Mr. drs. B. van der Sloot en F.J. Zuiderveen Borgesius***

De amendementen van de Richtlijn Burgerrechten op de e-Privacyrichtlijn

148

Trefwoorden:
opt-in, cookies, meldplicht datalekken, Richtlijn 2002/58/EG, Richtlijn 2009/136/EG

De e-Privacyrichtlijn, betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, is onlangs gewijzigd door de Richtlijn Burgerrechten. De wijzigingen worden in dit artikel benoemd en becommentarieerd. Enkele van de belangrijkste wijzigingen zijn de introductie van een opt-in-regel voor cookies, een meldplicht voor datalekken, de mogelijkheid voor providers om spammers in rechte aan te spreken en een artikel betreffende de implementatie en publiekrechtelijke handhaving van de e-Privacyrichtlijn.

1 Inleiding

De e-Privacyrichtlijn[1] is één van de basisteksten omtrent privacy en databescherming in de Europese Unie en bevat onder meer regelgeving met betrekking tot dataretentie, de veiligheid van netwerken, het gebruik van cookies en het tegengaan van spam. De e-Privacyrichtlijn complementeert de Algemene Privacyrichtlijn[2] op een aantal punten. Ook regelt de e-Privacyrichtlijn een aantal onderwerpen waar de Algemene Privacyrichtlijn over zwijgt. De e-Privacyrichtlijn uit 2002 is de opvolger van de ISDN-richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector,[3] die op vele punten aan modernisering toe was.[4] Nu de e-Privacyrichtlijn al acht jaar van kracht is en de digitale omgeving zich nog steeds in rap tempo ontwikkelt, is ook deze aan modernisering toe. De e-Privacyrichtlijnis hiervoor slechts eenmaal op een klein punt gewijzigd door de Dataretentierichtlijn uit 2006.[5] De Dataretentierichtlijn voegde in artikel 15 van de e-Privacyrichtlijnlid 1bis toe zodat lid 1 van artikel 15 van de e-Privacyrichtlijnniet van toepassing is op de Dataretentierichtlijn.

De Richtlijn Burgerrechten[6] uit november 2009 wijzigt de e-Privacyrichtlijn op tal van punten. Zij is onderdeel van de zogenoemde 'Telecoms Reform Package' dat voorziet in de algehele hervorming van de telecomregels die merendeels uit 2002 stammen.[7] Dit artikel richt zich op de tien amendementen van de Richtlijn Burgerrechten op de e-Privacyrichtlijn. Deze zullen in paragraaf 2 stuk voor stuk in een subparagraaf worden besproken. Eerst zal de nieuwe of gewijzigde tekst worden gepresenteerd, waarbij de wijzigingen in de tekst zijn vetgedrukt, daarna zal deze tekst van kort commentaar worden voorzien. Tot slot zullen in paragraaf 3 de belangrijkste

---

* **Bart van der Sloot is onderzoeker aan het Instituut voor Informatie Recht (IVIR) van de UvA. Hij werkt momenteel aan een commentaar op Richtlijn 2002/58/EG voor Concise European IT Law.**

** **Frederik Zuiderveen Borgesius is onderzoeksstudent aan het Instituut voor Informatie Recht (IVIR) van de UvA en werkzaam bij SOLV advocaten. Hij heeft twee onderzoeken afgerond naar Richtlijn 2009/136/EG.**

1 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juni 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie) (*PbEG* 2002, L 201/37). De (officieuze) geconsolideerde tekst is hier te vinden: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:NL:PDF>. (Alle in de voetnoten vermelde websites zijn voor het laatst geraadpleegd op 26 juni 2010.)

2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* 1995, L 281/31).

3 Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (*PbEG* 1998, L 24/1).

4 Zie voor een bespreking van de aanpassingen die de e-Privacyrichtlijn in 2002 met zich bracht onder meer W.A.M. Steenbruggen, 'Herziening hoofdstuk 11 Tw: Tijd voor een heroverweging?', *Computerrecht* 2003-1, p. 27-37; F. Debusseré, 'The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?', *International Journal of Law and Information Technology* 2005, Vol. 13, No. 1, p. 70-97; S.M. Kierkegaard, 'Lobbyism and the "opt in"/"opt out" cookie controversy. How the cookies (almost) crumbled: privacy & lobbyism', *Computer Law & Security Report* 2005-21, p. 310-322; C. Noorda, 'Nieuwe Europese regels voor cookies en spam', *Mediaforum* 2002-9, p. 272-277.

5 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (*PbEG* 2009, L 105/54). Wel moet worden opgemerkt dat deze Richtlijn tegen het fundamentele uitgangspunt van de bescherming van verkeers- en locatiegegevens van de e-Privacyrichtlijn ingaat, nu niet meer het verwijderen, maar het verplicht bewaren van gegevens wordt geregeld.

6 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (*PbEG* 2009, L 337/11).

7 Ten eerste vervangt Verordening 1211/2009 de European Regulators Group, die door de Commissie was geïnstalleerd om coöperatie en coördinatie tussen de nationale autoriteiten en de Commissie te bevorderen en een interne markt voor elektronische communicatienet-

wijzigingen worden samengevat en zullen er een aantal suggesties worden gedaan.

2 De amendementen van Richtlijn Burgerrechten op de e-Privacyrichtlijn

2.1 *Werkingssfeer en doelstelling*

Artikel 1 lid 1 wordt vervangen door:

'1. Deze Richtlijn *voorziet in de harmonisering van* de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden – met name het recht op een persoonlijke levenssfeer *en vertrouwelijkheid* – bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronische communicatieapparatuur en -diensten in de Gemeenschap.'

Artikel 1 betreft de werkingssfeer en de doelstelling van de Richtlijn. De Richtlijn Burgerrechten voegt aan de oorspronkelijke formulering '– met name het recht op een persoonlijke levenssfeer' toe 'en vertrouwelijkheid'. In plaats van 'Deze Richtlijn harmoniseert de regelgeving' wordt er nu gesproken van 'Deze Richtlijn voorziet in de harmonisering van de regelgeving'. Dit brengt geen substantiële wijziging met zich, maar voorziet slechts in een verduidelijking van de tekst.

2.2 *Definities*

Artikel 2 wordt als volgt gewijzigd:

letter c) wordt vervangen door 'locatiegegevens': gegevens die in een elektronisch communicatienetwerk *of door een elektronische communicatiedienst* worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven;[8]

letter e) wordt geschrapt;

de volgende letter wordt toegevoegd: *(i) 'inbreuk in verband met persoonsgegevens': een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Gemeenschap.*[9]

In de definitie van 'locatiegegevens' in artikel 2 onder c wordt aan 'in een elektronisch communicatienetwerk' toegevoegd 'of door een elektronische communicatiedienst'. Artikel 2 onder c van de Kaderrichtlijn[10] definieert een elektronische communicatiedienst als 'een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van [de Richtlijn Informatieprocedure II],[11] die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken.'[12] Een centraal element uit de definitie is dat de dienst geheel of hoofdzakelijk bestaat uit het overbrengen van signalen. Het gaat met andere woorden om een transmissiedienst. Typische voorbeelden van elektronische communicatiediensten zijn traditionele (spraak)telefoniediensten en het aanbieden van toegang tot het internet (internet access). Het aanbieden van content valt niet onder het begrip elektronische communicatiedienst.

Artikel 2 onder a van de Kaderrichtlijn definieert het begrip 'elektronisch communicatienetwerk' als volgt: 'de transmissiesystemen en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie'.

Doorgaans is de aanbieder van een elektronisch communicatienetwerk tevens de aanbieder van de elektronische communicatiedienst. Dit is echter niet altijd het geval. Aanbieders die zich bezighouden met resale of

---

werken en -diensten te creëren, door de Body of European Regulators for Electronic Communications (BEREC, <http://berec.europa.eu>). Hierdoor wordt de centralisatie van de bevoegdheden bevorderd, alhoewel veel van de macht in handen van de nationale autoriteiten blijft. Ten tweede wijzigt Richtlijn 2009/140/EG de Kaderrichtlijn (Richtlijn 2002/21/EG), de Toegangsrichtlijn (Richtlijn 2002/19/EG) en de Machtigingsrichtlijn (Richtlijn 2002/20/EG). Ten slotte wijzigt Richtlijn 2009/136/EG de Universele dienstrichtlijn (Richtlijn 2002/22/EG), de Verordening betreffende samenwerking met betrekking tot consumentenbescherming (Verordening EG nr. 2006/2004) en de e-Privacyrichtlijn.

8 Artikelen uit de Richtlijn worden letterlijk geciteerd; ten aanzien van het woord 'elektronische communicatienetwerk' is niet de spelling van de Richtlijn zelf, maar van de Telecommunicatiewet gevolgd, die spreekt van 'elektronisch communicatienetwerk'.

9 In de door de EG verspreidde (officieuze) geconsolideerde tekst is de definitie ingevoegd onder letter i. <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:NL:HTML>. De Richtlijn Burgerrechten vermeldt dat de definitie wordt ingevoegd onder letter h, terwijl letter h al de definitie van e-mail geeft.

10 Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten (Kaderrichtlijn) (*PbEG* 2002, L 108/33).

11 Richtlijn 98/34/EG van het Europees Parlement en de Raad van de Europese Unie van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (*PbEG* 1998, L 204/37).

12 Voor definities en begrippen die in de e-Privacyrichtlijn worden gebezigd dienen meerdere bronnen te worden geraadpleegd dan de e-Privacyrichtlijn zelf, zoals de Algemene Privacyrichtlijn en de Kaderrichtlijn.

wederverkoop van diensten van anderen kunnen aanbieders van een elektronische communicatiedienst zijn, terwijl zij niet tevens een elektronisch communicatienetwerk beheren. Hierbij valt te denken aan een bedrijf dat belminuten inkoopt bij KPN, waarbij het KPN is die het netwerk exploiteert. Door de wijziging vallen de verplichtingen die de e-Privacyrichtlijn oplegt ten aanzien van locatiegegevens ook op het bedrijf dat belminuten inkoopt bij KPN.

Letter E las: 'oproep: door middel van een openbare telefoondienst tot stand gebrachte verbinding die in real time tweeweg communicatie mogelijk maakt.' De definitie van oproep is verplaatst van de e-Privacyrichtlijn naar de Kaderrichtlijn.[13] Bovendien wordt de frase 'openbare telefoondienst' vervangen door 'een openbaar beschikbare elektronische communicatiedienst'. Verder komt de zinsnede 'in real time' te vervallen en wordt de term 'tweeweg communicatie' vervangen door 'tweewegspraakcommunicatie'.[14] Hiermee is de reikwijdte van deze definitie verruimd. Echter, Voice-over-IP-diensten ('VoIP-diensten') zoals Skype vallen niet onder het begrip elektronische communicatiedienst omdat zij zich niet bezighouden met transmissie. Indien met behulp van Skype een verbinding wordt gelegd met een vaste of mobiele telefoon, of andersom, valt de dienst wel onder het begrip elektronische communicatiedienst.

De definitie van het begrip 'inbreuk in verband met persoonsgegevens' is toegevoegd in artikel 2 onder i in verband met de invoering van een meldplicht met betrekking tot dergelijke inbreuken voor aanbieders van openbare elektronische communicatiediensten. Deze wordt hieronder behandeld in subparagraaf 2.4.

2.3 *Betrokken diensten*

Artikel 3 wordt vervangen door:

'Artikel 3 Betrokken diensten

Deze Richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische communicatiediensten over openbare communicatienetwerken in de Gemeenschap, *met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.*'

In artikel 3 zijn de woorden 'met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen' toegevoegd om zo de reikwijdte van de Richtlijn uit te breiden. Nu vallen bijvoorbeeld ook RFID-systemen (Radio Frequency Identification Devices) die gebruikmaken van radiofrequenties om gegevens op te vangen van RFID-chips onder de reikwijdte van de Richtlijn. Deze gegevens kunnen nadat ze zijn opgevangen, worden verstuurd over bestaande communicatienetwerken. RFID-systemen die aan openbare elektronische communicatienetwerken worden gekoppeld vallen nu ook onder de Richtlijn, waardoor de bepalingen in verband met veiligheidseisen, verkeers- en locatiegegevens en vertrouwelijkheid ook daarop van toepassing zijn.[15]

De oorspronkelijke leden 2 en 3 van artikel 3 zijn komen te vervallen. Ook daarmee is de reikwijdte van de Richtlijn vergroot. Leden 2 en 3 gaven de lidstaten de mogelijkheid om bepaalde eisen van de Richtlijn (in verband met nummeridentificatie en het doorschakelen van telefoongesprekken) niet van toepassing te verklaren op abonneelijnen die verbonden zijn met analoge centrales. Lidstaten hadden deze mogelijkheid echter slechts dan als het naleven van de eisen onevenredig veel economische middelen zou vergen of technisch onhaalbaar zou zijn. Thans is de Richtlijn zonder meer van toepassing op abonneelijnen die verbonden zijn met analoge centrales.

2.4 *Beveiliging van de verwerking*

Artikel 4 wordt als volgt gewijzigd:

De titel wordt vervangen door: 'Beveiliging van de verwerking';

Het volgende lid wordt ingevoegd:

'1bis Onverminderd Richtlijn 95/46/EG zorgen de in lid 1 bedoelde maatregelen ervoor dat in ieder geval:
- wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens;
- opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; en
- een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens;

De bevoegde nationale instanties kunnen de door de aanbieders van openbare elektronische communicatiediensten genomen maatregelen controleren en aanbevelingen formuleren over beste praktijken van het beveiligingspeil dat met deze maatregelen moet worden gehaald;'.

---

13 De definitie van 'oproep' wordt door Richtlijn 2009/140/EG geïntroduceerd in de Kaderrichtlijn artikel 2 onder s.

14 Zie ook Artikel 29 Werkgroep, *Advies 7/2000 over het door de Europese Commissie ingediende voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie van 12 juli 2000 COM(2000)38*, WP 36, Brussel: 2 november 2000, p. 8. Zie ook Artikel 29 Werkgroep, *Advies 2/2008 over de herziening van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-Privacyrichtlijn)*, WP 150, Brussel: 15 mei 2008, p. 4. (verder: 'Artikel 29 Werkgroep, WP 36, 2008').

15 Zie ook overweging 56 van de Richtlijn Burgerrechten; Europese Commissie, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* (COM(2007)96 final), Brussel: 15 maart 2007, p. 6; Europese Toezichthouder voor gegevensbescherming, *Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een richtlijn van het Europees Parlement en de Raad tot wijziging van met name Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)*, Brussel: 18 juli 2008 (*PbEG* 2008, C 181/01), par. II.1 (i) (verder: 'EDPS, Eerste advies').

De volgende leden worden ingevoegd:

'3. In geval van een inbreuk in verband met persoonsgegevens stelt de aanbieder van openbare elektronische communicatiediensten de bevoegde nationale instantie zonder onnodige vertraging in kennis van de inbreuk in verband met persoonsgegevens.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens en persoonlijke levenssfeer van een abonnee of een individuele persoon stelt de aanbieder ook de abonnee of de individuele persoon in kwestie onverwijld van de inbreuk in kennis.

Inkennisstelling van een betrokken abonnee of individuele persoon van een inbreuk op persoonsgegevens is niet vereist wanneer de aanbieder tot voldoening van de bevoegde instantie heeft aangetoond dat hij de gepaste technische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft.

Onverminderd de verplichting van de aanbieder om de betrokken abonnees en de individuele personen in kwestie in kennis te stellen, indien de aanbieder de abonnee of individuele persoon niet reeds in kennis heeft gesteld van de inbreuk in verband met persoonsgegevens, kan de bevoegde nationale instantie hem, na te hebben bezien of en welke ongunstige gevolgen uit de inbreuk voortvloeien, verzoeken dat te doen.

In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk op persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten. De kennisgeving aan de bevoegde nationale instantie bevat bovendien een omschrijving van de gevolgen van de inbreuk en van de door de aanbieder voorgestelde of getroffen maatregelen om de inbreuk in verband met persoonsgegevens aan te pakken.

4. Afhankelijk van eventuele technische tenuitvoerleggingsmaatregelen overeenkomstig lid 5 kunnen de bevoegde nationale instanties richtsnoeren en, waar nodig, instructies uitvaardigen betreffende de omstandigheden waarin de kennisgeving van de inbreuk in verband met persoonsgegevens door aanbieders noodzakelijk is, het voor deze kennisgeving toepasselijke formaat, alsmede de manier waarop de kennisgeving geschiedt. Tevens kunnen zij bijhouden of aanbieders aan hun kennisgevingsverplichtingen overeenkomstig dit lid hebben voldaan en, zo niet, dan leggen zij sancties op.

Aanbieders houden een zodanige inventaris bij van inbreuken op persoonsgegevens, o.m. de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, dat de bevoegde nationale instanties kunnen nagaan of de bepalingen van lid 3 worden nageleefd. De inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens.

5. Teneinde een samenhangende tenuitvoerlegging van de in de leden 2, 3 en 4 bedoelde maatregelen te waarborgen, kan de Commissie, na raadpleging van het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), de bij artikel 29 van Richtlijn 95/46/EG ingestelde werkgroep voor de bescherming van personen in verband met de verwerking van persoonsgegevens en de Europese Toezichthouder voor gegevensbescherming, technische uitvoeringsmaatregelen aannemen in verband met, onder meer, de omstandigheden, het formaat en de procedures die gelden voor de in dit artikel bedoelde informatieverstrekkings- en kennisgevingseisen. De Commissie betrekt bij het aannemen van die maatregelen alle relevante belanghebbenden, met name om informatie in te winnen over de beste technische en economische methoden die beschikbaar zijn voor de tenuitvoerlegging van dit artikel.

Deze maatregelen, die niet-essentiële onderdelen van deze Richtlijn beogen te wijzigen door haar aan te vullen, worden vastgesteld volgens de in artikel 14bis, lid 2, bedoelde regelgevingsprocedure met toetsing.'

Artikel 4 betreffende de beveiliging van de verwerking is uitgebreid van twee naar vijf leden. In artikel 1bis worden specifieke eisen toegevoegd aan de reeds bestaande algemene eis van lid 1 dat een aanbieder van openbare elektronische communicatiediensten (verder: 'Aanbieder') ervoor zorg moet dragen dat er passende technische en organisatorische maatregelen worden getroffen om de veiligheid van zijn diensten te garanderen.[16] Aanbieders moeten er in ieder geval voor zorgen dat (i) alleen gemachtigd personeel toegang heeft tot persoonsgegevens, (ii) persoonsgegevens worden beschermd en (iii) een beveiligingsbeleid wordt ingevoerd.[17] De bevoegde nationale instanties krijgen de bevoegdheid de genomen maatregelen te controleren en aanbevelingen te formuleren over het minimum beveiligingspeil.[18]

Er zijn drie bronnen waaruit verplichtingen met betrekking tot het veiligheidsbeleid kunnen blijken. Ten eerste schrijft artikel 17 van de Algemene Privacyrichtlijn voor dat de voor verwerking van persoonsgegevens verantwoordelijke passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen ten uitvoer dient te leggen. Ten tweede formuleert artikel 4 lid 1bis een drietal eisen. Tot slot kunnen de bevoegde nationale instanties aanbevelingen formuleren over de

16 Zie voor eisen aan de veiligheid en de integriteit van netwerken en diensten ook Hoofdstuk IIIbis van de vernieuwde Kaderrichtlijn (Richtlijn 2002/21/EG).
17 Zie ook overweging 57 van de Richtlijn Burgerrechten.
18 Zie ook overweging 60 van de Richtlijn Burgerrechten.

te nemen maatregelen en het beveiligingspeil waarnaar met deze maatregelen wordt gestreefd.[19]

De belangrijkste verandering ten aanzien van artikel 4 is de introductie van een meldplicht voor inbreuken in verband met persoonsgegevens in lid 3. Het begrip 'inbreuk in verband met persoonsgegevens' is gedefinieerd door het eerder genoemde artikel 2 onder h. Aanbieders[20] zijn verplicht om dergelijke 'datalekken' aan de bevoegde nationale instantie te melden. In gevallen waarin schade dreigt, dienen ook de degenen op wie de gegevens betrekking hebben te worden ingelicht. Indien Aanbieders niet aan deze verplichtingen voldoen zijn de nationale toezichthouders bevoegd sancties op te leggen.

De tweede zin van lid 3 schrijft voor dat de Aanbieder een abonnee of een natuurlijke persoon onverwijld in kennis stelt indien een inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben ten aanzien van hun persoonsgegevens of de persoonlijke levenssfeer. Het is aan de Aanbieder om te bepalen of een inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben. Een inbreuk moet als schadelijk voor de persoonsgegevens of het privéleven van een abonnee of persoon worden beschouwd, wanneer er bijvoorbeeld identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering of aantasting van de reputatie, met betrekking tot de levering van openbare communicatiediensten in de Gemeenschap het gevolg ervan kan zijn.[21]

De kennisgeving moet informatie bevatten over de door de aanbieder van de dienst genomen maatregelen om de inbreuk aan te pakken, evenals aanbevelingen voor de betrokken abonnee of persoon.[22] Er mogen aan abonnees geen kosten in rekening worden gebracht voor het verschaffen van informatie over veiligheidsrisico's.[23] De Aanbieder moet de aard van de inbreuk aan de abonnee melden, en de Aanbieder moet bijvoorbeeld een telefoonnummer en een e-mailadres vermelden waar de abonnee advies kan vragen.

Een datalek hoeft niet aan abonnees te worden gemeld als de Aanbieder kan aantonen dat hij gepaste technische beschermingsmaatregelen heeft genomen. Volgens de vierde zin van lid 3 maken dergelijke technologische beschermingsmaatregelen de gegevens onbegrijpelijk voor eenieder die geen recht heeft op toegang daartoe. Als alle gegevens onleesbaar gemaakt zijn door middel van bijvoorbeeld encryptie hoeft een datalek derhalve niet aan abonnees te worden gemeld. Als een Aanbieder een inbreuk niet heeft gemeld aan de abonnees omdat hij van mening was dat het onwaarschijnlijk was dat hieruit ongunstige gevolgen zouden voortvloeien, kan de bevoegde nationale instantie hem alsnog opdragen dat te doen.

De bevoegde nationale instanties zijn bevoegd richtsnoeren en instructies uit te vaardigen over de kennisgeving aan abonnees. Verder zijn zij bevoegd bij te houden of Aanbieders aan hun meldplicht hebben voldaan en indien zij in gebreke zijn gebleven om sancties op te leggen. De bevoegde nationale instanties en andere relevante nationale organen moeten over afdoende bevoegdheden en middelen beschikken om inbreuken daadwerkelijk aan een onderzoek te onderwerpen, inclusief de bevoegdheid om in verband met klachten alle benodigde relevante informatie op te vragen en sancties op te leggen in geval van niet-naleving.[24] De Richtlijn maakt niet duidelijk op welk soort sancties wordt gedoeld.

Op grond van lid 5 kan de Europese Commissie, na raadpleging van het Europees Agentschap voor netwerken informatiebeveiliging (ENISA),[25] de Artikel 29 Werkgroep[26] en de Europese Toezichthouder voor gegevensbescherming (EDPS),[27] technische uitvoeringsmaatregelen aannemen in verband met, onder meer, de omstandigheden, het formaat en de procedures die gelden voor de in dit artikel bedoelde informatieverstrekkings- en kennisgevingseisen. De Commissie kan maatregelen vaststellen volgens de in artikel 14bis lid 2 bedoelde regelgevingsprocedure met toetsing.[28]

Opmerkelijk is dat de in dit artikel geregelde verplichtingen in de e-Privacyrichtlijn is geplaatst en niet in de Algemene Privacyrichtlijn. Hierdoor vallen de verplichtingen ten aanzien van datalekkage slechts op elektronische communicatiediensten en niet op overige dienstaanbieders.

2.5 *Vertrouwelijk karakter van de communicatie (cookies)*

In artikel 5 wordt lid 3 vervangen door:

'3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering

19 Nu de Richtlijn spreekt over 'bevoegde nationale instanties' zijn de lidstaten vrij om het nationale 'College bescherming persoonsgegevens', de nationale 'OPTA' of een nieuwe instantie deze bevoegdheid toe te kennen. Indien de Europese regelgever de nationale 'OPTA's had willen aanwijzen zou gebruik zijn gemaakt van het begrip 'nationale regelgevende instanties' (artikel 2 onder f van de Kaderrichtlijn).
20 In deze situatie betreft het vooral internet service providers die toegang verschaffen tot het internet. Voor andere partijen die betrokken zijn bij internet, zoals banken, webwinkels, webhosters en aanbieders van websites, geldt de meldplicht niet.
21 Overweging 61 van de Richtlijn Burgerrechten.
22 Overweging 61 van de Richtlijn Burgerrechten.
23 Overweging 20 van de e-Privacyrichtlijn.
24 Overweging 69 van de Richtlijn Burgerrechten.
25 <www.enisa.europa.eu>.
26 <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm>.
27 <www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=nl>.
28 Zie par. 2.8 van dit artikel over artikel 14bis lid 2.

van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.'

Lid 3 van artikel 5, waaraan overweging 66 van de Richtlijn Burgerrechten invulling geeft, bevat een nieuwe regeling over onder meer cookies en software zoals adware en spyware.[29] Deze mogen slechts worden geplaatst indien de betrokken abonnee of gebruiker toestemming heeft verleend na te zijn voorzien van duidelijke en volledige informatie. Er zijn twee uitzonderingen op deze regel. Ten eerste hoeft een website-exploitant geen toestemming te vragen als een cookie wordt geplaatst met als enige doel de uitvoering van de verzending van communicatie. Er hoeft derhalve geen toestemming te worden gevraagd indien het plaatsen van een cookie nodig is in verband met de inlogprocedure van een onlinebank. Ten tweede hoeft er geen toestemming te worden gevraagd als een cookie strikt noodzakelijk is om een uitdrukkelijk gevraagde dienst te leveren. De inhoud van een virtueel winkelmandje kan derhalve ook zonder de toestemming van een klant worden opgeslagen via een cookie.

Er geldt nu, in tegenstelling tot het oude artikel, een opt-in-regel voor cookies en ad- en spyware. Deze in het bovenstaande artikel vervatte regel wordt echter genuanceerd door een overweging. Deze leest dat de wijze waarop informatie wordt verstrekt en het recht van weigering wordt aangeboden zo gebruikersvriendelijk mogelijk dient te zijn. Overweging 66 bepaalt: 'Wanneer dit technisch mogelijk en doeltreffend is, kan, overeenkomstig de desbetreffende bepalingen van [de Algemene Privacyrichtlijn], de toestemming van de gebruiker met verwerking worden uitgedrukt door gebruik te maken van de desbetreffende instellingen van een browser of een andere toepassing'. Bovendien hoeft de vereiste informatie en het recht van weigering slechts éénmaal per website te worden aangeboden.[30] Opmerkelijk is dat alhoewel uit overweging 66 lijkt te volgen dat toestemming voor cookies geautomatiseerd (via browserinstellingen) kan worden verkregen, een dergelijke regeling voor het verschaffen van informatie ontbreekt.[31]

2.6 *Verkeersgegevens*

Artikel 6 lid 3 wordt vervangen door:

'3. De aanbieder van een openbare elektronische communicatiedienst mag ten behoeve van de marketing van elektronische communicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn *voorafgaande* toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.'

Artikel 6 regelt de verwerking van verkeersgegevens. Verkeersgegevens zijn gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.[32] Op grond van artikel 6 lid 1 moeten verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronische communicatienetwerk of -dienst, wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie, worden gewist of geanonimiseerd, onverminderd de leden 2, 3 en 5, alsmede artikel 15 lid 1.

Lid 3 schrijft voor dat verkeersgegevens slechts gebruikt mogen worden voor marketing of diensten met toegevoegde waarde met toestemming van de abonnee of gebruiker. De oorspronkelijke zinsnede van lid 3 'daartoe zijn toestemming heeft gegeven' leest thans 'daartoe zijn voorafgaande toestemming heeft gegeven'. De achterliggende reden voor deze wijziging is enigszins onduidelijk. Zowel 'voorafgaande toestemming' als 'toestemming' lijken in dit artikel op voorafgaande toestemming te duiden. Dit zou ervoor pleiten om de wijziging simpelweg als een nadere verduidelijking te zien. Artikel 13 spreekt tevens van 'voorafgaande toestemming' en deed dit zowel voor als na de wijziging van Richtlijn 2009/136/EG. Anderzijds spreekt het nieuw ingevoegde artikel 5 lid 3 simpelweg van 'toestemming', wat op een verschil tussen 'toestemming' en 'voorafgaande toestemming' zou kunnen duiden. Wellicht kan dit verschil echter worden verklaard door het feit dat in artikel 5 lid 3 tevens gewag wordt gemaakt van een aan de toestemming voorafgaande informatievoorziening. Het meest waarschijnlijk is dat de toevoeging van het woord 'voorafgaande' moet worden gezien als een verduidelijking en niet als een aanvulling.

2.7 *Ongewenste communicatie (spam)*

Artikel 13 wordt vervangen door het volgende:

'Artikel 13 Ongewenste communicatie

1. Het gebruik van automatische oproep- *en communicatie*systemen zonder menselijke tussenkomst (automati-

29 Adware is software die automatisch advertenties toont of download nadat de software is geïnstalleerd. Adware verzamelt vaak gegevens over het klikgedrag van internetgebruikers. Spyware is software die informatie vergaart over een computergebruiker en deze doorstuurt naar een derde. Overweging 65 van de Richtlijn Burgerrechten bepaalt dat niet relevant is hoe dit soort software op de computer van de gebruiker wordt geplaatst; ook als deze wordt verspreid via cd's, cd-rom's of USB-sticks is het artikel van toepassing.

30 Overweging 25 van de e-Privacyrichtlijn.

31 Zie voor een uitgebreide bespreking van artikel 5 lid 3 van de vernieuwde e-Privacyrichtlijn: Artikel 29 Werkgroep, *Opinion 2/2010 on online behavioural advertising,* WP 171, Brussel: 22 juni 2010.

32 Artikel 2 onder b van de e-Privacyrichtlijn.

sche oproepapparaten), fax of e-mail met het oog op direct marketing kan alleen worden toegestaan met betrekking tot abonnees *of gebruikers* die daarin vooraf hebben toegestemd.

2. Onverminderd lid 1 kan een natuurlijke of rechtspersoon die van zijn klanten elektronische contactgegevens voor e-mail verkrijgt in het kader van de verkoop van een product of een dienst, overeenkomstig Richtlijn 95/46/EG, die elektronische contactgegevens gebruiken voor direct marketing van eigen gelijkaardige producten of diensten mits de klanten duidelijk en expliciet de gelegenheid wordt geboden kosteloos en op gemakkelijke wijze bezwaar te maken tegen het gebruik van die elektronische contactgegevens *op het ogenblik dat zij worden verzameld* en, ingeval de klant zich in eerste instantie niet tegen dat gebruik heeft verzet, bij elke boodschap.

3. De lidstaten nemen passende maatregelen om ervoor te zorgen dat ongevraagde communicatie met het oog op direct marketing in andere dan de in de leden 1 en 2 genoemde gevallen niet toegestaan is zonder toestemming van de betrokken abonnees *of gebruikers*, of ten aanzien van abonnees of gebruikers die dergelijke communicatie niet wensen te ontvangen, waarbij de keuze tussen deze mogelijkheden door de nationale wetgeving wordt bepaald, *met dien verstande dat beide mogelijkheden voor de abonnee of gebruiker kosteloos moeten zijn.*

4. Het is in ieder geval verboden *e-mail te verzenden met het oog op direct marketing* waarbij de identiteit van de afzender namens wie de *communicatie plaatsvindt, wordt gemaskeerd of verborgen, die in strijd is met artikel 6 van Richtlijn 2000/31/EG, en zonder dat een geldig adres wordt vermeld* waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten, *of e-mail die ontvangers aanmoedigt websites te bezoeken die in strijd zijn met dat artikel.*

5. Leden 1 en 3 gelden voor abonnees die natuurlijke personen zijn. De lidstaten zorgen er, in het kader van het Gemeenschapsrecht, en het toepasselijk nationaal recht tevens voor dat de rechtmatige belangen van andere abonnees dan natuurlijke personen met betrekking tot ongewenste communicatie voldoende zijn beschermd.

6. Onverminderd de administratieve voorzieningen die onder meer overeenkomstig artikel 15bis, lid 2, kunnen worden genomen, zorgen de lidstaten ervoor dat natuurlijke of rechtspersonen die een rechtmatig belang hebben bij de bestrijding van inbreuken op nationale, overeenkomstig dit artikel vastgestelde bepalingen, inclusief aanbieders van elektronische communicatiediensten die hun rechtmatige ondernemingsbelangen of de belangen van hun klanten beschermen, rechtsvorderingen voor dergelijke inbreuken kunnen instellen. De lidstaten kunnen tevens specifieke voorschriften vaststellen inzake sancties voor aanbieders van elektronische communicatiediensten die door nalatigheid bijdragen tot inbreuken op overeenkomstig dit artikel aangenomen nationale bepalingen.'

Dit artikel vervangt het oude artikel 13 in zijn geheel. Alleen lid 6 is echter geheel nieuw, leden 1 tot en met 4 worden gedeeltelijk gewijzigd. In lid 1 wordt ten opzichte van het oude artikel na 'tot abonnees' toegevoegd 'of gebruikers'. De nieuwe formulering brengt met zich dat niet alleen degene die een abonnement heeft afgesloten door dit artikel wordt beschermd, maar dat ook andere gebruikers, bijvoorbeeld familieleden of werknemers, onder de reikwijdte van dit artikel vallen. De definitie van 'gebruiker' uit artikel 2 onder a van de e-Privacyrichtlijn wijkt af van de definitie uit artikel 2 onder h van de Kaderrichtlijn, zodat in de e-Privacyrichtlijn rechtspersonen niet onder de definitie van 'gebruiker' vallen en ook degene die slechts een verzoek heeft gedaan om gebruik te maken van een openbare elektronische communicatiedienst niet onder de reikwijdte van de definitie valt. Artikel 2 onder k van de Kaderrichtlijn stelt dat een abonnee een natuurlijk- of een rechtspersoon is die partij is bij een overeenkomst met de aanbieder van openbare elektronische communicatiediensten voor de levering van die diensten, terwijl lid 5 van het hier besproken artikel 13 bepaalt dat ten aanzien van leden 1 en 3 slechts natuurlijke personen als abonnees gelden. De behandeling van de complexe vraag hoe een direct marketeer dient aan te tonen dat elke gebruiker en niet slechts de op een dienst geabonneerde toestemming heeft verleend valt buiten het bestek van dit artikel.

Ook wordt in lid 1 'oproepsystemen' vervangen door 'oproep- en communicatiesystemen'. Hiermee is gekozen voor een meer techniekneutrale formulering.[33] De term 'communicatiesysteem' wordt overigens nergens gedefinieerd. Uit overweging 67 van de Richtlijn Burgerrechten blijkt dat maatregelen om abonnees te beschermen tegen indringing in hun privéleven door ongevraagde mededelingen voor directmarketingdoeleinden door middel van e-mail ook van toepassing zijn op SMS, MMS en andere soortgelijke toepassingen. Eén van de doelstellingen van deze wijziging was om ook spam verstuurd via Bluetooth, zogenoemde Bluespam, onder de reikwijdte van dit artikel te brengen.[34] Het is echter twijfelachtig of dit is gelukt aangezien artikel 2 onder D van de e-Privacyrichtlijn leest dat onder 'communicatie' wordt verstaan informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen, terwijl dit niet het geval is ten aanzien van Bluetooth-applicaties waarbij er vanuit één plek een signaal wordt uitgezonden met het bereik van een aantal meter, dat kan worden ontvangen door een

33 Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement, Draft opinion on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on consumer protection cooperation (2007/0248(COD), Brussel: 10 juni 2008, Amendement 54, p. 35.

34 Artikel 29 Werkgroep, *Advies 2/2008 over de herziening van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-Privacyrichtlijn),* WP 150, Brussel: 15 mei 2008, p. 5 (verder: 'Artikel 29 Werkgroep, WP 150, 2008'). Artikel 29 Werkgroep, *Advies 1/2009 over de voorstellen tot wijziging van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie (e-privacyrichtlijn)*,WP159, Brussel: 10 februari 2009, p. 10 (verder: 'Artikel 29 Werkgroep, WP 159, 2009'). Aldus ook: E. Kosta, P. Valcke & D. Stevens: '"Spam, spam, spam, spam … Lovely spam!" Why is Bluespam different?', *International Review of Law, Computers & Technology* 2009 (23:1), p. 89-97, p. 93 en p. 96.

potentieel oneindig aantal voorbijgangers.[35] Anderzijds lijkt het erop dat de frase 'andere soortgelijke toepassingen' breed genoeg is geformuleerd om daar bijvoorbeeld Bluetooth-applicaties onder te laten vallen. De vraag dringt zich echter op wat precies als 'soortgelijk' moet worden beschouwd.

In lid 2 wordt 'die elektronische contactgegevens bij het verzamelen ervan' vervangen door 'op het ogenblik dat zij worden verzameld'.[36] Dit brengt geen substantiële wijziging met zich. Lid 3 voegt wederom na 'abonnees' 'of gebruikers' toe. Bovendien begon het oorspronkelijke lid met de zinsnede 'De lidstaten nemen passende maatregelen om ervoor te zorgen dat, zonder kosten voor de abonnee,' terwijl nu de sectie over kosten voor de abonnee is verplaatst naar het einde van het lid dat nu luidt 'met dien verstande dat beide mogelijkheden voor de abonnee of gebruiker kosteloos moeten zijn.' Hierdoor is onomstotelijk vast komen te staan dat beide mogelijkheden kosteloos moeten zijn en dat derhalve de zinsnede niet slechts refereert aan de mogelijkheid om toestemming vooraf te vereisen, maar ook aan de mogelijkheid deze communicatie in zijn geheel onmogelijk te maken.

Lid 4 wijzigt 'elektronische post met het oog op direct marketing te verzenden' in 'e-mail te verzenden met het oog op direct marketing'. Dit brengt geen substantiële wijziging met zich. Daarnaast wordt de vroegere bewoording 'communicatie plaatsvindt wordt gemaskeerd of verborgen of zonder dat een geldig adres' vervangen door 'communicatie plaatsvindt, wordt gemaskeerd of verborgen, die in strijd is met artikel 6 van [de e-Commercerichtlijn], en zonder dat een geldig adres wordt vermeld.' Artikel 6 van de e-Commercerichtlijn regelt de informatieplicht met betrekking tot commerciële communicatie. Commerciële communicatie die deel uitmaakt van een dienst van de informatiemaatschappij moet herkenbaar zijn als commerciële communicatie. Ook moet degene voor wiens rekening deze communicatie geschiedt duidelijk te identificeren zijn. Indien het advertenties betreft moeten deze als zodanig herkenbaar zijn en moeten de voorwaarden van de aanbieding gemakkelijk te vervullen zijn en duidelijk en ondubbelzinnig worden aangeduid. Tot slot moeten volgens artikel 6 van de e-Commercerichtlijn ook verkoopbevorderende wedstrijden duidelijk als zodanig herkenbaar zijn en moeten de deelnemingsvoorwaarden gemakkelijk te vervullen zijn en duidelijk en ondubbelzinnig worden aangeduid. Het nieuwe lid 4 van artikel 13 specificeert dat voldaan moet worden aan de eisen van artikel 6 van de e-Commercerichtlijn.

Nieuw in lid 4 van artikel 13 is verder de laatste zinsnede 'of e-mail die ontvangers aanmoedigt websites te bezoeken die in strijd zijn met dat artikel.' Ook e-mails die verwijzen naar een website die in strijd is met lid 4 vallen derhalve onder de reikwijdte van dit lid. Dit ziet op phishing: het oplichten van mensen door ze te lokken naar een valse website waarbij zij worden verleid hun gegevens te verstrekken door in te loggen of een webformulier in te vullen.

De grootste wijziging in artikel 13 geschiedt door de invoeging van lid 6 in artikel 13, dat geheel nieuw is. Het complementeert het tevens nieuw ingevoegde artikel 15bis betreffende de handhaving en uitvoering van de Richtlijn via administratieve organen. Lid 6 van artikel 13 voorziet in civielrechtelijke rechtsmiddelen voor personen, in het bijzonder aanbieders van elektronische communicatiediensten die een rechtmatig ondernemingsbelang hebben bij de bestrijding van ongewenste communicatie, om inbreukmakers in rechte aan te spreken. Hierdoor kunnen spammers worden aangesproken wegens misbruik van het netwerk. Deze mogelijkheid bleek niet expliciet uit de oude Richtlijn. Deze nieuwe vorderingsmogelijkheid stelt de provider in staat zijn klanten tegen spam te beschermen; klanten die zelf vaak het geld, de kennis of de tijd missen om een dergelijke juridische procedure te starten. A-contrario lijkt dit lid erop te wijzen dat een provider slechts voor overtredingen met betrekking tot artikel 13 een civiele procedure kan starten. Hierop heeft de European Data Protection Supervisor dan ook kritiek geuit.[37] De Artikel 29 Werkgroep heeft tevergeefs aanbevolen deze regel ook van toepassing te verklaren op artikel 5 lid 3.[38] Desalniettemin moet worden opgemerkt dat lidstaten vrij zijn te bepalen dat partijen ook in andere dan de in de Richtlijn genoemde gevallen vorderingsbevoegdheden kunnen toekennen.

Overweging 68 van de Richtlijn Burgerrechten bepaalt tot slot dat om spam te bestrijden aanbieders van elektronische communicatiediensten aanzienlijke investeringen moeten doen. Deze aanbieders zijn ook beter geplaatst dan de eindgebruikers qua kennis en middelen om spammers op te sporen en te identificeren. De aanbieders van e-maildiensten en andere aanbieders van diensten moeten derhalve over de mogelijkheid beschikken om een rechtsvordering in te leiden tegen spammers en zo de belangen van hun klanten als onderdeel van hun eigen rechtmatige ondernemingsbelangen, te verdedigen. Tot slot kunnen lidstaten sancties opleggen met betrekking tot aanbieders van elektronische communicatiediensten die door nalatigheid bijdragen aan inbreuken door spam.

2.8 *Comitéprocedure*

Het volgende artikel wordt ingevoegd:

'Artikel 14bis Comitéprocedure

1. De Commissie wordt bijgestaan door het comité voor communicatie dat is ingesteld bij artikel 22 van Richtlijn 2002/21/EG (Kaderrichtlijn).

35 <www.comms.scitech.susx.ac.uk/fft/bluetooth/BNEP_0_95a.pdf>.
36 Ook wordt 'elektronische post' vervangen door 'e-mail'. Dit lijkt echter een vertaalfout aangezien de term in de Engelse tekst ongewijzigd is gebleven.
37 EDPS, Eerste advies, par. II. 4.
38 Artikel 29 Werkgroep, WP 150, 2008.

2. Wanneer naar dit lid wordt verwezen, zijn artikel 5bis, leden 1 tot en met 4, en artikel 7 van Besluit 1999/468/EG van toepassing, met inachtneming van artikel 8 van dat besluit.

3. Wanneer naar dit lid wordt verwezen, zijn artikel 5bis, leden 1, 2, 4 en 6, en artikel 7 van Besluit 1999/468/EG van toepassing, met inachtneming van artikel 8 van dat besluit.'

Artikel 22 van de Kaderrichtlijn heeft het Comité voor Communicatie (COCOM) geïnstalleerd. Het COCOM krijgt door meerdere wijzigingen uit de 'Telecom Reform Package' een grotere rol. De bevoegdheden van het COCOM staan genoemd in het Tweede Comitologiebesluit,[39] waarnaar zowel artikel 22 van de Kaderrichtlijn als artikel 14bis van de hier besproken Richtlijn verwijzen. Het COCOM brengt advies uit over voorstellen van de Commissie. Dit geschiedt ofwel adviserend, ofwel regulerend, ofwel via regulering met toetsing.[40] Deze laatste mogelijkheid is vervat in artikel 5bis, dat per amendement bij een Besluit van de Raad[41] in het Tweede Comitologiebesluit is ingevoegd. Dit biedt de Raad en het Parlement de mogelijkheid om zich tegen de aanneming van een ontwerp van maatregelen wanneer zij te kennen geven dat de Commissie haar bevoegdheden te buiten is gegaan of wanneer het ontwerp niet verenigbaar is met het doel of de inhoud van het besluit of niet strookt met het subsidiariteits- of evenredigheidsbeginsel.[42]

Leden 2 en 3 van artikel 14bis stellen dat als er naar één van beide leden wordt verwezen er verschillende delen van het Tweede Comitologiebesluit van toepassing zijn. Na amendering van de Richtlijn Burgerrechten verwijst artikel 4 lid 5 van de e-Privacyrichtlijn naar lid 2 van artikel 14bis. In zowel lid 2 als lid 3 van artikel 14bis wordt de regulerende bevoegdheid met toetsing uit artikel 5bis van het Tweede Comitologiebesluit van toepassing verklaard. Lid 2 van artikel 14bis regelt de normale procedure, terwijl lid 3 een spoedprocedure regelt. Aanvankelijk verklaarde artikel 4 lid 5, toen nog artikel 4 lid 4, de spoedprocedure van toepassing in spoedeisende gevallen. Echter, deze verwijzing is tijdens het wetgevingsproces komen te vervallen waardoor er vooralsnog geen bepaling verwijst naar het derde lid van artikel 14bis.[43]

2.9 *Toepassing van een aantal bepalingen van de Algemene Privacyrichtlijn*

In artikel 15 wordt het volgende lid ingevoegd:

'1ter. Aanbieders zetten interne procedures op voor de afhandeling van verzoeken om toegang tot persoonsgegevens van gebruikers op de grondslag van nationale bepalingen die overeenkomstig lid 1 zijn aangenomen. Zij verstrekken aan de bevoegde nationale instantie op verzoek gegevens over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.'

Dit amendement is ingevoegd op initiatief van het Europees Parlement. Aanbieders moeten interne regels opstellen voor de afhandeling van verzoeken tot de verstrekking van persoonsgegevens van hun gebruikers indien de verzoeken op de grondslag van nationale bepalingen overeenkomstig lid 1 van artikel 15 zijn genomen. Artikel 15 lid 1 bepaalt dat de lidstaten wettelijke maatregelen mogen treffen ter beperking van de reikwijdte van de in deze Richtlijn vervatte plichten rond het vertrouwelijk karakter van de communicatie, de verwerking van verkeersgegevens, weergave en beperking van de identificatie van het oproepende en het opgeroepen nummer en andere locatiegegevens dan verkeersgegevens. Dit mag als dit noodzakelijk is in een democratische samenleving, redelijk en proportioneel is en om de openbare veiligheid te waarborgen of om strafbare feiten of onbevoegd gebruik van het elektronische communicatiesysteem als bedoeld in artikel 13 lid 1 van de Algemene Privacyrichtlijn (betreffende de uitzonderingen en beperkingen van de verplichtingen die in die Richtlijn staan opgesomd) te voorkomen, te onderzoeken, op te sporen en te vervolgen. Lidstaten kunnen onder meer wetgevingsmaatregelen treffen omgegevens gedurende een beperkte periode te bewaren. Artikel 15 lid 1ter stelt nu dat de dienstverleners op verzoek gegevens zullen verstrekken over deze procedure aan de bevoegde nationale instantie betreffende het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en hun antwoord.

De strekking van artikel 15 lid 1ter is tijdens het totstandkomingsproces afgezwakt. Het oorspronkelijke voorstel van het Parlement verplichtte diensverleners de onafhankelijke autoriteiten voor gegevensbescherming onverwijld in kennis te stellen van ieder verzoek om toegang tot persoonsgegevens van gebruikers te verstrekken. De desbetreffende onafhankelijke autoriteit voor gegevensbescherming moest vervolgens 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 Raad was hier echter tegen gekant en derhalve heeft het Parlement de inhoud en de strekking van dit lid afgezwakt.

2.10 *Uitvoering en handhaving*

Het volgende artikel wordt ingevoegd:

39 Besluit van de Raad van 28 juni 1999 tot vaststelling van de voorwaarden voor de uitoefening van de aan de Commissie verleende uitvoeringsbevoegdheden (*PbEG* 1999, L 184/23).

40 <http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/comm_committee/index_en.htm>.

41 Besluit van de Raad van 17 juli 2006 tot wijziging van Besluit 1999/468/EG tot vaststelling van de voorwaarden voor de uitoefening van de aan de Commissie verleende uitvoeringsbevoegdheden (*PbEG* 2006, L 200/11).

42 Besluit van de Raad van 17 juli 2006 tot wijziging van Besluit 1999/468/EG tot vaststelling van de voorwaarden voor de uitoefening van de aan de Commissie verleende uitvoeringsbevoegdheden (*PbEG* 2006, L 200/11), overweging 2.

43 Zie ook Artikel 29 Werkgroep, WP 150, 2008, p. 4.

'Artikel 15bis Uitvoering en handhaving

1. De lidstaten stellen de regels vast inzake de sancties in voorkomend geval met inbegrip van strafrechtelijke sancties, die van toepassing zijn op overtredingen van de ter uitvoering van deze Richtlijn vastgestelde nationale bepalingen en nemen de nodige maatregelen om de toepassing van die sancties te verzekeren. De aldus vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend en kunnen worden toegepast met betrekking tot de hele periode van een overtreding, zelfs indien de overtreding vervolgens is recht gezet. De lidstaten stellen de Commissie uiterlijk op 25 mei 2011 in kennis van die bepalingen en geven onverwijld kennis van eventuele latere wijzigingen.

2. Onverminderd de mogelijkheid tot beroep op de rechter zorgen de lidstaten ervoor dat de bevoegde nationale instantie en, in voorkomend geval, andere nationale organen bevoegd zijn de in lid 1 bedoelde overtredingen te doen ophouden.

3. De lidstaten zorgen ervoor dat de bevoegde nationale instantie en, in voorkomend geval, andere nationale organen over de nodige onderzoeksbevoegdheden en -middelen beschikken, met inbegrip van de bevoegdheid 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.

4. De bevoegde nationale instanties kunnen maatregelen goedkeuren om een doeltreffende grensoverschrijdende samenwerking bij de handhaving van de overeenkomstig deze Richtlijn vastgestelde nationale wetten te waarborgen en geharmoniseerde voorwaarden te creëren voor het aanbieden van diensten waarbij grensoverschrijdende gegevensstromenbetrokken zijn.

De nationale regelgevende instanties bezorgen de Commissie ruime tijd voor de goedkeuring van deze maatregelen een samenvatting van de redenen voor optreden, de geplande maatregelen en de voorgestelde aanpak. De Commissie kan na onderzoek van deze informatie en na raadpleging van het ENISA en de bij artikel 29 van Richtlijn 95/46/EG ingestelde werkgroep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, opmerkingen over deze informatie maken of aanbevelingen met betrekking tot deze informatie doen, met name om ervoor te zorgen dat de beoogde maatregelen geen negatieve gevolgen voor de werking van de gemeenschappelijke markt hebben. De nationale regelgevende instanties houden bij hun besluit over de maatregelen maximaal met de opmerkingen en aanbevelingen van de Commissie rekening.'

De e-Privacyrichtlijn bevatte oorspronkelijk geen artikel dat expliciet inging op de uitvoering en de handhaving van die Richtlijn. In plaats daarvan werd verwezen naar de algemene Privacyrichtlijn. Dit nieuw ingevoegde artikel bevordert de implementatie, de handhaving en de harmonisering van de genomen maatregelen. Lid 1 bepaalt dat lidstaten regels vast dienen te stellen inzake de sancties die van toepassing zijn op overtredingen van (de implementatiewet van) de e-Privacyrichtlijn. Deze sancties moeten doeltreffend, evenredig en afschrikkend zijn. Overweging 70 van de Richtlijn Burgerrechten stelt dat voor de tenuitvoerlegging en de handhaving van de e-Privacyrichtlijn samenwerking tussen de nationale regelgevinginstanties van meerdere lidstaten dikwijls nodig zal zijn, bijvoorbeeld bij de bestrijding van grensoverschrijdende spam en spyware. Met het oog op een vlotte en snelle samenwerking in deze gevallen, moeten door de desbetreffende nationale instanties procedures worden omschreven, die door de Commissie moeten worden onderzocht, bijvoorbeeld in verband met de hoeveelheid en het formaat van de tussen instanties uitgewisselde informatie of de in acht te nemen termijnen. Met dergelijke procedures zullen ook de daaruit voortvloeiende verplichtingen voor marktactoren kunnen worden geharmoniseerd, hetgeen bijdraagt aan de totstandbrenging van gelijke mededingingsvoorwaarden in de Gemeenschap.

Lid 2 bepaalt dat onverminderd de mogelijkheid tot beroep op de rechter, de bevoegde nationale instantie de in lid 1 bedoelde overtredingen mogen doen ophouden. Dit is een minder tijdrovende procedure dan een gerechtelijke procedure. Dit kan wenselijk zijn in verband met het versturen van spam, dat in se een aanhoudende gedraging is.[44] Lid 3 van artikel 15bis bepaalt dat om hun taak goed te kunnen vervullen, de nationale autoriteiten over de nodige onderzoeksbevoegdheden en -middelen moeten beschikken. Dit is extra belangrijk aangezien het bewijs vaak in elektronische vorm bestaat en kan zijn opgeslagen op verschillende computers en apparaten of netwerken.[45]

Lid 4 biedt een extra stimulans voor een grensoverschrijdende aanpak van illegale praktijken ten aanzien van gegevensstromen en biedt een extra mogelijkheid voor de Commissie om harmonisatie van maatregelen te bevorderen zodat zij geen negatieve gevolgen hebben voor de werking van de gemeenschappelijke markt.

3 Samenvatting en aanbevelingen

De e-Privacyrichtlijn die in 2002 is aangenomen, was aan modernisering toe. De Richtlijn Burgerrechten wijzigt de Richtlijn nu op een aantal punten. Zo zijn thans een aantal in de Richtlijn opgesomde verplichtingen zonder meer van toepassing op abonneelijnen die verbonden zijn met analoge centrales en vallen situaties waarin de Radio Frequency Identification Devices zijn verbonden met een openbaar communicatienetwerk ook onder de reikwijdte van de Richtlijn. Aanbieders van openbare elektronische communicatiediensten hebben na wijziging van de e-Privacyrichtlijn de plicht om datalekken aan de bevoegde nationale instantie te melden en indien schade dreigt moeten zij ook hun abonnees inlichten. Er is een

44 EDPS, Eerste advies, kantlijnnummer 61.
45 EDPS, Eerste advies, kantlijnnummer 60.

opt-in-regeling geïntroduceerd met betrekking tot cookies en ad- en spyware en de Richtlijn heeft na wijziging een sterker handhavingskader, zowel in publiekrechtelijke als in civielrechtelijke zin. Dit zijn nuttige en welkome aanvullingen.

Toch schiet de Richtlijn ook na wijziging op een aantal punten te kort. Zo is de Richtlijn niet van toepassing op besloten gebruikersgroepen en bedrijfsnetwerken,[46] geldt de meldplicht voor datalekken niet ten aanzien van bedrijven die een onlinebank, een forum, een social network of een webwinkel aanbieden,[47] is de verplichting ten aanzien van datalekkage slechts van toepassing op de onder de reikwijdte van de e-Privacyrichtlijn vallende entiteiten, valt te betwijfelen of gebruikers door middel van hun browserinstellingen bewust en geïnformeerd toestemming geeft voor het plaatsen van cookies, valt te betwijfelen of Bluetooth ook onder het spamartikel valt,[48] valt te betreuren dat de mogelijkheid voor providers om spammers in rechte aan te spreken met betrekking tot ad- en spyware niet Europees is geregeld[49] en valt te betreuren dat dienstverleners niet verplicht zijn de onafhankelijke autoriteiten voor gegevensbescherming onverwijld in kennis te stellen van ieder verzoek om toegang tot persoonsgegevens van gebruikers te verstrekken, die vervolgens de bevoegde gerechtelijke autoriteiten in kennis zouden stellen van de gevallen waarin naar haar oordeel de toepasselijke bepalingen van de nationale wet niet zijn nageleefd. Per saldo is de vernieuwing van de e-Privacyrichtlijn dan ook een dappere poging om de Richtlijn aan te passen aan de huidige stand van de techniek, maar het is de vraag of de Richtlijn het opnieuw acht jaar lang zonder aanpassingen zal kunnen stellen.

46 Zie ook: Overweging 55 van de Richtlijn Burgerrechten. Artikel 29 Werkgroep, WP 36, 2008, paragraaf 2. Artikel 29 Werkgroep, *Advies 8/2006 over de herziening van het regelgevingskader voor elektronische communicatienetwerken en -diensten, met bijzondere aandacht voor de ePrivacyrichtlijn*, WP 126, Brussel: 26 september 2006, par. 2 (verder: 'Artikel 29 Werkgroep, WP 126, 2006'). EDPS, Eerste advies, par. II.1 (ii); Europese Toezichthouder voor gegevensbescherming, *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),* Brussel: 6 juni 2009 (*PbEG* 2009, C 128/28), par. III (verder: 'EDPS, Tweede advies').

47 Zie ook: Artikel 29 Werkgroep, WP 126, 2006; Artikel 29 Werkgroep, WP 150, 2008, p. 2; EDPS, Eerste advies, par. II.2; EDPS, Tweede advies, par. II. De Europese regelgever gaat ervan uit dat er later een algemene meldplicht voor datalekken dient te worden ingevoerd; zie overweging 59 van de Richtlijn Burgerrechten.

48 Artikel 29 Werkgroep, WP 159, 2009, p. 10.

49 Zie ook: EDPS, Eerste advies, par. II. 4; Artikel 29 Werkgroep, WP 150, 2008.