

Privacy en telecommunicatiediensten

Van Ma Bell naar Big Brother?

door

R.A. Smit

Aard: Afstudeerverslag

Omvang: 94 pagina's

Datum: 22 november 1991

TECHNISCHE UNIVERSITEIT DELFT

Faculteit der Elektrotechniek

Vakgroep Telecommunicatie- en

Verkeersbegeleidingssystemen

Hoogleraar: Prof. dr. J.C. Arnbak

Begeleiders: Prof. ir. C. de Jong

Ir. J.R. Westerveld

Codenummer: A-440

Periode: maart 1991 - november 1991

Trefwoorden: Privacy, intelligente net, C7-signalering, telecommunicatiediensten,
faciliteiten

Voorwoord

Dit afstudeerverslag is tot stand gekomen bij de vakgroep Telecommunicatie- en Verkeersbegeleidingssystemen van de Faculteit der Elektrotechniek aan de Technische Universiteit Delft.

Geconstateerd kan worden dat een verdieping in de privacy-problematiek een multidisciplinaire aangelegenheid is waarbij juridische, technische en sociologische aspecten een rol spelen. Dit is mede wat het onderwerp van dit verslag enerzijds zo boeiend anderzijds zo moeilijk te doorgronden maakt.

Ik bedank hier ir. J.R. Westerveld voor zijn adviezen. In het bijzonder bedank ik prof. ir. C. de Jong voor de persoonlijke begeleiding bij het uitvoeren van mijn onderzoek. Uit de gesprekken die wij met elkaar hadden zijn waardevolle opmerkingen, ideeën en suggesties voortgekomen.

R.A. Smit,

's-Gravenhage, 22 november 1991.

Inhoudsoverzicht

Voorwoord	iii
Samenvatting	ix
Summary	x
1. Inleiding	1
2. Privacy	3
2.1. Privacy in de telecommunicatie	3
2.1.1. Inhoud van de communicatie	3
2.1.2. Totstandkoming van de communicatie	4
2.2. Wat is privacy?	5
2.2.1. Persoonsgegevens en persoonsregistratie	6
2.3. Relaties tussen privacy en gegevens in de telecommunicatie	8
2.4. Samenvatting	10
3. Diensten in een modern telecommunicatienet	11
3.1. Netdiensten en tele-informatiediensten	11
3.2. Basisdiensten en supplementaire diensten	13
3.3. Faciliteiten, functies en diensten	14
3.4. Samenvatting	14
4. Ontwikkelingen in het telecommunicatienet	17
4.1. Een kort historisch overzicht	17
4.2. Signalering	18
4.2.1. Gemeeneweg signalering	20
4.2.2. C7-signalering als basis voor geavanceerde netdiensten	22
4.2.3. Signaleringsboodschappen	23

4.3.	Het intelligente net	24
4.3.1.	Het concept	24
4.3.2.	Architectuur	25
4.4.	ISDN	28
4.5.	Mobiele communicatie	29
4.5.1.	Het GSM-netwerksysteem	29
4.6.	Het datanet	33
4.6.1.	Schakelprincipes	33
4.6.2.	Pakketvorm en overdracht	34
4.6.3.	Netdiensten in een datanet	34
4.7.	Componenten in een modern telecommunicatienet	35
4.8.	Samenvatting	37
5.	Koppeling van systemen	39
5.1.	Fysieke koppeling	39
5.2.	Koppeling van gegevensbestanden	40
5.3.	Het privacyaspect van koppelingen	41
5.4.	Samenvatting	41
6.	Knelpunten	43
6.1.	Knelpunten in C7-signalering	43
6.2.	Knelpunten in het intelligente net	45
6.3.	Knelpunten in mobiele communicatie	46
6.4.	Samenvatting	47
7.	Maatregelen om privacy te waarborgen	49
7.1.	Wanneer is privacy gewaarborgd?	49
7.2.	Privacy-beschermende maatregelen	49
7.2.1.	Juridische bescherming	49
7.2.2.	Systeemtechnische en organisatorische bescherming	51
7.2.3.	Sociale bescherming	51

7.2.4.	Technische alternatieven	52
7.3.	Samenvatting	55
8.	Enkele praktijksituaties	57
8.1.	Caller ID	57
8.1.1.	Ontwikkelingen in de Verenigde Staten en in Frankrijk ...	58
8.1.2.	De situatie in Nederland	60
8.1.3.	Europese richtlijn	61
8.2.	Gespecificeerde rekening	62
8.3.	Autotelefoon	63
8.4.	Telegids	64
8.5.	Samenvatting	64
9.	Conclusies en aanbevelingen	65
9.1.	Conclusies	65
9.2.	Aanbevelingen	65
Literatuur		67
Appendix A:	Bepalingen beveiliging en geheimhouding inzake telecommunicatie	71
Appendix B:	Entiteiten bij informationele privacy	73
Appendix C:	Besluit algemene richtlijnen telecommunicatie	75
Appendix D:	COM(90) 314 final-SYN 288, Brussel, 13 september 1990	77
Appendix E:	Enkele actuele krantenknipsels	81
Lijst van afkortingen		83

Samenvatting

Er blijken in de telecommunicatie twee gebieden te onderscheiden met betrekking tot de privacy. Het eerste gebied heeft betrekking op de inhoud van de communicatie. Het tweede gebied heeft betrekking op het feit dat de communicatie tot stand is gebracht. In dit tweede gebied, waarop in dit verslag de nadruk ligt, betreft het gegevens over de abonnee, ten opzichte van zowel de telecommunicatieorganisatie als van degene waarmee gebeld wordt en ieder ander die toegang zou krijgen tot die gegevens. Deze gegevens kunnen de relationele en informationele privacy aantasten. Het onderscheid hiertussen vervaagt, omdat de bedreigingen van beide vormen van privacy in elkaar overvloeien.

In de telecommunicatie worden supplementaire diensten geleverd, die de basisdienst van een gevraagde net- of tele-informatiedienst op een specifiek punt wijzigen of aanvullen. Deze extra diensten kunnen aan de abonnee worden geleverd door gebruik te maken van de gemeneweg signalering C7 en het intelligente net. De knelpunten met betrekking tot de privacy bevinden zich in de functies die nodig zijn om deze supplementaire diensten te kunnen leveren. Hierbij dient een onderscheid te worden gemaakt tussen opslag van gegevens in databases en transport van het abonneenummer over het telecommunicatienet.

Door de fysieke koppeling van netten kunnen verschillende gegevensbestanden gekoppeld worden. Maatregelen voor de bescherming van privacy, die hierdoor bedreigd wordt, kunnen op vier manieren worden gerealiseerd, te weten:

- juridische bescherming;
- systeemtechnische en organisatorische bescherming;
- sociale bescherming;
- technische alternatieven.

Uiteindelijk zijn alle vier nodig om tot een afdoende bescherming van de privacy te komen. Door enkele cases te behandelen wordt het bovenstaande geïllustreerd om een concretere beeldvorming bij de lezer te bereiken.

Summary

There appears to be a distinction between two areas concerning telecommunication privacy. The first area deals with the substance of the message. The second area deals with the fact itself that the communication was made. The second area on which the emphasis will be put in this report, concerns the data of the subscriber both in relation to the telecommunication company and to the party he is calling, as well as any who happens to get admission to the data. These data can affect the relational and the informational privacy. The distinction between these two fades, because the threats are coinciding.

In telecommunications supplementary services modify or augment the basic service offered by a bearer service or teleservice. These supplementary services will be offered to the subscriber making use of common channel signalling system no. 7 and the intelligent network. Bottlenecks, in relation to privacy, are to be found in functional elements, that handle the supplementary services. A distinction however must be made between storage of data in databases and transport of the telephone number of the subscriber.

Due to integration of networks, linking of databases becomes possible. Measures for protection of privacy must be taken and will be realised by:

- legislation;
- security;
- social protection;
- technical alternatives.

Finally all measures must be taken into account if sufficient protection of privacy is required. Discussion of several cases illustrates the above and helps to create a certain impression for the reader.

1. Inleiding

De huidige voortgang van de techniek zorgt ervoor dat er nieuwe diensten c.q. produkten ontstaan, waarmee de samenleving gediend zou zijn. Op het gebied van de telecommunicatie kan daarbij gedacht worden aan het ISDN (Integrated Services Digital Network). Dit systeem doet ons belanden in een tijdperk waarin vele handelingen thuis geregeld kunnen worden. Het uitvoeren van financiële transacties, het bestellen van goederen en het raadplegen van bepaalde gegevens zullen vanaf een terminal plaats gaan vinden. Naast deze zijn er vele andere ontwikkelingen op dit gebied te signaleren.

Feit is echter dat moderne netten voor dit soort communicatie systemen gebruik moeten maken van specifieke gegevens om een bepaalde dienst te kunnen leveren. Een van de gevolgen hiervan kan zijn dat, met deze gegevens, persoonsgebonden informatie beschikbaar komt waaruit de hele handel en wandel van individuen kan worden nagegaan.

In dit afstudeerverslag zal een analyse plaatsvinden van de faciliteiten, de hierbij benodigde functies en de hieruit voortkomende diensten, die naast de huidige basisdiensten, in het moderne telecommunicatienet geleverd kunnen worden. Hierbij wordt nagegaan of en in hoeverre deze diensten een inbreuk op de privacy betekenen. Er zal gebruik worden gemaakt van bestaande theorieën die worden toegepast op de moderne telecommunicatie.

Bij de identificatie van de oproeper (Caller ID) bijvoorbeeld, worden gegevens van de oproeper bij de opgeroepene op een display getoond. Hierbij kan men de vraag stellen of de oproeper dat eigenlijk wel wenst. En wat doet het systeem met deze identificeringsinformatie? Echter identificeert de oproeper zich niet dan is het niet mogelijk de desbetreffende dienst te verlenen. In zo'n geval kan een opgeroepene die een systeem gebruikt dat op deze identificatie is gebaseerd soms minder adequaat reageren dan hij wenst.

Nu staan we dus voor een dilemma: Dienstverlening versus privacy!

In de titel 'Privacy en telecommunicatiediensten' vinden we twee begrippen die in het kader van dit afstudeerverslag een nadere afbakening behoeven. Het eerste begrip, privacy, wordt nader uitgewerkt in hoofdstuk 2. Eerst wordt een aantal gebieden onderscheiden waardoor inbreuk op de privacy in de telecommunicatie kan ontstaan. Vervolgens wordt een nadere invulling aan privacy gegeven waarbij onderscheid wordt gemaakt in relationele en informationele privacy.

In hoofdstuk 3 wordt op het tweede begrip, telecommunicatiediensten, ingegaan. Hier vindt een uiteenzetting plaats van de termen faciliteiten, functies en diensten.

De technische ontwikkeling van het telecommunicatienet wordt besproken in hoofdstuk 4.

In hoofdstuk 5 wordt de (fysieke) koppeling van netten behandeld.

Aan de hand van de besproken ontwikkelingen in het telecommunicatienet wordt in hoofdstuk 6 aangegeven waar de mogelijke knelpunten zitten. Zo komen de begrippen privacy en telecommunicatiediensten samen.

Voor de bescherming van privacy kunnen op verschillende gebieden maatregelen worden genomen. In hoofdstuk 7 wordt hier nader op ingegaan.

Hoofdstuk 8 geeft een aantal praktijksituaties weer, waarin gebruik gemaakt wordt van verscheidene artikelen.

In het afsluitende hoofdstuk 9 worden conclusies getrokken en aanbevelingen gegeven omtrent privacy en telecommunicatie.

2. Privacy

2.1. Privacy in de telecommunicatie

Wanneer we in de telecommunicatie praten over privacy zijn er twee gebieden te onderscheiden. Het eerste gebied heeft betrekking op de inhoud van de communicatie. Inbreuk op de privacy vindt plaats door het opvangen, opnemen etcetera van de boodschappen door een partij anders dan de oproeper of de opgeroepene, bijvoorbeeld het aftappen van een telefoonlijn. Het tweede gebied heeft betrekking op het feit op zich dat de communicatie tot stand is gebracht [1]. Wie gebruikt welke dienst, wanneer en met wie?

Met deze tweedeling zijn we er echter nog niet. Het laatste gebied blijkt namelijk op haar beurt weer onder te verdelen in gegevens¹ welke niet beschikbaar zijn voor de abonnee (deze gegevens zijn uiteraard wel beschikbaar in het systeem) en gegevens welke beschikbaar komen aan de abonnee. Had in het verleden voornamelijk het eerste gebied de aandacht van de wetgever, tegenwoordig zijn zowel het eerste als het tweede gebied van invloed op de privacywetgeving.

2.1.1. Inhoud van de communicatie

Al vanaf dat telefonie algemeen beschikbaar was vindt het aftappen van telefoongesprekken plaats. Dat dit een inbreuk op de privacy betekent zal duidelijk zijn. Ten aanzien van de bescherming van de privacy bestaan er bepalingen tegen het af luisteren van telefoongesprekken. Daarnaast bestaan er afzonderlijke regelingen voor geheimhouding en beveiliging van telegraaf, telex en datanet. In appendix A wordt een overzicht gegeven van deze regelingen.

¹Gegevens: Een weergave van feiten, begrippen of instructies op overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of door geautomatiseerde middelen.

Vergelijk informatie: De betekenis die een persoon toekent aan gegevens op basis van afspraken met betrekking tot die gegevens.
[2]

Toepassing van moderne communicatietechnieken heeft echter tot gevolg dat typen van gegevensoverdracht en -uitwisseling technisch niet meer te onderscheiden zullen zijn. Over één en hetzelfde middel lopen de diverse soorten van gegevens in een zelfde, niet van elkaar te onderscheiden, (gedigitaliseerde) vorm. Dit verschilt van de situatie waarin een duidelijk onderscheid bestaat tussen de communicatievormen: gesprekken liepen over telefoondraden, brieven waren op papier geschreven etcetera. De commissie Franken heeft de betreffende bepalingen nader gestructureerd en aangegeven waar wetswijzigingen wenselijk zouden zijn. [2]

2.1.2. Totstandkoming van de communicatie

Bij de totstandkoming van de communicatie betreft het gegevens over de abonnee, ten opzichte van zowel de telecommunicatieorganisatie, als van degene waarmee gebeld wordt en ieder ander die toegang zou kunnen krijgen tot die gegevens. Gegevens omtrent verzenders en ontvangers, alsmede de aard van het berichtenverkeer, kunnen namelijk worden vastgelegd door partijen bij de gegevensuitwisseling (wie praat met wie, hoelang en wanneer). Naast het verzamelen, opslaan en doorgeven van gegevens kan men personen ook direct volgen in hun dagelijkse communicatie. Voor de telecommunicatieorganisatie ontstaat op deze manier de mogelijkheid de gegevensuitwisseling te analyseren en zo elektronische profielen van abonnees te maken. De tendens in de communicatietechnologie is het-altijd-en-overal-bereikbaar-zijn [3]. Als draadverbindingen hier niet in slagen via nieuwe faciliteiten als 'follow-me' schakelingen, dan zorgt de mobiele communicatie hier wel voor. Daarmee wordt de abonnee in principe traceerbaar, doordat in het telecommunicatiesysteem gegevens over de lokatie van de abonnee worden opgeslagen.

Het zal duidelijk zijn dat abonneegebonden gegevens, die niet direct aan de abonnee ter beschikking staan, wel door de telecommunicatieorganisatie gebruikt kunnen worden. Als deze gegevens op een andere manier gebruikt worden dan waarvoor ze bedoeld zijn, zal duidelijk zijn dat dit een bedreiging van de privacy van de abonnee inhoudt.

Het prijsgeven van abonneegegevens is in bepaalde gevallen een nevenaspect van het telefoongebruik. Hier valt te denken aan de gespecificeerde rekening waarin precies aangegeven wordt met welk nummer de abonnee, hoe lang gebeld heeft. Of 'caller ID' waarbij het nummer van de oproeper zichtbaar wordt gemaakt op een display bij de opgeroepene. Door deze faciliteiten komen gegevens over de abonnee terecht bij degene waarmee gebeld wordt of bij een ieder ander die toegang zou kunnen krijgen tot die gegevens. Ook hier wordt de privacy van de abonnee bedreigd.

Dat de gegevens die vrij (kunnen) komen door het gebruik van de communicatie een aantasting van de privacy van de abonnee kunnen zijn, is iets dat steeds meer onderkend wordt [1]. In het kader van dit verslag, waarin die diensten geanalyseerd zullen worden waarbij persoonsgerichte informatie vrij kan komen, ligt het voor de hand het gebied af te bakenen tot het tweede, de totstandkoming van de communicatie. Het eerste gebied, betrekking hebbend op inhoud van de communicatie, zal in slechts in een enkel geval aangehaald worden.

2.2. Wat is privacy?

Privacy is een van oorsprong Amerikaanse (rechts)term met als Nederlands equivalent 'persoonlijke levenssfeer'. Met alleen deze omschrijving wordt echter nog geen concreet beeld verkregen van wat privacy inhoudt. Als er naar de literatuur gekeken wordt en de betekenissen die er zijn toegekend aan het begrip privacy, kan vastgesteld worden dat twee benaderingen zijn te onderscheiden [4]:

- 1) relationele privacy (selectieve contactlegging)
- 2) informationele privacy (selectieve openbaarmaking).

Relationele privacy houdt een verandering van de persoonlijke vrijheid in, ten gevolge van het lastig gevallen worden. Het gaat hier om het recht op selectieve contactlegging en de controle van het individu over de eigen ruimte en omgeving. Informationele privacy

doelt op een aantasting van de persoonlijke vrijheid ten gevolge van opslag, bewerking en gebruik van gegevens van de betreffende persoon [5]. Het gaat om de controle van een individu over gegevens van zichzelf en over de informatie en de beslissingen die hierop gebaseerd worden.

Het recht op informationele privacy voor het individu wordt vanuit de wet ondersteund, ondermeer vanuit de Grondwet (artikel 10), het Wetboek van Strafrecht (artikel 139 lid a t/m g) en de Wet Persoonsregistraties (WPR). Deze wetten bieden een aantal middelen om aan de invulling van het recht op informationele privacy gestalte te kunnen geven. De plicht van de registratiehouder om informationele privacy te waarborgen wordt vooral door de WPR opgelegd. De relationele privacy wordt slechts in zeer algemene zin door de Grondwet gedekt [6].

2.2.1. Persoonsgegevens en persoonsregistratie

Het begrip persoonsgegeven is zodanig dat ook minder relevante gegevens er onder vallen. Zodra een object gerelateerd is aan een individu vormen namelijk tevens alle, aan het object gerelateerde gegevens, persoonsgegevens. In Nederland wordt deze oprekking geblokkeerd door het begrip persoonsgegeven te beperken tot die gegevens die, gezien de strekking van de Wet Persoonsregistraties, relevant zijn [7].

Een persoonsgegeven wordt in de WPR (artikel 1) als volgt gedefinieerd:

'Persoonsgegeven: een gegeven dat herleidbaar is tot een individuele natuurlijke persoon.'

Het begrip persoonsregistratie (WPR artikel 1) is zeer ruim. De definitie is als volgt:

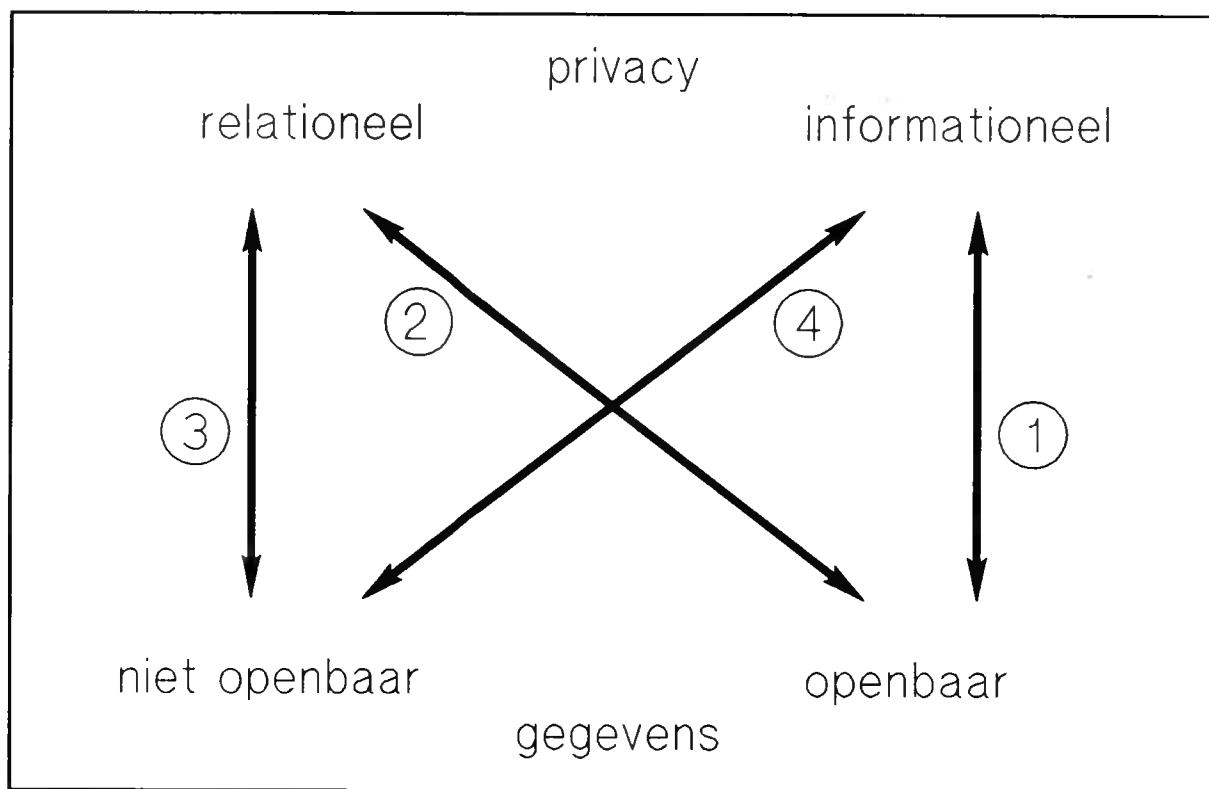
'Persoonsregistratie: Een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens, die langs geautomatiseerde weg

wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd.'

Enerzijds biedt de WPR de enige wettelijke bescherming voor de informationele privacy in netwerken, anderzijds gaat deze wet voorbij aan het dynamische karakter van gegevensstromen in netwerken. Juist door dit dynamische karakter wordt de WPR ondermijnd. Deze problematiek wordt besproken in hoofdstuk 7.

2.3. Relaties tussen privacy en gegevens in de telecommunicatie

Bedreigingen van de relationele en informationele privacy kunnen op verschillende



Figuur 2-1: Relaties tussen privacy en gegevens

manieren ontstaan. Om duidelijk te maken hoe dat kan gebeuren wordt in deze paragraaf het gebied dat betrekking heeft op het feit dat de communicatie tot stand is gebracht in relatie gebracht met deze relationele en informationele privacy. In figuur 2-1 zijn de mogelijke relaties weergegeven.

Openbare gegevens zijn, in deze figuur, gegevens over de abonnee die door de telecommunicatieorganisatie buiten het telecommunicatiesysteem wordt gebracht. Niet openbare gegevens representeren dan vanzelfsprekend gegevens die aan de telecommunicatieorganisatie voorbehouden blijven.

De faciliteit caller ID lijkt in eerste instantie een prachtige beschermer van de relationele privacy. Men kan de privacy van de opgeroepene immers belangrijker noemen dan de

privacy van de oproeper die zonder toestemming contact wil krijgen. De informationele privacy van de oproeper wordt bedreigd door registratie van zijn pogingen tot contactlegging (zie (1) in de figuur). Wat velen echter niet realiseren is dat opgeroepen zich in veel gevallen achteraf zullen moeten verantwoorden aan oproepers waarom zij hen niet mochten spreken. Of bijvoorbeeld, waarom zij hen niet mogen zien bij de toekomstige beeldtelefonie [6].

Wanneer een abonnee door een enquêteur gebeld wordt komt de relationele privacy van de abonnee in het geding. De abonnee krijgt iemand aan de lijn die op basis van het telefoonnummer, verkregen uit het telefoonboek, contact zoekt en om informatie verzoekt (zie (2) in de figuur). Hierbij kan men de vraag stellen of de opgeroepene dat eigenlijk wel wenst. Belt de enquêteur naar aanleiding van eerder verkregen informatie, zoals arbeidsverleden, dan komt ook de informationele privacy in het geding.

Zoals al in paragraaf 2.1.2 vermeld is, is de tendens in de hele communicatietechnologie het-altijd-en-overal-bereikbaar-zijn. Enerzijds duiden deze ontwikkelingen op een communicatiebehoefte, anderzijds hebben zij het effect dat het 'individu tot in de diepste poriën van het maatschappelijke weefsel en in elke omgeving volgbaar wordt' [6]. Het wordt moeilijker zich aan het altijd en overal bereikbaar zijn te onttrekken. Waar men dit wel doet/kan doen zal men zich in toenemende mate moeten verantwoorden. Daarmee komen we op een belangrijke bedreiging van de relationele privacy (zie (3) in de figuur). Tevens ontstaat er een bedreiging van de informationele privacy doordat in het telecommunicatiesysteem gegevens over de lokatie van de abonnee worden opgeslagen (zie (4) in de figuur). De abonnee is immers traceerbaar.

Hieruit komt naar voren hoezeer informationele en relationele privacy met elkaar samenhangen of het nu gaat om het maken van profielen van personen, het afgeven van gegevens bij de contactlegging of het altijd en overal bereikbaar zijn. Het toezicht dreigt algemeen te worden.

2.4. Samenvatting

Er blijken in de telecommunicatie twee gebieden te onderscheiden met betrekking tot de privacy. Het eerste gebied heeft betrekking op de inhoud van de communicatie. Het tweede gebied heeft betrekking op het feit dat de communicatie tot stand is gebracht. In dit tweede gebied betreft het gegevens over de abonnee, ten opzichte van zowel de telecommunicatieorganisatie als van degene waarmee gebeld wordt en ieder ander die toegang zou krijgen tot die gegevens.

In dit rapport ligt de nadruk op het gebied welke betrekking heeft op het feit dat de communicatie tot stand is gebracht.

Tevens is aan het begrip privacy een nadere invulling gegeven. Twee kanten van het begrip privacy zijn hieruit naar voren gekomen, namelijk 'relationele privacy' en 'informationele privacy'. Relationele privacy houdt een inperking van de persoonlijke vrijheid in, ten gevolge van het lastig gevallen worden; informationele privacy doelt op een aantasting van de persoonlijke vrijheid ten gevolge van opslag, bewerking en gebruik van gegevens van de betreffende persoon.

Tot slot zijn de relationele en informationele privacy in relatie gebracht met het gebied dat betrekking heeft op het feit dat de communicatie tot stand is gebracht. Hieruit is gebleken dat deze privacy gebieden zeer nauw met elkaar zijn verbonden en dat het onderscheid tussen relationele en informationele privacy vervaagt, omdat de bedreigingen van beide vormen van privacy in elkaar overvloeien.

3. Diensten in een modern telecommunicatienet

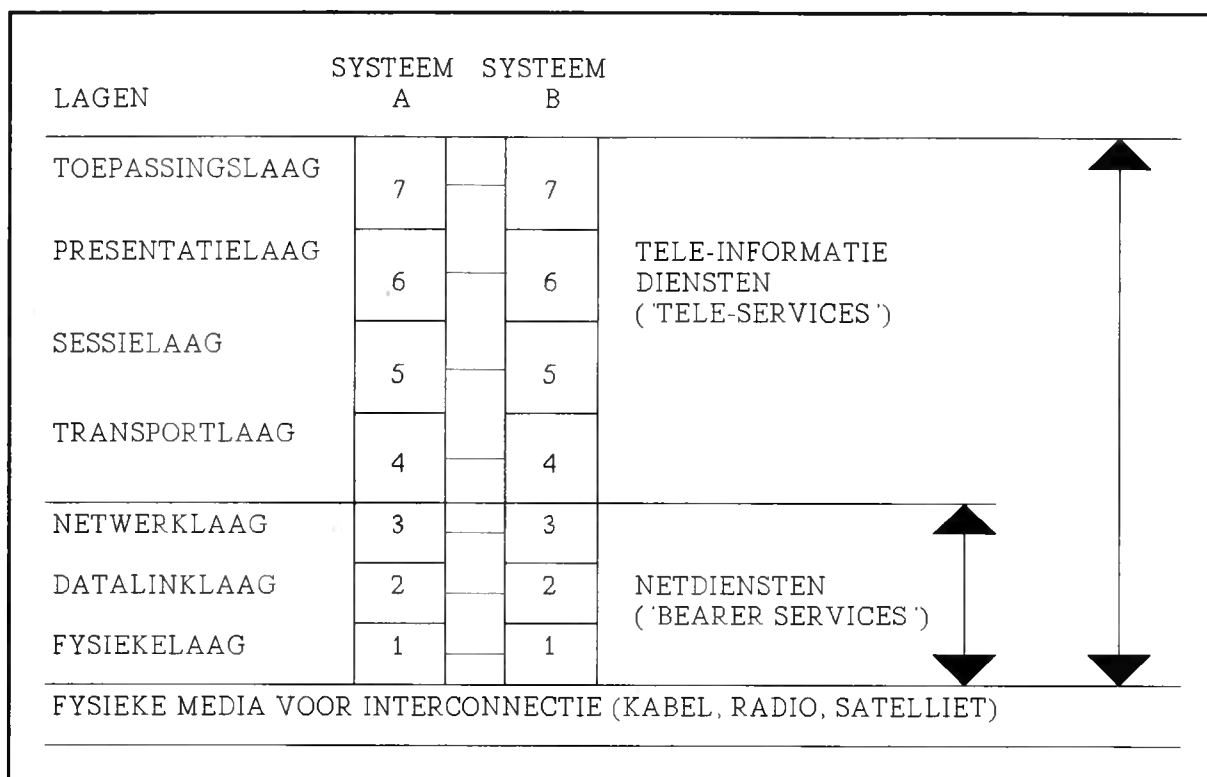
De huidige voortgang van de techniek zorgt ervoor dat het voor de gebruiker mogelijk wordt om toegang te krijgen tot een scala van telecommunicatiediensten. Naast telefonie komen voor een breed publiek tekstcommunicatie, elektronische berichtendiensten, maar ook diensten waarbij identificatie van de gebruiker vereist is, zoals Videl en de elektronische betaaldiensten (thuiswinkelen en thuisbankieren), beschikbaar. De diensten kunnen worden onderverdeeld in verschillende hoofdgroepen, namelijk net- en tele-informatiediensten met ieder basis- en supplementaire diensten [8]. Gezien de verscheidenheid van deze groepen en het feit dat privacyaspecten op verschillende dienstengroepen terug te voeren zijn is een nadere uitwerking hiervan op zijn plaats.

3.1. Netdiensten en tele-informatiediensten

Netdiensten ('bearer services') bieden de mogelijkheid om informatie uit te wisselen tussen twee aansluitingen van het telecommunicatienet. Ze worden bepaald door de neteigenschappen. Netdiensten gebruiken uitsluitend protocollen uit de onderste drie lagen van het OSI-model¹ (Open Systems Interconnection) voor gegevenstransport tussen de aansluitpunten (zie figuur 3-1). Een voorbeeld van een netdienst is het verzorgen van een 64 kbit/s circuitgeschakelde verbinding.

Naast deze netdiensten bestaan ook de tele-informatiediensten ('tele-services'). Deze diensten leveren de door de gebruiker gevraagde diensten en maken gebruik van een netdienst. Tele-informatie diensten gebruiken naast de protocollen uit de onderste drie lagen van het OSI-model ook protocollen uit de bovenste lagen (4 t/m 7, zie figuur 3-1). Voorbeelden van tele-informatiediensten zijn:

¹Open System Interconnection-model is een door de ISO (International Standards Organisation) ontworpen referentiemodel dat het elektronische informatie voorzieningsproces opdeelt in zeven lagen.



Figuur 3-1: Net- en tele-informatiediensten volgens het OSI-model

- telefonie: de mogelijkheid om door middel van het gesproken woord op afstand interactief te communiceren;
- teletex: de mogelijkheid om berichten uit te wisselen tussen geheugens van telexapparaten volgens gestandaardiseerde protocollen;
- videotex: de mogelijkheid voor de gebruiker om informatiebestanden te raadplegen;
- facsimile: de mogelijkheid documenten elektronisch over te brengen.

De informatie zelf behoort niet tot één van deze lagen, maar valt buiten het OSI-model [9][10]. De aanlevering van deze informatie is eigenlijk een derde dienst.

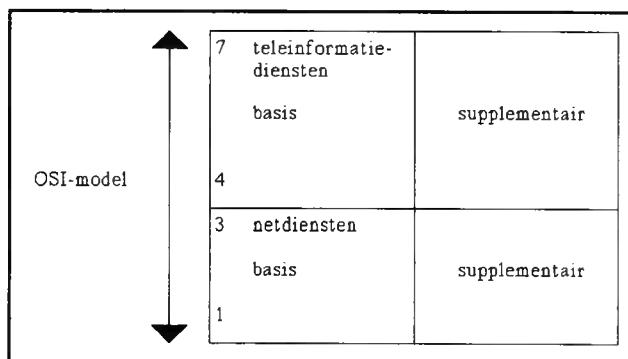
Buiten deze bestaande tele-informatiediensten zullen voor de gebruikers nieuwe diensten mogelijk zijn, zoals het simultaan communiceren door middel van spraak en beeld met één of meer andere gebruikers. Ook zal het mogelijk zijn om berichten in de vorm van spraak, tekst en beeld op te slaan en op een later tijdstip te versturen of op te vragen.

Tevens kan men vanaf een terminal produktgegevens opvragen, bestellingen en bankoverschrijvingen doen of teksten invoeren en bewerken.

3.2. Basisdiensten en supplementaire diensten

Naast het onderscheid tussen net- en tele-informatiediensten kan ook onderscheid worden gemaakt tussen basis- en supplementaire diensten ('supplementary services'). Supplementaire diensten zijn diensten die de basisdienst van een gevraagde net- of tele-informatiedienst op een specifiek punt wijzigen of aanvullen (zie figuur 3-2). Ze worden niet gescheiden aangeboden als zelfstandige diensten. Voor de gebruiker is het van belang dat de werking van deze

supplementaire diensten onafhankelijk is van de tele-informatiediensten; eenzelfde supplementaire dienst kan gebruikt worden bij verschillende diensten. Veelal verhogen supplementaire diensten het gebruikersgemak, zoals verkort kiezen of nummerherhaling. Ook kunnen deze diensten de bereikbaarheid van de



Figuur 3-2: Basis- en supplementaire diensten in het OSI-model

opgeroepene vergroten, zoals automatisch terugbellen bij het bezet zijn of niet-beantwoorden, het doorschakelen van een oproep of het geven van een oproepaankondiging. Daarnaast kunnen zij de kwaliteit van de dienstverlening verhogen, zoals oproeper-identificatie (caller ID) of identificatie van de opgeroepene, en de wijze van betalen vereenvoudigen. Naast genoemde voordelen zijn hier natuurlijk ook nadelen aan verbonden. Deze nadelen hebben veelal betrekking op de privacy.

3.3. Faciliteiten, functies en diensten

Faciliteiten kan men omschrijven als uitbreidingen op de basisdienst van een gevraagde net- of tele-informatiedienst. Door middel van verschillende functies wordt de daar uit voortkomende supplementaire dienst geleverd. Hierbij kan dezelfde functie worden gebruikt voor diverse basisdiensten opdat een zelfde soort supplementaire dienst kan worden geleverd. Zo kan bijvoorbeeld het functionele element 'transmissie van de abonnee-lijnidentificatie' voor verschillende basisdiensten worden gebruikt.

Vaak worden faciliteiten ook als supplementaire diensten aangeduid. Dit is echter niet juist. Anders gezegd, is:

- de faciliteit de extra mogelijkheid;
- de functie het hulpmiddel van de faciliteit om het doel te bereiken;
- en de dienst het beoogde doel.

Een voorbeeld ter illustratie: De faciliteit 'direct doorschakelen', wordt mogelijk gemaakt door verschillende functies met als doel dat abonnee B door A bij C kan worden gebeld. Stond in de vorige paragraaf vermeld dat de nadelen van supplementaire diensten veelal betrekking hebben op de privacy, in deze paragraaf wordt duidelijk waar deze privacy bedreigers hun oorzaak vinden, namelijk bij de functies die nodig zijn om de desbetreffende supplementaire dienst te leveren.

3.4. Samenvatting

Netdiensten bieden de mogelijkheid om informatie uit te wisselen tussen twee aansluitingen in het net. Naast de netdiensten onderscheidt men de tele-informatiediensten. Bij de tele-informatiediensten is het bijvoorbeeld mogelijk om gebruik te maken van de teletex- of videotexdienst. Ook kan men onderscheid maken tussen basis- en supplementaire diensten. De supplementaire diensten zijn diensten, die de

basisdienst van een gevraagde net- of tele-informatiediensten op een specifiek punt wijzigen of aanvullen. Afhankelijk van de geleverde (supplementaire) dienst kan een inbreuk op de privacy ontstaan.

Om duidelijk te maken waar de privacy bedreigers hun oorzaak vinden heeft een uiteenzetting van de termen faciliteiten, functies en diensten plaatsgevonden. Hieruit is gebleken dat het de functies zijn die er voor zorgen dat er privacy bedreigende situaties optreden. Een voorbeeld hiervan is het functionele element 'transmissie van de abonneelijnidentificatie' waardoor voor verschillende basisdiensten abonnee-identificatie kan plaatsvinden.

4. Ontwikkelingen in het telecommunicatienet

In dit hoofdstuk zal in grote lijnen de evolutie van de telecommunicatie behandeld worden. Deze evolutie gaat door. Verder wordt dan ook, in grote lijnen, beschreven wat wij van het toekomstige net mogen verwachten, met in het bijzonder de C7-signalering, het intelligente net en de mobiele communicatie. Ook het gebied van de datacommunicatie zal de nodige aandacht krijgen.

4.1. Een kort historisch overzicht

De schakelsystemen voor automatische telefonie hebben zich in een periode van meer dan 100 jaar ontwikkeld van (kleine) handcentrales tot de moderne geïntegreerde netwerksystemen zoals deze nu beschikbaar zijn.

De handbediende centrales welke omstreeks 1880 hun intrede deden, boden ondanks de technische eenvoud van hun uitvoering een aantal aantrekkelijke faciliteiten. Deze faciliteiten werden gekenmerkt door een grote aanpasbaarheid en variatie in de dienstverlening aan de abonnees, als gevolg van de menselijke intelligentie van de telefonistes. Genoemd kunnen worden: vocaal kiezen (er hoeft geen nummer gedraaid te worden), kiezen onder naam (het nummer hoeft niet bekend te zijn), betaling door opgeroepene, omleiden naar ander nummer bij het bezet zijn of geen respons krijgen etcetera. Bij het invoeren van automatisering gingen deze faciliteiten aanvankelijk volledig verloren om tijdens de technologische evolutie geleidelijk aan weer terug te komen, een proces dat tot op de dag van vandaag nog niet is voltooid. De handcentrale bestaat in concept uit een spreekwegennetwerk, en een centrale besturing in de persoon van de telefoniste. Aan deze handbediening kleefden echter ook bezwaren, welke tot automatisering aanleiding hebben gegeven. Door fysieke beperkingen, zoals armlengte, kon een telefoniste slechts een gering aantal abonnees rechtstreeks bedienen, terwijl de verwerkingscapaciteit beperkt was tot 30 à 40 gesprekken per uur [11]. Als gevolg hiervan ontstonden bij grote drukte lange wachttijden. De tussenkomst van telefonistes zorgde

ook nog voor een ander probleem, zij wisten immers wie met wie in gesprek was en wat er gezegd werd. Zij moesten continu luisteren en vragen of het gesprek geëindigd was om te weten te komen of de lijn vrijgegeven kon worden [12]. Het privacy probleem dateert dus al uit de begindagen van de telefonie.

In 1892 werd het eerste automatische systeem volgens Strowger ingevoerd, een zogenaamd direct systeem met kiesschijfbesturing. Dit systeem was een grote stap voorwaarts met echter een hele reeks beperkingen, welke men zich langzamerhand bewust werd. Zoals het ontbreken van geheugen wat tot een gebrek aan flexibiliteit bij de routing leidt; aangezien de kiezers rechtstreeks door de cijfers worden ingesteld is in het oorspronkelijke telefoonnet de te volgen route volledig en uitsluitend door het gekozen nummer bepaald. Door een groeiend inzicht in de mogelijkheden van de automatische schakelsystemen ontstonden steeds hogere organisatievormen waarbij de instelapparatuur van de doorschakelapparatuur gescheiden werd. Ook de routeringsmogelijkheden werden krachtiger en het principe van alternatieve routing maakte een economische opzet van netwerken mogelijk, waardoor netten met vele dwarsverbindingen ontstonden. Door centralisering van de besturingsfuncties kon ook de diversiteit in dienstverlening aan de abonnees geleidelijk worden teruggewonnen. Deze evolutie werd mogelijk gemaakt door, en ging samen met, de evolutie op het gebied van de technologie. Fundamenteel hierbij zijn het beschikbaar komen van steeds grotere geheugens tegen steeds lagere kosten en de grote vlucht die de micro-elektronica heeft genomen. Met de komst van de eerste digitaaldoorgeschakelde centrale in 1980 is de stap gezet naar een geheel digitale verbinding tussen aangeslotenen en dus de mogelijkheid geboden om dataverkeer via het telefoonnet af te wikkelen. [11]

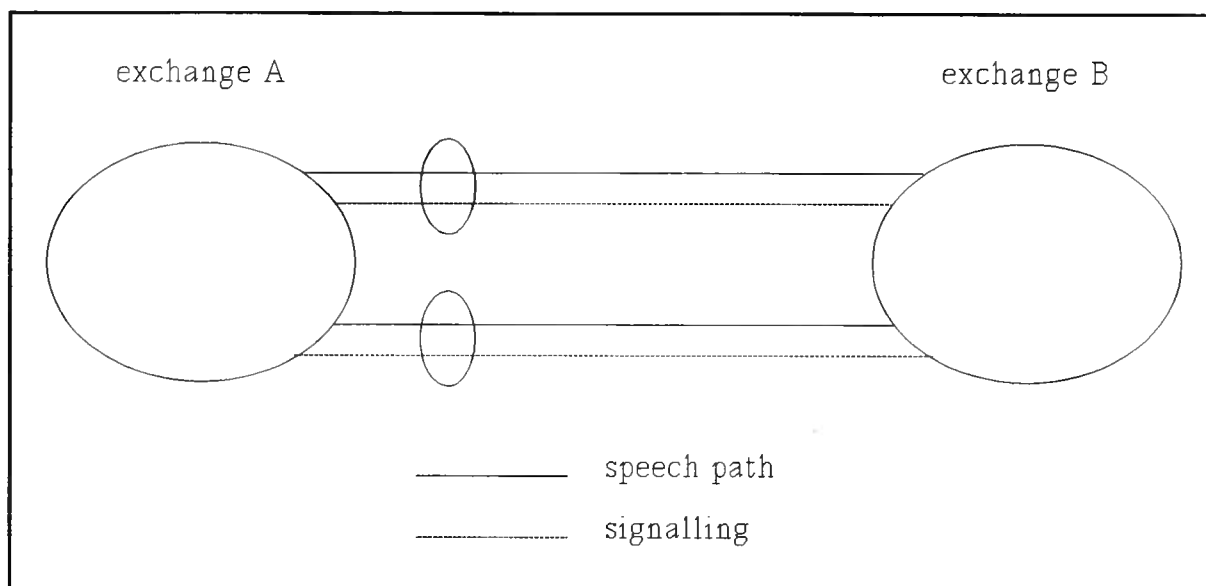
4.2. Signalering

Voor het opbouwen, instandhouden en het verbreken van een (telefoon)verbinding tussen twee abonnees is uitwisseling van gegevens nodig tussen de abonnee en de centrale en tussen de centrales onderling. Deze uitwisseling van gegevens noemt men

signaleren. In de begindagen van de telefonie geschiedde het signaleren zeer simpel. Het merendeel van de signaleringsinformatie werd verbaal uitgewisseld tussen abonnee en telefonistes en tussen de telefonistes onderling. De komst van de semi-automatische en vol-automatische schakelsystemen, gebaseerd op elektromechanische schakelsystemen, heeft geleid tot de ontwikkeling van een aantal signaleringssystemen, geoptimaliseerd naar de eisen van deze systemen. Door het toepassen van computertechnieken voor de besturing van schakelnetwerken enerzijds en het toepassen van digitale transmissiemiddelen anderzijds, ontstaat een digitaal telecommunicatienet waarover een groot aantal diensten geboden kan worden. Deze nieuwe diensten hebben een grotere signaleringsbehoefte tussen centrales tot gevolg. Om aan deze behoefte te voldoen is een geavanceerd signaleringssysteem noodzakelijk.

4.2.1. Gemeneweg signalering

De conventionele manier van signaleren houdt in dat de signaleringsinformatie over

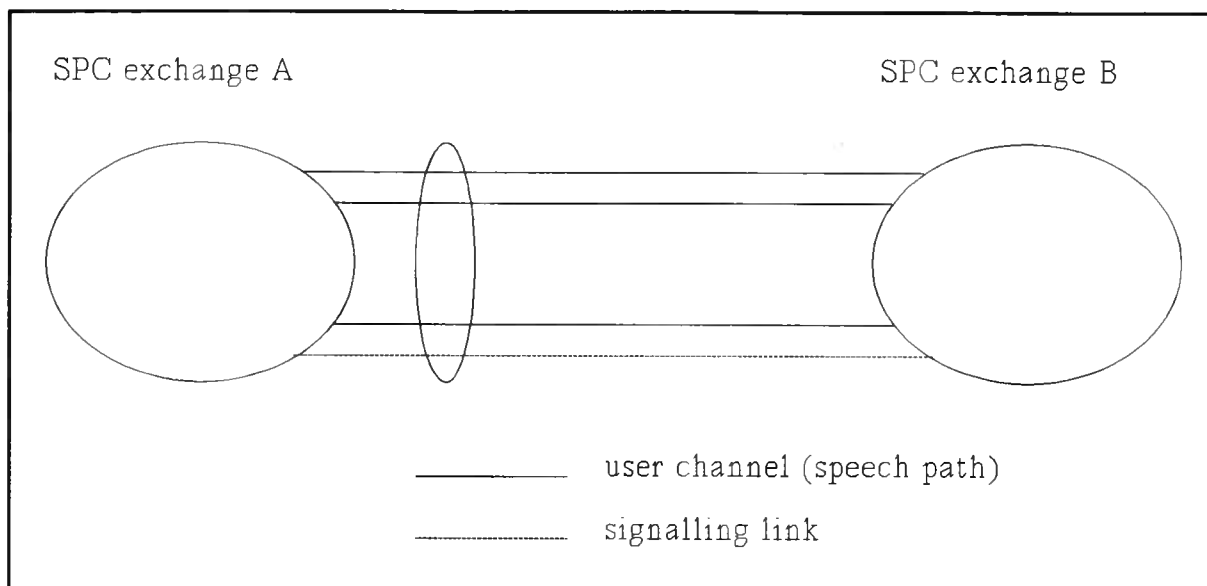


Figuur 4-1: Kanaalgebonden signalering

hetzelfde pad wordt overgebracht als de spraak: kanaalgebonden signalering (zie figuur 4-1).

Een vernieuwende stap is gezet met de ontwikkeling van een signaleringssysteem waarbij spreekweg en signaleringspad tussen centrales gescheiden zijn: common channel signalling (gemeneweg signalering) (zie figuur 4-2).

De kern bestaat uit een directe koppeling van de besturingscomputers van SPC (stored program control) centrales over een apart net. Er ontwikkelt zich een parallelnet aan het telefoonnet. Dit parallelnet is uitgerust met eigen schakelcentrales, ook wel Signal Transfer Points (STP) genoemd, waarover boodschappen verzonden worden die bijvoorbeeld ten doel hebben een vrije weg tussen de centrale van de oproeper en die van de op te roepene te vinden.



Figuur 4-2: Gemeeneweg signalering

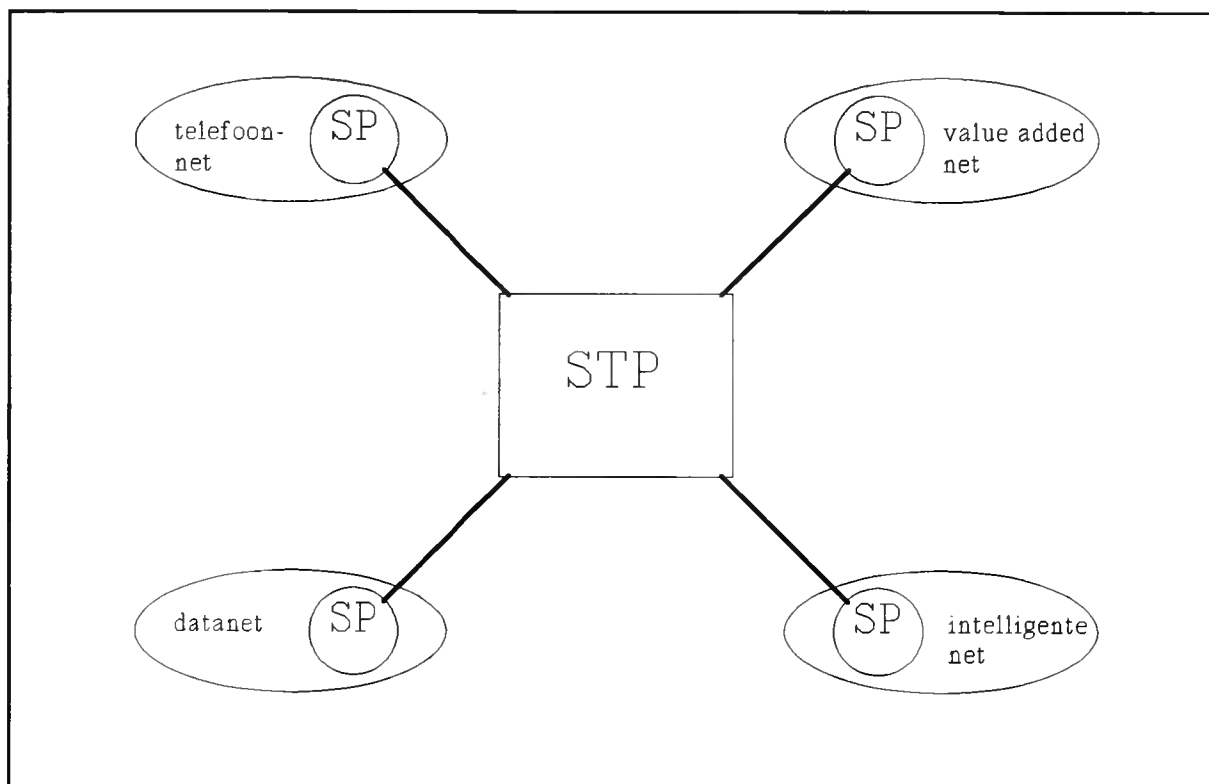
Met dit Common Channel Signalling System No. 7 (CCSS 7, het 7e systeem dat door CCITT is vastgelegd, en in de vaktaal vaak aangeduid als C7) kan ook tijdens de verbinding informatie worden uitgewisseld tussen plaatsen in het net waar diensten gegenereerd kunnen worden, zodat een abonnee bijvoorbeeld additionele steun kan invoeren. De netexploitant kan, ten behoeve van de eigen bedrijfsvoering, die informatie overbrengen en verzamelen die betrekking heeft op de verkeersintensiteit en -omvang, storingen, de mate van bereikbaarheid van abonneediensten etc. De diensten die op deze wijze aan de abonnee kunnen worden geleverd zijn:

- identificatie van de oproeper (A-abonnee)
- identificatie van de opgeroepene (B-abonnee)
- besloten gebruikersgroep
- omleiding van een oproep naar een ander aansluitpunt
- oproep in de wachtstand bij bezet zijn van opgeroepene
- oproepherhaling na vrijkomen van bezette opgeroepene
- signalering tussen abonnees

Voor de laatste mogelijkheid is het nodig dat een aangepast signaleringsstelsel tussen abonnees en centrales tot stand komt. Hier kan ISDN een grote rol spelen. [9][13]

4.2.2. C7-signalering als basis voor geavanceerde netdiensten

De toepassing van C7-signalering gaat verder dan alleen die in het telefoonnet. In figuur 4-3 is te zien hoe een STP de overgangsfunctie tussen de Signalling Points (SP) van



Figuur 4-3: C7 en verschillende telecommunicatienetten

verschillende netten vervuld. [14]

Het C7-signaleringssysteem is modulair van opzet en maakt onderscheid in een 'Message Transfer Part' (MTP) en diverse 'User Parts' (UP). Het MTP zorgt voor een betrouwbaar transportsysteem ten behoeve van de uitwisseling van signaleringsberichten tussen de UP's. In de UP's zijn de functies en procedures gedefinieerd behorend bij een specifieke toepassing. Zo zijn in het 'Telephone User Part' (TUP) de signaleringsfuncties en -procedures gedefinieerd voor de telefonietoepassing. Eveneens zijn te onderscheiden een 'Data User Part' (DUP), en een 'ISDN User Part' (ISDN-UP). Deze UP's kunnen worden getypeerd als signaleringsgebruikers.

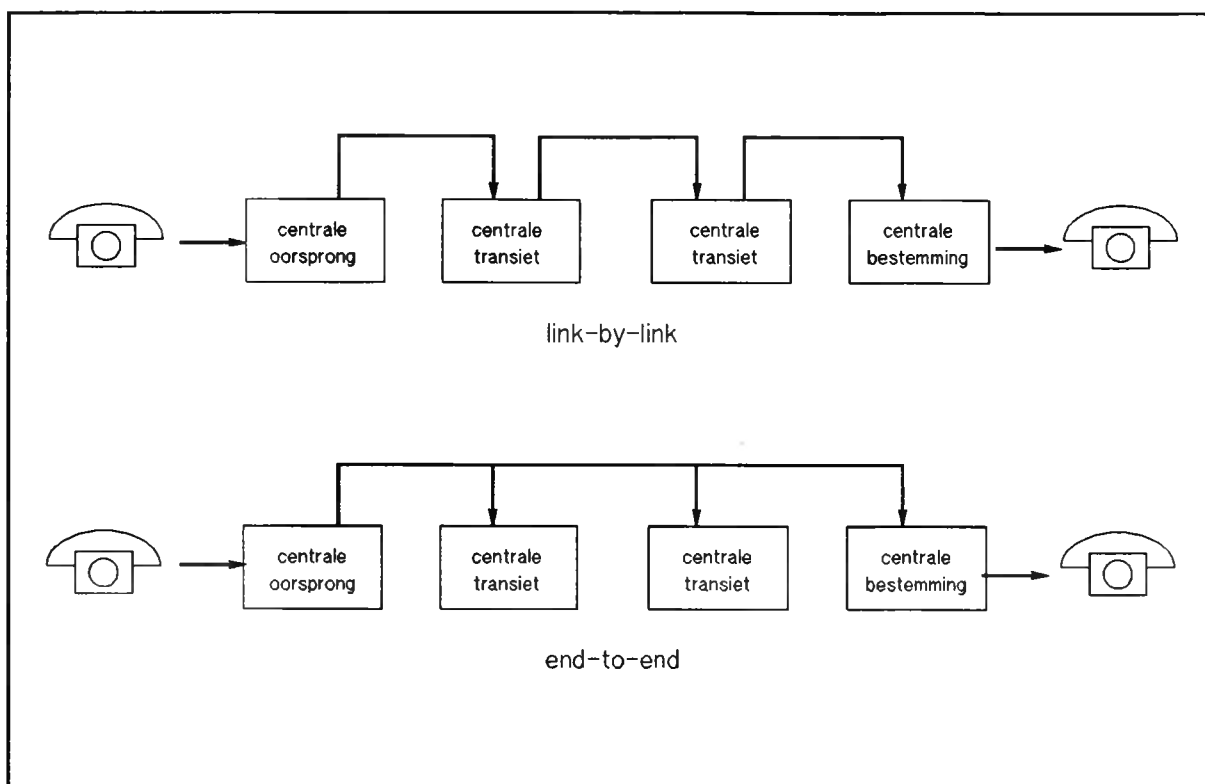
Daarnaast biedt het transportsysteem de mogelijkheid om niet-signalerings specifieke informatie tussen de gebruikers over te brengen. Als voorbeelden van deze als exploitatieve gebruikers te typeren UP's kunnen beheer, onderhoud en tarifieringstoepassingen worden genoemd, het 'Operations, Maintenance and Administration Part' (OMAP). De interface tussen een SSP (Service Switching Point) en een SCP (Service Control Point) in een intelligent net is gebaseerd op het C7-signaleringsstelsel. Hiervoor is het 'Transaction Capabilities Application Part' (TCAP) beschikbaar (zie paragraaf 4.3.2).

4.2.3. Signaleringsboodschappen

Het opbouwen en verbreken van de circuitgeschakelde verbinding vindt plaats door link-by-link berichten. Deze berichten worden door elke centrale in de weg van de netverbinding ontvangen. De ontvangende centrale gebruikt een deel van de informatie voor het routeren en zendt de informatie weer in zijn geheel naar de volgende centrale. De categorie van link-by-link signaleringsboodschappen omvat:

- Boodschappen voor het tot stand brengen van een oproep
- Vrijgaveboodschappen

Voor de introductie van het ISDN zal de circuit-gerelateerde link-by-link signalering niet langer voldoende zijn. Daarom dient de link-by-link signalering te worden aangevuld met een end-to-end signalering tussen de bron- en bestemmingscentrales. Alhoewel end-to-end signalering betrekking kan hebben op een oproep is deze niet rechtstreeks gerelateerd aan de besturing van de circuitgeschakelde verbinding. Bij end-to-end signalering is de zendende centrale namelijk gedurende de gehele signaleringsprocedure de centrale van oorsprong. Steeds wordt zoveel informatie opgevraagd en verzonden als voor het instellen van de weg naar de volgende centrale nodig is. Zodra deze weg is ingesteld wordt de signaleringsontvanger in de inkomende centrale afgeschakeld (zie figuur 4-4). De functies voor end-to-end signalering bevatten berichten voor:



Figuur 4-4: Link-by-link en end-to-end signalering

- Verzoeken om een aanvullende service
- Verzending van informatie die betrekking heeft op een aanvullende service
- Deactiveren van aanvullende services
- Informatie van de opgeroepen gebruiker wanneer de oproepende gebruiker de oproep opschort (zonder verbreken) en deze daarna hervat (bijvoorbeeld voor het verplaatsen van een terminal van de ene contactdoos naar een andere)
- Informatieverzoek van een gekoppelde centrale of een gateway-centrale
- Overdracht van gebruiker naar gebruiker informatie

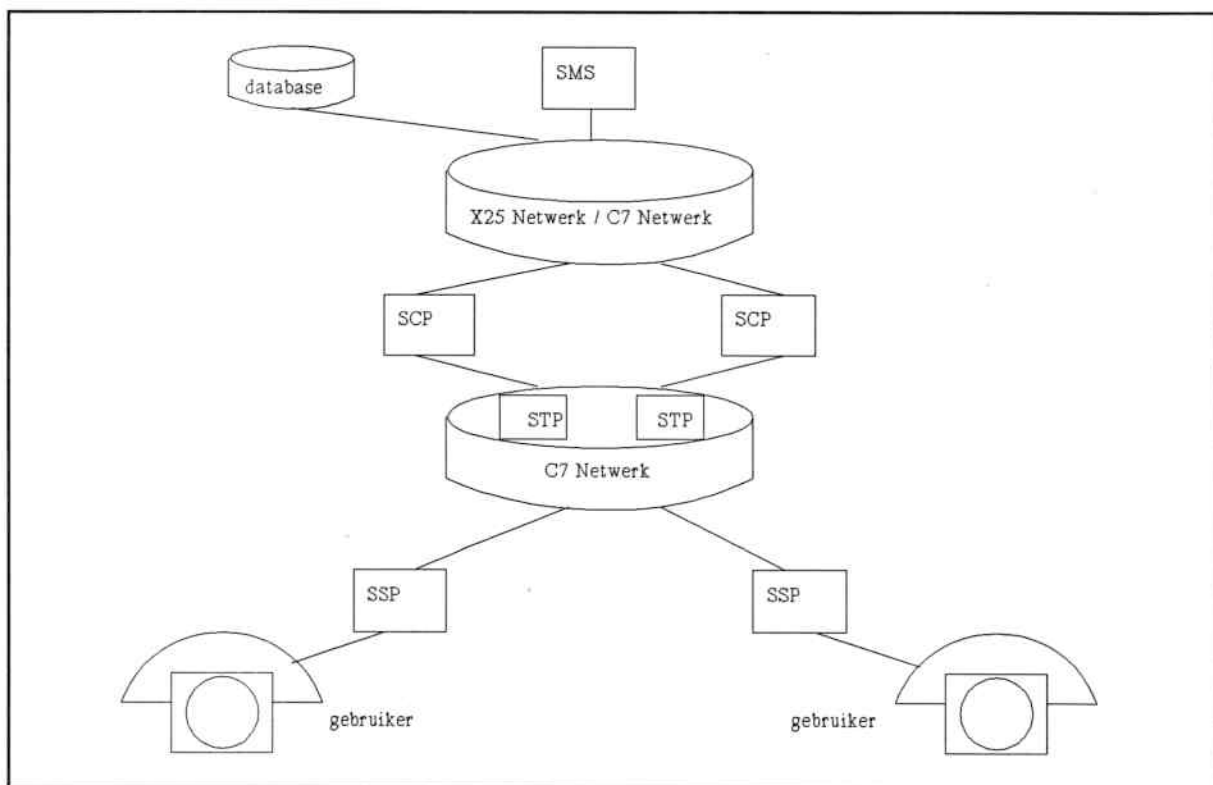
4.3. Het intelligente net

4.3.1. Het concept

Bijzondere faciliteiten in verbindingsopbouw, routing en tarifiering worden volgens het concept van het intelligente net niet in de programmatuur van de SPC-centrales

vastgelegd maar in één of meer aparte computersystemen die met de centrales via het signaleringsnet (C7) communiceren. Op deze manier ontstaat een ontkoppeling tussen de primaire schakelfuncties van de centrales en de extra faciliteiten. Wil men nu een dienst introduceren of wijzigen dan hoeft men niet in het net in te grijpen, maar kan men volstaan met de veranderingen daar uit te voeren waar de centraal opgeslagen software is geïnstalleerd. Zo wordt de exploitatie van het zuivere verbidingsnet gescheiden van de exploitatie van de overige door het net verleende diensten.

4.3.2. Architectuur

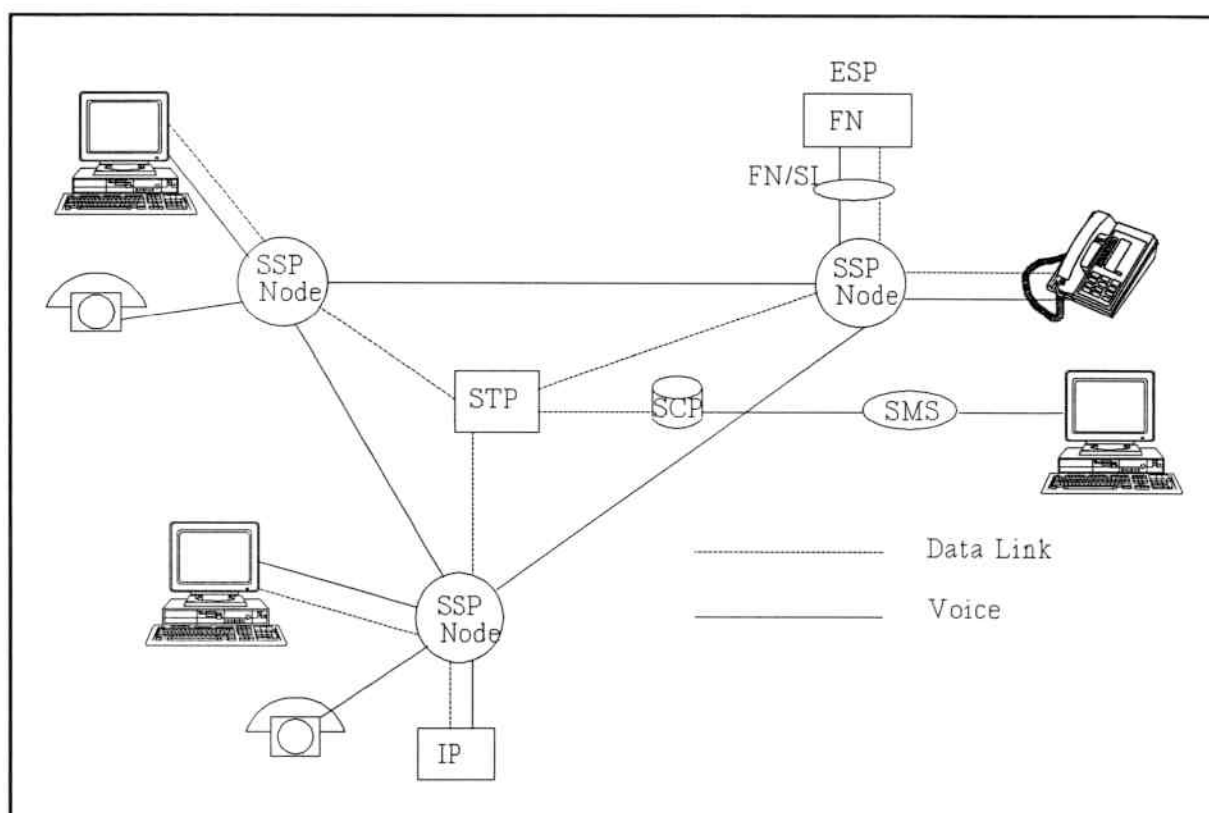


Figuur 4-5: Architectuur van het intelligente net

Een intelligent net is in feite geen net maar een architectuur (zie figuur 4-5). In deze architectuur is het mogelijk om als dienstenleverancier op een eenvoudige manier de dienst te introduceren of te veranderen. Dit is mogelijk doordat er voor elke dienstenleverancier eenzelfde toegang tot het telefoonnet is. Voor de netexploitant is het op een eenvoudige manier mogelijk het schakelnet te exploiteren. Voor de

dienstenafnemer is deze architectuur ook van belang, doordat het nu heel eenvoudig mogelijk is om gebruik te maken van een dienst.

De grote lijnen van dit principe staan in figuur 4-6. In deze figuur is een apart verkeersnet aanwezig waarin de verbindingen worden gerealiseerd. De dienstenleveranciers hebben via een aparte aansluiting toegang tot dit net om hun dienstenpakket te introduceren of aan te passen. Dit introduceren of aanpassen van de diensten is mogelijk vanaf eigen lokatie (Extern Service Point (ESP) geheten). Er zijn evenveel ESP's als er dienstenleveranciers zijn. Vanaf deze lokatie hebben de dienstenleveranciers beschikking over een Feature Node (FN) waarin al hun middelen en gegevens voor de exploitatie van hun dienst staat vermeld.

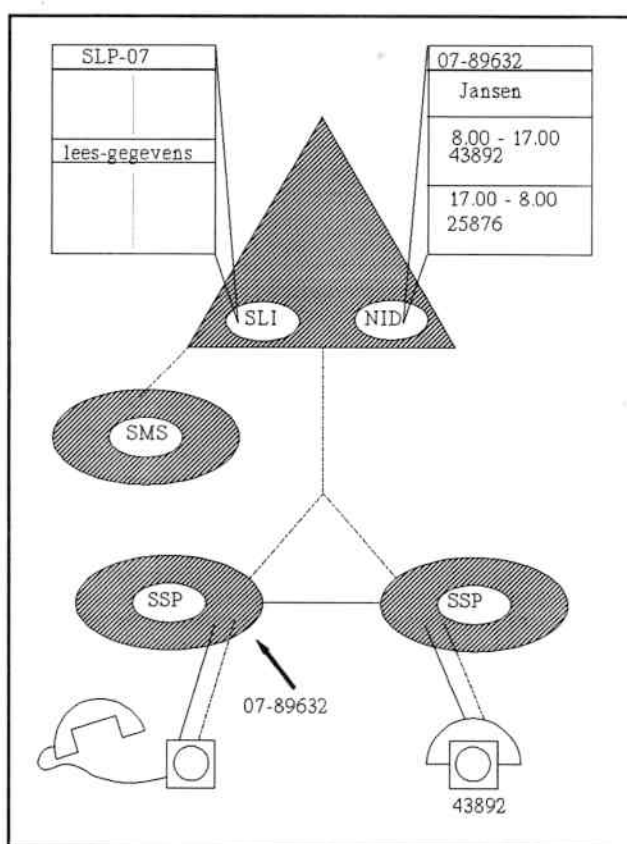


Figuur 4-6: Componenten in het intelligente net

De nettoegang is het scheidingsvlak tussen de apparatuur van de dienstenleveranciers en het net. Er is ook nog een speciale interface, de Service Interface (SI), die er voor zorgt dat niet iedereen via de nettoegang de mogelijkheid heeft om als dienstleverancier te opereren. Alle verwerkte informatie van de dienstenleverancier wordt via het

signaleringsnet en het Signal Transfer Point (STP) ontvangen door het Service Control Point (SCP). Hier wordt alle informatie opgeslagen in een database. Het Service Maintenance System (SMS) houdt de activiteiten van de dienstenleverancier in de gaten, en treedt indien nodig ordenend op. Als een dienst wordt aangevraagd door een abonnee wordt de informatie opgevraagd in de SCP. De informatie wordt eerst via de STP en het signaleringsnet naar de betreffende Service Switching Points (SSP) getransporteerd alvorens deze gebruikt kan worden. Mocht het nodig zijn om de afnemer van de diensten toe te spreken, dan komen deze uit de daartoe geactiveerde Intelligent Peripheral (IP). [9][15]

Een voorbeeld van informatie over een dienst is gegeven in figuur 4-7. De heer Jansen is overdag op kantoor en 's avonds thuis. Hij wil gebeld worden waar hij zich op dat moment bevindt. Daartoe neemt hij een abonnement op de adresseringsdienst. De heer Jansen maakt zijn wensen kenbaar via het nummer 07-89632. Daar wordt gezorgd dat hij als abonnee op de dienst wordt ingeschreven. Concrete data met betrekking tot zijn wensen worden door de heer Jansen toegevoegd en in het ESP wordt ervoor gezorgd dat deze in de Network Information Database worden opgeslagen. Zijn wensen worden in een Service Logic Program (SLP) vastgelegd en actief gemaakt in een



Figuur 4-7: Voorbeeld werking intelligent netwerk

Service Logic Interpreter (SLI). Vervolgens verzorgt het programma geheel de routing van voor Jansen bestemde telefoongesprekken, die overdag op 43892 en 's avonds op 25876 aankomen. De dienst is bereikbaar onder een speciaal nummer. De abonnee kan

de gegevens van de dienstverlening, zoals tijdstip, zelf aanpassen. Hierbij zijn de verbindingfunctie en de dienstenfunctie van elkaar ontkoppeld.

4.4. ISDN

Het ISDN is door het CCITT (Comité Consultatif International de Télégraphie et Téléphonie) als volgt gedefinieerd:

'An ISDN is a network, in general evolving from a telephony IDN¹, that provides end-to-end digital connectivity to support a wide range of services, to which users have access by a limited set of standard multipurpose user-network interfaces.'

Volgens dit concept zullen, gebaseerd op een volledig digitaal en van gemeneweg signalering voorziene telecommunicatienet, ook de abonneelijnen digitaal zijn en toegang geven tot zowel circuit- als pakketgeschakelde diensten en netten. Voor de toegang tot het ISDN zijn twee structuren voor het gebruikerskoppelvlak vastgelegd. De basistoegang biedt twee onafhankelijke 64 kbit/s B-kanalen voor de gebruikersinformatie en een D-kanaal van 16 kbit/s voor signalering ten behoeve van de beide B-kanalen (basistoegang 2B+D, 144 kbit/s). Dit signaleringskanaal D kan gezien worden als de lokale tegenhanger van het verkeerssignaleringsnet C7 [9]. Tevens is er een primaire toegang die 30 onafhankelijke 64 kbit/s B-kanalen biedt voor gebruikersinformatie en een D-kanaal van 64 kbit/s voor de signalering van de 30 B-kanalen (primaire toegang 30B+D, 2 Mbit/s).

Het grote voordeel voor de gebruiker van het ISDN is, dat er geen sprake meer zal zijn van verschillende soorten adressen, adresseermethoden en faciliteiten voor de verschillende diensten. Dit betekent dat de wijze van verbindingsofbouw voor data-, spraak-, tekst- en beeldverkeer hetzelfde is. [11]

¹IDN: *Integrated Digital Network*

4.5. Mobiele communicatie

In vergelijking met de ontwikkelingen in de vaste netstructuren, is er in de mobiele sector sprake van een turbulente toestand. Hierin zou wel eens de grootste verschuiving van de telecommunicatie kunnen plaats vinden.

Kern van het gebeuren is dat met de moderne micro-elektronica handzame apparaten kunnen worden gemaakt die op zak gedragen worden. Deze handzaamheid werkt de ontwikkeling van 'persoonsgebonden communicatie' in de hand. Deze vorm van communicatie staat tegenover het begrip 'adresgebonden communicatie'.

In beginsel geeft iedere aansluiting op een net dat met kabel is uitgevoerd toegang tot een bepaalde plaats; het adres. Eenmaal met het adres verbonden, moet men soms verder vragen om een persoon aan de lijn te krijgen. Voor persoonlijke communicatie is het adres momenteel nog steeds een onmisbare tussenstap. Wanneer (zak)apparatuur beschikbaar is die als 'adres' een persoonskenmerk heeft, roept men geen adres, maar een persoon op. Alle middelen die hier onder vallen vat men samen onder het begrip 'Personal Communications Network' (PCN). Een representatief voorbeeld van persoonsgebonden communicatie is het toekomstige pan-Europese digitale autotelefoonnet. Dit zogenoemde GSM-netwerksysteem wordt in de volgende paragraaf besproken.

4.5.1. Het GSM-netwerksysteem

In een openbaar landnetwerk als het telefoonnet (of het ISDN) zijn alle abonnees eenduidig gekoppeld aan een vast punt van het netwerk. Hierdoor kan het routeren naar de abonnee geschieden op basis van eenmalig te implementeren routeerstructuren.

Waarborging van de echtheid van een mobiele abonnee kan niet op basis van de eenduidigheid van de aansluiting plaatsvinden; de abonnee kan op een willekeurig punt

in het cellulaire netwerk aankoppelen en een oproep genereren. Ook het routeren van een oproep naar een abonnee kan niet op een éénmalig te implementeren routeertabel gebaseerd worden. Het kan zelfs zo zijn dat de verbinding in het net tijdens een gesprek veranderd moet worden als gevolg van het overschrijden van een celgrens door de abonnee (handover, zie hierna).

Hierom zijn ten opzichte van het ISDN aan het GSM-PLMN (Public Land Mobile Network) de volgende functies toegevoegd:

-Authenticatie

Voordat een abonnee toegestaan wordt een oproep uit te plaatsen, vindt een procedure plaats waarmee de authenticiteit van de abonnee aangetoond wordt.

-Paging

Op inkomende oproepen wordt in een cel omgeroepen dat de opgeroepen abonnee moet reageren. Na reactie ontstaat een eenduidige relatie tussen abonnee en netwerk waarin het mogelijk is een verbinding op te bouwen.

-Locatieregistratie

Een abonnee kan overal in Europa zwerven (roaming). Europa is daarom opgedeeld in een groot aantal 'location areas'. Het netwerk houdt bij in welk location area de abonnee zich bevindt. De abonnee is er daarbij zelf verantwoordelijk voor dat het netwerk weet in welk location area hij zich bevindt. Zijn 'mobiel station' (MS) kan daartoe verandering van location area detecteren. Na detectie van verandering van het location area zal het MS een location updating procedure starten.

-Handover

Indien een MS communiceert met het netwerk, kan het voorkomen dat de verbindingskwaliteit zover afneemt dat het noodzakelijk wordt over te schakelen naar een ander basisstation. Deze procedure wordt handover genoemd.

-Identificatie

In het GSM-PLMN is het wenselijk de door geheel Europa zwervende abonnees met universele nummers aan te kunnen geven. Met name voor procedures binnen het netwerk is een dergelijk nummer bijzonder prettig. Dit nummer wordt het IMSI, International Mobile Subscriber Identity, genoemd. Het IMSI is geen deel van het ISDN of telefoonnet nummerplan. Het IMSI bestaat uit de volgende delen:

MCC - Mobile Country Code

MNC - Mobile Network Code

MSIN - Mobile Subscriber Identity Number

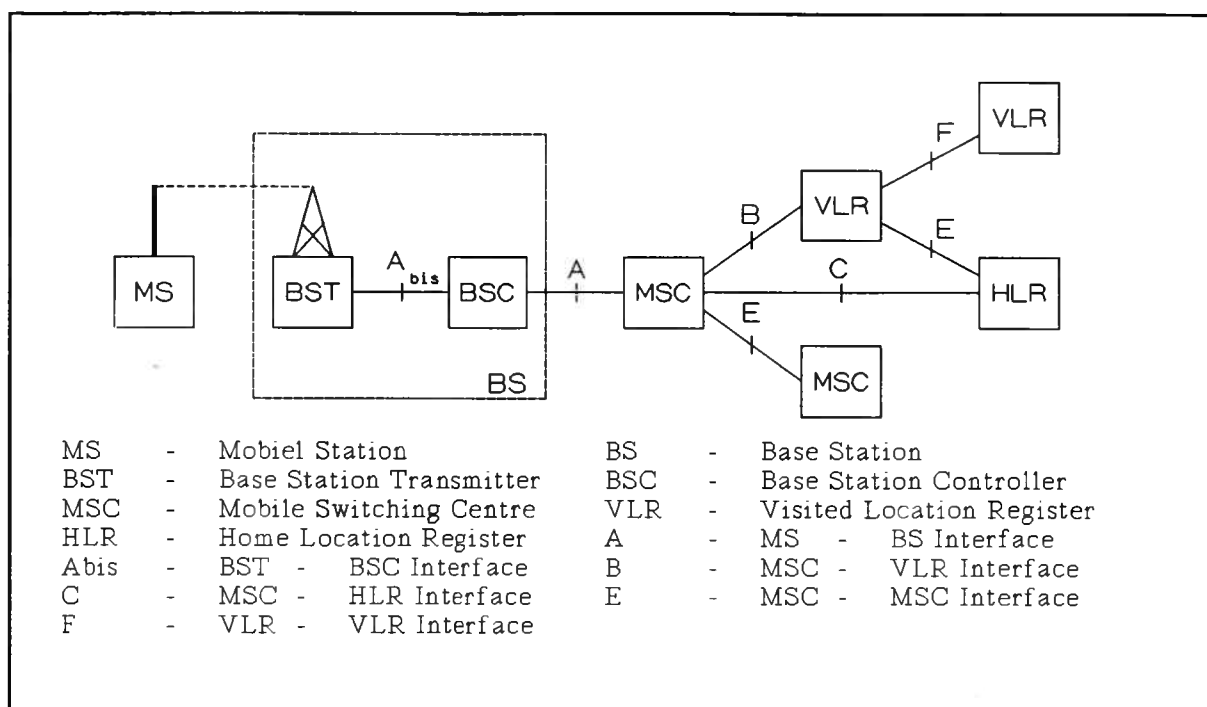
De GSM-abonnee is echter bereikbaar onder een gewoon, per land individueel vast te stellen, ISDN-nummer, vergelijkbaar met een telefoonnummer. Het PLMN zorgt voor conversie van dit nummer naar het IMSI, een nummer waar de abonnee geen weet van heeft.

-Versleuteling

Bij digitale transmissie is het mogelijk een zeer waterdichte versleuteling van de op de radioweg overgezonden gebruikersdata (spraak) toe te passen. Procedures voor sleuteltoewijzing zijn gedefinieerd, gebruik makend van de procedures voor authenticatie.

Om de koppeling van netwerken binnen Europa (met per land verschillende centrale leveranciers) mogelijk te maken is voor het GSM-PLMN een netwerk architectuur vastgesteld (zie figuur 4-8).

In de netwerkarchitectuur zijn functieblokken (MS-HLR) en koppelvlakken of interfaces (A-F) gedefinieerd. Elk koppelvlak is vervolgens ingevuld met besturingsprotocollen.



Figuur 4-8: *Netwerkarchitectuur van het GSM-PLMN*

Het MS is met de abonnee verbonden op de gebruikersinterface. Deel van deze interface is een smartcardkoppeling. Omdat de identiteit van de abonnee/MS voor het netwerk bepaald wordt door deze smartcard, is het in principe mogelijk de abonnee op een willekeurig MS te laten bellen/oproepen. Deze smartcard bevat onder andere gegevens voor het authenticatieprotocol.

Het basisstation is in twee delen opgesplitst; één deel dat de werkelijke transmissiefuncties uitvoert, het BST, en een deel dat één of meer BST's aanstuurt, het BSC. Het BSC neemt alle functies voor het besturen van het kanaalgebruik voor z'n rekening. Schakelfuncties worden vervuld door het MSC, evenals een groot aantal procedures voor het besturen van het systeem (handover, locatieregistratie). In het netwerk zijn twee soorten lokatie registers. In het HLR is permanent opgeslagen waar de abonnee zich bevindt. Dit geschiedt in de vorm van het MSRN (Mobile Subscribe Roaming Number), een nummer dat volgens ISDN-nummerplan conventies is samengesteld en daardoor tevens voor een gemakkelijke routing, volgens bestaande protocollen, naar de abonnee gebruikt kan worden.

Ook andere aansluitgegevens (rekening, dienst abonnementen) staan in het HLR opgeslagen. Het HLR is daarmee een database die voor elke oproep naar een GSM-abonnee geraadpleegd wordt. Het VLR bevat een deel van de gegevens uit de HLR's van de abonnees, die zich in de location area(s) van dat VLR bevinden. Het VLR vervult ook functies in eventuele procedures, waarmee de geheimhouding van de abonnee op de radio-weg gewaarborgd wordt. Hierbij wordt het TMSI (Temporary Mobile Subscriber Identity) in plaats van het IMSI op de radio interface gebruikt. TMSI toewijzing vindt plaats in combinatie met sleuteltoewijzingsprocedures en authenticatieprocedures. [16]

4.6. Het datanet

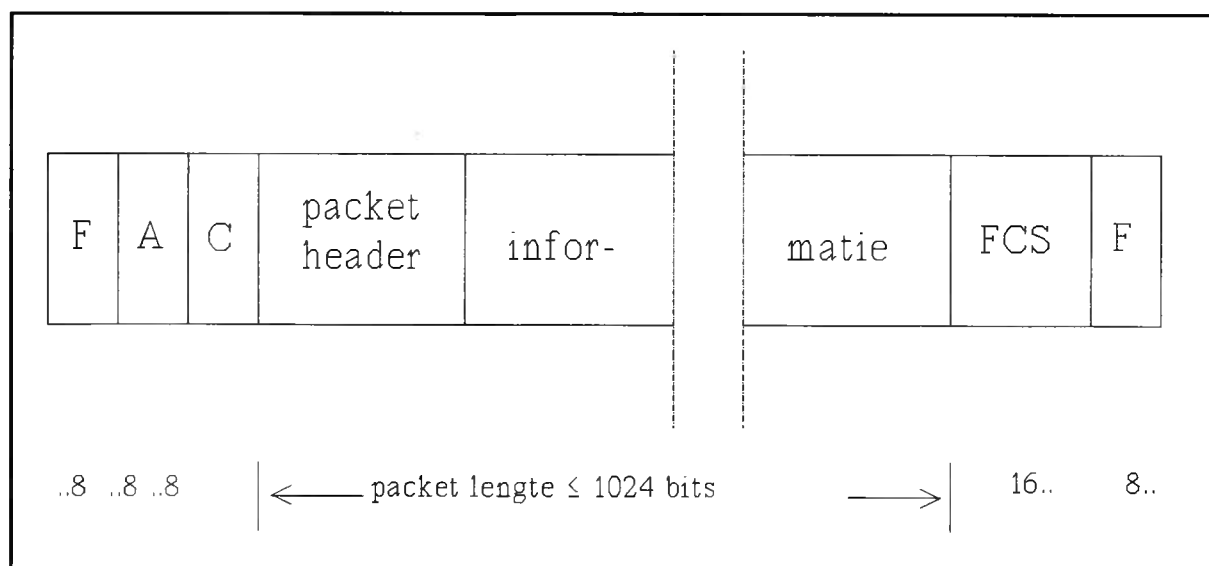
4.6.1. Schakelprincipes

De eigensoortige ontwikkeling in de computersector heeft de aandacht gevestigd op netarchitecturen die ingrijpend verschillen van de conventionele telefoonnetten. In een telefoonnet wordt voor de duur van het gesprek een verbinding aan de abonnees ter beschikking gesteld. Dit draagt de naam circuit switching (circuit schakelen). Voor het verzenden van een bericht hoeft dit echter niet: het is mogelijk een bericht aan het net af te geven met het verzoek dit af te leveren aan het bijgevoegde adres. Dergelijke systemen zijn gebouwd en dragen de naam 'message switching' (MS). Het principe van MS berust op het van knooppunt naar knooppunt doorzenden van het bericht, bij ieder knooppunt weer een nieuwe richting zoekend en controlerend of het bericht foutloos is overgekomen.

Om de lange transporttijden bij MS te beperken is men ertoe overgegaan het bericht in stukken van gelijke grootte op te delen en de stukken volgens het MS principe te verzenden. Deze wijze van overdragen heeft de naam 'packet switching' (pakket schakelen) gekregen. Daarnaast bestaat de mogelijkheid dat de gebruiker over een circuitgeschakeld net beschikt.

4.6.2. Pakketvorm en overdracht

In figuur 4-9 is de structuur van een pakket aangegeven. De feitelijk over te brengen informatie heeft een ruimte van 1024 bit. Samen met de begeleidende informatie voor het verzenden is het pakket ingeklemd tussen twee vlaggen (F) om begin en einde van het pakket aan te geven. De begeleidende informatie is gestructureerd volgens het OSI-model. De foutencontrole (FCS) vindt per overdracht tussen twee gekoppelde



Figuur 4-9: Pakketstructuur

knooppunten plaats (laag 2). Adres en netfaciliteiten zijn in A en C opgenomen. Hier bevinden we ons op laag 3 van het OSI-model. [17]

4.6.3. Netdiensten in een datanet

Een datanet is zoals al in paragraaf 4.6.1. te lezen viel, een pakketgeschakeld net. Ieder pakket bevat een adres en begeleidende informatie over verdere bestemming ten huize van de ontvanger. Door de begeleidende informatie van het informatiepakket zijn de volgende diensten mogelijk:

- besloten gebruikersgroep, al of niet met de mogelijkheid van verkeer naar leden buiten de groep
- identificatie van oproeper en opgeroepene
- keuze van de snelheid
- éénrichtingskanalen
- ingaaand of uitgaand verkeer uitsluiten
- opgeroepene laten betalen, al of niet na toestemming

Deze netdiensten lijken veel op de diensten die door de C7-signalering aan de abonnee geleverd kunnen worden. Dit is niet verwonderlijk want wat de header voor het pakketschakelen is, is het aparte signaleringskanaal voor het circuitschakelen. [9]

4.7. Componenten in een modern telecommunicatienet

Achtereenvolgens zijn in dit hoofdstuk besproken:

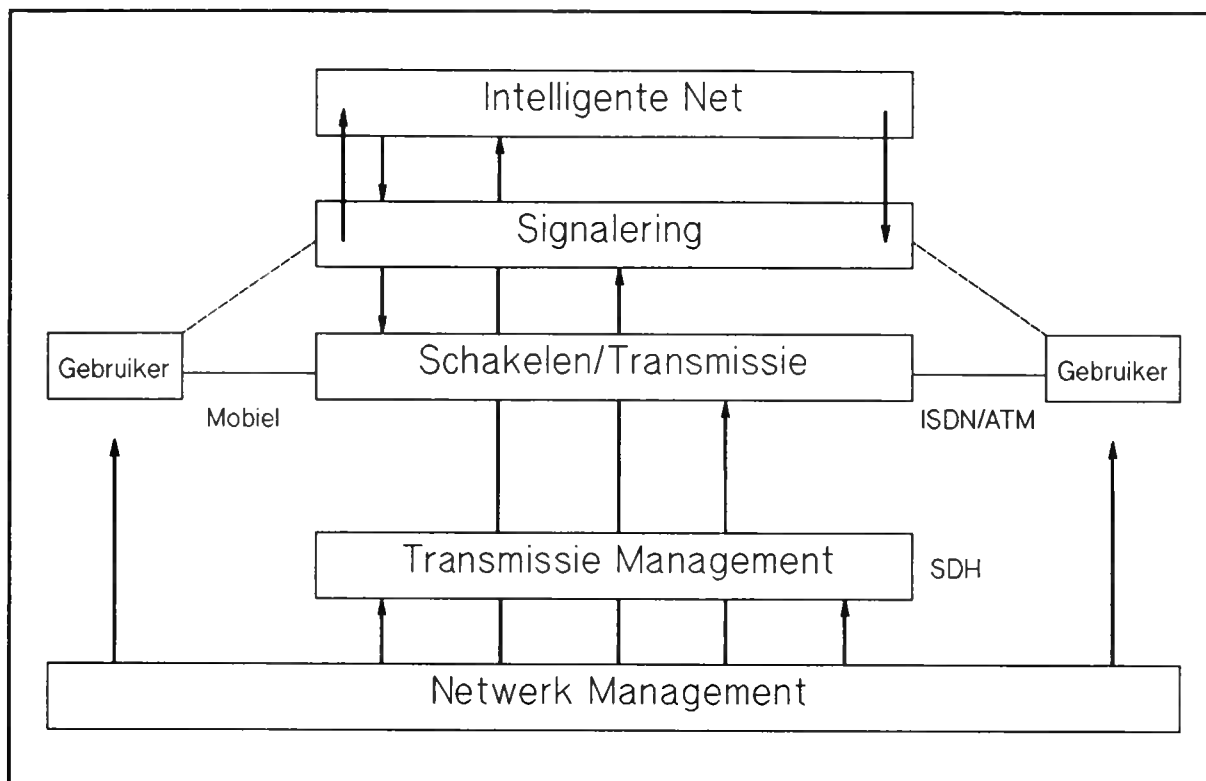
- de C7-signalering
- het intelligente net
- het ISDN
- de mobiele communicatie
- het datanet

Tezamen vormen deze componenten de basis voor de diensten die aan de gebruiker geleverd kunnen worden. In deze paragraaf zal, tot slot van dit hoofdstuk, de samenhang tussen deze componenten verduidelijkt worden (zie figuur 4-10). Het ISDN en de mobiele communicatie vormen de toegang voor de gebruiker tot een scala van diensten. Dit vindt plaats door middel van eindapparatuur bij de gebruiker, bijvoorbeeld een mobiele telefoon of een ISDN-terminal. Het belangrijkste verschil tussen deze twee vindt zijn oorsprong in persoonsgebonden en adresgebonden communicatie. Bij persoonsgebonden communicatie moet direct informatie over de lokatie van de abonnee

worden opgeslagen, terwijl dit bij een ISDN-abonnee pas het geval is als een supplementaire dienst wordt geleverd, die informatie over de lokatie nodig heeft. Dit is dan ook de reden dat zij apart in de figuur zijn opgenomen.

In de tweede plaats wordt de gebruiker de mogelijkheid geboden rechtstreeks van de C7-signalering gebruik te maken (signalering tussen abonnees). De C7-signalering biedt de gebruiker, naast 'normale signalerings boodschappen', mogelijkheden voor supplementaire diensten. Het signaleringsnet dient op haar beurt als een betrouwbaar transportmiddel voor het intelligente net. Op die manier worden de bijzondere faciliteiten in verbindingsofbouw, routing en tarifiering aan de gebruiker geleverd.

In hoofdstuk 3 zijn reeds de faciliteiten, functies en diensten besproken. Kijken we nu naar figuur 4-10 dan zien we dat op het gebruikersniveau de diensten worden geleverd. Dit wordt mogelijk doordat de faciliteiten, die zich op het hoogste niveau bevinden, door functies worden afgehandeld. Daarnaast biedt het signaleringsniveau zelf functies en faciliteiten. De diensten blijven echter op het gebruikers niveau staan.



Figuur 4-10: Componenten in een modern telecommunicatienet [9]

De gebieden in figuur 4-10 die betrekking hebben op management zijn slechts voor de volledigheid weergegeven. In het kader van dit verslag worden zij niet behandeld.

4.8. Samenvatting

Door gebruik te maken van de gemeneweg signalering C7 kunnen extra diensten aan de abonnee worden geleverd zoals: identificatie oproeper, identificatie opgeroepene, besloten gebruikersgroep etcetera. Door de gemeneweg signalering is het mogelijk om via een apart signaleringsnet, dat parallel aan het schakelnet ligt, het complete telefoonnet te besturen. Door het intelligente net is de mogelijkheid ontstaan om snel nieuwe diensten te leveren aan de abonnee. Echter de invoering daarvan gebeurt los van de transportstructuur. Verbindingsfunctie en dienstenfunctie zijn ontkoppeld.

Door de integratie van de huidige netten ontstaat het Integrated Services Digital Network (ISDN). Door het ISDN worden netdiensten aangeboden, via welke het mogelijk is om

64 kbit/s zowel circuit- als pakket-geschakelde verbindingen op te bouwen voor spraak en datatransport.

De huidige ontwikkeling in de mobiele sector wordt gekenmerkt door het persoonsgericht zijn. Deze vorm van communicatie staat tegenover het begrip 'adresgebonden communicatie'. Als voorbeeld is het toekomstige GSM-netwerksysteem besproken.

Het datanet is ontstaan door de grote groei in het computergebruik. Als gevolg van deze groei ontstond de vraag naar de mogelijkheid van transporteren van computergegevens. In dit net is de wijze van overdragen gebaseerd op pakketschakelen. Hierbij wordt het te verzenden bericht in even grote stukken opgedeeld, waarna het verzonden wordt. Ieder pakket bevat een adres waar het afgeleverd moet worden en begeleidende informatie. Door de begeleidende informatie zijn onder andere de volgende diensten mogelijk: identificatie van de oproeper of opgeroepene, besloten gebruikers groep, opgeroepene laten betalen (al of niet met zijn toestemming). Deze netdiensten lijken veel op de diensten die door C7 aan de abonnee geleverd kunnen worden, want wat de header voor het pakketschakelen is, is het aparte signaleringskanaal voor het circuitschakelen.

Ook is de samenhang tussen de componenten, welke de basis vormen voor de diensten die aan de gebruiker geleverd kunnen worden, besproken. Achtereenvolgens zijn dit het intelligente net, de C7-signalering en de toegang tot het telecommunicatienet door middel van eindapparatuur (mobiel of ISDN).

5. Koppeling van systemen

Koppeling van systemen kan op verschillende niveaus plaatsvinden. Er kan onderscheid worden gemaakt tussen:

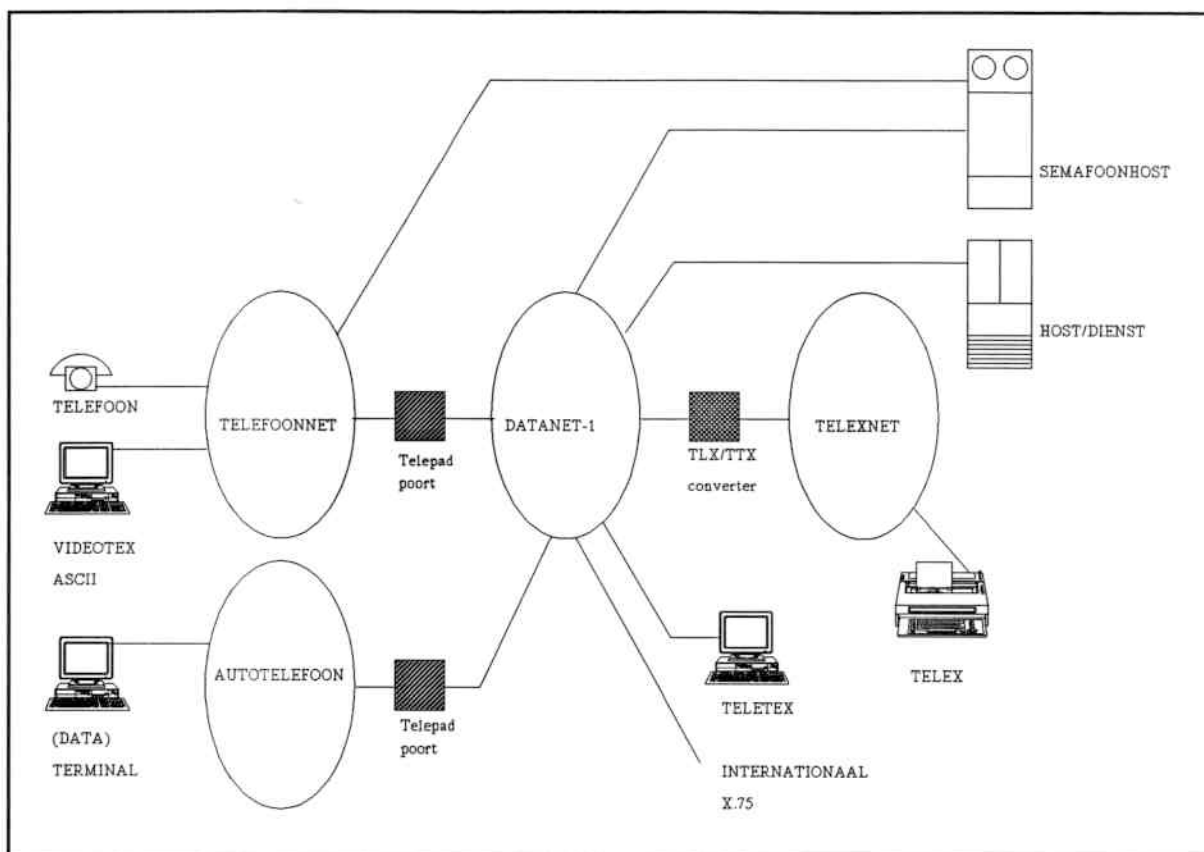
- fysieke koppeling,
- koppeling van gegevensbestanden.

5.1. Fysieke koppeling

Onder fysieke koppeling wordt verstaan het, via transmissielijnen of via elektromagnetische golven, met elkaar in verbinding brengen van twee of meer systemen. Hierbij nemen gekoppelde computers berichten of gegevens van elkaar over en/of fungeren ze als tussenstation voor het doorgeven daarvan. [4]

Een voorbeeld van een koppeling van twee netten is die van een toegang tot het datanet via het telefoonnet. Het doel van zo'n koppeling is kleingebruikers ook in de gelegenheid te stellen gebruik te maken van het datanet, zonder de lasten van een directe aansluiting te dragen. Een ander doel is nieuwe diensten bereikbaar te maken. In figuur 5-1 zijn de momenteel gerealiseerde koppelingen tussen de netten in beeld gebracht. In figuur 4-3 viel reeds te zien dat de C7-signalering voor verschillende netten kan worden gebruikt.

Hierbij doet zich tevens de ontwikkeling voor dat communicatiesignalen qua vorm niet of nauwelijks meer te onderscheiden zijn; wat dat betreft is er een samenvloeien van, in digitale vorm voorkomende, telefoongesprekken, telexverkeer, uitwisseling van gegevens tussen computers, beeld, etcetera. De vele soorten van koppelbare netwerken met verschillende protocollen en de vele stations die bestanden kunnen passeren, maken het moeilijker om na te gaan waar een bestand (ver)blijft.



Figuur 5-1: Gerealiseerde koppelingen in Nederland

5.2. Koppeling van gegevensbestanden

De toegenomen mogelijkheden in de automatisering in het algemeen en de telematica in het bijzonder, maken het mogelijk een koppeling tussen verschillende bestanden tot stand te brengen. Onder het koppelen van bestanden wordt verstaan het geautomatiseerd vergelijken van gegevens die betrekking hebben op een zelfde persoon, uit verschillende bestanden. Nadat koppeling op dit niveau heeft plaatsgevonden, bestaat de mogelijkheid om de (persoons)gegevens uit de diverse bestanden samen te voegen. In dat geval spreekt men van integratie van (gegevens)bestanden. Dit integreren van gegevensbestanden kan leiden tot een (bijna) volledige persoonsbeschrijving, een 'blauwdruk' van een individu. Hierdoor kunnen de meest uiteenlopende doelstellingen worden nagestreefd.

5.3. Het privacyaspect van koppelingen

Uit het voorgaande is gebleken dat de verbinding van lokale bestanden in netwerken kan leiden tot een creatie, bewerking en gebruik van persoonsgegevens dat, zonder maatregelen te treffen, aan vrijwel iedere controle ontsnapt, ook doordat het te controleren gebied grootschaliger wordt en dus moeilijker te beheersen. De processen in netwerken zijn zo snel en gecompliceerd dat zij voor het individu ondoorzichtig, ongrijpbaar en oncontroleerbaar dreigen te worden.

Bij het vergelijken van bestanden kunnen bepaalde personen of categorieën van personen opgespoord worden. Dit wordt meestal gelegitimeerd met de noodzaak om fraude van geregistreerden en fouten en bestanden op te sporen. In feite kunnen hiermee echter de meest uiteenlopende doelstellingen nagestreefd worden, waaronder puur commerciële. De technieken op dit terrein worden steeds krachtiger, in steeds kortere tijd kunnen als maar grotere bestanden tegen elkaar afgedraaid worden.

Door het integreren van bestanden kunnen profielen van personen gemaakt worden. Op deze manier wordt de afstand tot de bron van de gegevens echter steeds groter. Bij de bewerking zijn in feite nieuwe gegevens gecreëerd (vaak met een ander doel dan dat van de oorspronkelijke registratie). De betrokken persoon wordt vrijwel nooit op de hoogte gebracht van deze bewerkingen en nieuwe doelstellingen. Er kunnen hierbij gemakkelijk fouten worden gemaakt en onjuiste veronderstellingen gehanteerd worden. Door dit alles wordt de informationele privacy in sterke mate bedreigd.

5.4. Samenvatting

Door de fysieke koppeling kunnen verschillende gegevensbestanden gekoppeld worden. Hierdoor ontstaat de mogelijkheid bijna volledige profielschetsen van personen te creëren. De informationele privacy kan hierdoor in het geding komen.

6. Knelpunten

Het gebied van de adresgebonden communicatie zal ontwikkelen naar persoonsgebonden communicatie. De overgang van kanaalgebonden signalering naar gemeneweg signalering samen met de introductie van het intelligente net is de andere ontwikkeling die ervoor zorgt dat de dienstverlening voor de gebruiker groter wordt. Feit is echter dat voor de levering van deze diensten gegevens nodig zijn, waardoor persoonsgerichte informatie beschikbaar komt. Anderzijds is er de datacommunicatie. In het datanet worden soortgelijke diensten geleverd, met als verschil dat dit, hoofdzakelijk, een pakketgeschakeld net is. In dit hoofdstuk zullen die zaken van de C7-signalering, het intelligente net en de mobiele (persoonsgebonden) communicatie, aan de orde komen, welke in relatie tot de privacy van belang zijn. Kortom waar zitten de knelpunten?

6.1. Knelpunten in C7-signalering

Zoals reeds in paragraaf 4.2.2 is vermeld, kunnen het TUP en het ISDN-UP getypeerd worden als signaleringsgebruikers. De knelpunten voor deze signaleringsgebruikers zitten in de signaleringsinformatie. Er bestaan immers standaard boodschappen onder meer voor het tot stand brengen van een oproep (zie paragraaf 4.2.3). Hiervoor worden onderscheiden [18]:

IAM Initial Address Message

Boodschap in de zendrichting die het uitgaande circuit reserveert. Hierin worden verstuurd:

- de adresinformatie: volledig nummer van de opgeroepen gebruiker.
- informatie die wordt vereist voor de oproepverwerking, bijvoorbeeld aanvullende services, waarmee rekening wordt gehouden tijdens het opbouwen van een oproep.

SAM Subsequent Address Message

Transporteert, indien van toepassing, de digits die zich niet in de IAM bevinden.

ACM Address Complete Message

De opgeroepen gebruiker is vrij (en compatibel) en heeft de oproep beantwoord met ALERT (Alerting).

ANS Answer

Oproep geaccepteerd door de opgeroepen gebruiker met CONN (Connect).

Nemen we nu de supplementaire dienst 'identificatie van de oproeper' in beschouwing, dan blijkt dat deze op twee manieren te leveren is. Beide manieren vinden hun oorsprong in de signaleringsinformatie. De eerste mogelijkheid is dat het bovengenoemde IAM hiervoor zorgt. In het IAM wordt dan direct het nummer van de oproepende abonnee meegestuurd. Een tweede mogelijkheid is dat na een verzoek van de opgeroepene, door middel van een 'ISDN-UP information request' boodschap, het nummer wordt getransporteerd. Tevens heeft de oproeper de mogelijkheid 'Calling Line Identity Restriction' (CLIR) te activeren. Wanneer deze optie geactiveerd is wordt rechtstreeks door het IAM verhinderd dat het telefoonnummer van de oproeper bij de opgeroepene getoond wordt. [19]

De 'call forwarding'¹ dienst is, naast identificatie van de oproeper, de andere privacy bedreiger die zijn oorsprong vindt in de signaleringsinformatie. Deze dienst wordt op de volgende manier gerealiseerd: wanneer een IAM ontvangen is, wordt in de centrale van een opgeroepene waarvoor call forwarding geactiveerd, is vastgesteld of het nummer waarnaar omgeleid moet worden zich in dezelfde centrale bevindt. Als dit het geval is wordt de abonnee op het omgeleide nummer gebeld en wordt een ACM naar de centrale van de oproeper gestuurd. Als het nummer waarnaar omgeleid moet worden daarentegen aan een andere centrale verbonden is, wordt vanuit de oorspronkelijke bestemmingscentrale een IAM met het omgeleide nummer en het gekozen nummer

¹ Call forwarding: De mogelijkheid dat een oproep wordt omgerouteerd naar een andere aansluiting. Dit kan gebeuren als de aansluiting bezet is, als de oproep niet binnen een bepaalde tijd wordt beantwoord of altijd.

getransporteerd naar de centrale van het omgeleide nummer. Tot slot wordt, vanuit de centrale van het omgeleide nummer, een ACM naar de centrale van de oproeper gestuurd. [19]

Ook al zijn de supplementaire diensten, die door C7 aan de gebruiker geleverd kunnen worden gebaseerd op het transport van het telefoonnummer van de oproeper, er is toch een wezenlijk verschil tussen de bovengenoemde diensten. Dit verschil zit in het opslaan van gegevens. Voor het leveren van de supplementaire dienst 'identificatie van de oproeper' hoeft namelijk niets in het telecommunicatiesysteem te worden opgeslagen. Voor de 'call forwarding' dienst is dit wel het geval, er moet immers in het systeem bekend zijn naar wie het gesprek omgeleid dient te worden.

Deze privacy bedreigende supplementaire diensten worden volledig op het C7-signaleringsniveau volgens figuur 4-10 afgehandeld. Dat wil zeggen dat zowel de functies als de faciliteiten zich op dit niveau bevinden. In andere gevallen dient het C7-signaleringsnet als een betrouwbaar transportmiddel voor de overdracht van niet-signalerings specifieke informatie. Door middel van het Transaction Capabilities Application Part (TCAP) wordt dan een voorziening gevormd voor interactief gebruik in gedistribueerde toepassingen [18]. De knelpunten moeten dan niet in het signaleringssysteem gezocht worden.

6.2. Knelpunten in het intelligente net

Het belangrijkste kenmerk van het intelligente net is de snelle toegang tot grote gecentraliseerde databases. Het in de vorige paragraaf genoemde TCAP wordt gebruikt voor de toegang tot deze netwerk-databases. Supplementaire diensten die door het intelligente net geleverd kunnen worden zijn bijvoorbeeld:

- Universeel nummer (zie voorbeeld paragraaf 4.3)
- Credit Card oproepen

Knelpunten in het intelligente-net-concept moeten worden gezocht in de creatie van deze databases. Aan de hand van de, in deze databases opgeslagen, informatie wordt bepaald waar een gesprek naar toe moet worden gerouteerd of wordt de geldigheid van een credit card gecontroleerd.

Om deze diensten te kunnen leveren is een aantal 'Service Independent Building Blocks' (SIB's) gedefinieerd. Applicatie ontwerpers wordt het op deze manier mogelijk gemaakt snel bestaande diensten te wijzigen of nieuwe diensten te ontwikkelen. De SIB's zijn als softwarefuncties in de SCP en SSP geïmplementeerd. Er bestaan onder andere functies voor routing, authenticatie, location updating. [20]

De privacy bedreigers op het niveau van het intelligente net (zie figuur 4-10) worden door deze SIB's gevormd, zij zorgen ervoor dat informatie wordt opgeslagen. Het C7-signaleringssysteem biedt de mogelijkheid om deze niet-signalerings specifieke informatie over te brengen. Wel kan, afhankelijk van de applicatie en in combinatie, gebruik worden gemaakt van C7-signaleringsboodschappen. De functies kunnen zich dus zowel op het niveau van het intelligente net, als op het signaleringsniveau bevinden. De faciliteiten bevinden zich op het niveau van het intelligente net.

6.3. Knelpunten in mobiele communicatie

Mobiele abonnees kan men zien als continue gebruikers van het 'follow me' principe. Er moet in het systeem direct en continu informatie over de lokatie van de abonnee worden opgeslagen, dit in tegenstelling tot een ISDN-abonnee. Bij deze is dit pas het geval als een supplementaire dienst verlangt wordt, die informatie over de lokatie van de abonnee nodig heeft. Het in paragraaf 4.5.1 besproken GSM-netwerksysteem is een dienst welke volgens het principe van het intelligente net geleverd kan worden [21].

Het zal duidelijk zijn dat de functie 'location updating', welke beschikbaar is als een SIB, het knelpunt vormt. Wanneer deze procedure voltooid is zal de database van het HLR

(home location register) immers weer up-to-date zijn. Door de vertaling van het ISDN-nummer naar het IMSI en TMSI valt in de VLR's niet te achterhalen waar de mobiele abonnee zich bevindt.

De location updating procedure gaat in het GSM-netwerksysteem als volgt te werk; zodra het MS merkt dat er een wijziging optreedt in het Location Area waar het rondrijdt, zendt het een LU-Request (Location Updating Request) naar het netwerk. Hierin staat de code van het location area waar het MS vandaan komt. Het MSC gaat het hem toegewezen VLR vragen om de gegevens van dit binnenrijdende MS op te nemen. Het VLR moet vervolgens weten wie dit MS is. Hiervoor wordt het oude VLR van het MS geraadpleegd. Location updating vindt vervolgens in het HLR plaats. Dit HLR zorgt er ook voor dat de informatie in het oude MSC gewist wordt. Het nieuwe VLR geeft via het MSC aan dat de location updating procedure is gelukt. [16]

6.4. Samenvatting

De knelpunten in het telecommunicatiesysteem blijken door een aantal functies, in dit telecommunicatiesysteem, weergegeven te kunnen worden. Op het signaleringsniveau gaat het om het transport van het telefoonnummer van de oproeper. Dit transport wordt verzorgd door de signaleringsboodschap IAM.

Op het niveau van het intelligente net zijn Service Independent Building Blocks gedefinieerd. Zo beschrijft iedere SIB een basisfunctie voor het leveren van een faciliteit volgens het intelligente net concept. De SIB's vormen dan ook de knelpunten bij het intelligente net, zij zorgen voor het creëren en raadplegen van de databases die nodig zijn voor het leveren van een supplementaire dienst.

Bij de mobiele communicatie ontstaat de situatie waar zowel de faciliteit (het-altijd-en-overal-bereikbaar-zijn) als de functie (gegevens over de lokatie door middel van een location updating procedure) het probleem voor de privacy vormen.

7. Maatregelen om privacy te waarborgen

7.1. Wanneer is privacy gewaarborgd?

Privacy wordt veelal beschouwd als gewaarborgd indien:

- onbevoegden geen kennis kunnen nemen van (persoonsgebonden) gegevens;
- zij die wel bevoegd zijn van dergelijke gegevens kennis te nemen, deze kennis niet misbruiken;
- gegevens anoniem zijn opgenomen.

7.2. Privacy-beschermende maatregelen

Er zijn vier soorten van privacybescherming die kunnen worden toegepast bij netwerken:

- juridische bescherming;
- systeemtechnische en organisatorische bescherming;
- sociale bescherming: vormen van weigering, van zeggenschap en gedragsregulering;
- technische alternatieven

Momenteel is de aandacht hoofdzakelijk gevestigd op de twee eerstgenoemde soorten.

7.2.1. Juridische bescherming

De Wet persoonsregistraties vormt in Nederland vrijwel de enige wettelijke bescherming voor de informationele privacy in netwerken. De aspecten van relationele privacy worden slechts in zeer algemene zin door de Grondwet gedekt. [6]

Het probleem met de WPR is echter dat hoofdbegrippen als persoonsregistratie en houder vreemd zijn aan het dynamische karakter van gegevensstromen in netwerken. Gegevens in netwerken worden voortdurend verzameld, herzien en gebruikt. Zij zijn steeds in beweging, niet alleen wat hun plaats, maar ook wat hun status in het informatieverwerkend proces betreft [22]. Met het laatste wordt onder meer bedoeld dat de registratie wel zeer kortstondig kan zijn, maar toch lang genoeg om in het praktische gebruik de privacy te bedreigen. Een voorbeeld is de voortdurende waarneming van gebruiksgegevens (wie raadpleegt welke informatie, hoe lang en hoe vaak) bij videotex, die gecombineerd kunnen worden met abonneegegevens die wel opgeslagen zijn (zie ook appendix E: Elektronisch bestellen heeft weinig toekomst, Persoonsgegevens kunnen probleem worden). De Wet gaat echter niet uit van verzameling maar van 'blijvende neerslag of opslag' van persoonsgegevens.

Het is zeer moeilijk de 'houder' te bepalen van bestanden die voortdurend in beweging zijn. In de WPR (artikel 1) wordt de houder gedefinieerd als:

'degene die de zeggenschap heeft over een persoonsregistratie.'

In de Memorie van Toelichting is dit degene die 'bevoegd is het doel, de inhoud en het gebruik daarvan te bepalen'. Of hieronder de hoogste leiding van een organisatie verstaan moet worden of, bijvoorbeeld, het hoofd van een afdeling is niet duidelijk [7]. Van beslissend belang is dat de houder de doelstelling van de registratie omschrijft en dat deze ook de taakverdeling voor personen die toegang hebben tot de gegevens bepaalt.

Een belangrijke vraag voor de bescherming van de persoonlijke levenssfeer in verband met nieuwe diensten is ook in hoeverre er eigenlijk sprake is van 'persoonsgegevens'; vallen de bewegingen van een individu die in telemetrische toepassingen met behulp van sensors worden geregistreerd daaronder? Of de digitale verwerking van stemgeluiden door de elektronische post [23]?

7.2.2. Systeemtechnische en organisatorische bescherming

Bij systeemtechnische beveiliging gaat het om bewaking, afsluiting, gebruik van toegangspassen en een zo veilig mogelijke constructie van netwerken. Deze beveiliging blijft kwetsbaar, zoals regelmatig in de kranten te lezen valt, als het gaat om computerinbraken, virussen en platliggende systemen. De commissie Franken heeft voorgesteld de verantwoordelijkheid bij het betreffende bedrijf zelf te leggen. Het inbreken in computers wordt dan ook slechts strafbaar gesteld indien een bedrijf voldoende maatregelen heeft genomen om zijn computergegevens te beschermen [2].

Organisatorische maatregelen zijn bedoeld voor het afbakenen van taken, bevoegdheden en verantwoordelijkheden [24]. Hierbij worden procedures vastgelegd in de vorm van draaiboeken en toegangsregelingen. Bij bestanden met persoonsgegevens worden dan bijvoorbeeld personen aangewezen die bepaalde dingen met deze bestanden mogen doen, terwijl anderen geen toegang krijgen.

7.2.3. Sociale bescherming

De min of meer bewuste weigering van consumenten om aan elektronisch verkeer deel te nemen, onder meer vanwege de geringere persoonlijke autonomie en het risico, is de belangrijkste aanleiding geweest voor banken en videotex-bedrijven om zelf met gedragscodes te komen.

Op dezelfde dag als de WPR in werking trad het Privacycharter voor het Bankwezen in werking. Met deze code gaan de banken uit eigen beweging verder dan zij volgens de WPR zouden hoeven. Met name de verwachte aarzeling van de consumenten om aan het elektronisch betalingsverkeer deel te nemen was hier de oorzaak van. Onzekerheid over privacybescherming zou een van de remmende factoren zijn.

Bij Viditel is het in principe mogelijk dat de PTT kan vastleggen wie welke informatie, hoe lang, hoe vaak raadpleegt. In de Viditelkode is echter vastgelegd dat gebruiksgegevens slechts door middel van steekproeven bij anonieme gebruikers mogen worden ingewonnen. Hierin staat tevens omschreven dat de leveranciers bij direct interactief contact met de gebruikers slechts bepaalde gegevens van hen mogen vragen. De gebruiker wordt op de hoogte gesteld van het doel van deze gegevensinwinning en bezit inzage-, correctie- en verwijderingsrecht.

7.2.4. Technische alternatieven

Wat de technische alternatieven betreft kunnen de volgende oplossingen aangedragen worden:

- 1) minder grootschaligheid
- 2) minder integratie
- 3) een zo kaal mogelijke openbare infrastructuur
- 4) meer decentrale apparatuur
- 5) meer decentrale coderingen

ad 1: In plaats van grootschaliger netwerken aan te leggen bespeurt men een ontwikkeling naar lokaal begrensde netwerken die onderling gekoppeld kunnen worden. Dit biedt de gelegenheid tot het nemen van extra veiligheidsmaatregelen en reglementering. Bovendien kunnen op deze manier verschillende soorten netwerken met een afwijkende registratie van het gebruik met elkaar verbonden worden. [6]

Een mogelijkheid is, dat in plaats van een ongedeeld grootschalig schakelnetwerk, een combinatie van glasvezelnetwerken, die in een zogenaamde busstructuur honderd abonnees koppelen aan een lokale centrale van het publieke schakelnetwerk, wordt gerealiseerd. De netbeheerder (PTT) is in dit ontwerp slechts verantwoordelijk voor de transmissie op het laatst genoemde netwerk. Hij kan de ontvanger en de inhoud van het

bericht niet identificeren. De ontvangst wordt pas gedecodeerd op het bestemmingsadres in het lokale netwerk. [6]

De beheerder kent op deze manier wel de zender en de soort dienst die deze vraagt of aanbiedt en de transmissietijd. Er is zo een scheiding van gebruikers- en gebruiksgegevens ontstaan.

Als de netbeheerder tevens dienstenleverancier is zal hij de verbindingsgegevens die hij als transporteur krijgt aangeboden gescheiden moeten houden van de verrekeningsgegevens die hij nodig heeft als beheerder. De verbindingsgegevens moeten na het totstandkomen van de verbinding worden vernietigd. De verrekeningsgegevens mogen als de gebruiker hier om verzoekt een nadere specificatie omvatten met betrekking tot tijdstip, duur en inhoud.

ad 2: Het is twijfelachtig of de integratie van spraak, data, tekst en beeld voor het consumentengebruik wel zo gewenst is. Afzonderlijke verbindingen kunnen zeker even functioneel zijn. Zo bestaat er een alternatief voor het ISDN en zijn opvolger het IBCN (Integrated Broadband Communication Network). Dit gaat lijnrecht in tegen te heersende tendens naar integratie. Er wordt voorgesteld de bestaande netwerken voor spraak, data/tekst en beeld afzonderlijk te verbeteren. Voor de telefonietoepassing zou daarbij niet gebruik gemaakt moeten worden van op software gebaseerde schakelsystemen (waarin de nummers van de beller en ontvanger geregistreerd worden), maar van nieuwe micro-elektronische hardware-schakelingen. Het telefoonverkeer blijft dan, indien gewenst, anoniem. [6]

ad 3: Een van de grootste twistpunten bij de aanleg van openbare netwerken is de vraag waar de meeste 'intelligentie' moet worden opgenomen; in het netwerk zelf, of in de eindapparatuur. De producenten van netwerken pleiten uiteraard voor het eerste en die van eindapparatuur voor het laatste. Vanuit privacy oogpunt lijkt dit laatste het aantrekkelijkst. Zo wordt het waarschijnlijker dat alleen de netwerkbeheerder de beschikking krijgt over verbindings- en gebruikersgegevens. Die kunnen privacy-gevoelig

zijn (abonneegegevens gekoppeld aan adres, soort, duur en regelmaat van communicatie), maar men kan vastleggen dat zij meteen na het bijschrijven op een verzamelrekening vernietigd moeten worden. Gedetailleerde gebruiksgegevens kunnen dan zowel bij de zender als de ontvanger geregistreerd worden in hun intelligente eindapparatuur, maar los van elkaar, en op anonieme basis. Dit voorstel is een ware ramp voor marktonderzoek en marketing, die immers steeds specifiekere gebruikersgroepen in kaart wil brengen.

Precies het tegenovergestelde voorstel lijkt ook bruikbaar vanuit privacy-oogpunt. Alle 'intelligentie' zit dan in het netwerk. De beheerder krijgt dus beschikking over alle mogelijke gegevens. Hij zal dan echter scherp gereguleerd moeten worden.

ad 4: De meest effectieve oplossing voor de privacy-problematiek is het geheel of gedeeltelijk uitschakelen van het registrerende centrum. Het meest vergaand is het gebruik van volledig decentrale apparatuur. In opmars is nu de CD-ROM die een enorme opslagcapaciteit bezit en daarmee een directe concurrent is van de on-line database. De gebruiker heeft dan thuis de beschikking over verschillende discs waarop hij de voor hem nuttige informatie kan raadplegen. Extra informatie valt te verkrijgen door extra discs te kopen.

Deze apparatuur biedt geen oplossing voor de registratiediensten. Op dit gebied ontwikkelt zich echter een reeks decentrale middelen gebaseerd op het principe van de strippenkaart of tegoedbon. Het meest primitief is de magneet-strippenkaart die slechts voor kleinere dingen bruikbaar is, omdat deze nauwelijks 'intelligentie' bezit en gemakkelijk te kopiëren is. Meer mogelijkheden worden geboden door chipkaarten met een éénmalig beschrijfbaar geheugen. De volgende in de rij is de 'smart card'. Deze bevat niet alleen een geheugen maar ook een kleine microprocessor die zelf bewerkingen kan uitvoeren zonder dat dit van buiten af beïnvloedbaar of controleerbaar is. De kaart kan gebruikt worden voor allerlei transacties. In de on-line koppeling die dan aangegaan wordt schuilt ook het grote gevaar van dit technische alternatief. Mits gebruikers gedwongen worden

om hun kaart in een on-line systeem te pluggen en deze kaart vervolgens leeggezogen wordt met centrale opslag van de meest recente gegevens, dan zijn we met dit alternatief wat betreft privacybescherming van de wal in de sloot terecht gekomen. Van beslissend belang zijn dus de condities waaronder decentrale middelen worden gebruikt. De gebruiker dient hierover zoveel mogelijk controle te hebben (het wel of niet gebruiken, welke gegevens worden wel on-line afgegeven en welke niet). Belangrijk hierbij zijn decentrale coderingen.

ad 5: Bij de huidige systemen ligt het accent vaak alleen op veiligheid van de instantie die zich tegen personen willen beschermen, terwijl in de nieuwe opzet alle partijen hun belangen kunnen beschermen. De grondslag van deze benadering is dat personen over sleutels beschikken die geheim blijven voor instanties en instanties op hun beurt sleutels ontwerpen die geheim blijven voor personen. Tijdens een transactie gebruiken beide partijen deze sleutels om elkaar een gecodeerde bevestiging van de bijzonderheden van de transactie te verschaffen die in geval van geschillen als bewijsmateriaal kan dienen.

[6]

7.3. Samenvatting

Maatregelen voor de bescherming van privacy kunnen op vier manieren worden gerealiseerd, te weten:

- juridische bescherming;
- systeemtechnische en organisatorische bescherming;
- sociale bescherming: vormen van weigering, van zeggenschap en gedragsregulering;
- technische alternatieven

Gezien de besproken resultaten van deze maatregelen zullen zij uiteindelijk alle vier nodig zijn om tot een afdoende bescherming van de privacy te komen.

8. Enkele praktijksituaties

In hoofdstuk 6 viel te lezen welke nieuwe diensten geleverd zullen worden. In dit hoofdstuk zullen een aantal van deze diensten in de vorm van cases behandeld worden. De beschrijvingen hebben tot doel de voorgaande hoofdstukken te illustreren en daarmee een concretere beeldvorming bij de lezer te bereiken.

8.1. Caller ID

Zoals in de inleiding reeds is gezegd geeft Caller ID degene die wordt opgebeld de mogelijkheid, voordat hij de hoorn opneemt, de identiteit van de beller te achterhalen, doordat diens telefoonnummer op een display verschijnt. Het is zelfs mogelijk additioneel een kort berichtje mee te sturen, bijvoorbeeld een steekwoord, zodat degene die wordt gebeld al weet waarover de ander hem wil spreken. Een belangrijk voordeel wordt daarmee al snel duidelijk: doordat je weet wie er belt, kun je beslissen of je de betreffende persoon wel of niet (nu) te woord wil staan. Een ander veel genoemd voordeel is dat anonieme telefoontjes (bedreigingen, hijgers) vrijwel onmogelijk worden.

Naast bovenvermelde voordelen hebben tegenstanders van Caller ID op diverse belangrijke nadelen gewezen: zo functioneren bijvoorbeeld psychische hulpdiensten en tipgevers van de politie alleen optimaal wanneer de anonimiteit gegarandeerd is. Een ander bezwaar doemt op wanneer Caller ID niet standaard bij een toestel wordt geleverd, maar als een extra, tegen bijbetaling verkrijgbare, faciliteit. Dit heeft als negatieve consequentie dat de beller van te voren niet weet of degene die hij belt wel of niet over een Caller ID beschikt. De vraag is uiteraard wiens belang voorrang heeft: dat van de oproeper of dat van de opgeroepene?

8.1.1. Ontwikkelingen in de Verenigde Staten en in Frankrijk

Onder meer in de Verenigde Staten en in Frankrijk zijn reeds ervaringen opgedaan met Caller ID en privacybescherming. In de Verenigde Staten is de discussie met name sinds de uitspraak van het Hof van Pennsylvania op 30 mei 1990 hoog opgelaaide. De telefoonmaatschappij Bell Atlantic wilde in Pennsylvania Caller ID als extra faciliteit op de markt brengen. Het Hof was echter van mening dat Caller ID in strijd met de af luisterwet (Wiretap Act) was en meer algemeen

'that an individual has a right to privacy in the use of his or her telephone and that unauthorized seizure or disclosure of one's telephone number will not be permitted by the courts of this commonwealth'.

Ook het voorstel de invoering met een 'blocking device' te combineren, dat wil zeggen met een mogelijkheid om de identificatie tijdelijk uit te zetten, deed het Hof niet van mening veranderen. Het is nog niet duidelijk wat deze uitspraak zal betekenen voor de andere staten in de VS; zo ging de Public Service Commission in het district Columbia recentelijk wel accoord met een dergelijke gecombineerde invoering.

In Frankrijk houdt men zich al langer met Caller ID bezig. Op grond van de Franse privacywet is de Commission Nationale de l'Informatique et des Libertés (CNIL) ingesteld [25]. Deze commissie heeft onder andere de taak advies uit te brengen over de invoering van nieuwe technologieën, waarbij persoonsgegevens worden verwerkt.

In 1985 is de CNIL om een advies gevraagd over de invoering van Caller ID in het kader van een ISDN-proefproject. De CNIL oordeelde dat haar in beginsel zowel de privacy van de oproeper, als die van de opgeroepene, na aan het hart lag. Om de belangen van beide partijen veilig te stellen, stelde zij voor om voor de duur van het project Caller ID optioneel ter beschikking te stellen, zodanig dat degene die gebeld wordt voordat de communicatie tot stand komt het nummer van de beller kan opvragen. De gebelde heeft dan het voordeel van Caller ID, de beller kan alsnog weigeren zijn identiteit bloot te

geven, en de gebelde kan vervolgens nog steeds beslissen of hij het gesprek nu wel of niet wil. De CNIL vond deze oplossing het beste, omdat de privacy van de beller in bepaalde gevallen een essentiële voorwaarde voor het uitoefenen van de vrijheid van communicatie vormt. De CNIL sprak verder uit dat deze procedure bij ieder gesprek gevolgd zou moeten kunnen worden (case-by-case basis). Het advies van de CNIL werd niet integraal door de Franse Direction Générale des Telecommunications (DGT) overgenomen. Naar aanleiding van de gemaakte opmerkingen besloot DGT om:

- iedere abonnee bij eerste aansluiting op het net te laten kiezen voor wel of geen permanente identificatiemogelijkheid
- Caller ID als extra faciliteit aan te bieden waarvoor betaald moet worden.

De CNIL vond deze oplossing niet helemaal bevredigend, met name omdat, ook wanneer men Caller ID als extra faciliteit wenst, het best nog wel eens voor kan komen dat men op bepaalde momenten toch anoniem wenst te bellen. Desalniettemin heeft de CNIL zich bij deze oplossing neergelegd voor de duur van het project.

Een latere adviesaanvraag betrof de invoering van Caller ID in de Parijse regio (met een digitale telefooncentrale) met verbindingen naar analoge centrales in heel Frankrijk. Technisch gezien ontstonden hierdoor twee verschillende situaties: allereerst de situatie waarin twee abonnees zijn aangesloten op het digitale net en dus beide de mogelijkheid hebben Caller ID als faciliteit te verkrijgen [25]. Hier oordeelde de CNIL dat de privacy afdoende was geregeld: men had het technisch namelijk zo geregeld dat de abonnees van geval tot geval via een extra toets op hun toestel konden beslissen of zij wel of niet hun nummer bekend wilden maken. De tweede situatie betreft het geval waarin een abonnee, aangesloten op een 'ouderwetse' analoge centrale, een abonnee belt die op een moderne digitale centrale is aangesloten. Hier is het niet mogelijk dat een gebelde aangesloten op de 'ouderwetse' centrale zijn telefoonabonnement uitbreidt met Caller ID. Bovendien kan hij niet weten, wanneer hij zelf belt, of de betrokken abonnee nu wel of niet over deze faciliteit beschikt. Dit is opgelost door de invoering van 34-nummers: degene die aangesloten is op een analoge centrale en die zijn nummer niet wenst prijs te geven,

draait nu 34 voor het eigenlijke abonnee-nummer, waardoor identificatie wordt verhinderd.

8.1.2. De situatie in Nederland

In Nederland is de techniek nog wat minder ver ontwikkeld dan in de Verenigde Staten en in Frankrijk. Toch zal ook hier de invoering van Caller ID niet meer lang op zich laten wachten. De vraag is uiteraard of en in hoeverre de privacybescherming in Nederland afdoende is geregeld. Een eerste constatering is dat waarschijnlijkheid de WPR niet van toepassing zal zijn: deze veronderstelt immers de aanwezigheid van een persoonsregistratie. Het verschijnen van een enkel nummer op een schermje kan moeilijk als zodanig worden opgevat [26]. Een andere mogelijkheid is wellicht PTT Telecom, net als haar zusterorganisatie in Frankrijk, te verplichten tot het aanbieden van Caller ID op een optionele en case-by-case basis. In Nederland is de aanleg, instandhouding en exploitatie van de openbare infrastructuur opgedragen aan PTT Nederland NV. De rechten en plichten met betrekking tot telecommunicatie worden uitgevoerd door de dochtermaatschappij PTT Telecom BV. Op grond van Artikel 8 Wet op de Telecommunicatievoorzieningen (WTV) geeft de Minister aan deze verplichting tot aanleg, instandhouding en exploitatie van de openbare infrastructuur nader inhoud in de Algemene Richtlijnen (zie appendix C). De PTT is verplicht deze richtlijnen, althans ten aanzien van het te bereiken resultaat, op te volgen. Met betrekking tot de privacybescherming zegt Artikel 8 lid 3 sub e WTV dat:

'3. De richtlijnen (..) bevatten uitgangspunten en maatstaven voor:

(..)

e. de bescherming van de persoonlijke levenssfeer met betrekking tot de krachtens artikel 4, eerste lid, omschreven diensten en vaste verbindingen;

(..)'.

De uitwerking van Artikel 8 lid 3 sub e in de Algemene Richtlijnen heeft op dit moment alleen betrekking op de verplichting voor PTT Telecom het grondwettelijk gegarandeerde telefoon en telegraafgeheim na te leven. Concluderend kan dan ook worden gesteld dat op dit moment in Nederland het juridisch kader om privacy en Caller ID met elkaar te verzoenen nog ontbreekt. Een aanvulling van de Algemene Richtlijnen met betrekking hierop lijkt ten zeerste gewenst [26].

8.1.3. Europese richtlijn

Op 13 september 1990 is een Ontwerp Richtlijn van de EEG gepubliceerd betreffende [27]:

'the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks'

Zie appendix D. Deze richtlijn behandelt onder meer Caller ID. Het ontwerp (in artikel 12 en 13) komt in grote mate overeen met de in Frankrijk gekozen oplossing: abonnees aangesloten op een digitale centrale moeten de mogelijkheid hebben van geval tot geval de Caller ID uit te schakelen. Zowel beller als gebelde dienen over deze mogelijkheid te kunnen beschikken. Abonnees die van een analoge centrale naar een digitale centrale bellen moeten op de hoogte worden gebracht van Caller ID en de mogelijkheid gegeven worden deze faciliteit uit te sluiten, zowel permanent als, indien gewenst, van geval tot geval. Caller ID zonder blockingsmogelijkheid kan tijdelijk worden toegestaan om hijgers of andere lastige telefoontjes te kunnen achterhalen of ter opsporing van delicten. Verder kunnen op verzoek alarmdiensten een permanente ontheffing krijgen van het blocking device.

8.2. Gespecificeerde rekening

Genieten van een 06-sexlijn, je hart uitstorten bij een SOS hulpdienst, informatie vragen bij de aidslijn, of gewoon anderhalf uur 'kleppen' met een kennis. Gezin en partner leven straks mee. Het voeren van privé gesprekken op het werk. De werkgever leeft straks mee. Het bewijzen van onschuld of schuld van een verdachte. Detectives en politie leven straks mee. De privacy van de telefoon staat op het spel. De PTT gaat volgend jaar gespecificeerde rekeningen sturen (zie appendix E: PTT Telecom gaat specificatie gesprekskosten op telefoonnota voorbereiden).

De consumentenbond staat achter de PTT. De vereniging stelt dat zich, door de gespecificeerde nota, minder problemen over de afrekening zullen voordoen. Fouten en storingen komen meteen aan het licht. De consument zou met de nieuwe nota in de hand, precies kunnen aanwijzen welke telefoongesprekken hij absoluut niet heeft gevoerd. Volgens de Stichting Waakzaamheid Persoonsregistratie is dit onzin. Elk telefoongesprek wordt geregistreerd, niet de rechtmatigheid ervan. Bij problemen blijft de welles nietes situatie bestaan. [28]

Voor het bedrijfsleven is de gespecificeerde rekening direct en indirect een groot voordeel. De werkgever houdt grip op het aantal gevoerde privégesprekken van de werknemer. Bovendien kunnen werkgever en werknemer de te vergoeden zakelijke gesprekken beter aantonen bij de fiscus.

Echter de privacy van een opgeroepene bij een volledig gespecificeerde rekening wordt ook aangetast. Wordt bijvoorbeeld een verkeerd telefoonnummer gekozen, staat dit nummer wel op de rekening van de oproeper.

Het dilemma van dienstverlening versus privacy steekt de kop weer op. De Europese Commissie onderkent dit door de PTT's te adviseren de laatste 4 cijfers niet op de rekening te vermelden. Dit zou echter de belanghebbende op een verkeerd spoor kunnen brengen: Een 06-nummer is niet enkel een sexlijn, maar ook een autotelefoonnummer.

In de Verenigde Staten spelen op het moment de volgende vragen: Van wie is het telefoonnummer? Is dit het bezit van de abonnee of van de telefoonmaatschappij? Wie kan ermee doen wat hij wil? De telefoonmaatschappijen gaan ervan uit dat het telefoonnummer hun eigendom is. De advocaat Thomas McManus zegt dat de wet hierover niet duidelijk is. [12][29]

8.3. Autotelefoon

In de huidige situatie zijn autotelefoongesprekken eenvoudig af te luisteren [30]. Voor weinig geld zijn radio's of scanners te koop die het frequentiegebied van de autotelefoons kunnen aftasten. Volgens de PTT zijn de autotelefoon-bezitters op de hoogte van die beperkte privacy en wordt hen dat van tevoren ook duidelijk gemaakt. Het af luisteren is te voorkomen door de autotelefoon aan te sluiten op een codeerapparaat.

Het scannen van de telefoongesprekken is niet verboden. Wordt de opgevangen informatie echter gebruikt of misbruikt, dan begaat de af luisterende persoon een strafbaar feit [2]. Met de komst van het GSM-systeem (zie paragraaf 4.5.1) wordt het af luisteren van autotelefoongesprekken echter onmogelijk.

Het aantal louche praktijken dat per autotelefoon wordt geregeld, is zeer groot. Zo legde een directeur vanuit zijn auto de administrateur uit hoe hij omvangrijke bedragen kon wegschrijven uit de boekhouding. Ook werd een gesprek gevoerd waarin twee lieden 'even' een strategie uitstippelden om een bedrijf failliet te verklaren. Zelf hielden ze daar een aardige cent aan over. [30]

Hoewel het de politie nuttige informatie kan opleveren, heeft zij eerst toestemming nodig van de rechter-commissaris, voordat zij kan overgaan tot het af luisteren van gesprekken.

Er is ook een geval bekend van een verdachte, die aan de hand van bestanden die de PTT bijhoudt, kon aantonen dat hij op het moment van de misdaad ergens anders

vertoefde [29]. Zo kan iets dat gezien wordt als aantasting van de informationele privacy ook positief werken. Maar gaan we nu niet toe naar een strafrechtelijk systeem, waarbij mensen hun onschuld moeten bewijzen door een stuk privacy bloot te geven?

8.4. Telegids

Via videotex bestaat er voor de gebruiker de mogelijkheid het elektronische gegevensbestand van 008 op te roepen. Hierbij was het mogelijk bij een nummer de bijbehorende naam en adresgegevens te achterhalen. Welliswaar is dat ook mogelijk door de nummers die in het telefoonboek staan vermeld handmatig te vergelijken, door de snelheid waarmee dit via videotex kon plaatsvinden ontstond echter een grotere bedreiging van de privacy. In appendix E is de huidige stand van zaken te lezen (PTT zwicht voor privacy, Bedreiging privacy met Telegids blijft mogelijk ondanks beperking zoekmethoden door PTT).

8.5. Samenvatting

Deze beschrijvingen hadden de bedoeling de voorgaande hoofdstukken te illustreren en daarmee een concretere beeldvorming bij de lezer te bereiken.

9. Conclusies en aanbevelingen

9.1. Conclusies

Supplementaire diensten kunnen door het intelligente net en de C7-signalering eenvoudig aan de gebruiker geleverd worden.

Gegevens die door het leveren van supplementaire diensten vrijkomen, kunnen een bedreiging vormen voor de informationele privacy en in mindere mate voor de relationele privacy. Het betreft hier gegevens over de abonnee ten opzichte van zowel de telecommunicatieorganisatie, als van degene waarmee gebeld wordt en een ieder ander die toegang heeft tot deze gegevens.

De knelpunten bevinden zich in de functies die nodig zijn om deze supplementaire diensten te kunnen leveren. Hierbij dient een onderscheid te worden gemaakt tussen opslag van gegevens in databases en transport van het abonneenummer over het telecommunicatienet.

Door koppeling van systemen ontstaat de mogelijkheid dat gegevensbestanden geïntegreerd kunnen worden. Hierdoor kan een profielschets van een persoon gecreëerd worden. Om toch de privacy van een persoon te kunnen waarborgen zullen dus maatregelen getroffen moeten worden.

9.2. Aanbevelingen

Bij regelgeving op het gebied van privacy moet ervoor worden opgepast dat er geen verspreiding plaatsvindt van de bepalingen naar de afzonderlijk wetten toe. De WPR is ervoor om de privacy te waarborgen en dient daarom een overkoepelende wet te zijn.

Als de netbeheerder tevens dienstenleverancier is moet hij er voor zorgen dat:

- de gegevens die onder zijn beheer vallen op organisatorische en systeemtechnische wijze beschermt zijn;
- de verbindingsgegevens gescheiden blijven van de verrekeningsgegevens;
- de verbindingsgegevens na het totstandkomen van de verbinding vernietigd worden;
- de verrekeningsgegevens vernietigd worden aan het einde van de wettelijke termijn waarin de factuur kan worden betwist.

Als een bedrijf of netbeheerder of dienstenleverancier is dient zij op bovengenoemde manier zorg te dragen voor de gegevens die zij beheert.

Bij het leveren van supplementaire diensten dient de oproeper ervan op de hoogte te worden gebracht dat de opgeroepene over deze dienst beschikt. Bijvoorbeeld:

- een toon of gesproken boodschap ter indicatie van een doorschakeling;
- een toon of verlengd abonneenummer ter indicatie van Caller ID, zodat de oproeper de gelegenheid heeft om identificatie uit te schakelen.

De ontwerp richtlijn voor privacybescherming bij digitale communicatie, ontworpen door de Europese Commissie, zou bepalingen moeten bevatten voor tele-informatiediensten die in het algemeen gelden. Nu zijn slechts telefonie, teleshopping en videotex in de bepalingen opgenomen. Men zou kunnen redeneren dat de richtlijn niet op andere diensten van toepassing is, behalve op wat in de algemene bepalingen staat.

De abonnee moet beter op de hoogte worden gebracht van zijn rechten, zoals inzagerecht in zijn gegevens. Ook het doel van het aanleggen van een bestand waarin persoonsgegevens zijn opgenomen moet aan de abonnee worden vermeld.

De vraag hoever gegaan moet worden met het nemen van maatregelen om privacy te beschermen is er één die niet direct kan worden beantwoord. Er zal steeds een afweging moeten worden gemaakt tussen verschillende belangen. Men moet zich echter wel realiseren dat het verkrijgen van absolute privacy ondenkbaar is.

Literatuur

- [1] Katz, James E.,
"US telecommunications privacy policy",
Telecommunications policy, December 1988, pp. 353-368.
- [2] Franken, H.,
Informatietechniek & Strafrecht: Rapport van de commissie computercriminaliteit,
Staatsuitgeverij, Ministerie van Justitie, april 1987,
ISBN 90 12 05543 1.
- [3] Fineberg, Victoria, Lingham, Shankar, Yu, James I.,
"Wireless Impact on Personal Telecommunications Services",
Telecommunication Acces Networks, Technology and Service Trends, pp. 69-75,
Elsevier Science Publishers B.V. (North-Holland), 1991.
- [4] Enden, P.C.M. van der,
Privacy, een kwaliteitsaspect van informatiesystemen,
1988 Samsom Uitgeverij bv, Alphen aan den Rijn,
ISBN 90 14 03913 1.
- [5] Holvast, J.,
Op weg naar een risicoloze maatschappij?,
Academic Service, Schoonhoven 1986.
- [6] Dijk, Jan van,
"Netwerken en privacy: bedreiging en juridische bescherming",
Privacy en Registratie, september 1989, nr. 3, pag. 4-10.
- [7] Pous, V. de,
Computer privacy in Nederland: Uitleg, inzicht, vragen en antwoorden inzake de Wet
persoonsregistraties,
Kluwer, Deventer 1989,
ISBN 90 268 1933 1.
- [8] Zoete, J.M.M. de, Graaf, M. de,
"Diensten en gebruiksaspecten van diensten in het ISDN",
Het PTT-Bedrijf, december 1986, Deel XXIV nr. 1-4, pag. 52-60.
- [9] Jong, C. de,
Telecommunicatie, i.h.b. Strategieën voor Openbare Structuren,
Collegedictaat eel, december 1990,
TU Delft, Faculteit der Wijsbegeerte en Technische Maatschappijwetenschappen,
Sectie Maatschappelijke en Organisatorische Aspecten van de Telecommunicatie.

- [10] Jong, C. de,
Waarmee kan ik u van dienst zijn?: Vraag en aanbod in de telecommunicatie
Rede uitgesproken bij de aanvaarding van het ambt van deeltijd hoogleraar in de
Maatschappelijke en Organisatorische Aspecten van de Telecommunicatie aan de
Faculteit der Wijsbegeerte en Technische Maatschappijwetenschappen van de Technische
Universiteit Delft op 6 juni 1990.
- [11] Goebertus, H.J.,
Telecommunicatie, i.h.b. de Industriële Aspecten,
Collegedictaat 174, oktober 1987,
TU Delft, Faculteit der Elektrotechniek,
Vakgroep Telecommunicatie- en Verkeersbegeleidingssystemen.
- [12] Katz, James E.,
"Caller-ID, privacy and social processes",
Telecommunications policy, October 1990, pp. 372-411.
- [13] Beukers, R.A.,
Elektronische Automatische Telefonie,
Collegedictaat 1100,
TU Delft, Faculteit der Elektrotechniek,
Vakgroep Telecommunicatie- en Verkeersbegeleidingssystemen.
- [14] Cambré, E. and Smouts, M.,
"CCITT No 7 Network as the Basis for Advanced Public Network Services",
Electrical Communication, Volume 63, No. 4, 1989.
- [15] Alvarez Mazo, L., Larrocha, R. and Martin, M.,
"General Characteristics of Intelligent Networks",
Electrical Communication, Volume 63, No. 4, 1989, pp. 314-320.
- [16] Kegel, A., Arnbak, J.C. e.a.,
Communicatie-systemen b.o.,
Collegedictaat 178, januari 1991,
TU Delft, Faculteit der Elektrotechniek,
Vakgroep Telecommunicatie- en Verkeersbegeleidingssystemen.
- [17] Tanenbaum, A.S.,
Computer Networks, second edition,
1988, Prentice-Hall, Inc., Englewood Cliffs.
ISBN 0-13-166836-6.
- [18] Peter Bocker,
ISDN: Concepten, methoden en systemen,
Kluwer Technische Boeken B.V., Deventer.

- [19] Modarressi, A.R., Skoog, R.A.,
"Signalling System No. 7: A Tutorial",
IEEE Communications Magazine, July 1990, pp. 19-35.
- [20] Richards, Philip,
"Rapid service delivery and customization in a developing network infrastructure",
Telecommunications, April 1991, pp. 33-36.
- [21] Ballard, M., Issenmann, E., Moya Sanchez, M.,
"Cellular Mobile Radio as an Intelligent Network Application",
Electrical Communication, Volume 63, No. 4, 1989, pp. 389-399.
- [22] Moret EDP Audit,
Automatisering onder controle, Edp-auditing als volwassen beroep,
1989 Kluwer Bedrijfswetenschappen,
ISBN 90-267-1339-8.
- [23] Kuitenbrouwer, F.,
"Nieuwe diensten en privacybescherming",
Computerrecht 1989/1, pag. 17-20.
- [24] Bemelmans, Th.M.A., Pool, J.A. van der, Zwaneveld, N.J.M., red.,
Poly-Automatiserings Zakboekje, 2e editie,
1988 Koninklijke PBNA BV, Arnhem,
ISBN 90-6228-086-2 geb.
- [25] Gebhardt, H.P.,
"La protection des données nominatives dans les telecommunications",
Le Communicateur, no. 9, avril 1990, p. 99-109.
- [26] Nugter, A.C.M.,
"Privacybescherming en 'Caller ID'",
Ars aequi: juridisch studentenblad 39 (1990) 12 (december), pag. 945-948.
- [27] Berkvens, J.M.A.,
"Privacybescherming COM(90)314 FINAL - SYN 287 en 288, Brussel, 13 september 1990",
Computerrecht 1990/5, pag. 263-272.
- [28] "PTT zet alle gedraaide nummers op nota: Stiekem bellen is afgelopen",
De Telegraaf, 3 augustus 1991, pag. T5.
- [29] Jole, Francisco,
"Dreigende vooruitgang: het superieure telefoonnet en de gevaren",
De Tijd, 26 januari 1990, pag. 26-29.

[30] "Privacy een flop bij autotelefoon",
Rotterdams Dagblad, 26 juni 1991.

[31] Berkvens, J.M.A., Hoeken, H. van,
Telecommunicatie in Nederland: juridische aspecten,
1986 Uitgeverij Kluwer B.V., Deventer,
ISBN 90-267-1135-2.

Appendix A: Bepalingen beveiliging en geheimhouding inzake telecommunicatie

Beveiliging en geheimhouding in verband met telegrafie en telefonie zijn niet eenduidig geregeld [31]. Telegraaf, telefoon, telex en datanet kennen verschillende regelingen voor geheimhouding en beveiliging. Zie tabel A-1.

In de Telegraafbeschikking wordt veel aandacht besteed aan het gebruiken van codes, terwijl in de datanetvoorwaarden de gebruiker 'alle maatregelen mag treffen' noodzakelijk voor 'veilige overeenkomst' van gegevens. De PTT heeft bij DN-1 (Datanet 1) een inspanningsverplichting met betrekking tot geheimhouding. Het Wetboek van Strafrecht kent een aantal strafbepalingen voor inbreuken op de telegrafie en telefonie, niet echter voor telex- en datanetinbreuken anders dan vernieling waarvoor het Wetboek van Strafrecht een speciale bepaling kent. Op grond van de Wet op de Telecommunicatievoorzieningen is de PTT verplicht de in de Algemene Richtlijnen opgenomen bepalingen op te volgen. Het wetboek van strafrecht kent een verzameling afzonderlijke bepalingen voor het af luisteren van gesprekken met behulp van apparatuur. In algemene voorwaarden zijn aansprakelijkheidsbeperkingen te vinden en verboden tot hinder.

<i>Regeling</i>	<i>Artikel</i>	<i>Inhoud</i>	<i>Doel</i>
Grondwet	13	telefoon- en telegraafgeheim	tfn, tgf, tlx, DN-1
Wetboek van Strafrecht	351	vernieling	tfn, tgf, tlx, DN-1
	374	telegramgeheim	tgf
	374 bis	telefoon af luisteren	tfn
	375	medeplichtigheid ambtenaren	tgf,tfn
	139c	af luisteren gesprekken	tfn
	139d	af luisteren gesprekken	tfn
	139e	af luisteren gesprekken	tfn
	272	geheimhoudingsplicht	algemeen

<i>Regeling</i>	<i>Artikel</i>	<i>Inhoud</i>	<i>Doel</i>
WTV	8	beveiliging geheimhouding bescherming persoonlijke levenssfeer	algemeen
AMvB RTR	16.1	veiligheid Staat	tfn
	23.1, 2	geheimhouding	tfn
TGB	3	geheimhouding	tgf
DN-1	3	geheimhouding	DN-1
Alg. VTA	8	verbod hinder	tfn
Voorw.	10.1, 2	beperking aansprakelijkheid	tfn
	12.1	beperking aansprakelijkheid	tfn
TGF	3.2, 4	geheimtaal	tgf
VTXA	7.1	verbod hinder	tlx
	10.1, 2	beperking aansprakelijkheid	tlx
AV-DN-1	5	toegang personeel	DN-1
	9	verbod hinder	DN-1
	12	beperking aansprakelijkheid	DN-1
	14	encryption	DN-1

Tabel A-1: Bepalingen beveiliging en geheimhouding inzake telecommunicatie in Nederland

tfn: telefoon WTV: Wet op de Telecommunicatievoorzieningen VTA: Voorwaarden telefoonaansluitingen
 tgf: telegraaf TLB: Telexbesluit VTXA: Voorwaarden telex-aansluitingen
 tlx: telex RTR: Rijkstelefoonreglement AV-DN-1: Voorwaarden aansluiting Datanet 1
 TGB: Telegraafbesluit
 DN-1: Datanetbesluit

Appendix B: Entiteiten bij informationele privacy

Bij informationele privacy zijn drie entiteiten te onderkennen die met elkaar in relatie staan, te weten:

- het individu waarop de gegevens betrekking hebben,
- de bestands- c.q. registratiehouder,
- derden die van, bij de registratiehouder geregistreerde, persoonsgegevens gebruik maken.

Zo kunnen, in de relatie individu versus registratiehouder, gegevens van één persoon bij meer dan één registratiehouder voorkomen en kan één registratiehouder op zijn beurt gegevens van meerdere personen beheren. Dit is schematisch weergegeven in figuur B-1.

Informationele privacy wordt in deze figuur gedefinieerd vanuit het IVU-principe (de drie hoofdfasen van het informatieverwerkend proces: Invoer, Verwerking, Uitvoer [22]) en vanuit twee invalshoeken, namelijk die vanuit het individu als gegevensbron en die vanuit de bestands-/registratiehouder als direct verantwoordelijke voor de privacy bescherming. Deze invalshoeken dient men als volgt te interpreteren:

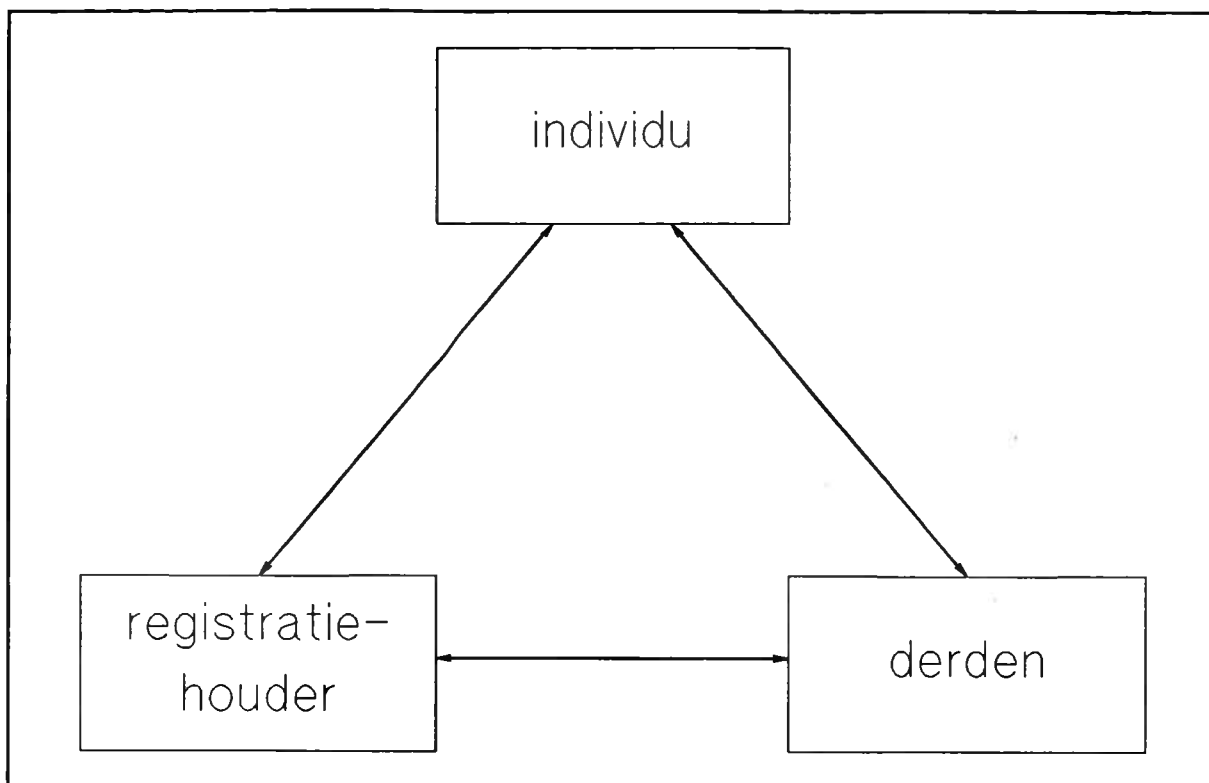
Vanuit het individu:

Informationele privacy is het recht op een juiste verzameling en bewerking, een juist gebruik en een veilige opslag van (vaak in vertrouwen, al dan niet verplicht afgestane) persoonsgegevens en op een controle daarvan.

Vanuit de bestands-/registratiehouder:

De garandering van informationele privacy voert tot de plicht om bovengenoemde informationele privacy te waarborgen.

Een en ander ontslaat de groep 'derden' uiteraard niet van de verplichting zorgvuldig met persoonsgegevens, verkregen van bestands-/registratiehouders, om te gaan. Indien derden



Figuur B-1: Entiteiten bij informationele privacy

gegevens, verkregen van bestands-/registratiehouders, opnemen in een eigen registratie, behoren zij op dat moment en voor die registratie uiteraard tot de entiteit bestands-/registratiehouder.

Op basis van een contract zal de registratiehouder een overeenkomst met de geregistreerde moeten sluiten om de informationele privacy te garanderen.

Appendix C: Besluit algemene richtlijnen telecommunicatie

16 december 1988/Nr. TP/10431 Hoofddirectie
Telecommunicatie en Post

De Minister van Verkeer en Waterstaat, Gelet op artikel 8 van de Wet op de telecommunicatievoorzieningen (Stb. 1988, 520);

Besluit:

Voor PTT Nederland NV de volgende algemene richtlijnen ten aanzien van de aan haar in artikel 3, derde lid, en artikel 4, eerste en tweede lid, van de wet op de telecommunicatie voorzieningen opgedragen verplichtingen terzake van de telecommunicatie-infrastructuur respectievelijk de verzorging van telecommunicatiediensten en de terbeschikkingstelling van het gebruik van vaste verbindingen:

(..)

§3 Geheimhouding

3.1 De houder van de concessie draagt er zorg voor, dat bij de bedrijfsvoering met betrekking tot de telecommunicatie-infrastructuur en de diensten het grondwettelijk telefoon- en telegraafgeheim wordt nageleefd.

3.2 De houder van de concessie draagt er zorg voor, dat bij de bedrijfsvoering met betrekking tot de telecommunicatie-infrastructuur en de diensten de wettelijke regelingen ter bescherming van de persoonlijke levenssfeer in acht worden genomen en is, indien dat voor de bescherming van de persoonlijke levenssfeer noodzakelijk blijkt, verplicht verdergaande waarborgen te stellen aangaande het door hem verzorgen en beheren van informatie omtrent de contractanten van een dienst

3.3 De houder van de concessie is verplicht in de arbeidsvoorwaarden voor zijn personeel bepalingen op te nemen ter bescherming van de persoonlijke levenssfeer van de gebruikers van de telecommunicatie-infrastructuur en de diensten, inclusief het geheimhouden van informatie over hun telecommunicatieverkeer. Voor zover derden zijn betrokken bij de uitvoering van activiteiten met betrekking tot de infrastructuur en de diensten, dient de houder van de concessie er voor zorg te dragen dat ten aanzien van die derden en hun personeel overeenkomstige bepalingen worden gesteld.

(..)

's-Gravenhage, 16 december 1988.

De Minister voornoemd,
N. Smit-Kroes.

Toelichting

(..)

Paragraaf 3 Geheimhouding

3.1 en 3.2 De houder van de concessie dient de telecommunicatie-infrastructuur naar de stand van de technische mogelijkheden onder afweging van de hiermee gepaard gaande kosten zo goed mogelijk te beveiligen tegen inbreuk door derden. Hierbij valt behalve aan bescherming tegen kennisneming door derden van de getransporteerde gegevens ook te denken aan een adequate bescherming en beveiliging tegen kennisneming door onbevoegden van gegevens omtrent de contractanten.

3.3 Uiteraard zullen naast de bedoelde bepalingen ook bepalingen worden opgenomen met betrekking tot de geheimhouding van bedrijfsgegevens van de houder van de concessie. Ten aanzien van personeel van derden zullen voorts maatregelen worden getroffen met betrekking tot een adequaat toezicht op de aanwezigheid (toegangscontrole etc.) en op de door hen verrichte activiteiten in de telecommunicatie-infrastructuur (voortdurend toezicht door personeel van de houder van de concessie), e.d.

(..)

Appendix D: COM(90) 314 final-SYN 288, Brussel, 13 september 1990

SYN 288

Voorstel voor een richtlijn van de Raad betreffende de bescherming van persoonsgebonden gegevens en van de persoonlijke levenssfeer in het kader van openbare digitale telecommunicatienetten, met name in het kader van het digitaal netwerk voor geïntegreerde diensten (ISDN) en van de openbare mobiele netwerken.

Artikel 1

1. De Lid-Staten, doen de nodige specifieke bepalingen in werking treden om de bescherming van persoonsgebonden gegevens en de persoonlijke levenssfeer in de telecommunicatiesector te waarborgen.
2. Deze richtlijn voorziet in de harmonisatie van bepalingen die nodig zijn om een gelijk beschermingsniveau van de persoonlijke levenssfeer in de Gemeenschap te waarborgen en om te voorzien in het vrije verkeer van telecommunicatiediensten en -apparatuur in en tussen de Lid-Staten.

Artikel 2

1. Onverminderd de algemene bepalingen van Richtlijn .../EEG betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens van de Raad is de onderhavige richtlijn van toepassing op het verzamelen, opslaan en behandelen van persoonsgebonden gegevens door telecommunicatieorganisaties in samenhang met de levering van openbare telecommunicatiediensten in openbare digitale communicatie-netwerken in de Gemeenschap, en met name over het digitale netwerk voor geïntegreerde diensten (ISDN) en over de openbare digitale mobiele netwerken.
2. Indien een Lid-Staat nog geen digitaal netwerk voor geïntegreerde diensten (ISDN) of openbare digitale mobiele netwerken heeft ingevoerd, worden de bepalingen van deze richtlijn uitgevoerd voor zover zij eveneens op diensten op basis van analoge netwerken van toepassing zijn.

Artikel 3

In de zin van deze richtlijn wordt verstaan onder:

1. 'persoonsgegevens'; iedere inlichting met betrekking tot een geïdentificeerd of identificeerbaar persoon.
2. 'telecommunicatieorganisatie'; een openbare of particuliere instelling waaraan een Lid-Staat bijzondere of exclusieve rechten verleent om in een openbaar telecommunicatienet en, in voorkomend geval, in openbare telecommunicatiediensten te voorzien.
3. 'openbaar telecommunicatienetwerk'; de openbare telecommunicatie-infrastructuur waarmee signalen tussen bepaalde eindpunten van het net langs draad, microgolf,

optische drager of andere elektromagnetische dragers kunnen worden overgedragen.

4. 'openbare telecommunicatiedienst'; een telecommunicatiedienst waarvan de levering door de Lid-Staten specifiek aan, met name, één of meer telecommunicatieorganisaties werd toevertrouwd.

Artikel 4

1. Verzameling, opslaan en behandeling van persoonsgebonden gegevens door een telecommunicatieorganisatie is alleen geoorloofd voor telecommunicatiedoelinden; en met name om verbindingen voor de transmissie van stem, gegevens of beelden tot stand te brengen, om rekeningen te maken, om telefoongidsen samen te stellen en voor andere rechtmatige bedrijfsdoelinden zoals opheffing van storingsen, voorkomen van misbruiken van de apparatuur van de telecommunicatieorganisatie, of registratie van binnenkomende oproepen in overeenstemming met artikel 13, lid 1.
2. De telecommunicatieorganisatie mag de gegevens niet gebruiken om elektronische profielen van de abonnees of om van afzonderlijke abonnees classificaties naar categorie te maken.

Artikel 5

1. Persoonsgebonden gegevens van de abonnee mogen worden samengebracht en opgeslagen voor zover dit noodzakelijk is om de overeenkomst met de telecommunicatieorganisatie te sluiten, uit te voeren, te wijzigen of te beëindigen. Na beëindiging van het contract dienen de gegevens te worden verwijderd tenzij en voor zolang deze moeten worden bewaard om klachten te behandelen, kosten terug te vorderen of aan andere verplichtingen te voldoen die, in overeenstemming met het Gemeenschapsrecht, door de Lid-Staat bij de wet zijn opgelegd.
2. De inhoud van de verzonden informatie mag na het eind van de transmissie niet door de telecommunicatieorganisatie worden bewaard behalve op grond van verplichtingen die, in overeenstemming met het Gemeenschapsrecht, door de Lid-Staat bij de wet zijn opgelegd.

Artikel 6

De abonnee heeft het recht

1. met redelijke tussenpozen en zonder buitensporige wachttijden of kosten zich ervan te vergewissen of persoonsgebonden gegevens van hem/haar zijn opgeslagen en te eisen dat deze gegevens hem/haar in een begrijpelijke vorm worden medegedeeld,

2. te eisen dat deze gegevens naargelang van het geval worden verbeterd of gewijzigd indien deze werden behandeld in strijd met de voorschriften die, in overeenstemming met het Gemeenschapsrecht, door de lidstaten bij wet zijn opgelegd.

Artikel 7

1. In beginsel dienen alle persoonsgebonden gegevens die op telecommunicatienetwerken en -diensten betrekking hebben, vertrouwelijk te blijven.
2. De persoonsgebonden gegevens mogen buiten de dienst of het netwerk van de telecommunicatieorganisaties niet worden bekendgemaakt zonder dat dit bij de wet uitdrukkelijk is toegestaan of zonder voorafgaande schriftelijke toestemming van de abonnee. Een abonnee zal alleen dan worden geacht deze toestemming te hebben gegeven indien dit in de vorm van een specifiek antwoord op verzoek van de telecommunicatieorganisatie is geschied. Zonder de voorafgaande schriftelijke toestemming van de abonnee mogen deze persoonsgebonden gegevens niet worden bekendgemaakt aan personen binnen de telecommunicatieorganisatie die niet bij de geleverde diensten betrokken zijn.
3. De telecommunicatieorganisatie mag het leveren van haar diensten niet van een dergelijke toestemming afhankelijk stellen.

Artikel 8

1. De telecommunicatieorganisatie dient te voorzien in een doeltreffende, met de stand van de techniek overeenstemmende beveiliging van de persoonsgebonden gegevens tegen ongeoorloofde toegang of gebruik.
2. Indien een bijzonder risico bestaat dat de beveiliging van het netwerk wordt doorbroken, bijvoorbeeld op het gebied van de mobiele radiotelefonie, dient de telecommunicatieorganisatie de abonnee van deze risico's op de hoogte te stellen en hem een 'punt-tot-punt'-versleuteling aan te bieden.

Artikel 9

1. Rekeninggegevens bestaande uit het telefoonnummer of de identificatie van het abonneetoestel, het adres van de abonnee en het toesteltype, het totaal aantal voor de berekeningsperiode aan te rekenen eenheden, het opgeroepen telefoonnummer, het type, en de duur van de gedane oproepen en/of de verzonden hoeveelheid gegevens en andere, voor de factuur noodzakelijke inlichtingen zoals vooruitbetaling, betaling in termijnen, afsluitingen en aanmaningen mogen worden opgeslagen en behandeld.
2. Deze algemene opslag van de rekeninggegevens wordt toegestaan tot het einde van de wettelijke termijn waarin de factuur kan worden betwist.

Artikel 10

1. Verkeersgegevens die de voor het tot stand brengen van de oproep, voor het opstellen van de rekeningen of voor andere bedrijfsdoeleinden noodzakelijke persoonsgebonden gegevens bevatten, zoals het telefoonnummer van de

oproepende en opgeroepen abonnee, de aanvangs- en eindtijd van iedere oproep, en de door de abonnee gebruikte communicatiediensten, mogen worden verzameld, opgeslagen en behandeld voor zover dat voor de levering van de verlangde telecommunicatiedienst noodzakelijk is.

2. De verkeersgegevens die in de schakelcentrales van de telecommunicatieorganisaties worden opgeslagen, moeten na beëindiging van de oproep worden verwijderd, tenzij anoniem worden gemaakt of voor het opmaken van de rekeningen of andere rechtmatige doeleinden als bedoeld in artikel 4 noodzakelijk zijn.

Artikel 11

Op verzoek van de abonnee mag een gedetailleerde opgave van de oproepen worden afgegeven. Deze opgave bevat onder meer de telefoonnummers van de opgeroepen abonnees zonder de laatste vier cijfers van die nummers.

Artikel 12

1. Met betrekking tot de gesprekken tussen abonnees die met een digitale centrale zijn verbonden, dient de oproepende abonnee in staat te zijn om voor iedere oproep afzonderlijk te verhinderen dat de identificatie van zijn/haar telefoonnummer op het gegevensscherm van het toestel van de opgeroepen abonnee verschijnt of in het geheugen van dat toestel wordt geregistreerd. De transmissie van het telefoonnummer mag op verzoek van de oproepende abonnee door de telecommunicatieorganisatie eveneens blijvend worden verhinderd.
2. De opgeroepen abonnee kan erom verzoeken dat de identificatie van alle inkomende oproepen blijvend worden verhinderd; hij/zij moet eveneens in staat zijn om naargelang van het geval het gegevensscherm van zijn/haar toestel uit te schakelen, of de registratie in het geheugen van het toestel te onderbreken ten einde de identificatie van inkomende oproepen onmogelijk te maken. De opgeroepen abonnee moet in staat zijn alleen die inkomende oproepen te aanvaarden waarvan het oproepende abonneenummer geïdentificeerd is.
3. Met betrekking tot de communicatie tussen abonnees die met digitale centrales zijn verbonden en een abonnee die met een analoge centrale is verbonden, dient deze laatste op de hoogte te worden gebracht van de identificering van zijn/haar telefoonnummer en dient hij/zij de mogelijkheid te hebben deze voorziening op verzoek blijvend te doen uitschakelen. Deze abonnee moet die identificering ook naargelang van de oproep kunnen uitschakelen.

Artikel 13

1. Gedurende een beperkte periode mag de telecommunicatieorganisatie de uitschakeling van deze identificatie van het oproepende nummer blokkeren.
 - a. op verzoek van een abonnee die om opsporing van kwaadwillige oproepen verzoekt. In dat geval dienen de gegevens met de identificatie van de oproepende abonnees door de telecommunicatieorganisatie te worden opgeslagen

en op verzoek ter beschikking te worden gesteld van de autoriteit die in de betrokken Lid-Staat met de preventie of de vervolging van misdrijven is belast;

b. op specifiek bevel van de rechter ter voorkoming of vervolging van ernstige misdrijven.

2. Op verzoek dient een blijvende blokkering van deze voorziening ter beschikking te worden gesteld van

a. door de Lid-Staat erkende organisaties die noodoproepen beantwoorden en behandelen en

b. door de Lid-Staat erkende of geëxploiteerde brandweerdiensten.

3. De telecommunicatieorganisaties dienen de nodige maatregelen te treffen om ervoor te zorgen dat deze blokkering zowel op nationaal als op communautair niveau werkt.

Artikel 14

1. Oproepen mogen door de opgeroepen abonnee slechts naar een derde worden omgeleid indien deze derde daarmee heeft ingestemd; de derde kan het omleiden beperken tot oproepen waarvan het nummer van de oproepende abonnee is geïdentificeerd; de derde moet door middel van een specifiek signaal van het bericht dat de oproep werd omgeschakeld, op de hoogte worden gebracht.

2. De oproepende abonnee moet tijdens het tot stand brengen van de verbinding automatisch ervan op de hoogte worden gebracht dat de oproep naar een derde wordt doorgeschakeld.

Artikel 15

1. Indien derden toegang hebben tot de inhoud van telefoongesprekken met gebruikmaking van technische voorzieningen zoals luidsprekers of andere uitrustingen op het toestel, of deze gesprekken voor eigen gebruik of gebruik door derden op band worden bewaard, dienen voorzieningen te worden getroffen om, alvorens het verspreiden of opslaan een aanvang neemt en tijdens de volledige duur ervan, de betrokken partijen door middel van daartoe geëigende procedures van deze verbreiding of opslag op de hoogte te brengen.

2. Lid 1 is niet van toepassing in de gevallen bedoeld in artikel 13, lid 1.

Artikel 16

1. De telecommunicatieorganisatie dient ervoor te zorgen dat het telefoonnummer en andere persoonsgebonden gegevens van de abonnee met name met betrekking tot de hoeveelheid en de aard van zijn/haar bestelling bij gebruik van de tele-winkel-dienst of met betrekking tot de door middel van een videotex-dienst aangevraagde informatie, slechts wordt opgeslagen voor zover dit strikt noodzakelijk is om de dienst te leveren en door de dienstverlener uitsluitend wordt gebruikt voor door deze abonnee toegestane doeleinden.

2. Onverminderd artikel 20 mag de dienstverlener geen elektronische profielen van de abonnees of classificaties

per categorie van afzonderlijke abonnees maken zonder hun voorafgaande schriftelijke toestemming.

Artikel 17

1. Abonnees die ongewenste oproepen ontvangen waarin reclame voor een levering wordt gemaakt, of waarin levering van goederen en diensten wordt aangeboden, kunnen de telecommunicatieorganisaties die dergelijke berichten doorzendt, ervan in kennis stellen dat zij die oproepen niet wensen te ontvangen.

2. De telecommunicatieorganisatie moet alle noodzakelijke maatregelen treffen om aan de transmissie van dergelijke berichten naar de betrokken abonnees een einde te maken. Voorts dient de telecommunicatieorganisatie een lijst van kennisgevingen bij te houden in een door de toezichthoudende autoriteit voorgeschreven en in een door deze laatste inspecteerbare ten einde dergelijke oproepen voortaan te beletten.

Artikel 18

1. Bij de tenuitvoerlegging van de bepalingen van deze richtlijn dienen de Lid-Staten met inachtnaam van de leden 2 en 3 van dit artikel ervoor zorg te dragen dat aan het eindtoestel of aan andere telecommunicatieapparatuur geen dwingende eisen voor specifieke technische voorzieningen worden gesteld waardoor het in de handel brengen van apparatuur en het vrij verkeer van deze apparatuur in en tussen de Lid-Staten kan worden belemmerd.

2. Wanneer bepalingen slechts kunnen worden uitgevoerd door specifieke technische kenmerken voor het schrijven, dienen de Lid-Staten de Commissie daarvan op de hoogte te brengen volgens de procedures van Richtlijn 83/189/EEG van de Raad waarin in een informatieprocedure op het gebied van technische normen en voorschriften is voorzien.

3. In voorkomend geval dient de Commissie ervoor te zorgen dat gemeenschappelijke Europese normen worden opgesteld voor de implementatie van speciale technische kenmerken. In overeenstemming met de richtlijn .../EEG van de raad (betreffende de onderlinge aanpassing van de wetgevingen der Lid-Staten inzake telecommunicatie-eindapparatuur met inbegrip van de wederzijdse erkenning van de conformiteit) en met Beschikking 87/95/EEG van de Raad van 22 december 1986 betreffende normalisatie op het gebied van informatietechnologie en telecommunicatie.

Artikel 19

1. De bepalingen van deze richtlijn die betrekking hebben op de telefoondienst zijn toepasselijk op andere openbare digitale communicatie-diensten van toepassing voor zover deze diensten een vergelijkbaar risico voor de persoonlijke levenssfeer van de gebruiker vertegenwoordigen.

2. De voor de toepassing van lid 1, noodzakelijke maatregelen worden door de Commissie vastgesteld nadat het in artikel 22 bedoelde comité volgens de in artikel 23 vastgelegde procedure werd geraadpleegd.

Artikel 20

Indien het voor de volledige verwezenlijking van de doelstellingen van deze richtlijn nodig is de bepalingen ervan ook op andere dienstverleners dan de telecommunicatieorganisaties toe te passen, kan de Commissie de nodige maatregelen vaststellen om deze richtlijn voor die dienstverleners te doen gelden nadat het in artikel 22 bedoelde comité volgens de procedure van artikel 23 werd geraadpleegd.

Artikel 21

De nadere regels voor de toepassing van deze richtlijn en de wijzigingen om deze richtlijn aan nieuwe technische ontwikkelingen aan te passen worden door de Commissie vastgesteld nadat het in artikel 22 bedoelde comité volgens de procedure van artikel 23 werd geraadpleegd.

Artikel 22

1. De bij artikel 27 van de Richtlijn .../EEG van de raad (betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens), ingestelde Groep voor de bescherming van persoonsgegevens vervult de taken waarin artikel 28 van genoemde richtlijn voorziet, eveneens voor de maatregelen ter bescherming van persoonsgebonden gegevens die tot de werkingssfeer van de onderhavige richtlijn behoren.
2. De Groep krijgt voor de doeleinden van de onderhavige richtlijn een specifieke samenstelling.

Artikel 23

1. De procedure van artikel 30 van de Richtlijn .../EEG van de Raad (betreffende de bescherming van personen in verband met de behandeling van persoonsgegevens), is van toepassing.
2. Het Comité dat in het kader van de in lid 1 bedoelde procedure is ingesteld, krijgt voor de doeleinden van de onderhavige richtlijn een specifieke samenstelling.

Artikel 24

1. De Lid-Staten doen uiterlijk op 1 januari 1993 de wettelijke en bestuursrechtelijke bepalingen in werking treden die noodzakelijk zijn om aan deze richtlijn te voldoen. In de overeenkomstig de eerste alinea vastgestelde bepalingen wordt uitdrukkelijk naar deze richtlijn verwezen.
2. De Lid-Staten delen de Commissie de tekst mee van de nationaalrechtelijke bepalingen die zij op het door deze richtlijn bestreken gebied vaststellen.

Artikel 25

Deze richtlijn is gericht tot de Lid-Staten.

Appendix E: Enkele actuele krantenknipsels

Rotterdams Dagblad
28 juni 1991

PTT zwicht voor privacy

Den Haag - Vanaf maandag kan niemand meer via de zogeheten Telegids achterhalen welke naam en welk adres bij een bepaald telefoonnummer horen. De PTT heeft de mogelijkheid stopgezet in verband met de bescherming van de privacy. Of de maatregel tijdelijk is en of de mogelijkheid later weer wordt ingevoerd met de beschermende maatregelen, weet de PTT nog niet. Vanaf begin 1990 was het mogelijk via Videotex het elektronische gegevensbestand van 008 op te roepen. Door een telefoonnummer in te toetsen kon je zien van wie een bepaald nummer is.

de Volkskrant
6 augustus 1991

Bedreiging privacy met Telegids blijft mogelijk ondanks beperking zoekmethoden door PTT

PTT Telecom heeft zijn openbare 008-databank, Telegids, gekortwiekt. Tot voor kort was het via Telegids mogelijk om aan de hand van een telefoonnummer de bijbehorende naam en het adres op te sporen. „In het belang van de bescherming van de persoonlijke levenssfeer” is een einde gemaakt aan deze zoekmogelijkheid.

Met een personal computer kan voor 37 cent per minuut in Telegids worden gekeken. Ondanks de afschaffing van de privacy-bedreigende zoekmethode blijft Telegids een snellere en ruimere service dan het papieren telefoonboek en de menselijke 008-dienst. In Telegids kan nog steeds worden gezocht op naam en woonplaats en op adres. Het zoeken op telefoonnummer maakte het cirkeltje rond: een naam leverde een adres op, het adres leidde soms tot meerdere nummers en die nummers legden in dat geval vaak connecties met andere personen en bedrijven bloot. Het kan niet worden verheeld dat uitgerekend journalisten het instrument konden waarderen.

Ook was het zoeken op nummer voor sommige bedrijven een discrete manier om te controleren of een beller geen valse naam had opgegeven.

Een andere toepassing van Telegids was *direct marketing*: voor een verhuisbedrijf bijvoorbeeld kunnen naam en adres van particulieren die hun huis in de krant te koop zetten, heel waardevol zijn.

Er is weinig fantasie voor nodig om te bedenken hoe het systeem kon worden misbruikt voor het aantasten van de privacy: telefoonterreur kan zich uitbreiden tot terreur aan de deur.

De alleenstaande die per advertentie (mét telefoonnummer) voor de maand september een reisgenoot zoekt, kan wel eens het slachtoffer worden van een *high tech* inbreker. PTT Telecom zegt in een mededeling aan de Telegids-gebruikers dat het zoeken op nummer „op deze wijze niet langer mogelijk” gemaakt kan worden.

In de woorden „op deze wijze” schuilt het addertje.

Bedrijven kunnen namelijk de gegevens uit het telefoonboek in digitale vorm gewoon bij PTT Telecom kopen en in hun eigen computer zetten.

Een klein computerprogramma heropent vervolgens de mogelijkheid om op nummer te zoeken.

Ook de kwaadwillende gecomputeriseerde particulier hoeft niet onthand te zijn. Met een scanner kunnen delen van het telefoonboek kosteloos naar een personal computer worden overgeheveld. Klaar voor misbruik.

(John Schoonbrood)

computable
17 mei 1991

Elektronisch bestellen heeft weinig toekomst
Persoonsgegevens kunnen probleem worden

DEN HAAG - Het kopen per computer komt zeer langzaam van de grond. Het elektronisch bestellen van goederen door consumenten zal voorlopig nog een marginaal verschijnsel blijven. Het Economisch Instituut voor het Midden- en kleinbedrijf (EIM) noemt het elektronisch winkelen "op korte termijn geen reële optie".

van onze CORRESPONDENT

Dat blijkt uit het rapport 'Nederlandse postorderbedrijven in Europees perspectief'. Op het gebied van elektronisch berichtenverkeer voor particulieren loopt Frankrijk voorop, omdat men in dit land beschikt over Minitel. In andere Europese landen, waaronder Nederland, zijn wel experimenten gedaan met soortgelijke systemen, maar hiervan is nooit op grote schaal gebruik gemaakt.

Met betrekking tot de informatietechnologie zullen maatregelen om te komen tot gestandaardiseerde internationale communicatie- en informatienetwerken voor postorderbedrijven in het algemeen gunstig zijn. Allereerst valt te denken aan een betere beheersing van de goederenstroom. Door directe verbindingen tussen orderontvangst en magazijnen in verschillende landen kunnen orders veel sneller worden uitgevoerd. Bovendien is er minder kans op fouten. Ook kunnen klanten beter worden geholpen, omdat informatie over bijvoorbeeld levertijden veelal sneller beschikbaar zal zijn. Verder zullen klanten wellicht ook via koppeling van videotextdiensten in verschillende landen zelf aankopen kunnen verrichten, zoals dat nu al mogelijk is voor Belgen via videotex.

De postorderbedrijven hebben uitgebreide databases met gegevens over hun klanten. Niet onbelangrijk voor hen is de Europese ontwerpverplichting Gegevensbescherming, die op 1 januari 1993 in werking moet treden. Hierdoor zullen in alle EG-landen dezelfde regels gaan gelden omtrent wie welke gegevens, en onder welke voorwaarden, in databases mag aanhouden.

De voorgestelde bepalingen in de richtlijn zijn aanzienlijk strikter dan de bepalingen zoals die nu gelden ten aanzien van persoonsregistratie in Nederland, omdat individueel toestemming moet worden gevraagd of gegevens in de database mogen worden opgenomen. Bovendien moeten bedrijven kunnen aantonen dat er een wettelijke basis is voor registratie van persoonsgegevens.

Persbericht PTT Telecom 42/1991

PTT Telecom gaat specificatie gesprekskosten op telefoonnota voorbereiden.

PTT Telecom begint binnenkort op grote schaal met het aanpassen van de telefooncentrales om specificatie van de gesprekskosten op de telefoonnota mogelijk te maken. Voor 1 januari 1994 moet iedere aangesloten klant in Nederland voor het eerst een gespecificeerde nota hebben ontvangen, mits die klant is aangesloten op een computergestuurde telefooncentrale. Op die datum is circa 85 procent van de klanten aangesloten op een dergelijk type centrale en een jaar later is dat 100 procent.

Jaarlijks stuurt PTT Telecom bijna 40 miljoen telefoonnota's aan zo'n 6 miljoen aangesloten klanten (die gezamenlijk beschikken over 7 miljoen aansluitingen). Tot nu toe bevatte zo'n nota slechts de abonnementskosten en het totaal van de gesprekskosten, met daarnaast eventueel de huur van apparatuur. Straks zullen -gratis- op de nota een aantal categorieën van gesprekken worden vermeld, zoals lokale en interlokale gesprekken, internationale gesprekken, 06-, autotelefoon- en semafoongesprekken en kosten voor zogenoemde sterendiensten (bijvoorbeeld de dienst direct doorschakelen). Op zijn verzoek kan de klant een volledige specificatie ontvangen van alle van zijn aansluiting gevoerde gesprekken of voor één of meer van de genoemde categorieën. Dat zal de klant circa 5 cent per gespecificeerd gesprek gaan kosten.

De ombouwoperatie van de telefooncentrales voorziet erin dat deze centrales naast omvangrijke schakeltaken ook een compleet administratief proces moeten aankunnen. Om de gigantische gegevensstroom (nu gemiddeld ruim 21 miljoen gesprekken per dag) administratief te kunnen verwerken heeft PTT Telecom onlangs een contract gesloten met Tandem Computers BV voor de levering van computerapparatuur die hiervoor geschikt is, de allernieuwste NonStop systemen: Cyclone en CLX 800.

De benodigde programmatuur voor deze computers wordt geleverd door GTE Data Service Inc., een dochter van het Amerikaanse telecommunicatiebedrijf GTE. GTE zal haar computerprogramma Universal Measurement Service (UMS), dat in haar eigen verzorgingsgebieden in de Verenigde Staten van Amerika al jaren wordt gebruikt, tijdig aanpassen voor gebruik door PTT Telecom.

Lijst van afkortingen

ACM	Adress Complete Message
ALERT	Alerting
ANS	Answer
BS	Base Station
BSC	Base Station Controller
BST	Base Station Transmitter
CCITT	Comité Consultatif International de Télégraphie et Téléphonie
CCSS 7	Common Channel Signalling System No. 7
CLIR	Calling Line Identity Restriction
CNIL	Commission Nationale de l'Informatique et des Libertés
CONN	Connect
CT	Cordless Telephone
DGT	Direction Générale des Telecommunications
DUP	Data User Part
ESP	Extern Service Point
FN	Feature Node
GSM	Group Special Mobile
HLR	Home Location Register
IAM	Initial Address Message
IBCN	Integrated Broadband Communication Network
IDN	Integrated Digital Network
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
ISDN-UP	ISDN-User Part
ISO	International Standards Organisation
IP	Intelligent Peripheral
LU-Request	Location Updating-Request
MCC	Mobile Country Code
MNC	Mobile Network Code
MRUP	Mobile Radio User Part
MSC	Mobile Switching Centre
MS	Message Switching
MS	Mobiel Station
MSIN	Mobile Subscriber Identity Number
MSRN	Mobile Subscriber Roaming Number
MTP	Message Transfer Part
OMAP	Operations Maintenance and Administration Part
ONA	Open Network Architecture
OSI-model	Open System Interconnection-model
PCN	Personal Communications Network
PLMN	Public Land Mobile Network
SAM	Subsequent Address Message
SCP	Service Control Point

SI	Service Interface
SIB	Service Independent Building Block
SP	Signalling Point
SPC	Stored Program Control
SLI	Service Logic Interpreter
SLP	Service Logic Program
SMS	Service Maintenance System
SSP	Service Switching Points
STP	Signal Transfer Point
TCAP	Transaction Capabilities Application Part
TMSI	Temporary Mobile Subscriber Identity
TUP	Telephone User Part
UP	User Part
VLR	Visited Location Register
WPR	Wet Persoonsregistraties
WTV	Wet op de Telecommunicatievoorzieningen