoet, *v)* de ontvangers van de kennisgeving.

Overzicht van de benaderingen van de Commissie, de Raad en het EP

13. Het Europees Parlement, de Commissie en de Raad hebben de kennisgeving van inbreuken op de beveiliging op verschillende manieren benaderd. Het EP heeft in zijn eerste lezing de door de Commissie oorspronkelijk voorgestelde regeling voor de kennisgeving van inbreuken op de beveiliging gewijzigd ([10]). Voor het EP moet de meldingsplicht niet alleen voor aanbieders van openbare elektronische-communicatiediensten gelden, maar ook voor aanbieders van diensten van de informatiemaatschappij. Voorts zouden in deze benadering alle inbreuken in verband met persoonsgegevens aan de nationale regelgevende instantie of de bevoegde instanties (samen „de bevoegde instanties") gemeld moeten worden. Wordt de inbreuk door de bevoegde instanties als *ernstig* aangemerkt, dan zouden zij de aanbieders van openbare elektronische-communicatiediensten en de aanbieders van diensten van de informatiemaatschappij verzoeken, de getroffen persoon hiervan onverwijld in kennis te stellen. Voor inbreuken die een imminent en rechtstreeks gevaar inhouden, zouden deze ondernemingen de natuurlijke personen eerder inlichten dan de bevoegde instanties, en hun besluit niet afwachten. De verplichting om consumenten van een inbreuk in kennis te stellen, geldt niet voor entiteiten die aan de bevoegde instanties kunnen aantonen dat zij *„gepaste technische beschermingsmaatregelen"* hebben genomen die de gegevens onbegrijpelijk maken voor wie deze gegevens niet mag inzien.

14. Ook de Raad vindt dat zowel abonnees als bevoegde instanties in kennis moeten worden gesteld, maar alleen wanneer de *betrokken entiteit* de inbreuk inschat als een *ernstig risico* voor de persoonlijke levenssfeer van de abonnee (identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering of aantasting van de reputatie).

15. De Commissie handhaaft in haar gewijzigd voorstel de door het EP ingestelde verplichting om de autoriteiten van alle inbreuken in kennis te stellen. In tegenstelling tot het EP maakt de Commissie in het gewijzigde voorstel wel een uitzondering op de verplichte kennisgeving aan de getroffen natuurlijke personen, nl. wanneer de aanbieder van de openbare elektronische-communicatiediensten aan de bevoegde instantie aantoont *i)* dat *„er slechts een zeer geringe kans bestaat"* dat als gevolg van de inbreuk schade (bijv. economisch verlies, sociale schade of identiteitsdiefstal) wordt berokkend of *ii) „gepaste technische beschermingsmaatregelen"* zijn toegepast op de gegevens waarop de inbreuk betrekking had. Een en ander betekent dat de Commissie voor de kennisgeving aan natuurlijke personen de toegebrachte schade als uitgangspunt neemt.

([10]) Zie hierover met name de amendementen 187, 124 tot en met 127 alsook 27, 21 en 32 van het EP.

16. Belangrijk is dat de bevoegdheid om te bepalen of een inbreuk ernstig is, of naar redelijkerwijs mag worden aangenomen schade zal berokkenen, in de benadering van het EP ([11]) en de Commissie uiteindelijk bij *de bevoegde instanties* berust. De Raad daarentegen laat dit besluit over aan de *betrokken entiteiten*.

17. Voor de Raad en de Commissie gelden de voorgestelde bepalingen alleen voor de aanbieders van openbare elektronische-communicatiediensten, en niet, zoals in de tekst van het EP, voor aanbieders van diensten van de informatiemaatschappij.

Definitie van een inbreuk op de beveiliging

18. Het verheugt de EDPS dat een inbreuk op de beveiliging in de drie wetgevingsvoorstellen op dezelfde manier wordt gedefinieerd, nl. als een inbreuk *„op de beveiliging die geresulteerd [heeft] in een accidentele of onwettige vernietiging, verlies of wijziging of in niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens, verstuurd, opgeslagen of anderszins verwerkt […]* ([12])".

19. Deze definitie is welkom, omdat zij ruim genoeg is om het merendeel van de situaties te bestrijken waarin kennisgeving van een inbreuk op de beveiliging gerechtvaardigd zou zijn.

20. Ten eerste heeft de definitie betrekking op situaties waarin een derde partij zich op een *ongeoorloofde* manier *toegang* heeft verschaft tot persoonsgegevens, bijvoorbeeld door in te breken in een server die persoonsgegevens bevat, en die informatie op te vragen.

21. Ten tweede bestrijkt de definitie ook situaties waarin persoonsgegevens verloren of vrijgegeven zijn, en het bewijs van een ongeoorloofde toegang nog geleverd moet worden. Het gaat dan om situaties waarin persoonsgegevens mogelijk verloren zijn geraakt (bijv. cd-roms, USB-drives, of andere draagbare apparatuur), of openbaar worden gemaakt door regelmatige gebruikers (een gegevensbestand over of van werknemers dat onbedoeld en tijdelijk via het internet beschikbaar wordt gesteld op een voor het publiek toegankelijke plaats). Omdat er vaak geen aanwijzingen zullen zijn dat deze gegevens al dan niet op een bepaald moment door niet gemachtigde derde partijen ingezien of gebruikt mogen worden, lijkt het raadzaam dit soort situaties in de definitie op te nemen. De EDPS beveelt dan ook aan deze definitie van een inbreuk op de beveiliging te handhaven, en haar op te nemen in artikel 2 van de e-privacyrichtlijn; dit zou beter passen in de algemene structuur van de richtlijn en de duidelijkheid ten goede komen.

([11]) Behalve wanneer er imminent en rechtstreeks gevaar dreigt: in dat geval lichten de betrokken entiteiten eerst de consumenten in.

([12]) Artikel 2, van het gemeenschappelijk standpunt (punt h)) en het gewijzigd voorstel (punt i)) en artikel 3, lid 3, van de eerste lezing van het EP.

Entiteiten waarvoor de meldingsplicht zou moeten gelden

22. Wat het EP betreft, geldt de meldingsplicht zowel voor aanbieders van openbare elektronische-communicatiediensten als voor aanbieders van diensten van de informatiemaatschappij. Volgens de Raad en de Commissie, daarentegen, zouden alleen aanbieders van openbare elektronische-communicatiediensten, zoals telecommunicatiebedrijven en aanbieders van internettoegang, natuurlijke personen op de hoogte moeten brengen wanneer er een inbreuk op de beveiliging heeft plaatsgevonden die persoonsgegevens compromitteert. Voor andere sectoren, zoals onlinebanken, onlinekleinhandels, aanbieders van e-gezondheidsdiensten en anderen geldt deze verplichting niet. De EDPS acht het vanuit het oogpunt van de openbare orde essentieel dat kennisgeving ook verplicht wordt gesteld voor diensten van de informatiemaatschappij, waaronder onlineondernemingen, onlinebanken, aanbieders van e-gezondheidsdiensten enz.

23. Ten eerste kan weliswaar niet ontkend worden dat telecommunicatiebedrijven doelwit zijn van inbreuken op de beveiliging die een meldingsplicht rechtvaardigen, maar dit geldt evenzeer voor andere categorieën van ondernemingen/aanbieders. Onlinekleinhandels, onlinebanken, onlineapotheken kunnen evenzeer, of zelfs meer dan telecommunicatiebedrijven, het slachtoffer van dergelijke inbreuken zijn. De risicoafweging lijkt niet te rechtvaardigen dat de meldingsplicht voor inbreuken beperkt wordt tot aanbieders van openbare elektronische-communicatiediensten. De ervaring in andere landen toont aan dat een bredere aanpak nodig is. In de Verenigde Staten, bijvoorbeeld, hebben bijna alle staten (op dit ogenblik meer dan 40) wetgeving betreffende de melding van inbreuken op de beveiliging vastgesteld die een ruimer toepassingsgebied heeft, en niet alleen geldt voor aanbieders van openbare elektronische-communicatiediensten, maar voor alle entiteiten die de betrokken persoonsgegevens in hun bezit hebben.

24. Ten tweede moge duidelijk zijn dat inbreuken op de categorieën van persoonsgegevens die op regelmatige basis door aanbieders van openbare elektronische-communicatiediensten worden verwerkt, gevolgen kunnen hebben voor de persoonlijke levenssfeer van natuurlijke personen, maar dit geldt evenzeer, of zelfs meer, voor de categorieën van persoonsgegevens die verwerkt worden door aanbieders van diensten van de informatiemaatschappij. Immers, banken en ander financiële instellingen kunnen in het bezit zijn van bijzonder vertrouwelijke gegevens (bijvoorbeeld met betrekking tot bankrekeningen), die bij openbaarmaking misbruikt kunnen worden voor identiteitsdiefstal. Ook de bekendmaking van bijzonder gevoelig informatie over de gezondheid door onlinegezondheidsdiensten kan bijzonder schadelijk zijn voor natuurlijke personen. De verschillende categorieën van persoonsgegevens die kunnen worden gecompromitteerd, vormen daarom ook een argument om de meldingsplicht voor inbreuken op de beveiliging uit te breiden, ten minste tot aanbieders van informatiemaatschappijdiensten.

25. Tegen deze verruiming van het toepassingsgebied van het artikel, d.w.z. van de entiteiten waarop deze bepaling van toepassing zou moeten zijn, zijn juridische bezwaren ingebracht. Zo is met name beoogd dat de e-privacyrichtlijn alleen voor aanbieders van openbare elektronische-communicatiediensten geldt, wat is ingeroepen als argument tegen een uitbreiding van de meldingsplicht tot aanbieders van diensten van de informatiemaatschappij.

26. De EDPS wijst in dit verband op het volgende: *i)* er is geen enkel juridisch argument in te brengen tegen het verruimen van het toepassingsgebied van sommige bepalingen van de richtlijn tot andere actoren dan aanbieders van openbare elektronische-communicatiediensten. Dit is geheel ter beoordeling van de communautaire wetgever; *ii)* er zijn andere precedenten in de huidige e-privacyrichtlijn van van toepassing verklaring op andere entiteiten dan aanbieders van openbare elektronische-communicatiediensten.

27. Artikel 13, bijvoorbeeld, waarin instemming vooraf verplicht wordt gesteld, is niet alleen van toepassing op aanbieders van openbare elektronische-communicatiediensten, maar op alle ondernemingen die ongevraagd berichten sturen. Voorts is artikel 5, lid 3, van de e-privacyrichtlijn, waarbij onder meer verboden wordt informatie zoals cookies in de eindapparatuur van de verbruiker op te slaan, bindend, niet alleen voor aanbieders van openbare elektronische-communicatiediensten, maar voor iedereen die probeert informatie op te slaan of toegang te verkrijgen tot informatie die is opgeslagen in de eindapparatuur van natuurlijke personen. De Commissie heeft in het lopende wetgevingsproces zelfs voorgesteld de toepassing van artikel 5, lid 3, te verruimen, omdat dergelijke technologieën (cookies/spyware) niet alleen via elektronische-communicatiesystemen verspreid worden, maar op alle mogelijke andere manieren (verspreiding door downloaden van het internet of via media voor externe gegevensopslag, zoals cd-roms, USB-sticks, flash drives enz.). Al deze positieve elementen moeten behouden worden, en vormen tegelijkertijd een nuttig precedent voor de lopende discussie over het toepassingsgebied.

28. Voorts hebben de Commissie en het EP, en eigenlijk ook de Raad, in het huidige wetgevingsproces een nieuw artikel 6, lid 6 bis, voorgesteld (bespreking zie *infra*) dat van toepassing is op andere entiteiten dan aanbieders van openbare elektronische-communicatiediensten.

29. Tot slot is het zeer waarschijnlijk dat burgers, gelet op het algemene positieve effect van een meldingsplicht voor inbreuken op de beveiliging, in situaties waarin hun persoonsgegevens zijn gecompromitteerd, altijd een dergelijke gunstige behandeling zullen verwachten, niet alleen van aanbieders van openbare elektronische-communicatiediensten, maar ook van aanbieders van diensten van de informatiemaatschappij. Het risico bestaat dat burgers in hun verwachtingen teleurgesteld worden indien zij, bijvoorbeeld, niet worden ingelicht wanneer een onlinebank de gegevens over hun bankrekening is kwijtgeraakt.

30. De EDPS is er dan ook van overtuigd dat de meldingsplicht voor inbreuken op de beveiliging alleen ten volle effect zal sorteren indien zij zowel voor aanbieders van openbare elektronische-communicatiediensten, als voor aanbieders van diensten van de informatiemaatschappij geldt.

De drempel voor kennisgeving

31. Wat de drempel voor kennisgeving betreft, is het meest geschikte van de drie voorgestelde criteria volgens de EDPS in het gewijzigd voorstel van de Commissie te vinden („*een zeer geringe kans […] dat de consumentenrechten en -belangen […] worden geschaad*"). Wel is het zaak het woord „schaden" ruim genoeg te definiëren om alle vormen van negatieve impact op de persoonlijke levenssfeer of andere rechtmatige belangen van natuurlijke personen te bestrijken. Anders is een nieuw criterium te verkiezen, waarbij kennisgeving verplicht zou zijn wanneer „redelijkerwijs mag worden aangenomen dat de inbreuk negatieve gevolgen zal hebben voor natuurlijke personen".

32. Het EP, de Commissie en de Raad verschillen, zoals eerder reeds gezegd, van mening over de omstandigheden („de drempel" of „het criterium" genoemd) die tot kennisgeving aan natuurlijke personen verplichten. Het aantal meldingen dat natuurlijke personen ontvangen, zal uiteraard in hoge mate afhangen van de drempel die, of het criterium dat, voor kennisgeving wordt vastgesteld.

33. Volgens de Raad en de Commissie moet tot kennisgeving worden overgegaan wanneer de inbreuk „*een ernstig risico voor de persoonlijke levenssfeer van de abonnee vormt*" (Raad) en wanneer er meer dan „*een zeer geringe kans bestaat dat de consumentenrechten en -belangen […] worden geschaad*" (Commissie). Voor het EP is het criterium voor kennisgeving aan natuurlijke personen de „*ernst van de inbreuk*" (d.w.z. kennisgeving aan natuurlijke personen is verplicht wanneer de inbreuk „*ernstig*" wordt geacht). Beneden deze drempel is kennisgeving niet nodig ([13]).

34. De EDPS beseft dat betoogd kan worden dat natuurlijke personen bij een schending van hun persoonsgegevens in alle omstandigheden het recht hebben van deze inbreuk op de hoogte te worden gebracht. Maar de vraag dringt zich op of dit, in het licht van andere belangen en overwegingen, wel een geschikte oplossing is.

35. Geopperd is dat een meldingsplicht voor alle gevallen waarin persoonsgegevens gecompromitteerd zijn — met andere woorden een onbegrensde plicht — kan leiden tot een buitensporig aantal meldingen en kennisnemingsmoeheid, waardoor de aandacht voor dit probleem zou afnemen. De EDPS is gevoelig voor dit argument, maar wil tegelijkertijd zijn bezorgdheid uiten over een eventueel buitensporig aantal meldingen, omdat dat kan wijzen op wijdverspreide tekortkomingen in de gangbare praktijk op het gebied van informatiebeveiliging.

36. De EDPS is zich bewust van mogelijk negatieve gevolgen van overmatige kennisgeving, en wil ertoe bijdragen dat het wettelijk kader dat voor kennisgeving van inbreuken op de beveiliging wordt aangenomen, niet tot dit resultaat leidt. Indien natuurlijke personen regelmatig meldingen van inbreuken ontvangen, ook in situaties waarin dit geen negatieve gevolgen, schade of noodsituatie veroorzaakt, lopen we het risico een van de basisdoelstellingen van de kennisgeving te ondermijnen, omdat natuurlijke personen dan, ironisch genoeg, deze meldingen zouden gaan negeren in situaties waarin zij wel degelijk stappen zouden moeten nemen om zich te beschermen. Daarom is het zaak het juiste evenwicht te vinden en ervoor te zorgen dat meldingen zinvol zijn; wanneer natuurlijke personen niet op meldingen reageren, zal een kennisgevingsregeling immers een zeer beperkt nut hebben.

37. Om een passend criterium aan te nemen, dat geen aanleiding geeft tot buitensporig veel kennisgevingen dienen, naast de drempel voor kennisgeving, andere factoren in overweging te worden genomen, zoals de definitie van een inbreuk op de beveiliging en de informatie die onder de meldingsplicht valt. De EDPS merkt in dat verband op dat, in het licht van de ruime definitie van een inbreuk op de beveiliging (zie *supra*), de drie benaderingen alle tot een hoog aantal meldingen kunnen leiden. Een andere reden voor bezorgdheid over overmatige kennisgeving is het feit dat de definitie van een inbreuk op de beveiliging betrekking heeft op alle categorieën van persoonsgegevens. De EDPS beschouwt dit als de juiste aanpak (geen beperking wat betreft de categorieën van persoonsgegevens waarvoor kennisgeving verplicht is), in tegenstelling tot andere benaderingen zoals in de Amerikaanse wetgeving waar in de voorschriften wordt uitgegaan van de gevoeligheid van de informatie, maar beschouwt dit niettemin ook als een factor waarmee rekening moet worden gehouden.

38. Rekening houdend met het samenstel van variabelen acht de EDPS het dan ook raadzaam in de tekst een drempel of criterium voor de verplichting tot kennisgeving op te nemen.

39. De voorgestelde criteria (de inbreuk vormt een „ernstig *risico voor de persoonlijke levenssfeer*" of er bestaat meer dan „*een zeer geringe kans*" op schade) lijken beide betrekking te hebben op, bijvoorbeeld, sociale of reputatieschade en economisch verlies. Met deze criteria zouden situaties bestreken worden waarin zich een risico op identiteitsdiefstal voordoet doordat niet-openbare identificatiegegevens (bijv. paspoortnummers) zijn vrijgegeven, of waarin informatie over het privéleven van een natuurlijk persoon wordt vrijgegeven. De EDPS juicht deze aanpak toe. Hij is ervan overtuigd dat een meldingsplicht voor inbreuken op de beveiliging niet het optimale effect zou sorteren indien de regeling beperkt blijft tot inbreuken die economische schade veroorzaken.

([13]) Zie voetnoot 11 voor de uitzondering op deze regel.

40. Van de twee voorgestelde criteria heeft het criterium van de Commissie (meer dan „*een zeer geringe kans*" op schade) de voorkeur van de EDPS, omdat het natuurlijke personen een beter niveau van bescherming biedt. De kans dat inbreuken onder de meldingsplicht vallen, is veel groter wanneer er meer dan „*een zeer geringe kans*" op schade voor de persoonlijke levenssfeer van een natuurlijk persoon moet zijn, dan wanneer de inbreuk een „*ernstig risico*" op dergelijke schade dient te vormen. Alleen de inbreuken met een ernstig risico voor de persoonlijke levenssfeer in het toepassingsgebied opnemen, zou het aantal te melden inbreuken aanzienlijk beperken, en aanbieders van openbare elektronische-communicatiediensten en aanbieders van diensten van de informatiemaatschappij een onredelijk grote beoordelingsmarge laten bij het beantwoorden van de vraag of een inbreuk gemeld moet worden; het zal voor hen immers veel makkelijker te rechtvaardigen zijn dat er geen „*ernstig risico*" op schade is, dan dat de kans op schade „*zeer gering*" is. Overmatige kennisgeving wordt met het criterium van het „ernstige risico" ongetwijfeld voorkomen, maar de bescherming van de privacybelangen van natuurlijke personen dient, alles bij elkaar genomen, het voordeel van de twijfel te krijgen: het is een absoluut minimum dat natuurlijke personen beschermd worden wanneer redelijkerwijs mag worden aangenomen dat een inbreuk hen schade zal berokkenen. Bovendien zal de uitdrukking „*meer dan een zeer gering risico*" in de praktijk efficiënter zijn, zowel voor de betrokken entiteiten als voor de bevoegde autoriteiten, omdat de inbreuk en de context ervan objectief geëvalueerd moeten worden.

41. Inbreuken in verband met persoonsgegevens kunnen schade veroorzaken die moeilijk te kwantificeren is, en die per geval kan verschillen. Het bekend worden van dezelfde categorie van gegevens kan, naargelang de omstandigheden van de betrokkene, aanzienlijke of integendeel weinig schade veroorzaken. Indien de schade materieel, aanzienlijk of ernstig moet zijn, is dit als criterium niet geschikt. De door de Raad voorgestelde formulering, bijvoorbeeld, dat de inbreuk de persoonlijke levenssfeer *ernstig* moet schenden, zou natuurlijke personen onvoldoende bescherming bieden, omdat volgens dit criterium de gevolgen voor de persoonlijke levenssfeer „ernstig" moeten zijn. Bovendien laat dit ruimte voor subjectieve evaluatie.

42. „*Meer dan een zeer gering risico op schade*" lijkt dus een passend criterium om te bepalen of een inbreuk op de beveiliging gemeld moet worden, maar toch blijft het de EDPS zorgen baren dat hiermee mogelijk niet alle situaties bestreken worden waarin kennisgeving aan natuurlijke personen gerechtvaardigd is, d.w.z. alle situaties waarin redelijkerwijs mag worden aangenomen dat de inbreuk negatieve gevolgen zal hebben voor de persoonlijke levenssfeer of andere legitieme rechten van natuurlijke personen. Daarom zou een criterium overwogen kunnen worden waarbij kennisgeving verplicht wordt gesteld „*wanneer redelijkerwijs mag worden aangenomen dat de inbreuk negatieve gevolgen zal hebben voor natuurlijke personen*".

43. Bijkomend voordeel van dit alternatieve criterium is dat het spoort met de EU-wetgeving inzake gegevensbescherming. Zo wordt in de richtlijn gegevensbescherming meermaals verwezen naar de inbreuken op de rechten en vrijheden van betrokkenen. In artikel 18 en overweging 49 (verplichting om verwerkingen van gegevens aan te melden bij de gegevensbeschermingsautoriteiten), bijvoorbeeld, wordt lidstaten de mogelijkheid geboden om vrijstelling van deze verplichting te verlenen voor de categorieën verwerkingen waarbij „*een inbreuk op de rechten en vrijheden van de betrokkenen onwaarschijnlijk is*". Een soortgelijke formulering is te vinden in artikel 13, lid 6, van het gemeenschappelijk standpunt, dat rechtspersonen de mogelijkheid biedt juridische actie te ondernemen tegen spammers.

44. Aangenomen mag tevens worden dat de betrokken entiteiten, en met name de voor de handhaving van gegevensbeschermingswetgeving bevoegde instanties, beter met dit alternatieve criterium vertrouwd zullen zijn, wat het voor hen ook makkelijker zal maken een inbreuk aan het vastgestelde criterium te toetsen.

Entiteit die een inbreuk op de beveiliging aan het criterium zal toetsen

45. Wat het EP (behalve wanneer er onmiddellijk gevaar dreigt) en de Commissie (gewijzigd voorstel) betreft, berust de bevoegdheid om inbreuken op de beveiliging te toetsen aan het criterium dat tot kennisgeving aan de betrokken natuurlijke personen verplicht, bij de nationale instanties.

46. De EDPS hecht veel waarde aan een regeling waarin het toetsen aan het criterium wordt toevertrouwd aan een ter zake bevoegde instantie, omdat dit een zekere garantie biedt voor de correcte toepassing van de wet. Op die manier kan verhinderd worden dat ondernemingen een inbreuk ten onrechte kwalificeren als niet schadelijk/ernstig en kennisgeving vermijden wanneer die wel degelijk vereist is.

47. Tegelijkertijd vreest de EDPS dat een regeling waarbij de evaluatiebevoegdheid bij de autoriteiten berust, niet werkbaar en moeilijk toe te passen, of in de praktijk zelfs contraproductief zal zijn, waardoor natuurlijke personen zelfs minder goede garanties op gegevensbescherming zouden hebben.

48. Het risico is immers dat gegevensbeschermingsautoriteiten overspoeld worden met meldingen van inbreuken op de beveiliging, en dat het evalueren van die inbreuken een zeer zware opgave wordt. Om een inbreuk aan het criterium te kunnen toetsen, zullen de bevoegde instanties immers voldoende interne informatie moeten ontvangen, die vaak van technisch ingewikkelde aard zal zijn en die zij zeer snel zullen moeten verwerken. Gelet op de moeilijkheidsgraad van deze evaluaties en op het feit dat sommige instanties over beperkte middelen beschikken, vreest de EDPS dat het voor de bevoegde instanties bijzonder moeilijk wordt om deze opdracht te vervullen, en dat een en ander ten koste van andere belangrijke prioriteiten zou gaan. Deze regeling zou voor de bevoegde instanties bovendien onevenredig belastend kunnen zijn, omdat zij, indien een inbreuk als niet ernstig wordt aangemerkt en natuurlijke personen toch schade wordt berokkend, aansprakelijk zouden kunnen worden gesteld.

49. Bijkomend probleem is dat tijd een sleutelrol speelt bij het beperken van de risico's van een inbreuk op de beveiliging. Tenzij de bevoegde instanties in staat zijn zeer snel met een evaluatie te komen, vormt de extra tijd die zij voor deze afweging nodig hebben, een risico op meer schade voor de betrokken natuurlijke personen. Ironisch genoeg zou deze verscherpte maatregel, die tot doel heeft natuurlijke personen beter te beschermen, tot gevolg hebben dat zij minder bescherming genieten dan in een regeling met directe kennisgeving.

50. De EDPS acht het dan ook verkieslijk een regeling te treffen waarbij het toetsen van een inbreuk aan het criterium wordt overgelaten aan de betrokken entiteiten, zoals door de Raad wordt voorgesteld.

51. Om mogelijke misbruiken uit te sluiten, bijvoorbeeld van entiteiten die een inbreuk niet melden wanneer dat duidelijk wel nodig is, is het van het allergrootste belang de hierna beschreven gegevensbeschermingsgaranties in de regeling op te nemen.

52. Ten eerste spreekt het voor zich dat de verplichting van de betrokken entiteiten om een inbreuk aan het kennisgevingscriterium te toetsen, moet samengaan met een andere verplichting, nl. om alle inbreuken die aan het criterium voldoen, te melden aan de bevoegde instanties. De betrokken entiteiten moeten verplicht worden de bevoegde instanties in kennis te stellen van de gemelde inbreuken en van de motivering en inhoud van elke kennisgeving.

53. Ten tweede moet de bevoegde instanties een volwaardige toezichtsfunctie worden toegekend. In die functie krijgen zij het recht — maar niet de plicht — na te gaan in welke omstandigheden de inbreuk heeft plaatsgevonden, en passende corrigerende maatregelen op te leggen ([14]). Daarbij moeten zij de mogelijkheid krijgen niet alleen tot kennisgeving aan natuurlijke personen te verplichten (als dat al niet gebeurd is), maar ook om maatregelen op te leggen ter voorkoming van verdere inbreuken. De bevoegde instanties moeten in dit verband afdoende bevoegdheden en middelen krijgen, alsook de nodige ruimte om te bepalen wanneer op de melding van een inbreuk op de beveiliging wordt ingegaan. Op die manier zouden de bevoegde instanties selectief kunnen optreden en een onderzoek instellen naar, bijvoorbeeld, grote, echt schadelijke inbreuken op de beveiliging, waarbij zij nagaan of de wetsvoorschriften zijn nageleefd en die naleving ook kunnen afdwingen.

54. Daarom beveelt de EDPS aan om, ter aanvulling op de in de e-privacyrichtlijn (bijv. artikel 15 bis, lid 3) en de gegevensbeschermingsrichtlijn vastgestelde bevoegdheden, het volgende toe te voegen: *„Indien de betrokken abonnee of persoon nog niet van de inbreuk in kennis is gesteld, kan de bevoegde nationale instantie, na beoordeling van de aard van de inbreuk, de aanbieders van openbare elektronische-communicatiediensten en de aanbieders van diensten van de informatiemaatschappij verzoeken dit alsnog te doen.*".

55. Voorts beveelt de EDPS het EP en de Raad aan het voorstel van het EP (amendement 122, artikel 4, lid 1 bis) te bevestigen, zodat entiteiten verplicht worden hun systemen en de persoonsgegevens die zij willen verwerken, in kaart te brengen en de risico's ervan te evalueren. Op grond van deze bepaling zullen entiteiten een precies en op hun systeem toegesneden overzicht opstellen van de beveiligingsmaatregelen die zij toepassen; dit overzicht hoort ter beschikking te staan van de bevoegde instanties. Deze verplichting zal de betrokken entiteiten — en uiteindelijk ook de bevoegde instanties, in hun toezichtsfunctie — in geval van inbreuk op de beveiliging helpen bepalen of het compromitteren van deze gegevens negatieve gevolgen kan hebben voor of schade berokkenen aan natuurlijke personen.

56. Ten derde dienen betrokken entiteiten, wanneer zij verplicht worden om te bepalen of natuurlijke personen van een inbreuk in kennis moeten worden gesteld, ook verplicht te worden om een volledig en gedetailleerd intern evaluatieverslag bij te houden, waarin alle inbreuken en eventuele kennisgevingen daarvan vermeld staan, alsook de maatregelen die zijn genomen om herhaling te voorkomen. Dit interne evaluatieverslag moet ter beschikking staan van de bevoegde instanties, met het oog op controle en eventueel onderzoek, zodat zij hun toezichtsrol kunnen uitoefenen. Hiertoe zou een bepaling kunnen worden ingevoegd in de volgende zin: *„Aanbieders van openbare elektronische-communicatiediensten en aanbieders van diensten van de informatiemaatschappij maken en bewaren een uitvoerig verslag over alle inbreuken op de beveiliging die zich hebben voorgedaan, de nuttige technische informatie in dit verband en de corrigerende maatregelen die zij hebben genomen. In dit verslag wordt ook verwezen naar alle meldingen die aan de betrokken abonnees of personen, alsook aan de bevoegde nationale instanties zijn gedaan, met vermelding van de datum en inhoud ervan. Het verslag wordt desgevraagd aan de bevoegde nationale instantie voorgelegd.*".

57. Uiteraard zou het, met het oog op de coherente toepassing van het genoemde criterium en van andere relevante aspecten van het wetgevingskader voor inbreuken op de beveiliging (bijvoorbeeld het formaat en de procedures voor meldingen), nuttig zijn dat de Commissie, na overleg met de EDPS, de Groep artikel 29 en andere betrokkenen, technische uitvoeringsmaatregelen aanneemt.

([14]) Die toezichtsbevoegdheid wordt toegekend in artikel 15 bis, lid 3: *„De lidstaten waken erover dat de bevoegde nationale instanties, en, waar passend, andere nationale instanties, over alle nodige onderzoeksbevoegdheden en -middelen beschikken, met inbegrip van de mogelijkheid alle relevante informatie op te vragen die zij nodig kunnen hebben om de overeenkomstig deze richtlijn vastgestelde nationale bepalingen te monitoren en na te doen leven.*"

Ontvangers van de meldingen

58. Wat de ontvangers van de meldingen betreft, verkiest de EDPS de terminologie van het EP en de Commissie boven die van de Raad. Het EP heeft het woord „abonnees" vervangen door „gebruikers", de Commissie spreekt van „abonnees" en „betrokken personen". Volgens de bepaling van zowel het EP als de Commissie, dienen niet alleen huidige abonnees, maar ook voormalige abonnees en derden, zoals gebruikers die met de betrokken entiteiten in contact treden zonder abonnee te zijn, een melding ontvangen. De EDPS is ingenomen met deze aanpak, en roept het EP en de Raad op deze benadering te handhaven.

59. Wel is de terminologie in de eerste lezing van het EP niet overal coherent, wat verholpen zou moeten worden. Zo is het woord „abonnees" in de meeste, maar niet in alle, gevallen vervangen door „gebruikers", soms staat er „consumenten". Dit moet worden gelijkgetrokken.

III. TOEPASSINGSGEBIED VAN DE E-PRIVACYRICHTLIJN: OPENBARE EN PARTICULIERE NETWERKEN

60. In de huidige e-privacyrichtlijn wordt in artikel 3, lid 1, bepaald op welke entiteiten de richtlijn in hoofdzaak van toepassing is, nl. entiteiten die gegevens verwerken „*in verband met*" de levering van openbare elektronische-communicatiediensten over openbare netwerken ([15]). Voorbeelden van openbare elektronische-communicatiediensten zijn de verstrekking van internettoegang, de transmissie van informatie via elektronische netwerken, mobiele en vaste telefoon, enz.

61. Het EP heeft een amendement 121 aangenomen waarbij, middels een aanpassing van artikel 3 van het oorspronkelijke Commissievoorstel, het toepassingsgebied van de e-privacyrichtlijn verruimd wordt tot „*de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare en particuliere communicatienetwerken en voor het publiek toegankelijke particuliere netwerken in de Gemeenschap, […]*" (artikel 3, lid 1, van de e-privacyrichtlijn). Jammer genoeg was dit amendement voor de Raad en de Commissie moeilijk aanvaardbaar, en hebben zij het niet in hun gemeenschappelijk standpunt respectievelijk gewijzigd voorstel overgenomen.

Toepassing van de e-privacyrichtlijn op voor het publiek toegankelijke particuliere netwerken

62. Ter bevordering van een consensus dringt de EDPS er dan ook op aan de kern van amendement 121 over te nemen. Voorts stelt hij een wijziging voor om verder te verduidelijken welke categorieën van diensten onder dit verruimde toepassingsgebied zouden vallen.

63. Particuliere netwerken worden vaak gebruikt om elektronische-communicatiediensten, zoals internettoegang, te verstrekken aan een onbekend aantal mensen, dat mogelijk heel groot kan zijn. Dit geldt, bijvoorbeeld, voor internettoegang in internetcafés en wifipunten in hotels, restaurants, luchthavens, treinen en op andere voor het publiek toegankelijke plaatsen, waar dergelijke diensten vaak ter aanvulling op andere diensten (dranken, logies, enz.) worden aangeboden.

64. In al deze gevallen wordt een communicatiedienst (bijvoorbeeld internettoegang) ter beschikking gesteld aan het publiek, niet via een openbaar netwerk, maar via een netwerk dat als particulier kan worden beschouwd, d.w.z. een netwerk dat particulier wordt geëxploiteerd. Voorts kan worden geargumenteerd dat de volledige e-privacyrichtlijn, of ten minste een aantal artikelen daarvan, niet op het verstrekken van deze diensten van toepassing is, omdat de communicatiedienst in de genoemde gevallen weliswaar aan het publiek wordt verstrekt, maar het netwerk een particulier, en geen openbaar netwerk is ([16]). Een en ander betekent dat de door de e-privacyrichtlijn gegarandeerde fundamentele rechten in deze gevallen niet worden beschermd, en dat rechtsongelijkheid ontstaat tussen gebruikers die het internet betreden via openbare telecommunicatiemiddelen en gebruikers die hetzelfde doen met particuliere middelen, terwijl het risico voor de persoonlijke levenssfeer en de persoonsgegevens in al deze gevallen even groot is. Er lijken dan ook argumenten te zijn voor het in de huidige richtlijn bestaande verschil in behandeling tussen communicatiediensten die worden verstrekt via een particulier dan wel een openbaar netwerk.

65. Een amendement zoals amendement 121 van het EP, dat zou strekken tot een uitbreiding van het toepassingsgebied van de e-privacyrichtlijn tot de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over *particuliere* communicatienetwerken, zou door de EDPS dan ook gesteund worden.

66. De EDPS beseft dat dit onvoorziene en mogelijk onbedoelde gevolgen zou kunnen hebben. Het vermelden van particuliere netwerken in het dispositief van de richtlijn kan er op zich al toe leiden dat het toepassingsgebied ruimer dan bedoeld geïnterpreteerd wordt. Hoewel dit

([15]) „*Deze* richtlijn *is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken*".

([16]) *A contrario* kan betoogd worden dat deze communicatiediensten, zelfs al gaat het om een particulier netwerk, aan het publiek worden verstrekt, en het verstrekken van deze diensten derhalve onder het bestaande wetgevingskader valt, ondanks het particuliere netwerk. In Frankrijk, bijvoorbeeld, zijn werkgevers die hun werknemers toegang tot het internet verschaffen, op gelijke voet gesteld met dienstverleners die internettoegang op commerciële basis verschaffen. Die interpretatie wordt niet algemeen geaccepteerd.

niet de strekking is van amendement 121, zou volgens een letterlijke of strikte interpretatie ervan betoogd kunnen worden dat ook eigenaars van met wifi uitgeruste huizen ([17]), waar iedereen binnen het bereik ervan (meestal het huis) verbinding kan maken, onder de richtlijn vallen. Om dit te voorkomen stelt de EDPS voor amendement 121 anders te formuleren en het toepassingsgebied van de e-privacyrichtlijn te verruimen tot *„de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare en voor het publiek toegankelijke particuliere netwerken in de Gemeenschap, …”*.

67. Dit kan helpen verduidelijken dat alleen particuliere netwerken die voor het publiek toegankelijk zijn, onder de e-privacyrichtlijn zouden vallen. Door de bepalingen van de e-privacyrichtlijn *alleen* op de *voor het publiek toegankelijke particuliere netwerken* (en niet op alle particuliere netwerken) toe te passen wordt een drempel ingebouwd waardoor de richtlijn alleen van toepassing zal zijn op communicatiediensten die worden verstrekt via particuliere netwerken die bewust voor het publiek worden *opengesteld*. Met die formulering wordt duidelijker beklemtoond dat de *beschikbaarheid* van het particuliere netwerk *voor het grote publiek* het basiscriterium is voor de eventuele toepasselijkheid van de richtlijn (naast het verstrekken van een openbare communicatiedienst). Met andere woorden: indien het netwerk, ongeacht of het openbaar of particulier is, bewust voor het publiek wordt opengesteld teneinde een openbare communicatiedienst, zoals internettoegang, te verstrekken — zelfs al is dit ter aanvulling op een andere dienst, zoals een hotelkamer — valt deze categorie van diensten/netwerken onder de e-privacyrichtlijn.

68. De EDPS is van mening dat deze aanpak, waarbij de bepalingen van de e-privacyrichtlijn worden toegepast op *voor het publiek toegankelijke particuliere netwerken,* spoort met de aanpak die wordt gevolgd in verscheidene lidstaten, waar deze categorie van diensten, alsook door zuiver particuliere netwerken verstrekte diensten volgens de autoriteiten onder het toepassingsgebied van nationale bepalingen ter uitvoering van de e-privacyrichtlijn vallen ([18]).

69. Om meer rechtszekerheid te bieden aangaande de entiteiten die onder het nieuwe toepassingsgebied vallen, kan het nuttig zijn in de e-privacyrichtlijn een definitie van „voor het publiek toegankelijke particuliere netwerken” op te nemen, die als volgt zou kunnen luiden: *„voor het publiek toegankelijk particulier netwerk: een particulier geëxploiteerd netwerk waartoe het grote publiek in de regel onbeperkt toegang heeft, al dan niet tegen betaling of in samenhang met andere diensten of aanbiedingen, behoudens aanvaarding van de geldende voorwaarden*”.

70. In de praktijk betekent dit dat particuliere netwerken in hotels en andere instellingen die het grote publiek via een particulier netwerk toegang verstrekken tot het internet, onder het toepassingsgebied zouden vallen. Het verstrekken van communicatiediensten in een zuiver particulier netwerk, daarentegen, waar de dienst verstrekt wordt aan een beperkte groep identificeerbare personen, zou er niet onder vallen. Virtuele particuliere netwerken en huizen van consumenten die met wifi zijn uitgerust, zouden niet onder de richtlijn vallen, net zo min als diensten die verstrekt worden in louter interne netwerken van ondernemingen.

Particuliere netwerken onder het toepassingsgebied van de e-privacyrichtlijn

71. Het uitsluiten van particuliere netwerken als zodanig moet beschouwd worden als een overgangsmaatregel, die nadere bespreking behoeft. Deze optie blijft immers niet zonder gevolgen op het gebied van de persoonlijke levenssfeer, en betreft bovendien een groot aantal mensen, die het internet meestal betreden via bedrijfsnetwerken; daarom kan het in de toekomst nodig zijn deze kwestie opnieuw te bekijken. Om dit debat te voeden beveelt de EDPS aan in de e-privacyrichtlijn een overweging op te nemen op grond waarvan de Commissie een openbare raadpleging zou organiseren over het toepassen van de e-privacyrichtlijn op alle particuliere netwerken, met inbreng van de EDPS, gegevensbeschermingsautoriteiten en andere betrokken partijen. Voorts kan in die overweging gepreciseerd worden dat de Commissie op grond van deze openbare raadpleging een geschikt voorstel moet doen om de categorieën van entiteiten die onder de e-privacyrichtlijn vallen te verruimen of te beperken.

72. Voorts moeten de artikelen van de e-privacyrichtlijn gewijzigd worden, zodat in alle bepalingen van het dispositief naast de openbare netwerken ook de voor het publiek toegankelijke particuliere netwerken worden vermeld.

IV. VERWERKING VAN VERKEERSGEGEVENS VOOR BEVEILIGINGSDOELEINDEN

73. Tijdens het wetgevingsproces in verband met de herziening van de e-privacyrichtlijn hebben ondernemingen die beveiligingsdiensten verstrekken, te kennen gegeven dat in de e-privacyrichtlijn een bepaling moet worden opgenomen waarbij het verzamelen van verkeersgegevens met het oog op een doeltreffende onlinebeveiliging wordt gewettigd.

([17]) Een typisch voorbeeld zijn lokale netwerken (LAN's).
([18]) Zie voetnoot 16.

74. Hiertoe heeft het EP amendement 181 aangenomen ter invoeging van een nieuw artikel 6, lid 6 bis, waarbij het verwerken van persoonsgegevens voor beveiligingsdoeleinden uitdrukkelijk wordt toegestaan: „*Onverminderd de naleving van andere bepalingen dan die van artikel 7 van Richtlijn 95/46/EG en artikel 5 van deze richtlijn, kunnen verkeersgegevens worden verwerkt in het legitieme belang van de datacontroleur die technische maatregelen uitvoert om de netwerk- en informatieveiligheid, zoals gedefinieerd in artikel 4, letter c), van Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 houdende oprichting van het Europees Agentschap voor netwerk- en informatieveiligheid, te verzekeren van een openbare of particuliere elektronische communicatiedienst, een dienst van de informatiemaatschappij of de daarmee samenhangende terminal- en elektronische communicatieapparatuur, uitgezonderd wanneer deze belangen moeten wijken voor het hogere belang van de fundamentele rechten en vrijheden van de datasubjecten. Deze verwerking wordt beperkt tot wat voor deze beveiliging strikt noodzakelijk is.*".

75. De Commissie heeft dit amendement in haar gewijzigd voorstel in beginsel aanvaard, maar heeft door het schrappen van de woorden „*Onverminderd [...] van deze richtlijn*" een kernbepaling weggenomen die tot doel had de naleving van de andere bepalingen van de richtlijn te garanderen. De Raad heeft een gewijzigde versie hiervan aangenomen, waarin de belangrijke bepalingen inzake bescherming en het afwegen van belangen die in amendement 181 zijn ingebouwd, nog verder worden uitgehold: „*Verkeersgegevens mogen worden verwerkt voor zover dit strikt noodzakelijk is ter waarborging […] van de netwerk- en informatiebeveiliging, als omschreven in artikel 4, punt c), van Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging.*".

76. Zoals hieronder zal worden toegelicht is artikel 6, lid 6 bis, overbodig en kan het aanleiding geven tot misbruik, in het bijzonder indien het wordt aangenomen zonder de belangrijke waarborgen, het zinsonderdeel betreffende het naleven van de andere bepalingen van de richtlijn en de belangenafweging. De EDPS beveelt dan ook aan dit nieuwe lid te verwerpen, of er ten minste voor te zorgen dat een bepaling over dit onderwerp de verschillende waarborgen biedt die in het door het EP aangenomen amendement 181 waren vervat.

Rechtsgronden voor het verwerken van verkeersgegevens die in de huidige wetgeving betreffende gegevensbescherming van toepassing zijn op elektronische communicatiediensten en andere verantwoordelijken voor de verwerking van gegevens

77. In hoeverre het verwerken van verkeersgegevens door verstrekkers van openbare elektronische-communicatiediensten wettelijk is, is bepaald in artikel 6 van de e-privacyrichtlijn, dat het verwerken van verkeersgegevens beperkt tot een klein aantal doeleinden, zoals facturering, interconnectie en marketing. Verwerking kan alleen onder bepaalde voorwaarden, zoals toestemming van de betrokken personen in geval van marketing. Andere voor de verwerking verantwoordelijken, zoals aanbieders van diensten van de informatiemaatschappij, kunnen verkeersgegevens verwerken in het kader van artikel 7 van de gegevensbeschermingsrichtlijn, waarin is bepaald dat voor de verwerking verantwoordelijken persoonsgegevens kunnen verwerken indien zij ten minste aan een van de in het artikel opgesomde rechtsgrondslagen, ook rechtsgronden genoemd, voldoen.

78. Een voorbeeld van zo'n rechtsgrondslag is artikel 7, punt a), van de gegevensbeschermingsrichtlijn, waarin is bepaald dat de betrokkene toestemming moet verlenen. Een onlinekleinhandel, bijvoorbeeld, die verkeersgegevens wil verwerken met het oog op de verzending van reclame- of marketingmateriaal, zal hiervoor de toestemming van de betrokkene moeten vragen. Een andere in artikel 7 vastgestelde rechtsgrondslag maakt het mogelijk in bepaalde omstandigheden verkeersgegevens te verwerken voor beveiligingsdoeleinden (bijvoorbeeld beveiligingsondernemingen die beveiligingsdiensten aanbieden). Basis hiervoor is artikel 7, punt f), waarin is bepaald dat het verwerken van persoonsgegevens door voor de verwerking verantwoordelijken is toegestaan wanneer dit „*noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene […] niet prevaleren.*". In de gegevensbeschermingsrichtlijn wordt niet nader vermeld in welke situaties het verwerken van persoonsgegevens aan deze bepaling zou voldoen. Die afweging wordt per geval gemaakt door voor de verwerking verantwoordelijken, vaak in overeenstemming met nationale gegevensbeschermingsautoriteiten en andere autoriteiten.

79. Bekeken moet worden hoe artikel 7 van de gegevensbeschermingsrichtlijn zich verhoudt tot het voorgestelde artikel 6, lid 6 bis, van de e-privacyrichtlijn. In het nieuwe artikel 6, lid 6 bis, wordt nader bepaald onder welke omstandigheden aan het bepaalde in artikel 7, punt f), zou worden voldaan, in die zin dat het verwerken van verkeersgegevens met het oog op netwerk- en informatiebeveiliging wordt toegestaan (nieuw artikel 6, lid 6 bis) op grond van het gerechtvaardigde belang van de voor verwerking verantwoordelijke (artikel 7, punt f).

80. De EDPS acht het voorgestelde artikel 6, lid 6 bis, overbodig en nutteloos. Vanuit juridisch oogpunt is het in beginsel niet nodig vast te stellen of een specifieke vorm van gegevensverwerking (in dit geval de verwerking van verkeersgegevens voor beveiligingsdoeleinden), aan het bepaalde in artikel 7, punt f), van de gegevensbeschermingsrichtlijn voldoet, in welk geval op grond van artikel 7, punt a), toestemming van de betrokkene noodzakelijk kan zijn. Zoals reeds eerder opgemerkt, wordt deze afweging in de meeste gevallen op uitvoeringsniveau gemaakt, door voor de verwerking verantwoordelijken (ondernemingen) in overleg met gegevensbeschermingsautoriteiten, en, waar nodig, door de rechter. In het algemeen kan volgens de EDPS in specifieke gevallen worden aangenomen dat de rechtmatige verwerking van verkeersgegevens voor beveiligingsdoeleinden, waarbij de fundamentele

rechten en vrijheden van betrokkenen niet worden geschaad, aan de voorschriften van artikel 7, punt f), van de gegevensbeschermingsrichtlijn zal voldoen, en dat derhalve niets deze vorm van verwerking in de weg staat. Bovendien zijn er geen precedenten, noch in de gegevensbeschermings-, noch in de e-privacyrichtlijn, van afzonderlijke of specifieke bepalingen voor aparte categorieën van gegevensverwerkingsactiviteiten die aan het bepaalde in artikel 7, punt f), zouden voldoen, en dergelijke uitzonderingen zijn ook niet nodig gebleken. Integendeel, in vele gevallen kan dit soort activiteiten probleemloos onder de bestaande tekst worden gevat. Een wettelijke bepaling ter bevestiging van deze evaluatie is dus in beginsel overbodig.

Artikel 6, lid 6 bis: de versies van het EP, de Raad en de Commissie

81. Hoewel het door het EP aangenomen amendement 181 overbodig is, moet worden beklemtoond dat in deze bepaling tot op zekere hoogte de in de gegevensbeschermingswetgeving vastgestelde beginselen met betrekking tot de persoonlijke levenssfeer en de gegevensbescherming terug te vinden zijn. Amendement 181 kan dus van belang zijn voor de gegevensbescherming en de persoonlijke levenssfeer, indien bijvoorbeeld de woorden „in specifieke gevallen" worden toegevoegd, zodat het artikel selectief kan worden toegepast, of indien een specifieke bewaartermijn wordt vastgesteld.

82. Amendement 181 bevat een aantal positieve elementen. Er wordt bevestigd dat verwerking moet voldoen aan alle andere gegevensbeschermingsbeginselen die van toepassing zijn op het verwerken van persoonsgegevens („*Onverminderd de naleving van andere bepalingen […] van Richtlijn 95/46/EG en […] van deze richtlijn*"). Voorts heeft amendement 181 niet alleen tot doel het verwerken van verkeersgegevens voor beveiligingsdoeleinden toe te staan, maar wordt ook een evenwicht vastgesteld tussen de belangen van de entiteit die verkeersgegevens verwerkt, en de belangen van de personen wier gegevens verwerkt worden, zodat deze vorm van gegevensverwerking alleen kan plaatsvinden op voorwaarde dat de belangen van de fundamentele rechten en vrijheden van de betrokkenen niet voor de belangen van de gegevensverwerkende entiteit moeten wijken („*uitgezonderd wanneer deze belangen moeten wijken voor het hogere belang van de fundamentele rechten en vrijheden van de betrokkene*"). Dit zinsdeel is essentieel, omdat op grond hiervan het verwerken van verkeersgegevens wel in specifieke gevallen kan worden toegestaan, maar een entiteit deze bepaling niet kan inroepen om massaal verkeersgegevens te gaan verwerken.

83. De door de Raad aangepaste versie van het amendement bevat lovenswaardige elementen: zo zijn de woorden „*strikt noodzakelijk*" gehandhaafd, wat het beperkte toepassingsgebied van dit nieuwe lid beklemtoont. Daar staat tegenover dat in de versie van de Raad de hogergenoemde garanties op het gebied van gegevensbescherming en persoonlijke levenssfeer zijn geschrapt. Hoewel in beginsel de algemene bepalingen inzake gegevensbescherming van toepassing zijn, ongeacht of er telkens uitdrukkelijk naar verwezen wordt, kan artikel 6, lid 6 bis, in de versie van de Raad geïnterpreteerd worden als werd volledige discretionaire bevoegdheid verleend om verkeersgegevens te verwerken, zonder dat daarbij de garanties op het gebied van gegevensbescherming en persoonlijke levenssfeer die in de regel bij het verwerken van verkeersgegevens van toepassing zijn, in acht moeten worden genomen. Verkeersgegevens, zo kan op basis hiervan geargumenteerd worden, mogen verzameld, opgeslagen en verder gebruikt worden zonder inachtneming van de gegevensbeschermingsbeginselen en de specifieke verplichtingen die anders op verantwoordelijke partijen van toepassing zijn, zoals het kwaliteitsbeginsel, of de verplichting tot eerlijke en rechtmatige verwerking en tot vertrouwelijke en veilige bewaring van de gegevens. Bovendien staat in de versie van de Raad niets over toepasselijke gegevensbeschermingsbeginselen betreffende termijnen voor het opslaan van informatie, noch betreffende specifieke termijnen voor dit lid, wat kan leiden tot de interpretatie dat het verzamelen en verwerken van verkeersgegevens voor beveiligingsdoeleinden voor onbepaalde termijn is toegestaan.

84. Voorts heeft de Raad in bepaalde delen van de tekst de bescherming van de persoonlijke levenssfeer afgezwakt, door een potentieel ruimere formulering. Het schrappen van „*het legitieme belang van de voor de verwerking verantwoordelijke*", bijvoorbeeld, doet vragen rijzen over de categorieën van entiteiten die zich op deze uitzondering zouden kunnen beroepen. Deze wijziging mag er in geen geval toe leiden dat voor gebruikers of rechtspersonen een achterpoortje in de wetgeving wordt opengezet.

85. Recente ervaringen in het EP en de Raad tonen aan dat het moeilijk is bij wet te bepalen in welke mate en onder welke voorwaarden het verwerken van gegevens voor beveiligingsdoeleinden wettelijk kan plaatsvinden. Het is weinig waarschijnlijk dat bestaande of toekomstige artikelen de evidente risico's op een te ruime toepassing van de uitzondering (voor andere dan louter beveiligingsdoeleinden of door entiteiten die niet van de uitzondering gebruik zouden mogen maken) zouden wegnemen,waarmee niet gezegd is dat deze vorm van verwerking in geen geval mag plaatsvinden. Maar of en in hoeverre dit kan worden toegestaan, kan beter beoordeeld worden op uitvoeringsniveau. Entiteiten die tot dergelijke verwerking willen overgaan, zouden het toepassingsgebied en de voorwaarden moeten bespreken met de gegevensbeschermingsautoriteiten en, eventueel, met de Groep artikel 29. Als alternatief kan in de e-privacyrichtlijn een artikel worden opgenomen waarbij het verwerken van verkeersgegevens voor beveiligingsdoeleinden wordt toegestaan, mits de gegevensbeschermingsautoriteiten hiertoe uitdrukkelijk toestemming verlenen.

86. Aangezien artikel 6, lid 6 bis, enerzijds risico's inhoudt voor het fundamentele recht van natuurlijke personen op gegevensbescherming en een persoonlijke levenssfeer, en anderzijds, zoals in dit advies is uitgelegd, vanuit juridisch oogpunt overbodig is, acht de EDPS het verkieslijk het voorgestelde artikel 6, lid 6 bis, in zijn geheel te schrappen.

87. Wordt er, in weerwil van de aanbeveling van de EDPS, toch een bepaling in de zin van één van de huidige versies van artikel 6, lid 6 bis, aangenomen, dan moeten hierin in ieder geval de bovengenoemde garanties op het gebied van gegevensbescherming worden opgenomen. De bepaling moet ook correct worden geïntegreerd in de bestaande structuur van artikel 6, bij voorkeur als een nieuw lid 2 bis.

V. **DE MOGELIJKHEID VOOR RECHTSPERSONEN OM INBREUKEN OP DE E-PRIVACYRICHTLIJN VOOR DE RECHTER TE BRENGEN**

88. Het EP heeft amendement 133 aangenomen, dat de mogelijkheid die aanbieders van internettoegang en andere rechtspersonen, zoals consumentenorganisaties, zou worden geboden om inbreuken op de e-privacyrichtlijn voor de rechter te brengen, uitbreidt tot alle bepalingen van de richtlijn ([19]). Jammer genoeg heeft noch de Commissie, noch de Raad dit geaccepteerd. De EDPS acht dit amendement zeer positief en beveelt aan het te handhaven.

89. Om dit amendement naar waarde te kunnen schatten dient voor ogen te worden gehouden dat de schade die een individu kan worden berokkend op het gebied van de persoonlijke levenssfeer en gegevensbescherming, op zich meestal niet volstaat om een rechtszaak te beginnen. Mensen stappen in de regel niet individueel naar de rechter omdat ze spam hebben ontvangen, of omdat hun naam ten onrechte is opgenomen in een abonneelijst. Met dit amendement kunnen consumenten- en werknemersorganisaties die de collectieve verdediging van consumentenbelangen op zich nemen, namens de consument de zaak aanhangig maken bij een rechtbank. Verwacht mag bovendien worden dat een grotere diversiteit in de handhavingsmechanismen een betere naleving in de hand zal werken, en de daadwerkelijke toepassing van de bepalingen van de e-privacyrichtlijn ten goede zal komen.

90. Er zijn precedenten in het wetgevingskader van een aantal lidstaten waar nu reeds een mogelijkheid tot collectieve actie wordt voorzien, zodat consumenten of belangengroepen een schadevergoeding kunnen eisen van de partij die de schade heeft veroorzaakt.

91. In een aantal lidstaten biedt de wetgeving inzake mededinging ([20]) consumenten en belangengroepen (naast de *getroffen concurrent*) de mogelijkheid een rechtszaak te beginnen tegen de entiteit die de inbreuk heeft begaan. De *ratio* van deze benadering is dat ondernemingen die de mededingingswetten overtreden, hier in de regel voordeel uit halen, omdat consumenten die slechts geringe schade ondervinden, meestal niet geneigd zijn hiervoor naar de rechter te stappen. Dit geldt *mutatis mutandis* ook voor gegevensbescherming en de persoonlijke levenssfeer.

92. Nog belangrijker is dat een nieuwe bepaling die rechtspersonen, zoals consumentenorganisaties en aanbieders van openbare elektronische-communicatiediensten, de mogelijkheid biedt de zaak aanhangig te maken bij de rechter, de positie van de consument versterkt en de naleving van gegevensbeschermingswetgeving in het algemeen ten goede komt. Een hoger risico op gerechtelijke vervolging zal ondernemingen die de wet niet naleven, ertoe aanzetten meer te investeren in de naleving van de gegevensbeschermingswetgeving, wat op lange termijn tot een betere bescherming van de persoonlijke levenssfeer en van consumenten zal leiden. De EDPS roept het EP en de Raad dan ook op een bepaling aan te nemen die rechtspersonen de mogelijkheid biedt elke inbreuk op een bepaling van de e-privacyrichtlijn voor de rechter te brengen.

([19]) Artikel 13, lid 6, van de eerste lezing van het EP.

([20]) Zie, bijvoorbeeld, artikel 8 van de Duitse wet betreffende oneerlijke concurrentie (*Gesetz gegen unlauteren Wettbewerb* of UWG).

VI. **CONCLUSIE**

93. Het gemeenschappelijk standpunt van de Raad, de eerste lezing van het EP en het gewijzigd voorstel van de Commissie bevatten, in verschillende mate, positieve elementen die de bescherming van de persoonlijke levenssfeer en de persoonsgegevens van natuurlijke personen ten goede zouden komen.

94. De EDPS ziet evenwel ook ruimte voor verbetering, in het bijzonder wat het gemeenschappelijk standpunt betreft, waarin de Raad jammer genoeg een aantal van de amendementen van het EP die een passende bescherming van de persoonlijke levenssfeer en de persoonsgegevens van natuurlijke personen moeten helpen garanderen, niet heeft overgenomen. De EDPS dringt er bij het EP en de Raad op aan, de garanties met betrekking tot de persoonlijke levenssfeer die in de eerste lezing van het EP worden geboden, te herstellen.

95. De EDPS acht het voorts raadzaam een aantal van de bepalingen van de richtlijn te stroomlijnen, met name de bepalingen betreffende inbreuken op de beveiliging: kennisgeving van inbreuken zal volgens de EDPS alleen ten volle effect sorteren indien het wetgevingskader van meet af aan goed is opgesteld. Tot slot beveelt de EDPS aan, een aantal bepalingen van de richtlijn beter en duidelijker te formuleren.

96. De EDPS dringt er derhalve bij het EP en de Raad op aan, meer te doen om sommige bepalingen van de e-privacyrichtlijn te verbeteren en te verduidelijken, en te opteren voor heropneming van de door het EP in eerste lezing aangenomen amendementen ter waarborging van een passend niveau van bescherming van de persoonlijke levenssfeer en van gegevens. De punten 97, 98, 99 en 100 bevatten een samenvatting van de vraagstukken die ter bespreking voorliggen, en een aantal aanbevelingen en redactionele voorstellen. De EDPS roept alle betrokkenen op hiermee rekening te houden in de aanloop naar de definitieve aanneming van de e-privacyrichtlijn.

Inbreuk op de beveiliging

97. Het Europees Parlement, de Commissie en de Raad hebben de kennisgeving van inbreuken op de beveiliging op verschillende manieren benaderd. De drie voorgestelde regelingen verschillen van elkaar onder meer wat betreft de entiteiten waarvoor de verplichting geldt, het criterium of de drempel voor kennisgeving, de betrokkenen die recht hebben op kennisgeving enz. Het EP en de Raad moeten alles in het werk stellen om tot een solide wetgevingskader te komen, en daarom wordt het volgende aanbevolen:

— de definitie van een inbreuk op de beveiliging in de teksten van het EP, de Raad en de Commissie moet *behouden* blijven: zij is ruim genoeg om de meeste situaties te bestrijken waarin kennisgeving van een inbreuk op de beveiliging gerechtvaardigd zou zijn

— wat betreft de entiteiten die onder de voorgestelde meldingsplicht zouden moeten vallen: aanbieders van diensten van de informatiemaatschappijen dienen in het toepassingsgebied te worden opgenomen. Onlinekleinhandels, onlinebanken, onlineapotheken kunnen evenzeer, of zelfs meer dan telecommunicatiebedrijven, het slachtoffer van dergelijke inbreuken zijn. Burgers zullen een melding verwachten, niet alleen wanneer een aanbieder van internettoegang het slachtoffer is van een inbreuk op de beveiliging, maar vooral wanneer dit hun onlinebank of onlineapotheek overkomt.

— Wat de drempel voor kennisgeving betreft is het criterium van het gewijzigde voorstel (meer dan „*een zeer geringe kans op schade*") geschikt voor een werkbare regeling. Wel is het zaak het woord „schade" zo ruim te definiëren dat alle vormen van negatieve impact op de persoonlijke levenssfeer of andere rechtmatige belangen van natuurlijke personen eronder vallen. Anders is een nieuw criterium te verkiezen, waarbij kennisgeving verplicht zou zijn wanneer „*redelijkerwijs mag worden aangenomen dat de inbreuk negatieve gevolgen zal hebben voor natuurlijke personen*". Het door de Raad voorgestelde criterium, dat de inbreuk de persoonlijke levenssfeer *ernstig* moet schenden, zou natuurlijke personen onvoldoende bescherming bieden, omdat volgens dit criterium de gevolgen voor de persoonlijke levenssfeer „ernstig" moeten zijn. Dit laat bovendien ruimte voor subjectieve evaluatie.

— Wat betreft de afweging of een betrokken entiteit personen van een inbreuk in kennis moet stellen, kan het ontegenzeglijk positief zijn hierbij een bevoegde instantie te betrekken, maar het is niet denkbeeldig dat dit onpraktisch en moeilijk zal blijken te zijn, en dat hieraan middelen voor andere belangrijke prioriteiten zullen worden opgeofferd. Indien de bevoegde instanties niet in staat zijn bijzonder snel te reageren, vreest de EDPS dat deze regeling natuurlijke personen zelfs minder bescherming zal bieden dan voorheen, en dat zij voor de instanties zelf te belastend zal zijn. Alles bij elkaar genomen adviseert de EDPS dan ook een regeling *in te voeren* waarbij de afweging of tot een melding moet worden overgegaan, door de betrokken entiteit zelf wordt gemaakt.

— Om autoriteiten in staat te stellen toezicht te houden op de door de betrokken entiteiten gemaakte afwegingen met betrekking tot de meldingsplicht, moeten de volgende garanties *worden ingebouwd*:

  — de entiteiten *moeten verplicht worden* alle inbreuken die aan het vastgestelde criterium voldoen, aan de autoriteiten te melden.

  — aan de autoriteiten *moet* een toezichtsrol *worden toegekend* zodat zij selectief en dus efficiënt kunnen optreden. Met het oog hierop de volgende bepaling invoegen: „*Indien de betrokken abonnee of persoon nog niet van de inbreuk in kennis is gesteld, kan de bevoegde nationale instantie, na beoordeling van de aard van de inbreuk, de aanbieders van openbare elektronische-communicatiediensten en de aanbieders van diensten van de informatiemaatschappij verzoeken dit alsnog te doen.*"

  — *er moet* een nieuwe bepaling *worden aangenomen* waarbij entiteiten verplicht worden een volledig en gedetailleerd intern evaluatieverslag bij te houden. Die bepaling zou als volgt kunnen luiden: „*Aanbieders van openbare elektronische-communicatiediensten en aanbieders van diensten van de informatiemaatschappij maken en bewaren een uitvoerig verslag over alle inbreuken op de beveiliging die zich hebben voorgedaan, de nuttige technische informatie in dit verband en de corrigerende maatregelen die zij hebben genomen. In dit verslag wordt ook verwezen naar alle meldingen die aan de betrokken abonnees of personen, alsook aan de bevoegde nationale instanties zijn gedaan, met vermelding van de datum en inhoud ervan. Het verslag wordt desgevraagd aan de bevoegde nationale instantie voorgelegd.*"

— Met het oog op een coherente toepassing van het kader voor inbreuken op de beveiliging *moet* de Commissie *worden gemachtigd* om, na overleg met de EDPS, de Groep artikel 29 en andere betrokkenen, technische uitvoeringsmaatregelen aan te nemen.

— Wat betreft de natuurlijke personen aan wie de inbreuk moet worden gemeld, *moet* de terminologie van de Commissie of het EP („betrokken personen" of „getroffen gebruikers") *worden gebruikt*, omdat deze alle natuurlijke personen bestrijkt van wie de persoonsgegevens zijn gecompromitteerd.

Voor het publiek toegankelijke particuliere netwerken

98. Vaak worden communicatiediensten niet via openbare netwerken ter beschikking van het publiek gesteld, maar via particulier geëxploiteerde netwerken (bijvoorbeeld wifipunten in hotels, luchthavens), waarvan inderdaad kan worden beweerd dat ze buiten het toepassingsgebied van de richtlijn vallen. Het EP wil middels amendement 121 (artikel 3) het toepassingsgebied van de richtlijn verruimen tot openbare en particuliere communicatienetwerken, alsook tot voor het publiek toegankelijke particuliere netwerken. Het EP en de Raad wordt in dit verband het volgende aanbevolen:

— de kern van amendement 121 *behouden*, maar *herformuleren* zodat het toepassingsgebied van de e-privacyrichtlijn alleen verruimd wordt tot „*de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare en voor het publiek toegankelijke particuliere netwerken in de Gemeenschap, …*". Louter particulier geëxploiteerde netwerken (in tegenstelling tot voor het publiek toegankelijke particuliere netwerken) zouden niet expliciet onder het toepassingsgebied vallen.

— alle bepalingen in het dispositief dienovereenkomstig *aanpassen,* zodat naast openbare netwerken expliciet melding wordt gemaakt van voor het publiek toegankelijke particuliere netwerken.

— de volgende definitie *invoegen*: *„voor het publiek toegankelijk particulier netwerk: een particulier geëxploiteerd netwerk waartoe het grote publiek in de regel onbeperkt toegang heeft, al dan niet tegen betaling of in samenhang met andere diensten of aanbiedingen, behoudens aanvaarding van de geldende voorwaarden*". Dit biedt meer rechtszekerheid aangaande de entiteiten die onder het nieuwe toepassingsgebied vallen.

— een nieuwe overweging *aannemen* op grond waarvan de Commissie een openbare raadpleging zou organiseren over de toepassing van de e-privacyrichtlijn op alle particuliere netwerken, met inbreng van de EDPS, de Groep artikel 29 en alle betrokkenen. Preciseren dat de Commissie op grond van deze openbare raadpleging een geschikt voorstel moet doen om de categorieën van entiteiten die onder de e-privacyrichtlijn vallen te verruimen of te beperken.

Verwerking van verkeersgegevens voor beveiligingsdoeleinden

99. Het EP heeft in eerste lezing amendement 181 (artikel 6, lid 6 bis) aangenomen, waarbij de verwerking van verkeersgegevens voor beveiligingsdoeleinden wordt toegestaan. De Raad heeft in zijn gemeenschappelijk standpunt een nieuwe versie aangenomen, waarin een aantal garanties met betrekking tot de persoonlijke levenssfeer wordt afgezwakt. De EDPS beveelt het EP en de Raad in dit verband het volgende aan:

— dit artikel volledig *verwerpen* omdat het overbodig is en, in geval van misbruik, een groot risico zou kunnen inhouden voor de bescherming van gegevens en de persoonlijke levenssfeer van natuurlijke personen;

— indien toch een variant van de huidige versie van artikel 6, lid 6 bis, wordt aangenomen, de in dit advies besproken garanties met betrekking tot gegevensbescherming (te vergelijken met die van het amendement van het EP) *in de tekst opnemen.*

Juridische actie tegen inbreuken op de e-privacyrichtlijn

100. Het Parlement heeft amendement 133 (artikel 13, lid 6) aangenomen dat rechtspersonen de mogelijkheid biedt om elke inbreuk op een bepaling van de e-privacyrichtlijn voor de rechter te brengen. Dit amendement is jammer genoeg niet overgenomen door de Raad. De Raad en het EP wordt aanbevolen:

— *hun goedkeuring te hechten* aan de bepaling waarbij rechtspersonen zoals consumenten- en werknemersorganisaties elke inbreuk op een bepaling van de e-privacyrichtlijn (en niet alleen op de bepalingen betreffende spam, zoals op dit ogenblik in het gemeenschappelijk standpunt en het gewijzigd voorstel wordt voorgesteld) voor de rechter kunnen brengen. Meer diversiteit in de handhavingsmechanismen zal een betere naleving en de daadwerkelijke toepassing van de bepalingen van de e-privacyrichtlijn ten goede komen.

De zaak tot een goed einde brengen

101. Het EP en de Raad hebben met betrekking tot al deze vraagstukken de opdracht goede regels en bepalingen op te stellen die werkbaar en functioneel zijn en verenigbaar met de rechten van natuurlijke personen op een persoonlijke levenssfeer en op bescherming van hun gegevens. De EDPS heeft goede hoop dat de betrokken partijen hun uiterste best zullen doen om deze zaak tot een goed einde te brengen, en hoopt dat dit advies hiertoe zal bijdragen.

Gedaan te Brussel, 9 januari 2009.

Peter HUSTINX

Europees Toezichthouder voor gegevensbescherming