



**00350/09/NL
WP 159**

**Advies 1/2009 over de voorstellen tot wijziging van Richtlijn 2002/58/EG betreffende
privacy en elektronische communicatie (e-privacyrichtlijn)**

Goedgekeurd op 10 februari 2009

Deze groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. De groep is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat C (Civiel recht, grondrechten en burgerschap) van het directoraat-generaal Justitie, vrijheid en veiligheid van de Europese Commissie, B-1049 Brussel, België, bureau LX-46 01/06.

Website: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp118_nl.pdf

Inhoudsopgave

1. Achtergrond.....	3
2. kennisgeving van inbreuk op persoonsgegevens	4
2.1. Opmerkingen.....	4
2.2. Vrijstellingen van de kennisgevingsplicht	6
3. Verkeersgegevens.....	7
3.1. Verwerking van verkeersgegevens voor beveiligingsdoeleinden	7
4. IP-adressen	8
5. Informatie van gegevensbeschermingsautoriteiten	9
6. Ongevraagde communicatie.....	10
7. Browserinstellingen.....	10
8. Rechtsvorderingen van natuurlijke of rechtspersonen	11
9. Andere kwesties	11
10. Conclusie.....	12

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995¹,

Gelet op artikel 29 en artikel 30, lid 1, onder a), en lid 3, van die richtlijn, alsook op artikel 15, lid 3, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002,

Gelet op artikel 255 van het Verdrag tot oprichting van de Europese Gemeenschap en op Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie,

Gelet op het reglement van orde van de Groep,

HEEFT HET VOLGENDE ADVIES GOEDGEKEURD:

1. ACHTERGROND

Op 13 november 2007 heeft de Commissie een voorstel aangenomen voor een richtlijn ("het voorstel") tot wijziging van Richtlijn 2002/58/EG (e-privacyrichtlijn) betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten ("de kaderrichtlijn").

In eerste lezing heeft het Europees Parlement amendementen op het voorstel goedgekeurd ("de amendementen van het Parlement"), waarop de Europese Commissie op 6 november 2008 heeft geantwoord in COM(2008) 723 definitief ("de opmerkingen van de Commissie").

Vervolgens bereikte de Raad van de Europese Unie op 27 november 2008 een politiek akkoord ("het akkoord van de Raad").

De Groep Gegevensbescherming artikel 29 wil de amendementen van het Parlement, de opmerkingen van de Commissie en het akkoord van de Raad van commentaar voorzien.

De Groep wijst erop dat zij al twee adviezen heeft goedgekeurd over de voorstellen tot wijziging van het regelgevingskader voor elektronische communicatienetwerken en -diensten (Advies 8/2006 van 26 september 2006² en Advies 2/2008 van 15 mei 2008³).

Hoewel het de Groep verheugt dat rekening is gehouden met een aantal van haar eerdere aanbevelingen, wil zij de aandacht vestigen op enige essentiële aspecten van zaken die aan de orde zijn gesteld na de eerste lezing van het Parlement en van de Raad; de Groep zal niet alle opmerkingen uit haar eerdere adviezen herhalen; deze blijven echter wel van toepassing.

¹ PB L 281 van 23.11.1995, blz. 31, http://ec.europa.eu/justice_home/fsj/privacy/

² http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_nl.pdf

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_nl.pdf

2. KENNISGEVING VAN INBREUK OP PERSOONSGEGEVENS

2.1. Opmerkingen

De Groep steunt ten volle het voorstel om artikel 4 van de e-privacyrichtlijn aan te scherpen door verstrekkers van openbaar beschikbare elektronische communicatiediensten ertoe te verplichten inbreuken op de beveiliging te melden. Kennisgevingen van inbreuken kunnen een belangrijk instrument worden waarmee de gegevensbeschermingsautoriteiten er gericht en doeltreffender op kunnen toezien dat de dienstverleners zich houden aan de verplichting om passende beveiligingsmaatregelen te treffen.

Met betrekking tot kennisgevingen van inbreuk op persoonsgegevens beveelt de Groep algemeen gesteld de volgende aanpak aan:

- de bevoegde nationale regelgevende instantie wordt in kennis gesteld wanneer het risico zich voordoet van nadelige gevolgen⁴ voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens;
- het is belangrijk dat getroffen gebruikers onmiddellijk door de dienstverleners in kennis worden gesteld wanneer een inbreuk op de beveiliging waarschijnlijk nadelige gevolgen⁵ heeft voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens, onverminderd de mogelijkheid van de bevoegde nationale regelgevende instantie om informatie over de inbreuk openbaar te maken en de dienstverlener ertoe te dwingen informatie over de inbreuk bekend te maken,
- elke dienstverlener dient een register⁶ bij te houden van alle inbreuken op persoonsgegevens.

De Groep stelt tevens vast dat de drie voorstellen (van het Parlement, de Commissie en de Raad) beveiliging en inbreuken op persoonsgegevens behoorlijk verschillend benaderen, met name wat betreft:

- het toepassingsgebied van de verplichting (dat in de amendementen van het Parlement alle diensten van de informatiemaatschappij omvat, maar wat de Raad en Commissie betreft tot openbaar beschikbare elektronische communicatiediensten beperkt is); de Groep is er uitgesproken voorstander van, de verplichting uit te breiden tot alle diensten van de informatiemaatschappij;
- de entiteit die bevoegd is te beslissen tot kennisgeving aan personen (voor het Parlement en de Commissie de bevoegde instantie, maar wat de Raad betreft de dienstverlener);

⁴ Het risico van nadelige gevolgen moet worden beoordeeld aan de hand van elementen als de hoeveelheid en de aard van de gegevens waarop de inbreuk betrekking heeft, alsook de impact van de inbreuk op een individu (bijvoorbeeld identiteitsdiefstal, financieel verlies, verlies van economische activiteit of van werkgelegenheidsmogelijkheden, of een combinatie van deze of soortgelijke omstandigheden). De kwalitatieve en kwantitatieve criteria ter beoordeling van de impact van nadelige gevolgen moeten nader worden vastgesteld in het kader van de comitéprocedure. Hierbij moet ervoor worden gewaakt dat de autoriteiten met kleine zaken worden overspoeld en dat burgers onnodig worden gealarmeerd.

⁵ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_nl.pdf

⁶ Deze registers moeten worden opgezet volgens een vast model, zodat zij kunnen worden gecontroleerd door de bevoegde nationale regelgevende instantie.

- de soorten inbreuken die moeten worden gemeld (volgens het voorstel van het Parlement en de opmerkingen van de Commissie alle inbreuken, maar volgens het akkoord van de Raad alleen ernstige inbreuken);
- en de te informeren personen (abonnees en andere personen wat betreft het Parlement en de Commissie, maar alleen abonnees als het aan de Raad ligt).

Toepassingsgebied van de kennisgeving: diensten van de informatiemaatschappij

De Groep is een uitgesproken voorstander van de amendementen 187/rev en 184 van het Parlement. **Kennisgevingen van inbreuk op persoonsgegevens moeten ook verplicht worden voor andere diensten van de informatiemaatschappij, aangezien deze diensten een steeds grotere rol spelen in het dagelijks leven van de Europese burger** en hierbij steeds meer persoonsgegevens worden verwerkt. Online-transacties, zoals elektronisch bankieren, medische dossiers in de privésector en internetwinkelen zijn maar een paar voorbeelden van diensten die gepaard kunnen gaan met inbreuken op persoonsgegevens die aanzienlijke risico's meebrengen voor een groot aantal Europese burgers. Als deze verplichtingen worden beperkt tot openbaar beschikbare elektronische communicatiediensten, worden zij slechts van toepassing op een zeer beperkt aantal belanghebbenden. Kennisgevingen van inbreuk op persoonsgegevens – een middel om personen te beschermen tegen de risico's van identiteitsdiefstal, financieel verlies, verlies van economische activiteit of van werkgelegenheidsmogelijkheden of lichamelijke schade – zouden hierdoor veel minder effect hebben.

De Groep betreurt het dan ook ten zeerste dat dit voorstel geen steun heeft gekregen van de Commissie en de Raad; zij wijst erop dat een aantal bepalingen uit de e-privacyrichtlijn al van toepassing is op zaken die strikt genomen niet onder elektronische communicatiediensten vallen⁷.

Verantwoordelijkheid en criteria voor kennisgeving

De betrokken dienstverleners moeten verantwoordelijk zijn voor de beoordeling van de risico's die voortvloeien uit inbreuken op persoonsgegevens; zij zijn het best in staat om op basis van de door de autoriteiten vastgestelde beoordelingsregels snel te bepalen of de betrokken personen in kennis gesteld moeten worden. **Onverminderd hun verplichting om elke inbreuk waarbij het risico van nadelige gevolgen bestaat aan de bevoegde nationale regelgevende instanties te melden, moeten dienstverleners vaststellen of abonnees of andere personen op de hoogte moeten worden gebracht. Om ervoor te zorgen dat het publiek juiste en relevante voorlichting krijgt, kunnen de bevoegde nationale regelgevende instanties zo nodig beslissen de inbreuk openbaar te maken, en kunnen zij de dienstverlener ertoe dwingen informatie over de inbreuk bekend te maken.**

⁷ Sommige bepalingen van de e-privacyrichtlijn, zoals artikel 5, lid 3, (cookies en spyware) en artikel 13 (ongevraagde berichten) zijn al van algemene aard en niet alleen van toepassing op elektronische communicatiediensten.

Deze mogelijke uitbreiding tot buiten het strikte toepassingsgebied van openbaar beschikbare elektronische communicatiediensten is ook voorstelbaar in andere situaties. De Commissie heeft namelijk voorgesteld om het toepassingsgebied van artikel 5, lid 3, uit te breiden tot gevallen waarin cookies en spyware meegeleverd worden met media als cd-roms of USB-sticks, die niet onder openbaar beschikbare elektronische communicatiediensten vallen.

Aangezien de kennisgeving wordt verricht door de dienstverlener, **is het van groot belang dat de richtlijn waarborgen bevat om te verzekeren dat inbreuken niet zijn verzwegen**, dat de inbreuk correct is beoordeeld en dat betrokken personen altijd in kennis zijn gesteld wanneer dit nodig was.

De autoriteiten zullen meer kennisgevingen ontvangen, zodat zij erop kunnen toezien dat dienstverleners betrokken personen in kennis stellen. Het model van de kennisgeving dient op Europees niveau te worden geharmoniseerd en moet objectieve en duidelijke criteria bevatten ter beoordeling van de ernst van nadelige gevolgen van de inbreuk. Voorts moet de bevoegde nationale regelgevende autoriteit controleren of de dienstverlener de inbreuk correct heeft beoordeeld en of er naar aanleiding van de inbreuk passende maatregelen zijn getroffen. **Om te voorkomen dat inbreuken worden verzwegen is het ten slotte van groot belang dat de bevoegde nationale regelgevende instantie op grond van de richtlijn strafrechtelijke financiële sancties (boetes)⁸ mag opleggen, wanneer een dienstverlener personen of de nationale bevoegde instantie niet of onjuist in kennis stelt van inbreuken op persoonsgegevens.**

De soorten inbreuken waarvan individuele betrokkenen in kennis moeten worden gesteld: het begrip 'nadelige gevolgen'

Het doet de Groep genoegen dat er een nieuwe definitie van "inbreuk op persoonsgegevens" is opgenomen in artikel 2⁹, zoals voorgesteld in de opmerkingen van de Commissie¹⁰.

De Groep stelt evenwel vast dat in de drie voorstellen verschillend wordt verwoord welke inbreuken aan betrokkenen moeten worden gemeld. Derhalve **beveelt de Groep aan om betrokkenen in kennis te stellen van inbreuken op de beveiliging die nadelige gevolgen zouden kunnen hebben voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens.** Overweging 29 van het akkoord van de Raad bevat ter zake een aantal nuttige voorbeelden.

In kennis te stellen personen

De Groep stelt tevreden vast dat er in de amendementen van het Parlement¹¹ wordt voorgesteld in overweging 29 te verwijzen naar "individuele abonnee", "getroffen gebruikers" en "bevoegde nationale instantie". In het akkoord van de Raad worden de kennisgevingen beperkt tot "abonnees", waardoor de getroffen personen niet op de hoogte worden gebracht van bepaalde inbreuken op persoonsgegevens beschreven in Advies 2/2008.

2.2. Vrijstellingen van de kennisgevingsplicht

De Groep erkent dat kennisgevingen van inbreuken informatie moeten bevatten over de omstandigheden van de inbreuk, onder meer over de vraag of de persoonsgegevens al dan niet met behulp van encryptie of andere middelen waren beschermd; deze informatie is van groot belang voor de bevoegde nationale regelgevende instantie wanneer zij moet bepalen welke

⁸ Het is de Groep bekend dat het Parlement, de Commissie en de Raad bepalingen van deze strekking hebben voorgesteld in een nieuw artikel 15 bis, lid 1.

⁹ Zie de opmerkingen van de Commissie over amendementen 187/rev en 184 van het Parlement.

¹⁰ Het begrip "inbreuk op persoonsgegevens" is echter algemeen en moet niet worden beperkt tot gegevensverwerking in verband met de verlening van openbaar beschikbare elektronische communicatiediensten; het begrip moet in elk geval ook betrekking hebben op diensten van de informatiemaatschappij.

¹¹ Amendement 183

actie ten aanzien van de dienstverlener er eventueel moet worden ondernomen naar aanleiding van een inbreuk.

De Groep is er echter geen voorstander van te voorzien in vrijstelling¹² van de kennisgevingsplicht voor gevallen waarin duidelijk is dat de dienstverlener "passende technologische beveiligingsmaatregelen heeft getroffen, en dat deze maatregelen werden toegepast op de gegevens die bij de inbreuk op de beveiliging betrokken waren." Een dergelijke bepaling zou de kwaliteit en het nut van de aan de getroffen personen verstrekte informatie aanzienlijk beperken. Getroffen gebruikers kunnen wellicht alleen passende stappen nemen om de risico's te verminderen waarmee zij te maken krijgen, wanneer zij toereikend zijn geïnformeerd. Derhalve **benadrukt de Groep het belang van het kennisgevingsmodel en hecht zij eraan dat er een risicobeoordeling wordt verricht om vast te stellen of burgers in kennis moeten worden gesteld, ongeacht de technische maatregelen die getroffen werden ter bescherming van hun gegevens.**

3. VERKEERSGEGEVENS

3.1. Verwerking van verkeersgegevens voor beveiligingsdoeleinden

In een nieuw artikel 6, lid 6 bis, stellen het Parlement, de Raad en de Commissie voor om een nieuwe uitzondering op te nemen in de e-privacyrichtlijn, om de verwerking van verkeersgegevens voor beveiligingsdoeleinden toe te staan.

De Groep is zich ervan bewust dat "aanbieders van beveiligingsdiensten" gebruikmaken van beveiligingsoplossingen¹³ (zoals antivirus- en antispamsoftware, firewalls en indringerdetectiesystemen) waarvoor verkeersgegevens moeten kunnen worden verwerkt ter bescherming van de persoonsgegevens van de gebruikers en ter beveiliging van de dienst zelf. Zij vreest echter dat de huidige formulering legitimiteit verleent aan grootschalige "deep packet inspection"¹⁴, zowel in het netwerk als in de apparatuur van de gebruiker, zoals diens ADSL-modem, terwijl het huidige juridisch kader al specificiert in welke gevallen gegevensverkeer mag worden verwerkt voor beveiligingsdoeleinden.

De rechtsgronden voor de verwerking van verkeersgegevens door openbaar beschikbare elektronische communicatiediensten en voor de verwerking van persoonsgegevens door de daarvoor verantwoordelijke zijn vervat in artikel 6 van de e-privacyrichtlijn en artikel 7 en artikel 17 van de richtlijn over gegevensbescherming. De mate waarin persoonsgegevens mogen worden verwerkt voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke is vastgelegd in artikel 7, onder f), van de richtlijn over gegevensbescherming; dit belang mag niet prevaleren boven de belangen en de fundamentele rechten en vrijheden van de betrokkene. De voor de verwerking verantwoordelijke dient krachtens artikel 17 van de richtlijn over gegevenbescherming ook *"passende technische en organisatorische maatregelen ten uitvoer [...] te leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, dan wel tegen enige andere vorm van onwettige*

¹² Zie overweging 29 van de amendementen van het Parlement (amendement 122) en de overwegingen 29 en 32 van het akkoord van de Raad.

¹³ In de eindapparatuur van de gebruiker of in het netwerk.

¹⁴ "Deep packet inspection" omvat uiterst invasieve technieken voor het volgen en traceren van gedragspatronen.

verwerking." De vastgestelde maatregelen moeten ook in verhouding staan tot risico's die de verwerking meebrengt en tot de aard van de te beschermen gegevens.

De Groep benadrukt ook dat de reikwijdte van amendement 180 van het Parlement is toegelicht in de opmerkingen van de Commissie. **De Werkgroep stelt vast dat uit de door de Commissie voorgestelde formulering glashelder blijkt dat de verwerking van verkeersgegevens onder de richtlijn over gegevensbescherming valt.** Aanbieders van beveiligingsdiensten dienen de nationale gegevensbeschermingsautoriteiten derhalve altijd in kennis te stellen wanneer dit nodig is, en ervoor te zorgen dat de betrokken personen hun rechten kunnen uitoefenen.

Ten slotte wijst de Groep erop dat er al verkeersgegevens voor beveiligingsdoeleinden worden verwerkt door lidstaten die specifieke maatregelen hebben genomen conform artikel 15, lid 1, van de e-privacyrichtlijn, op grond waarvan de lidstaten wettelijke maatregelen mogen treffen in afwijking van het beginsel dat verkeersgegevens¹⁵, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, moeten worden gewist of anoniem gemaakt, ter voorkoming van ongeoorloofd gebruik van het elektronische communicatiesysteem.

Om de hierboven uiteengezette redenen is **het voorstel voor een nieuw artikel 6, lid 6 bis, niet nodig.**

4. IP-ADRESSEN

Het Parlement en de Commissie stellen voor een nieuwe overweging (27 bis) over IP-adressen toe te voegen¹⁶.

De specifieke verwijzing naar het werk van de Groep in de opmerkingen van de Commissie valt in goede aarde. De Groep is echter geen voorstander van het voorstel om dit punt uitdrukkelijk in een richtlijn op te nemen.

In deze **blijft de Groep bij haar eerdere advies**¹⁷: *"Tenzij de internetdienstverlener dus met absolute zekerheid gegevens van niet-identificeerbare gebruikers kan onderscheiden, zal hij alle IP-informatie voor alle zekerheid als persoonsgegevens moeten behandelen."*

IP-adressen hebben meestal betrekking op identificeerbare personen. Identificeerbaar wil zeggen te identificeren door de aanbieder of op andere wijze, met behulp van bijkomende identificatiemiddelen zoals cookies, of in de interactie met internetdiensten waarbij de betrokkene expliciet of impliciet wordt geïdentificeerd.

In overweging 26 van de richtlijn over gegevensbescherming staat duidelijk dat *"moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren"*.

¹⁵ Vastgesteld in artikel 6, lid 1.

¹⁶ Amendement 185 van het Parlement.

¹⁷ Advies 4/2007 over het begrip persoonsgegeven en het advies over gegevensbescherming in verband met zoekmachines

Persoonsgegevens wordt in de richtlijn over gegevensbescherming omschreven als informatie "betreffende" een persoon, en er wordt vaak gebruik gemaakt van IP-adressen om gebruikers te herkennen en een aparte behandeling te geven, bijvoorbeeld door gericht te adverteren of een gebruikersprofiel bij te houden.

De Groep wil de Commissie wel ondersteunen bij de door het Parlement voorgestelde werkzaamheden inzake IP-adressen¹⁸, maar is net als de Commissie van mening dat een inhoudelijke bepaling in een richtlijn niet de meest aangewezen manier is om dit te regelen en dat een verplichte verslaggeving "voor doeleinden die niet onder het toepassingsgebied van deze richtlijn vallen", niet zinvol is.

5. INFORMATIE VAN GEGEVENSBEWAKERS

In eerste lezing heeft het Parlement amendement 136 op artikel 15 van de e-privacyrichtlijn goedgekeurd, dat vervolgens is gewijzigd in de opmerkingen van de Commissie. Volgens dit voorstel dienen alle aanbieders van telecommunicatiediensten en -netwerken en alle verleners van diensten van de informatiemaatschappij de bevoegde gegevensbeschermingsautoriteit in kennis te stellen van elk verzoek "ontvangen overeenkomstig lid 1"¹⁹, en moet de betrokken autoriteit elk verzoek onderzoeken en de bevoegde gerechtelijke autoriteiten in kennis stellen van de gevallen waarin naar haar oordeel de toepasselijke bepalingen van de nationale wet niet zijn nageleefd.

De voorgestelde kennisgevingsplicht is een nuttige aanvulling die ten goede komt aan de doorzichtigheid en de controle door de regelgevende instanties. Maar hoewel deze bepaling de gegevensbeschermingsautoriteiten veel betere toezichts- en handhavingsmogelijkheden biedt, waardoor beter kan worden gewaakt over de rechtmatigheid van de toegang tot informatie, leidt zij ook tot een administratieve last, zowel voor de betrokken ondernemingen als voor de gegevensbeschermingsautoriteiten. De Groep is dan ook bezorgd over het toenemend aantal te behandelen verzoeken van gerechtelijke autoriteiten²⁰ en over de nieuwe verantwoordelijkheid van gegevensbeschermingsautoriteiten om elk afzonderlijk gerechtelijk onderzoek te controleren. Hiervoor moeten de financiële en personele middelen van deze autoriteiten aanzienlijk worden uitgebreid.

Volgens de Groep zou een jaarlijkse meldplicht ook kunnen volstaan. De te melden gegevens zouden betrekking kunnen hebben op de interne procedures voor het beantwoorden van verzoeken om toegang tot persoonsgegevens van gebruikers, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en de eventuele moeilijkheden die zich hebben voorgedaan. Ook is het van groot belang een dergelijke meldplicht op EU-niveau te harmoniseren en uit te werken.

¹⁸ Amendementen 139 en 186/rev

¹⁹ Met daarin een beschrijving van de gegevensbewaringsverplichtingen vastgesteld in de richtlijn betreffende de bewaring van gegevens (2006/24/EG).

²⁰ Veel telecommunicatie-exploitanten ontvangen honderden verzoeken per dag.

6. ONGEVRAAGDE COMMUNICATIE

In amendement 131 van het Parlement wordt verduidelijkt dat de definitie van "e-mail" in artikel 2, onder h), ook van toepassing is op mms en vergelijkbare technologieën.

Ten eerste stelt de Groep vast dat overweging 40 van de e-privacyrichtlijn al duidelijk maakt dat deze definitie op sms van toepassing is²¹.

Ten tweede is het nodig om artikel 13, lid 1, aan te passen aan nieuwe technologieën, overeenkomstig het in overweging 4 vervatte beginsel²². De huidige formulering van artikel 13, lid 1, veronderstelt dat de betrokkene al is aangesloten op het netwerk waarmee het bericht (een telefoongesprek of een e-mail) wordt overgebracht. De bepaling heeft geen betrekking op gevallen waarin een gebruiker wordt uitgenodigd om zich aan te sluiten op een netwerk dat uitsluitend advertenties aanbiedt. Bluetooth-marketingapplicaties werken dikwijls op deze manier.

Het stemt de Groep dan ook tevreden dat de opmerkingen van de Commissie over het toepassingsgebied van artikel 13 voornamelijk het gebruik van het woord "communicatie" toelichten, en dat de nieuwe overweging verwijst naar "vergelijkbare technologieën". Zo wordt gewaarborgd dat voor Bluetooth-marketingapplicaties voorafgaande toestemming nodig is, in overeenstemming met de opmerkingen die de Groep in Advies 2/2008 maakte over de noodzaak "gebruikers van media voor draadloze kortereafstandscommunicatie [te] beschermen tegen ongewenste communicatie zoals in artikel 13 is gedefinieerd." Er zou ook uitdrukkelijk naar Bluetooth kunnen worden verwezen in overweging 40.

Ten derde neemt de Groep, haar opmerking in Advies 2/2008 over het gebruik van het begrip "abonnee" in artikel 13 gedachtig, tevreden kennis van de in het akkoord van de Raad voorgestelde formulering.

Zeer nuttig is ten slotte ook het voorstel van de Raad om artikel 13, lid 2, te wijzigen door de bepaling "elektronische contactgegevens [...] op het ogenblik dat zij worden verzameld" in te voegen. Zo wordt ondubbelzinnig duidelijk gemaakt op welk moment gebruikers in de gelegenheid moeten worden gesteld om bezwaar te maken tegen het gebruik van hun elektronische contactgegevens voor direct-marketing.

7. BROWSERINSTELLINGEN

De Groep is uitgesproken tegenstander van amendement 128 van het Parlement, dat inhoudt dat voorafgaande toestemming kan worden verkregen via de standaardinstellingen van de browser. Hoewel dit amendement is opgenomen in de opmerkingen van de Commissie en het akkoord van de Raad, wil de Groep er graag iets over opmerken.

²¹ Omschreven in artikel 2, onder h), van de e-privacyrichtlijn.

²² Hierin wordt gesteld dat de e-privacyrichtlijn "moet worden aangepast aan de ontwikkelingen op de markten en van de technologieën voor elektronische communicatiediensten, teneinde te voorzien in een gelijke mate van bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor gebruikers van openbaar beschikbare elektronische communicatiediensten, ongeacht de technologieën waarvan gebruik wordt gemaakt."

De Groep acht het niet alleen een formeel probleem dergelijk technologisch jargon op te nemen in de richtlijn - zij is ook bezorgd over de uitholling van het begrip toestemming en het daaruit voortvloeiende gebrek aan doorzichtigheid.

De meeste browsers werken met standaardinstellingen die ervoor zorgen dat de gebruikers niet worden geïnformeerd over pogingen om iets op te slaan op of toegang te verkrijgen tot hun eindapparatuur. De standaardinstellingen van browsers moeten "privacyvriendelijk" zijn, maar mogen geen middel zijn om de vrije, specifieke en op informatie berustende toestemming van de gebruiker te verkrijgen, zoals bedoeld in artikel 2, onder h), van de richtlijn over gegevensbescherming.

Ten aanzien van cookies is de Groep van mening dat de voor de verwerking van de cookies verantwoordelijke de gebruikers in zijn privacyverklaring moet informeren en niet mag afgaan op de (standaard-)instellingen van de browser. De gekozen formulering is overigens niet alleen van toepassing op de bestaande cookies, maar op iedere nieuwe technologie die kan worden ingezet om gedragspatronen te traceren van de gebruikers van een browser.

8. RECHTSVORDERINGEN VAN NATUURLIJKE OF RECHTSPERSONEN

De Groep steunt het voorstel van het Parlement²³ om in artikel 13, lid 6, te bepalen dat natuurlijke of rechtspersonen die worden getroffen door inbreuken op nationale, overeenkomstig de e-privacyrichtlijn vastgestelde bepalingen, dergelijke inbreuken bij de rechter aanhangig kunnen maken.

Deze bepaling zal de rechten van de gebruiker beslist ten goede komen en ertoe bijdragen dat de bedrijfstak betere beveiligingsmethoden ontwikkelt.

9. ANDERE KWESTIES

Ten slotte stelt de Groep tevreden vast dat:

- de wetgever phishing strafbaar wil stellen²⁴;
- de Commissie en de Raad rekening hebben gehouden²⁵ met het verzoek van de Groep om te worden geraadpleegd in het kader van de in artikel 4, lid 4, uiteengezette comitéprocedure;
- de Groep is betrokken bij de raadpleging overeenkomstig artikel 15a, lid 4;
- de Groep zal worden geraadpleegd bij de voorbereiding van het verslag over de toepassing van de gewijzigde e-privacyrichtlijn²⁶;
- de Commissie, de Raad en het Parlement willen verduidelijken dat de e-privacyrichtlijn van toepassing is op nieuwe technologieën, zoals RFID²⁷ en NFC, waarbij gebruik wordt gemaakt van contactloze identificatiesystemen op basis van radiofrequenties.

²³ Amendement nr. 133

²⁴ Amendement 132 van het Parlement.

²⁵ In haar opmerking bij amendement 127 van het Parlement.

²⁶ Amendement 139 en amendement 186/rev. van het Parlement.

²⁷ Artikel 3 en overweging 28.

10. CONCLUSIE

De Groep Gegevensbescherming artikel 29 geeft de Europese wetgevers, naast de andere punten die in dit advies aan de orde worden gesteld, vooral in overweging om het toepassingsgebied van de verplichting voor diensten van de informatiemaatschappij om kennis te geven van inbreuken op persoonsgegevens te verruimen, gelet op de enorme impact hiervan op de bescherming van persoonsgegevens van de Europese burger.

Gedaan te Brussel, 10.2.2009

*Voor de werkgroep
De voorzitter
Alex TÜRK*