

# **Een juridische blik op WiFi**

De kleine aanbieder van dichtbij bekeken

Johan de Jong

Wetenschapswinkel Rechten, Universiteit Utrecht  
Begeleid door de disciplinegroep Rechtstheorie

April 2005

CIP GEGEVENS KONINKLIJKE BIBLIOTHEEK, DEN HAAG

Jong, J.D.C. de.

Een juridische blik op WiFi / J.D.C. de Jong

Utrecht: Wetenschapswinkel Rechten, Universiteit Utrecht.

Begeleid door de disciplinegroep Rechtstheorie.

ISBN 90-5213-131-7

trefw: WiFi, internet service provider, Telecommunicatiewet.

Deze uitgave mag geheel of gedeeltelijk geciteerd worden mits de auteur en de Wetenschapswinkel Rechten vermeld worden en mits geen wijzigingen in het geciteerde worden aangebracht.



## Voorwoord

Wat is er nu mooier dan studie en hobby te combineren? Dat was mijn eerste gedachte toen ik in het U-blad de aankondiging van de Wetenschapswinkel las over een onderzoeksvraag omtrent WiFi. Ik was op zoek naar een scriptieonderwerp waar ik met veel plezier aan zou werken en daar stond het. Uiteraard kon ik niet anders dan reageren.

Sinds mijn vader in 1989 zijn eerste IBM 286 computer in huis haalde, was ik geboeid door het fenomeen computer. Uiteraard begon dat met spelletjes. Langzamerhand leerde ik ook het besturingssysteem Dos kennen en leerde commando's uit mijn hoofd. Met vallen en opstaan leerde ik meer.

Inmiddels ken ik de pc waar ik nu op werk van binnen en van buiten. Toch koos ik voor rechten als studie, ook dat had mijn interesse en dit bleek geen verkeerde keuze. De voorliefde voor computers en elektronica is gebleven en ik ben dan ook blij dit te kunnen combineren met mijn studie.

Allereerst wil ik mijn ouders bedanken voor het begrip dat ik het druk had met mijn onderzoek en uiteraard voor het feit dat ze mij kennis hebben laten maken met het fenomeen computer. Daarnaast wil ik Tina van der Linden bedanken voor haar goede begeleiding, nimmer aflatende ondersteuning en richtinggevende raad bij mijn onderzoek. Ik dank ook Aldebert Wiersinga voor zijn technische kennis, heldere inzichten en visie als niet-jurist. Wim van Althuis bedank ik voor de kennis van het bedrijfsleven en de lopende projecten. Natuurlijk bedank ik ook Rebecca van Musscher voor het vertrouwen dat zij in mij stelde voor wat betreft dit onderzoek en de algemene ondersteuning. Alle vier wil ik jullie bedanken voor de tekstuele adviezen en het nakijkwerk.

Ik wens u veel leerzaam leesplezier.

Utrecht, februari 2005

Johan D.C. de Jong

Dit onderzoek is afgerond in april 2005.



## Samenvatting

In dit onderzoek staat de volgende vraag centraal: *‘Wat zijn de rechten en plichten van de spelers, die niet als primair bedrijfsdoel telecommunicatie en datacommunicatie hebben, op de markt voor WiFi?’*. Om tot beantwoording van deze vraag te komen zijn enkele deelvragen geformuleerd. De eerste deelvraag is: *‘Wat zijn nu eigenlijk de rollen op de markt voor WiFi en wie zijn de spelers?’*. De tweede deelvraag luidt: *‘Welke regelgeving is van toepassing op de kleine spelers op de markt van WiFi?’*. De laatste deelvraag is het logische vervolg daarop: *‘Kan de relevante regelgeving direct worden toegepast op de eerder geïdentificeerde spelers op de markt?’*.

Alvorens de juridische aspecten te beschouwen wordt eerst de techniek besproken. WiFi staat voor *‘Wireless Fidelity’*, een verzamelnaam voor draadloze netwerken die voldoen aan de IEEE 802.11x-standaard. WiFi werkt via een hoge frequentie: 2,4 of 5 Gigahertz en heeft een snelheid van respectievelijk 11 dan wel 54 megabits per seconde. De techniek werkt met zenders en ontvangers, die beiden in één apparaat zijn verenigd om zodoende communicatie mogelijk te maken. Om via WiFi op het internet te komen, moet de aanbieder van een draadloos toegangspunt met WiFi-techniek dit toegangspunt koppelen met een vaste internetverbinding. Het toegangspunt is slechts een netwerkaansluitpunt. WiFi kan voor verschillende toepassingen worden gebruikt.

Op de markt voor WiFi zijn verschillende rollen te onderscheiden. Dit zijn achtereenvolgens de locatiehouder, de operator, de accessprovider, de internet service provider, de hosting provider, de content provider, de diensten provider en de eindgebruiker. Deze rollen kunnen door verschillende spelers worden vervuld, maar een speler kan ook meerdere rollen hebben in het WiFi-proces.

Op de spelers en rollen is vooral de Telecommunicatiewet van toepassing. Deze wet spreekt over elektronische communicatienetwerken en –diensten. Een begrip waar WiFi onder te brengen is. Voor het gebruik van de frequentie benodigd voor WiFi is geen vergunning nodig, zodat ook de apparatuur vrij gebruikt kan worden. Wel geldt voor storingen aan en door WiFi-apparatuur dat de WiFi-gebruiker gehouden is om de storing te voorkomen, omdat hij een vergunningvrije frequentie gebruikt. Voor het plaatsen van een antenne kan een vergunning nodig zijn als deze aan de voorgevel of in het zicht wordt geplaatst. De antenne is echter niet bijzonder groot. Voor het plaatsen van een antenne en apparatuur op een pand van een andere eigenaar moet een overeenkomst worden gesloten ten behoeve van het gebruik van de locatie. Bij weigering van plaatsing van de antenne door een eigenaar met een economische machtspositie kan de Mededingingswet in bepaalde gevallen uitkomst bieden. De Mededingingswet verbiedt het misbruik maken van de economische machtspositie.

Bij het aanbieden van een draadloos netwerktoegangspunt is het van belang om onderscheid te maken tussen openbare en niet-openbare netwerken of diensten daar dit verschil maakt voor de Telecommunicatiewet. Bij openbaarheid hoort namelijk een registratieplicht met kosten en een aftapverplichting. Een aanbieder met een draadloos netwerktoegangspunt is geen openbare aanbieder, indien hij het alleen aan zijn klanten aanbiedt. Voor location based services is het noodzakelijk dat degene wiens locatiegegevens bekend zijn, vooraf toestemming geeft voor het gebruik ervan.

Om een hacker eenvoudig aansprakelijk te stellen voor inbreuk op de WiFi-verbinding is het van belang deze te beveiligen. Hier gaat een signaal van uit, zodat de daad van de hacker altijd onrechtmatig is. Daarnaast verdient het aanbeveling een registratie bij te houden van de gebruikers, om bij onregelmatigheden de desbetreffende gebruiker direct op te kunnen sporen. Zo is ook openbaarheid van het netwerk weer een stap verder weg. Concluderend kan gesteld

worden dat de aanbieder van een draadloos netwerktoegangspunt alleen een *doorgeefluik* is, terwijl de achterliggende internet service provider het openbare netwerk beheert.

## Lijst van afkortingen

BW	Burgerlijk Wetboek
GHz	Gigahertz
GSM	<i>Global System for Mobile Communications, mobiele telefoon</i>
ICT	Informatie en Communicatie Technologie
ISP	Internet Service Provider
Jo	Juncto
MKB	Midden- en Kleinbedrijf
Mw	Mededingingswet
mW	Milliwatt
OPTA	<i>Onafhankelijke Post en Telecommunicatie Autoriteit</i>
PDA	Personal Digital Assistant
Sr	Strafrecht
Tw	Telecommunicatiewet 1998
VROM	Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu
WiFi	Wireless Fidelity





# Inhoudsopgave

Voorwoord	i
Samenvatting	iii
Lijst van afkortingen	v
Inhoudsopgave	vii
<b>1 Inleiding en onderzoeksopzet</b>	<b>1</b>
1.1 Inleiding	1
1.2 Probleemstelling	1
1.3 Deelvragen	2
1.4 Basisbegrippen en beperkingen	2
<b>2 Werking WiFi en haar toepassing</b>	<b>5</b>
2.1 Techniek van WiFi	5
2.2 Voorbeelden van WiFi-toepassingen	7
<b>3 Rollen en spelers op de markt voor WiFi</b>	<b>9</b>
3.1 Locatiehouder	9
3.2 Operator	9
3.3 Accessprovider	9
3.4 Internet service provider	10
3.5 Hosting provider	10
3.6 Content provider	11
3.7 Diensten provider	11
3.8 Gebruiker/Klant	11
<b>4 De juridische blik</b>	<b>13</b>
4.1 Frequentiegebruik	13
4.2 Antenneplaatsing	14
4.3 Het aanbieden van een netwerk of dienst	15
4.4 Misbruik en aansprakelijkheid	17
<b>5 Conclusies en aanbevelingen</b>	<b>21</b>
Geraadpleegde bronnen	23
Bijlagen Relevante wet- en regelgeving	25
Bijlage I Burgerlijk Wetboek	25
Bijlage II Mededingingswet	26
Bijlage III Regeling gebruik van frequentieruimte zonder vergunning	26
Bijlage IV Wetboek van Strafrecht	27
Bijlage V Telecommunicatiewet	28
Bijlage VI Wet bescherming persoonsgegevens	37
Bijlage VII Wetsvoorstel Computercriminaliteit II	38

# 1 Inleiding en onderzoeksopzet

## 1.1 Inleiding

Draadloos internet, WiFi, het lijken synoniemen voor modern en geweldig. Overal duiken de termen op en iedereen schermt ermee, de ICT-tijdschriften voorop. Daarbij wordt vooral gewezen op het gebruiksgemak en soms ook op de gevaren van het openstellen van een draadloze verbinding. De WiFi-techniek maakt het mogelijk om met een laptop in te loggen op een draadloos netwerk, waarna het internet in de meeste gevallen beschikbaar is.

Stel je zit op een terras op de Neude in Utrecht en je wilt kijken of je nog nieuwe e-mail hebt. Dan is het vrij simpel om met een laptop met daarin een draadloze netwerkkaart in te loggen op het WiFi-netwerk dat open staat voor een ieder die het wil gebruiken. Dit netwerk is in opdracht van de gemeente Utrecht aangelegd door Mobilander, een draadloze Internet Service Provider. Denkbaar is ook een winkel of horecagelegenheid die aan de klanten een draadloze internettoegang biedt. Maar wat zijn de rechten en plichten van de spelers op de markt voor draadloze ICT-toepassingen, die van origine een ander bedrijfsdoel hebben?

Hierbij is het van belang te melden dat WiFi een techniek is die vrij is van licenties. Om gebruik te maken van de frequenties waarop de WiFi-techniek werkt, is dus geen licentie vereist. Unité vroeg zich af wat de rechten en plichten zijn van deze spelers. Daarom wordt er middels deze scriptie voor het project Utrecht Verbindt via de Wetenschapswinkel Rechten onderzoek gedaan naar de kleinere spelers op de markt voor draadloze ICT-toepassingen en hun rechten en plichten. Zodoende kan duidelijkheid worden geboden aan de spelers op de markt, met name aan de MKB-ondernemers.

Het project waar deze onderzoeksvraag deel van uitmaakt heet Utrecht Verbindt. Dit onderzoek is het juridische deelonderwerp. Het project heeft als doel het overdragen van kennis aan bedrijven en organisaties in de binnenstad van Utrecht over de technologie en toepassingen van draadloze breedbandverbindingen (WiFi). Het project laat het belang zien van samenwerkingsverbanden die het innoverende vermogen van de regio verhoogt en het brengt zowel 'thuis'gebruikers als grote gebruikers van WiFi dicht bij elkaar. De kennis uit dit project is niet alleen bestemd voor de betrokken partijen maar voor het gehele MKB.

Helaas hebben veel bedrijven momenteel nog een onduidelijk beeld van de toepassingen van draadloos breedband internet. Men wordt overspoeld met informatie waardoor er sterk behoefte is aan opheldering. Dit voorlichtingsproject over de toepassingen van draadloos breedband internet in de binnenstad van Utrecht probeert de kennis over dit onderwerp te bundelen en te verspreiden onder de kennisvragers.

Dit project is een initiatief van Unité met (IC)trust en Mobilander in samenwerking met de Wetenschapswinkel Rechten van de Universiteit Utrecht, de Hogeschool voor de Kunsten Utrecht en de Academie voor Digitale Communicatie. Unité (Utrechts netwerk voor innovatie en technologie) heeft als doel het stimuleren van innovatie en technologie in de provincie Utrecht.

## 1.2 Probleemstelling

Het doel van dit onderzoek is het verkrijgen van inzicht in de rechten en plichten van de partijen bij het aanbieden van draadloze ICT-toepassingen of WiFi-toegang. Daarbij is het vooral van belang om te kijken naar wat er al geregeld is en wat nog geregeld moet worden.

De oorspronkelijke onderzoeksvraag van Unité luidde: 'Is een kleine aanbieder van WiFi aan te merken als Service-provider?' Om het onderzoek goed in een juridisch kader te plaatsen is er voor gekozen om deze vraag algemener te stellen, zodat alle spelers er informatie uit kunnen

putten. Deze spelers zijn de organisaties die niet als voornaamste bedrijfsdoel het aanbieden van WiFi-toegang of -diensten hebben.

De onderzoeksvraag die aan de basis staat van dit onderzoek, luidt:

*Wat zijn de rechten en plichten van de spelers, die niet als primair bedrijfsdoel telecommunicatie en datacommunicatie hebben, op de markt voor WiFi?*

### 1.3 Deelvragen

Om de hoofdvraag goed te kunnen beantwoorden wordt gewerkt met enkele deelvragen die in beginsel per hoofdstuk worden uitgewerkt.

- De eerste deelvraag luidt als volgt: *‘Wat zijn nu eigenlijk de rollen op de markt voor WiFi en wie zijn de spelers?’*. Deze deelvraag komt aan bod in hoofdstuk drie ‘Rollen en spelers op de markt voor WiFi’.
- De tweede deelvraag is vooral van praktische aard: *‘Welke regelgeving is van toepassing op de kleine spelers op de markt van WiFi?’*. Deze deelvraag is van belang voor hoofdstuk vier ‘De juridische blik’.
- De derde deelvraag sluit aan op de tweede deelvraag: *‘Kan de relevante regelgeving direct worden toegepast op de eerder geïdentificeerde spelers op de markt?’*. Deze vraag wordt uitgewerkt en beantwoord in hoofdstuk vier.

### 1.4 Basisbegrippen en beperkingen

Voor het onderzoek is het van belang bepaalde begrippen nader te definiëren:

- WiFi: Wireless Fidelity. Het gaat hier om draadloze dataoverdracht middels een frequentie (2,4 of 5 Ghz). Deze frequentie is licentievrij, wel is er een standaard verplicht voor het gebruik van apparatuur, genaamd ieee 802.1X.<sup>1</sup>
- Markt: Het geheel van transacties en samenwerkingsverbanden op, in dit geval, het gebied van draadloze toepassingen middels WiFi.
- Rollen op de markt: De verschillende functionele entiteiten die zich op de markt voor Wifi kunnen voordoen.
- Spelers op de markt: In dit onderzoek wordt hieronder begrepen de aanbieders van WiFi die dit niet als hoofdbedrijfsvoering hebben, denk hierbij aan retail, horeca, gemeenten en dergelijke.
- Internet Service provider: De professionele toegangsverlener van een internetaansluiting met de basisdiensten, zoals e-mail.
- Accessprovider: De toegangsverlener tot een computernetwerk
- Intranet: Intern netwerk van computers, anders dan internet beperkt door accessprovider qua aantal en mogelijkheden.
- Server: Centrale computer in een netwerk, bedoeld voor het opslaan van gegevens (database) en afhandeling van netwerkverkeer
- PDA: Personal Digital Assistant, een draagbare elektronische zakcomputer in handzame vorm voor de belangrijkste dagelijkse functies zoals agenda en notities.
- IP-adres: Het adres op internet waar een website exclusief is te bereiken, te vergelijken met een telefoonnummer.

---

<sup>1</sup> De IEEE is een internationale organisatie die het gebruik van radiofrequenties licentieert. Zodoende geeft zij ook een licentie af voor het vrij gebruiken van bepaalde frequenties voor draadloze dataoverdracht. Zie ook:

[http://www.ieee.org/portal/index.jsp?pageID=corp\\_level1&path=about/802std&file=index.xml&xsl=generic.xsl](http://www.ieee.org/portal/index.jsp?pageID=corp_level1&path=about/802std&file=index.xml&xsl=generic.xsl)

- Elektronisch communicatienetwerk: Transmissiesystemen, waaronder mede begrepen de schakel- of routeringsapparatuur en andere middelen, die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, waaronder satellietnetwerken, vaste en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt en netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie.<sup>2</sup>
- Elektronische communicatiedienst: Transmissiesystemen, waaronder mede begrepen de schakel- of routeringsapparatuur en andere middelen, die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, waaronder satellietnetwerken, vaste en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt en netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie.<sup>3</sup>
- Openbare elektronische communicatiedienst: Elektronische communicatiedienst die beschikbaar is voor het publiek.<sup>4</sup>
- Openbaar elektronisch communicatienetwerk: Elektronisch communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om openbare elektronische communicatiediensten aan te bieden, waaronder mede wordt begrepen een netwerk, bestemd voor het verspreiden van programma's voor zover dit aan het publiek geschiedt.<sup>5</sup>

Naast deze begrippen is het ook erg belangrijk om beperkingen aan te geven. De grootste beperking is die van de spelers op de markt. Dit onderzoek is bedoeld om onderzoek te doen naar de kleinere spelers op de markt, vooral de MKB-ondernemers. De grote spelers zoals KPN en andere Internet Service providers zullen dus buiten de reikwijdte van dit onderzoek vallen. Dit is ook logisch gezien het feit dat deze spelers zich primair richten op het aanbieden van internettoegang en bijvoorbeeld draadloos internet. De huidige wetgeving lijkt voor hen voldoende houvast te bieden. Zij hebben ook de middelen om daar zelfstandig onderzoek naar te (laten) verrichten. Tevens richt Unité zich op het MKB, des te meer een reden om dit onderzoek daar op te richten.

Daarnaast beperkt het onderzoek zich tot de werking van WiFi. Er wordt alleen een schets gegeven van de werking van draadloze ICT-netwerken en hun toepassingen die voor een goed begrip en toepassing van de materie noodzakelijk zijn. Immers dit is een juridische en geen technische scriptie.

In de media is het laatste (half)jaar veel te doen over de beveiliging van bedrijfsnetwerken die via WiFi bereikbaar zijn. Bedrijfsgegevens zouden vrij toegankelijk zijn en het kraken van het netwerk een fluitje van een cent. Dit valt echter buiten dit onderzoek, daar het hier voornamelijk gaat om de rechten en plichten van de aanbieder van WiFi. Deze aanbieder stelt vaak geen netwerk beschikbaar, maar slechts een toegangspunt, het accespoint. Beveiliging van bedrijfsnetwerken doet in dat geval niet ter zake, daar andere computers en gegevens niet beschikbaar zijn voor de individuele gebruiker. Waar beveiliging wel ter sprake komt is het punt van de toegang. Er is een verschil tussen open en gesloten netwerken. Op een open netwerk kan iedereen inloggen met een laptop of PDA. Bij een gesloten netwerk is een aanmelding vereist, veelal via een wachtwoord en inlognaam of een andere vorm van toegangsbeveiliging. Hierbij komt ook de beveiliging van het dataverkeer kijken, vooral van belang bij bewakingsdoeleinden en dergelijke.

---

<sup>2</sup> Artikel 1.1 sub e Telecommunicatiewet.

<sup>3</sup> Artikel 1.1 sub f Telecommunicatiewet.

<sup>4</sup> Artikel 1.1 sub g Telecommunicatiewet.

<sup>5</sup> Artikel 1.1 sub h Telecommunicatiewet.

Verder zullen ook de location based services beschouwd worden. Dit houdt in dat middels WiFi de plaats van een persoon, of beter gezegd zijn laptop of PDA bepaald kan worden en zodoende reclame of informatie zou kunnen worden verzonden. Hoe verhoudt dit zich tot het recht? In dit onderzoek staat dus centraal hoe de dienst die de verstreker van WiFi aanbiedt, wordt gekwalificeerd in de relevante wetgeving en de rechten en plichten die daar uit voortvloeien.

## 2 Werking WiFi en haar toepassing

Voor een goed begrip van de WiFi-markt en de spelers die daar op opereren is het noodzaak inzicht te verkrijgen in de werking van de techniek die achter de term WiFi schuil gaat. In dit hoofdstuk wordt allereerst een beschrijving gegeven van de werking van WiFi. Zodra dit helder is worden de mogelijke toepassingen van WiFi besproken.

### 2.1 Techniek van WiFi

WiFi staat voor 'Wireless Fidelity' en is een verzamelnaam voor draadloze netwerken die voldoen aan de IEEE 802.11x-standaard. De benaming is afgeleid van de naam van de organisatie: Wi-Fi Alliance.<sup>6</sup> Door het standaardiseren van de draadloze communicatie kan apparatuur van verschillende fabrikanten met elkaar communiceren, dus men is niet aan één fabrikant gebonden als men zijn WiFi-toepassing kiest. Dit maakt universeel gebruik mogelijk. Voorwaarde is wel een juiste toepassing van de technische standaard, die alleen mag worden gebruikt na officiële goedkeuring van de Wi-Fi Alliance. Dit is het WiFi-keurmerk, met bijbehorend logo.



WiFi bestaat uit een zender en ontvanger, die in één apparaat zijn samengebracht. Zowel de aanbieder van de toegang tot het draadloze WiFi-netwerk, meestal bedoeld voor het bieden van internettoegang, als de gebruiker heeft een WiFi-apparaat nodig. In feite werkt het hetzelfde als een eenvoudige walkietalkie, zoals die verkrijgbaar zijn bij de speelgoedwinkel. Walkietalkies kunnen zowel geluid verzenden als ontvangen. WiFi werkt net zo, zij het dat nu elektronische data worden verzonden in plaats van geluid.

Er zijn verschillende varianten op de standaard 802.11x. De eerste standaard die werd ontwikkeld is de 802.11b-standaard. Deze werkt via de 2,4 Gigahertz en heeft een maximaal haalbare bandbreedte voor datatransport van 11 megabit per seconde. Zijn opvolger is de 802.11g-standaard. Deze werkt eveneens via de 2,4 Gigahertzfrequentie en heeft een maximale bandbreedte voor datatransport van 54 megabit per seconde. Dit is ongeveer de helft van de snelheid van de huidige bekabelde netwerken, die draaien op 100 megabit per seconde. De 802.11b-standaard heeft dus een snelheid van een tiende van een bekabeld netwerk. Het voordeel van beide standaarden is dat ze op dezelfde frequentie werken. Daardoor zijn ze onderling uitwisselbaar, met de aantekening dat de maximaal haalbare snelheid dan de snelheid is van de laagste standaard.

Naast deze standaarden is er ook nog de 802.11a-standaard. Deze werkt op de 5 Gigahertzfrequentie en heeft een maximale bandbreedte voor datatransport van 54 megabit per seconde. Deze standaard werkt niet samen met de b en g-standaard, daardoor is zij in Nederland nooit echt van de grond gekomen. Er is inmiddels ook WiFi-apparatuur ontwikkeld die met andere snelheden werkt, er is echter nog geen standaard voor overeengekomen door de IEEE.

---

<sup>6</sup> Ooijevaar, R., 'Zo werkt WiFi – De techniek achter 801.11b/g' Computer Totaal Praktijkgids Thuisnetwerk, najaar (2004), p. 42.



7

Hoe komt men nu via de WiFi-verbinding op het internet? Daarvoor is het nodig dat de aanbieder van een draadloos toegangspunt met WiFi-techniek dit toegangspunt aansluit op het internet. Dit zal veelal gebeuren via een glasvezelnetwerk of het ADSL, dan wel TV-kabelnetwerk. Dit zijn 'vaste' verbindingen met een groot netwerk van internetproviders en accessproviders die via centrale punten zijn verbonden met het 'Internet'. Als het draadloze toegangspunt deze aansluiting heeft gemaakt, kan een gebruiker middels zijn of haar netwerkkaart met WiFi-techniek en een antenne, die los dan wel ingebouwd is, toegang verkrijgen op dit draadloze toegangspunt en zo het internet gebruiken. Voor een winkelier of een kroegbaas is het eenvoudig een hotspot te maken voor zijn klanten. Een hotspot is een centraal draadloos inlogpunt, met antenne, waar een gebruiker verbinding mee kan zoeken.

De winkelier of kroegbaas heeft twee dingen nodig om zijn klanten (of zelfs voorbijgangers) een verbinding te kunnen laten maken met zijn netwerk of het internet. Allereerst een accesspoint en daarnaast een vaste internetverbinding of netwerkverbinding met het accesspoint. Om toegang te verkrijgen tot het internet via een hotspot is het niet altijd nodig dat men een wachtwoord en inlognaam nodig heeft. Dit is aan de eigenaar van het accesspoint, hoe hij dit instelt. Er zijn bedrijven die er een vergoeding voor vragen zoals KPN,<sup>8</sup> maar er zijn ook bedrijven die vrije toegang aanbieden, zonder gebruikersnaam en wachtwoord, of aan de gebruiker alleen vragen zich te registreren om een gebruikersnaam en wachtwoord te verkrijgen. De beveiligingen en aanmeldingstechnieken kan de eigenaar van een accesspoint zelf instellen via een verbinding met het accesspoint, vaak per computer die via een fysieke netwerkkabel verbonden is met het accesspoint. Dit is een commerciële overweging, het vragen van een vergoeding impliceert wel een openbare aanbieding.

Het accesspoint heeft fysiek contact met het internet middels een ADSL, kabel of glasvezelverbinding. Daarmee heeft hij ook een IP-nummer om uniek herkenbaar te zijn voor de verzending van datapakketjes. Dit is het zogenaamde externe IP-nummer. Om nu de computers en andere apparatuur die verbonden zijn of kunnen zijn met het accesspoint te kunnen laten communiceren en in staat te stellen om datapakketjes te ontvangen en te verzenden, is het nodig dat zij ook een (tijdelijk) IP-nummer krijgen. Dit is het zogenaamde interne IP-nummer. Voor

<sup>7</sup> Bron: <http://www.oreillynet.com/wireless/2003/03/21/graphics/image007.jpg>

<sup>8</sup> Zie bijvoorbeeld de openingspagina van de Hotspots van KPN: <https://portal.hotspotsvankpn.com/>



de buitenwereld hebben zij echter allen één IP-nummer, het is de router in het accespoint die de van buiten verkregen datapakketjes verstuurt naar de juiste gebruiker. Dit betekent dus dat als men een IP-nummer herleidt, dit altijd uitkomt bij de eigenaar van de internetverbinding die gekoppeld is aan het accespoint. Bijvoorbeeld de kroegbaas. De eindgebruiker is hier dus in beginsel onvindbaar.

## 2.2 Voorbeelden van WiFi-toepassingen

De WiFi-techniek is allereerst en vooral inzetbaar voor draadloze toegangverlening tot het internet, een intranet of het onderling verbinden van apparatuur. Daarvoor is de techniek in beginsel ook ontwikkeld. Het was de bedoeling een draadloze verlenging te maken voor het netwerkstopcontact. Daarbij werd vooral gedacht aan kantooromgevingen en woonhuizen. Het was oorspronkelijk de bedoeling die verlenging alleen binnen het pand mogelijk te maken, een zogenaamde beschermde omgeving. Op het moment dat dit aansloeg, begon men WiFi ook meer en meer te gebruiken om buiten het pand verbindingen tot stand te brengen. Met alle problemen van dien, zoals beveiliging en storing.

De WiFi basisdiensten:

- Om WiFi in te kunnen zetten voor toegangverlening tot het internet plaatst de aanbieder van deze toegang een draadloos toegangspunt, met een vaste internetaansluiting.
- Daarnaast kan de WiFi-techniek worden ingezet om klanten toegang te verlenen tot een intranet, zodat zij met behulp van een beschikbaar gestelde PDA of eigen apparatuur de productstatus in kunnen zien, door een catalogus kunnen bladeren, plaats van producten kunnen opvragen en voorraad kunnen bekijken. Denk hierbij bijvoorbeeld aan warenhuizen, zoals De Bijenkorf of Ikea. Hierbij is het niet zo dat men dan per definitie ook toegang heeft tot internet, het kan wel. Voor de genoemde catalogustoepassing is internettoegang bijvoorbeeld niet noodzakelijk als alle informatie op de centrale computer staat in het intranet, de zogenaamde interne server.
- De WiFi-techniek kan verder worden gebruikt om draadloze beveiligingscamera's te koppelen aan een netwerk of scherm, hoewel daar ook andere mogelijkheden toe zijn. Een belangrijke toepassing van WiFi is het mogelijk maken van een draadloze 'point-to-point' verbinding, hierbij worden twee apparaten met elkaar verbonden via een WiFi-verbinding. Zij kunnen via die verbinding met elkaar communiceren. Een goed voorbeeld hiervan is een verbinding tussen de computer en de printer. Via deze verbinding kan de computer een printopdracht geven en de printer zijn status aan de computer doorgegeven. Het betreft hier een verbinding die buiten de onderlinge communicatie niet verder zendt of ontvangt.
- Het is door middel van WiFi ook mogelijk om te bepalen waar de persoon, of beter gezegd het apparaat met WiFi-apparatuur, zich bevindt die is verbonden met een bepaald accespoint. Dit heet location based service en geeft bijvoorbeeld bedrijven de mogelijkheid een klant die langs hun winkel loopt een uitnodiging te sturen op zijn GSM, PDA of eventueel laptop. Een volgende stap van location based service is het maken van een game, waarbij andere leden van een groep moeten worden gelokaliseerd en foto's moeten worden gemaakt van het doel. De personen kunnen worden opgespoord omdat via WiFi in combinatie met een digitale stadkaart de locatie kan worden bepaald van andere spelers.<sup>9</sup>

---

<sup>9</sup> <http://wifi.hku.nl>



### 3 Rollen en spelers op de markt voor WiFi

Zonder het definiëren van de rollen op de markt voor WiFi en de spelers die deze rollen kunnen vervullen is het niet mogelijk om de markt in een juridisch kader te plaatsen. In dit hoofdstuk worden allereerst de mogelijke rollen op de markt geïdentificeerd, waarbij de mogelijke spelers die in dit onderzoek ter zake doen worden genoemd.

Bij het aanbieden van WiFi en het verlenen van toegang tot internet zijn er verschillende rollen te onderscheiden in het proces. Alle rollen kunnen vervuld worden door één enkele speler, of per rol door een andere speler.

#### 3.1 Locatiehouder

De locatiehouder stelt zijn locatie beschikbaar of zijn gebruiksrecht op een locatie, waar een antenne voor WiFi geplaatst kan worden. De locatie kan zijn een gebouw, een mast, een reclamezuil of gewoon een stuk grond. De locatiehouder verschaft slechts de mogelijkheid om een antenne te plaatsen. Een goed voorbeeld is de Neudeflat in Utrecht, de eigenaar daarvan heeft toestemming gegeven een antenne op het dak te plaatsen om de Neude en een stuk van de Oude Gracht te voorzien van een WiFi-netwerk. De voor de hand liggende spelers zijn vastgoedondernemers, gemeenten, onderwijsinstellingen en alle detail- en horecaondernemers met gehuurd of eigen vastgoed.



Een WiFi-antenne van 60 centimeter.<sup>10</sup>

#### 3.2 Operator

De operator brengt de verbindingen tot stand met en op het backbone netwerk, dat is het achterliggende, grotere netwerk, het internet. Het zijn veelal de grote bedrijven zoals KPN en Versatel, die deze rol vaak samen met het zijn van internet service provider uitvoeren. Het kunnen ook lokale spelers zijn, zoals bijvoorbeeld Catharijnenet, die het Utrechtse glasvezelnet voor de gemeente activeert. De operator heeft een direct contact met de internet service provider, hosting provider of diensten provider. De operator kan de gemeente zijn, zoals bij Catharijnenet, maar zal veelal een grotere speler zijn.

#### 3.3 Accessprovider

De accessprovider verleent de toegang tot het netwerk en eventueel het internet. Alleen door contact te maken via zijn accesspoint<sup>11</sup> is het mogelijk het internet te gebruiken. Zijn dienst

<sup>10</sup> Bron: <http://www.wirelessleiden.nl/techniek/>

<sup>11</sup> Zowel draadloos als via een netwerkkabel of andere vaste verbinding.

bestaat uit niet meer dan het aanbieden van een fysiek knooppunt dat toegang geeft tot andere diensten. Daarvoor reikt hij aan iedere verbinding die tot stand wordt gebracht met zijn knooppunt een uniek intern IP-adres uit. Dit adres is benodigd om de communicatie goed te laten verlopen en er voor te zorgen dat de juiste informatie bij de juiste gebruiker terechtkomt. Het uitreiken van een IP-adres gebeurt vrijwel altijd volledig automatisch door het accesspoint zelf. Een goed voorbeeld is KPN met DirectInternet.<sup>12</sup>

Er is een verschil tussen fixed accessproviders en wireless accessproviders. De fixed accessprovider biedt een dienst aan, zijnde de toegang tot het internet of een andere dienst. De wireless accessprovider echter geeft alleen maar het signaal door, de aanbidding van de diensten gebeurt door een achterliggende fixed accessprovider, waarmee het wireless accesspoint verbonden is.

De fixed accessprovider is meestal een professioneel bedrijf dat netwerkinfrastructuren aanlegt en de toegang tot het internet inhuurt bij derden, de Internet Service Providers. Een voorbeeld van een fixed accessprovider is Versatel, die zich vooral richt op de aanleg van glasvezelnetwerken voor bedrijven en de aansluiting daarvan op internet. Uiteraard kunnen andere spelers ook als fixed accessprovider optreden, zij doen dit dan in combinatie met de functie van operator, locatiewaarder of internet service provider.

Een wireless accessprovider is bijvoorbeeld de gemeente die naast het houden van de locatie ook de apparatuur laat plaatsen voor eigen rekening, benodigd voor de WiFi-verbinding. Of een detailhandelaar die naast het registreren van de klant en het afhandelen van zijn betaling voor internettoegang ook de apparatuur plaatst die nodig is voor de WiFi-verbinding. De wireless accessprovider is vrijwel altijd eigenaar van de geplaatste antennes.

### **3.4 Internet serviceprovider**

De internet serviceprovider maakt het mogelijk het internet daadwerkelijk te betreden door aan de gebruiker een uniek adres te geven, het externe IP-adres, en zijn verbinding met de rest van het grotere internetnetwerk tot stand te brengen. Daarnaast levert hij daarbij de meest basale diensten zoals e-mail. De Internet Service Provider kan een professionele aanbieder zijn zoals Planet Internet of XS4ALL. Ook een kleine aanbieder kan dit doen door de toegang tot internet in te kopen. Hij is dan feitelijk wireless of fixed accessprovider, maar de klant kan hem zien als internet service provider. Of hij dat ook is wordt in paragraaf 4.3 behandeld. Juridisch is het begrip openbaar elektronisch communicatienetwerk van belang. Ook daarover meer in paragraaf 4.3.

### **3.5 Hosting Provider**

De hosting provider stelt een server beschikbaar om een koppeling naar het internet te maken, bijvoorbeeld om websites op te plaatsen of andere toepassingen. Dit wordt ook wel serverruimte genoemd, maar gaat verder dan alleen ruimte. Ook beheer en beveiliging zijn belangrijk. Het aanbieden van een server kan in principe iedereen met een vaste internetverbinding. De grotere hosting providers hebben een directe aansluiting op snellere en grotere internetverbindingen, waardoor hun hostingruimte betrouwbaarder en sneller is. De thuisgebruiker kan echter ook hosting provider zijn door een pc als server te laten functioneren en daarop een website te plaatsen die toegankelijk is voor derden. Hosting providers zijn steeds vaker kleinere spelers, met een beperkte ruimte. Alle spelers kunnen in principe hosting provider zijn. Naast de schaalvoordelen van de grotere hosting providers staat de betere klantrelatie van de kleinere spelers, die een meer persoonlijke benadering hanteren in tegenstelling tot de grotere hosting providers.

---

<sup>12</sup> <http://www.kpn.com/kpn/show/id=284630>

### 3.6 Content provider

De content provider biedt nieuws en informatie op het internet aan. Dit zijn de websites, fora en mailservices. Een ieder kan content provider zijn. Zodra iemand informatie op het internet publiceert, in welke vorm dan ook, is deze persoon content provider. Dit is dus in principe iedereen met een website, iedereen die wel eens wat op een forum heeft gepubliceerd en iedereen die een e-mail nieuwsbrief heeft verstuurd. Denk hierbij aan content providers zoals de nieuwssite nu.nl, maar ook allerlei verenigingen, stichtingen en enthousiastelingen die hun informatie op het internet publiceren. Naast deze content aanbieders die in principe los staan van de provider, zijn er ook vele betaalde vormen van content. Dan schuift de rol van de content provider op naar de diensten provider.

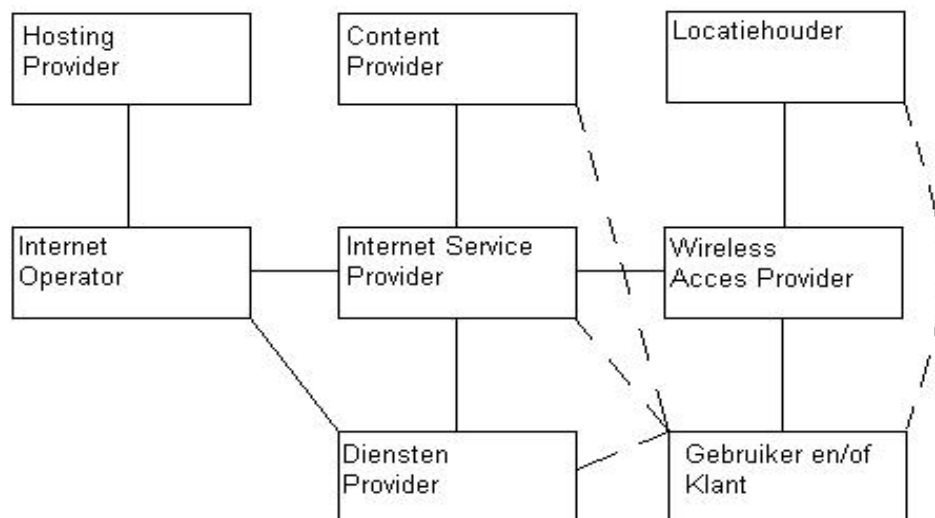
### 3.7 Diensten provider

De diensten provider heeft een rekeningrelatie met de klant voor een bepaalde dienst, al dan niet met eigen content of content van derden er achter. Daarbuiten hoeft hij niets te doen. Hij biedt de desbetreffende dienst aan, al dan niet tegen betaling en de klant kan deze afnemen. Alle overige taken laat hij dan aan anderen over of huurt hij in. De diensten provider kan er echter ook voor kiezen de dienst zelf te ontwikkelen. De diensten provider zal vooral een zakelijke speler zijn. Denk hierbij aan de detailhandelaar, gemeente of horeca die een dienst zoals bestellen, catalogusfuncties of een spel aanbieden. De meeste retailketens bieden diensten op internet aan, denk aan Free Record Shop en boekhandel Broese. Maar ook kranten zoals het NRC met toegang tot dossiers, waarvoor betaald moet worden.

### 3.8 Gebruiker/Klant

Uiteindelijk is er altijd een gebruiker of klant die gebruik maakt van de geboden (WiFi) dienst of content. Voor deze gebruiker is vaak de locatie en de wireless accessprovider direct zichtbaar. Afhankelijk van de gebruikte dienst zal er ook een relatie liggen tussen de gebruiker en de diensten en/of content provider en mogelijk ook met de ISP. De operator en hosting provider rollen zijn voor de gebruiker veelal niet direct zichtbaar.

Mogelijke onderlinge verhoudingen en verbindingen:



Stippellijnen zijn mogelijke verbindingen, gewone lijnen zijn directe verbindingen.



## 4 De juridische blik

Na de beschrijving van de spelers en de mogelijke rollen die zij kunnen vervullen wordt in dit hoofdstuk een beschouwing gegeven van het juridische kader. Daarbij is de Telecommunicatiewet een belangrijke vindplaats voor wetgeving omtrent WiFi. Dit is ook logisch gezien de inhaalslagen en aanvullingen op de originele tekst van de Telecommunicatiewet van 1998.<sup>13</sup> De laatste wijziging is in werking getreden op 19 mei 2004.<sup>14</sup> Hierbij werd het Europese richtlijnenkader voor de communicatiesector en de privacyrichtlijn omgezet in nationale wetgeving, voor een belangrijk deel uitgewerkt in een wijziging van de Telecommunicatiewet.

Dientengevolge wordt telecommunicatie niet meer als zodanig gedefinieerd in de Telecommunicatiewet. Daar voor in de plaats staat nu de elektronische communicatiedienst in artikel 1.1 sub f Telecommunicatiewet (Tw). Zij wordt als volgt gedefinieerd:

‘Elektronische communicatiedienst: 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.’

WiFi valt onder deze noemer als de techniek gebruikt wordt voor allerlei diensten die al dan niet tegen vergoeding worden geleverd, zoals de in het vorige hoofdstuk genoemde internettoegang, catalogustoegang en andere diensten. WiFi valt hier niet onder als het wordt gebruikt om informatie over te zenden die later verspreid moet worden, denk aan krantenredacties en sportfotografen.

### 4.1 Frequentiegebruik

Voordat er datapakketjes of andersoortige informatie kan worden verzonden en ontvangen via de ether is er een frequentie nodig. Artikel 3.3 lid 1 Tw geeft aan dat voor het gebruik van frequentieruimte een vergunning vereist is van de minister, welke op aanvraag kan worden verleend. Op basis van artikel 3.1 Tw heeft de minister een frequentieplan opgesteld, waarin de frequenties 2,4 GHz en 5 GHz vrij zijn voor gebruik door middel van draadloze datatoepassingen, indien het uitzendvermogen niet meer bedraagt dan 100, respectievelijk 200 milliwatt.<sup>15</sup> Dit staat gelijk aan een bereik van ongeveer 100 meter, dat is nog minder dan een tiende van het bereik van een GSM-antenne. Vanwege deze vrijstelling is voor het gebruik van WiFi geen aparte vergunning benodigd. Alle randapparatuur die voldoet aan de normen van het frequentieplan kan vrij gebruikt worden om draadloze dataverbindingen op te zetten.

Vrij gebruik betekent ook dat er in principe een grotere kans op storingen bestaat, nu er geen regulatie is van de gebruikers en de gebruikte kanalen binnen een frequentie. Voor storingen geldt als basisregel artikel 1 van de Regeling gebruik van frequentieruimte zonder vergunning.<sup>16</sup> Deze regeling is een uitwerking van artikel 3.4 lid 2 Tw. Het komt er op neer dat het gebruik van de frequentieruimte vrij is zolang er geen andere radiozendapparatuur of elektronische, dan wel elektrische apparaten worden gestoord. Ook de WiFi-apparatuur valt onder deze regeling, aldus artikel 2 lid 1 sub k van de Regeling gebruik van frequentieruimte zonder vergunning. In Bijlage 7 van deze regeling wordt de apparatuur expliciet genoemd.

<sup>13</sup> Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie. Staatsblad 1998, 610.

<sup>14</sup> Staatsblad 2004, 207.

<sup>15</sup> Zie het Nationaal frequentieplan, publicatie 2002, <http://www.ez.nl/content.jsp?objectid=18684>

<sup>16</sup> Besluit van 15 oktober 2003 nr. EZT/5003907 JZ.

Bij storingen door de WiFi-apparatuur aan andere apparatuur is de gebruiker van de WiFi-apparatuur gehouden de storing te voorkomen. Denk hierbij niet alleen aan het storen van bijvoorbeeld de communicatie van de hulpdiensten maar ook storing van draadloze huistelefoons of GSM-verkeer. Storingen tussen WiFi-gebruikers onderling is te voorkomen door andere kanalen te kiezen, want een WiFi-frequentie is opgedeeld in veertien verschillende kanalen (kleine stukjes bandbreedte). Wie er echter zijn systeem moet aanpassen ten gunste van de ander is niet wettelijk geregeld. Daarin zal vooralsnog samen een oplossing moeten worden gezocht. Logisch is dat de daarbij het kostenaspect een rol speelt. Gezien de eenvoudige kanalenomschakeling van de WiFi-apparatuur moet dit geen probleem vormen.

Moeilijker wordt het echter als andere apparatuur wordt gestoord, dan zal het immers aan de frequentie op zich liggen en niet aan het gebruikte kanaal. Een beperking van het zendvermogen kan dan een oplossing brengen, maar daarvoor is technische kennis benodigd. Het kan dan zover komen dat het door de overige apparatuur in de directe omgeving onmogelijk is om de WiFi-apparatuur te gebruiken. Deze kans op storingen is niet bijzonder groot als het maximale zendvermogen van de apparatuur laag is. Er kan dan gedacht worden aan een andere locatie om de apparatuur te plaatsen, zodat de het storingsveld verkleind of opgeheven kan worden. Voor een locatiehouder kan dit een andere positionering van de apparatuur betekenen of zelfs het op zoek gaan naar een andere locatie door de accessprovider. Het testen van de locatie en de apparatuur kan een hoop problemen al aan het licht brengen voordat het draadloos netwerk daadwerkelijk in gebruik wordt genomen.

## 4.2 Antenneplaatsing

Om een antenne te plaatsen aan een eigen gebouw is een lichte bouwvergunning nodig als deze op of aan de voorgevel wordt geplaatst, zichtbaar vanaf de openbare weg. Ook is slechts een lichte bouwvergunning nodig als de antenne op een andere plaats wordt geplaatst, maar hoger is dan vijf meter.<sup>17</sup> Dit volgt uit artikel 3 lid 1 sub e van het Besluit bouwvergunningvrije en lichtbouwvergunningplichtige bouwwerken.<sup>18</sup> Dit is een uitwerking van artikel 43 lid 1 sub c van de Woningwet.<sup>19</sup> Zoals we reeds zagen in paragraaf 3.1, is een antenne voor WiFi niet van een zodanige omvang dat deze direct als storend zou kunnen worden ervaren. Het zal daarom geen problemen opleveren als de antenne op het dak wordt geplaatst. Dit is slechts anders als het een monument betreft. Eventueel kan dit worden nagevraagd bij de gemeente. Een verdere uitweiding hierover gaat het onderwerp van dit onderzoek te buiten.

Voor de plaatsing van een antenne op een bouwwerk van een andere eigenaar zal in beginsel een overeenkomst moeten worden gesloten met de eigenaar van dit bouwwerk, de zogenaamde locatiehouder. Dit kan in de vorm van een huurcontract of iets dergelijks. Er is geen recht op plaatsing van een antenne, ook al kan deze noodzakelijk zijn voor het netwerkverkeer van de desbetreffende antennehouder. Dit is wel expliciet geregeld voor houders van een vergunning voor het gebruik van een frequentie,<sup>20</sup> maar WiFi is zoals gezegd vergunningvrij. Gezien het feit de een speler een wireless accesspoint vooral in zijn eigen directe omgeving wil opzetten, gebruikt men eigen locaties. Als er contractueel niets verboden is omtrent antenneplaatsing, dan kan de huurder of pachter van een pand in principe gewoon een antenne plaatsen. Uiteraard rekening houdend met de maximale formaten voor vergunningvrije plaatsing zoals eerder genoemd in deze paragraaf.

Als het voor het goed functioneren van het WiFi-netwerk noodzakelijk is dat gebruik wordt gemaakt van een bepaalde locatie, maar de locatie-eigenaar weigert dit, kan de

---

<sup>17</sup> Folder antenneplaatsing VROM: [http://www.vrom.nl/docs/wonen/folder\\_\(schotel\)antennes.doc](http://www.vrom.nl/docs/wonen/folder_(schotel)antennes.doc)

<sup>18</sup> Wet van 29 augustus 1991 tot herziening van de Woningwet.

<sup>19</sup> Besluit van 13 juli 2002.

<sup>20</sup> Artikel 3.11 lid 1 Tw.



Mededingingswet<sup>21</sup> (Mw) eventueel uitkomst bieden. Artikel 24 Mw verbiedt het misbruik maken van de economische machtspositie. Het moet dus wel gaan om een locatiehouder met een machtspositie. Dit kan bijvoorbeeld een vastgoedondernemer zijn die vrijwel alle panden bezit op een bepaalde locatie, of een antenneopstelpunt van een bepaalde GSMprovider. Voor een waar misbruik van de machtspositie door de locatiehouder is echter wel wat meer nodig dan alleen het bezit van een bepaalde locatie of omgeving. Allereerst moet de misbruiker een onderneming zijn om onder artikel 24 Mw te vallen, dit vermeldt lid 1 van het genoemde artikel:

‘Het is ondernemingen verboden misbruik te maken van een economische machtspositie.’

De economische machtspositie vormt de kern, dit is een zodanig belang dat de concurrentie beperkt zou kunnen worden. De omstandigheden van het geval bepalen of er daadwerkelijk misbruik wordt gemaakt van de machtspositie. Bij een marktaandeel van 50% wordt in principe aangenomen dat zij een machtspositie hebben, aldus het Hof van Justitie van de EG.<sup>22</sup> Misbruik is een breed begrip en kan zowel bestaan uit het weigeren van toegang tot de locatie, als uit het weigeren van toegang tot de technische faciliteiten waardoor van het antenneopstelpunt in de praktijk geen gebruik kan worden gemaakt omdat men bijvoorbeeld geen stroom kan krijgen.<sup>23</sup>

Het plaatsen van een WiFi-antenne door een wireless accessprovider kan zoals gezegd problemen opleveren, maar het is aannemelijk dat deze problemen overkomelijk zijn. Een locatiehouder heeft vaak het voordeel ook gebruik te kunnen maken van het WiFi-netwerk, opgezet door de wireless accessprovider. Ook is de WiFi-antenne met zijn bescheiden 30 tot 60 centimeter niet echt een storend element te noemen.

#### **4.3 Het aanbieden van een netwerk of dienst**

Indien er een antenne is geplaatst met daaraan gekoppeld een accesspoint dat een toegestane frequentie gebruikt, rijst de vraag wat het gebruiksdoel is. Als men de Telecommunicatiewet bestudeert blijkt dit namelijk een cruciale vraag. Uit de Telecommunicatiewet blijkt dat al gauw wordt uitgegaan van het feit dat een netwerk of dienst te kwalificeren is als een *openbaar* netwerk of *openbare* dienst.

Artikel 1.1 sub e Tw noemt een *elektronisch communicatienetwerk*:

‘transmissiesystemen, waaronder mede begrepen de schakel- of routeringsapparatuur en andere middelen, die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, waaronder satellietnetwerken, vaste en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt en netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie.’

De WiFi-techniek valt hier onder omdat zij bestaat uit een transmissiesysteem, het accesspoint met de WiFi-module in de apparatuur van de gebruiker, dat het mogelijk maakt signalen over te brengen middels radiogolven. Sub f van hetzelfde artikel definieert vervolgens de *elektronische communicatiedienst*:

‘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.’

---

<sup>21</sup> Wet van 22 mei 1997, houdende regels omtrent de economische mededinging (Mededingingswet).

<sup>22</sup> HvJ EG, zaak C62/86 AKZO v. Commissie, Jur. 1991, p. I-1453.

<sup>23</sup> Ontleend aan Prof. mr. P.J. Slot e.a., Inleiding mededingingsrecht, Boom Juridische uitgevers, Den Haag 2002.

WiFi is dus reeds te classificeren als een elektronisch communicatienetwerk. Het is ook een elektronische communicatiedienst omdat via het WiFi-netwerk signalen worden overgebracht. De inhoud en het doel van deze signalen zijn niet van belang.

Interessanter wordt het als we ons vervolgens afvragen of het aangeboden WiFi-netwerk ook valt onder de definitie van een *openbare* elektronische communicatiedienst van artikel 1.1 sub g Tw:

‘elektronische communicatiedienst die beschikbaar is voor het publiek.’

Sub h van artikel 1.1 Tw, het openbaar elektronisch communicatienetwerk:

‘elektronisch communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om openbare elektronische communicatiediensten aan te bieden, waaronder mede wordt begrepen een netwerk, bestemd voor het verspreiden van programma's voor zover dit aan het publiek geschiedt.’

Pas als er gekeken wordt naar de gevolgen van het zijn van een openbaar netwerk of een openbare dienst, wordt duidelijk waarom het verschil tussen het *openbaar* of *niet-openbaar* zijn zo belangrijk is. Een aanbieder van een openbaar netwerk of een openbare dienst dient zich te registreren bij de OPTA, zoals blijkt uit artikel 2.1 lid 1 Tw jo. artikel 1.1 sub b. Dit bestaat uit het indienen van een formulier met de noodzakelijke gegevens. Daarnaast is men een registratievergoeding en een jaarvergoeding verschuldigd. De registratievergoeding voor 2004 was €450,-, de jaarlijkse bijdrage voor het toezicht bedroeg voor een openbare elektronische communicatiedienst € 2.810,- en voor het aanbieden van een openbaar elektronisch communicatienetwerk zelfs €7.760,-.<sup>24</sup> Dit zijn nogal forse bedragen voor een ondernemer die zijn klanten slechts een extraatje wil bieden in de vorm van draadloze internettoegang in zijn café of winkel. Aan de andere kant zijn het redelijke bedragen voor commerciële uitbaters van WiFi, zoals KPN.

Naast deze registratie kent de Telecommunicatiewet nog een aantal verplichtingen voor openbare aanbieders. Artikel 11.2 tot en met 11.5a Tw zien op de bescherming van de persoonsgegevens en de persoonlijke levenssfeer. Krachtens artikel 11.2 Tw dient de aanbieder van een openbare elektronische communicatiedienst of een communicatienetwerk zorg te dragen voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk, dan wel zijn dienst. Artikel 11.3 Tw werkt dit verder uit met verplichtingen aangaande de veiligheid van het netwerk en de beveiliging van de opslag van de persoonsgegevens, alsmede een mededelingsplicht van de mogelijke beveiligingsrisico's aan de eindgebruiker. Artikel 11.5 Tw geeft aan wat de aanbieder van een dienst of netwerk mag met de verkeersgegevens en hoe lang hij deze mag bewaren. In principe mag hij verkeersgegevens gekoppeld met persoonlijke gegevens zolang bewaren als hij wettelijk de tijd heeft te factureren aan de desbetreffende klant. Daarna mogen verkeersgegevens alleen nog geanonimiseerd bewaard worden of met persoonsgegevens als de klant daarvoor toestemming geeft in het kader van marktonderzoek of levering van diensten met toegevoegde waarde.

Belangrijk is ook artikel 11.5a Tw. Dit artikel handelt over de locatiegegevens van de eindgebruiker. Deze mogen slechts beperkt worden bewaard, alleen als de gegevens zijn geanonimiseerd of als de eindgebruiker toestemming heeft gegeven tot verwerking van de gegevens ten behoeve van levering van een dienst met toegevoegde waarde. Hierbij is ook het begrip location based services van belang. Dit houdt in dat van een gebruiker de locatiegegevens worden aangewend om een dienst te verlenen, zoals informatie over een gebouw waar de gebruiker langsloopt, een aanbieding van de bakker op die locatie of een spel

---

<sup>24</sup> Regeling vergoedingen OPTA 2004, WJZ 3073685.

zoals het hotspots spel dat ontwikkeld wordt door de Hogeschool voor de Kunsten te Utrecht.<sup>25</sup> Hierbij moet de gebruiker dus vooraf toestemming geven voor het gebruik van de locatiegegevens. Dit geldt te meer voor reclame-uitingen, artikel 11.7 Tw geeft aan dat hiervoor ook altijd vooraf toestemming moet worden gegeven, het zogenaamde opt-in systeem. Dit alles geldt voor natuurlijke personen krachtens artikel 11.8 Tw.

De aftapbaarheidsverplichting van het netwerk of de dienst is geregeld in artikel 13.1 tot en met 13.5 Tw. Vooral artikel 13.1 Tw is van belang, dit bepaalt dat het openbare netwerk of de dienst alleen dan mag worden gebruikt als het de mogelijkheid heeft om afgetapt te kunnen worden. De overige artikelen zijn vooral bevoegdheidsverleningen en verwijzingen naar de juiste regelgeving.

Zoals gezegd gelden al deze regels dus voor *openbare* elektronische communicatienetwerken of openbare diensten. Is een netwerk niet openbaar, dan gelden deze regels dus ook niet.

Bekijken we het WiFi-netwerk en de daaraan gekoppelde diensten, dan zien we dat er verschillen bestaan met een gewoon communicatienetwerk. Wat de wireless accessprovider namelijk doet is het draadloos doorsluizen van een aansluiting met een fixed accessprovider, dat is de internet service provider. De fixed accessprovider levert de dienst en heeft (of gebruikt) het netwerk. Hij is de registratieplichtige in de zin van artikel 2.1 Tw en hij heeft de aftapverplichting. De wireless accessprovider geeft alleen een draadloos netwerkaansluitpunt. Hij bepaalt of hierop een ieder, dan wel alleen zijn klanten of geregistreerde gebruikers toegang hebben. Dit is het verschil tussen een open of een closed netwerk. De grens van het openbaar aanbieden van een elektronisch communicatienetwerk of een openbare dienst blijkt daar echter niet te liggen. Het bedrijf Surfnet, dat de verschillende universitaire netwerken koppelt en daarnaast ook eigen draadloze WiFi-netwerken exploiteert in de studentensteden is een goed voorbeeld. Zij hebben een wireless access point dat gratis en vrij toegankelijk is voor studenten en medewerkers van de opleidingsinstituten, en betaald voor andere gebruikers.<sup>26</sup> Er is altijd een registratie nodig, allereerst om te controleren of men recht heeft op gratis of betaalde toegang. Daarnaast kan zo een stukje beveiliging worden ingebouwd. Surfnet is niet geregistreerd bij de OPTA. Zij biedt namelijk alleen maar de toegang aan, het draadloze netwerkcontact. Het is de achterliggende internet serviceprovider die de dienst levert, namelijk toegang tot internet.

De spelers in dit onderzoek kunnen hier lering uit trekken. Door het registreren van de gebruikers, of het beperkt uitdelen van toegangscode, bijvoorbeeld alleen aan klanten, blijft het netwerk buiten de openbaarheid. Bijkomend voordeel is dat men het netwerk kan beveiligen voor ongewenste bezoekers zoals hackers en meelifers. Met deze maatregelen wordt voorkomen dat men zich moet registreren bij de OPTA. De aftapbaarheidsverplichting ligt bij de internet service provider. Dat is degene waar het wireless accesspoint uiteindelijk fysiek mee verbonden is, bijvoorbeeld Planet Internet of KPN.

#### **4.4 Misbruik en aansprakelijkheid**

Het hebben van een WiFi-netwerk is één, het beheren en beveiligen ervan is weer een heel ander punt. Er is geen wettelijke beveiligingsverplichting zolang het geen *openbaar* beschikbaar netwerk betreft, omdat de Telecommunicatiewet dan niet van toepassing is op het netwerk. Het kan echter toch zeer handig zijn om het netwerk wel te beveiligen en een soort van logboek bij te houden. Beveiliging is alleen al om die reden interessant, omdat dan voorkomen kan worden dat het voor een buitenstaander al te makkelijk wordt om op het netwerk te komen en de afzonderlijke computers van gebruikers te kunnen benaderen of de snelheid nadelig te kunnen beïnvloeden. Ook voorkomt men met een beveiliging dat het netwerk eenvoudig kan worden aangewezen als een openbaar netwerk.

---

<sup>25</sup> <http://wifi.hku.nl>

<sup>26</sup> <http://www.surfnet.nl>

Juridisch gezien geeft het beveiligen een bepaalde waarborg en een signaal. Men beveiligt een netwerk omdat men niet wil dat onbevoegden er gebruik van maken. Doen zij dit toch dan kunnen zij aansprakelijk worden gesteld, bijvoorbeeld via de onrechtmatige daad van artikel 6:162 Burgerlijk Wetboek (BW). De onrechtmatigheid van het gedrag is dan immers al gegeven omdat men de beveiliging omzeilt. Ook strafrechtelijk maakt dit de zaak een stuk makkelijker. Computervredebreuk, artikel 138a Strafrecht (Sr), is aanwezig als er een beveiliging wordt omzeild of doorbroken, dan wel als men een valse hoedanigheid aanneemt. Een beveiliging is dus onontbeerlijk voor een beroep op dit artikel.

Daarnaast kan het van belang zijn te weten wat de gebruikers voor activiteiten ontplooiën op het netwerk, omdat deze gedragingen onrechtmatig kunnen zijn. Denk hierbij van het uiten van doodsbedreigingen op een forum, het verspreiden van kinderporno, het illegaal verspreiden van auteursrechtelijk beschermd materiaal of het hacken van een website. Bij een strafrechtelijk onderzoek daarnaar zal men proberen de dader te vinden. Maar wie is nu de dader? Het algemene externe IP-adres is het adres dat bij de andere kant vermeld wordt als het verbindende adres. Het IP-adres is vergelijkbaar met een telefoonnummer. Aan dit adres zitten dus ook verdere gegevens gekoppeld, zoals de naam van de gebruiker. Het IP-adres van het accesspoint is in beginsel het IP-adres van de boosdoener. Immers, alleen intern heeft de gebruiker van dit accesspoint een apart IP-nummer, het zogenaamde interne IP-nummer. Als er verder niets wordt bijgehouden of men gewoon niet weet wie er op het accesspoint inloggen, dan kan de daadwerkelijke dader ook niet worden aangewezen. De accesspointhebbende zou dan in theorie wel eens zelf aansprakelijk kunnen zijn voor de gedraging. Er kan immers niet bewezen worden dat het een ander was dan de accesspointhebbende. Dit is uiteraard onwenselijk.

Deze aansprakelijkheidsvraag is inmiddels vervat in het privaatrecht. Na de Scientology-uitspraak<sup>27</sup> is artikel 6:196c BW totstandgekomen. De rechter hanteerde in deze zaak het volgende criterium: 'een internet service provider hoeft geen vooraf toezicht uit te oefenen op het door de gebruikers gepubliceerde, maar dient na kennisname van de onrechtmatigheid van deze publicaties passende maatregelen te treffen.' Het ingevoegde artikel 196c bepaalt in lid 1 dat degene die niet het initiatief neemt tot doorgifte van de informatie, niet bepaalt aan wie de informatie wordt doorgegeven en de doorgegeven informatie niet heeft geselecteerd of gewijzigd, niet aansprakelijk is voor de doorgegeven informatie.

Lid 1.

Degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het doorgeven van van een ander afkomstige informatie of het verschaffen van toegang tot een communicatienetwerk is niet aansprakelijk voor de doorgegeven informatie indien:

- a. niet het initiatief tot het doorgeven van de informatie neemt;
- b. niet degene is die bepaalt aan wie de informatie wordt doorgegeven; en
- c. hij de doorgegeven informatie niet heeft geselecteerd of gewijzigd.

Daarvoor is het van belang dat degene die doorsluis, diensten van de informatiemaatschappij verricht zoals bedoeld in artikel 3:15d BW: 'Onder dienst van de informatiemaatschappij wordt verstaan elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn.' De WiFi-provider verricht in deze zin een dienst van de informatiemaatschappij. De aanbieder daarvan is dus als puur doorgiftepunt niet privaatrechtelijk aansprakelijk voor de doorgegeven informatie. Op grond van artikel 6:196c lid 4 BW is de aanbieder niet aansprakelijk als hij niet redelijkerwijs weet of behoort te weten dat de informatie onrechtmatig is, dan wel deze direct verwijdt nadat hij het wel redelijkerwijs weet of behoorde te weten.

---

<sup>27</sup> Rb. Den Haag 9 juni 1999 LJN-nummer AA1039.

De strafrechtelijke aansprakelijkheid voor de doorgegeven informatie is in het huidige recht nog niet afdoende geregeld en theoretisch kan een acces provider aansprakelijk worden gesteld voor de aangeboden informatie, als de gebruiker niet te achterhalen valt. In het wetsvoorstel Computercriminaliteit II<sup>28</sup> wordt een wijziging van de artikelen 53 en 418 van het Wetboek van Strafrecht voorgesteld met als doel de acces provider die zonder opzet handelt buiten schot te houden. Het voorstel voor artikel 53 Sr bepaalt dat de tussenpersoon niet als zodanig wordt vervolgd indien de tussenpersoon zijn identiteit bekend heeft gemaakt bij de verspreiding van de informatie, dan wel gegevens heeft verstrekt waardoor die informatie kan worden achterhaald. Voorts is de tussenpersoon niet aansprakelijk als de tussenpersoon de gegevens van de dader vrijgeeft na een eerste aanmaning, afgegeven bij het gerechtelijk vooronderzoek of de dader bekend is. Ook is de tussenpersoon niet aansprakelijk als hij na eerste aanmaning al het redelijkerwijs mogelijke heeft gedaan om verdere verspreiding van de informatie te voorkomen. Artikel 418 Sr houdt een strafbaarstelling in indien de tussenpersoon hier niet aan voldoet. Let wel dat deze artikelen de tussenpersoon definiëren als 'een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in woord, beeld of geluid afkomstig van derden.'. Wellicht valt de aanbieder van het wireless access point niet geheel onder deze definitie. Zijn dienst is echter dezelfde en daarom biedt dit wetsvoorstel een duidelijke aanwijzing.

Om de theoretische strafrechtelijke aansprakelijkheid voor de aangeboden informatie niet te dragen, is het nodig om te weten wie de uiteindelijke gebruiker is. Privaatrechtelijk biedt artikel 6:196c BW inmiddels een bescherming. Voor het voorkomen van de theoretische strafrechtelijke aansprakelijkheid zal men allereerst de gebruikers moeten gaan registreren om er achter te komen wie welk interne IP-adres gebruikt. Dit adres wordt immers vrijwel altijd automatisch toegewezen door het accespoint. Een mogelijk bestaat in de vorm van het MAC-adres. Dit is een uniek nummer, dat gekoppeld is aan de netwerkkaart die wordt gebruikt. Iedere netwerkkaart heeft er één, omdat het nummer nodig is voor een goede begeleiding van de verschillende datapakketjes. Het MAC-adres is echter wel te wijzigen of te verhullen middels software. Het MAC-adres wordt ook niet geregistreerd bij de aankoop van een netwerkkaart, dus zal de aanbieder van een WiFi-netwerk dit zelf moeten doen. Een registratie met een unieke gebruikersnaam en wachtwoord is daarom een betere optie. Daarbij is van belang dat zijn register dan voldoet aan de eisen gesteld in artikel 8 van de Wet Bescherming Persoonsgegevens. Sub a van dit artikel geeft aan dat de betrokkene voor de verwerking van zijn persoonsgegevens ondubbelzinnig toestemming moet geven. De gegevens moeten alleen voor eigen gebruik bestemd zijn. De toestemmingverlening kan bijvoorbeeld gebeuren door middel van een beginscherm dat de gebruiker van het WiFi access point te zien krijgt en waar hij naast het aanmaken van een gebruikersnaam en wachtwoord toestemming geeft voor de verwerking van zijn persoonsgegevens, dan wel middels een formulier dat hij ondertekent. Gebruik bij het onderzoek naar strafbare feiten van deze gegevens is dan mogelijk. De persoonsgegevens mogen worden verwerkt krachtens sub d van dit artikel. Het betreft een noodzakelijke gegevensverwerking ter vrijwaring van een vitaal belang van de betrokkene. Naast de registratie van de gebruikers moet de eigenaar van het WiFi-netwerk er voor zorgen dat hij in ieder geval de inloggegevens verzamelt. Zo kan hij zien wie er wanneer via zijn accespoint communiceert. Dit is met unieke gebruikersnamen minder moeilijk.

De registratie van de inloggegevens kan gecombineerd worden met de toegangverlening tot het netwerk. Zo blijft er een gesloten groep van gebruikers. Daarnaast moet er bepaald worden welk netwerkverkeer er plaats vond zodat gedrag gekoppeld kan worden aan de persoon. Dit betekent wel een inbreuk op de privacy. De netwerkbeheerder kan immers zien met welk IP-adres de gebruiker contact had middels zijn accespoint en wanneer. Er zullen derhalve goede waarborgen moeten zijn voor de bescherming van de privacy en persoonsgegevens van de gebruiker. Een mogelijkheid is het gebruik van een computer die alle informatie bijhoudt, vergaart en opbergt in een digitale kluis, zonder dat de opgeslagen informatie direct beschikbaar is. Deze computer

---

<sup>28</sup> Handelingen Tweede Kamer 26 671 1-2, vergaderjaar 1998-1999.

moet worden afgeschermd van het netwerk en internet, om te verhinderen dat derden de informatie kunnen bemachtigen.

Aangezien de wireless accessprovider alleen maar een doorgeefluik is, een draadloos netwerkaansluitpunt biedt, ligt de eindaansprakelijkheid bij de voorliggende fixed accessprovider of internet service provider. Het is echter aan te bevelen zelf een registratie bij te houden van de klanten die gebruik maken van het draadloos netwerk. Door deze registratie te combineren met het uitdelen van de netwerktoegang en de bijpassende wachtwoorden levert dit een minimum aan administratieve werkzaamheden een maximum aan voordeel op. Niet alleen is het netwerk niet openbaar, maar bij problemen en onrechtmatigheden door een van de gebruikers, kan deze via de registratiegegevens snel worden opgespoord.

In de praktijk blijkt echter dat de professionele access providers geen goed voorbeeld geven. Zij registreren de gebruikers niet of nauwelijks. Ook zijn zij naar eigen zeggen niet aansprakelijk voor de aangeboden informatie, de klant draagt aansprakelijkheid. Er zijn dan ook niet of nauwelijks algemene voorwaarden te vinden bij deze aanbieders. Men is dus niet echt bang voor juridische aansprakelijkheid.

## 5 Conclusies en aanbevelingen

De vraag die in dit onderzoek centraal staat, luidt: *‘Wat zijn de rechten en plichten van de spelers, die niet als primair bedrijfsdoel telecommunicatie en datacommunicatie hebben, op de markt voor WiFi?’*.

De eerste deelvraag die daarbij gesteld werd was: *‘Wat zijn nu eigenlijk de rollen op de markt voor WiFi en wie zijn de spelers?’*. Deze deelvraag is beantwoord in hoofdstuk drie. Daar zagen we dat er verschillende rollen zijn op deze markt, maar dat de belangrijkste rollen voor dit onderzoek die van locatiehouder en wireless accessprovider zijn. Hier bleek ook dat er vele soorten spelers zijn die deze rollen kunnen vervullen. Zeker de rol van wireless accessprovider is voor vrijwel iedereen bereikbaar en toegankelijk.

De tweede deelvraag in dit onderzoek was: *‘Welke regelgeving is van toepassing op de kleine spelers op de markt van WiFi’*. In hoofdstuk vier zagen we dat dit voornamelijk de Telecommunicatiewet is, voor wat betreft elektronische communicatienetwerken en –diensten. Specifieke regelgeving voor WiFi is er (nog) niet. Voor wat betreft antenneplaatsing kan de Woningwet geraadpleegd worden. De Mededingingswet kan vervolgens een houvast bieden bij problemen met een locatiehouders met een economische machtspositie. Voor wat betreft aansprakelijkheid van derden is artikel 6:162 en volgende van het Burgerlijk Wetboek van belang. Het artikel 6:196c BW en het wetsvoorstel Computercriminaliteit II betreffen de mogelijke aansprakelijkheid voor de aangeboden informatie.

De derde deelvraag sloot daar op aan: *‘Kan de relevante regelgeving direct worden toegepast op de eerder geïdentificeerde spelers op de markt?’*. In hoofdstuk vier is gebleken dat de regelgeving voor een groot deel gewoon kan worden toegepast op de spelers en de technieken. Zij levert problemen op voor wat betreft het begrip **‘openbaar’** in de Telecommunicatiewet. Het zou voor de spelers binnen de WiFi-markt, maar ook anderen waar de Telecommunicatiewet op van toepassing is, goed zijn als het begrip openbaar werd omschreven in artikel 1.1 van deze wet. Jurisprudentie is er nog niet over dit begrip in de Telecommunicatiewet. Daardoor ontwikkelt de markt zelf de grenzen, zoals het genoemde voorbeeld van marktpartij Surfnet in paragraaf 4.3. Voor de wireless accessprovider heeft dit als voordeel dat hij dus geen openbaar netwerk beheert en geen openbare dienst aanbiedt, hij hoeft dus niet aan allerlei verplichtingen te voldoen die bij een openbaar netwerk of een openbare dienst horen.

De hoofdvraag is uiteindelijk beantwoord in hoofdstuk vier. De rechten die ‘kleine’ spelers hebben zijn het vrije gebruik van de frequenties voor WiFi en de apparatuur die aan de gestelde normen voldoen, behorende bij die frequenties. Daarnaast hebben ze de mogelijkheid om met die apparatuur een wireless access point op te richten, zodat klanten of gebruikers via het access point kunnen inloggen op het internet of een soortgelijk netwerk. Dit behoudens storingen. Bij storingen heeft de wireless accessprovider de plicht om er iets aan te doen. Ook als de ene wireless accessprovider storing ondervindt van de andere wireless accessprovider, zijn beiden gehouden maatregelen te nemen.

Omdat de wireless accessprovider slechts een draadloos netwerkaansluitpunt creëert en in feite alleen doorgeefluik is, is dit niet aan te merken als een *openbaar* netwerk of een *openbare* dienst. Daardoor hoeft hij niet te voldoen aan allerlei verplichtingen die de Telecommunicatiewet stelt voor openbare netwerken, zoals een registratieplicht van het netwerk en aftapbaarheid. Deze plichten liggen immers al bij de voorliggende fixed accessprovider of internet service provider, waar het wireless access point toegang toe geeft.

Het is de wireless accessprovider aan te bevelen om de gebruikers van het access point te registreren, om bij problemen de gebruiker te kunnen identificeren en de veiligheid van het netwerk te garanderen.

Dit alles bij elkaar overziend kan gesteld worden dat het voor een MKB-ondernemer, gemeente of horeca-instelling niet moeilijk is om voor de eigen klanten een wireless netwerkaansluitpunt te creëren. Zodra men echter een geheel vrij toegankelijk en dus openbaar netwerk in de zin van de Telecommunicatiewet wil opzetten, doet men er verstandig aan om dit te laten opzetten en beheren door een professioneel bedrijf. Zo voorkomt men zelf registratieplichtig te worden bij de OPTA en aftapbaarheid mogelijk te maken.

Een wireless access provider is slechts een doorgeefluik, terwijl de achterliggende internet service provider het openbare netwerk beheert. Een hele geruststelling voor de wireless access provider, er is nu geen registratieplicht. Zijn aansprakelijkheid is middels een technisch eenvoudig systeem te beperken. Het aanmaken van een unieke gebruikersnaam en een uniek wachtwoord zijn voldoende.



## Geraadpleegde bronnen

### Literatuur:

- H. Bouwman e.a., ITER 65: Interconnectie: het vaste telefoonnet, het mobiele net en internet, SDU, Den Haag 2004
- D. Briere, Draadloos netwerken voor dummies, Addison Wesley, Amsterdam 2003
- J.M.E. van Bruegel en E.J. Daalder, Telecommunicatierecht : de parlementaire geschiedenis van de Telecommunicatiewet, Sdu uitgevers, Den Haag 1999
- E.J. Dommering, Handboek telecommunicatierecht, SDU, Den Haag 1999
- E.J. Dommering, Zes jaar bestuur en rechtspraak in de telecommunicatiemarkt, Cramwinckel, Amsterdam 2003
- Mr. N. Doorduyn, Wi-Fi, een juridisch buitenbeentje in opmars, in JAVI nr. 6, 2004 p. 205-210
- H. Franken e.a., ITER 63, Zeven essays over informatietechnologie en recht, SDU, Den Haag 2003
- H. Franken, H.W.K. Kaspersen, A.H. de Wild, Recht en Praktijk: Recht en computer, Kluwer, Deventer 1997
- ICTrust in opdracht van de gemeente Utrecht, 2ConnectU/Wireless Internet: een praktische haalbaarheidsstudie, 2003
- G. Nijssse, Veilig ondernemen, Academic Service, Den Haag 2004
- P.W.M. Rutten, M. Poel, Marktontwikkelingen in de digitale infrastructuur : knelpunten bij de toegankelijkheid en de pluriformiteit van de digitale snelweg, Rathenau instituut, Den Haag 2002
- M.H.M. Schellekens, Aansprakelijkheid van Internetaanbieders, In eigen beheer, Maastricht 2001
- B.W. Schemer, ITER 64: Opsporing vs. Privacy in peer-to-peer netwerken, SDU, Den Haag 2003
- A.H.J. Schmidt e.a., Telecommunicatiewet : de tekst van de Telecommunicatiewet voorzien van commentaar met toevoeging van aanverwante nationale en Europese regelgeving, Kluwer, Deventer 2001
- Prof. mr P.J. Slot e.a., Inleiding mededingingsrecht, Boom Juridische uitgevers, Den Haag 2002
- H. van Steenis, Computable ICT woordenboek 2003, VNU Business Publications, Haarlem 2002
- J.S. Svensson, S. Zouridis, Waarden en normen in de virtuele wereld : twee verkennende studies met discussie, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente 2004
- A. Wagemans, B.B. van Bockstaele, Snelgids WiFi, Easy Computing, Haarlem 2003

### Tijdschriften:

- Computer Totaal Praktijkgids Thuisnetwerk najaar 2004
- C'T Magazine September 2004
- Juridische Aspecten van Internet, JAVI, verschillende jaargangen

### Digitale bronnen:

<http://www.howstuffworks.com/wireless-network.htm>

Artikel over werking van draadloze netwerken

<http://www.netkwesties.nl/editie88/artikel2.php>

Artikel over WiFi

<http://www.senter.nl/asp/page.asp?id=i000014&alias=sec>

Subsidieregeling elektronische communicatie via het Ministerie van Economische Zaken

<http://www.wirelessleiden.nl>

Site van de WiFi-community te Leiden



## Bijlagen relevante Wet- en Regelgeving

### I Burgerlijk Wetboek

#### Artikel 3:15d

1. Degene die een dienst van de informatiemaatschappij verleent, maakt de volgende gegevens gemakkelijk, rechtstreeks en permanent toegankelijk voor degenen die gebruik maken van deze dienst, in het bijzonder om informatie te verkrijgen of toegankelijk te maken:

- a. zijn identiteit en adres van vestiging;
- b. gegevens die een snel contact en een rechtstreekse en effectieve communicatie met hem mogelijk maken, met inbegrip van zijn elektronische postadres;
- c. voor zover hij in een handelsregister of een vergelijkbaar openbaar register is ingeschreven: het register waar hij is ingeschreven en zijn inschrijvingsnummer, of een vergelijkbaar middel ter identificatie in dat register;
- d. voor zover een activiteit aan een vergunningsstelsel is onderworpen: de gegevens over de bevoegde toezichthoudende autoriteit;
- e. voor zover hij een gereguleerd beroep uitoefent:
  - de beroepsvereniging of -organisatie waarbij hij is ingeschreven,
  - de beroepstitel en de lidstaat van de Europese Unie of andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte waar die is toegekend,
  - een verwijzing naar de beroepsregels die in Nederland van toepassing zijn en de wijze van toegang daartoe;
- f. voor zover hij een aan de BTW onderworpen activiteit uitoefent: het btw-identificatienummer zoals bedoeld in artikel 2a, eerste lid, onder g, van de Wet op de Omzetbelasting 1968.

2. De dienstverlener geeft aanduidingen van prijzen in een dienst van de informatiemaatschappij duidelijk en ondubbelzinnig aan, met de uitdrukkelijke vermelding of, en zo mogelijk welke, belasting en leveringskosten daarbij inbegrepen zijn.

3. Onder dienst van de informatiemaatschappij wordt verstaan elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn. Een dienst wordt langs elektronische weg verricht indien deze geheel per draad, per radio, of door middel van optische of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen met behulp van elektronische apparatuur voor de verwerking, met inbegrip van digitale compressie, en de opslag van gegevens.

#### Artikel 6:162

1. Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden.

2. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond.

3. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.

#### Artikel 6:196c

1. Degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het doorgeven van van een ander afkomstige informatie of het verschaffen van toegang tot een communicatienetwerk is niet aansprakelijk voor de doorgegeven informatie, indien hij:

- a. niet het initiatief tot het doorgeven van de informatie neemt;
- b. niet degene is die bepaalt aan wie de informatie wordt doorgegeven; en

- c. hij de doorgegeven informatie niet heeft geselecteerd of gewijzigd.
- 2. Voor de toepassing van lid 1 wordt onder het enkele doorgeven van van een ander afkomstige informatie en het enkele verschaffen van toegang tot een communicatienetwerk mede verstaan de geautomatiseerde, tussentijdse en tijdelijke opslag van de doorgegeven informatie, voor zover deze opslag uitsluitend geschiedt ten behoeve van het doorgeven van die informatie en de duur van deze opslag niet langer is dan daarvoor redelijkerwijs noodzakelijk is.
- 3. Degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het geautomatiseerd, tussentijds en tijdelijk opslaan van een ander afkomstige informatie voor zover het opslaan enkel geschiedt om het later doorgeven van die informatie aan anderen op hun verzoek doeltreffender te maken, is niet aansprakelijk voor het geautomatiseerd, tussentijds en tijdelijk opslaan van de informatie indien hij:
  - a. de informatie niet wijzigt;
  - b. de toegangsvoorwaarden voor de informatie in acht neemt;
  - c. de in de bedrijfstak geldende of gebruikelijke regels betreffende de bijwerking van de informatie naleeft;
  - d. niet de in de bedrijfstak geldende of gebruikelijke technologie voor het verkrijgen van gegevens over het gebruik van de informatie wijzigt, en
  - e. prompt de nodige maatregelen neemt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken, zodra hij weet dat de informatie is verwijderd van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe onmogelijk is gemaakt, of dat een bevoegde autoriteit heeft bevolen de informatie te verwijderen van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe heeft verboden.
- 4. Degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het op verzoek opslaan van een ander afkomstige informatie, is niet aansprakelijk voor de opgeslagen informatie, indien hij:
  - a. niet weet van de activiteit of informatie met een onrechtmatig karakter en, in geval van een schadevergoedingsvordering, niet redelijkerwijs behoort te weten van de activiteit of informatie met een onrechtmatig karakter, dan wel
  - b. zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt.
- 5. Het hiervoor bepaalde staat niet in de weg aan het verkrijgen van een rechterlijk verbod of bevel.

## **II Mededingingswet**

### Artikel 24

- 1. Het is ondernemingen verboden misbruik te maken van een economische machtspositie.
- 2. Het tot stand brengen van een concentratie als omschreven in artikel 27 wordt niet aangemerkt als het misbruik maken van een economische machtspositie.

## **III Regeling gebruik van frequentieruimte zonder vergunning**

### Artikel 1

De gebruiker van frequentieruimte waarvoor geen vergunning is vereist, zorgt ervoor dat door het gebruik van het gewenste signaal van het radiozendapparaat geen storing of belemmering wordt veroorzaakt in andere radiozendapparaten dan wel in overige elektrische of elektronische apparaten.

### Artikel 2

- 1. Als categorieën radiozendapparaten, bedoeld in artikel 3.4, eerste lid, onder a, van de Telecommunicatiewet, worden aangewezen:
  - a. randapparaten die bestemd zijn voor aansluiting op een mobiel openbaar telefoonnetwerk;

- b. randapparaten die bestemd zijn voor aansluiting op een openbaar satellietstelsel, ten behoeve van mobiele communicatie, met uitzondering van het nood-, spoed en veiligheidsverkeer;
  - c. randapparaten, zijnde koordloze telefoons, die bestemd zijn voor aansluiting op een openbaar telefoonnetwerk op een vaste locatie, mits de in bijlage 1 aangegeven frequentiebanden en de daarbij behorende gebruiksvoorschriften in acht worden genomen;
  - d. radiozendapparaten voor algemene radiocommunicatie in de 27 MHz-frequentieband (CB), mits de in bijlage 2 aangegeven frequentiebanden en de daarbij behorende gebruiksvoorschriften in acht worden genomen;
  - e. randapparaten die bestemd zijn voor aansluiting op een openbaar telecommunicatienetwerk ten behoeve van plaatsbepaling;
  - f. mobiele VHF/UHF radiozendapparaten voor landmobiel gebruik die daadwerkelijk en krachtens een daartoe gesloten overeenkomst onderdeel zijn van een besloten netwerk, dat deel is van een radionetwerk met dynamische frequentietoewijzing ten behoeve waarvan een vergunning is verleend voor het gebruik van frequentieruimte (trunkinginstallatie);
  - g. mobiele radiozendapparaten behorend tot een digitaal radionetwerk met dynamische frequentietoewijzing, mits de in bijlage 3 aangegeven frequentieband en de daarbij behorende gebruiksvoorschriften in acht worden genomen;
  - h. mobiele UHF radiozendapparaten, werkend in de frequentieband 446 MHz, bedoeld voor algemeen gebruik ten behoeve van spraak over korte afstand (PMR 446), mits de in bijlage 4 aangegeven frequentiebanden en de daarbij behorende gebruiksvoorschriften in acht worden genomen;
  - i. randapparaten, zijnde satellietgrondstations, mits de in bijlage 5 aangegeven frequentiebanden en de daarbij behorende gebruiksvoorschriften in acht worden genomen;
  - j. randapparaten voor mobiele communicatie via ionisatiesporen van meteoren, mits de in bijlage 6 aangegeven frequentieband en de daarbij behorende gebruiksvoorschriften in acht worden genomen;
  - k. de in bijlage 7 bedoelde categorieën radiozendapparaten, mits de in die bijlage aangegeven frequentiebanden en de daarbij behorende gebruiksvoorschriften in acht worden genomen.
2. Onder de aanwijzing, bedoeld in het eerste lid, vallen slechts apparaten die voldoen aan het bij of krachtens het Besluit randapparaten en radioapparaten bepaalde.

Bijlage 7 behorend bij artikel 2, eerste lid, onder k

Categorie 3 Radiozendapparaten bestemd voor Local Area Netwerken, RLANs

	Frequentieband	Vermogen	Kanaalraster	Duty-cycle
A	2400–2483.5 MHz	100 mW e.i.r.p.	–	–
B	5150–5350 MHz	200 mW e.i.r.p.	–	–
C	5470–5725 MHz	1 W e.i.r.p.	–	–
D	17.1–17.3 GHz	100 mW e.i.r.p.	–	–

#### IV Wetboek van Strafrecht

Artikel 138a

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredsbreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij

- a. daarbij enige beveiliging doorbreekt of
  - b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.
2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredsbreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een

geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.

3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens

- a. met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;
- b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

## **V Telecommunicatiewet**

### Artikel 1.1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

- a. Onze Minister: Onze Minister van Economische Zaken;
- b. college: college, genoemd in artikel 2 van de Wet Onafhankelijke post- en telecommunicatieautoriteit;
- c. directeur-generaal van de Nederlandse mededingingsautoriteit: directeur-generaal van de Nederlandse mededingingsautoriteit, bedoeld in artikel 2, tweede lid, van de Mededingingswet;
- d. nationale regelgevende instantie: instantie in een andere lidstaat van de Europese Unie die krachtens het recht van die lidstaat is belast met een of meer regelgevende of daarmee verband houdende uitvoerende taken die zijn toegekend in de richtlijnen nrs. 2002/19/EG, 2002/20/EG, 2002/21/EG, 2002/22/EG of 2002/58/EG;
- e. elektronisch communicatienetwerk: transmissiesystemen, waaronder mede begrepen de schakel- of routeringsapparatuur en andere middelen, die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, waaronder satellietnetwerken, vaste en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt en netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie;
- f. elektronische communicatiedienst: 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. Het omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van de notificatierichtlijn die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken;
- g. openbare elektronische communicatiedienst: elektronische communicatiedienst die beschikbaar is voor het publiek;
- h. openbaar elektronisch communicatienetwerk: elektronisch communicatienetwerk dat geheel of hoofdzakelijk wordt gebruikt om openbare elektronische communicatiediensten aan te bieden, waaronder mede wordt begrepen een netwerk, bestemd voor het verspreiden van programma's voor zover dit aan het publiek geschiedt;
- i. aanbieden van een elektronisch communicatienetwerk: het bouwen, exploiteren, beheren of beschikbaar stellen van een elektronisch communicatienetwerk;
- j. bijbehorende faciliteiten: bij een elektronisch communicatienetwerk of een elektronische communicatiedienst behorende faciliteiten die het aanbieden van diensten via dat netwerk of die dienst mogelijk maken of ondersteunen, alsmede systemen voor voorwaardelijke toegang en elektronische programmagidsen;
- k. netwerkaansluitpunt: fysiek punt waarop een abonnee de toegang tot een openbaar communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het netwerkaansluitpunt bepaald door middel van een specifiek netwerkadres, dat met een abonneenummer of -naam kan zijn verbonden;
- l. toegang: het aan een andere onderneming beschikbaar stellen van netwerkonderdelen, bijbehorende faciliteiten of diensten onder uitdrukkelijke voorwaarden al dan niet op exclusieve

basis ten behoeve van het aanbieden van elektronische communicatiediensten of het verspreiden van programma's aan het publiek door die onderneming;

m. interconnectie: specifiek type toegang dat wordt gerealiseerd tussen exploitanten van openbare netwerken, inhoudende het fysiek en logisch verbinden van openbare communicatienetwerken die door dezelfde of een andere onderneming worden gebruikt om het de gebruikers van een onderneming mogelijk te maken te communiceren met die van dezelfde of van een andere onderneming of toegang te hebben tot diensten die door een andere onderneming worden aangeboden;

n. gebruiker: natuurlijke persoon of rechtspersoon die gebruik maakt van of verzoekt om een openbare elektronische communicatiedienst;

o. eindgebruiker: natuurlijke persoon of rechtspersoon die van een openbare elektronische communicatiedienst gebruik maakt of wil gaan maken en die niet tevens openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten aanbiedt;

p. abonnee: natuurlijke persoon of rechtspersoon die partij is bij een overeenkomst met een aanbieder van openbare elektronische communicatiediensten voor de levering van dergelijke diensten;

q. consument: natuurlijke persoon die gebruik maakt van of verzoekt om een openbare elektronische communicatiedienst voor andere dan bedrijfs- of beroepsdoeleinden;

r. onderneming: onderneming in de zin van artikel 81, eerste lid, van het Verdrag tot oprichting van de Europese Gemeenschap;

s. onderneming die beschikt over een aanmerkelijke marktmacht: onderneming die alleen of tezamen met andere ondernemingen over een economische kracht beschikt die haar in staat stelt zich in belangrijke mate onafhankelijk van haar concurrenten, klanten en uiteindelijk consumenten te gedragen;

t. transnationale markt: bij beschikking, bedoeld in artikel 15, vierde lid, van richtlijn nr. 2002/21/EG, gedefinieerde markt die ten minste een gedeelte van Nederland beslaat;

u. huurlijn: publiekelijk ter beschikking gestelde transparante transmissiecapaciteit tussen twee netwerkaansluitpunten van een of meer elektronische communicatienetwerken, zonder routeringsfuncties waarover gebruikers kunnen beschikken als onderdeel van de geleverde huurlijn;

v. minimumpakket van huurlijnen: door de Commissie van de Europese Gemeenschappen op grond van de artikelen 17 en 22 van richtlijn nr. 2002/21/EG of de artikelen 18 en 37 van richtlijn nr. 2002/22/EG vastgesteld minimumpakket van huurlijnen, zoals vermeld in een lijst van in het Publicatieblad van de Europese Gemeenschappen gepubliceerde normen;

w. openbaar telefoonnetwerk: elektronisch communicatienetwerk dat wordt gebruikt om openbare telefoondiensten aan te bieden; het ondersteunt de overdracht tussen netwerkaansluitpunten van spraakcommunicatie en ook andere vormen van communicatie, zoals fax en data;

x. openbare telefoondienst: dienst die voor het publiek beschikbaar is voor uitgaande en binnenkomende gesprekken;

y. programma: programma als bedoeld in artikel 1, eerste lid, onder f, van de Mediawet;

z. kabels: kabels en de daarbij behorende ondersteuningswerken, beschermingswerken en signaalinrichtingen, alsmede inrichtingen, bestemd om daarin verbinding tot stand te brengen tussen kabels in, op of boven openbare gronden enerzijds en kabels in gebouwen en daarmee één geheel vormende gronden anderzijds dan wel tussen laatstgenoemde kabels onderling;

aa. openbare gronden:

- 1°. openbare wegen met inbegrip van de daartoe behorende stoepen, glooiingen, bermen, sloten, bruggen, viaducten, tunnels, duikers, beschoeiingen en andere werken;
- 2°. wateren met de daartoe behorende bruggen, plantsoenen, pleinen en andere plaatsen, die voor eenieder toegankelijk zijn;

bb. nummer: cijfers, letters of andere symbolen, al dan niet in combinatie, die bestemd zijn voor toegang tot of identificatie van gebruikers, netwerkexploitanten, diensten, netwerkaansluitpunten of andere netwerkelementen;

cc. nummeridentificatie:

1°. faciliteit om het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd aan het opgeroepen netwerkaansluitpunt te verstrekken, voordat de verbinding tot stand wordt gebracht;

2°. faciliteit om het nummer van het opgeroepen netwerkaansluitpunt dan wel het nummer waarmee een individuele gebruiker kan worden geïdentificeerd aan het oproepende netwerkaansluitpunt te verstrekken, voordat de verbinding tot stand wordt gebracht;

dd. in de handel brengen: het voor de eerste maal afleveren na vervaardiging in de Europese Economische Ruimte, het invoeren in de Europese Economische Ruimte uit een land daarbuiten, alsmede het in gebruik nemen na vervaardiging of invoer uit een land buiten de Europese Economische Ruimte in de Europese Economische Ruimte;

ee. openbaar telecommunicatienetwerk: elektronisch communicatienetwerk dat geheel of gedeeltelijk wordt gebruikt om openbare telecommunicatiediensten aan te bieden, voor zover het netwerk niet gebruikt wordt voor het verspreiden van programma's;

ff. openbare telecommunicatiedienst: voor het publiek beschikbare dienst die geheel of gedeeltelijk bestaat in het overbrengen van signalen via een elektronisch communicatienetwerk, voor zover deze dienst niet bestaat uit het verspreiden van programma's;

gg. apparaten: elektrische en elektronische apparaten alsmede uitrustingen en installaties, die elektrische of elektronische componenten bevatten;

hh. randapparaten:

1°. apparaten die bestemd zijn om op een openbaar telecommunicatienetwerk te worden aangesloten, zodanig dat zij:

a. rechtstreeks op netwerkaansluitpunten kunnen worden aangesloten, of

b. kunnen dienen voor interactie met een openbaar telecommunicatienetwerk via directe of indirecte aansluiting op netwerkaansluitpunten ten behoeve van de overbrenging, verwerking of ontvangst van informatie;

2°. radiozendapparaten die geschikt zijn om op een openbaar telecommunicatienetwerk te worden aangesloten;

3°. apparaten voor satellietgrondstations tenzij bij of krachtens hoofdstuk 10 anders is bepaald, doch met uitsluiting van speciaal geconstrueerde apparatuur die bedoeld is voor gebruik als onderdeel van een openbaar telecommunicatienetwerk;

ii. radiozendapparaten: apparaten die naar hun aard bestemd zijn voor het zenden of het zenden en ontvangen van radiocommunicatiesignalen;

jj. elektromagnetische compatibiliteit: eigenschap van apparaten, om op bevredigende wijze in hun elektromagnetische omgeving te kunnen functioneren zonder zelf elektromagnetische storingen te veroorzaken die ontoelaatbaar zijn voor alles wat zich in die omgeving bevindt;

kk. systeem voor voorwaardelijke toegang: elke technische maatregel of regeling waarbij toegang tot een beschermde radio- of televisie-omroepdienst in begrijpelijke vorm afhankelijk wordt gemaakt van een abonnement of een andere vorm van voorafgaande individuele machtiging;

ll. applicatieprogramma-interface: een software interface tussen externe toepassingen, die beschikbaar is gesteld door omroepen, dienstenleveranciers, alsmede de hulpmiddelen in de eindapparatuur;

mm. Internationaal Telecommunicatieverdrag: het op 22 december 1992 te Genève tot stand gekomen Statuut en Verdrag van de Internationale Unie voor Telecommunicatie met de daarbij behorende bijlagen en reglementen (Trb. 1993, 138), de op 14 oktober 1994 te Kyoto tot stand gekomen Akten van wijziging van het Statuut en het Verdrag van de Internationale Unie voor Telecommunicatie (Trb. 1995, 201) en de op 6 november 1998 te Minneapolis tot stand gekomen Akten van wijziging van het Statuut en het Verdrag van de Internationale Unie voor Telecommunicatie (Trb. 2001, 90);

nn. richtlijn nr. 2002/19/EG: Richtlijn nr. 2002/19/EG van het Europees Parlement en de Raad van de Europese Unie van 7 maart 2002 inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten (Toegangsrichtlijn) (PbEG L 108);



oo. richtlijn nr. 2002/20/EG: Richtlijn nr. 2002/20/EG van het Europees Parlement en de Raad van de Europese Unie van 7 maart 2002 betreffende de machtiging voor elektronische-communicatienetwerken en -diensten (Machtigingsrichtlijn) (PbEG L 108);

pp. richtlijn nr. 2002/21/EG: Richtlijn nr. 2002/21/EG van het Europees Parlement en de Raad van de Europese Unie van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (Kaderrichtlijn) (PbEG L 108);

qq. richtlijn nr. 2002/22/EG: Richtlijn nr. 2002/22/EG van het Europees Parlement en de Raad van de Europese Unie van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten (Universeledienstrichtlijn) (PbEG L 108);

rr. certificaat: elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt;

ss. gekwalificeerd certificaat: certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid, en is afgegeven door een certificatie dienstverlener die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid;

tt. certificatie dienstverlener: een natuurlijke persoon of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent;

uu. middel voor het aanmaken van elektronische handtekeningen: geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van elektronische handtekeningen te implementeren;

vv. veilig middel voor het aanmaken van elektronische handtekeningen: een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid;

ww. elektronische handtekening: elektronische handtekening als bedoeld in artikel 15a, vierde lid, van Titel 1, afdeling 1A van Boek 3 van het Burgerlijk Wetboek;

xx. ondertekenaar: voor de toepassing van deze wet geldt de definitiebepaling van artikel 15a, vijfde lid, van Titel 1, afdeling 1A van Boek 3 van het Burgerlijk Wetboek;

yy. openbare betaaltelefoon: voor het publiek toegankelijk telefoontoestel waarmee uitgaande gesprekken gevoerd kunnen worden en waarvan de betaling voor het gebruik kan geschieden door middel van munten, krediet- of debetkaarten of vooruitbetaalde telefoonkaarten;

zz. notificatierichtlijn: richtlijn nr. 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 en regels betreffende de diensten van de informatiemaatschappij (PbEG L 204).

### Artikel 2.1

1. Degene die een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst aanbiedt dan wel bijbehorende faciliteiten aanlegt of aanbiedt, met uitzondering van degene die een elektronische programmagids aanbiedt, doet daarvan mededeling aan het college.
2. Het college stelt vast welke gegevens bij de mededeling aan het college worden overgelegd, alsmede de wijze waarop de mededeling wordt gedaan. Die gegevens betreffen in ieder geval de naam, het adres, de vestigingsplaats, respectievelijk de woonplaats en een beschrijving van de in het eerste lid bedoelde netwerken, diensten of faciliteiten. Het college doet hiervan mededeling in de Staatscourant.
3. De gegevens, bedoeld in het tweede lid, worden slechts verzameld ten behoeve van de goede uitvoering van deze wet en zijn beperkt tot hetgeen strikt noodzakelijk is voor het vaststellen van de identificatie van degene, bedoeld in het eerste lid.
4. Het college registreert degene, bedoeld in het eerste lid, na ontvangst van de in dat lid bedoelde mededeling en de daarbij behorende gegevens.
5. Voor het aanbieden of afgeven van gekwalificeerde certificaten aan het publiek is een registratie door het college vereist van de certificatie dienstverlener die in Nederland een vestiging heeft. Bij de aanvraag van een registratie legt de certificatie dienstverlener documenten over waaruit de overeenstemming met de bij en krachtens artikel 18.15, eerste en tweede lid,

bedoelde eisen blijkt. Het college is bevoegd te bepalen welke andere gegevens bij de aanvraag van een registratie dienen te worden overgelegd.

6. Een certificatie dienstverlener waarvan door een organisatie als bedoeld in artikel 18.16, eerste lid, is vastgesteld dat wordt voldaan aan de eisen, gesteld bij of krachtens artikel 18.15, eerste en tweede lid, kan om te voldoen aan het bepaalde krachtens de tweede volzin van het vijfde lid, volstaan met het overleggen van een geldig bewijs van die vaststelling.

### Artikel 3.3

1. Voor het gebruik van frequentieruimte is een vergunning vereist van Onze Minister welke op aanvraag kan worden verleend.

2. Vergunningen voor het gebruik van frequentieruimte ten behoeve van de uitvoering van vitale overheidstaken, van het verzorgen van taken op het terrein van de publieke omroep bedoeld in artikel 1, onder t, van de Mediawet, of ter uitvoering van een wettelijk voorschrift worden bij voorrang verleend. Onverminderd het derde lid bepaalt Onze Minister, in overeenstemming met het gevoelen van de ministerraad, in hoeverre en in welke omvang vergunningen voor het gebruik van frequentieruimte anders dan voor de uitvoering van de in artikel 13c, eerste lid, van de Mediawet, genoemde taak van de publieke omroep bij voorrang worden verleend. Bij regeling van Onze Minister, in overeenstemming met Onze Minister van Onderwijs, Cultuur en Wetenschappen, wordt bij de vaststelling van de omvang van de frequentieruimte die aan de publieke omroepinstellingen bij voorrang bij vergunning wordt verleend, bepaald welke technische eigenschappen de uitzendingen van de programma's van de publieke omroepinstellingen dienen te hebben.

3. Bij het verlenen van vergunningen voor het gebruik van frequentieruimte op het terrein van de publieke omroep wordt het navolgende in acht genomen:

- a. voor ieder programmanet als bedoeld in artikel 40, eerste en derde lid van de Mediawet, wordt ten minste een vergunning verleend op zodanige wijze dat een landelijk bereik van het programma mogelijk is en rekening wordt gehouden met artikel 16 van de Mediawet;
- b. voor iedere provincie wordt ten minste één vergunning voor het gebruik van frequentieruimte verleend ten behoeve van de uitzending van het radioprogramma, bedoeld in artikel 1, onder j, van de Mediawet, van de instelling die ten behoeve van de desbetreffende provincie zendtijd voor regionale omroep heeft verkregen, op zodanige wijze, dat een provinciaal bereik van het programma mogelijk is;
- c. indien in een provincie aan twee of meer regionale omroepinstellingen op grond van de Mediawet zendtijd is toegewezen, zal, onverminderd artikel 3.6, aan elk van de omroepinstellingen vergunning voor het gebruik van frequentieruimte worden verleend voor een bereik dat ten minste gelijk is aan de onderscheidene verzorgingsgebieden, voorzover dit technisch mogelijk is;
- d. aan iedere instelling die op grond van de Mediawet voor lokale omroep zendtijd heeft verkregen, zal, onverminderd artikel 3.6, ten behoeve van de uitzending van haar radioprogramma vergunning voor het gebruik van frequentieruimte worden verleend voor een bereik dat ten minste gelijk is aan het verzorgingsgebied van het programma, voorzover dit technisch mogelijk is, en een doelmatig gebruik van het frequentiespectrum zich daartegen niet verzet.

4. De verlening van vergunningen in andere gevallen dan bedoeld in het tweede lid geschiedt:

- a. op volgorde van binnenkomst van de aanvragen;
- b. door middel van een vergelijkende toets, al dan niet met inbegrip van een financieel bod, of
- c. door middel van een veiling.

5. De keuze voor toepassing van een van de procedures, bedoeld in het vierde lid, geschiedt door Onze Minister, met dien verstande dat voorzover het de verlening van vergunningen voor het gebruik van frequentieruimte door of ten behoeve van commerciële omroepinstellingen als bedoeld in artikel 1, onder dd, van de Mediawet betreft, de keuze geschiedt door Onze Minister in overeenstemming met Onze Minister van Onderwijs, Cultuur en Wetenschappen. Daarbij wordt, met inachtneming van het frequentieplan en het beginsel van non-discriminatie, tevens nader de bestemming van de frequentieruimte bepaald waarop de keuze betrekking heeft.

6. Voorzover de in het vijfde lid bedoelde keuze betrekking heeft op het al dan niet toepassen van het financiële bod bij de toepassing van de vergelijkende toets, geschiedt deze tevens in overeenstemming met Onze Minister van Financiën.

7. Nadat op grond van een op basis van het vijfde en zesde lid gemaakte keuze een vergunning voor een bepaalde bestemming is verleend, wordt, zolang er in die bestemming nog houders van vergunningen voor het gebruik van frequentieruimte zijn, bij elke volgende uitgifte van frequentieruimte voor die bestemming een vergelijkbare procedure toegepast, tenzij dit ten gevolge van gewijzigde omstandigheden betreffende het gebruik van die frequentieruimte niet langer leidt tot een optimaal gebruik van frequentieruimte.

8. De uitvoering van de procedure, bedoeld in het vierde lid, onder b, geschiedt indien het de verlening van vergunningen voor het gebruik van frequentieruimte door of ten behoeve van commerciële omroepinstellingen betreft, door Onze Minister van Onderwijs, Cultuur en Wetenschappen in overeenstemming met Onze Minister.

9. Bij of krachtens algemene maatregel van bestuur worden, met inachtneming van richtlijn nr. 2002/20/EG, regels gesteld terzake van de verlening, wijziging en verlenging van vergunningen. Deze regels hebben in ieder geval betrekking op:

- a. de eisen die, voorafgaande aan een van de procedures, bedoeld in het vierde lid, aan een aanvrager worden gesteld om in aanmerking te komen voor een vergunning,
- b. de toepassing en uitvoering van de procedures, bedoeld in het vierde lid, en
- c. de criteria die worden toegepast bij een vergelijkende toets als bedoeld in het vierde lid, onder b.

10. Onze Minister kan besluiten dat een of meer aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten worden uitgesloten van het verkrijgen van een vergunning voor het gebruik van bij dat besluit te bepalen frequentieruimte indien die vergunning wordt verleend volgens een procedure als bedoeld in het vierde lid, onder b, of onder c, met dien verstande dat dit slechts kan geschieden indien dat met het oog op de totstandbrenging of instandhouding van daadwerkelijke mededinging noodzakelijk is.

11. De vergunning wordt verleend voor een bij die vergunning te bepalen termijn. De vergunning kan worden verlengd met een door Onze Minister te bepalen termijn.

#### Artikel 3.4

1. In afwijking van artikel 3.3 is geen vergunning vereist voor gebruik van in het frequentieplan aangewezen frequentieruimte die:

- a. al dan niet tezamen met bij ministeriële regeling aan te wijzen categorieën van radiozendapparaten voor een in het frequentieplan aangegeven bestemming door eenieder mag worden gebruikt;
- b. tot gebruik strekt van door Onze Minister aan te wijzen overheidsorganen, belast met de zorg voor de veiligheid van de staat, de defensie alsmede de handhaving van de rechtsorde.

2. Bij of krachtens algemene maatregel van bestuur worden regels gesteld terzake van het gebruik van de aangewezen frequentieruimte, bedoeld in het eerste lid, alsmede terzake van de aanwijzing, bedoeld in het eerste lid, onderdeel a.

#### Artikel 11.2

Onverminderd de Wet bescherming persoonsgegevens en het overigens bij of krachtens deze wet bepaalde dragen de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk, onderscheidenlijk zijn dienst.

#### Artikel 11.3

1. De in artikel 11.2 bedoelde aanbieders treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen,

rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.

2. De in artikel 11.2 bedoelde aanbieders dragen er zorg voor dat de abonnees worden geïnformeerd over:

- a. bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;
- b. de eventuele middelen waarmee de onder a bedoelde risico's kunnen worden tegengegaan, voor zover het andere maatregelen betreft dan die welke de aanbieder op grond van het eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten.

#### Artikel 11.4

1. De aanbieder van een openbare elektronische communicatiedienst is verplicht de abonnee op diens verzoek:

- a. geleverde elektronische communicatiediensten door middel van geheel of gedeeltelijk niet-gespecificeerde nota's in rekening te brengen;
- b. de mogelijkheid te bieden kosteloos en op eenvoudige wijze de doorschakeling van oproepen van derden naar het bij hem in gebruik zijnde netwerkaansluitpunt ongedaan te maken.

2. Bij algemene maatregel van bestuur kunnen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van oproepende gebruikers en opgeroepen abonnees regels worden gesteld met betrekking tot het specificeren van nota's voor geleverde elektronische communicatiediensten. Deze regels kunnen onder meer betrekking hebben op de toekenning van rechten aan abonnees, de behandeling van klachten, de verstrekking van informatie en de vergoeding van kosten. Bij de algemene maatregel van bestuur kunnen aan het college taken worden opgedragen en bevoegdheden verleend.

3. Bij algemene maatregel van bestuur kunnen regels worden gesteld ten aanzien van de keuzemogelijkheden voor de wijze van betaling van geleverde elektronische communicatiediensten.

#### Artikel 11.5

1. De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst verwijderen dan wel anonimiseren de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees of gebruikers, zodra deze verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie, onverminderd het tweede, derde en vijfde lid.

2. De aanbieder mag verkeersgegevens verwerken die noodzakelijk zijn voor facturering, waaronder het opstellen van een factuur voor een abonnee of voor degene die zich tegenover de aanbieder rechtens verbonden heeft die factuur te voldoen, dan wel ten behoeve van een betaling van verleende toegang. De verkeersgegevens mogen worden verwerkt tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen.

3. De aanbieder van elektronische communicatiediensten mag voorts de in het eerste lid bedoelde verkeersgegevens verwerken, voor zover en voor zolang dat noodzakelijk is voor:

- a. marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, of
- b. de levering van diensten met toegevoegde waarde, mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor zijn toestemming heeft gegeven. De abonnee of gebruiker kan de gegeven toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

4. De aanbieder stelt de abonnee of gebruiker in kennis van de soorten verkeersgegevens die worden verwerkt voor de in het tweede en derde lid bedoelde doeleinden alsmede omtrent de duur van de verwerking. Voor zover het de verwerking van verkeersgegevens ten behoeve van de doeleinden, bedoeld in het derde lid betreft, wordt de desbetreffende informatie verstrekt voorafgaand aan het verkrijgen van de in dat lid bedoelde toestemming van de abonnee of gebruiker.

5. De verwerking van verkeersgegevens in overeenstemming met het eerste tot en met vierde lid mag alleen geschieden door personen die werkzaam zijn onder het gezag van de aanbieder voor facturering, verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude alsmede marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.
6. De aanbieder mag de verkeersgegevens verstrekken aan personen en instanties die zijn belast met de berechting van enig geschil dan wel de beslissing van een geschil als bedoeld in de artikelen 12.1, 12.2 voor zover van toepassing, of 12.9.

#### Artikel 11.5a

1. De verwerking van locatiegegevens, niet zijnde verkeersgegevens, betreffende abonnees of gebruikers van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten, is slechts geoorloofd, indien:
  - a. deze gegevens zijn geanonimiseerd, of
  - b. de desbetreffende abonnee of gebruiker voor de verwerking van deze gegevens toestemming heeft gegeven ten behoeve van de levering van een dienst met toegevoegde waarde.
2. Voorafgaand aan het verkrijgen van toestemming als bedoeld in het eerste lid, onderdeel b, verstrekt de aanbieder van de toegevoegde waardedienst aan de abonnee of gebruiker de volgende informatie:
  - a. de soort locatiegegevens die zullen worden verwerkt;
  - b. de doeleinden waarvoor de locatiegegevens worden verwerkt;
  - c. de duur van de verwerking, en
  - d. of de gegevens aan een derde zullen worden verstrekt ten behoeve van de levering van de dienst met toegevoegde waarde.
3. De verwerking van de gegevens ten behoeve van de levering van een dienst met toegevoegde waarde als bedoeld in het eerste lid, onderdeel b, is slechts toegestaan voor zover en voor zolang dat noodzakelijk is voor de levering van de desbetreffende dienst. In afwijking van de eerste volzin mag de aanbieder van de dienst met toegevoegde waarde die gegevens verwerken die noodzakelijk zijn voor het opstellen van een factuur. Artikel 11.5, tweede lid, laatste volzin, is van overeenkomstige toepassing.
4. Een abonnee of gebruiker kan de verleende toestemming voor de verwerking van de hem betreffende gegevens op elk moment intrekken.
5. De aanbieder van een dienst met toegevoegde waarde biedt aan de abonnee of gebruiker wiens gegevens worden verwerkt de mogelijkheid om kosteloos en op eenvoudige wijze de verwerking van diens gegevens tijdelijk te beletten voor elke overbrenging van communicatie of elke verbinding met het openbare elektronische communicatienetwerk dat gebruikt wordt voor de levering van de desbetreffende dienst.
6. De verwerking van de gegevens mag slechts plaatsvinden door personen die werkzaam zijn onder het gezag van de aanbieder of de derde, bedoeld in het tweede lid, onder d, en is beperkt tot die gegevens die noodzakelijk zijn om de dienst met toegevoegde waarde te kunnen aanbieden.

#### Artikel 11.7

1. Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is uitsluitend toegestaan, mits de verzender kan aantonen dat de desbetreffende abonnee daarvoor voorafgaand toestemming heeft verleend, onverminderd hetgeen is bepaald in het tweede lid.
2. Een ieder die elektronische contactgegevens voor elektronische berichten heeft verkregen in het kader van de verkoop van zijn product of dienst mag deze gegevens gebruiken voor het overbrengen van communicatie voor commerciële, ideële of charitatieve doeleinden met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische

contactgegevens, en, indien de klant hiervan geen gebruik heeft gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Artikel 41, tweede lid, van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing.

3. Bij het gebruik van elektronische berichten voor de in het eerste lid genoemde doeleinden dienen te allen tijde de volgende gegevens te worden vermeld:

- a. de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht, en
- b. een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten.

4. Het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is toegestaan, tenzij de desbetreffende abonnee te kennen heeft gegeven dat hij communicatie waarbij van deze middelen gebruik wordt gemaakt, niet wenst te ontvangen en indien de abonnee bij elke overgebrachte communicatie de mogelijkheid wordt geboden om verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Aan de abonnee worden in dat geval geen kosten in rekening gebracht van voorzieningen waarmee wordt voorkomen dat hem een ongevraagde communicatie wordt overgebracht.

#### Artikel 11.8

De toepassing van de artikelen 11.6 en 11.7 is beperkt tot abonnees die natuurlijke personen zijn.

#### Artikel 13.1

1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten stellen hun telecommunicatienetwerken en telecommunicatiediensten uitsluitend beschikbaar aan gebruikers indien deze aftapbaar zijn.

2. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de technische aftapbaarheid van openbare telecommunicatienetwerken en openbare telecommunicatiediensten.

#### Artikel 13.2

1. Aanbieders van openbare telecommunicatienetwerken zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld.

2. Aanbieders van openbare telecommunicatiediensten zijn verplicht medewerking te verlenen aan de uitvoering van een bevel op grond van het Wetboek van Strafvordering dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van door hen verzorgde telecommunicatie.

3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen organisatorische en personele maatregelen en te treffen voorzieningen met betrekking tot aftappen.

#### Artikel 13.2a

1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126n of artikel 126u van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens over een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst en het telecommunicatieverkeer met betrekking tot die gebruiker.

2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de aanbieders aan de vordering of het verzoek voldoen en de wijze waarop de gegevens, bedoeld in het eerste lid, beschikbaar worden gehouden.

### Artikel 13.3

Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot het beslechten van geschillen tussen aanbieders en de bevoegde autoriteiten over de voorzieningen door middel van welke de door een tap te verkrijgen telecommunicatie door aanbieders wordt doorgegeven.

### Artikel 13.4

1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126na, eerste lid, of 126ua, eerste lid, van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het verstrekken van gegevens terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een openbaar telecommunicatienetwerk dan wel een openbare telecommunicatiedienst.

2. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten voldoen aan een vordering op grond van artikel 126na, tweede lid, of 126ua, tweede lid, van het Wetboek van Strafvordering dan wel een verzoek op grond van artikel 29 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het op bij algemene maatregel van bestuur te bepalen wijze achterhalen en verstrekken van de gegevens, bedoeld in het eerste lid. Teneinde aan deze verplichting te kunnen voldoen bewaren de aanbieders bij algemene maatregel van bestuur aan te wijzen gegevens voor een periode van drie maanden, vanaf het tijdstip waarop deze gegevens voor de eerste maal zijn verwerkt.

3. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de aanbieders aan een vordering of een verzoek, bedoeld in het eerste en tweede lid, voldoen en de wijze waarop de gegevens, bedoeld in het eerste lid, beschikbaar worden gehouden.

### Artikel 13.5

1. Aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zijn verplicht gegevens met betrekking tot een bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2 dan wel een vordering of een verzoek als bedoeld in artikel 13.2a of artikel 13.4, eerste of tweede lid te beveiligen tegen kennisneming door onbevoegden alsmede geheimhouding te betrachten met betrekking tot deze gegevens.

2. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de te nemen maatregelen in verband met de beveiliging, bedoeld in het eerste lid.

## **VI Wet bescherming persoonsgegevens**

### Artikel 8

Persoonsgegevens mogen slechts worden verwerkt indien:

- a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
- b. de gegevensverwerking noodzakelijk is voor de uitvoering van de overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van de overeenkomst;
- c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
- d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
- e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
- f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het

belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

## **VII Wetsvoorstel Computercriminaliteit II**

*Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie  
Handelingen Tweede Kamer 26 671 1-2, vergaderjaar 1998-1999*

### Artikel 53 Strafrecht komt te luiden

1. Bij misdrijven gepleegd door de drukpers of door enig ander middel voor de openbaarmaking of verspreiding van uitingen in woord, beeld of geluid, wordt de tussenpersoon als zodanig niet vervolgd, indien:

- a. de tussenpersoon bij de openbaarmaking of verspreiding zijn identiteit heeft bekendgemaakt dan wel gegevens heeft verstrekt waardoor zijn identiteit kan worden achterhaald;
- b. de dader bekend is dan wel de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle aanwijzingen heeft gegeven die redelijkerwijs van hem kunnen worden geveerd teneinde de dader te achterhalen, en
- c. de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle handelingen heeft verricht die redelijkerwijs van hem kunnen worden geveerd ter voorkoming van verdere verspreiding;

2 Bij de beoordeling van de strafbaarheid van de tussenpersoon worden alleen die uitingen in aanmerking genomen waarop zijn opzet was gericht.

3 Onder de tussenpersoon, bedoeld in dit artikel, wordt verstaan: een persoon die zijn beroep of bedrijf maakt van openbaarmaking of verspreiding van uitingen in woord, beeld of geluid afkomstig van derden.

### Artikel 418 Strafrecht komt te luiden

1. Hij die als tussenpersoon opzettelijk enige uiting in woord, beeld of geluid van strafbare aard afkomstig van een ander openbaar maakt of verspreidt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie, indien:

- a. de tussenpersoon bij de openbaarmaking of verspreiding noch zijn identiteit heeft bekendgemaakt, noch gegevens heeft verstrekt waardoor zijn identiteit kan worden achterhaald;
- b. noch de dader bekend is, noch de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, alle aanwijzingen heeft gegeven die redelijkerwijs van hem kunnen worden geveerd teneinde de dader te achterhalen;
- c. de tussenpersoon op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, heeft nagelaten alle handelingen te verrichten die redelijkerwijs van hem kunnen worden geveerd ter voorkoming van verdere verspreiding.

2. Onder de tussenpersoon, bedoeld in het eerste lid, wordt verstaan: een persoon die zijn beroep of bedrijf maakt van de openbaarmaking of verspreiding van uitingen in woord, beeld of geluid afkomstig van derden.