# Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie

Koops, E.J.; Smits, J.M.

*Publication date:*
2014

*Document Version*
Publisher's PDF, also known as Version of record

# Verkeersgegevens en artikel 13 Grondwet

## Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie

*Bert-Jaap Koops en Jan Smits*

*m.m.v. Frank van der Kroon*

# Colofon

## Verkeersgegevens en artikel 13 Grondwet

**Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie**

**Auteurs**
prof.dr. B.J. Koops
prof.dr.mr. J.M. Smits

met medewerking van ir. F.J. van der Kroon MBA

**Opdrachtgever**
Deze studie is geschreven in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

ISBN: 9789462400900

Dit boek is een uitgave van:
Wolf Legal Publishers (WLP)
Postbus 313
5060 AH Oisterwijk
info@wolfpublishers.nl
www.wolfpublishers.com

# Inhoudsopgave

# Afkortingen

| | |
|---|---|
| ACR/NEMA | American College of Radiology - National Electrical Manufacturers Association |
| ATM | Asynchronous Transfer Mode |
| BSC | Base Station Controller, |
| BSN | BurgerServiceNummer |
| BTS | Base Transceiver Station (Basis-zend/ontvangststation waarmee de GSM rechtstreeks communiceert) |
| BVerfG | Bundesverfassungsgericht [Duits federaal constitutioneel hof] |
| BZK | Binnenlandse Zaken en Koninkrijksrelaties |
| CLI | Calling Line Identification / Nummerherkenning |
| DICOM | Digital Imaging and Communications in Medicine |
| DNS | Domain Name System |
| DTMF | Dual Tone Multi-Frequency |
| EDI | Electronic Data Interchange |
| EHRM | Europees Hof voor de Rechten van de Mens |
| EU | Europese Unie |
| EVRM | Europees Verdrag van de Rechten van de Mens |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile telecommunications |
| Gw | Grondwet |
| HLR | Home Location Register |
| HR | Hoge Raad |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| IANA | Internet Assigned Numbers Authority |
| IAX | Inter-Asterisk eXchange protocol |
| ICT | informatie- en communicatietechnologie |
| IETF | Internet Engineering Task Force |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISP | Internet Service Provider |
| IVR | Interactive Voice Response |
| MAC | Media Access Control |
| MQTT | Message Queue Telemetry Transport |
| MSC | Mobile Switching Centre |
| MSN | Microsoft Service Network |

| | |
|---|---|
| NAW | naam, adres, woonplaats |
| NJ | Nederlandse Jurisprudentie |
| OFTP | Odette File Transfer Protocol |
| ONP | Open Network Provision |
| OSI | Open Systems Interconnection |
| POTS | Plain Old Telephone System |
| PTT | Posterijen, Telegrafie en Telefonie |
| Rb. | Rechtbank |
| RFC | Request for Comment |
| RFID | Radio Frequency IDentification |
| RSS | Really Simple Syndication |
| SIP | Session Initiation Protocol |
| SMS | Short Message Service |
| SMSc | Short Message Service centre |
| SMTP | Simple Mail Transfer Protocol |
| Sr | Wetboek van Strafrecht |
| SS7 | Common Channel Signalling System #7 |
| Stb. | Staatsblad |
| Sv | Wetboek van Strafvordering |
| TCP | Traffic Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| VoIP | Voice over Internet Protocol [spraaktelefonie via Internet] |
| VS | Verenigde Staten |
| Wbp | Wet bescherming persoonsgegevens |
| Wiv 2002 | Wet op de inlichtingen- en veiligheidsdiensten 2002 |
| WODC | Wetenschappelijk Onderzoek- en Documentatiecentrum |
| WPolG | Wet Politiegegevens |
| XML | eXtended Markup Language |
| XMPP | eXtensible Messaging and Presence Protocol |

# Voorwoord

*Grondwet voor het Koninkrijk der Nederlanden*

*Artikel13*
*1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.*
*2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.*

De wetgever beoogt om artikel 13 Grondwet (Gw) – het huidige brief-, telefoon- en telegraafgeheim – te actualiseren.[1] In oktober 2012 is een concept-wetsvoorstel in consultatie gegeven.[2] In dat wetsvoorstel worden verkeersgegevens – gegevens als wie met wie wanneer belt of mailt – uitgesloten van bescherming onder artikel 13, omdat zij niet de inhoud van communicatie betreffen. Wanneer verkeersgegevens echter wel geheel of ten dele mede op de inhoud van de communicatie betrekking hebben, zouden zij als inhoud moeten worden behandeld. In de praktijk is het niet eenvoudig om te bepalen wanneer verkeersgegevens (mede) op inhoud betrekking hebben.

Daarom heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties opdracht gegeven een onderzoek uit te voeren naar de huidige betekenis en eventuele problemen bij de technische en juridische kwalificatie van verkeersgegevens in het licht van de bescherming van artikel 13 Gw. Het onderzoek bevat een technische en een juridische component. Het technische deel, uitgevoerd door Jan Smits met medewerking van Frank van der Kroon, is gericht op de technische kwalificatie van verkeersgegevens. Het juridische deel, uitgevoerd door Bert-Jaap Koops, concentreert zich op de juridische kwalificatie van verkeersgegevens.

Beide onderzoeken tezamen beogen een beeld op te leveren in hoeverre het vanuit technisch en juridisch opzicht mogelijk is verkeersgegevens in het grijze gebied tussen verkeersgegevens en inhoud van communicatie te kwalificeren in het licht van de herziening van artikel 13 Gw.

De studies zijn uitgevoerd van november 2012 tot februari 2013. In dit boek zijn de twee deelstudies gebundeld. Dit boek biedt daarmee een

---

1 Zie *Kamerstukken II* 2011/12, 31 570, nrs. 20-21. Over de (lange) voorgeschiedenis, zie Staatscommissie Grondwet 2010 en de bespreking in *Tijdschrift voor Constitutioneel Recht* 2011 nr. 2, met verwijzingen.

2 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, http://www.internetconsultatie.nl/briefentelecommunicatiegeheim (geraadpleegd 1 oktober 2013). Relevante onderdelen zijn opgenomen in de bijlage aan het eind van dit boek.

integrale reflectie op het onderscheid tussen verkeersgegevens en communicatie-inhoud in een sterk aan veranderingen onderhevig communicatielandschap. De visie die hierin wordt gepresenteerd op de betekenis en de (on) houdbaarheid van het onderscheid tussen verkeersgegevens en inhoud is niet alleen van belang voor de herziening van artikel 13 Gw, maar ook voor de verdere ontwikkeling van het straf(proces)recht en het bestuursrecht rond elektronische communicatie in de toekomst.

# Deel 1.
# Technische kwalificatie van verkeersgegevens in het licht van artikel 13 Grondwet

*Jan Smits*
*m.m.v. Frank van der Kroon*

# 1. Inleiding

In dit deel worden de resultaten beschreven van het technische deel van het onderzoek dat is uitgevoerd in het kader van het concept-wetsvoorstel ter aanpassing van artikel 13 Gw.[3] In dat wetsontwerp worden, in navolging van de commissie-Franken[4] en commissie-Thomassen,[5] verkeersgegevens als zodanig uitgesloten van de bescherming van artikel 13 Gw, aangezien zij geen inhoud van communicatie betreffen. Alleen voor zover verkeersgegevens raken aan de inhoud van communicatie, zouden ze beschermwaardig kunnen zijn onder artikel 13.

Tot nu toe wordt het brief-, telegraaf- en telefoongeheim in de Nederlandse Grondwet gewaarborgd in artikel 13. Telegrammen en brieven worden echter niet erg veel meer geschreven, en bellen doen we inmiddels in velerlei vormen, en die noemen we ook al lang niet altijd meer telefonie. Midden jaren tachtig tot aan eind jaren negentig was Nederland het land waar de semafoon het meest werd gebruikt. Een bijzonder technisch apparaatje waarmee heel korte berichtjes konden worden ontvangen, meestal niet meer dan *012-3456789 terugbellen.* Met de doorbraak naar het grote publiek van zowel de mobiele telefoon als Internet in het midden van de jaren negentig is enerzijds e-mail en anderzijds sms een steeds belangrijkere vorm van communicatie geworden. Tevens vertrouwen we niet langer meer op een gang naar de bibliotheek en/of de papieren encyclopedie om iets op te zoeken maar heeft een zoekvraag op Internet deze functie vrijwel geheel vervangen.

Sinds het begin van deze eeuw zien we allerlei vormen van communicatie en elektronische correspondentie opkomen die technologisch mogelijk worden gemaakt die echter (allang) niet meer onder de met techniek aangeduide definitie van het bestaande artikel 13 Gw vallen. Er bestaat echter geen grondwettelijke bescherming voor e-mail en andere vormen van elektronische communicatie zoals die voor brieven en andere poststukken wel geldt. Vandaar dat het voorstel is gedaan voor een wijziging van dit grondwetsartikel.

De opdracht betreft een onderzoek naar de huidige betekenis en eventuele problemen bij de kwalificatie van verkeersgegevens in het licht van de

---

3 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, http://www.internetconsultatie.nl/briefentelecommunicatiegeheim (geraadpleegd 1 oktober 2013).

4 Commissie Grondrechten in het digitale tijdperk 2000, *Kamerstukken II* 2000/01, 27 460, nr. 1, bijlage 1.

5 Staatscommissie Grondwet 2010, bijlage bij *Kamerstukken I* 2011/12, 31570, nr. A, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/11/15/rapport-staatscommissie-grondwet.html (geraadpleegd 1 oktober 2013).

bescherming van artikel 13 Grondwet. De technische en juridische deelstudies beogen samen een beeld op te leveren in hoeverre het eventuele uiteenlopen van de technologische en juridische kwalificatie van verkeersgegevens problematisch is in het licht van de herziening van artikel 13 Gw. De vraagstelling voor beide onderzoeken is: welke typen verkeersgegevens moeten juridisch beschermwaardig worden geacht onder artikel 13 Gw, gelet op de ratio en functie van artikel 13, en in hoeverre zijn deze typen juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit?

De deelvragen die daarbij vooral vanuit technologisch perspectief worden bezien, zijn de volgende:

1. Welke grijze gebieden bestaan er tussen verkeersgegevens en inhoud van communicatie?
2. Kunnen verkeersgegevens in de grijze gebieden worden geclassificeerd in een typologie van verschillende manieren waarop verkeersgegevens samenhangen met inhoud?

De nadruk ligt op de vraag onder welke omstandigheden verkeersgegevens zodanig verbonden zijn met inhoud van communicatie dat zij onder de reikwijdte van artikel 13 Gw zouden moeten vallen.

Onder verkeersgegevens worden hier verstaan *gegevens die worden verwerkt voor het overbrengen van communicatie of voor de facturering van die dienst,* zoals de formulering luidt in Artikel 11.1 onder b van de Telecommunicatiewet.

Zij ontstaan dus zodra communicatie gepleegd wordt, maar ook al bij het aanmelden bij (of abonneren op) een communicatiedienst. Denk hierbij aan het aanvragen van een telefoonabonnement; bij het toekennen van de aanvraag wordt de naam van de abonnee aan het toegekende telefoonnummer gekoppeld.

De verkeersgegevens die bij de communicatieprocessen ontstaan kunnen, op zichzelf of gekoppeld aan andere gegevens, een gedetailleerd beeld geven van het gedrag en interesses van individuen. Er bestaan daarom bij verschillende partijen belangstelling voor het gebruik van verkeersgegevens, bijvoorbeeld:

- bij justitie; voor het opsporen van verdachten
- bij commerciële bedrijven; voor het gebruik van individuele marketing.

De term verkeersgegevens werd in de telecom-regelgeving voor het eerst gebruikt in de richtlijn 97/66/EG. In deze richtlijn staat het volgende over verkeersgegevens beschreven:[6]

---

[6] Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *Publicatieblad* Nr. L 024 van 30/01/1998, p. 1-8.

> 'Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt om oproepen tot stand te brengen en die worden opgeslagen door degene die een openbaar telecommunicatienetwerk en/of een algemeen beschikbare telecommunicatiedienst verzorgt, moeten bij beëindiging van de oproep worden gewist of anoniem gemaakt.'[7]

Als we de inhoud van communicatie willen beschermen, maar geïnteresseerde partijen wel onder voorwaarden inzage willen geven in verkeersgegevens, dan is het maken van onderscheid tussen verkeersgegevens en inhoud noodzakelijk, en wel zodanig dat daar in de (rechts)praktijk mee gewerkt kan worden.

Dit deel beschrijft in enig detail hoe in de verschillende vormen van elektronische communicatie de inhoud van de boodschap wordt overgebracht, welke rol de verkeersgegevens daar in spelen, en waar de moeilijkheden zitten in het scheiden van verkeersgegevens en inhoud.

---

[7] Deze duiding is enger dan de eerder gegeven definitie, want heeft slechts betrekking op openbare telecommunicatiediensten en -netwerken; daarnaast ziet de omschrijving ook op verantwoordelijkheid bij beëindiging dienstverlening.

# 2. Telecommunicatie

## 2.1. Inleiding

Zoals in de inleiding vermeld is het voorstel voor de nieuwe formulering van lid 1 van artikel 13 van de Grondwet:

> 'Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.'

Wat verstaan we in dit verband onder telecommunicatie? In de memorie van toelichting:[8]

> 'Het telecommunicatiegeheim in de zin van artikel 13 ziet op een uitleg die ruimer is dan het begrip telecommunicatie of het moderne synoniem daarvan, elektronische communicatie, zoals dat gebruikt wordt in bijvoorbeeld de Telecommunicatiewet, de Europese Richtlijnen of in het Verdrag van de Internationale Unie voor Telecommunicatie. In specifieke telecommunicatieregelgeving wordt onder het begrip 'telecommunicatie' enkel 'elektronische' communicatie verstaan. Het begrip biedt binnen deze specifieke regelgeving dus geen ruimte voor eventuele nieuwe, mogelijk nog te ontwikkelen (niet-elektronische) communicatiemiddelen. Dat achten wij niet opportuun met het oog op mogelijke technologische ontwikkelingen en toepassingen in de communicatietechniek in de verre toekomst. Hoewel naar de huidige stand van de wetenschap het niet waarschijnlijk is, kan immers niet worden uitgesloten dat in de toekomst ook communicatiemiddelen – anders dan elektronische - tot wasdom komen. Omwille van de bestendigheid van de bescherming van het belang bij privé-communicatie geven wij derhalve de voorkeur aan een ruimere uitleg van het begrip 'telecommunicatie' dan thans gebruikelijk is in het kader van de genoemde regelingen.'

Telecommunicatie (samenstelling uit het griekse *τηλε* ofwel tèle = ver en het Latijnse *communicare* = mededelen), telemededelen: het verplaatsen van informatie van de ene plaats naar een andere zonder dat iets of iemand zich fysiek verplaatst.[9] Voor een betrouwbare overdracht van informatie zijn er communicatiekanalen in de vorm van kabels (glas/koper) dan wel het elektromagnetisch spectrum, nodig. Door deze transmissiekanalen te koppelen met randapparatuur, multiplexers (om signalen te mengen en weer uiteen te rafelen) en schakelapparatuur (bijvoorbeeld een telefooncentrale, een IP-

---

8 http://www.internetconsultatie.nl/briefentelecommunicatiegeheim/document/651, p. 10, geraadpleegd 1 oktober 2013.

9 Moderne vormen zijn: (mobiele) telefoon, radio, televisie en internet; een oudere vorm is telegrafie. Experimenten om te communiceren op afstand zijn zeer oud (vuur, rooksignalen, heliograaf, de optisch-mechanische telegrafie, semaforen enzovoorts.

router of een ATM-switch om signalen de juiste paden te laten bewandelen) ontstaan telecommunicatienetwerken waarop grote aantallen gebruikers kunnen worden aangesloten.

Artikel 1.1, onder e, van de telecommunicatiewet definieert niet 'telecommunicatie', maar 'elektronisch communicatienetwerk':

> 'elektronisch communicatienetwerk: transmissiesystemen, waaronder mede begrepen de schakel- of routeringsapparatuur, netwerkelementen die niet actief zijn en andere middelen, die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, waaronder satellietnetwerken, vaste en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt en netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie.'[10]

Om hetgeen onder telecommunicatie wordt verstaan zo eenduidig mogelijk af te bakenen gaan we in de volgende paragrafen nader op het begrip in.

## 2.2. Huidige en toekomstige communicatiemiddelen

Gemiddeld genomen duurt het tot volledige wasdom komen van nieuwe technologische toepassingen een hele (mensen)generatie, dus tenminste ca. 30 jaar. Fundamenteel nieuwe technieken hebben een lange weg te gaan voordat ze (grootschalig) kunnen worden toegepast. En de wetgever heeft dan zeker tijd hierop te reageren. Laten we ter illustratie even kort stilstaan bij de technologische 'oorsprong' van de computer en telecommunicatiemogelijkheden die dat gaf.

De basis voor de massaal te produceren computer en de enorme potentie van de telecommunicatie is in 1948 gelegd met de uitvinding van de transistor.[11] Telegraaflijnen, tot dan toe de enige trans-Atlantische communicatielijnen moesten tot 1956 wachten alvorens die transistors als versterkers voor onderzeese telefoonkabels konden dienen. Vanaf dat moment ging het hard met de ontwikkeling van computers en telecommunicatie, maar toch was weer een volgende technologische doorbraak nodig, namelijk het opeenstapelen van grote hoeveelheden (vooral transistor) componenten op een chip alvorens de doorbraak naar de massa kon plaatsvinden.

---

[10] Artikel 1.1, onder e, Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), *Stb.* 610.

[11] En wellicht al met Lee DeForest die in 1906 duidelijk maakte hoe je een (elektromagnetisch) signaal kon versterken: http://en.wikipedia.org/wiki/Audion, geraadpleegd 1 oktober 2013. Maar even zo gemakkelijk kan worden verwezen naar de uitvindingen/ontdekkingen van Charles Babbage, Heinrich Hertz, Thomas Edison, Gugliemo Marconi, enzovoorts.

De doorbraak waar we nu op wachten heeft met fotonenschakelingen te maken.[12] Dat die er komt is zeker. Maar alvorens die grootschalig kan worden toegepast zijn we op zijn snelst zeker 20 jaar verder.

Eerst hebben we een (uit fundamenteel onderzoek voortkomende) doorbraak nodig. Het duurt meestal 10-15 jaar alvorens de eerste mogelijke toepassingen zichtbaar worden. Vervolgens duurt het ca. 10 jaar alvorens praktische toepassingen worden bedacht (topsectorenbeleid) en die hebben dan weer ca. 10 jaar nodig voordat ze worden omarmd door de maatschappij. Van uitvinding tot grootschalige toepassing ca. 40 jaar. Dat lijken redelijke termijnen voor een eventuele volgende noodzakelijke aanpassing van de Grondwet.

Laten we nog even stilstaan bij alle huidige en toekomstige communicatiemiddelen. Tesla, toch een van de meest innovatieve en originele denkers met betrekking tot 'dragers' voor boodschappen was er van overtuigd dat je daarvoor ook bliksem kon gebruiken. Flinke bliksemschichten produceren waarmee je dan boodschappen de oceaan over zou kunnen schieten.[13] Het is net een beetje anders gelopen, we gebruiken nu glasvezelkabels en hele kleine lichtflitsjes, maar in de kern had hij natuurlijk gelijk. We hebben het hier over de vraag of er een andere 'drager' dan het elektro-magnetisch spectrum mogelijk is. Dat is dus de vraag naar de manier waarop een boodschap van Zender naar Ontvanger te krijgen is (en vice versa). Op dit moment is het licht en het radiospectrum ontsloten als drager. Wanneer we naar de technologische vooruitgang kijken ten aanzien van het 'oprekken' van de mogelijkheden van het elektromagnetisch spectrum is het maar zeer de vraag of er ooit behoefte aan een andere drager zal zijn buiten het elektromagnetisch spectrum. Temeer daar we de technische mogelijkheden van fotonen(licht) schakelingen nog maar net hebben ontdekt. Hier zal nog heel veel vooruitgang worden geboekt, wat weer terug zal slaan om de mogelijkheden van het elektromagnetisch spectrum op te rekken.

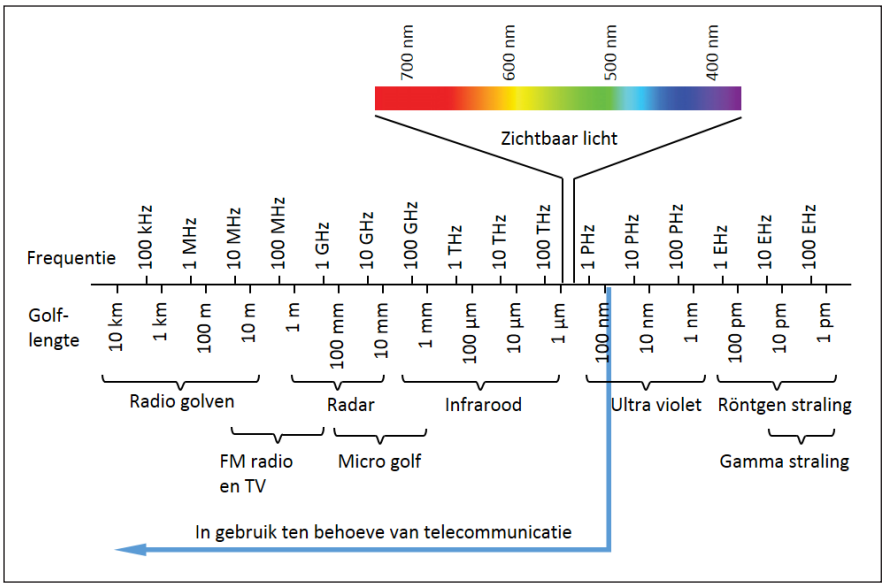
Wanneer geprobeerd wordt het bovenstaande visueel weer te geven kan in de afbeelding hieronder duidelijk gemaakt welk gedeelte van elektromagnetisch spectrum op dit moment geschikt is gemaakt voor gebruik in de telecommunicatie. Ten tijde van Hertz en Marconi zaten we helemaal links in de afbeelding, zie hieronder Figuur 1.[14] Rondom de Tweede Wereldoorlog kwam daar radar bij. Daarvoor al de mogelijkheid om door middel van modulatietechniek AM en FM radio-omroep veel efficiënter en kwalitatief beter te maken. Vervolgens ontwikkelden zich de mogelijkheden van infrarode en optische overbrengingstechnieken.

---

12 http://web.mit.edu/newsoffice/2011/quantum-light-0909.html#!prettyPhoto, geraadpleegd 1 oktober 2013.

13 Zie daarvoor Wardenclyffe vision, zoals beschreven in http://en.wikipedia.org/wiki/Wardenclyffe_Tower, geraadpleegd 1 oktober 2013.

14 http://nl.wikipedia.org/wiki/Netwerkprotocol, geraadpleegd 1 oktober 2013.




**Figuur 1 Ontwikkeling toegankelijk maken elektromagnetisch gebied**

*Andersoortige dragers voor boodschappen:* Het is zeer wel denkbaar dat (bijv. met behulp van nanotechnologie) chemische stofjes/bacteriën gebruikt zullen worden als dragers voor bepaalde andere stoffen (boodschappen, om cellen aan/uit te zetten om te stoppen/doorgaan met groeien, of juist stoppen met produceren van een bepaald stofje voor in een lichaam). Maar om deze vormen van 'informatietransport' onder toekomstig artikel 13 Gw te laten vallen lijkt niet erg voor de hand te liggen. Zo ook zal het verspreiden van bepaalde luchtjes in een winkel om consumenten aan te zetten tot het kopen van producten, niet onder telecommunicatie vallen. En hoewel al werkelijkheid geen onderwerp voor artikel 13 Gw.

## 2.3. Definities telecommunicatie

De Internationale Telecommunicatie Unie hanteert een aantal (verschillende) definities voor (onderdelen van) telecommunication (telecommunicatie).[15] Hier halen we slechts de meest relevante aan.

- Telecommunicatie: 'Any transmission and/or emission and reception of signals representing signs, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.'.[16]

---

15 Zie voorts Bijlage 1 voor een uitgebreide lijst met definities, die een rol zouden kunnen spelen bij het nader juridisch definiëren van de relevante begrippen.

16 ITU-R V.662-3 (1.06).

- Transmission: 'The action of conveying signals from one point to one or more other points.
  NOTES
  1 Transmission can be effected directly or indirectly, with or without intermediate storage.
  2 The use of the English word "transmission" in the sense of "emission" is deprecated.'[17]
- Transmission channel: 'A means of transmission of signals in one direction between two points.
  Note 1 - Several channels may share a common path; for example each channel is allocated a particular frequency band or a particular time slot.
  Note 2 - In some countries the term "communication channel" or its abbreviation "channel" is also used to mean "telecommunication circuit", i.e. to encompass the two directions of transmission. This usage is deprecated.
  Note 3 - A transmission channel may be qualified by the nature of the transmitted signals, or by its bandwidth, or by its digit rate; for example: telephone channel, telegraph channel, data channel, 10 MHz channel, 34 Mbit/s channel.'[18]
- Message: 'An instance of the primary class of information object conveyed by means of message transfer, and comprising an envelope and content.'[19]
- Content: 'The information conveyed by the document, other than the structural information, and that is intended for human perception'.[20]

Interessant zijn nog de definities afkomstig uit het ITU verdrag die samenhangen met het vertrouwelijk houden van inhoud en het vertrouwelijk 'maken' van een kanaal.

- Vertrouwelijkheid: 'A security principle that works to ensure that information is not disclosed to unauthorized subjects'.[21]
- Vertrouwelijkheid van inhoud: 'This element of service allows the originator of a message to protect the content of the message from disclosure to recipients other than the intended recipient(s). Content Confidentiality is on a per-message basis, and can use either an asymmetric or a symmetric encryption technique'.[22]
- Vertrouwelijkheid van verkeersstroom (traffic flow confidentiality): 'A confidentiality service to protect against traffic analysis'.[23]

---

17 ITU-T D.180 (09/2005), Sector: Standardization (ITU-T).
18 Standardization (ITU-T): I.113 (97), 501.
19 ITU-T J.380 (11/2011) Sector: Standardization (ITU-T).
20 F.400/X.400 (99), A.15, Sector: Standardization (ITU-T).
21 F.400/X.400 (99), B.26, Sector: Standardization (ITU-T).
22 ITU-T X.1521 (04/2011), Sector: Standardization (ITU-T).
23 F.400/X.400 (99), B.26, Sector: Standardization (ITU-T).

De functie van deze definities hangt samen met het verstrekken van eenduidige begrippen aan de opstellers van internationaal geaccepteerde teksten voor de hantering van bepaalde technische termen.[24]

## 2.4. Ordening communicatievormen

In deze paragraaf komen diverse manieren van (technisch) onderscheiden van overdracht van informatie en van de in de inleiding genoemde marktpartijen aan de orde. Technisch kan al bij het moment van verzenden worden besloten een bericht als een een-op-een gerichte informatie-uitwisseling te laten plaatsvinden dan wel als een omroepbericht, bestemd voor zoveel mogelijk (en dus ongerichte) ontvangers, zie verder paragraaf 2.4.2.

Als tweede indeling kan worden gewezen op de manier waarop in het EU mededingingsrecht gebruik is gemaakt van verschillende onderscheidingen, zoals bijvoorbeeld infrastructuurdiensten versus netwerkdiensten en toegevoegde waarde diensten, in dit verband wordt dan vaak gesproken over lagenmodellen, zie paragraaf 2.4.3. Ook is het mogelijk informatie-uitwisseling te zien in bepaalde 'stromen', waarbij afhankelijkheid bestaat van, dan wel, de plaats waar de informatie ligt 'opgeslagen' dan wel, het moment en bij wie het initiatief ligt voor het aangaan van de informatie-uitwisseling: in de literatuur wordt dit het verkeersstromenmodel genoemd (zie paragraaf 2.4.4).[25]

### *2.4.1. Protocollen*

Om een boodschap van een zender naar een ontvanger te krijgen is het nodig afspraken te maken over de manier waarop dit dan tussen zender en ontvanger gebeurt. Daarom is een protocol eigenlijk een gedragsovereenkomst. Hier zijn van belang protocollen die samenhangen met het gebruik van telecommunicatie.

Een (communicatie)protocol bevat afspraken omtrent:

- identificatie van de verschillende communicerende componenten;[26]

---

[24] De definities worden opgevoerd om te tonen dat in de techniek veel gelijkluidende, maar verschillende definities de rondte doen. De wetgever wacht een formidabele taak orde in de definitiechaos te scheppen, immers, in de Gw zal vermoedelijk de tekst komen staan: telecommunicatie(geheim). Dan moet duidelijk zijn wat er in dit kader precies onder telecommunicatie wordt verstaan.

[25] Bordewijk en Van Kaam 1982 tekenden voor het oorspronkelijke basisidee. In een Advies van de Mediaraad (Mediaraad 1993) werd het idee verder uitgewerkt. Het kreeg zijn definitieve vorm in diverse publicaties van Bekkers en Smits eind jaren negentig, zie bijvoorbeeld Bekkers en Smits 1997, p. 30. Het belang van dit model is het feit dat de formulering van de nieuwe tekst nadrukkelijk het initiatief van de telecommunicatie mee in overweging neemt om te besluiten wat beschermingswaardig is.

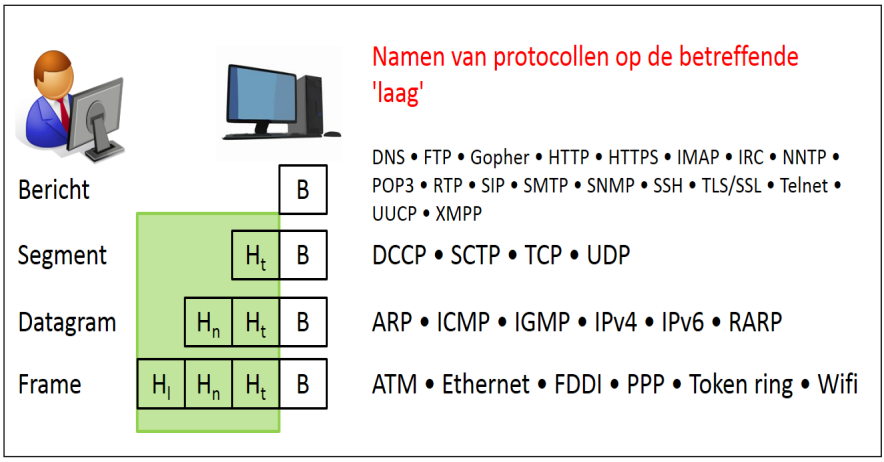
[26] Adres van verzender en ontvanger staan daarin, maar ook: wat is dit voor type

- het onderhandelen over het tot stand komen van de communicatie;
- de betekenis van de over en weer gezonden gegevens en informatieblokken, en
- het afbreken van de communicatiestroom.

In dit onderzoek gaat het hoofdzakelijk om die gedragsafspraken zoals die worden gehanteerd in de telecommunicatie:

> 'Binnen de telecommunicatie is een communicatieprotocol een set van regels en afspraken voor de representatie van data, signalering, authenticatie en foutdetectie, nodig voor het verzenden van informatie over een communicatiemedium. De communicatieprotocollen voor digitale computernetwerken hebben vele eigenschappen bedoeld om er voor te zorgen dat er betrouwbare data-uitwisseling kan plaatsvinden over een onbetrouwbaar communicatiekanaal of medium. Een communicatieprotocol is eigenlijk het volgen van bepaalde regels, zodat een systeem goed kan communiceren en daardoor informatie uit kan wisselen. Deze regels worden in een norm of standaard vastgelegd'.[27]

In Figuur 2 een weergave van de namen van de protocollen en zoals deze zijn gekoppeld aan de laag waarop het 'inpakken' van de communicatie (inhoud) plaatsvindt (zie verder paragraaf 2.4.3 en voor uitgebreidere uitleg Bijlage 2).




**Figuur 2 Protocolnamen en 'laag' van Internetberichtenuitwisseling**

bericht. Een protocol kent bijna altijd verschillende typen berichten: om bijvoorbeeld een sessie te starten of te beëindigen stuur je andere berichten dan wanneer inhoud wordt verstuurd.

27 Voor definities http://nl.wikipedia.org/wiki/Protocol#Communicatieprotocol, geraadpleegd 1 oktober 2013.

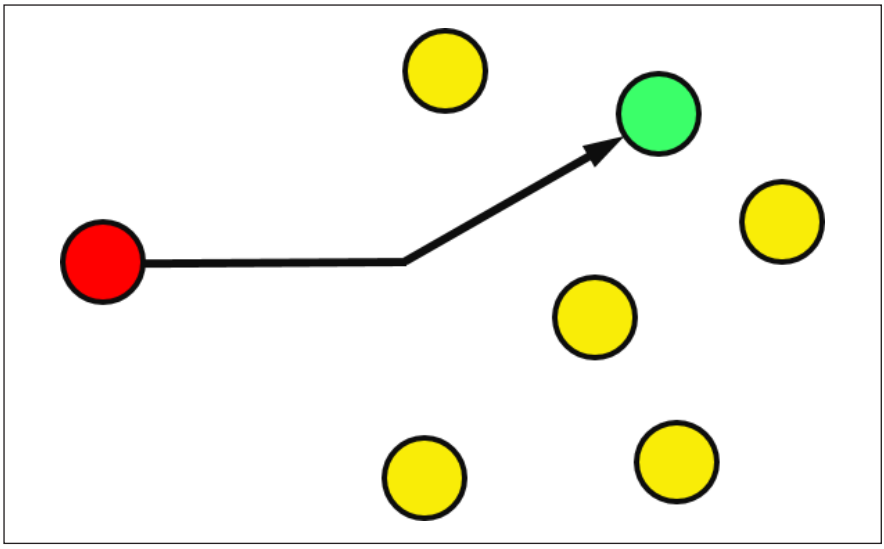
*2.4.2. Vormen van Internetcommunicatie*

Het versturen van berichten via het Internet gebeurt op verschillende manieren, daarvoor worden namen voor diensten als peer-to-peer, unicast en multicast, broadcast gebruikt. Voor de efficiëntie (en daarmee de kosten) van te versturen datapakketten aan eindgebruikers bestaat een significant verschil tussen data die wordt verstuurd aan:

- een individuele eindgebruiker
    - Unicast, point-to-point
- een bepaalde groep eindgebruikers
    - Multicast
- alle mogelijke eindgebruikers
    - Broadcast
    - Anycast

**Unicast**

Op Internet wordt normaal gesproken unicast gebruikt, ook wel point-to-point genoemd. A chat met B, C e-mailt D, E bekijkt een YouTube filmpje. Voor elke ontvanger wordt een apart signaal verstuurd (zie Figuur 3). Als 50 gebruikers hetzelfde signaal ontvangen, wordt dit 50 keer verstuurd, wat veel ruimte kost in het kernnetwerk.

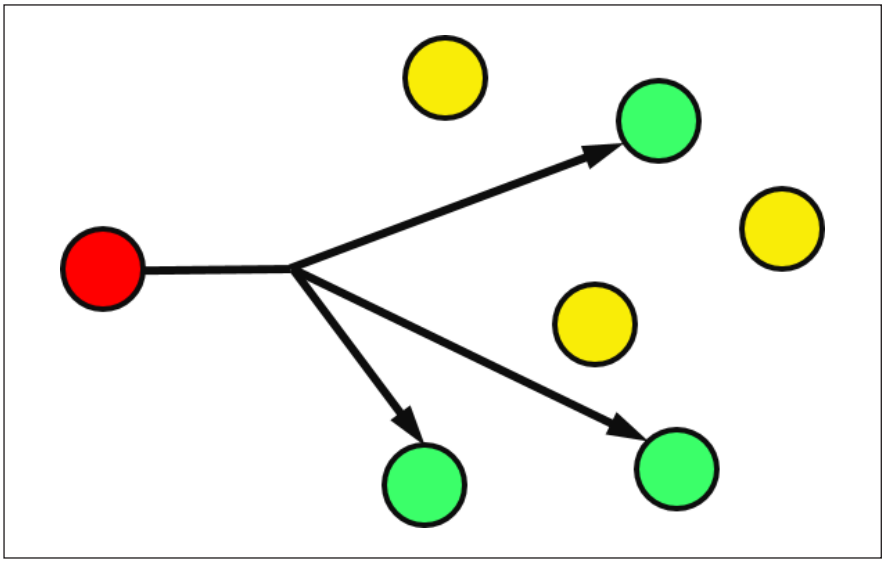


**Figuur 3 Unicast: Van één bron naar één ontvanger**[28]

Unicast: het verzenden van een pakket met informatie naar één bestemming.

[28] Bron: http://en.wikipedia.org/wiki/Unicast (ook van: Figuur 4, Figuur 5 en Figuur 6).

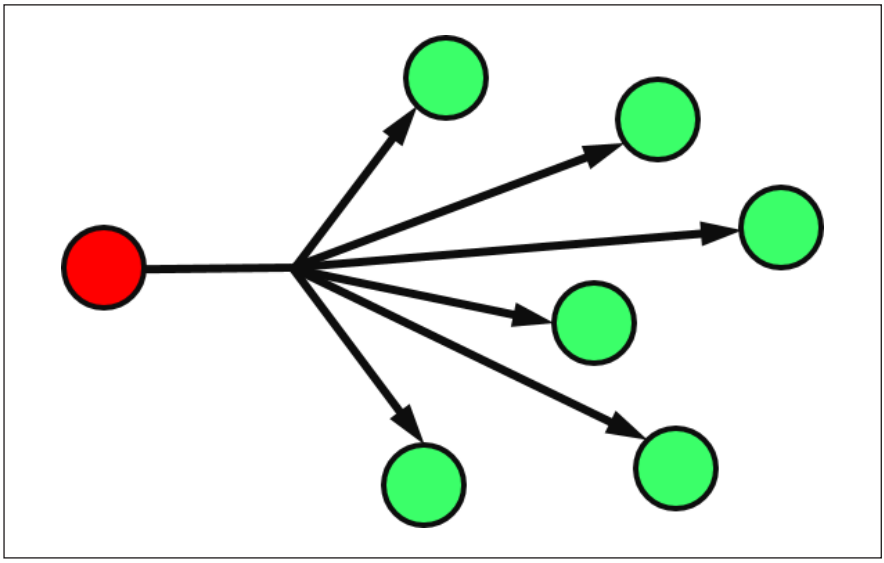
**Multicast**
Om data efficiënt aan een groep gebruikers te sturen, kan multicast worden gebruikt, ook wel point-to-multipoint genoemd. Hierbij wordt één signaal geleid tot de adressen van die geregistreerde gebruikers, door het signaal te kopiëren op routeringpunten naar de nodige, maar niet alle, paden. Hierbij is in het kernnetwerk maar één signaal nodig, zoals ook bij broadcast, maar kan wel aan een bepaalde groep worden gezonden (zie Figuur 4). Deze efficiëntie vereist echter meer intelligentie en handelingen bij routering dan broadcast of unicast.



**Figuur 4 Een Multicast van één enkele bron naar een geselecteerde groep hosts**

Multicast: het verzenden van een pakket naar alle bestemmingen die daar interesse voor getoond hebben. Een voorbeeld van een multicast is een (in feite iedere) mededeling in een groepsgesprek.

**Broadcast**
Voor 'omroep' (radio via de ether of via 'de kabel') wordt broadcast gebruikt, ook wel point-to-all genoemd (zie Figuur 5). Hierbij wordt eenmaal een signaal uitgezonden in het hele netwerk en kan iedereen dit ontvangen.



**Figuur 5 Een broadcast van een bron naar alle bestemmingen binnen het netwerk**

Broadcast: het verzenden van een pakket naar alle bestemmingen die tot een gegeven netwerk behoren.[29]

### Anycast

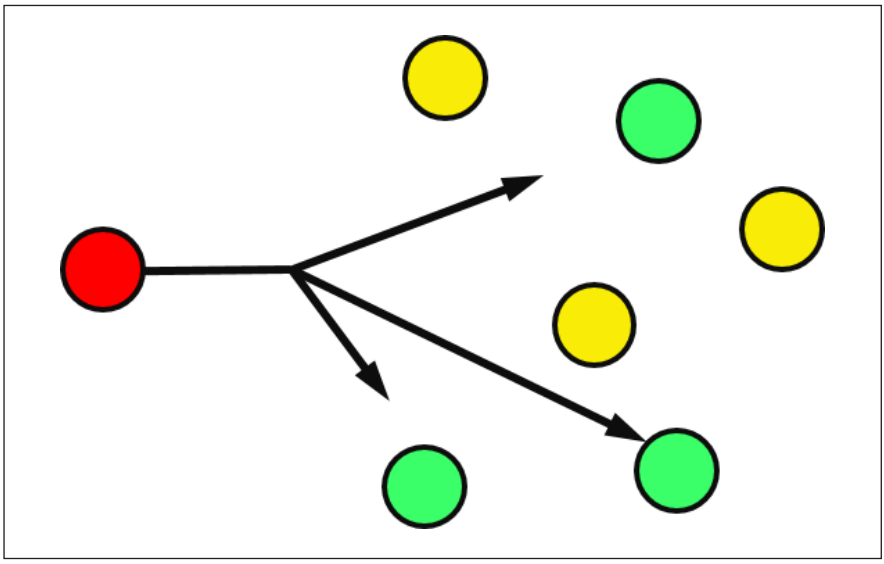
Wanneer een host[30] gegevens wil versturen naar een andere host van een bepaald type, maar het daarbij niet uitmaakt welke host specifiek de gegevens ontvangt, spreken we van anycast. De voordelen van anycasting zijn redundantie en schaalbaarheid van aangeboden diensten; indien meerdere servers een bepaalde service aanbieden op hetzelfde anycast-adres, kan het uitvallen van een server gecompenseerd worden door deze tijdelijk uit de routeringstabellen te halen.

Voor diensten op basis van UDP (zoals bijvoorbeeld Skype) is anycast echter zeer geschikt, net als voor bepaalde TCP-gebaseerde applicaties. Een goed voorbeeld hiervan is het DNS-protocol. Zo bevinden bijna alle DNS-rootservers zich in een anycast-cloud en ook DNS service providers bieden anycast-DNS service.

---

29 http://nl.wikipedia.org/wiki/Broadcast_(netwerk), geraadpleegd op 1 oktober 2013.

30 Host: een apparaat of programma dat een dienst of diensten verleent aan een kleiner of minder capabel apparaat of programma. Anycast is een techniek die af en toe gebruikt wordt door internetapparatuur om berichten 'verder' te krijgen naar de juiste bestemming, maar is voor deze discussie niet echt relevant (wel voor de compleetheid)



**Figuur 6 Anycast**

Anycast: Waarbij één bron data verzendt naar de dichtstbijzijnde host van een bepaalde klasse.[31]

*2.4.3. Lagenmodellen*

In de telecommunicatie is het heel gebruikelijk om op allerlei manieren functionele onderscheidingen te maken. Dat geldt niet alleen de techniek, waar bijvoorbeeld het OSI model een grote rol kent.

In het recht was een bepaalde indeling nodig voor bijvoorbeeld markttoetreding van nieuwe partijen. Ook de manier waarop in marktregulering zoals in het mededingingsrecht naar de sector wordt gekeken laat allerlei vormen van indelingen en lagen zien. Na de liberalisering en privatisering zoals die eind jaren 80 begin jaren 90 door de EU werd opgelegd was een onderscheid naar infrastructuur-diensten, netwerkdiensten en toegevoegde waardediensten gebruikelijk. Daaronder werd dan het volgende verstaan.

*Infrastructuurdiensten*
De infrastructuurbeheerders leveren transmissiecapaciteit aan dienstenaanbieders en eindgebruikers. De capaciteit kan in een groot aantal vormen geleverd worden. ONP-bepalingen bevatten gedetailleerde regelingen waarmee de EU-overheid probeerde de staatsmonopolies van weleer opener en

[31] http://commons.wikimedia.org/w/index.php?title=File:Anycast.svg&page=1, geraadpleegd 1 oktober 2013. Zie ook http://nl.wikipedia.org/wiki/Anycast, geraadpleegd 1 oktober 2013.

transparanter te maken.[32] Zo werden er pan-Europese minimumpakketten gedefinieerd die elke operator diende te leveren.

*Netwerkdiensten*
De netwerkdiensten leveren routering van verschillende vormen van informatie tussen en naar eindgebruikers. Het gaat hier om de routering van spraak, data en beeld. Het regime voor het aanbod van netwerkdiensten houdt in beginsel geen verband met het infrastructuurregime: de netwerkdienstenaanbieders mogen zelf de meest geschikte capaciteitsaanbieder kiezen. Voorbeelden van netwerkdiensten zijn:
- telefonie (mobiel en vast);
- datatransport (mobiel en vast);
- radio- en televisiedistributie.

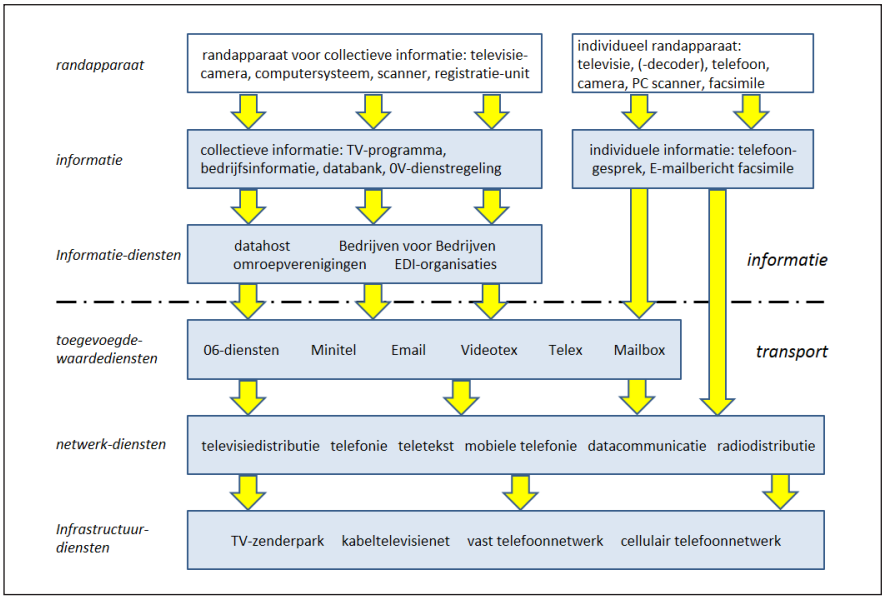
*Toegevoegde waardediensten*
De aanbieders van toegevoegde waarde diensten ten slotte leveren aanvullingen op de standaard-routering van de netwerkdienstenaanbieders, voegt daar faciliteiten aan toe en levert toegang tot informatiebestanden. Voorbeelden zijn:
- 0800 en 0900-diensten;
- teletekst.

Deze indeling waarbij ook nog vaak een onderscheid tussen inhoud en transport (in het Engels *content* en *conduit*) werd gemaakt kan op onderstaande manier grafisch worden weergegeven:[33]

---

[32] ONP staat voor Open Network Provision. De EU heeft diverse ONP-Richtlijnen uitgebracht: één Kaderrichtlijn en een aantal specifieke Richtlijnen, zoals ONP-spraaktelefonie. Het oorspronkelijke doel van deze Richtlijnen is het garanderen van een objectieve en non-discriminatoire toegang tot infrastructurele voorzieningen en diensten waarop bijzondere of uitsluitende rechten berusten. In dat verband is in elke specifieke ONP-Richtlijn een minimumpakket van te leveren voorzieningen vastgelegd. Ook zijn beginselen voor tarifering opgenomen.

[33] Bekkers en Smits 1997, p. 30.




**Figuur 7 Grafische weergave opdeling in lagen**

Dit onderscheid in drie lagen, infrastructuur-, netwerk- en toegevoegde waardediensten, dat heel gebruikelijk was in de afgelopen decennia is inmiddels verlaten. De Europese en Nederlandse regelgeving kent nu nog maar twee 'lagen', elektronische communicatienetwerken en elektronische communicatiediensten. In de Nederlandse wet vinden we dit onderscheid terug in artikel 1.1 Telecommunicatiewet, onder e en f, zo is er een elektronisch communicatienetwerk en een elektronische communicatiedienst. De wet verstaat onder:

> 'e. elektronisch communicatienetwerk: transmissiesystemen, waaronder mede begrepen de schakel- of routeringsapparatuur, netwerkelementen die niet actief zijn en andere middelen, die het mogelijk maken signalen over te brengen via kabels, radiogolven, optische of andere elektromagnetische middelen, waaronder satellietnetwerken, vaste en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt en netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie;
>
> f. elektronische communicatiedienst: gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd

> of redactioneel wordt gecontroleerd. Het omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van de notificatierichtlijn die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische communicatienetwerken'.

Het benoemen van lagen in de (EU) regelgeving ten behoeve van de mededinging en markttoetreding en regulering behelzen echter een totaal andere lading als het benoemen en bespreken van 'lagen' in de Internettechniek.

Het nieuwe EU-regime voor de telecommunicatiemarkt is aangenomen en geïmplementeerd in 2002, en wordt met enige regelmaat aan de actualiteit aangepast. Het 'telecompakket' 2002, was bedoeld om het regelgevingskader voor de telecommunicatiesector te wijzigen teneinde de sector van elektronische telecommunicatie concurrerender te maken. Dit pakket bevat een aantal hieronder kort te duiden regelingen. Het pakket bestaat uit een kaderrichtlijn en vier specifieke richtlijnen:

1. de richtlijn betreffende de machtiging voor elektronische communicatienetwerken en -diensten ('machtigingsrichtlijn');
2. De richtlijn inzake de toegang tot en interconnectie van elektronische communicatienetwerken en bijbehorende faciliteiten ('toegangsrichtlijn');
3. De richtlijn inzake de universele dienst ('universele dienstrichtlijn');
4. De richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer ('richtlijn betreffende privacy en elektronische communicatie').

Deze lijst wordt aangevuld met een beschikking inzake een regelgevingskader voor het radiospectrumbeleid ('radiospectrumbeschikking'). Dit 'telecompakket' is in december 2009 gewijzigd door de beterregelgevenrichtlijn en de burgerrechtenrichtlijn. Tevens werd een orgaan van Europese regelgevende instanties voor elektronische communicatie (BEREC) opgericht. [34]

### *2.4.4. Verkeersstromenmodel*

Het is ook interessant om de weg van de informatiestroom te volgen: is er sprake van één bron of van meerdere bronnen? En van slechts één ontvanger of juist van meerdere ontvangers? Die vier mogelijke situaties zijn in Tabel 1 weergegeven.

---

[34] Zie voor verwijzingen en samenvatting van hetgeen het totale 'telecompakket' behelst: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_nl.htm, geraadpleegd 1 oktober 2013.

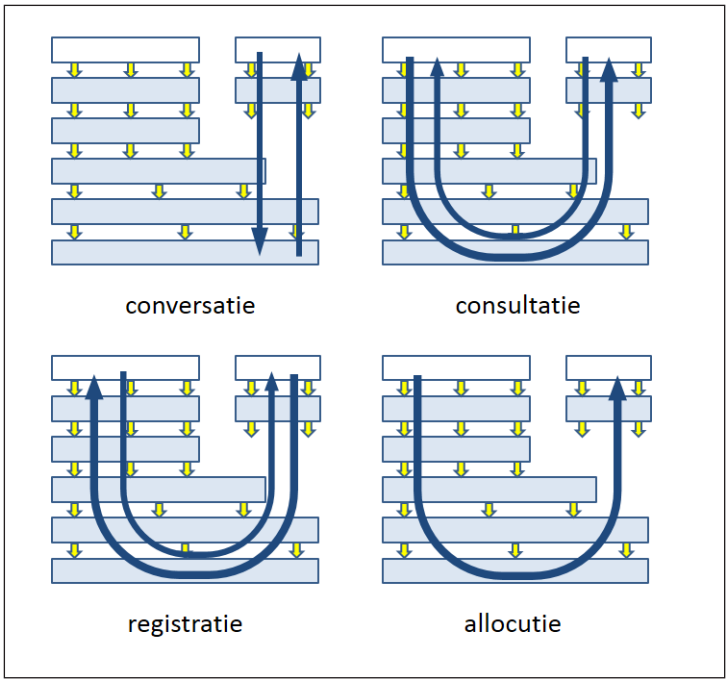
| | Individueel informatiebestand | Centraal informatiebestand |
|---|---|---|
| Individuele dienstregeling | Conversatie | Consultatie |
| Centrale dienstregeling | Registratie | Allocutie |

**Tabel 1 De vier informatie-verkeerspatronen**

In de linkerkolom staan communicatievormen waarbij de informatie-inhoud individueel bepaald is. Vaak betreft het hier persoonsgebonden en daarom soms ook gevoelige informatie. Daarom is bescherming door middel van privacyregels van belang, en soms is zelfs het grondwettelijk communicatiegeheim van toepassing. In de rechter kolom staan informatievormen waarbij het informatiebestand centraal wordt beheerd en waarbij de inhoud meer algemene (bestuurlijke of collectieve) belangen behartigt. Hier is juist het auteurs- en distributierecht van belang.

Het klassieke onderscheid tussen individuele en collectieve informatiestromen vinden we ín bijna alle landen terug in de regulering, waarbij de wetgeving voor telefonie (conversatie) traditioneel volledig los staat van die voor radio en televisie (allocutie). Door nieuwe gebruiksvormen vervagen echter de grenzen en is het vaak onduidelijk onder welke regelgeving een dienst moet vallen. Uitzending gemist bijvoorbeeld is een consultatiedienst (en het opvragen/bekijken daarvan dient onder de geheimhoudingsclausule van artikel 13 te vallen), terwijl de uitzending zelf een allocutieve dienst is die onder de vrijheid van meningsuiting valt.[35] Hieronder worden in Figuur 8 de verkeerspatronen uit Tabel 1 afgebeeld op de in Figuur 7 en omliggende tekst uitgelegde lagenmodel.

[35] Bekkers en Smits 1997, p. 32.




**Figuur 8 Verkeersstromen afgebeeld op lagenmodel van Figuur 7**

# 3. Verkeersgegevens

Juristen wil ik graag waarschuwen wanneer ze onderstaande tekst lezen. Vaak wordt het recht c.q. een juridische formulering gebruikt hieronder, maar het onderliggende fenomeen wat voortdurend geduid wordt is de technische verschijningsvorm.

## 3.1. Globale beschrijving, historie

In de allervroegste toepassingen van telefonie werden de degenen die met elkaar telefonisch contact wilden hebben gewoon met draden met elkaar verbonden die boven de straat hingen, wat een nogal wanordelijk straatbeeld opleverde.[36] Met een paar honderd abonnees is dat al bijna niet meer te doen dus kwamen er exchanges (switchboards). In het begin meestal mannen en later veelal vrouwen[37] verbonden op verzoek van degene die belde, het ene toestel (adres) met het andere. Vanaf dit moment in het gebruik van moderne telecommunicatiemiddelen maakte het adresseren (verkeersgegevens: 'Met wie kan ik U doorverbinden?'), deel uit van het telecommuniceren.

In 1962 was Nederland, na Zwitserland het tweede land op de wereld dat geen schakelcentrales/telefonistes meer kende voor het binnenlandse telefoonverkeer. Voortaan was telefoneren mogelijk zonder menselijke tussenkomst.

Netnummers bevatten naast de plaatsaanduiding ook 'verkeersinformatie' voor de PTT om überhaupt een telefoonverbinding tot stand te brengen tussen bijvoorbeeld Groningen (050) en Utrecht (030). Binnen een grotere plaats waren er ook weer verschillende centrales, een afgebakend gedeelte van de stad waar een nummer met een 6 of 8, etc., begon. Na deze plaatsaanduiding in een bepaalde wijk in een stad volgde dan nog het 'restant' van het abonneenummer. In de eerste plaats waren deze verkeersgegevens nodig om vanuit het bellende nummer, de oproepende centrale en ontvangende centrale naar een telefoonabonnee te telefoneren. Met andere woorden, deze gegevens waren nodig voor het tot stand brengen van de verbindingen. Daarnaast werden de verkeersgegevens gebruikt om een rekening op te kunnen maken. Aangezien het meeste telefoonverkeer tot ver in de jaren zeventig lokaal verkeer was, koste toentertijd het lokaal bellen maar één tik, interlokaal bellen daarentegen werd afgerekend tegen de duur van het gesprek met één tik per minuut. Het verbinden tussen twee gebruikers gebeurde dus

---

[36] Zie een tekening van telefoondraden boven Broadway in 1889 op http://www.maggieblanck.com/NewYork/SU.html, geraadpleegd 1 oktober 2013.

[37] http://chestofbooks.com/reference/Wonder-Book-Of-Knowledge/The-Story-In-The-Telephone.html#.UNBufW_K5y0, geraadpleegd 1 oktober 2013.

lange tijd handmatig via telefonistes, internationaal gebeurde dat nog tot ver in de jaren tachtig. Verkeersgegevens waren als het ware opgeslagen bij de telefonistes. Tijdseenheden tellen om een rekening te versturen was internationaal al afgesproken tijdens een ITU vergadering in Boedapest in de 19e eeuw. Tot zeer recent werden verkeersgegevens slechts 'onthouden' om tikken (tijdseenheden) met de abonnee te kunnen afrekenen.

De rol van verkeersgegevens in het proces van telefoneren is verder beschreven in paragraaf 4.1. Het proces van een gesprek opbouwen, in stand houden en beëindigen – van het afnemen van de hoorn van de haak, het herkennen van die gebeurtenis door de telefooncentrale, het genereren van een kiestoon (vroeger), het ontvangen van de door de beller gedraaide dan wel getoetste nummers, het tot stand brengen van een verbinding (ook nu nog) enzovoorts – wordt signalering genoemd. Het vandaag de dag gebruikte signaleringsprotocol is Common Channel Signalling System #7, beter bekend als SS7.

## 3.2. Ontwikkeling door digitalisering

Door de komst van steeds meer bedrijfstelefooncentrales, het gebruik van chips in publieke telefooncentrales, de moderniseringen die mogelijk werden door ISDN, kwamen de 'verkeersgegevens' steeds meer in het zicht van de gewone gebruiker. PTT kon al begin jaren negentig van de vorige eeuw door middel van Calling Line Identification / Nummerherkenning (CLI) het bellende nummer gaan doorgeven aan het opgeroepen nummer.[38] We kregen rekeningen met daarop de duur van het gesprek en de gebelde nummers, en de prijs natuurlijk.

Door de invoering van de GSM telefoonnetwerken (midden jaren negentig) kwam er nog een ander noodzakelijk verkeersgegeven bij, namelijk de locatie van de opgeroepene moet 'bekend' zijn aan de mobiele netwerkoperator, omdat anders het tot stand brengen van een gesprek tussen twee (mobiele) telefoons niet mogelijk is. Met andere woorden, aanvankelijk 'wisten' de PTT's de locaties in het vaste telefoonnet vanwege het gebruik van netnummers en de wijkcentrales; in het mobiele net werd dit opgelost doordat alle aangeschakelde telefoons zich meerdere malen per minuut aan het netwerk melden om te 'vertellen' waar ze zijn, opdat de apparatuur van de operator in staat is te bepalen via welke 'masten' de verbinding tot stand gebracht kan worden.

Door liberalisering en privatisering, maar vooral ook door de komst van Internet, zijn veel van deze functionaliteiten niet langer meer verstopt in netwerken maar kunnen zij ook door niet-netwerk eigenaren worden 'gekend'. Toen ook nog eens verkeersgegevens onderdeel van de EU privacy discussie werden, niet in de laatste plaats omdat de telefoonmaatschappijen niet

---

38 Smits 1993.

beperkt wensten te worden in de manier waarop ze de verkeersgegevens van haar klanten mochten gebruiken, brak als het ware het moment aan waarop verkeersgegevens 'loskwamen' van de boodschap.

### 3.3. Bruikbaarheid voor meerdere doelen

Uit bovenstaande weergave van de ontwikkeling van verkeersgegevens blijkt dat zij nodig zijn om de communicatie tot stand te brengen, te behouden, te beëindigen en de gepleegde communicatie in rekening te kunnen brengen, maar ook dat de hoeveelheid verschillende soorten verkeersgegevens daarnaast in de loop van de tijd flink toenam en vooral ook daardoor de verkeersgegevens zelf waardevolle informatie zijn gaan bevatten.

Het is dan ook niet vreemd dat verschillende partijen zeer geïnteresseerd zijn om kennis te kunnen nemen van de verkeersgegevens, denk hierbij aan:

- Telecomexploitanten (Marketing en Onderhoudsdienst);
- Justitie;
- Verkeersmanagement (ter bestrijding van files), en
- Retail (Marketing).

Elk van deze partijen heeft zijn eigen motieven voor een interesse in de verkeersgegevens. Die hoeven hier overigens niet besproken te worden.

### 3.4. Retentie: limitatief opgesomde verkeersgegevens

Op zichzelf hoeven we hier vanuit technologische oogpunt geen aandacht aan de dataretentie richtlijn te besteden, ware het niet dat deze richtlijn limitatief opsomt voor welke gegevens deze richtlijn geldt. In artikel 5 van de Richtlijn 2006/24/EG betreffende de bewaring van gegevens[39] staat precies voorgeschreven welke verkeersgegevens bewaard moeten blijven. Wellicht biedt een dergelijke benadering de mogelijkheid om ook op nationaal (grondwettelijk) niveau te vertrekken vanuit het beschermen van de gehele berichtenuitwisseling om daarna te bepalen welke verkeersgegevens van bescherming ex artikel 13 Gw uitgesloten kunnen worden. Vooruitlopend op later te trekken conclusies over de wenselijkheid bepaalde verkeersgegevens in beginsel ook onder de bescherming van Artikel 13 Gw te laten vallen, biedt een dergelijke benadering een mogelijkheid om bepaalde van te voren voor iedereen kenbare gegevens van die bescherming ex artikel 13 Gw uit te sluiten.

---

[39] Artikel 5, Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatie-netwerken en tot wijziging van Richtlijn 2002/58/EG, *PbEG* L 105/54 van 13.4.2006.

'1. De lidstaten zorgen ervoor dat de volgende categorieën gegevens ter uitvoering van deze richtlijn worden bewaard:

a) gegevens die nodig zijn om de bron van een communicatie te traceren en te identificeren:

1. in het geval van telefonie over een vast netwerk:
   i) het telefoonnummer van de oproeper,
   ii) naam en adres van de abonnee of de geregistreerde gebruiker;
2. in het geval van internettoegang, e-mail over het internet en internettelefonie:
   i) de toegewezen gebruikersidentificatie(s),
   ii) de gebruikersidentificatie en het telefoonnummer toegewezen aan elke communicatie die het publieke telefoonnetwerk binnenkomt,
   iii) naam en adres van de abonnee of de geregistreerde gebruiker aan wie het IP-adres, de gebruikersidentificatie of het telefoonnummer was toegewezen op het tijdstip van de communicatie;

b) gegevens die nodig zijn om de bestemming van een communicatie te identificeren:

1. in het geval van telefonie over een vast netwerk en mobiele telefonie:
   i) het telefoonnummer (de telefoonnummers) die werden opgeroepen en, in het geval van aanvullende diensten zoals call forwarding of call transfer, het nummer (de nummers) waarnaar de verbinding is doorgeleid,
   ii) naam (namen) en adres (adressen) van de abonnee(s) of de geregistreerde gebruiker(s) (…).'

# 4. Verkeersgegevens in huidige telecommunicatiepraktijk

In dit hoofdstuk wordt kort geschetst op welke wijze verkeersgegevens heden ten dage (januari 2013) worden gebruikt om sneller, gemakkelijker, goedkoper, etc., berichten te kunnen transporteren. In Bijlage 2 treft U een korte uitleg over protocollen zoals die worden gehanteerd in de telecommunicatie en Internet. In onderstaande paragrafen wordt per dienst/techniek/protocol globaal aangeven hoe het werkt, waar en hoe verkeersgegevens een rol spelen en wordt een analyse gegeven van de problemen in scheiding van inhoud en verkeersgegevens.

## 4.1. Telefonie

De rol van verkeersgegevens in het proces van telefoneren is beschreven in deze en de volgende paragraaf (4.2). Het proces van een gesprek opbouwen, in stand houden en beëindigen – van het afnemen van de hoorn van de haak, het herkennen van die gebeurtenis door de telefooncentrale, het genereren van een kiestoon (vroeger), het ontvangen van de door de beller gedraaide dan wel getoetste nummers, tot het tot stand brengen van een verbinding (ook nu nog) – wordt signalering genoemd. Het vandaag de dag gebruikte signaleringsprotocol is Common Channel Signalling System #7, beter bekend als SS7. In telefonie kan de scheiding tussen verkeersgegevens en inhoud van de communicatie in het algemeen scherp worden gelegd: de inhoud is hetgeen uitgewisseld wordt over het spraakkanaal, de signalerings-signalen en -gegevens zijn verkeersgegevens. Er zijn echter technische implementaties waarbij de grens niet scherp is: 1) toonkiezen, en 2) *premium rate*-nummers (betaal- c.q. gratis nummers).[40]

### *4.1.1. Toonkiezen*

DTMF (Dual Tone Multi-Frequency)[41] is een systeem dat wordt gebruikt in de telefonie om opdrachten te versturen (voornamelijk het te vormen telefoonnummer) binnen de frequentiebandbreedte van spraak. DTMF is een 'inband' systeem: deze signaaldata zit in dezelfde frequentieband als de hoofddata, de spraakband. Terwijl men op de toetsen drukt, wordt het luis-

---

[40] Ook keuzemenu's waarbij je intoetst en/of spreekt richting een computer. Ook dat is allemaal te scharen onder de noemer toonkiezen. Spreken richting een computer is inderdaad een ander voorbeeld van 'inhoud' die werkt als verkeersgegeven (minder erg dan andersom, wel weer een grijs gebied).

[41] http://nl.wikipedia.org/wiki/DTMF, geraadpleegd 1 oktober 2013.

tergedeelte van de telefoon even uitgeschakeld, zodat men zelf de toontjes nauwelijks hoort. Drukt men tijdens een gesprek op de knopjes, dan hoort de gesprekspartner ze wel.

Tweetonig (Dual Tone): er worden twee frequenties ('piepjes') tegelijk uitgezonden. In totaal worden er acht frequenties gebruikt. Steeds wordt er één van de vier laagste en één van de vier hoogste tegelijk uitgezonden, dat maakt het mogelijk zestien verschillende combinaties te maken (vier bij vier).

De frequenties zijn zo gekozen dat er door menging van deze frequenties geen frequentie kan ontstaan die bij deze acht staat. Men koos voor een menging van twee tonen, zodat een decoder niet zou reageren op toevallige spraakinformatie. Naast de cijfers *0* tot en met *9*, om een nummer te kiezen, zijn er ook de signalen * (sterretje) en # (hekje). Het gebruik van deze tekens is afhankelijk van de telefonie-aanbieder. De letters *A*, *B*, *C* en *D* worden nauwelijks gebruikt en zijn oorspronkelijk bedoeld om de prioriteit van het gesprek aan te geven. De frequenties zijn:

| | **1209 Hz** | **1336 Hz** | **1477 Hz** | **1633 Hz** |
|---|---|---|---|---|
| **697 Hz** | 1 | 2 | 3 | A |
| **770 Hz** | 4 | 5 | 6 | B |
| **852 Hz** | 7 | 8 | 9 | C |
| **941 Hz** | * | 0 | # | D |

**Tabel 2 DTMF signalen**

Moderne (mobiele) telefoons zijn tegenwoordig vaak uitgerust met een aparte functie om DTMF(-reeksen) te verzenden. Vaak werkt dat door het nummer in te toetsen, gevolgd door een P en de reeks. Als men dus het nummer 0611111111P1234 intoetst, zal het toestel eerst verbinding leggen met het nummer vóór de P (0611111111), waarna hij de DTMF-reeks na de P (1234) uitzendt. Deze toepassing wordt vooral gebruikt voor besturing op afstand.

**DTMF**-tonen worden ook vaak gebruikt voor besturing op afstand, bijvoorbeeld:

- Bediening van een antwoordapparaat op afstand: Wanneer namelijk een telefoonverbinding eenmaal tot stand is gekomen, luistert de telefooncentrale niet meer naar de DTMF-tonen.
- Selectie bij het bellen naar een bedrijf: Er wordt dan gebruikgemaakt

van een IVR-systeem (Interactive voice response). Er wordt dan door een computer gevraagd wat men wenst en de oproeper moet antwoorden door een cijfers in te toetsen (het 'keuzemenu').

Van het laatste hieronder een uitgewerkt voorbeeld: 'Luistert' U even mee met het volgende keuzemenu:

*Dit nummer kost € 0,10 per minuut met een maximum van € 25,--.*

*Wij kunnen U sneller van dienst zijn indien U nu Uw BurgerServiceNummer intoetst.*

De beller toetst: *123456789*.

Elk cijfer kent een andere toon; die tonen en daarmee de cijfers worden door de opgeroepene herkend en opgeslagen en vervolgens als sleutel gebruikt voor een zoekvraag in een database. Het systeem antwoordt terug:

*Goedemiddag meneer Smits, waarmee kan de fiscus U van dienst zijn?*

*1) Aanvragen van een VAR DGA.*

*2) Aanvragen van VAR WUO.*

*3) Aanvragen van een VAR.*

*Wanneer U geen keuze maakt wordt U zo spoedig mogelijk door een medewerker te woord gestaan.*

Door nu opnieuw een cijfer in te toetsen wordt de interesse van de oproeper aan het systeem van de opgeroepen bekendgemaakt. Het grijze gebied is hier dat een signaal dat normaal gesproken een verkeersgegeven is (een toon die overeenkomt met een bepaalde toets op telefoontoestel) nu wordt gebruikt als een middel om inhoud over te brengen: dit is mijn Burgerservicenummer, hierin ben ik geïnteresseerd. Om te kunnen bepalen welke keuzen zijn gemaakt door die toetsen in te drukken moet men wel de inhoud van het keuzemenu kennen, maar daar is eenvoudig achter te komen voor een overheid of andere instantie die kennis heeft kunnen nemen van die keuzetonen; die kent immers ook het gekozen telefoonnummer, en kan door het nummer zelf te kiezen het keuzemenu en eventuele submenu's beluisteren.

De vraag is wel of een instantie die verkeersgegevens mag inzien, de in het gesprek verstuurde DTMF-tonen ook te zien krijgt, die worden immers tijdens het gesprek en in de spraakband verzonden; aan de andere kant zijn de ingetoetste nummers zichtbaar in het display van het toestel waarmee zij verzonden zijn, volgend op het gebelde nummer (en dat is een verkeersgegeven).

*4.1.2 Premium rate numbers*

Informatienummers *(premium rate numbers)* zijn telefoonnummers die voor bepaalde diensten worden gebruikt en vaak ook nog eens een afwijkende vorm van beprijzen kennen: zoals 0800-nummers (gratis) en 0900-nummers (betaald).[42] Dergelijke specifieke nummers kennen we al lang in het telefoonnet. Oorspronkelijk 'zaten' dit soort specifieke nummers heel laag in de nummering, zo was er een nummer dat men kon bellen voor de tijdmelding (002) dan wel voor het weer (003).

Daarnaast zijn bepaalde groepen van nummers toegewezen aan bepaalde typen van 'dienstverlening'. Zoals nummers beginnend met 0906 voor erotische diensten en 0909-nummers voor amusement, spelletjes en prijsvragen. Uit de verkeersgegevens sec kan niet de precieze inhoud worden afgeleid, maar het nummer geeft wel een globale indicatie van de inhoud. Dat geldt ook voor sommige niet-geografische nummers, zoals 112 (alarmnummer) en 144 (meldpunt dierenmishandeling).

Door het weergegeven van letters op de cijfertoetsen van een telefoon werd naambellen mogelijk.

| | | |
|---|---|---|
| **0900-SLAAPCOACH** | **0900-BASICFIT** | **0800-CITYBOX** |
| **0900-DIERINNOOD** | **0900-PCMONTEUR** | **0900-KEYEXPERT** |

***Tabel 3 Voorbeelden van naamnummers***

Het combineren van naamnummers met toonkiezen maken het mogelijk al tijdens het 'opbouwen'; van het gesprek zoveel informatie te verzamelen zodat de beller meteen op de goede plaats in de organisatie terecht komt. Vanzelfsprekend levert dit dan ook weer 'veel' verkeersgegevens op die (veel) inhoud verraden.

## 4.2. Fax

Het telefoonnet is niet geschikt om tekst over te brengen, het is uitermate goed ingericht voor het overbrengen van geluid c.q. spraak. Toen ingenieurs na moesten denken over de mogelijkheden van teksttransport (anders dan telex en telegraaf) door middel van het telefoonnet, werd de telefax geboren. Een pagina tekst is niets anders dan het onderscheid tussen wit (papier) en zwart (een gedrukte letter). Daarnaast moest nog worden afgesproken in hoeveel stappen het 'oog' om zwart/wit te lezen over het papier zou worden geschoven, gemiddeld genomen gebeurde dat in circa 60 stappen. Dus de 'leeskop' ging 60 keer heen en terug over een A4, en 'las' zwart of wit. Aan

[42] Zie http://nl.wikipedia.org/wiki/Informatienummer (geraadpleegd 1 oktober 2013).

een hoge toon werd wit gekoppeld en een lage zwart, en die aaneenschakeling van tonen werden aan de andere kant verstaan en de printer drukte een klein 'puntje wit' (niets) bij hoog en een klein puntje zwart bij laag, en aldus kon het spraaknetwerk telefonie ook worden gebruikt voor het overbrengen van tekst.[43]

### 4.3. Sms

De Short Message Service is bedacht als een manier om korte berichten naar mobiele telefoons te kunnen sturen, gebruikmakend van het signaleringskanaal. Zo kon een kanaal, dat een groot deel van de tijd vrij beschikbaar was, nuttig worden gebruikt tegen zeer beperkte kosten.

Een sms-bericht kan maximaal 140 bytes groot zijn. Hierin passen 140 8-bits ( =1 byte) tekens. Er bestaan methodes om meerdere berichten te combineren voor het versturen van langere berichten. De gebruikers dienen echter per bericht van 140 bytes te betalen. Bij het versturen van meerdere berichten worden extra data gebruikt om aan te geven dat het om een 'multi-part'-bericht gaat. Hiervoor worden 7 bytes (of acht 7-bits tekens) van elk bericht gebruikt. Bij het versturen van een bericht dat uit twee sms-berichten bestaat, kunnen niet 320 (= 2 × 160) maar 304 (= 2 × (160-8)) tekens worden verzonden. Sms-berichten kunnen ook gebruikt worden voor het versturen van data, bijvoorbeeld plaatjes (als achtergrond van het telefoonscherm) of een melodie die gebruikt kan worden als beltoon.

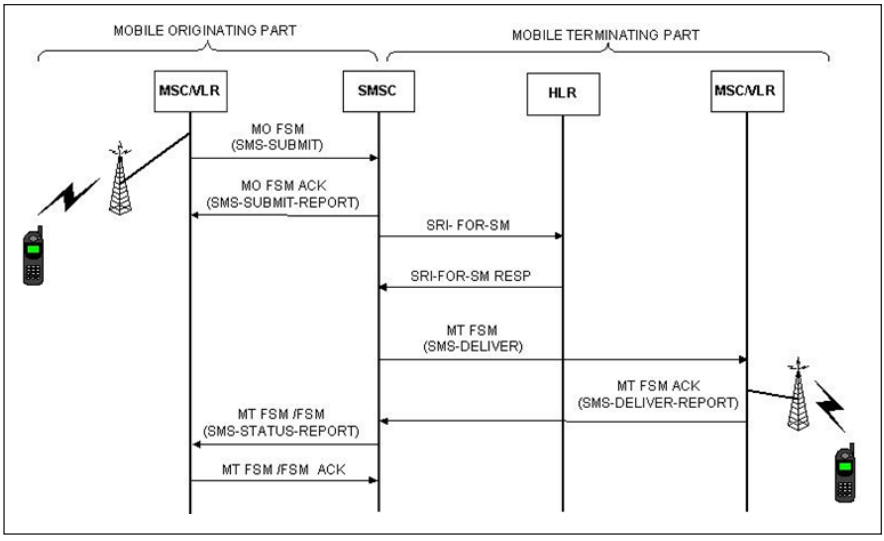
Sms wordt normaal gesproken getransporteerd over het signaleringskanaal en kan daarom afgeleverd worden aan de gebruiker terwijl deze een mobiel telefoongesprek voert. Sms-berichten worden vanuit de mobiele telefoon naar de berichtencentrale gestuurd. Deze slaat het bericht op en poogt -indien nodig meerdere keren- het bericht af te leveren. Na een in te stellen tijd (standaard 3 dagen) wordt het bericht gewist. Het is mogelijk om een bevestiging van de aflevering van een sms-bericht te verkrijgen van de berichtencentrale.

Sms-verkeer gaat als signaleringsverkeer van handset via BTS (Base Transceiver Station, het basis-zend/ontvangststation waarmee de GSM rechtstreeks communiceert) naar BSC (Base Station Controller, die meerdere BTS'en beheert) en MSC (Mobile Switching Centre, de telefooncentrale van een mobiel telefoonnetwerk) naar de SMSc (Short Message Service Centre, de berichtencentrale, zie hieronder Figuur 12). De SMSc slaat het bericht op in zijn buffer en zal vervolgens trachten de locatie van de ontvanger te bepalen (via het signaleringsnetwerk zal de MSC waar de ontvanger op is 'ingelogd' worden opgevraagd in de HLR van het netwerk van de ontvanger). De SMSc zal het sms'je vervolgens afleveren aan die MSC, die op

---

[43] Het (relatief simpele) opnemen van de aaneenschakeling van tonen zou deze tekst ook op een andere plaats hebben kunnen afdrukken.

zijn beurt probeert het sms'je af te leveren op het toestel van de ontvanger. Als dit is gelukt dan stuurt het ontvangende toestel een bevestiging terug aan de SMSc die - indien de verzender daarom heeft gevraagd bij verzending - een afleverbevestiging zal sturen aan het toestel van de afzender. Dit toestel zal dat onmiddellijk in het display weergeven. Indien aflevering is mislukt zal de SMSc op een vooraf ingesteld ritme (retry-schedule) opnieuw proberen het sms'je af te leveren. Dit ritme is in het begin met korte tussenpozen en zal na verloop van de tijd een steeds grotere tussenpoos hebben. Als na enige dagen (vaak 72 uur) het bericht nog niet is afgeleverd zal het bericht uit de buffer van de SMSc worden gewist. De zender kan dit korter instellen maar nooit langer dan het staat ingesteld in de SMSc.[44] In de vorm van een figuur ziet dat er dan zo uit: [45]




**Figuur 9 Grafische weergave SMS-berichtencentrale**

Deze hierboven beschreven vorm is de traditionele vorm, wanneer een nieuwere vorm van standaarden worden gebruikt zoals GPRS (General Packet Radio Service) dan kan het SMS verkeer anders verlopen. Bij het versturen van een SMS via GPRS wordt niet het signaleringskanaal (dat een kleine capaciteit heeft) gebruikt om sms-berichten te transporteren, maar het voor spraak 'gereserveerde' gedeelte van het netwerk. Hiertoe is overgegaan om de mogelijkheid te creëren grotere berichten dan 160 tekens te sturen, en

---

[44] Zie ook http://nl.wikipedia.org/wiki/GSM_(communicatie), geraadpleegd 1 oktober 2013.

[45] Afkomstig van http://learntelecom.com/wp-content/uploads/2010/07/SMS-Call-Flow1.jpg, geraadpleegd 1 oktober 2013.

andere bestanden dan alleen tekstbestanden (MMS, multi media messages). Echter, ook gewone SMS berichten kunnen zo worden verstuurd.

Bij SMS is dus sprake van een grijs gebied, want er wordt inhoud gestuurd over een kanaal dat eigenlijk gemaakt is voor het transporteren van verkeersgegevens. Dit is op zich nog niet heel verwarrend; het wordt wel raar als een SMS bericht zowel via dit signaleringskanaal als via de spraakband kan worden verstuurd, en communicatie via deze beide kanalen verschillend gekwalificeerd zou worden. Een SMS bericht via een spraakkanaal zou altijd beschermd worden door artikel 13, de informatie die via een signaleringskanaal wordt verstuurd valt normaal gesproken niet onder artikel 13, tenzij het een SMS bericht betreft? Daarbij moet verder nog bedacht worden dat de gebruiker die het SMS bericht verstuurt zich in het algemeen niet bewust is van welk kanaal voor het versturen gebruikt wordt. GSM-telefoons kunnen afhankelijk van de beschikbaarheid van GPRS (of UMTS) zelf schakelen tussen de verschillende netwerken om de hoogst mogelijke communicatiesnelheid te halen.

### 4.4. Email

De onderwerp-regel in een e-mail bericht is ongetwijfeld het bekendste voorbeeld van communicatie die algemeen als inhoud wordt gezien , maar die wordt verstuurd als ware het een verkeersgegeven. Een e-mail wordt namelijk verstuurd als een bericht dat bestaat uit twee delen: de *headerregels*, en de *body*. De headerregels bevatten elke een naam en een waarde. De vier belangrijkste headervelden die vrijwel altijd terug te vinden zijn in een e-mail zijn:

| | |
|---|---|
| From: | Het e-mail adres (met eventueel de naam) van de zender. |
| To: | Het e-mail adres (met eventueel naam) van de ontvanger. |
| Date: | De lokale tijd en datum van het moment waarop het bericht werd verstuurd. |
| Subject: | Een vrij in te vullen veld met (in de praktijk nagenoeg altijd) een korte omschrijving van de inhoud van de e-mail. |

Volgens RFC 2822,[46] de specificatie van het SMTP protocol dat vrijwel universeel wordt gebruikt voor het versturen van e-mail over het Internet, zijn er maar drie headerregels verplicht: het datum veld, het adres van de geadresseerde en het adres van de afzender. Het subject veld is dus optioneel, het hoeft niet te worden ingevuld, maar omdat het voor vrijwel iedereen de meest praktische manier is om e-mails van elkaar te onderscheiden is het niet gebruiken van de subject regel een inbreuk op het praktisch nut van e-mail.

---

[46] http://www.ietf.org/rfc/rfc2821.txt, geraadpleegd 1 oktober 2013.

Daarnaast worden nog andere header velden frequent gebruikt:

| | |
|---|---|
| Cc: | Carbon Copy, wordt gebruikt om een kopie van de e-mail naar andere personen te sturen. |
| Bcc: | Blind Carbon Copy. De namen van de ontvangers van de kopie worden niet getoond aan de ontvanger. |
| Received: | Informatie over de reisweg van de e-mail, gegenereerd door de e-mail server(s) of relays waar de e-mail op zijn reis over het Internet door is verwerkt. |
| Contenttype: | Informatie over hoe de inhoud van de e-mail moet worden weergegeven. |

SMTP is een bijzonder protocol, omdat de inhoud die moet worden overgebracht niet in één keer bij de geadresseerde wordt afgeleverd, maar in eerste instantie bij de mail-server waar de geadresseerde zijn 'brievenbus' heeft. Om de e-mails op te halen moet de gebruiker zelf verbinding zoeken met de mailserver (in de praktijk gebeurt dit de meeste gevallen automatisch bij het opstarten van de e-mail client, bijvoorbeeld Outlook of Eudora).

Van belang is echter dat de mails opgeslagen worden op een centrale plaats, namelijk de email-server van een Internet-provider of een groot bedrijf. Daardoor zijn e-mails relatief eenvoudig in te zien of te doorzoeken door degenen met toegang tot die server. Verder kan van de inhoud kennis genomen worden zonder dat de geadresseerde dat bemerkt (hetgeen bij andere elektronische communicatie zowel als gewone post ook kan, maar slechts met aanzienlijk meer moeite).

Naast het grijze gebied van de subject-regel die inhoud is, maar als verkeersgegeven verstuurd wordt, is er dus het aandachtspunt van de toegankelijkheid van e-mails door anderen dan de geadresseerden.

## 4.5. RSS feeds: uitgestelde consultatie

Veel Internetgebruikers hebben een aantal favoriete websites die voortdurende nieuwe inhoud bevatten, zoals de websites van kranten en omroepen, en die soms wat minder vaak nieuwe inhoud bevatten, zoals blogs. Van alle nieuwe inhoud is meestal slechts een deel interessant voor een individuele Internetgebruiker. Het kost veel tijd en moeite om meerdere websites dagelijks door te spitten en op zoek te gaan naar de interessante berichten; om dat proces te automatiseren zijn zogenaamde webfeeds bedacht: berichten die automatisch naar geïnteresseerde Internetgebruikers gestuurd worden die aangegeven hebben op de hoogte gehouden te willen worden van alle nieuwe berichten op die webserver op één of meerdere gebieden. Het bekendste systeem voor webfeeds is Really Simple Syndication (RSS). De werking is voor een gebruiker zeer eenvoudig: er is een applicatie nodig om de feeds in te ontvangen (bijvoorbeeld Outlook), of er kan gebruik worden gemaakt van speciale webpagina's zoals Google Reader. Het enige

dat dan nodig is, is op de website met interessante informatie te kijken of zij webfeeds aanbieden.


**Figuur 10 RSS feed**

Op bovenstaande site, http://www.nrc.nl/ is dat inderdaad het geval en dat wordt vrijwel altijd aangegeven door het oranje RSS-icoon. Door op dit icoon te klikken en aan te geven met welke applicatie de webfeeds ontvangen moeten worden is het 'abonnement' op deze dienst in werking gezet. RSS maakt gebruik van XML-berichten.

## 4.6. Browsen

Door met een browser webpagina's op te vragen (browsen, ook wel websurfen of kortweg surfen) doet zich opnieuw het fenomeen voor dat een gebruiker iets over de inhoud van zijn communicatie prijsgeeft in dat deel van de te transporteren data dat in beginsel vanuit technisch oogpunt moet worden gezien als verkeersgegeven.

### *4.6.1. Simpele webpagina*

Een webpagina wordt opgevraagd door een zogenaamde Uniform Resource Locator (URL) in de adresregel van de browser in te voeren. In zijn eenvoudigste vorm is een URL het unieke adres dat de locatie van een webpagina op Internet aangeeft: zo zou *www.voorbeeld.com/dezepagina*
de URL kunnen zijn van het bestand *dezepagina.html* op de server met de naam *www* die de host is van het domein *voorbeeld.com*. De browser stuurt het volgende:

```
GET /dezepagina.html HTTP/1.1
Host: www.voorbeeld.com
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
```

```
Referer: HTTP://www.tue.nl/index.php
Cookie: COOKIE data .......... data .......
[blanco regel]
```

Na de blanco regel volgt in het verzoek geen data. Het hele bericht is alleen een header, maar het geeft aan van welke pagina de gebruiker de inhoud wil opvragen. Nota bene: door de Referer (eigenlijk: referrer, maar de spelfout is in de standaard terechtgekomen) regel, is ook zichtbaar welke pagina de gebruiker hiervóór heeft opgevraagd, daarover later meer. De server antwoordt met:

```
HTTP/1.x 200 OK
Date: Thu, 15 Apr 2010 12:12:02 GMT
Content-Type: text/html
Server: Apache/1.3.34 (Unix) FrontPage/5.0.2.2635
PHP/4.4.0 mod_ssl/2.8.25 OpenSSL/0.9.8a
X-Powered-By: PHP/4.4.0
Content-Type: text/html
Content-Length: 1354
[blanco regel]
<html>
<body>
<h1>Deze Pagina Titel</h1>
(Alle HTML die de inhoud van DezePagina weergeeft.)
</body>
</html>
```

Dit bericht bevat na de lege regel, de inhoud van deze pagina.html. De inhoud die wordt prijsgegeven in de header is vergelijkbaar met de subject-regel in een e-mail: de gevraagde pagina zal in veel gevallen iets zeggen over de inhoud. Echter, bij URL's kan het prijsgeven veel verder gaan, zie de volgende paragrafen.

*4.6.2. Zoekopdracht*

Een zoekopdracht in Google (binnen de door Google zelf geleverde browser Chrome) met de woorden *internetconsultatie artikel 13 grondwet*, levert de volgende URL op:

> https://www.google.nl/webhp?sourceid=chrome-instant&rlz=1C1SKPC_enNL341&ion=1&ie=UTF-8#hl=nl&tbo=d&rlz=1C1SKPC_enNL341&sclient=psy-ab&q=**internetconsultatie**%20**artikel**%20**13**%20**grondwet**&oq=&gs_l=&pbx=1&fp=39b63b13594cdc97&bpcl=39650382&ion=1&bav=on.2,or.r_gc.r_pw.r_qf.&biw=1280&bih=933

Maar tikken we een vervolgvraag in, dan zorgt het (HTTP-protocol) ervoor

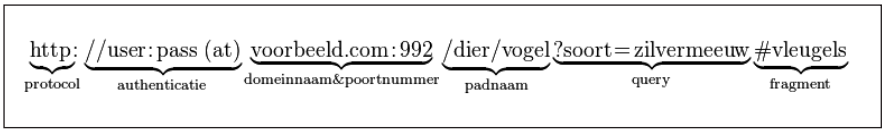
dat wanneer ik een tweede zoekvraag intik, *tuchtrechter moszkowicz,* de URL er als volgt uitziet:

> https://www.google.nl/webhp?sourceid=chrome-instant&rlz=1C1SKPC_enNL341&ion=1&ie=UTF-8#hl=nl&gs_rn=1&gs_ri=serp&tok=-rIoiY1Z-v6oL50FG67LwFw&pq=**internetconsultatie**%20**artikel**%20**13**%20**grondwet**&cp=16&gs_id=1r&xhr=t&q=**tuchtrechter**+**moszkowicz**&pf=p&tbo=d&rlz=1C1SKPC_enNL341&sclient=psy-ab&oq=tuchtrechter+mos&gs_l=&pbx=1&bav=on.2,or.r_gc.r_pw.r_qf.&fp=4e53b0bc1e5ffbf5&bpcl=40096503&ion=1&biw=1163&bih=848

In **vet** de woorden die ik de eerste en de tweede keer intikte, de URL sluit dus in waar ik vandaan kom, de referrer wordt ingesloten. Met andere woorden binnen het HTTP (en vergelijkbare protocollen) wordt altijd weergegeven wat je laatste (activiteit en op welke site) referrer was. Zo is het voor de sites waar de bezoeker naar toe gaat bijzonder gemakkelijk om ook meteen maar gauw even op te slaan waar U vandaan kwam (en vaak staat dus daar ook nog eens de laatst bedreven activiteit bij). Nu moet u niet denken dat dit alleen met zoekvragen in Google, Bing, Ask, Yahoo of iets dergelijks gaat, nee dit gebeurt altijd wanneer U surft van het ene naar het andere http adres. Dus van elk http:// adres zoals dat vrijwel altijd in Uw browser staat.

*4.6.3. Inloggen via een URL*

Een URL is ook op een andere manier nog te verrijken met gebruikersgegevens. In Figuur 13 is de opbouw van een URL (zoals die voor de meeste protocollen geldt) weergegeven:[47]

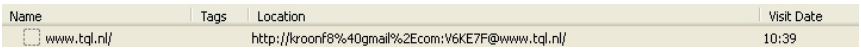



**Figuur 11 Algemene opbouw van een URL**

Door vóór het domein de user-id en het password van de gebruiker mee te geven kan de gebruiker in één keer inloggen op de dienst die de betreffende website verleent. Dit is inhoud die een gebruiker normaal gesproken niet graag prijsgeeft aan partijen die om welke reden dan ook toestemming hebben de verkeersgegevens in te zien van willekeurige Internetgebruikers.

---

[47] http://nl.wikipedia.org/wiki/Uniform_Resource_Locator, geraadpleegd 1 oktober 2013.




**Figuur 12 Voorbeeld van URL met inloggegevens**

Het is (iets) veiliger wanneer in de URL https:// staat, omdat dan het http protocol over een beveiligd (versleuteld) kanaal wordt getransporteerd.

## 4.7. TCP/IP

In deze paragraaf wordt aandacht geschonken aan twee zaken die nader illustreren dat in het Internetverkeer het onderscheid tussen inhoud van communicatie en verkeersgegevens slechts zeer moeilijk eenduidig is te maken.

### *4.7.1. Encapsulation*

In Bijlage 2 wordt de werking van TCP/IP globaal uitgelegd. Het blijkt dat Internetapplicaties de gegevens die zij willen versturen naar hun tegenhanger op een andere computer, aanbieden aan TCP. Deze gegevens zijn vaak verpakt in een bericht dat uit een header en een body bestaat, maar laten we ervan uitgaan dat we in dit geval keurig de scheiding mogen aanbrengen: de header bevat de verkeersgegevens, de body de inhoud van de communicatie. Echter, voor TCP is dit hele bericht de 'payload', de inhoud die getransporteerd moet worden. TCP plakt er zijn eigen header voor, met zijn eigen verkeersgegevens. Dit hele TCP-pakket geeft TCP weer door aan IP (met het verzoek: IP, zorg dat dit pakket op het juiste netwerk terechtkomt waar de geadresseerde computer aan verbonden is). Voor IP is dit TCP-pakket de payload, en IP plakt er ook weer zijn eigen header voor.

### *4.7.2. Herleidbare protocollen*

Het inpakken van de te communiceren inhoud is in een TCP/IP netwerk een rechttoe-rechtaan proces, de applicatie biedt aan aan TCP, die biedt aan aan IP, en die biedt aan aan de datalink (meestal Ethernet, al dan niet in de vorm van wifi), waarna het pakket daadwerkelijk getransporteerd kan worden in de vorm van radiogolven, elektrische signalen of lichtsignalen. Na aankomst moeten deze pakketten weer worden uitgepakt: de datalink geeft het pakket aan IP, die weer aan TCP, maar aan welke applicatie geeft TCP het pakket weer door? Er draaien vele applicaties op die bestemmingscomputer. De oplossing voor deze kwestie is aangebracht door elke applicatie zijn eigen 'poort' te laten gebruiken, een stuk geheugen in de computer die alleen door die applicatie mag worden gebruikt. Beide applicaties in de verzendende en ontvangende computer moeten aangeven van welk poortnummer zij gebruik willen maken. In de header van een TCP-pakket wordt dit poortnummer meegegeven. Dit poortnummer bepaalt dus voor welke applicatie of protocol

op de ontvangende computer de body van dat TCP-pakket bestemd is.

Het is natuurlijk niet praktisch als elke keer besloten moet worden van welke poort een applicatie nu weer eens gebruik zal maken, daardoor heeft de IANA een groot aantal poortnummers vast aan applicaties toegewezen.[48] Echter, daardoor kan iemand die Internet-pakketten weet te onderscheppen, door ze uit te pakken tot op TCP-niveau, al iets afleiden over de inhoud, ook al is het een niet vaak voorkomende applicatie.

Bijvoorbeeld poortnummer 4242 wordt gebruikt door het DICOM[49] protocol, dat wordt gebruikt om medische bestanden te versturen(of poort 104 voor ACR/NEMA Digital Imaging and Communications in Medicine; poorten 3305 en 6619 voor OFTP - (exchange of business documents); poort 9091 voor Bittorrent; 9212 voor het Financial Information eXchange protocol en zo voorts). [50] Een hacker, al dan niet in overheidsdienst, kan met een computer met speciale 'sniffer' software pakketten onderscheppen, maar hij zou DICOM op die computer moeten hebben draaien om DICOM pakketten te kunnen uitpakken op dat niveau. Hij komt zonder DICOM niet verder dan uitpakken tot TCP niveau. Door echter in de header van de TCP-pakketten te kijken, kan hij wel afleiden dat het om DICOM informatie gaat. Dit is een voorbeeld hoe een behoorlijk zuiver verkeersgegeven toch iets prijs kan geven over de inhoud van communicatie.

Deze vaststelling wordt geïllustreerd door hetgeen in Bijlage 3 zichtbaar is gemaakt, waar met een sniffer van onderschepte pakketjes kan worden vastgesteld dat zij voor poortnummer 17500 zijn bestemd, en dat het dus om Dropbox LanSync Discovery communicatie gaat.

## 4.8. Overvloed aan verkeersgegevens

Deze paragraaf beschrijft geen protocol, techniek of dienst, maar een aantal trends waaruit kan worden afgeleid dat het substantiële digitale spoor dat veel mensen in onze samenleving al dagelijks achterlaten, in de toekomst alleen nog maar groter wordt.

### *4.8.1. Ubiquitous computing*

Daar waar de computer nu al alomtegenwoordig lijkt, zullen computers voor nog veel meer doeleinden worden gebruikt dan nu al het geval is. De computers zijn nu al lang niet meer alleen de apparaten op of onder het bureau, of op de keukentafel, of in de broekzak, maar ze zijn ingebouwd in onze

---

48 https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt, geraadpleegd 1 oktober 2013.

49 http://en.wikipedia.org/wiki/Dicom, geraadpleegd 1 oktober 2013.

50 http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers, geraadpleegd 1 oktober 2013.

omgeving. Ze zitten al in onze auto's, tv's, in de klimaatregeling, soms al in onze elektriciteitsmeters, en ze zullen in veel meer apparaten en andere gebruiksvoorwerpen doordringen. We zijn ons nu al vaak niet eens meer bewust waar computer(tje)s een rol spelen, en of, en hoe die communiceren met de buitenwereld.

### *4.8.2. The Internet of Things*

Het Internet der Dingen is in het kort een ontwikkeling omtrent de verbinding tussen alledaagse objecten (bijvoorbeeld je tas, schoen of koelkast) binnen een netwerk. Ieder te bedenken object kan en zal vermoedelijk in de nabije voorzien worden van technologie waardoor deze binnen een netwerk (het Internet) als een uniek 'ding' herkend kan worden en met andere 'dingen' in verbinding kan staan.

Bijvoorbeeld: een chip in je schoenen registreert hoeveel stappen je op een dag hebt gezet en geeft dit door aan een website. Een andere chip in je telefoon (of jas) registreert door middel van GPS de route die je vandaag door Nederland maakt. Thuisgekomen plof je op de bank en op één van je apparaten krijg je een bericht dat je nog niet voldoende lichaamsbeweging hebt gehad voor vandaag en het verstandig is om nog wat 'actiefs' te gaan doen.

Deze verbinding tussen (meestal jouw) 'dingen' zorgt voor een andere kijk op de manier waarop het Internet ook ingezet zal gaan worden. Niet langer meer alleen het zoeken naar informatie, het uitwisselen van berichten, en het lezen van sites, maar om de (monitoring en registratie van) dingen in ons alledaagse leven. De dingen die we daarbij gebruiken worden ook een wezenlijk onderdeel van dit netwerk. Technologieën en ontwikkelingen die daarbij een grote rol spelen zijn onder andere RFID, sensoren (al aanwezig in mobiele telefoons, kompas, vertragingssensor, licht/donkersensor, etc.) en IPv6. RFID chips zorgen ervoor dat alle objecten gemakkelijk uniek herkend kunnen worden. Sensoren kunnen de aanwezigheid van mensen en andere dingen monitoren en registreren en daar weer op handelen. Het aan de gang zijn van het opschalen van IPv4 naar IPv6 zorgt ervoor dat er een bijna oneindig aantal aan IP-adressen ter beschikking is om alle 'dingen' in een/het netwerk aan te kunnen sluiten.[51]

---

[51] Zie bijvoorbeeld Castellani e.a. 2010.

**Van interactie naar resonantie**
Tijdens een lezing vertelde Rob van Kranenburg dat de ontwikkelingen rondom het Internet der Dingen erg snel gaan, sneller dan hij zelfs had verwacht. Steeds meer 'dingen' worden geschikt gemaakt om in het netwerk opgenomen te worden. Hij ziet dat het Internet der Dingen een aantal fundamentele veranderingen met zich mee brengt. De volgende zaken zijn mij het meest bijgebleven (mijn eigen interpretatie).
De verschuiving van interactie naar resonantie. In de 'klassieke' situatie ben je als gebruiker gericht op zoek naar informatie. Het is een bewuste actie. Bij het Internet der Dingen is de interactie veel meer onbewust, waarbij de omgeving en de objecten altijd informatie vergaren zonder directe interventie van de gebruiker. Interactie tussen mens en omgeving zal intuïtiever zijn. Door de verwevenheid in het alledaagse leven zijn veel mensen waarschijnlijk bekend met de werking van de dingen die ze gebruiken. Daarnaast kunnen objecten door middel van sensoren en persoonsherkenning anticiperen op de individuele gebruiker en daardoor meer gerichte informatie aanbieden.
Steeds minder discrete media. Onder discrete media zouden televisie, radio, tijdschriften, boeken etc. geschaard kunnen worden. Bij het gebruik van deze media is er geen sprake van connectiviteit. Je consumeert het en vormt er een eigen beeld bij. Nieuwe media als Twitter, Facebook, YouTube staan volop in verbinding met elkaar. De dingen waarmee we interacteren registreren ook onze handelingen, anticiperen daarop en maken deze weer inzichtelijk voor andere dingen.[152]

Zo is het ontwikkelen van het zogenaamde Message Queue Telemetry Transport (MQTT) berichten-protocol dat het versturen van telemetrie data regelt, naar een server of telemetrische makelaar. Dit protocol maakt het mogelijk juist informatie te verstrekken/uit te wisselen in zeer smalbandige of zeer beperkende technische omgevingen. Hierboven was sprake van RFID chips, maar er is nog een heel scala aan 'apparaatjes' die gegevens over ons verzamelen, te denken valt aan: 1) sensoren 2) actuatoren 3) mobiele telefoons 4) in auto's, laptops, PC's opgenomen (embedded) systemen.

Plaatsen, programma's omgevingen waar nu al van het MQTT protocol gebruik wordt gemaakt: [53]

1. in Facebook Messenger iPhone, Android, and Windows apps;
2. mooie toepassing in Say It, Sign It: Real-time avatar rendering van British Sign Language;

---

[52] Wietse van Bruggen, 'Het Internet der Dingen: een revolutie?', 29 juli 2010, doet verslag van een lezing gegeven door Rob van Kranenburg, zie http://innovatie.kennisnet.nl/het-internet-der-dingen-een-revolutie-3/, geraadpleegd 1 oktober 2013. Maar lees ook over toepassingen die aande orde kwamen op de Dutch Technology Week in juni 2012, zie http://www.technischweekblad.nl/het-internet-der-dingen.265078.lynkx met een verslag, geraadpleegd 1 oktober 2013.

[53] http://mqtt.org/projects, geraadpleegd 1 oktober 2013.

3. Andy's Twittering House: het huis dat twittert,[54] etc.
Andy Stanford-Clark, Directeur 'Uitvindingen' bij IBM, heeft alle stopcontacten, lampen, kranen, ramen en deuren en zelfs muizenvallen uitgerust met sensoren, en die verbonden met een interface op zijn pc. Elke sensor-meting die aan vooraf bepaalde criteria voldoet, genereert een Tweet, waardoor Stanford-Clark altijd en overal in staat is de gebeurtenissen in zijn huis op een verbluffend detail-niveau te volgen. Het project is enerzijds bedoeld als een experiment om te tonen wat met eenvoudige middelen al mogelijk is, anderzijds ervaart Stanford-Clark de voordelen van bijvoorbeeld zeer nauwkeurig geïnformeerd worden over je energieverbruik; zijn gezin verbruikt sinds ze zich zo bewust zijn van hun energieconsumptie een derde minder dan daarvoor.

*4.8.3. Always On-line*

Hyperconnected, nooit meer niet verbonden en dus altijd verbonden. Altijd staan de apparaten die je omringen/aanwezig zijn, in de ontvang-, en meteen in de zendstand als jij dat wilt. Vooral jonge mensen voelen zich afgesneden van de wereld als ze niet on-line zijn.

*4.8.4. Aanwezigheid (Presence) in Skype, MSN, WhatsApp, etc.*

WhatsApp is bijvoorbeeld een applicatie die bij het opstarten/aanzetten van je apparaat onmiddellijk iedereen die je toestemming hebt gegeven laat weten dat je (weer) terug on-line bent. Je bereidheid weer inhoud te willen ontvangen wordt zeer bekend gemaakt. Het aanzetten en je 'present' melden in WhatsApp, of bij Skype of bij MSN, wordt beschermd onder artikel 10 Grondwet, want de presentmelding is een 'verkeersgegeven' – of is het toch inhoud? 'Hallo ik ben er weer, ik kan weer berichten ontvangen/zenden'. Als het je (aan)melden wordt vertaald in een mededeling als: 'Hallo ik ben er weer,' dan zou het wel onder artikel 13 Gw vallen.

[54] Zie http://news.bbc.co.uk/2/hi/technology/8113914.stm, een filmpje over de manier waarop het daar gebeurd is.

# 5. Conclusies

Het kwalificeren van het correspondentie- of communicatiegeheim in de huidige Grondwetsbepaling is gekoppeld aan de drager en het bijbehorende netwerk, het brievenbus-postbode-voordeurnetwerk, het telegraafnetwerk en het telefoonnetwerk. Naast dit netwerk was er ook nog een telexnetwerk, een semafoonnetwerk en een omroepnetwerk. Er zijn nu vele andere soorten communicatienetwerken, en onvermijdelijk zullen nieuwe technologische ontwikkelingen weer andere communicatienetwerken doen ontstaan. Eén van de conclusies uit dit onderzoeksrapport luidt dan ook: wil een herformulering van artikel 13 een voldoende lange tijd mee kunnen gaan, dan dient *de nu door een technische omschrijving in de huidige (Grond)wet geduide relatie tussen 'drager' en 'het te beschermen belang' ontkoppeld te worden.*

Elke vorm waarin (potentiële) boodschappen kunnen worden vastgelegd zijn inmiddels vatbaar voor digitalisering. Anders gezegd, een (papieren) brief, een telegram, een (opgenomen) telefoongesprek, een sms-je, een omroepprogramma, kunnen worden 'omgezet' naar bits. Dit 'verbitten' van tekst, beeld en geluid kan ook nog op verschillende manieren gebeuren terwijl de 'inhoud' niet verandert net zoals een niet-gedigitaliseerd bericht op verschillende manieren kan worden verzonden. Bijvoorbeeld als volgt:

1. men kan een brief met een vulpen op papier schrijven;
2. men kan dezelfde brief typen op een typemachine;
3. men kan dezelfde brief typen in een tekstverwerker en printen, al deze vormen kunnen op de ouderwetse (slakkenpost) van een envelop, adressering, porto worden voorzien;
4. ook kan de brief op een 'open' briefkaart worden geschreven en na voldoende te zijn gefrankeerd kunnen envelop/briefkaart 'op de bus';
5. de informatie vastgelegd in de verschillende vormen kunnen ook worden gefotografeerd en als foto worden verstuurd, via de normale post;
6. men kan de brief in de vorm van een e-mail gieten;
7. men kan de brief als een aaneengeschakelde hoeveelheid sms-en versturen;
8. dan wel via een app als WhatsApp over het Internet versturen;
9. ook kan de 'brief' worden voorgelezen en opgenomen op een taperecorder, de eigen voicemailbox, op de eigen smartphone, en vervolgens als tape met de reguliere post worden verstuurd, dan wel in een voicemailbox gezet waar vervolgens een ander toegang toe wordt verschaft, het op de smartphone opgenomen geluidsbestand kan met e-mail worden verzonden.

Allemaal vormen waarbij er net als bij het aan het papier toevertrouwen van de informatie niet onmiddellijk van versturen sprake is. Er is met andere woorden nog een 'extra' handeling nodig, namelijk het 'toevertrouwen' aan een postbode/verzender voor het werkelijk inbrengen in het netwerk waarbij zorggedragen wordt voor het vervoer naar de ontvanger. En 'verbitte' informatie laat zich gemakkelijk

via de alom aanwezige elektronische communicatienetwerken transporteren, dus van zender naar ontvanger brengen, van bron naar bestemming, waar ook ter wereld.

Met andere woorden, de nu in artikel 13 Gw gebezigde kwalificaties (brief/telegraaf/telefoon) zijn allerminst adequaat wat betreft het benoemen en duiden van de correcte potentiële elektronische 'postboden'. Een andere kwalificatie kan ook nog zijn dat de huidige bepaling geformuleerd is op een techniekafhankelijke manier: telefoon/telegraaf. Een techniekafhankelijke formulering maakt het kunnen 'volgen' van de technologische ontwikkelingen juridisch en zeker ook grondwettelijk lastig. Vandaar dat het streven van de grondwetgever om de formulering zoveel mogelijk techniekonafhankelijk te maken lovenswaardig is. Daarvoor was het allereerst nodig te bezien in welke elektronische verschijningsvormen boodschappen verpakt kunnen worden en als zodanig worden aangeboden aan een derde, een vervoerder, een postbode.

De technische realiteit wordt, zoals eerder aangegeven, geschetst door de verschillende technieken die op dit moment worden gebruikt om elektronisch boodschappen uit te wisselen op verschillende dimensies te analyseren. In Bijlage 4 wordt een korte inleidende schets gegeven over hoe verschillende manieren van communiceren gebruikmaken van verschillende protocollen en verschillende transmissiekanalen. Echter, ook andere dimensies werden betrokken in de analyse, zo is er een verschil of een bericht gericht is aan één specifiek ander individu (unicast), aan een groep individuen (multicast) of aan iedereen die het maar horen wil (broadcast).

De inhoud van een uitwisseling van informatie dient juridisch te worden beschermd, door middel van een klassiek grondrecht: een nieuw te formuleren artikel 13 Gw. Dus de overheid mag het bericht niet lezen of op enige andere wijze kennis nemen van de inhoud. Als uit 'omstandigheden' af te leiden valt wat de inhoud van de uitwisseling van informatie ongeveer zal zijn, mag de overheid – zonder machtiging van de bevoegde autoriteit – geen kennis nemen van die 'omstandigheden'. Inzage in verkeersgegevens creëert in sommige / veel gevallen die 'omstandigheden'. Een strikte scheiding aanbrengen tussen de verkeersgegevens waarvan inzage de 'omstandigheden' wel, respectievelijk niet, inhoud zijn, leidt tot de ongewenste situatie dat bij ieder nieuw verkeersgegeven die afweging gemaakt moet worden: is het een verkeersgegeven dat kwalificeert als inhoud of is het een 'gewoon' verkeersgegeven? Allerlei verschillende typen van protocollen bevatten allerlei duidingen van inhoud: mail; financieel; vertrouwelijk TLS/HTTPS, maar ook aanwezigheid in XMPP, etc.

Wanneer het onderscheid tussen verkeersgegevens en inhoud als scheidslijn wordt gebruikt, met als argument dat een gedeelte van de informatie-uitwisseling (dat van de verkeersgegevens) door een ander grondrecht (namelijk artikel 10 Gw) wordt beschermd dan het andere gedeelte (de inhoud) dan zal de rechter die moet toetsen of in een bepaald geval artikel 13 Gw in het geding is, de hele tijd deskundigen nodig hebben om te duiden wat nu precies verkeersgegevens zijn en wat niet. De ontwikkeling gaat snel, op dit ogenblik circa 150 verschillende veel gebruikte applicatie-protocollen, waarvan er veel uit de tijd raken maar waar er

ook almaar nieuwe opduiken.[55]

Uiteindelijk is de verwachting dat er alleen een Internetachtig mondiaal omspannend systeem zal zijn, waarbij de systematiek van 'inpakken' (encapsulation) zoals in paragraaf 4.7.1 werd aangegeven, leidend zal zijn.

De scheiding tussen verkeersgegevens enerzijds en inhoud van het te versturen bericht anderzijds is, gelet op de al bestaande praktijk van het 'aanroepen' van protocollen/poortnummers door de door gebruikers geïnstalleerde applicaties, ondoenlijk geworden (denk hierbij aan het zelf te kiezen email-programma, VoIP, elektronisch bankieren, zoekvragen aan een zoekmachine stellen, surfen van de ene naar de andere website, het versturen van bloeddruk en bloedsuikerwaarde na een simpel prikje via een aan de mobiele telefoon gekoppelde priksensor, hartslaggegevens via een hardloop-app op een mobiele telefoon en die vervolgens weer opslaan, grafisch weergeven op de eigen (thuis)computer).

Het is nu al praktisch en financieel ondoenlijk – en in de toekomst wordt dat nog lastiger – inhoud en verkeersgegevens (langs technische weg) te scheiden.

Hier mag een ander fenomeen niet onvermeld blijven. Een persoon die meer dan twee of drie brieven per dag verstuurt is slecht denkbaar. Dat was in vroeger tijden niet anders. Een persoon die gemiddeld twee uur per dag het Internet, zowel privé als zakelijk gebruikt is normaal heden ten dage. In die twee uur wordt een groot aantal verschillende activiteiten ondernomen. De hoeveelheid communicatie is dus sterk toegenomen met de ontwikkeling van nieuwe communicatiemiddelen. Wanneer van al die activiteiten alleen maar de verkeersgegevens toegankelijk zouden komen op grond van een eventueel te maken onderscheid tussen verkeersgegevens en inhoud, is het vrij gemakkelijk geworden de inhoud van al die verschillende (Internet)activiteiten te duiden, zonder daadwerkelijk de inhoud te kennen.

Samenvattend kan nu worden vastgesteld dat deze studie antwoord geeft op de vragen:

a) Welke grijze gebieden bestaan er tussen verkeersgegevens en inhoud van communicatie (incl. de vraag wanneer is iets inhoud en wanneer niet)?
b) Kunnen verkeersgegevens in de grijze gebieden worden geclassificeerd naar de verschillende manieren waarop verkeersgegevens samenhangen met inhoud?

Beantwoording van vraag a) vormt hoofdbestanddeel van dit deel. Er blijken veel grijze gebieden te bestaan, van de bekende onderwerp-regel in e-mails en sms-berichten tot minder bekende voorbeelden als DTFM-signalen in telefoongesprekken en presentiemeldingen in applicaties als WhatsApp tot het in het algemeen onbekende fenomeen van poortnummers in TCP/IP pakketten. Koops gaat in het juridische deel diep in op de vraag wat onder 'inhoud' van communicatie

---

[55] Dat zijn de meest gebruikte, kijken we naar IANA lijst dan zijn het er enige duizenden. Zie voor de uitgebreide lijst http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml, geraadpleegd 15 november 2013, met de laatste update van de lijst van 13 november 2013.

moet worden verstaan, en wat onder verkeersgegevens valt. Voor de beantwoording van bovenstaande vragen is uitgegaan van de definitie dat onder verkeersgegevens worden verstaan: gegevens die worden verwerkt voor het overbrengen van communicatie of voor de facturering van die dienst. Inhoud is dan alle communicatie die wordt verstuurd, en die geen verkeersgegevens zijn.

Door een – in al zijn beknoptheid – toch uitvoerig overzicht te geven van de wijze waarop telecommunicatie plaatsvindt, en de rol van verkeersgegevens daarin kan vraag b) eigenlijk al bevestigend beantwoord worden, want de classificatie kan net zo uitgebreid gemaakt worden als nodig tot ieder verkeersgegeven in een apart klasse valt. In de context waarin de vraag gesteld is, zou ik hem nu als volgt willen beantwoorden: ja, het zou kunnen *op enig moment in de tijd*. Daarbij zijn echter wel drie kanttekeningen te plaatsen:

1) *Paradox in de vraagstelling.* In de memorie van toelichting bij het wetsvoorstel Wijziging artikel 13 Grondwet staat:
   *'de modernisering van artikel 13 zal moeten leiden tot een techniekonafhankelijke benadering van de reikwijdte.'*
   Echter, elke telecommunicatie maakt gebruik van techniek. Elke techniek moet naast de over te brengen inhoud van de communicatie (het bericht) ook informatie gebruiken en verzenden om het bericht op de juiste bestemming te krijgen en de dienst te kunnen factureren: verkeersgegevens. Dus verkeersgegevens zijn per definitie afhankelijk van de gebruikte techniek.
2) *Praktisch.* Techniek ontwikkelt snel. Bij iedere ontwikkeling die tot nieuwe vormen van verkeersgegevens leidt, moet de scheiding tussen inhoud en verkeersgegevens voor die nieuwe techniek gemaakt worden. Vandaar dat de frase 'op enig moment in de tijd' is toegevoegd aan het antwoord.
3) *Fundamenteel.* Scheiding aanbrengen tussen 'inhoud' en 'verkeersgegevens' dient om inhoud te beschermen en verkeersgegevens minder of niet te beschermen. Maar uit de grote hoeveelheid verkeersgegevens die mensen door het intensieve gebruik van allerlei vormen van telecommunicatie achterlaten en het feit dat verkeersgegevens vaak al iets prijsgeven over de strekking van de inhoud valt zo veel over het doen en laten van die mensen af te leiden dat daarmee de inbreuk op de vertrouwelijkheid van communicatie groter is dan kennis nemen van de inhoud van een (klein) deel van de communicatie die mensen plegen.

Op grond van de derde kanttekening zou er dus iets voor te zeggen zijn om alle verkeersgegevens onder de bescherming van artikel 13 Gw te laten vallen. Daarmee zou echter voorbij worden gegaan aan het belang van opsporingsdiensten, voor wie inzage in verkeersgegevens een routinematig onderdeel vormt voor opsporingsactiviteiten. Een richting voor een oplossing is al gegeven in de paragraaf over retentie. Van een bepaalde set van verkeersgegevens kan worden besloten dat die zonder rechterlijke last door opsporingsdiensten mogen worden ingezien. Deze limitatieve lijst kan periodiek worden herzien, en eventueel uitgebreid met nieuwe verkeersgegevens, als daartoe aanleiding bestaat.

# Bijlage 1
## Relevante definities zoals afkomstig uit ITU-verdragsteksten

| |
|---|
| Sector : Radiocommunication (ITU-R) - Recommended |
| Abbreviation : *None* |
| **Term : telecommunication** |
| Definition : Rec. ITU-R V.662 - Communication by wire, radio, optical or other electromagnetic systems. NOTE – The following definition is given in the Constitution of the International Telecommunication Union (Geneva, 1992) (CS 1012) (and RR No. 1.3): Any transmission, emission or reception of signs, signals, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. |

| |
|---|
| Source : RR. 1.3, CS 1012; |
| Publications : Recommendation ITU-R V.662-3 (2000) - Ap. 2, § 1 (1.06); |
| Sector : Radiocommunication (ITU-R) - Recommended |
| Abbreviation : None |
| **Term : (telecommunication) circuit** |
| Definition : Rec. ITU-R V.662-3 - A combination of two transmission channels, permitting transmission, in both directions between two points, of the signals exchanged between the same terminals. Note 1 – If the telecommunication is by nature unidirectional, e.g. long-distance television transmission, the term “circuit” is sometimes used to designate the single transmission channel providing the facility, but this usage is deprecated. Note 2 – A telecommunication circuit may be qualified by the nature or characteristics of the transmitted signals; for example: telephone circuit, telegraph circuit, data circuit, digital circuit. Note 3 – Such characteristics of the transmission channels as bandwidth, digit rate, may be different in the two directions of transmission. Note 4 – In telephony, usage of the term “telephone circuit” is generally limited to a telecommunication circuit directly connecting two switching centres. |

| |
|---|
| Publications : Recommendation ITU-R V.662-3 (2000) - Ap. 2, § 2 (2.03); |
| Sector : Radiocommunication (ITU-R) - Recommended |
| Abbreviation : None |
| **Term : conversation (in telecommunication)** |
| Definition : Rec. ITU-R V.662-3 - An exchange of information between terminals. |

| |
|---|
| Publications : Recommendation ITU-R V.662-3 (2000) - Ap. 2 (3.06); |
| Sector : Radiocommunication (ITU-R) - Recommended |
| Abbreviation : None |
| **Term : sending (in telecommunication), transmission (deprecated in this sense)** |
| Definition : Rec. ITU-R V.662-3 - The production of a signal at an input port of a transmission line or into a transmission medium. Note - In French the term "émission" has other meanings in radiocommunications, as given in Recommendation ITU-R V.573. |

| |
|---|
| Publications : Recommendation ITU-R V.662-3 (2000) - Ap. 2, § 1 (1.04); |
| Sector : Standardization (ITU-T) |
| Abbreviation : TLC |
| **Term : telecommunication** |
| Definition : Any process that enables a correspondent to pass to one or more given correspondents (telegraphy or telephony), or possible correspondents (broadcasting), information of any nature delivered in |

any usable form (written or printed matter, fixed or moving pictures, words, music, visible or audible signals, signals controlling the functioning of mechanisms, etc.) by means of any electromagnetic system (electrical transmission by wire, radio transmission, optical transmission, etc., or a combination of such systems).

Source : Q.9 (88), 0002
Sector : Standardization (ITU-T)
Abbreviation : TLC
**Term : telecommunication**
Definition : Any transmission and/or emission and reception of signals representing signs, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

Source : G.701 (93), 1006; I.112 (93), 110; M.60 (93), 1017
Sector : Standardization (ITU-T)
Abbreviation : None
**Term : business messages**
Definition : The actual information communicated as part of a business transaction. A message will contain multiple layers. At the outside layer, an actual communication protocol must be used (such as HTTP or SMTP). SOAP is an ebXML recommendation as an envelope for a message "payload". (Business Documents.) Other layers may deal with encryption or authentication.

Source : M.3050.4 (04), B.1.12
Sector : Standardization (ITU-T)
Abbreviation : None
**Term : answer message (ANM)**
Definition : A message sent in the backward direction indicating that the call has been answered. In semi-automatic working, this message has a supervisory function. In automatic working, this message is used in conjunction with charging information in order to: - start metering the charge to the calling subscriber (see Recommendation Q.28); and - start measurement of call duration for international accounting purposes (see Recommendation E.260).

Source : Q.762 (99), 2.2; Q.1902.2 (01), 5.2
Sector : Standardization (ITU-T)
Abbreviation : None
**Term : (digital) transmission path**
Definition : The whole of the means of transmitting and receiving a digital signal of specified rate between two digital distribution frames (or equivalent) at which terminal equipment or switches will be connected. Terminal equipment are those at which the signal originates or terminates. A transmission path is connected through one or more digital sections.

Source : I.113 (97), 501
Sector : Standardization (ITU-T)
Abbreviation : None
**Term : (transmission) channel**
Definition : A means of transmission of signals in one direction between two points. Note 1 - Several channels may share a common path; for example each channel is allocated a particular frequency band or a particular time slot. Note 2 - In some countries the term "communication channel" or its abbreviation "channel" is also used to mean "telecommunication circuit", i.e. to encompass the two directions of transmission. This usage is deprecated. Note 3 - A transmission channel may be qualified by the nature of

| |
|---|
| the transmitted signals, or by its bandwidth, or by its digit rate; for example: telephone channel, telegraph channel, data channel, 10 MHz channel, 34 Mbit/s channel. |

| |
|---|
| Source : Sup. 29 Ser. G (93), A |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : multicast transmission** |
| Definition : A transmission of the same data unit from a single source to multiple destinations in a single invocation of a service. |

| |
|---|
| Source : X.601 (00), 5.1.3 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : occasional transmissions** |
| Definition : All those which do not fall within the definition of regular transmissions. Some occasional transmissions may be subject to special contractual arrangements. |

| |
|---|
| Source : D.180 (02), 3.5.2 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : simple transmissions** |
| Definition : are one-way transmissions from a point of origin in one country to a receiving point in another. |

| |
|---|
| Sector : Standardization (ITU-T) |
| Abbreviation : Tx |
| **Term : transmission** |
| Definition : The action of conveying signals from one point to one or more other points. NOTES 1 Transmission can be effected directly or indirectly, with or without intermediate storage. 2 The use of the English word "transmission" in the sense of "emission" is deprecated. |

| |
|---|
| Source : I.112 (93), 106; M.60 (93), 4106 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : TCP |
| **Term : transmission control protocol** |
| Definition : A set of rules used along with IP to send data in the form of message units between computers over the Internet. |

| |
|---|
| Publications : ITU-T J.380 (11/2011) |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : transmission medium** |
| Definition : The type of physical means to transmit data. For example, twisted pairs, coaxial cable, optical fibres and radio link. |

| |
|---|
| Source : F.700 (00), D.20 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : transmission link** |
| Definition : A means of transmission with specified characteristics between two points. NOTE - The type of |

| |
|---|
| the transmission path or the capacity is normally indicated, e.g. radio link, coaxial link, or 2048 Kbit/s link. (Rec. I.112) |

| |
|---|
| Source : M.60 (93), 4108 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : message** |
| Definition : The unit of communication between two logical services. |

| |
|---|
| Publications : ITU-T J.380 (11/2011) |
| Sector : Standardization (ITU-T) |
| Abbreviation : MS |
| **Term : message** |
| Definition : An instance of the primary class of information object conveyed by means of message transfer, and comprising an envelope and content. |

| |
|---|
| Source : F.400/X.400 (99), A.54 |
| Sector : Standardization (ITU-T) |
| Abbreviation : MS |
| **Term : message** |
| Definition : A defined entity of information from the subscriber to the exchange pertaining to a call or a control operation for a service sent in one sequence over the signalling medium. A message may consist of one or more characters transmitted in one or more blocks. |

| |
|---|
| Source : E.131 (88), A.5 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : content** |
| Definition : The information conveyed by the document, other than the structural information, and that is intended for human perception. |

| |
|---|
| Source : T.411 (93), 3.39 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : content** |
| Definition : In the context of message handling, an information object, part of a message, that the MTS neither examines nor modifies, except for conversion, during its conveyance of the message. |

| |
|---|
| Source : F.400/X.400 (99), A.15 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : content** |
| Definition : The information conveyed by the document, other than the structural information, and that is intended for human perception. |

| |
|---|
| Source : T.411 (93), 3.39 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : content model** |

| |
|---|
| Definition : All data between the start tag and end tag of an element that affects the structure of the element in the instance document. This could be attributes or other elements within an element. (This term is not used). |

| |
|---|
| Source : M.3030 (02), 3.1.4 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : user created content** |
| Definition : User created content is any form of content such as video, blog, images, audio, etc. that was created by end-users (average public) to be available for general public. |

| |
|---|
| Publications : ITU-T X.1244 (09/2008) |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : web content** |
| Definition : A web content is the textual, visual or aural content that is encountered as part of the user experiences on websites. It may include, among other things: text, images, sounds, videos and animations. |

| |
|---|
| Publications : ITU-T Y.2235 (11/2008) |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : short message service** |
| Definition : The services in telecommunication networks, which provide mobile phones, telephones and other SMEs to transfer and receive text messages through SMSCs that store messages if the receiving terminal cannot be contacted. |

| |
|---|
| Publications : ITU-T X.1242 (02/2009) |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : short message service** |
| Definition : Short message service refers to a kind of message service, which allows mobile phones, telephones and other short message entities to transfer and receive text messages through a device-named service centre implementing functions such as saving and delivering. |

| |
|---|
| Publications : ITU-T X.1231 (04/2008) |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : information format** |
| Definition : The information format describes the way in which messages and other data are encoded in a protocol. This can include information interface definition languages such as CORBA IDL, Internet protocol formats such as HyperText Markup Language (HTML), signalling message formats, voice and video coding schemes, and multiplexing schemes such as ATM and SDH. |

| |
|---|
| Source : Y.110 (98), 8.1.2.4 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : personal information** |
| Definition : Information about an individual which can be used to identify that individual. The specific information used for this identification will be that defined by national legislation. |

| |
|---|
| Publications : ITU-T X.1051 (02/2008) |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : personally identifiable information** |
| Definition : Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly. |

| |
|---|
| Publications : ITU-T X.1252 (04/2010) |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : signalling information** |
| Definition : The information content of a signal or a signalling message. |

| |
|---|
| Source : M.60 (93), 5008; Q.9 (88), 2050; Glos. VI.7, VI.8, VI.9 (88) |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : subscription information** |
| Definition : The information that reflects the subscribing relationship among an SS, an SP and the relying mobile network. Subscription information between a service subscriber and its home network contains the subscriber's private entity identifier (e.g., PID), the basic key material (e.g., a shared secret or a public-key certificate) and its lifetime, entity service permission flag (i.e., whether it is allowed to request a specific service), the supported authentication mechanism(s) (e.g., HTTP authentication and key agreement, Diffie-Hellman based authentication mechanisms, a biometric authentication mechanism, etc.), and the authentication inquiring and key generation mechanism (e.g., GBA, Kerberos, Mediation), etc. Subscription information between a service provider and a mobile network contains the provider's identity information and public entity identifier (e.g., UID) according to the service, optionally the basic key material (e.g., a shared secret or a public-key certificate) and its lifetime, entity service permission flag (e.g., whether it is allowed to provide a specific service), the supported authentication mechanisms (e.g., certificate-based TLS authentication mechanism, PSK-TLS, IPSec), and the authentication inquiring and key generation mechanism (e.g., GBA, Kerberos, Mediation), etc. |

| |
|---|
| Publications : ITU-T X.1124 (11/2007) |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : type of user information** |
| Definition : Possible values: - speech - sound - text - facsimile - text-facsimile - videotex - video - text-interactive |

| |
|---|
| Source : I.140 (93), A.1.1 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : traffic** |
| Definition : The information generated by the subscriber that is transported on the network (i.e., user voice or data). |

| |
|---|
| Publications : ITU-T Q.1742 (11/2011) |
| Sector : Standardization (ITU-T) - Recommended |

| |
|---|
| Abbreviation : None |
| **Term : data** |
| Definition : All bits or bytes transported over the channel that individually convey information. Data includes both user data and overhead bits. Data does not include bits or bytes that, by themselves, do not convey any information, such as bits in a sync frame. See also "data frame" and "data symbol". |

| |
|---|
| Publications : ITU-T G.993 (12/2011) |
| Sector : Standardization (ITU-T) |
| Abbreviation : DT |
| **Term : data** |
| Definition : The representation forms of information dealt with by information systems and users thereof. |

| |
|---|
| Source : X.902 (95), 3.2.6 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| Term : data communications |
| Definition : The digital transmission of information (other than voice). |

| |
|---|
| Publications : ITU-T Q.1742 (11/2011) |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : datagram** |
| Definition : The fundamental protocol data unit in a packet-oriented data delivery protocol. Typically, a datagram is divided into header and data areas, where the header contains full addressing information (source and destination addresses) with each data unit. Datagrams are most often associated with connectionless network and transport layer services. |

| |
|---|
| Source : J.200 (01), 3.1.40 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : proxy** |
| Definition : A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves. |

| |
|---|
| Source : J.160 (02), II.1.31; J.174 (02), 3.7 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : content confidentiality** |
| Definition : This element of service allows the originator of a message to protect the content of the message from disclosure to recipients other than the intended recipient(s). Content Confidentiality is on a per-message basis, and can use either an asymmetric or a symmetric encryption technique. |

| |
|---|
| Source : F.400/X.400 (99), B.26 |
| Sector : Standardization (ITU-T) - Recommended |
| Abbreviation : None |
| **Term : confidentiality** |
| Definition : A security principle that works to ensure that information is not disclosed to unauthorized subjects. |

| |
|---|
| Publications : ITU-T X.1521 (04/2011) |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : content confidentiality** |
| Definition : This element of service allows the originator of a message to protect the content of the message from disclosure to recipients other than the intended recipient(s). Content Confidentiality is on a per-message basis, and can use either an asymmetric or a symmetric encryption technique. |

| |
|---|
| Source : F.400/X.400 (99), B.26 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : traffic flow confidentiality** |
| Definition : A confidentiality service to protect against traffic analysis. |

| |
|---|
| Source : X.800 (91), 3.3.57 |
| Sector : Standardization (ITU-T) |
| Abbreviation : None |
| **Term : traffic flows control** |
| Definition : A set of mechanisms used to control the flow of packets. Traffic Flow Control can be used to prevent the network from becoming overloaded by regulating the input rate transmissions, or to prevent unauthorized use of network resources. |

# Bijlage 2
## Werking TCP/IP

### Het koppelen en adresseren van computers

Het Internet Protocol, of beter, de Internet Protocolstapel, is een verzameling communicatie-protocollen die worden gebruikt in het Internet en andere computer netwerken om gegevens van de ene computer naar een andere te krijgen. De vaak gebruikte naam voor de protocolstapel is TCP/IP, naar de twee belangrijkste protocollen daaruit: Transmission Control Protocol (TCP) en Internet Protocol (IP).

Het probleem hoe gegevens van de ene computer naar de andere te krijgen kan worden opgelost door de gegevens op een drager (magnetische tape, floppy disk, usb-stick) te zetten, en de drager naar de andere computer te brengen en de gegevens daar weer in te lezen. Als dat vaak moet gebeuren is het makkelijker om een kabel tussen de computers te leggen. Dan moet er wel een koppelpunt voor die kabel in de computer bestaan, en er moet software geschreven worden om gegevens over die kabel -*de data link*- te sturen.

De uitdaging wordt iets groter als er meerdere computers met elkaar verbonden moeten worden. De oplossing die als Ethernet het licht zag loste dat op door alle (in één gebouw) aanwezige computers aan te sluiten op één lange kabel. Elke computer kreeg een interface-kaart met een uniek nummer: de medium access controller met als nummer het zogenaamde MAC-adres.

Als er links en rechts van deze Local Area Netwerken (LANs) ontstaan, ontstaat de behoefte om de computers van die verschillende LANs met elkaar gegevens te laten uitwisselen. Daarvoor biedt het Internet Protocol uitkomst. Door elk netwerk een nummer toe te kennen, en alle computers op die netwerken weer een volgnummer op dat netwerknummer (het zgn IP-adres) zijn alle computers te adresseren. Het MAC-adres is daarvoor niet geschikt, omdat het MAC-adres door de fabrikant van de netwerkkaart wordt aangebracht en dat niet te wijzigen is. IP-adressen moeten dynamisch aan computers kunnen worden toegewezen.

De IP-netwerken zijn met elkaar verbonden via *routers.* Dat zijn apparaten die door intern opgebouwde tabellen weten over welke link ze een pakketje moeten doorsturen om hem naar zijn bestemming te krijgen. Hoe dat precies in zijn werk gaat zou nog vele pagina's uitleg vragen, en is voor het verhaal verder niet heel belangrijk. Wat relevanter is, is dat IP zijn best doet een pakketje gegevens bij het juiste adres te bezorgen, maar dat niet garandeert. Ook kunnen pakketjes voor dezelfde bestemming verschillende routes volgen, waardoor de pakketjes in de verkeerde volgorde aankomen. IP is 'onbetrouwbaar'. Om toch tot een betrouwbare gegevensoverdracht te komen maken applicaties gebruik van TCP. TCP verifieert dat het pakketje (datagram) dat aankomt zonder fouten is aangekomen (door middel van

een checksum). Verder geeft TCP aan elk pakketje van een bericht (een bericht wordt namelijk opgeknipt in meerdere pakketjes, omdat de pakketjes die TCP kan versturen een maximale grootte hebben) een volgnummer. Het TCP proces aan de kant van de ontvanger bevestigt elke aankomst van een pakket. Als een bevestiging te lang uitblijft, stuurt het zendende TCP proces het pakketje opnieuw. Ook kan TCP door de volgnummers de pakketjes in de juiste volgorde aan de applicatie aanbieden.

Het User Datagram Protocol (UDP) is een vereenvoudigde versie van het TCP protocol; het beperkt zich tot het verifiëren van de foutloze aankomst van het pakketje (datagram) en het geeft het pakket door aan de juiste applicatie. UDP is daardoor sneller dan TCP, maar net als IP niet 'betrouwbaar'.

De protocollen beschrijven dus hoe gegevens moeten worden opgeknipt in pakketjes, hoe de pakketjes moeten worden geadresseerd, verstuurd, gerouteerd en ontvangen. De toepassingen die gebruik maken van het Internet, en waarvan de werking vaak ook weer is vastgelegd in protocollen, *maken gebruik van de diensten van TCP*, dat *op zijn beurt weer gebruik maakt van de diensten van IP*. De protocollen worden als het ware op elkaar gestapeld.

| |
|---|
| Toepassingslaag:<br>DNS · FTP · Gopher · HTTP · HTTPS · IMAP · IRC · NNTP · POP3 · RTP · SIP · SMTP · SNMP · SSH · TLS/SSL · Telnet · UUCP · XMPP<br><br>Transportlaag:<br>DCCP · SCTP · TCP · UDP<br><br>Netwerklaag:<br>ARP · ICMP · IGMP · IPv4 · IPv6 · RARP<br><br>Datalinklaag:<br>ATM · Ethernet · FDDI · PPP · Token ring · Wifi |

**Tabel 4 De TCP/IP Protocol Stapel**

'Binnen de telecommunicatie is een communicatieprotocol een set van regels en afspraken voor de representatie van data, signalering, authenticatie en foutdetectie, nodig voor het verzenden van informatie over een communicatiemedium. De communicatieprotocollen voor digitale computernetwerken hebben vele eigenschappen bedoeld om er voor te zorgen dat er betrouwbare data-uitwisseling kan plaatsvinden over een onbetrouwbaar communicatiekanaal of medium. Een communicatieprotocol is eigenlijk het volgen van bepaalde regels, zodat een systeem goed kan communiceren en daardoor informatie uit kan wisselen. Deze regels worden in een norm of standaard vastgelegd'.[56]

[56] Voor definities http://nl.wikipedia.org/wiki/Protocol#Communicatieprotocol, geraadpleegd 1 oktober 2013.

De standaarden voor de internetprotocollen zijn de Requests voor Comments (RFC's) die door de IETF worden beheerd.

**Voorbeeldbericht in Internet omgeving (TCP/IP)**
Hieronder wordt uitleg gegeven over de manier waarop een bericht vanaf de email-applicatie op de ene computer, naar de email-applicatie op een andere computer wordt verstuurd door middel van het almaar 'inpakken' (in technische woorden: encapsulated) van het bericht met het toevoegen van 'adres'informatie zoals dat binnen communicatieprotocollen is afgesproken. Aan de zijde van FvdK wordt het bericht vervolgens in omgekeerde volgorde 'gestript' van de Header informatie (de verkeersgegevens) en na opdracht van hem opgehaald en in een email-applicatie van hem geladen.

Het volgende bericht wil ik door middel van email versturen naar mijn collega FvdK:

'Ik schrijf op dit ogenblik aan een rapport voor BZK over artikel 13 Grondwet.'

| |
|---|
| Ik schrijf op dit ogenblik aan een rapport voor BZK over artikel 13 Grondwet. |

**Tabel 5 Bericht**

en druk op verzenden. Vervolgens:

| | |
|---|---|
| Header (transport) | Ik schrijf op dit ogenblik aan een rapport voor BZK over artikel 13 Grondwet. |
| **Ht** | **B** |

**Tabel 6 Aan het bericht wordt Transport info toegevoegd (Ht)**

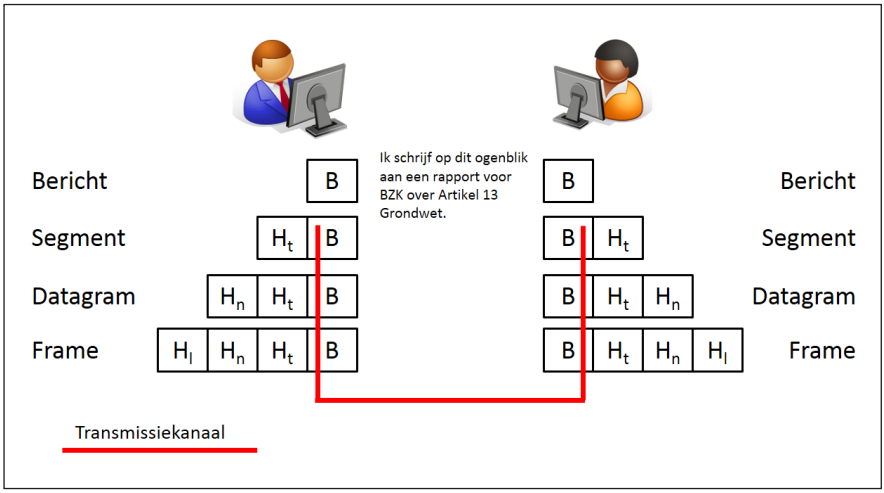
| | | |
|---|---|---|
| Header (network) | Header (transport) | Ik schrijf op dit ogenblik aan een rapport voor BZK over artikel 13 Grondwet. |
| **Hn** | **Ht** | **B** |

**Tabel 7 Aan het bericht wordt Netwerkinformatie (Hn) toegevoegd**

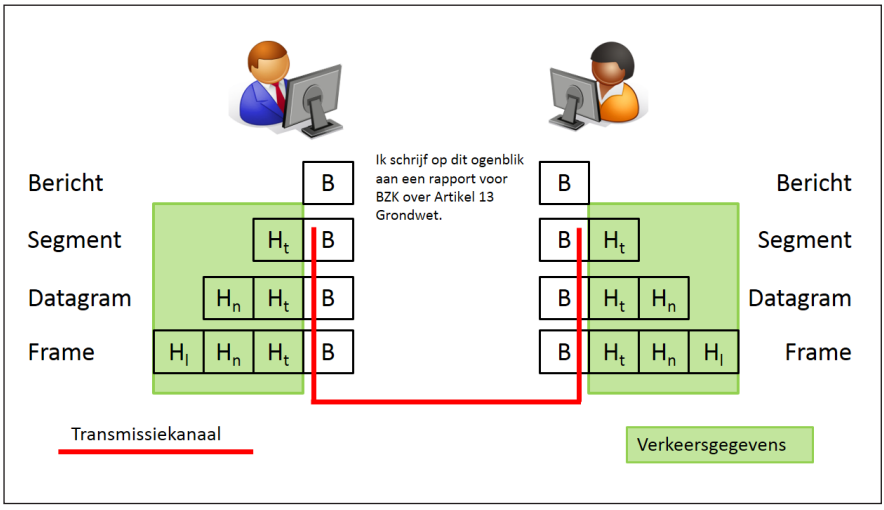
| Header (link) | Header (network) | Header (transport) | Ik schrijf op dit ogenblik aan een rapport voor BZK over artikel 13 Grondwet. |
|---|---|---|---|
| **Hl** | **Hn** | **Ht** | **B** |

**Tabel 8 Aan het bericht wordt naast Ht en Hn nog Hl toegevoegd**

Grafisch ziet bovenstaande beschrijving er uit zoals getekend in Figuur 17. Links in de figuur wordt het bericht ingetikt in een emailprogramma dat draait op de eigen notebook, PC, of iets dergelijks, bijvoorbeeld Outlook. Na op de 'verzenden' toets te hebben gedrukt wordt het bericht door het programma 'aangeboden' aan een e-mail verzendprotocol met als naam: SMTP, dat protocol voegt aan het bericht een header toe waarin adresinformatie wordt geschreven. Namelijk de adresinformatie van de verzender en die van de ontvanger. Op een wat 'dieper' niveau wordt vervolgens het door SMTP 'ingepakte' (encapsulated) bericht, opnieuw ingepakt, nu ten behoeve van de informatie die nodig is op netwerkniveau (om van het netwerk van de verzender naar dat van de ontvanger te kunnen worden verstuurd), op de link-laag (nog weer wat 'dieper' in het netwerk) wordt de adresinformatie toegevoegd die nodig is om het bericht ook werkelijk 'fysiek' te kunnen versturen en dan wordt het daadwerkelijk verstuurd. Aan de ontvangende kant gebeurt nu in omgekeerde volgorde precies hetzelfde, op de diepste laag wordt de adresinformatieheader van de link-laag eraf gehaald, aan de hogere laag aangeboden, die zijn adresinformatieheader er weer afhaalt, etc... Uiteindelijk wordt de inhoud zoals die verzonden is aangeboden aan het SMTP-proces aan de ontvangende kant.




**Figuur 13 Inpakken en versturen c.q. ontvangen en uitpakken van bericht**[57]




**Figuur 14 Duiding van headers als verkeersgegevens**

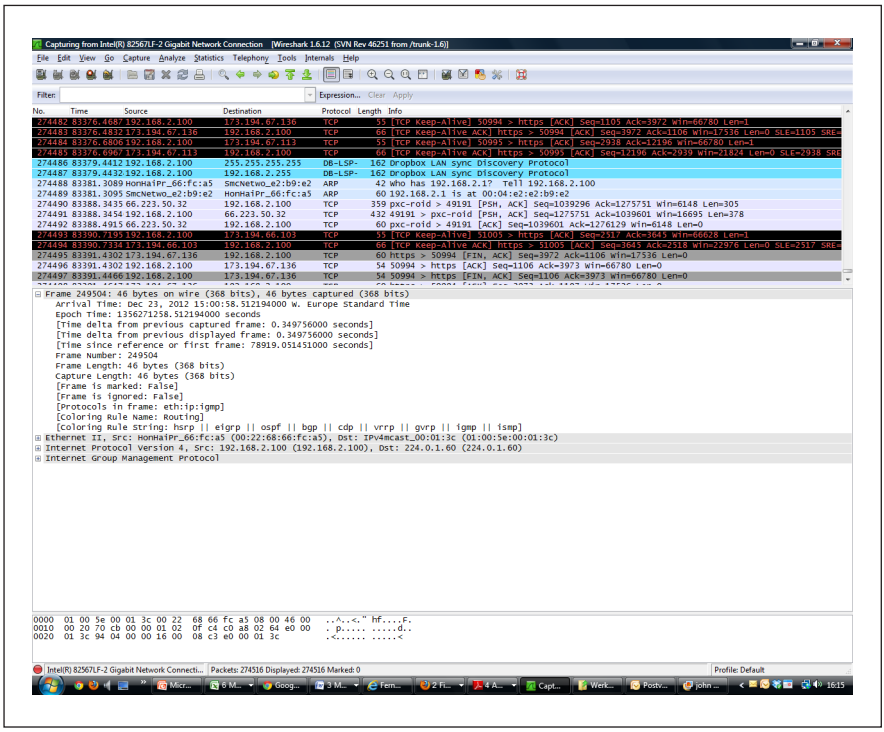
[57] http://nl.wikipedia.org/wiki/Netwerkprotocol, geraadpleegd 1 oktober 2013.

# Bijlage 3
## 'Sniffen' met WireShark

Een sniffer is een programma (applicatie) op een pc, of een speciaal voor dat doel gebouwd apparaat, dat in staat is netwerkverkeer te onderscheppen, analyseren en vast te leggen (loggen). WireShark is zo'n applicatie. Een gebruiker kan, wanneer hij (of zij) de applicatie op zijn eigen pc installeert, het door hem gegenereerde netwerkverkeer bezien.

In onderstaand voorbeeld is in de vijfde en zesde regel te zien dat de gebruiker Dropbox gebruikt, en dat die applicatie een protocol gebruikt om te bezien of de data op de pc van de gebruikers gesynchroniseerd moeten worden met de data zoals die bij Dropbox ('in de cloud') staan.

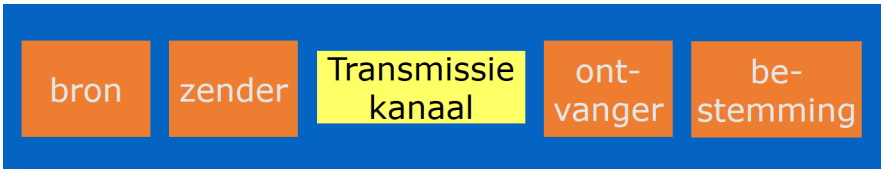
Van zo'n pakketje kan weer detail-informatie opgevraagd worden, in het voorbeeld is een pakketje (frame) van het IGMP protocol geopend.




**Figuur 15 WireShark**

# Bijlage 4
**Keuze van medium bepaalt de juridische bejegening?**

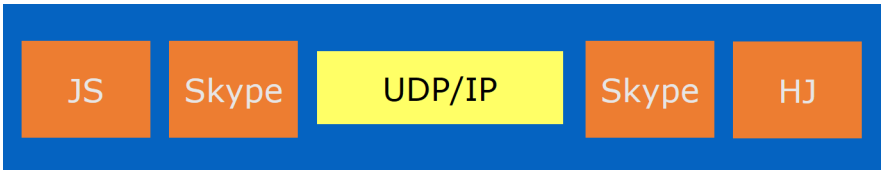
Elke (elektronische) vorm van communicatie kan op de volgende manier schematisch worden weergegeven:



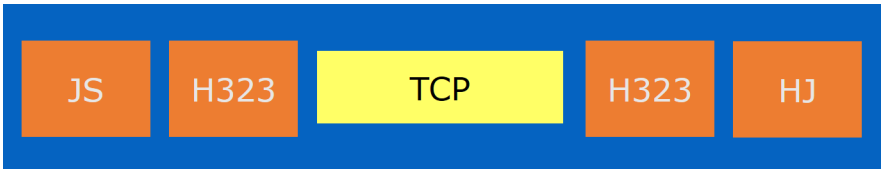

Wanneer we dit schema gebruiken om bijvoorbeeld het over afstand met elkaar spreken te duiden dan betekent dat voor het ouderwetse telefoongesprek via een vaste lijn, dat in geval Jan Smits de Bron is, zonder dat Jan Smits het weet wordt er ten behoeve van het opzetten van een telefoongesprek gebruik gemaakt van verschillende protocollen, onder andere het M1040 protocol voor 'vervoeren' van het gesproken woord en van het SS7 protocol voor het adresseren/routeren van het gesprek naar Heleen Janssen op haar kantoor in Den Haag. Dit gesprek maakt gebruik van de telefoondienst.

Daarmee valt dit gesprek onder de bescherming van artikel 13 omdat nu eenmaal het woordje telefoon wordt gebruikt: de telefoondienst. Schematisch weergegeven:


Wanneer ditzelfde gesprek via Skype (dat zijn eigen protocol gebruikt) plaatsvindt dan ziet het er zo uit:



Wanneer dit gesprek plaatsvindt als Voice over IP dienst dan ziet het er als volgt uit:




Drie manieren van transporteren van hetzelfde gesprek, drie verschillende protocollen, drie verschillende manieren van adresseren, en daardoor een verschillende juridische bejegening.

Wanneer het gaat om het uitwisselen van tekstberichten, SMS, e-mail en WhatsApp ziet het er schematisch als volgt uit:

Bij SMS:


Kenmerken van een sms-bericht, zie hierboven uitgebreid in par. 4.3.

Bij e-mail:


Bij WhatsApp:

Ook hier: drie manieren van transporteren van hetzelfde berichtje, drie verschillende protocollen, drie verschillende manieren van adresseren, en daardoor een verschillende juridische bejegening.

**Softphone**

Een softphone is een computerprogramma waarmee telefoongesprekken kunnen worden gemaakt waarbij het internet als 'drager' dient, dan werkt de gewone normale computer als telefoon in plaats van het speciaal voor dat doel ontworpen (harde) telefoontoestel. Vaak is een Softphone zo ontworpen dat deze er op het scherm hetzelfde uitziet als een gewone telefoon, de spraakverbinding loopt dan via een koptelefoon en microfoon.

Een dergelijke softphone heeft in technische zin heel erg weinig te maken met de oorspronkelijke manier van telefoneren. In feite wordt door middel van programmatuur de oude telefoonfunctie helemaal 'nagebouwd' op een computer, zelfs de manier waarop het 'gesprek' van zender naar ontvanger wordt gestuurd verschilt sterk met de oorspronkelijke wijze van telefoneren en spraakverbindingen opbouwen en gebruiken in het oude telefoonnet.

Waar bij het gebruik van een harde telefoon volkomen duidelijk is dat je slechts met een andere harde telefoon aan de andere kant werkelijk berichten kunt uitwisselen is dat bij een softphone nog niet zo voor de hand liggend. Immers beide kanten dienen over dezelfde communicatieprotocollen te beschikken. Ook de manier waarop het gesproken woord wordt omgezet in te versturen 'bits' is afhankelijk van audio codecs die op zijn minst met elkaar uitwisselbaar dienen te zijn, zo niet hetzelfde. Zo kan indien gebruik gemaakt wordt van Skype, ook echt alleen maar een gesprek plaatsvinden indien aan beide zijden Skype wordt gebruikt (Skype gebruikt immers een volkomen eigen protocol, in de internet terminologie een 'proprietary protocol'). Zo is Google Talk, ook een spraakuitwisselingsprogramma (VoIP) gebaseerd op een IETF protocol, namelijk XMPP. Daarnaast bestaat er voor het gebruik van softphones een specifiek protocol (IAX) dat afkomstig is uit een hele familie aan standaarden binnen het zogenaamde Asterisk protocol.

Als het eenmaal werkt, is het gebruik van een softphone nauwelijks te onderscheiden van een gewone telefoon. De werking is echter heel anders en de bescherming tegen kennisname van derden van de inhoud van de communicatie en de bescherming tegen kennisname van derden van de inhoud van de communicatie is daardoor anders; er zullen maar weinig gebruikers zijn die zich daar van bewust zijn.

# Deel 2.
# Juridische kwalificatie van verkeers-gegevens in het licht van artikel 13 Grondwet

*Bert-Jaap Koops*

# 1. Inleiding

In dit deel worden de resultaten beschreven van het juridisch deel van het onderzoek dat is uitgevoerd in het kader van het concept-wetsvoorstel ter aanpassing van artikel 13 Gw.

## 1.1. Doelstelling en vraagstelling

De **doelstelling** van dit onderzoek is eventuele probleemgevallen bij de juridische kwalificatie van verkeersgegevens te identificeren, eventuele discrepanties tussen de technische en juridische duiding van verkeersgegevens te inventariseren, en – voor zover haalbaar en relevant – oplossingsrichtingen te schetsen voor de bescherming van verkeersgegevens in wetgeving.
De **vraagstelling** luidt: welke typen verkeersgegevens moeten juridisch beschermwaardig worden geacht onder artikel 13 Gw, gelet op de ratio en functie van artikel 13, en in hoeverre zijn deze typen juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit?

Het onderzoek wordt geordend aan de hand van de volgende deelvragen die tezamen een antwoord geven op de algemene vraagstelling.

1. Wat is de 'inhoud' van communicatie, gelet op de ratio en functie van bescherming door artikel 13 Gw? Gaat het bijvoorbeeld om de hele inhoud of ook delen ervan, om letterlijke inhoud of om strekking?
2. Welke grijze gebieden bestaan er tussen verkeersgegevens en inhoud van communicatie?
3. Kunnen verkeersgegevens in de grijze gebieden worden geclassificeerd in een typologie van verschillende manieren waarop verkeersgegevens samenhangen met inhoud?
4. Welke typen verkeersgegevens, volgens de typologie uit vraag 3, zijn beschermwaardig onder artikel 13 Gw omdat zij 'inhoud' betreffen volgens het antwoord op vraag 1?
5. Welke aandachtspunten kunnen worden geformuleerd voor de keuzes die de wetgever moet maken ten aanzien van verkeersgegevens in het licht van de herziening van artikel 13 Gw?

## 1.2. Afbakening

Het onderzoek vindt plaats in het kader van het concept-wetsvoorstel ter aanpassing van artikel 13 Gw (hierna: wetsontwerp-2012).[58] In dat wetsontwerp

[58] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, http://www.

worden, in navolging van de commissie-Franken en de commissie-Thomassen, verkeersgegevens als zodanig uitgesloten van de bescherming van artikel 13 Gw, aangezien zij geen inhoud van communicatie betreffen. Alleen voor zover verkeersgegevens raken aan de inhoud van communicatie, zouden ze beschermwaardig kunnen zijn onder artikel 13. Dit onderzoek ziet daarom niet primair op de vraag of verkeersgegevens *als zodanig* bescherming behoeven onder artikel 13 Gw, hoewel die vraag niet helemaal losgekoppeld kan worden van de vraag naar de ratio en reikwijdte van artikel 13 Gw. Daarom wordt wel enige aandacht besteed aan de beschermwaardigheid van verkeersgegevens onder artikel 13 Gw in het algemeen, maar de nadruk ligt op de vraag onder welke omstandigheden verkeersgegevens zodanig verbonden zijn met inhoud van communicatie dat zij aanspraak kunnen maken op het beschermingsregime van communicatie-inhoud onder artikel 13 Gw.

## 1.3. Terminologie

Ter aanduiding van datgene wat artikel 13 Gw beoogt te beschermen, wordt in dit rapport kortheidshalve de term 'correspondentiegeheim' gebruikt. Dit sluit aan bij artikel 8 EVRM, dat de term 'correspondence' hanteert. Hiermee beoog ik niet om een nieuw begrip te introduceren in de discussie over artikel 13 Gw, maar simpelweg om een compact begrip voorhanden te hebben dat als koepelterm kan fungeren voor de verschillende termen die in de literatuur en wetgeving worden gebruikt (zoals brief-, telefoon- en telegraafgeheim; brief- en telecommunicatiegeheim; communicatiegeheim). Waar in dit rapport 'correspondentiegeheim' wordt gebruikt, moet dus gelezen worden de term die in de context door de desbetreffende auteur wordt gehanteerd om het beschermingsobject van artikel 13 Gw aan te duiden.

Onder 'verkeersgegevens' kunnen als werkdefinitie worden verstaan gegevens die worden verwerkt voor de afhandeling (transport of facturering) van telecommunicatie. (In par. 2.3 worden nadere definities genoemd voor dit begrip.)

## 1.4. Methoden van onderzoek

Het onderzoek is uitgevoerd op basis van literatuuronderzoek. Het literatuuronderzoek bestond uit een analyse van de wetsgeschiedenis van artikel 13 Gw, van de diverse voorstellen sinds de jaren '90 tot herziening hiervan, alsmede van rapporten en academische literatuur over verkeersgegevens en het correspondentiegeheim.

internetconsultatie.nl/briefentelecommunicatiegeheim (geraadpleegd 1 oktober 2013).

# 2. De ratio en reikwijdte van artikel 13 Grondwet

Van Dorst heeft opgemerkt dat het opvalt dat bij de behandeling van alle voorstellen die hebben geleid tot het huidige artikel 13 Gw 'nergens een beschouwing is ten beste gegeven over de grondslag van het postgeheim'.[59] De ratio en reikwijdte van artikel 13 Gw kunnen daarom alleen indirect worden afgeleid uit de wetsgeschiedenis en de doctrine. In dit hoofdstuk wordt eerst de wetgeschiedenis besproken, voor zover die aanknopingspunten bevat voor de ratio en reikwijdte, en vervolgens de doctrine. Relevante passages worden geciteerd, waarbij kernformuleringen betreffende de ratio en reikwijdte vet worden weergegeven. Op basis daarvan worden aansluitend de bevindingen samengevat om zicht te krijgen op wat precies aan inhoud van communicatie artikel 13 Gw beoogt te beschermen.

## 2.1. Wetsgeschiedenis

Bij de invoering van het briefgeheim in 1848 heeft de wetgever geen inhoudelijke argumentatie gegeven: de bepaling 'zal wel geene verdediging behoeven. Dat het geheim der brieven onschendbaar behoort te zijn, is eene bepaling die in de meeste grondwetten van Europa thans is opgenomen. Het gemis daarvan scheen de Nederlandsche Grondwet te ontsieren.'[60] In de wetsgeschiedenis is weinig te vinden over de vraag welk deel van de brief wordt beschermd: de inhoud of ook uiterlijke kenmerken.[61] De argumentatie van Thorbecke, de geestesvader van het briefgeheim uit 1848, suggereert dat het (vooral of alleen?) om de inhoud gaat:

> 'Het **openen of doen openen van iemands brieven** tegen zijnen wil, is geen mindere, ja gevaarlijker aanranding der bijzondere vrijheid, dan wanneer verklikkers in zijn huis worden gezonden, om zijne vertrouwelijke gesprekken af te luisteren, zoodat het, naar het voorbeeld van andere Staten, evenzeer te pas komt, den wetgever te verpligten, dat hij het geheim der brieven, als dat hij de woning van den ingezeten doe eerbiedigen.'[62]

De Staatscommissie die het Wetboek van Strafvordering van 1926 voorbereidde, hanteerde eveneens de interpretatie dat alleen de inhoud werd beschermd: 'De heer Schimmelpenninck vraagt, **of het brievengeheim niet geacht moet worden zich tot het feit der verzending zelve uit te**

---

59 Van Dorst 1982, p. 287.

60 *Handelingen II* 1847-1848, p. 350, geciteerd in Hofman 1995, p. 108.

61 Hofman 1995, p. 149.

62 *Bijlage Handelingen II* 1844-1845, p. 461, geciteerd in Hofman 1995, p. 107 (nadruk in dit citaat en de volgende citaten is toegevoegd).

**strekken**? Mag de post van het feit aan den O.v.J. kennis geven? De commissie meent de eerste vraag **ontkennend**, de tweede bevestigend te moeten beantwoorden.'[63] Met andere woorden, verkeersgegevens vallen niet onder de reikwijdte van het briefgeheim zoals ingevoerd in 1848.

Bij de totstandkoming van het huidige artikel 13 Gw ligt de nadruk op het kennisnemen van de inhoud van communicatie:

> 'Er is, naar het de ondergetekenden voorkomt, een belangrijk verschil tussen het brief- en telefoongeheim enerzijds en het telegraafgeheim anderzijds. Communicatie per brief of telefoon kan plaatsvinden zonder dat **de doorgevende instantie van de inhoud van de brief of het telefoongesprek kennis neemt**. Het vertrouwelijk karakter van deze communicatievormen is daardoor duidelijk **en de inhoud van brief en gesprek kan daarop worden afgestemd**.'[64]
>
> 'Met de staatscommissie en de opstellers van de Proeve van een nieuwe grondwet zijn wij van mening, dat naast de briefwisseling ook de communicatie door middel van telefoon en telegraaf een belangrijke plaats in het maatschappelijk verkeer heeft verworven en **in verband met het privé-karakter ervan** onder de grondrechten moet worden opgenomen.'[65]
>
> 'Dat betekent niet, dat er niet een **zeker karakterverschil tussen deze drie rechten** zou bestaan. Bij het briefgeheim gaat het om een communicatie die plaatsvindt in gesloten enveloppes, althans in een verpakking welke het oogmerk van de afzender tot uitdrukking brengt, **dat derden – waaronder de PTT – van de inhoud van de brief geen kennis nemen**. Bij het telegraafgeheim is dit aspect minder sterk aanwezig. Zo zal het open aangeboden of per telefoon opgegeven **telegram onvermijdelijk ter kennis moeten komen** van hen, die het telegram aannemen, doorzenden of telefonisch afleveren. Het telegraafgeheim komt in die gevallen vooral hierin tot uitdrukking, dat zij, **die ambtshalve van de inhoud van het telegram kennis nemen**, **daarover aan derden geen mededeling mogen doen**.
>
> Het telefoongeheim ligt wat het geheimhoudingsaspect betreft enigszins tussen de beide eerdergenoemde rechten in. Gezien de mate van automatisering van het telefoonverkeer, waardoor voor het telefoongesprek gewoonlijk geen tussenkomst van derden meer nodig is, benadert het telefoongeheim wat het geheimhoudingsaspect betreft het briefgeheim. Anders dan bij de briefwisseling is voor de telefoonverbinding evenwel de instandhouding van een ingewikkelde apparatuur vereist. Het is onvermijdelijk, dat deze apparatuur in haar verschillende onderdelen voortdurend wordt gecontroleerd en waar nodig wordt hersteld. Om te kunnen vaststellen of een verbinding goed verloopt is het echter noodzakelijk, dat op telefoongesprekken wordt ingeluisterd. Het **zou te ver gaan het telefoongeheim zo ruim op te vatten, dat ook deze technische controle en herstelwerkzaamheden, waarbij wel eens iets van een gesprek moet worden opgevangen, als inbreuken** op

---

63 Notulen 13e vergadering Staatscommissie, p. 16, Lindenberg 2002, p. 204.

64 *Kamerstukken II* 1970-71, 11 051, nr. 3, p. 20.

65 *Kamerstukken II* 1975-76, 13 872, nr. 3, p. 44.

> dit recht zouden worden aangemerkt. Zo ver strekt het in het onderhavige artikel voorgestelde recht zich niet uit; wel brengt het artikel mee, dat **hetgeen aldus wordt opgevangen niet aan derden mag worden doorgegeven**. Evenmin is het als een inbreuk op het telefoongeheim te beschouwen wanneer ten behoeve van de opsporing van zgn. telefoonplagers wordt geregistreerd tussen welke aansluitingen en op welke tijdstippen een verbinding tot stand werd gebracht, **zolang van de inhoud van het gesprek niet wordt kennis genomen**.
> (…) De telegrafie is niet meer beperkt tot de traditionele vorm van de open aangeboden berichten. Het hele netwerk van telexverbindingen valt er thans onder en deze communicatievorm functioneert veelal automatisch, hetgeen wil zeggen dat er van verzender tot ontvanger geen sprake behoeft te zijn van enige menselijke tussenkomst. De overheid is daar **niet meer gedwongen om van de inhoud van de verzonden berichten kennis te nemen**. Maar ook bij de open aangeboden berichten is het telegraafgeheim niet zonder betekenis in verband met het bovenvermelde feit, dat de **ambtenaar, die** het bericht ontvangt en **van de inhoud kennis neemt, tot geheimhouding verplicht is, welke geheimhoudingsplicht in beginsel ook tegenover andere overheidsfunctionarissen geldt**.' [66]
> 'Ten slotte zij opgemerkt, dat het telefoon- en telegraafgeheim alleen dan onschendbaar kan zijn wanneer degene, die zich van deze media bedient, er zijnerzijds zorg voor draagt dat van een geheim te houden communicatie sprake kan zijn. Wie een telefoongesprek voert met gebruikmaking van een ontvanginrichting voor **draadloze telefonie, zodat een ieder, die over een zodanige inrichting beschikt, het gesprek kan opvangen**, kan zich **niet op het grondrecht beroepen**.'[67]

Het gemeenschappelijke kenmerk bij alle communicatievormen is dat het bij het correspondentiegeheim gaat om het kennisnemen van de inhoud van de communicatie door de transporteur. Er bestaat een karakterverschil tussen brief, telefoongesprek en telegram, aangezien bij de transporteur bij de brief nooit, bij het telefoongesprek soms (voor technische controle) en bij het telegram meestal (behalve bij telex) kennis moet nemen van (een deel van) de inhoud om het bericht te kunnen transporteren. Maar ook wanneer de transporteur uit de aard der zaak kennis neemt van de inhoud van een bericht, geldt het correspondentiegeheim, in die zin dat de transporteur de inhoud niet mag doorvertellen aan derden.

Van Dorst verheldert deze reikwijdte door een onderscheid te maken tussen het postgeheim in enge zin en het postgeheim in ruime zin.

> 'De **ratio van het postgeheim in enge zin, t.w. de bescherming van het privé-leven** tegen inbreuk daarop van de zijde van de overheid (…). De technische ontwikkelingen (…) hebben er ook toe geleid dat de telefoon met de

---

66 *Kamerstukken II* 1975-76, 13 872, nr. 3, p. 44-45.
67 *Kamerstukken II* 1975-76, 13 872, nr. 3, p. 46

> brief kan concurreren als middel om **met de buitenwereld contact te onderhouden**, d.w.z. dat de gemiddelde telefoongebruiker **er niet op bedacht** zal zijn – en ook niet **behoeft te zijn – dat anderen kennis nemen van de inhoud** van het gesprek.'[68]
> 'Naast het postgeheim in enge zin, dat geënt is op de garantie van een "staatsvrije" privésfeer, staat het postgeheim in ruime zin, dat als het ware een uitvloeisel vormt van het eerste en daarmee onverbrekelijk is verbonden en dat zijn grond vindt in **het vertrouwen** dat de burger mag stellen in de functionarissen van de openbare post-, telefoon- en telegraafdienst, **dat dezen de kennis die zij opdoen bij de uitoefening van hun functie niet aan derden bekend zullen maken**. (…) Op grond van deze vertrouwensrelatie behoren de genoemde ambtenaren **geheimhouding** te betrachten **over alles wat zij bij de uitoefening van hun functie te weten komen omtrent post-, telefoon- en telegraafverkeer tussen bepaalde personen** (…).'[69]

Het correspondentiegeheim in ruime zin omvat volgens Van Dorst dus ook verkeersgegevens ('alles (…) omtrent post-, telefoon- en telegraafverkeer'), hoewel dat niet met zoveel woorden te lezen valt in de toelichting van de wetgever. De citaten uit de wetsgeschiedenis omtrent het correspondentiegeheim in ruime zin betreffen immers alleen de kennis die de transporteur in de uitoefening van zijn functie opdoet over de inhoud van de communicatie.

Wetsvoorstel 25443 sloot verkeersgegevens uit omdat zij niet inhoud van communicatie betreffen:

> 'Verkeersgegevens – daarbij gaat het om gegevens als het feit dat getelefoneerd wordt, met wie en waar – verschillen fundamenteel van het type informatie dat verkregen wordt bij de interceptie van de inhoud van vertrouwelijke communicatie en vallen op grond van hun aard reeds niet onder dit begrip. (…) Het **enkele feit dat verkeersgegevens informatie verschaffen omtrent het communicatieproces**, is **onvoldoende** rechtvaardiging om aan dit type gegevens hetzelfde niveau van **grondwettelijke bescherming** te geven als **aan de communicatieinhoud** zelf.'[70]

Vervolgens nam de Tweede Kamer een amendement aan waarmee ook verkeersgegevens binnen de reikwijdte van artikel 13 Gw werden gebracht: naast het correspondentiegeheim zelf bevatte artikel 13 lid 1 ook 'het geheim van de gegevens met betrekking tot communicatie als bedoeld in de eerste volzin'.[71] Dit werd niet gemotiveerd in het amendement en de behandeling in de Tweede Kamer beperkte zich tot algemeenheden als: 'Verkeersgegevens zijn onzes inziens een intrinsiek onderdeel van de vertrouwelijkheid van

---

68 Van Dorst 1982, p. 288.
69 Ibid., p. 289.
70 *Kamerstukken II* 1996-97, 25 443, nr. 3, p. 3-4.
71 *Kamerstukken II* 1997-98, 25 443, nr. 13.

communicatie en zouden dus onder artikel 13 moeten vallen.'[72] De Eerste Kamer had echter grote moeite met het wetsvoorstel (hoewel niet primair vanwege het opnemen van verkeersgegevens[73]); het wetsvoorstel werd daarom ingetrokken.[74]

De Commissie-Franken sloot zich aan bij de redenering uit wetsvoorstel 25 443:

> 'De Commissie is van mening dat **onvoldoende rechtvaardiging** bestaat om onderscheid aan te brengen in het grondwettelijke beschermingsniveau tussen categorieën persoonsgegevens op grond van het feit dat **zij gerelateerd zijn aan een inhoud** die zelfstandig grondwettelijke bescherming geniet.'[75]

Het gaat volgens de commissie dus om de inhoud zelf en niet om aan de inhoud gerelateerde gegevens. Dit werd overgenomen in een in 2004 gepubliceerd concept-wetsvoorstel ter actualisering van artikel 13 Gw, die de volgende toelichting gaf over de ratio en reikwijdte:

> '**Vertrouwelijkheid van communicatie** vormt in een democratische rechtsstaat een zwaarwegend belang. Door de kwetsbaarheid van communicatie vormt een inbreuk op vertrouwelijke communicatie in de ogen van de regering een ernstige schending van de persoonlijke levenssfeer van betrokkenen, die een specifieke hoge mate van bescherming rechtvaardigt. (…) Anders dan hetgeen de Registratiekamer aangeeft in het rapport "Grondrechten in het digitale tijdperk", bestaat naar de mening van de regering onvoldoende rechtvaardiging om verkeersgegevens onder de specifieke bescherming van artikel 13 te brengen. Deze conclusie hangt samen met het feit dat **verkeersgegevens weliswaar in de informatiesamenleving veel over personen kunnen zeggen**, maar dat datzelfde geldt voor veel meer gevoelige gegevens, die ook niet onder de werking van artikel 13 vallen. De **inhoud van vertrouwelijke communicatie** is onder een, ook door de Tweede Kamer gewenst, **hoog beschermingsregime** gebracht: voor een beperking is een rechterlijke last vereist. Er zijn **geen goede argumenten** aan te voeren om een onderscheid aan te brengen in het grondwettelijke beschermingsniveau tussen categorieën persoonsgegevens **op grond van het feit dat zij al dan niet gerelateerd zijn aan een inhoud** die zelfstandig grondwettelijke bescherming geniet.'[76]

---

72 *Handelingen II* 14 januari 1998, 41-3351.
73 Asscher 2000.
74 *Kamerstukken II* 1998-1999, 25 443, nr. 40d.
75 Commissie Grondrechten in het digitale tijdperk 2000, p. 160.
76 Voorstel van wet, bijlage bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin, 29 oktober 2004, kenmerk 0000018194, p. 5, 10.

De Raad van State kon zich in dit onderdeel vinden, maar drong aan op een nadere toelichting:

> 'De Raad kan zich verenigen met de opvatting dat verkeersgegevens niet dienen te worden beschouwd als bestanddeel van de door artikel 13 beschermde vertrouwelijke communicatie. (…) De kernvraag moet zijn of voor het beschermen van verkeersgegevens behoefte bestaat aan een soortgelijk met extra waarborgen omgeven regime. **De strekking van artikel 13 is dat burgers zonder inmenging vertrouwelijk met elkaar kunnen communiceren.** Zou iemand weten of vermoeden dat **de overheid weet welke telefoongesprekken hij voert**, dan zou dat voor hem reden kunnen zijn om bepaalde gesprekken niet meer te voeren. Dit **doorbreekt de vertrouwelijkheid van de communicatie op zichzelf niet, maar raakt wel de vrijheid van (tele)communicatie**. De Raad adviseert de toelichting op de nu gemaakte keuze om de bijzondere bescherming van artikel 13 geen betrekking te laten hebben op verkeersgegevens, te verbeteren.'[77]

Hoewel niet helemaal duidelijk is wat hier bedoeld wordt, lijkt de Raad te vragen om een scherper onderscheid tussen de vertrouwelijkheid van communicatie (waarop verkeersgegevens geen inbreuk maken) en het recht of de vrijheid om vertrouwelijk te kunnen communiceren (waarop verkeersgegevens, in de zin van 'welke telefoongesprekken' iemand voert, wel inbreuk maken). Vermoedelijk komt dat overeen met het onderscheid tussen het correspondentiegeheim in enge zin (vertrouwelijkheid van communicatie als zodanig) en in ruime zin (het vertrouwelijk kunnen communiceren). De Raad van State laat de mogelijkheid open dat dit laatste ook door artikel 13 beschermd wordt, naast de bescherming van vertrouwelijke communicatie als zodanig.

Het wetsontwerp-2012 grondt in navolging van de commissie-Thomassen artikel 13 Gw op het belang van privé-communicatie:

> 'De Staatscommissie Grondwet omschreef het belang van de bescherming van privé-communicatie als "men moet in een democratische samenleving **vertrouwelijk met elkaar kunnen communiceren, zonder de angst dat de overheid meeluistert**."[78] Deze invulling van **het rechtens te beschermen belang**, dat schuilgaat achter het huidige artikel 13, sluit in onze optiek naadloos aan bij het rechtens te beschermen belang achter het brief- en telecommunicatiegeheim in onderhavig wetsvoorstel. Met privé-communicatie wordt bedoeld communicatie die niet voor het publiek toegankelijk is, anders dan door de verzender aangewezen. (…) De privé-communicatie wordt specifiek beschermd door artikel 13 en wordt separaat beschermd **omdat**

---

77 Advies Raad van State 24 januari 2002, bijgevoegd bij Brief van de Minister van Bestuurlijke Vernieuwing en Koninkrijksrelaties aan de Koningin 29 oktober 2004, kenmerk 0000018194, p. 6-7.

78 Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010, p. 85.

> **de inhoud van de communicatie privé behoort te blijven**. (…) Burgers kunnen immers alleen dan privé communiceren indien zij **niet bevreesd hoeven zijn voor heimelijke inzage door derden die zijn betrokken bij de overdracht of de opslag van de inhoud van de communicatie**.'[79]

De nadruk ligt hier wederom op de vertrouwelijkheid van communicatie: artikel 13 Gw beschermt tegen kennisneming van de inhoud, zowel door de communicatieaanbieder als door de overheid in brede zin.

Dat artikel 13 Gw beschermt tegen kennisneming van de inhoud van communicatie, blijkt ook uit de formuleringen waarmee de wetgever het correspondentiegeheim in wetgeving heeft vormgegeven. Bij post gaat het om het openen (en, naar men mag aannemen, vervolgens lezen) van brieven, blijkens onder andere artikel 23 Wiv 2002 ('De diensten zijn bevoegd tot het openen van brieven en andere geadresseerde zendingen') en artikel 101 Sv ('kennisneming van de inhoud der' 'inbeslaggenomen pakketten, brieven, stukken en andere berichten'). Bij telecommunicatie gaat het om het opnemen (en afluisteren) van telecommunicatie, aldus onder andere artikel 25 Wiv 2002 en artikel 126m/t/zg Sv, alsmede om het opvragen van 'gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn' (art. 126ng/ug/zo Sv), waarmee de inhoud van bij de communicatieaanbieder opgeslagen email of stempost wordt bedoeld.

Samenvattend: in de loop van de geschiedenis is de grondwetgever ervan uitgegaan dat artikel 13 Gw beschermt tegen kennisneming van de inhoud van communicatie door de transporteur, en in het verlengde daarvan de overheid (strafvordering of veiligheidsdiensten) die via de transporteur de inhoud zou kunnen vorderen; dit is het correspondentiegeheim in enge zin. Artikel 13 Gw biedt ook bescherming wanneer het inherent is aan het transport dat de transporteur kennis neemt van (een deel van) de inhoud van communicatie, de transporteur mag de inhoud dan niet doorvertellen aan derden; dit is het correspondentiegeheim in ruime zin. Van oudsher vallen verkeersgegevens volgens de grondwetgever niet onder de reikwijdte van artikel 13 Gw; bij de herzieningsvoorstellen in de afgelopen jaren is die lijn grotendeels doorgetrokken: het correspondentiegeheim beschermt tegen kennisname van de inhoud maar niet tegen kennisname van het communicatieproces.

---

[79] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 9-10.

## 2.2. Literatuur

Sinds Van Dorst in 1982 opmerkte dat de wetgever nergens een beschouwing had gegeven over de grondslag van het postgeheim,[80] heeft de wetgever wel indicaties gegeven van de ratio van het correspondentiegeheim, maar een scherp of consistent beeld schetst daarvan valt niet op te maken uit de wetsgeschiedenis. In de wijzigingsvoorstellen van de afgelopen decennia worden wisselende formuleringen gehanteerd die niet precies dezelfde grondslag voor beschermwaardigheid kennen: het belang van vertrouwelijke communicatie, het belang van vertrouwelijkheid van communicatie of het belang vertrouwelijk te kunnen communiceren. De focus op bescherming tegen kennisneming van de inhoud door de transporteur en/of overheid suggereert dat de vertrouwelijkheid van communicatie voorop staat, dat wil zeggen de vertrouwelijkheid van datgene wat wordt gecommuniceerd. Tegelijkertijd vallen in de commissierapporten en wetsvoorstellen van de afgelopen decennia ook de nodige uitspraken te lezen die het correspondentiegeheim plaatsen in de context van het belang om vertrouwelijk te kunnen communiceren of het belang van vertrouwelijke of privé-communicatie; bij die ratio past eerder dat de vertrouwelijkheid van het communicatieproces wordt beschermd, oftewel niet alleen datgene wat er wordt gecommuniceerd maar ook dat en hoe er wordt gecommuniceerd.

In de literatuur waarin gepoogd wordt het correspondentiegeheim te duiden, veelal afkomstig van de Amsterdamse school, is deze laatste benadering dominant. Hoewel er verschillende accenten voorkomen in de benadering van het correspondentiegeheim, gaan de auteurs er vrijwel steeds van uit dat de ratio van bescherming vooral gelegen is in de bescherming van het communicatieproces als geheel. In die benadering vallen ook verkeersgegevens onder de reikwijdte van de bescherming.

Volgens Hofman wordt niet alleen de communicatievorm, maar ook het communicatieproces beschermd door artikel 13 Gw.[81] Hij vindt daarvoor steun in de interpretatie die het Europees Hof van de Rechten de Mens heeft gegeven aan het begrip 'correspondence' uit artikel 8 EVRM: 'niet alleen het afluisteren van de inhoud is verboden, maar evenzeer het verzamelen van verkeersgegevens, die een "integral element" vormen van de communicatie per telefoon'.[82] Deze geïntegreerde benadering wordt op Europees niveau breed gedeeld, bijvoorbeeld door de Artikel 29 Werkgroep:

'The Article 29 Working Party has dealt with the privacy aspects of interception of communications in its recommendation 2/9956. In this recommendation, the Working Party points out that each interception of

---

80 Zie noot 59.

81 Hofman 1995, p. 149 en 462.

82 Ibid., p. 103, verwijzend naar EHRM 2 augustus 1984, *Malone t. Verenigd Koninkrijk*, App.no. 8691/79.

telecommunications, defined as a third party acquiring knowledge of the **content and/or traffic data** relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services, **constitutes a violation** of an individual's right to privacy and **of the confidentiality of correspondence**.'[83]

Volgens Dommering beschermt het correspondentiegeheim het kanaal als geheel:

> 'waar het om draait: het brief- en telefoongeheim beschermen de verzender van een boodschap tegen de kennisneming van de inhoud daarvan door degene die met de verzending is belast, of tegen degenen die via de transporteur toegang tot de verzonden boodschap zouden kunnen hebben. Het gaat daarbij niet om de inhoud van de boodschap. Deze kan strikt geheim zijn (een bedrijfsgeheim, een liefdesverklaring), maar ook juist bestemd zijn om openbaar te worden gemaakt (een artikel, een ingezonden brief). Het gaat om de vertrouwelijkheid van het communicatie*kanaal*: het brief- en postgeheim zijn in hun essentie klassieke onthoudingsrechten, die op de beheerders van netten en aanbieders van informatietransportdiensten de plicht leggen **zich te onthouden van een inmenging in de verzonden boodschap**.'[84]

In deze benadering ziet de bescherming

> 'niet alleen op de inhoud van de boodschap, maar ook op de adresseergegevens, ook wel aangeduid als "verkeersgegevens". Het waarnemen en opslaan van gegevens (bij elektronische communicatie regel) vormt mede een inbreuk op het recht.'[85]
> 'Het gaat bovendien niet alleen om verkeersgegevens. Ik noem de adressering op de enveloppe, inloggegevens omtrent de verzending en het ophalen van e-mail berichten, naar de identiteit van de opgebelde gespecificeerde telefoonrekeningen en andere uitsluitend door het transport gegenereerde persoonsgegevens. Ik zou ze alle willen toerekenen aan het transportgeheim. Naar analogie van het Duitse recht zou men kunnen spreken van het *Auskunftverbot* (als pendant van het *Eindringeverbot*), het verbod feiten mee te delen over de omstandigheden van verzending. Hetgeen betekent dat ze alleen binnen de beperkingen van het transportgeheim aan derden kunnen worden verstrekt.'[86]

De ratio hiervan wordt goed verwoord door Asscher:

---

83 Article 29 Working Party 2000, p. 35.
84 Dommering 1997, p. 117.
85 Dommering 2000, p. 72.
86 Dommering 1997. In vergelijkbare zin: Studiecommissie VMC 1999, p. 6-7.

> 'Terwijl artikel 10 Grondwet ziet op de bescherming van de persoonlijke levenssfeer, ziet het transportgeheim op **de betrouwbaarheid van het communicatiekanaal**. Geheimhouding van verkeersgegevens dient deze betrouwbaarheid. Het gaat er dan ook niet zo zeer om dat verkeersgegevens veel over personen kunnen zeggen, belangrijker is dat **het vertrouwen dat de burger stelt in het communicatiekanaal** kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor **doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst**. Wanneer de burger er rekening mee moet houden dat wordt bijgehouden met wie hij wanneer en hoe lang communiceert en vervolgens deze informatie buiten het kader van de dienst voor allerlei doeleinden wordt verwerkt, zal hij niet meer **vrij kunnen communiceren**.'[87]

Dit sluit aan bij de visie die Van Dorst al in 1982 formuleerde op het correspondentiegeheim in ruime zin:

> 'Eigenlijk zou de grens al eerder, dus nog vóór het bekend maken van ambtelijk verkregen informatie, getrokken moeten worden, in dier voege dat het de ambtenaar verboden zou dienen te zijn van meer kennis te nemen dan voor de richtige vervulling van de hem opgedragen taak noodzakelijk is. (…) De bescherming die de burger aldus – op indirecte wijze – wordt geboden heeft dus **niet zozeer de geheimhouding van de inhoud** van de door hem gevoerde correspondentie ten doel, **maar meer de geheimhouding van alle feiten die noodzakelijkerwijs samenhangen met of noodzakelijkerwijs voortvloeien uit het gebruik van openbare diensten**. Te denken valt in dit verband aan informatie met betrekking tot de vraag of iemand met een ander in contact staat, met wie, waarover, etc., welke gegevens voor de vraagsteller zeer onthullend zouden kunnen zijn.'[88]

Volgens Steenbruggen is de ratio van het correspondentiegeheim dat het

> 'als een vooruitgeschoven **verdedigingslinie voor zowel het recht op privacy als de communicatievrijheid** functioneert. Als zodanig beschermt het grondrecht de vertrouwelijkheid van persoonlijke communicatie. (…) Bijkomende ratio is dat de burger ervan uit moeten [sic] kunnen gaan dat hij zijn **communicatie *veilig*** aan een aanbieder van openbare post en telecommunicatiediensten **kan toevertrouwen**.'[89]

In deze literatuur wordt aldus een visie op het correspondentiegeheim neergezet waarin de ratio van bescherming is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Gegeven die ratio ligt het voor de hand de reikwijdte van het correspondentiegeheim zich te laten uitstrekken over het communicatieproces als geheel. Het correspondentiegeheim – in ruime zin

---

87 Asscher 2003, p. 24.
88 Van Dorst 1982, p. 290.
89 Steenbruggen 2009, p. 69.

– omvat dan ook verkeersgegevens, omdat kennisneming van het communicatieproces door de overheid via de transporteur een inbreuk maakt op de vrijheid om vertrouwelijk te kunnen communiceren.

## 2.3. Afbakening van het begrip 'inhoud'

Hoewel de dominante visie in de literatuur een bredere reikwijdte hanteert dan de wetgever door ook verkeersgegevens onder de bescherming van het correspondentiegeheim te brengen, lost deze benadering het probleem van de afbakening van inhoud tegenover verkeersgegevens niet op. Het feit dat verkeersgegevens onder het correspondentiegeheim (zouden moeten) vallen, wil namelijk niet zeggen dat ze op dezelfde wijze beschermd moeten worden als inhoud.[90] Zoals de wetgever van 1983 heeft erkend dat er een karakterverschil bestaat tussen communicatievormen naar gelang het meer of minder vanzelfsprekend is dat de transporteur ter uitvoering van het transport kennis neemt van de inhoud, zo bestaat er een karakterverschil tussen het correspondentiegeheim in enge zin (dat een sterke werking heeft) en het correspondentiegeheim in ruime zin (dat een zwakkere werking heeft). Dat karakterverschil komt goed tot uiting in het historische gegeven dat de strafvorderlijke bevoegdheid tot het opvragen van verkeersgegevens aanvankelijk ook inhoud van telefoongesprekken omvatte, voor zover de telefoonoperator daarvan kennis had genomen bij het doorverbinden van het gesprek.[91] Met de automatisering van de telefonie was er geen operationele reden meer voor de operator om mee te luisteren (behalve het incidenteel inluisteren voor technische controle), waardoor de inhoud een vertrouwelijker karakter kreeg en verschoof naar het correspondentiegeheim in enge zin. Dit geeft aan dat er een afbakening nodig is, wellicht niet zozeer tussen inhoud en verkeersgegevens, maar vooral tussen gegevens waarvan de transporteur niet uit de aard van zijn functie kennis hoeft te nemen (waarvoor het sterkere correspondentiegeheim in enge zin geldt) en gegevens waarbij dat wel het ge-

---

[90] Vgl. bijvoorbeeld ibid., p. 56-57: 'Gelet op het bovenstaande zijn er goede gronden om de bescherming van verkeersgegevens en de bescherming van de inhoud van communicatie ineen te schuiven. (…) Dat betekent niet per definitie dat verkeersgegevens in alle gevallen dezelfde bescherming als de inhoud van communicatie moeten krijgen.'

[91] Een instructie bij de dienstorder van 29 december 1925 die diende om de bepalingen uit het nieuwe Wetboek van Strafvordering aan de ambtenaren der PTT ter kennis te brengen, gaf het volgende aan: 'De ambtenaren zijn eveneens verplicht aan den Officier van Justitie op diens vordering op grond van bovengenoemd artikel van het W. Sv. [art. 100, het latere art. 125f en huidige art. 126n, bjk] de door deze gewenschte inlichtingen te verstrekken terzake van alle telefonisch verkeer (*dus ook omtrent den inhoud der telefoongesprekken*, voor zoover de ambtenaar daarvan zonder schending van de ambtsplicht heeft kunnen kennis nemen)' (cursivering toegevoegd). INSTRUCTIE, behoorend bij dienstorder no. 831 van 29 December 1925 van het Hoofdbestuur der Posterijen en Telegrafie. Zie hierover Koops 2002, p. 118-119.

val is (waarvoor het zwakkere correspondentiegeheim in ruime zin geldt). In het huidige communicatielandschap heeft dit onderscheid een sterke parallel met het onderscheid tussen inhoud en verkeersgegevens.

Aangezien zowel wetgever als de literatuur hoofdzakelijk een onderscheid maken tussen inhoud en verkeersgegevens, waarbij in elk geval de inhoud van communicatie op een sterke bescherming kan rekenen en open gelaten wordt welke bescherming de verkeersgegevens zouden moeten krijgen, rijst de vraag wat nu precies onder inhoud valt. Hierover valt geen expliciete uitspraak te vinden in wetsgeschiedenis of literatuur. Indirecte aanknopingspunten kunnen worden gevonden in de precieze formulering die auteurs gebruiken om aan te duiden wat wel en niet onder 'inhoud' valt.

MacGillavry omschrijft inhoudelijke gegevens als 'gegevens die inzicht geven in de werkelijke inhoud van de communicatie'.[92] Hij omschrijft echter niet wat 'de werkelijke inhoud is'; mogelijk gaat het om de letterlijke inhoud van het bericht, maar mogelijk ook om de hermeneutische inhoud van de boodschap. Verkeersgegevens omschrijft hij als gegevens die informatie geven over het gebruik van de diensten van de ISP door de gebruiker.[93] De Commissie-Franken geeft evenmin een omschrijving van inhoud; zij stelt dat verkeersgegevens geen betrekking hebben op de inhoud van het gegevensverkeer maar dat zij 'gerelateerd zijn aan een inhoud die zelfstandig grondwettelijke bescherming geniet.'[94] Dit betekent dat verkeersgegevens niet zelf inhoud zijn maar in een zekere verhouding staan tot inhoud. Dat zou kunnen betekenen dat gegevens die een zeker inzicht geven in de inhoud maar niet letterlijk zelf tot de inhoud behoren, onder verkeersgegevens en niet onder inhoud vallen; de formulering kan echter ook simpelweg een meer technische aanduiding zijn van verkeersgegevens als zijnde meta-gegevens, zonder iets te zeggen over het feit of verkeersgegevens al dan niet samenhangen of tot op zekere hoogte samenvallen met inhoud.

Het wetsontwerp-2012 is iets explicieter in dit opzicht. Het ontwerp maakt een onderscheid tussen de technische kwalificatie en de juridische kwalificatie:

> 'De inhoud van de communicatie is overigens nog te onderscheiden van de **gegevens die worden gegenereerd** met betrekking tot de totstandkoming, de duur en het tijdstip van de communicatie. Deze gegevens worden hierna geduid als verkeersgegevens (…) Deze gegevens behoren niet primair tot het belang dat artikel 13 beoogt te beschermen, omdat zij **niet de inhoud van het bericht weergeven**. Niet kan worden uitgesloten dat zij daarvan **wel deel uitmaken indien zij nauw verband houden met de inhoud** van het bericht.'[95]

---

92 MacGillavry 2004, p. 231.
93 Ibid., p. 225.
94 Commissie Grondrechten in het digitale tijdperk 2000, p. 160.
95 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 12.

> 'Aandacht verdient evenwel dat de inhoud van telecommunicatie in technische zin soms ook als een verkeersgegeven wordt gezien. Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp **betrekking heeft op de inhoud** van de e-mail. Een ander voorbeeld is een sms-bericht: technisch gezien is een dergelijk bericht in zijn geheel een verkeersgegeven, maar juridische gezien omvat een sms-bericht – naast verkeersgegevens – tevens de inhoud van communicatie. De conclusie is dat aan de bescherming van artikel 13 niet kan afdoen dat gegevens die de inhoud van communicatie betreffen in technische zin als een verkeersgegeven worden beschouwd. **Verkeersgegevens die niet mede betrekking hebben op de inhoud van telecommunicatie vallen echter buiten de reikwijdte** van artikel 13.'[96]
> 'Ook voor verkeersgegevens die geheel of ten dele mede betrekking hebben op de inhoud van de communicatie, zoals de onderwerpregel van een e-mail en de in een internetzoekmachine ingevoerde zoekterm (…), geldt dat deze slechts [met rechterlijke machtiging] mogen worden gevorderd. (…) Als verkeersgegevens zijn krachtens de artikelen 126n, 126u en 126zh Sv (in het Besluit vorderen gegevens telecommunicatie) alleen **gegevens** aangewezen **die niet geheel of ten dele mede op de inhoud van de communicatie betrekking** hebben.'[97]

In deze passages worden drie licht verschillende formuleringen gebruikt voor de afbakening van verkeersgegevens en inhoud. Gegevens vallen onder inhoud als zij 'nauw verband houden met', 'mede betrekking hebben op' dan wel 'geheel of ten dele mede betrekking hebben op' de inhoud van communicatie. Het laatste criterium sluit aan bij de afbakening die Koops in 2003 maakte in de strafvorderlijke bevoegdheden:

> 'Een goed uitgangspunt hierbij is dat indien gegevens worden opgevraagd **die deels (hoe weinig ook) inhoud** van telecommunicatie **betreffen**, deze moeten vallen onder de telecomtap en niet onder de bevoegdheid van verkeersgegevens.'[98]

Deze formulering is potentieel zowel ruimer als beperkter dan die in wetsontwerp-2012. Het biedt een zo ruim mogelijke reikwijdte van de inhoud, door te expliciteren dat zodra gegevens ook maar enig deel van de inhoud betreffen, deze onder de bescherming van inhoud vallen; het wetsontwerp-2012 kan op deze manier worden geïnterpreteerd, maar laat ook de

---

96 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 17-18.

97 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 32. Vgl. ook het criterium zoals Steenbruggen 2009, p. 337 het formuleert in zijn voorstel voor een nieuw art. 13 Gw: verkeersgegevens worden als inhoud beschermd als zij '**mede betrekking hebben op de inhoud van de communicatie**'.

98 Koops 2003, p. 69.

mogelijkheid open dat gegevens ten minste voor een substantieel deel de inhoud moeten betreffen. Aan de andere kant is de formulering van Koops wat beperkter omdat het gaat om verkeersgegevens die inhoud 'betreffen', terwijl het wetsontwerp spreekt van gegevens die 'betrekking hebben op' inhoud. Hoewel de begrippen nauw verwant zijn, lijkt mij 'betreffen' een directere relatie aan te duiden dan 'betrekking hebben op'. In die lezing lijkt de formulering van Koops beperkt tot verkeersgegevens die zelf onderdeel uitmaken van de inhoud, terwijl de formulering van wetsontwerp-2012 de interpretatiemogelijkheid biedt om ook verkeersgegevens onder inhoud te laten vallen als zij een aanduiding geven van de (globale) inhoud maar niet zelf, letterlijk, deel uitmaken van de inhoud. Dit interpretatieverschil geeft aan dat het nodig is om meer greep te krijgen op wat precies het nauwe verband moet zijn van verkeersgegevens met inhoud om ze onder de bescherming van inhoud te brengen, maar ook op wat dan precies de 'inhoud zelf' is van een bericht waartoe verkeersgegevens in dat nauwe verband staan.

Fischer is de enige die een poging gedaan heeft een materiële omschrijving te geven van wat de inhoud van communicatie is. Hij definieert inhoud (*content data*) als:

> 'data for which the intermediary service provider is (conditionally) exempted from liability: data in a state of mere conduit, caching or hosting.'[99]

Dit lijkt op het eerste oog een wat merkwaardige omschrijving van het begrip 'inhoud van communicatie', omdat het is ontleend aan een juridische formulering betreffende de aansprakelijkheid van Internetaanbieders. De achterliggende gedachte van de aansprakelijkheidsuitsluiting is dat Internetaanbieders over het algemeen niet aansprakelijk zijn voor de inhoud van communicatie van hun gebruikers, tenzij zij zich die inhoud hebben eigen gemaakt en er daardoor mede verantwoordelijk voor zijn geworden. Dit biedt daarom een interessant aanknopingspunt voor het antwoord op de vraag wat onder 'inhoud' van communicatie moet worden volstaan: inhoud is datgene waarvoor de transporteur (in zijn rol van transporteur)[100] niet verantwoordelijk is. Of positief geformuleerd: inhoud is datgene wat valt onder de verantwoordelijkheid van de verzender.

Op deze manier kan inhoud functioneel worden afgebakend ten opzichte van verkeersgegevens, die dan gegevens zijn die wel vallen onder de verantwoordelijkheid van de transporteur. Dit zijn gegevens 'die betrekking hebben

---

99 Fischer 2010, p. 29-30.

100 Vgl. art. 54a Sr: 'Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt *als zodanig* niet vervolgd indien (…)'; de woorden 'als zodanig' betekenen dat hij onder bepaalde voorwaarden niet vervolgd wordt *als tussenpersoon*, maar mogelijk wel als (mede-)inhoudsaanbieder.

op de overdracht of op de opslag van het bericht'[101] of 'inlichtingen omtrent de wijze van totstandkoming en afwikkeling van het telecommunicatieverkeer'.[102] Ze worden ook wel aangeduid als 'inhoudloze transmissiegegevens'[103] of 'verbindingsgegevens'[104]. Een kernkarakteristiek van verkeersgegevens is dat de communicatiedeelnemer alleen invloed kan uitoefenen op het verkeersgegeven door haar communicatiegedrag aan te passen (bijvoorbeeld door een bepaald nummer niet te bellen, of op een ander tijdstip), maar geen controle heeft over de uiteindelijke inhoud van de verkeersgegevens.[105] Dit sluit goed aan bij de conceptualisering van Fischer dat inhoud onder de verantwoordelijkheid van de communicatiedeelnemer valt, omdat zij daar controle over kan uitoefenen.

Bepaalde omschrijvingen van verkeersgegevens leggen de nadruk op het feit dat de verkeersgegevens niet afkomstig zijn van de verzender maar door de transporteur zelf worden gegenereerd:

> 'de **gegevens die worden gegenereerd** met betrekking tot de totstandkoming, de duur en het tijdstip van de communicatie'.[106]

> '"verkeersgegevens" [zijn] computergegevens die verband houden met een met behulp van een computersysteem gevoerde communicatie, en **worden voortgebracht door een computersysteem** dat een onderdeel vormt van de communicatieketen, en de herkomst, de bestemming, de route, de tijd, de datum, de omvang, de duur of de aard van de betrokken dienst aanduiden.'[107]

De telecommunicatiewetgeving hanteert een wat ruimere definitie dan transportgegevens door ook gegevens die nodig zijn voor facturering onder de definitie te laten vallen: 'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan'.[108] In meer algemene zin kunnen verkeersgegevens daarom ook worden omschreven als

> 'alle feiten die noodzakelijkerwijs samenhangen met of noodzakelijkerwijs voortvloeien uit het gebruik van openbare [post- of telecommunicatie] diensten'.[109]

---

101 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 16.
102 HR 7 september 2004, LJN AO9090.
103 Smits 2006, p. 4.
104 Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010, p. 89.
105 Smits 2006, p. 404n.
106 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 12.
107 Art. 1(d) Cybercrime-Verdrag.
108 Art. 2(b) Richtlijn 2002/58/EG.
109 Van Dorst 1982, p. 290. In vergelijkbare zin Asscher 2003, p. 24, die spreekt over een inbreuk op het correspondentiegeheim wanneer 'verkeersgegevens worden verwerkt voor **doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst**.'

Voor een functionele specificering van welke gegevens noodzakelijk zijn voor de transporteur om zijn dienst te kunnen leveren, biedt Fischer een nuttig raamwerk. Fischer definieert verkeersgegevens aanvankelijk als 'data just processed for the provider's good reasons',[110] wat hij vervolgens nader uitwerkt in een preciezere definitie:

> 'Traffic data: electronic personal data on the actual use of the network **processed by intermediary service providers for three essential functions in three types of services**.
> The essential data processing functions of the intermediary service provider are:
> 1. service performance: data processing to carry out the service agreement with the user;
> 2. service accounting: data processing for billing and verification of the service;
> 3. service management: data processing for traffic management and network maintenance.
> The three types of services of the intermediary service provider are:
> 1. mere conduit: the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network;
> 2. caching: the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request;
> 3. hosting: the storage of information provided by a recipient of the service.'[111]

Volgens Fischer biedt dit een bruikbare juridische conceptualisering van het begrip verkeersgegevens, die het mogelijk maakt dit begrip te operationaliseren in de technische werkelijkheid. Om te bepalen of een gegeven een verkeersgegeven is, kan Fischers 3x3-test worden uitgevoerd: als het gegeven wordt verwerkt voor een van de drie essentiële functies van een van de drie typen dienstaanbieders, kan het worden gekwalificeerd als verkeersgegeven. Een waterdichte afbakening met inhoud biedt dat niet, omdat het denkbaar is dat bepaalde gegevens in de 3x3-matrix vallen maar ook onder Fischers definitie van inhoud, bijvoorbeeld als een webmailaanbieder een bericht opslaat terwijl iemand hem genotificeerd heeft dat de onderwerpsregel daarvan strafrechtelijk beledigend (art. 266 Sr) voor de ontvanger is.

---

[110] Fischer 2010, p. 23.
[111] Ibid., p. 30.

## 2.4. Conclusie

Het correspondentiegeheim bestaat uit een kern – het correspondentiegeheim in enge zin – die beschermt tegen kennisneming door de transporteur van communicatie (en door derden via hem) van de inhoud van communicatie. Het correspondentiegeheim kent tevens een periferie – het correspondentiegeheim in ruime zin – die beschermt tegen doorvertellen door de transporteur aan derden van kennis over (de inhoud van) communicatie waarvan hij voor de uitoefening van het transport kennis heeft genomen. Of het correspondentiegeheim in ruime zin ook beschermd wordt of zou moeten worden door artikel 13 Gw is niet eenduidig te bepalen. De wetgever heeft in de wetsgeschiedenis en de wijzigingsvoorstellen van de laatste jaren de nadruk gelegd op kennisneming van de inhoud van communicatie; artikel 13 Gw beschermt in die visie niet de vertrouwelijkheid van het communicatieproces maar alleen de vertrouwelijkheid van de inhoud van de communicatie die via een communicatiekanaal wordt getransporteerd. In de literatuur over de ratio van artikel 13 Gw domineert de visie dat dit artikel de vertrouwelijkheid van het communicatieproces beschermt, en daarmee de vrijheid om privé te kunnen communiceren; het correspondentiegeheim beschermt dan ook de gegevens die samenhangen met dat proces (wat overigens niet wil zeggen dat verkeersgegevens aanspraak zouden moeten maken op hetzelfde beschermingsniveau als inhoud). De wetgever lijkt deze laatste interpretatie niet te willen omarmen, hoewel diverse uitspraken over de ratio van het correspondentiegeheim wel spreken van de behoefte om de vrijheid om vertrouwelijk te kunnen communiceren te beschermen, wat wijst in de richting van bescherming van het gehele communicatieproces. In die zin lijkt er, anders dan in de literatuur van de Amsterdamse school, aan de interpretatie van de wetgever geen systematische visie ten grondslag te liggen over de ratio van het correspondentiegeheim.

Wat daar ook van zij, belangrijk is in elk geval wel dat het correspondentiegeheim in ruime zin onder de reikwijdte van artikel 13 Gw dient te vallen waar het de inhoud van communicatie betreft waarvan de aanbieder ter uitoefening van zijn functie kennis heeft genomen. Zou dat niet zo zijn, dan zou namelijk de grondwetsbepaling niet techniekonafhankelijk zijn; het zou er dan immers van afhangen hoe de aanbieder het communicatieproces inricht of een verzender aanspraak kan maken op het correspondentiegeheim: als de telefonieaanbieder om wat voor reden dan ook zou besluiten terug te gaan naar een schakelcentrale met een telefoonjuffrouw (zodat de operator bij de uitoefening van het transport veelal kennis neemt van de communicatie), zou de grondwettelijke bescherming van het telefoongesprek komen te vervallen. Dat kan niet de bedoeling zijn, nu het nadrukkelijk de intentie is om artikel 13 techniekonafhankelijk vorm te geven.[112] Daarom beschermt

[112] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 5.

artikel 13 Gw de inhoud van communicatie zowel in enge als in ruime zin.

Wat er daarbij onder 'inhoud' van communicatie moet worden verstaan, is niet expliciet af te leiden uit wetsgeschiedenis of literatuur. De enige materiële omschrijving van het begrip 'inhoud' in de literatuur, van Fischer, geeft echter wel een zinvol aanknopingspunt om gegevens te kwalificeren: onder inhoud kan worden verstaan datgene wat onder verantwoordelijkheid van de verzender valt, terwijl verkeersgegevens die gegevens zijn die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Deze categorieën sluiten elkaar niet volledig uit, maar de omschrijving verheldert wel wat de kern is van inhoud en van verkeersgegevens.

Voor de gevallen waarin er overlap bestaat, is de vraag wanneer verkeersgegevens als inhoud moeten worden behandeld: dat is het geval als zij, geheel of ten dele, (mede) betrekking hebben op de inhoud of (een deel van) de inhoud zelf betreffen. Wat onder 'betrekking hebben op' of 'betreffen' moet worden verstaan, is echter niet duidelijk. Het zou kunnen gaan om gegevens die in letterlijke zin deel uitmaken van de inhoud van de boodschap – dus een deel van de boodschap *zijn* – maar het zou ook kunnen gaan om gegevens die inzicht geven in (een deel van) de boodschap – dus *over* de boodschap *gaan* zonder zelf deel uit te maken van de boodschap.

Een functionele interpretatie van het criterium 'gegevens die (mede) betrekking hebben op de inhoud' zou, gelet op de ratio van bescherming, vermoedelijk meer in de richting van het laatste wijzen. De ratio van het correspondentiegeheim is immers, in de meest recente formulering van de wetgever, dat burgers 'vertrouwelijk met elkaar kunnen communiceren, zonder de angst dat de overheid meeluistert'[113] 'omdat de inhoud van de communicatie privé behoort te blijven.'[114] Het 'meeluisteren' zou, zoals hierboven aangegeven, niet alleen de letterlijke inhoud moeten omvatten, maar ook het doorvertellen van de inhoud door de aanbieder, en bij dit doorvertellen gaat het niet per se om het letterlijk citeren maar om het doorgeven van de (globale) inhoud van het bericht. Ook het doorvertellen van een deel van de inhoud zonder de hele inhoud te onthullen zou onder de bescherming moeten vallen; voor de angst van burgers dat de overheid meeluistert maakt het immers niet principieel uit of de overheid integraal of selectief meeluistert.

Op basis van bovenstaande analyse kan de eerste onderzoeksvraag als volgt worden beantwoord: de 'inhoud' van communicatie is deel van de communicatie dat valt onder de verantwoordelijkheid van de verzender (en niet van de transporteur). Gelet op de ratio van bescherming door artikel 13 Gw vallen hieronder ook gegevens die de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender.

---

[113] Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010, p. 85.

[114] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 9-10.

# 3. Grijze gebieden tussen verkeersgegevens en inhoud

In de literatuur alsook in de wijzigingsvoorstellen van de afgelopen jaren wordt regelmatig opgemerkt dat de scheidslijn tussen verkeersgegevens en inhoud soms moeilijk te trekken valt of vervaagt, dan wel dat het onderscheid anderszins aan relevantie verliest.

> 'Een andere belangrijke vraag betreft de huidige en toekomstige status van een aantal specifieke groepen gegevens zoals de "subject line" van een email of de bezochte webadressen en de omgang met zoekvragen. Hoe je die informatie, die in technische zin tot de verkeersgegevens behoort, maar die in feite veel over de inhoud vertelt, dient te behandelen, is in toenemende mate onduidelijk.'[115]

Bij surfgegevens, zoekvragen en de onderwerpsregel in een emailbericht vervaagt het onderscheid tussen verkeersgegevens en inhoud. Daarnaast wordt ook vaak gewezen op locatiegegevens en de opkomst van *data mining*, die de relevantie van het onderscheid ter discussie stellen. In dit hoofdstuk worden de grijze gebieden tussen verkeersgegevens en inhoud verkend door een overzicht te geven van alle voorbeelden die in de literatuur worden genoemd.

## 3.1. Surfgegevens

### *3.1.1. Algemeen*

De Artikel 29 Werkgroep geeft aan dat surfgegevens – de gegevens over welke webpagina's iemand heeft bezocht, oftewel de URL's[116] – verkeersgegevens zijn maar als inhoud moeten worden behandeld:

> 'In principle, this Article [artikel 5 van de voorloper van Richtlijn 2002/58/EG over vertrouwelijkheid van communicatie, bjk] refers to the content of the communication. The distinction between traffic data and content is not, however, easy to apply in the context of the Internet, and certainly not when referring to surfing. Surfing data could in principle be regarded as traffic data. However, the Working Party thinks that surfing through different sites should be seen as a form of communication and as such should be covered by the scope of application of Article 5.

---

115 Asscher en Ekker 2003, p. 104.

116 Zie http://nl.wikipedia.org/wiki/Uniform_Resource_Locator (geraadpleegd 1 oktober 2013) en Deel 1, par. 4.6.1.

> The surfing behaviour of an Internet user (navigation data) visiting different websites can in itself reveal a lot about the communication taking place. By knowing the names of the websites visited, one can in most cases gain a fairly accurate picture of the communication which has taken place. Furthermore, it is then **straightforward** for anyone armed with the traffic data **to** visit the site and **see exactly what content was accessed**.
>
> The Working Party thinks, therefore, that the surfing data of an Internet user **should receive the same level of protection as "content"**. This form of communication should therefore remain confidential. In this sense *click-streams* can be considered as falling within the scope of application of this Article.
>
> The new proposal for a revised directive defines "traffic data" in Article 2.1c): *"traffic data" shall mean any data processed in the course of or for the purpose of the transmission of a communication over an electronic communications network.* Navigation data would therefore fall within this definition and be considered as traffic data.
>
> The revision of this Directive has brought major improvements by extending the scope of Article 5 to cover not just the content of the communication but also the related traffic data. By giving equal protection to content and related traffic data **the (sometimes difficult) distinction between these concepts becomes less important**. The Working Party welcomes this improvement.'[117]

Hoewel de Werkgroep hierin stelt dat surfgegevens zonder meer op het niveau van inhoud moeten worden beschermd, is het rapport niet helemaal consistent; even verderop staat dat surfgegevens *mogelijk* hetzelfde beschermingsniveau moeten krijgen.[118] Ook MacGillavry formuleert het voorzichtig:

> 'Geconstateerd kan worden dat deze gegevens mede informatie over de inhoud van het berichtenverkeer geven. Met deze gegevens kan namelijk de bezochte pagina worden opgeroepen, zodat de inhoud van de bezochte pagina kan worden achterhaald. Om deze reden moeten dergelijke gegevens mogelijk ook als inhoudelijke gegevens worden beschouwd.'[119]

---

[117] Article 29 Working Party 2000, p. 50.

[118] 'Processing of header information (which might also include data on the content of the packets) should be considered as traffic data in the sense of Article 6 of Directive 97/66/EC (…)The list of websites visited by an Internet user (surfing behaviour) must in all cases be considered as traffic data (and *possibly* be given the same protection as content). Above all, this list should in principle be erased upon termination of the Internet session' (cursivering toegevoegd). Ibid., p. 51.

[119] MacGillavry 2004, p. 231.

Arno Smits geeft in zijn dissertatie over aftappen en verkeersgegevens een uitgebreide analyse van http-informatie en merkt op dat surfgegevens 'veelal communicatieve elementen bevatten'.[120] Het gaat daarbij echter niet zozeer om het feit dat surfgegevens direct samenhangen met inhoud, maar dat ze veel blootgeven over de interessesfeer, meer dan bij telefoonnummers (bijvoorbeeld als je een pizzeria of een escortservice belt) het geval is. Surfgegevens geven 'veel meer informatie over communicatiegedrag'.[121] Hij pleit daarom voor een heroverweging van de manier waarop dit type verkeersgegevens juridisch worden beschermd. Volgens hem kunnen IP-nummers (die het webdomein aangeven, bijvoorbeeld rijksoverheid.nl) als louter contactinformatie worden beschouwd en daarom als 'klassieke' verkeersgegevens worden behandeld, maar alle andere onderdelen van surfgegevens zouden meer juridische bescherming moeten krijgen dan klassieke verkeersgegevens (waarbij hij overigens in het midden laat of dat hetzelfde beschermingsniveau als communicatie-inhoud moet zijn).[122]

Volgens Koops hebben surfgegevens aanvullende bescherming nodig, niet zozeer omdat ze de interessesfeer blootgeven maar omdat 'een internetadres vaak direct [wijst] op de inhoud die wordt overgedragen.'[123] Ook Fischer vindt om deze reden dat surfgegevens extra bescherming nodig hebben; het zijn immers verkeersgegevens

> 'that link particular information contents to requesting individual users, while simultaneously revealing the nature of that content. In terms of sensitivity this is an important difference with regular traffic data, which in general do not disclose the content of the communication.'[124]

De (strafvorderlijke) wetgeving behandelt surfgegevens momenteel echter niet als inhoud, maar als verkeersgegeven:

> 'Ook de aanduiding van een website of een pagina binnen een website kan vallen onder het begrip verkeersgegevens. Een website en de pagina's binnen een website beschikken over een eigen nummer. Deze gegevens **geven inzicht in de belangstellingssfeer** van de gebruiker van telecommunicatie. Meer in het algemeen kan worden gesteld dat verkeersgegevens informatie kunnen opleveren over de soort instanties die benaderd worden door de gebruiker van telecommunicatie. Dit geeft informatie over de belangstellingssfeer van de gebruiker, net zoals zijn contacten met personen en instanties informatie over hem geven. Het **betreft echter niet het kennis nemen van (de inhoud van) de vertrouwelijke communicatie** van de gebruiker.'[125]

---

120 Smits 2006, p. 419.
121 Ibid.
122 Ibid., p. 399-400.
123 Koops 2003, p. 68-69. In gelijke zin Steenbruggen 2009, p. 56.
124 Fischer 2010, p. 35.
125 *Kamerstukken II* 2001/02, 28 059, nr. 3, p. 7.

Men zou deze redenering kunnen lezen als een formalistische interpretatie van het begrip inhoud van communicatie, in de zin dat een Internetadres niet de boodschap is maar een adresgegeven waar de boodschap vandaan gehaald moet worden; dat is formalistisch, omdat het in principe een peulenschil is om met het adresgegeven de inhoud van wat er gecommuniceerd is (de inhoud van de opgevraagde webpagina) te achterhalen, zoals de Artikel 29 Werkgroep aangeeft. (Waarbij overigens aangetekend moet worden dat in het huidige Internetlandschap een Internetpagina veelal samengesteld wordt uit allerlei onderdelen, die lang niet altijd zijn te construeren aan de hand van een URL.) Een wellicht meer plausibele lezing (aangezien inhoud tussen haakjes staat) is dat de (strafproces)wetgever hier de nadruk legt op het feit dat Internetpagina's publiek zijn en dus niet vertrouwelijk zijn; de inhoud van opgevraagde Internetpagina's is dus geen vertrouwelijke communicatie en zou om die reden niet onder het communicatiegeheim vallen. Om die reden vindt Patijn ook dat surfgegevens een sui generis-categorie vormen:

> 'Verder omvat de informatie omtrent de bezochte pagina tevens informatie over de inhoud van de communicatie die heeft plaatsgevonden. (…) Ik bepleit de daarop betrekking hebbende verkeersgegevens aan te merken als een categorie sui generis. Gegevens over surfgedrag missen het neutrale karakter van verkeersgegevens bij de klassieke telefonie. Aan de andere kant betreft de uit de verkeersgegeven kenbare inhoud van de communicatie geen vertrouwelijke communicatie. De inhoud van een website is immers openbaar.'[126]

Vanwege het niet-neutrale karakter zouden verkeersgegevens niet als 'klassieke' verkeersgegevens moeten worden behandeld, maar vanwege het openbare karakter van webpagina's zouden ze ook niet als inhoud van (vertrouwelijke) communicatie moeten worden behandeld; vandaar Patijns pleidooi voor een sui generis-benadering. In de visie van de opstellers van het wetsontwerp-2012 is het echter niet relevant of de gegevens die via Internet worden verzonden publiek of privaat van aard zijn; het gaat om de gerichtheid van de communicatievorm, niet om het karakter van de inhoud. In de termen van het verkeersstromenmodel valt onder het correspondentiegeheim niet alleen de communicatie van een individu met een individueel informatiebestand (conversatie), maar ook communicatie van een individu met een centraal informatiebestand (consultatie).[127] Ook 'het opvragen van informatie bij een geautomatiseerde beldienst of internetdienst [wordt] vanwege [de] gerichtheid beschermd door artikel 13.'[128] Dat consultatie beschermwaardig is, blijkt ook uit het feit dat *video-on-demand* onder de reikwijdte van artikel 13 Gw valt.[129]

---

[126] Patijn 2004, p. 135.
[127] Zie over het verkeersstromenmodel hieronder, par. 4.3, en Deel 1, par. 2.4.4.
[128] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 15.
[129] Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 16.

De kernvraag is dus niet of surfgegevens samenhangen met de inhoud van *vertrouwelijke* communicatie, maar of surfgegevens *dusdanig nauw* samenhangen met de inhoud van (niet-vertrouwelijke maar wel beschermde) communicatie dat zij als inhoud bescherming verdienen. Vaak is er een direct verband tussen een Internetadres en de inhoud die wordt overgedragen; door het Internetadres in te tikken ziet men immers de inhoud van de webpagina. Hoewel webpagina's in toenemende mate dynamisch worden, zijn er nog steeds veel (relatief) statische webpagina's (dat wil zeggen, waarvan de inhoud over langere tijd niet of weinig verandert), terwijl ook dynamische webpagina's vaak wel een deel inhoud bevatten dat relatief stabiel is. Aldus is het vaak eenvoudig om uit de URL de inhoud af te leiden van communicatie die van een webpagina naar een gebruiker is verstuurd. Het ligt daarom voor de hand om surfgegevens als inhoud te behandelen.

*3.1.2. Zoekmachinesurfgegevens*

Een bijzondere subcategorie van surfgegevens zijn surfgegevens van zoekmachines. Daarin is namelijk veelal de zoekterm opgenomen. 'Internetadressen kunnen bij zoekopdrachten ook inhoud (de zoektermen) bevatten.'[130] Jan Smits geeft hiervan het voorbeeld:[131]

> https://www.google.nl/webhp?sourceid=chrome-instant&rlz=1C1SKPC_enNL341&ion=1&ie=UTF-8#hl=nl&tbo=d&rlz=1C1SKPC_enNL341&sclient=psy-ab&q=**internetconsultatie**%20**artikel**%20**13**%20**grondwet**&oq=&gs_l=&pbx=1&fp=39b63b13594cdc97&bpcl=39650382&ion=1&bav=on.2,or.r_gc.r_pw.r_qf.&biw=1280&bih=933

waarin de zoekterm 'internetconsultatie artikel 13 grondwet' (hier **vet** weergegeven) is opgenomen. Naast het feit dat dit een surfgegeven is dat een direct verband houdt met de inhoud die wordt gecommuniceerd (van Google naar Jan Smits), bevat het ook letterlijk de inhoud van de communicatie van Jan Smits aan Google. Omdat het letterlijk de inhoud van communicatie weergeeft, zou het als inhoud moeten worden behandeld.[132] (Daarbij kan wel worden aangetekend dat het verkeersgegeven niet de inhoud bevat van de communicatie waar het betrekking op heeft – dat is namelijk de Internetpagina met de zoekmachineresultaten – maar de inhoud van een eerdere communicatie, namelijk de zoekvraag die voorafging aan de communicatie waar het verkeersgegeven betrekking op heeft. Dat is een aandachtspunt wanneer de wetgever de reikwijdte van artikel 13 Gw precies moet omschrijven, maar het lijkt mij als zodanig geen afbreuk te doen aan de beschermwaardigheid onder artikel 13. Het verkeersgegeven bevat immers inhoud van communicatie.)

---

130 Koops 2003, p. 68.
131 Deel 1, par. 4.6.2.
132 Zo ook Smits 2006, p. 399.

Overigens moet er wel een onderscheid worden gemaakt tussen de zoekterm (die inhoud is maar geen verkeersgegeven) en de URL waarin de zoekterm is opgenomen (die een verkeersgegeven is dat inhoud bevat). Dat onderscheid wordt niet altijd scherp gemaakt:

> 'De *URL* die de zoekopdracht bevat kan als verkeersgegeven worden gezien. Maar evengoed valt te verdedigen dat *de opdracht* aan de zoekmachine een "communicatie" is, en dus als inhoud geclassificeerd moet worden.'[133]

De tweede zin staat in principe los van de eerste zin, omdat het om verschillende objecten gaat; de auteur bedoelt echter – neem ik aan – dezelfde objecten aan te duiden. Ook het wetsontwerp is niet consistent door 'de in een internetzoekmachine ingevoerde zoekterm' te bespreken *als een verkeersgegeven*, dat bescherming als inhoud verdient omdat het geheel of ten dele mede betrekking heeft op de inhoud van de communicatie.[134] Bedoeld wordt hier de URL waarin de zoekterm is weergegeven.

Overigens onderscheidt de lagere wetgever bij mijn weten surfgegevens van zoekmachines niet als een aparte categorie. In de strafvordering worden zoekmachinesurfgegevens daarom behandeld als surfgegevens en daarmee (zie par. 3.1) als verkeersgegeven en niet als inhoud. Ze vallen in het Besluit vorderen gegevens telecommunicatie onder 'het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft (…) gehad'.[135] In tegenstelling tot wat het wetsontwerp-2012 stelt,[136] zijn naar huidig recht in de strafvordering dus wel verkeersgegevens aangewezen die betrekking hebben op inhoud, maar niet als inhoud worden behandeld. Wanneer zoekmachinesurfgegevens, zoals de kennelijke bedoeling is van het wetsontwerp-2012, wel als inhoud onder artikel 13 Gw behandeld moeten worden, zal (de interpretatie van) de lagere wetgeving in dit opzicht dus aangepast moeten worden.

Voor de praktijk hoeft dat niet onoverkomelijk te zijn; het is in beginsel technisch eenvoudig om, door een filter te gebruiken, in een lijst met bezochte Internetadressen zoekresultaten van de meest gebruikte zoekmachines uit te sluiten. Opmerking verdient daarbij echter dat ook gewone webpagina's middels een zoekfunctie laten zien waarop binnen de pagina is gezocht. Zo levert het zoeken op de webpagina van BZK op de zoekterm 'grondwet' de volgende URL op:

> http://www.rijksoverheid.nl/zoeken?zoeken-op=**grondwet**

---

133 Hes 2003, p. 16 (cursivering toegevoegd).

134 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 32.

135 Art. 2 onder c Besluit vorderen gegevens telecommunicatie, *Stb.* 2004, 394.

136 'Als verkeersgegevens zijn krachtens de artikelen 126n, 126u en 126zh Sv (in het Besluit vorderen gegevens telecommunicatie) alleen **gegevens** aangewezen **die niet geheel of ten dele mede op de inhoud van de communicatie betrekking** hebben.' Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 32.

Het zal daarom, wanneer zoekmachinesurfgegevens moeten worden behandeld als inhoud, niet voldoende zijn om URL's van (bekende) zoekmachines uit een lijst met verkeersgegevens te verwijderen. In plaats daarvan kan wel bijvoorbeeld de padnaam – het gedeelte van een URL dat volgt na het protocol (bijvoorbeeld http://) en domein (bijvoorbeeld google.nl/) – worden verwijderd, of het gedeelte dat volgt na een '?', omdat zoekvragen in een URL meestal na een vraagteken worden weergegeven.[137]

*3.1.3. Surfgegevens met inloggen*

Een URL is niet alleen opgebouwd uit een protocol (bijvoorbeeld http, https of ftp), een domeinnaam (bijvoorbeeld rijksoverheid.nl) en een padnaam (bijvoorbeeld /documenten-en-publicaties/rapporten/2010/11/11/rapport-staatscommissie-grondwet.html), maar kan ook een poortnummer (zie par. 3.7) bevatten. Daarnaast is het ook mogelijk om authenticatiegegevens mee te geven aan een URL, zodat automatisch ingelogd kan worden. De URL is namelijk opgebouwd als volgt:[138]

http://user:pass@voorbeeld.com:poortnummer/padnaam?zoekvraag#fragment

Jan Smits geeft een voorbeeld van een URL waarin een inlognaam is meegegeven:[139]

http://kroonf8@gmail.com:V6XE7F@www.tql.nl

Deze URL, die uit een logbestand afkomstig is, bevat het emailadres (kroonf8@gmail.com) en het (versleutelde) wachtwoord (V6XE7F)[140] van een gebruiker die op de webpagina www.tql.nl inlogt.

Het hangt er enigszins van af hoe de authenticatiegegevens in de URL terechtkomen of het inhoud van een concrete communicatiehandeling (namelijk het versturen van inlognaam en wachtwoord) betreft, of dat het een automatisch geïntegreerd proces van een webpaginabezoek + inloggen betreft. In het eerste geval zijn de authenticatiegegevens vergelijkbaar met zoekmachinesurfgegevens: ze bevatten rechtstreeks inhoud van een (direct

---

137 Zie http://nl.wikipedia.org/wiki/Uniform_Resource_Locator (geraadpleegd 1 oktober 2013).

138 http://nl.wikipedia.org/wiki/Uniform_Resource_Locator (geraadpleegd 1 oktober 2013).

139 Deel 1, par. 4.6.3. Letterlijk luidt de URL http://kroonf3%40gmail%2Ecom:V6XE7F@www.tql.nl/, ik heb voor het leesgemak hierin de hex codes die binnen URL's worden gebruikt (zie http://www.obkb.com/dcljr/charstxt.html (geraadpleegd 1 oktober 2013)) vervangen door hun karakter (%40 is een apenstaart, %2E is een punt).

140 Dit is het wachtwoord in versleutelde vorm, maar het kan wel worden gebruikt om in te loggen op de webpagina.

voorafgaande) communicatie. In het laatste geval zijn de authenticatiegegevens niet letterlijk inhoud van communicatie, maar ze betreffen wel duidelijk gegevens die onder verantwoordelijkheid van de verzender en niet onder die van de transporteur vallen. Het lijkt me ook evident dat dit type gegevens onder de ratio van het correspondentiegeheim bescherming als inhoud van communicatie verdient.

*3.1.4. Conclusie*

Bij surfgegevens in het algemeen is er vaak een direct verband tussen een Internetadres (URL) en de inhoud die wordt overgedragen; door het Internetadres in te tikken ziet men immers de inhoud van de webpagina. Surfgegevens zouden om die reden als inhoud moeten worden behandeld. Daarnaast geldt dat er specifieke onderdelen van surfgegevens zijn die wel rechtstreeks inhoud van communicatie afbeelden: in een URL die hoort bij een zoekopdracht staat veelal ook de zoekterm opgenomen, terwijl het ook mogelijk is dat een URL authenticatiegegevens bevat waarmee iemand inlogt op een webpagina. Hoewel het technisch mogelijk is om deze laatste typen gegevens uit te filteren uit een overzicht van bezochte webpagina's, versterkt het voorkomen van inhoud in URL's wel de algemene conclusie dat surfgegevens vaak direct verbonden kunnen worden met de inhoud van communicatie. Het ligt daarom meer voor de hand om alle surfgegevens integraal als inhoud te behandelen, dan om technische filters te gebruiken die bepaalde inhoudelijke onderdelen uit URL's filteren.

## 3.2. Email-onderwerpsveld

Het onderwerpsveld in een emailbericht is een van de duidelijkste voorbeelden van het grijze gebied tussen verkeersgegevens en inhoud:

> 'Hoe je die informatie [zoals de 'subject line' van een email], die in technische zin tot de verkeersgegevens behoort, maar die in feite veel over de inhoud vertelt, dient te behandelen, is in toenemende mate onduidelijk.'[141]

> 'Enerzijds lijkt het, naar de vorm, een verkeersgegeven, aangezien het over het netbericht gaat; anderzijds duidt het ook de inhoud aan, en wel zodanig dat het zelf als inhoud zou kunnen worden beschouwd. Veel netberichten hebben immers onderwerpen als "afspraak 20/8?" of "Norton SystemWorks 2002 Professional - 70% OFF - $29.99 with FREE UPS Ground Shipping! OptInFreebies Mailing List Member". (…) Het onderwerpsveld moet (…) beschouwd worden als inhoud'.[142]

---

[141] Asscher en Ekker 2003, p. 104.
[142] Koops 2003, p. 77-78.

> 'Voor wat betreft de onderwerpsregel in een mailbericht geldt dat het hier onmiskenbaar om gegevens met communicatieve elementen gaat. In sommige gevallen zal een onderwerpsregel zelfs het eigenlijke communicatiebericht inhouden.'[143]

Een voorbeeld van dat laatste is een (verder leeg) emailbericht waarvan de onderwerpsregel luidt: 'Goed interview op radio 1 ! Groeten, Ruud'.

Het wetsontwerp-2012 schaart de onderwerpsregel dan ook zonder meer onder de inhoud van communicatie:

> 'Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp betrekking heeft op de inhoud van de e-mail.'[144]

Het kwalificeren van de onderwerpsregel als inhoud ligt ook voor de hand vanuit de in hoofdstuk 2 gegeven omschrijving van inhoud als datgene wat onder de verantwoordelijkheid van de afzender valt. De onderwerpsregel wordt vrijelijk gekozen door de verzender en de transporteur is er niet (als transporteur) aansprakelijk voor.

### 3.3. Sms-bericht

Een ander voorbeeld van een verkeersgegeven dat direct inhoud betreft, is een sms-bericht. Hiervoor geldt dan ook hetzelfde als voor de onderwerpsregel van een emailbericht:

> 'technisch gezien is een dergelijk bericht in zijn geheel een verkeersgegeven, maar juridisch gezien omvat een sms-bericht – naast verkeersgegevens – tevens de inhoud van communicatie.'[145]

Het is evident dat een sms-bericht onverkort als inhoud moet worden behandeld, aangezien de keuze voor de tekst van het sms-bericht geheel bij de verzender ligt.

### 3.4. Telefoon-keuzemenu's

Een minder vaak aangehaald voorbeeld van een grijs gebied betreft gegevens die worden gegenereerd in telefoon-keuzemenu's:

---

143 Smits 2006, p. 420.
144 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 18.
145 Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 18.

> 'Bij sommige geautomatiseerde telefoongesprekken geven verkeersgegevens veel inhoud weer ("wilt u informatie over seksueel overdraagbare aandoeningen, toets 1, wilt u een medische controle aanvragen, toets 2, wilt u een inenting, toets 3").'[146]
> '*Wij kunnen U sneller van dienst zijn indien U nu Uw BurgerServiceNummer intoetst:*
> De beller toetst: *123456789*
> Elk cijfer kent een andere toon; die tonen en daarmee de cijfers worden door de opgeroepene herkend en opgeslagen en vervolgens als sleutel gebruikt voor een zoekvraag in een database. Het systeem antwoordt terug:
> *Goedemiddag Meneer Smits waarmee kan de fiscus U van dienst zijn.*
> *1) Aanvragen van een VAR DGA*
> *2) Aanvragen van VAR WUO*
> *3) Aanvragen van een VAR*
> *Wanneer U geen keuze maakt wordt U zo spoedig mogelijk door een medewerker te woord gestaan.*'[147]

In technische zin gaat het hier om een grijs gebied tussen verkeersgegevens en inhoud. Het indrukken van toetsen ten behoeve van keuzemenu's betreft tweetonige signalen dan wel, bij moderne mobiele telefoons een aparte functie, die worden verzonden nadat de verbinding tot stand is gekomen. Ze worden daarom normaliter niet als zodanig gegenereerd of geregistreerd door de transporteur, maar alleen door de verzender en ontvanger. Tegelijkertijd zijn de ingetoetste nummers wel zichtbaar in het leesvenster van het ontvangende toestel, en in die zin betreft het wel in technische zin verkeersgegevens.[148]

Vanuit de functionele benadering van inhoud gaat het duidelijk om inhoud, aangezien de afzender en niet de transporteur bepaalt of er een 2 of een 8 wordt ingetoetst. Ook is de transporteur niet verantwoordelijk voor de inhoud van het keuzemenu, dat is namelijk de gesprekspartner van de beller. In die zin lijken de keuzetonen op een URL: het is een vorm van consultatie waarbij de centrale dienst gegevens aanbiedt en de beller een keuze maakt tussen deze gegevens. De gegenereerde gegevens (beltonen) vormen daarbij evenals de URL veelal een directe indicatie van de inhoud die wordt overgedragen (mijn BSN is 123456789; ik wil informatie over seksueel overdraagbare aandoeningen). Dat is overigens alleen zo als de beltonen in verband (kunnen) worden gebracht met het keuzemenu (anders is een getallenreeks betekenisloos), maar dat zal in beginsel vaak het geval zijn omdat de overheid of een andere derde het telefoonnummer kan bellen en zelf het keuzemenu kan uitluisteren.

---

146 Koops 2003, p. 68n.
147 Deel 1, par. 4.1.1 (cursief in origineel).
148 Ibid.

### 3.5. Emailadres

In de literatuur wordt ook een enkele keer gewezen op de mogelijkheid dat een emailadres inhoud kan bevatten. Bij webmail kunnen immers zelf adressen worden aangemaakt, zoals jaikkomnaarpetersfeestje@yahoo.com,[149] die een indicatie bevatten van de inhoud van berichten die naar dat adres worden toegestuurd. Ook is het tegenwoordig gebruikelijk bij Internettoegangsabonnementen dat gebruikers zelf vijf of tien emailadressen kunnen aanmaken, waarbij ze bijvoorbeeld adressen kunnen genereren als janjansen@aanbieder.nl, janjansen-zakelijk@aanbieder.nl, blondejan@aanbieder.nl, janwilseks@aanbieder.nl en postzegelverzamelaar@aanbieder.nl. Op zich hebben deze adressen niet als zodanig betrekking op communicatie, maar ze kunnen wel samenhangen met de communicatie die via die adressen verloopt. Zo zal het adres janwilseks@aanbieder.nl vermoedelijk alleen voor communicatie over seksafspraakjes worden gebruikt, terwijl een bericht van of aan postzegelverzamelaar@aanbieder.nl allicht over postzegels zal gaan. De samenhang met de inhoud van concrete berichten is hier echter veel minder nauw dan bij de onderwerpsregel van email en het adres geeft hooguit een zeer globale aanduiding van de vermoedelijke inhoud van communicatie. Alleen webmailadressen die voor een specifiek doel zijn aangemaakt, zoals jaikkomnaarpetersfeestje@yahoo.com, hangen tamelijk nauw samen met de (globale) inhoud van communicatie. Of een bericht een aanmelding of afmelding bevat (of spam) valt echter niet uit het emailadres af te leiden – tenzij bekend is dat er een parallel adres neeikkomhelaasnietnaarpetersfeestje@yahoo.com is aangemaakt.

Als zodanig is er dan ook geen directe reden om emailadressen als inhoud te behandelen. Echter, vanuit de functionele omschrijving van inhoud als datgene waarvoor de afzender en niet de transporteur verantwoordelijk is, zouden veel emailadressen tegenwoordig wel aangemerkt kunnen worden als inhoud. De keuze voor het adres (voor de apenstaart) ligt immers bij de gebruiker, niet bij de transporteur. En de keuze voor een bepaald emailadres heeft niet zelden een communicatieve functie, namelijk het profileren van de identiteit van de gebruiker – zoals bij blondejan@aanbieder.nl of kattenliefhebber@aanbieder.nl het geval is. In het kader van de vrijheid om vertrouwelijk te kunnen communiceren zou in het digitale tijdperk ook het communicatieve aspect van identiteitsconstructie via de keuze van een emailadres beschermd kunnen worden.

Dat staat overigens wel ver af van hoe tot nu toe in de literatuur en in de wetsgeschiedenis aangekeken wordt tegen het correspondentiegeheim. Men kan er ook voor kiezen deze vorm van identiteitsconstructie te beschermen

---

[149] Koops 2003, p. 68n. Dit voorbeeld werd ontleend aan de werkelijkheid: het emailadres behoorde bij de verdediging van de dissertatie Blok 2002.

via het algemene privacy- en dataprotectierecht,[150] waarbij in aanmerking moet worden genomen dat zelfgekozen emailadressen ook gevoelige persoonsgegevens kunnen bevatten, zoals ijsbrandgroenlinks@aanbieder.nl, dovejanjansen@aanbieder.nl of leerfetisjist@aanbieder.nl. Gezien de inhoudelijke component die emailadressen tegenwoordig hebben, moet de wetgever zich in elk geval afvragen of emailadressen nog simpelweg als (inhoudsloze) identificerende gegevens mogen worden beschouwd die door elke opsporingsambtenaar mogen worden gevorderd zonder bevel van een officier van justitie (art. 126na/ua/zi Sv).

## 3.6. Informatienummers en naambellen

Informatienummers *(premium rate numbers)* zijn telefoonnummers die voor bepaalde diensten worden gebruikt en veelal een andere prijsstructuur hebben, zoals 0800- en 0900-nummers.[151] Vroeger had men de nummers 002 en 003 om respectievelijk de tijd en het weerbericht op te vragen. Bij deze laatste nummers kan men uit de verkeersgegevens – nummer + tijd – vrijwel exact de inhoud afleiden. Bij 0800- en 0900-nummers is dat niet zo, behalve als bekend is dat een bepaald nummer geautomatiseerde berichten geeft volgens een vast patroon.

Daarnaast zijn er 0906-nummers voor erotische diensten en 0909-nummers voor amusement, spelletjes en prijsvragen. Uit de contactgegevens kan niet de precieze inhoud worden afgeleid, maar het nummer geeft wel een globale indicatie van de inhoud. Dat geldt ook voor sommige niet-geografische nummers, zoals 112 (alarmnummer) en 144 (meldpunt dierenmishandeling).

Ook bij het zogeheten naambellen[152] kan op basis van het gebelde nummer worden vermoed waar het gesprek globaal over gaat. Wie 0900-PIZZA belt, zal vermoedelijk een pizza bestellen, en wie 0900-NOTARIS belt, wil vermoedelijk iets juridisch regelen. Er kan echter niet worden afgeleid om welke pizza's of rechtshandelingen het gaat.

Informatienummers en naambellen zijn vergelijkbaar met zelfgekozen emailadressen (zie par. 3.5): ze hebben tot op zekere hoogte betrekking op de inhoud van communicatie en ze vallen – door de keuze voor een specifiek nummer of nummertype – onder verantwoordelijkheid van de gesprekspartner en niet van de transporteur. Ze betreffen echter niet de inhoud zelf en meestal (behoudens bij geheel geautomatiseerde nummers als 003) kan ook niet meer dan de globale context van de inhoud worden afgeleid uit het nummer. Systematisch valt er iets voor te zeggen om ze als inhoud te behandelen omdat de keuze van de betekenisvolle gegevens niet bij de transporteur maar

---

150 Vgl. Agre 1998, Hildebrandt 2008.

151 Zie http://nl.wikipedia.org/wiki/Informatienummer (geraadpleegd 1 oktober 2013).

152 Zie onder http://nl.wikipedia.org/wiki/Naambellen#Gebruik_van_letters (geraadpleegd 1 oktober 2013).

bij de gesprekspartners ligt, maar evenals bij emailadressen staat dat ver af van hoe tot nu toe in de literatuur en in de wetsgeschiedenis aangekeken wordt tegen het correspondentiegeheim.

### 3.7. Poortnummers

Applicaties op Internet maken gebruik van verschillende poortnummers, zodat pakketjes op de juiste plaats op de bestemmingscomputer worden afgeleverd voor gebruik door de desbetreffende applicatie. Er zijn vele duizenden poortnummers, waarvan zo'n 1200 specifiek zijn toegewezen.[153] Zo wordt poort 104, evenals poorten 2761, 2762, 11112 gebruikt voor het Dicomprotocol (Digital Imaging and Communications in Medicine), waarmee informatie wordt uitgewisseld met of over medische afbeeldingen.[154] Poorten 3305 en 6619 worden gebruikt voor OFTP (Odette File Transfer Protocol), een protocol voor EDI (gestandaardiseerde uitwisseling van bedrijfsinformatie), poort 9212 voor het Financial Information eXchange-protocol, en poort 43594 voor het online multispelerspel RuneScape.[155]

Voor poortnummers geldt hetzelfde als voor informatienummers: ze geven een globale indicatie van de context waarin de communicatie plaatsvindt. Anders dan bij informatienummers ligt de keuze voor de koppeling van een bepaald poortnummer aan een bepaalde applicatie niet bij de communicatiepartners, maar bij de transporteur (in ruime zin: Internetstandaardiseringsorganisaties). Het zijn dus verkeersgegevens, maar ze geven wel een indicatie van het globale onderwerp van communicatie, bijvoorbeeld dat een medische scan wordt verstuurd of dat een gebruiker het spel RuneScape (en niet het spel Club Penguin Disney, waarmee poortnummer 6113 verbonden is) speelt.

### 3.8. Presentmelding

Bij diverse applicaties voor het onderhouden van contacten, wordt bij aanmelden en afmelden een bericht verzonden aan de contactpersonen (waarvoor de gebruiker toestemming heeft te geven om zijn aan- of afmelding te melden). Voorbeelden zijn MSN, Skype en WhatApp.[156] De melding van het apparaat van de gebruiker aan de apparaten van de contactpersonen wordt automatisch gegenereerd, maar dit gebeurt door de programmatuur van de eindgebruiker en niet door programmatuur van de transporteur. Het bericht

---

153 http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (geraadpleegd 1 oktober 2013).

154 http://en.wikipedia.org/wiki/Dicom (geraadpleegd 1 oktober 2013).

155 Zie http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (geraadpleegd 1 oktober 2013) en Deel 1, par. 4.7.2.

156 Zie ibid., p. 36.

met de strekking 'Jan Jansen is online' is dus communicatie die wordt beschermd onder het communicatiegeheim. Aan de verkeersgegevens van het bericht valt mogelijk de inhoud af te leiden, als het identificeerbaar is vanuit welke applicatie een bericht is verstuurd. In combinatie met tijdstip, zeker als de verkeersgegevens over een bepaalde periode bekend zijn waardoor communicatiepatronen zichtbaar worden, zal dan duidelijk zijn dat de verzender de boodschap 'ik ben online en sta open voor communicatie' dan wel 'ik meld me af' heeft verstuurd.

## 3.9. Internet der dingen

In het Internet der dingen[157] (dat nog in ontwikkeling is maar wel dichterbij komt) hebben allerlei objecten een identificerende chip, voorzien van een IPv6-adres, die draadloos in verbinding staat met het Internet.[158] Zo kan de koelkast doorgeven aan de supermarkt dat er melk geleverd moet worden, of een vuilnisbak op straat aan de vuilnisdienst dat hij bijna vol zit. Sensoren in de kleding kunnen lichaamsfuncties monitoren en automatisch doorgeven, bijvoorbeeld aan een webdienst die statistieken over iemands hardlopen en gezondheid bijhoudt, of aan een alarmnummer als de hartslag en bloeddruk boven kritische drempels uitgaan. Wanneer bekend is dat een IP-adres behoort bij een koelkast, vuilnisbak of trainingspak, zal men globaal het onderwerp van de communicatie kunnen afleiden uit de verkeersgegevens. Het zal onbekend zijn wat een trainingspak precies doorgeeft aan de aanbieder van een gezondheids-app, maar het zal in elk geval meetresultaten van lichaamsfunctioneren betreffen. Vanwege de specificiteit van objecten in het Internet der dingen zal het verband tussen verkeersgegevens en inhoud vaak nauwer zijn dan bij communicatie via naambellen of poortnummers het geval is. Het betreft evenwel niet de letterlijke inhoud, maar hooguit het onderwerp en eventueel de strekking van communicatie.

## 3.10. Locatiegegevens

Een aanbieder van mobiele telefonie moet weten waar een mobiele telefoon zich bevindt, om een gesprek of bericht door te kunnen geleiden. Daarom worden in het netwerk – als de telefoon aan staat – doorlopend locatiegegevens gegenereerd: de telefoon meldt zich bij de dichtstbijzijnde zendmast, die de locatie van de telefoon doorgeeft aan dienstaanbieder. Wanneer iemand met een mobiele telefoon daadwerkelijk communiceert, wordt ook het gegeven meegestuurd via welke zendmast de communicatie verloopt. Deze gegevens vallen onder de verantwoordelijkheid van de telecomaanbieder en zijn, volgens het Europese telecommunicatierecht, dus verkeersgegevens:

---

[157] Zie http://en.wikipedia.org/wiki/Internet_of_things (geraadpleegd 1 oktober 2013).
[158] Zie Deel 1, par. 4.8.2.

> 'In digitale mobiele netwerken worden locatiegegevens betreffende de geografische positie van de eindapparatuur van de mobiele gebruiker verwerkt om de transmissie van de communicatie mogelijk te maken. Dergelijke gegevens zijn verkeersgegevens'.[159]

Locatiegegevens worden vaak genoemd in literatuur over de privacy van telecommunicatie. Deels gaat dat over de vraag of locatiegegevens die worden gegenereerd wanneer een toestel in de paraatstand staat, wel of niet verkeersgegevens zijn; ze hangen immers niet samen met een concrete belhandeling en vallen daarom niet altijd onder de juridische definities van verkeersgegeven.[160] De vraag of locatiegegevens, voor zover ze verkeersgegevens zijn (dus wanneer ze samenhangen met een concrete communicatiehandeling), ook inhoud kunnen betreffen, komt echter niet aan de orde in de literatuur.

Auteurs bespreken meer in het algemeen de privacygevoeligheid van locatiegegevens. Arno Smits merkt op dat een mobiele telefoon als peilbaken kan gaan fungeren, zeker als de mobiele telefoon veel wordt gebruikt.[161] Vanwege de grotere privacygevoeligheid zouden locatiegegevens van mobiele telefoons volgens hem dan ook alleen met rechterlijke machtiging moeten kunnen worden opgevraagd.[162] Koops wijst op 'verfijnde' locatiegegevens die samenhangen met toegevoegdewaardediensten (zoals bedoeld in art. 9 Richtlijn 2002/58/EG), dat wil zeggen precieze locatiegegevens op basis van bijvoorbeeld driehoeksmeting.

> 'Zeker bij toegevoegdewaardediensten kan dit meer informatie opleveren, bijvoorbeeld wanneer iemand automatisch aanbiedingen op zijn mobiele toestel ge-sms't krijgt van de restaurants of supermarkten waar hij langs rijdt. Justitie kan dan op basis van de verkeersgegevens bijvoorbeeld een nauwkeurige route bepalen waar iemand heeft gereden.'[163]

Volgens Fischer kunnen verkeersgegevens daarom soms privacygevoeliger zijn dan de inhoud van communicatie:

> 'It is possible for traffic data to surpass the sensitivity of the communication content. Such can be the case with location data, a form of traffic data in mobile telephony. The telephone conversation (communication content) may be insignificant, but the relating location data may reveal a person's whereabouts, which are sometimes significant.'[164]

---

159 Richtlijn 2002/58/EG, overweging 35.
160 Zie Hes 2003, p. 37; Ekker 2003, p. 46; Asscher en Ekker 2003, p. 106; Smits 2006, p. 386.
161 Smits 2006, p. 369-370.
162 Ibid., p. 386.
163 Koops 2003, p. 82.
164 Fischer 2010, p. 5n .

De literatuur geeft aldus blijk van een bezorgdheid over de bescherming van locatiegegevens, vanwege het inzicht dat deze kunnen bieden in de verblijfplaatsen en bewegingspatronen van personen. Het belang van bescherming daarvan heeft echter niet primair te maken met de vrijheid om onbevangen privé te kunnen communiceren, maar meer met het algemene belang van privacy in het licht van de bewegingsvrijheid. Niettemin bestaat er wel een correlatie met het correspondentiegeheim. Vanuit de ratio die Asscher formuleerde – 'het vertrouwen dat de burger stelt in het communicatiekanaal kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van deze dienst'[165] – kan het verwerken van locatiegegevens voor andere doeleinden een verkillend effect hebben op de vrijheid van burgers te communiceren. Iemand zou zich bijvoorbeeld geremd kunnen voelen om te bellen wanneer hij zich in het gebied van de Amsterdamse Wallen bevindt, of wanneer een werknemer met een mobiele telefoon van het bedrijf een polikliniek bezoekt voor een medische klacht die hij (vooralsnog) voor de baas verborgen wil houden.

Het feit dat locatiegegevens beschermwaardig zijn vanuit de ratio van het correspondentiegeheim, staat echter los van de vraag of zij (alleen) verkeersgegevens zijn of (ook) inhoud. Hoewel de literatuur locatiegegevens niet koppelt aan de inhoud van communicatie, zal er in sommige gevallen wel een bepaald verband bestaan tussen een locatiegegeven en de (vermoedelijke) inhoud van een bericht. In het voorbeeld van de toegevoegdewaardediensten, zal het voor de hand liggen dat een sms van Albert Heijn aan een gebruiker die wordt verstuurd op een plaats en tijd dat de gebruiker zich binnen een straal van 500 meter van een Albert Heijn bevindt, een boodschap bevat over die Albert Heijn-vestiging en met een paar aanbiedingen van de week. Ook de inhoud van een sms-bericht van restaurant De Lange Muur aan een gebruiker van een toegevoegdewaardedienst die om 18:05 op de hoek van de straat van het restaurant rijdt, laat zich globaal raden. Met hoge waarschijnlijkheid weet men waarover een sms gaat die verzonden is in de nabijheid van De Grolsch Veste 30 seconden nadat Castaignos gescoord heeft. In het algemeen zal het echter minder waarschijnlijk zijn dat globaal uit tijd en plaats is af te leiden waarover een bepaalde communicatie ging. Duidelijk is echter wel dat in diverse gevallen – zeker als er verkeersgegevens over een langere periode beschikbaar zijn waaruit patronen zijn af te leiden – er een zekere correlatie kan bestaan tussen locatiegegevens (in combinatie met tijdstip) en de vermoedelijke globale inhoud van een communicatie.

## 3.11. Data mining

Door middel van *data mining* kunnen grote databestanden worden doorzocht om verbanden te vinden. Dit levert nieuwe kennis op, die met de groei

---

[165] Asscher 2003, p. 24; zie noot 87 en bijbehorende tekst.

van de informatiesamenleving in toenemende mate een gedetailleerd beeld van het persoonlijk leven van individuen kan betreffen.[166] Toegepast op verkeersgegevens kan *data mining* ook veel kennis opleveren.

Steenbruggen betoogt daarom dat de vooronderstelling dat inhoud per definitie gevoeliger is dan verkeersgegevens, nuancering behoeft. Op grond van verkeersgegevens kunnen 'door derden uitermate gedetailleerde communicatie- en interesseprofielen van gebruikers worden opgesteld. Onder omstandigheden kan deze informatie veel gevoeliger zijn dan de uitgewisselde informatie zelf.'[167] Hofman geeft daar een voorbeeld van: uit een bepaald communicatiepatroon zou bijvoorbeeld afgeleid kunnen worden dat mevrouw Y een verhouding heeft met de chef. 'Hieruit blijkt dat ook verkeersgegevens direct of indirect zeer gevoelig kunnen zijn met het oog op de persoonlijke levenssfeer.'[168]

Ekker geeft aan dat men door het koppelen van verkeersgegevens aan andere data men niet alleen veel te weten komen over het communicatiegedrag van personen en hun feitelijk handelen, maar soms ook over de inhoud van de communicatie.[169]

> 'Soms kan zodoende worden vastgesteld wat (ongeveer) de inhoud van de communicatie is geweest:
> - Alice heeft gebeld met haar advocaat, haar psycholoog, het ziekenhuis, de nummerinformatie van de PTT, de Sociale Dienst, het Bureau Kredietregistratie, of het alarmnummer van de brandweer.
> - Alice heeft ingelogd op de website van Alcoholics Anonymous en deelgenomen aan een chatsessie.
> - Alice heeft ingelogd op de website van de gemeente Amsterdam en op een bulletin-board kritiek geuit op het parkeerbeleid van de gemeente.
> - Alice heeft van de website van een politieke partij het partijprogramma gedownload en een folder besteld waarmee zij lid kan worden van die partij.[170]
>
> (…) Daarnaast kunnen verkeersgegevens iets zeggen over de inhoud van communicatie wanneer men ze combineert met andere informatie. Hieruit volgt een belangrijke constatering: informatie over het communicatiegedrag van individuen en soms ook de inhoud van de communicatie kan worden verkregen door verkeers- en persoonsgegevens met elkaar te combineren.'[171]

Met andere woorden, diverse van de hierboven geschetste grijze gebieden, waarbij verkeersgegevens een globale indicatie kunnen geven van de inhoud, worden nog grijzer wanneer verkeersgegevens gecombineerd worden

---

166 Zie algemeen Hildebrandt en Gutwirth 2008.
167 Steenbruggen 2009, p. 56-57.
168 Hofman 1995, p. 51.
169 Ekker 2003, p. 47.
170 Ibid., p. 48.
171 Ibid.

met andere databestanden. De combinatie van gegevens kan de interpretatie van wat bepaalde verkeersgegevens over de inhoud van een bepaalde communicatie vertellen, aanscherpen dan wel waarschijnlijker maken. Het koppelen van verkeersgegevens met andere politiegegevens in het kader van opsporing is niet onderworpen aan een rechterlijke machtiging (zie art. 11 WPolG). Van belang is daarbij dat de politie (evenals de veiligheidsdiensten) via openbrononderzoek door middel van geautomatiseerde systemen, zoals iColumbo, op een laagdrempelige manier (zonder rechterlijke machtiging) veel data kan verzamelen over personen.[172] De combinatie van data uit open bronnen en verkeersgegevens zou meer mogelijkheden kunnen bieden om verkeersgegevens in context te plaatsen en daarmee meer inzicht te krijgen in de vermoedelijke inhoud van een bericht dan bij analyse van losstaande verkeersgegevens mogelijk is.

## 3.12. Conclusie

In dit hoofdstuk zijn grijze gebieden behandeld die bestaan tussen verkeersgegevens en inhoud, waarmee de tweede deelvraag van dit onderzoek is beantwoord. De belangrijkste grijze gebieden die in de literatuur worden genoemd, zijn surfgegevens (waaronder ook zoekmachinesurfgegevens) en de onderwerpregel in een emailbericht en een sms-bericht. Deze laatste twee zijn technisch verkeersgegevens, maar juridisch duidelijk te kwalificeren als inhoud, omdat ze deel uitmaken van de feitelijke inhoud die onder verantwoordelijkheid van de verzender valt. Om deze reden zijn ook toonkeuzes die bij telefoon-keuzemenu's worden gebruikt, inhoud. Surfgegevens zijn niet letterlijk inhoud, maar wijzen vaak wel direct op de inhoud die tussen webpagina's en webgebruikers wordt getransporteerd. Het publieke karakter van deze inhoud doet daarbij niet af aan de eventuele beschermwaardigheid onder het communicatiegeheim; de beschermwaardigheid hangt af van de vraag of een URL dusdanig nauw samenhangt met de inhoud dat deze op dezelfde manier als inhoud beschermd zou moeten worden. Bij zoekmachinesurfgegevens is dat verband in elk geval directer, omdat zoektermen – die inhoud van communicatie zijn – vaak deel uitmaken van de URL van de pagina met zoekresultaten; hetzelfde geldt mutatis mutandis voor URL's die authenticatiegegevens voor inloggen bevatten.

Minder prominent worden in de literatuur soms andere grijze gebieden gesignaleerd. Het betreft dan emailadressen, informatienummers en naambellen, waarbij de zelfgekozen adressen een betekenis hebben die uitstijgt boven inhoudsloze adressen, waardoor enige samenhang ontstaat tussen het adres en de vermoedelijke globale inhoud van communicatie via dat adres. Dat geldt grosso modo ook voor poortnummers, de presentmelding bij webapplicaties en het Internet der dingen, waarbij er om uiteenlopende

[172] Zie Koops e.a. 2012a.

redenen enige correlatie bestaat tussen het gegeven dat communicatie plaatsvindt en de vermoedelijke globale inhoud van het berichtenverkeer. Het verband tussen verkeersgegevens en inhoud is in deze grijze gebieden minder sterk dan bij surfgegevens. Niettemin kan in bepaalde gevallen de context dusdanig zijn dat met behoorlijke waarschijnlijkheid het onderwerp, en soms ook de strekking, van communicatie kan worden afgeleid, zeker als verkeersgegevens over lange tijd beschikbaar zijn en/of gecombineerd worden met andere gegevens.

De opkomst van *data mining* versterkt de mogelijkheid dat verkeersgegevens onder omstandigheden inzicht bieden in de vermoedelijke inhoud van een bericht, maar kan ook leiden tot andersoortige inzichten in de persoonlijke levenssfeer van burgers. De literatuur weerspiegelt een bezorgdheid over de toenemende privacygevoeligheid van verkeersgegevens, die niet alleen communicatie- maar ook gedragspatronen kunnen blootleggen. Locatiegegevens zijn daarvan het prangendste voorbeeld. Soms zullen verkeersgegevens, ongeacht of ze verband houden met inhoud, dan ook gevoeliger zijn dan de inhoud van communicatie zelf. Naast de vraag die in dit onderzoek centraal staat, namelijk welke typen verkeersgegevens beschermwaardig zijn onder artikel 13 Gw gezien de ratio en functie van het correspondentiegeheim, is daarom een even belangrijke vraag voor de wetgever hoe verkeersgegevens afdoende juridisch beschermd kunnen worden gezien hun privacygevoeligheid in het algemeen.

# 4. Een typologie van verkeersgegevens

Nu de grijze gebieden in kaart zijn gebracht, is de vraag of deze op een zinvolle en werkbare manier kunnen worden geclusterd, zodat een classificatie ontstaat van verkeersgegevens aan de hand waarvan kan worden bepaald of verkeersgegevens al dan niet als inhoud zouden moeten worden behandeld. Hieronder worden verschillende mogelijke classificaties besproken, variërend van abstract-theoretisch tot meer concreet-pragmatisch.

## 4.1. Een conceptuele typologie

Een conceptuele typologie knoopt aan bij de conceptuele invulling van inhoud en verkeersgegevens. Deze begrippen kunnen, zoals betoogd in hoofdstuk 2, als volgt worden ingevuld:

- inhoud is datgene wat onder verantwoordelijkheid van de verzender valt;
- verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Dit betreft, in de vorm van Fischers 3x3-matrix, gegevens die nodig zijn voor
    - dienstuitvoering,
    - dienstafrekening of
    - dienstbeheer,

  door aanbieders van *mere conduit*, *caching* en *hosting*.[173]

De vraag of gegevens (primair) onder verantwoordelijkheid van de communicatiepartner(s) of onder die van de transporteur vallen, biedt een nuttig criterium om gegevens te classificeren. Het criterium werkt bijvoorbeeld goed om te onderbouwen waarom de email-onderwerpregel en het sms-bericht inhoud zijn en geen verkeersgegevens. Bij hybride gegevens, zoals de zoekmachine-URL die automatisch gegenereerd wordt ten behoeve van het transport maar die ook door de gebruiker gekozen inhoud bevat, geeft het criterium aan dat het gedeelte achter het "?" in de zoekmachine-URL (ook) inhoud is en wat daaraan voorafgaat (alleen) een verkeersgegeven. Bij andere grijze gebieden is het criterium echter niet eenduidig toepasbaar, omdat er daar een minder duidelijke correlatie bestaat tussen het verkeersgegeven en de inhoud van een concreet bericht. Er kan een hybride verantwoordelijkheid zijn, waarbij de transporteur grotendeels of geheel verantwoordelijk is voor een bepaald gegeven, en het dus strikt genomen niet om inhoud gaat, maar waarbij het verkeersgegeven wel in zekere mate correleert met de inhoud. Dat is bijvoorbeeld het geval bij poortnummers (zie par. 3.7) of bij emailadressen, die beheerd worden door de aanbieder maar waarbij de gebruiker een zekere mate van keuzevrijheid heeft voor de invulling ervan.

---

[173] Zie noot 111 en bijbehorende tekst.

Daarom kan een nadere conceptuele indeling worden gezocht om te helpen gegevens te classificeren als inhoud of als verkeersgegeven. Omdat het gaat om de manieren waarop verkeersgegevens kunnen relateren aan inhoud, ligt het voor de hand hiervoor het onderscheid uit de semiotiek te hanteren in verschillende soorten tekenrelaties. C.S. Peirce, de grondlegger van de semiotiek, heeft een onderscheid gemaakt in de manier waarop een teken naar een object kan verwijzen. Een teken kan verwijzen naar het object in de vorm van een:[174]

1. ***icoon***: een teken dat lijkt op het object, vanwege een bepaalde eigenschap die zowel het teken als het object hebben; daarvan zijn er drie soorten:
    a. ***afbeelding***: het teken lijkt op het object door een simpele gedeelde eigenschap, zoals een foto lijkt op de afgebeelde persoon of een onomatopee ("woef") op een geluid;
    b. ***diagram***: het teken lijkt op het object doordat de interne relaties tussen onderdelen vergelijkbaar zijn, zoals een stroomschema van een elektrische schakeling, of een organogram van een organisatie;
    c. ***metafoor***: het teken lijkt op het object door een andersoortige parallel, die abstracter is dan de simpele gedeelde eigenschap van de afbeelding; zo lijkt een computervirus niet letterlijk op een virus maar wel figuurlijk, door de eigenschappen onzichtbaar te zijn en zichzelf te vermenigvuldigen; daarom is 'virus' een metafoor voor bepaalde typen kwaadaardige programmatuur;
2. ***index***: een teken dat verwijst naar een object door een feitelijke relatie in de werkelijkheid, zoals een richtingaanwijzer met daarop 'Den Haag' naar Den Haag wijst, of een inhoudsopgave verwijst naar de inhoud van een document;
3. ***symbool***: een teken dat verwijst naar een object op basis van een gewoonte of afspraak, zoals de kleur rood verwijst naar gevaar, een verbod of karnemelk en de kleur groen naar milieuvriendelijkheid, een permissie of een giftige stof.

Deze typologie zou kunnen helpen om het verband tussen verkeersgegevens en inhoud nader te duiden. Zo is een sms een 1-op-1 afbeelding van de inhoud en is de onderwerpregel van een emailbericht een afbeelding van de inhoud omdat het meestal het onderwerp (en vaak de kern daarvan) omschrijft. Een URL verwijst indexicaal naar de inhoud van communicatie, omdat het direct verbonden is met de webpagina waarvan de inhoud wordt getransporteerd naar de gebruiker. Bij sommige opeenvolgingen van communicaties weerspiegelt de volgorde van typen berichten de vermoedelijke inhoud: als gebruiker A via een webformulier een bericht aan webpagina B stuurt, waarna direct een email van domein B naar A wordt gestuurd, en vervolgens A dertig seconden later een nieuwe URL van B aanklikt, is het zeer

---

[174] De beschrijving is ontleend aan http://en.wikipedia.org/wiki/Semiotic_elements_and_classes_of_signs onder "Icon, index, symbol" (geraadpleegd 1 oktober 2013).

waarschijnlijk dat het ingevulde webformulier een aanmelding bevatte, het emailbericht van B naar A een verzoek om de aanmelding te bevestigen, en de laatste URL een bevestiging van aanmelding. Zo vormt de direct opeenvolgende sequentie van webformulier-email-URL een diagram van de communicatie van een aanmelding.

Bij de presentmelding is het feit dat een bericht van een gebruiker naar diens contacten wordt verstuurd, een metafoor voor de inhoud "ik ben er weer". Sommige voorbeelden van locatiegegevens staan symbool voor de inhoud, wanneer er een sterk statistisch verband bestaat tussen de verkeersgegevens (op tijdstip x op plaats y een sms verzonden) en de vermoedelijke inhoud van het bericht ("U gaat nu de grens over"; "Aanbieding van De Lange Muur"; "Castaignos scoort 2-0!").

In het algemeen hebben afbeeldingen en diagrammen een sterk verband met het object waarnaar zij verwijzen, bij de afbeelding vanwege de eigenschap waarin het object zichtbaar is, bij het diagram vanwege de gelijkenis in structuur. Ook bij de index is het verband tamelijk sterk vanwege de feitelijke nabijheidsrelatie. Metaforen en symbolen hebben vaak een zwakker verband: ze verwijzen weliswaar naar het object, maar geven daarbij minder intrinsiek informatie over het object. Daarbij moet wel worden opgemerkt dat dit niet altijd zo is: een afbeelding of diagram kan zwak zijn doordat het slechts een enkele eigenschap of een abstracte structuur van het object weerspiegelt, terwijl een krachtige metafoor of sterk symbool treffend de kern van een object kan aanduiden.

In gevallen waarin het criterium of gegevens onder verantwoordelijkheid van de communicatiepartner(s) vallen, niet voldoende houvast biedt, kan de vervolgvraag worden gesteld of het verband tussen het verkeersgegeven en inhoud de vorm heeft van een afbeelding of diagram, van een index, of van een metafoor of symbool. In het geval het verkeersgegeven een afbeelding of diagram is van de inhoud, valt het in beginsel te kwalificeren als inhoud (tenzij het om een zwakke afbeelding of een abstract diagram gaat). Als het de vorm heeft van een index, is het als inhoud te kwalificeren als de overheid de feitelijke koppeling kan volgen tussen verkeersgegeven en inhoud; dat is typisch het geval bij surfgegevens. Als het echter de vorm heeft van een metafoor of symbool, kan het als verkeersgegeven worden behandeld en niet als inhoud (tenzij het om een sterke metafoor of sterk symbool gaat dat de kern van de inhoud aanduidt). Op deze manier valt bijvoorbeeld een onderscheid te maken in zelfgekozen emailadressen die een inhoudelijke (dat wil zeggen identiteitsconstruerende) component hebben: de meeste daarvan staan symbool voor de (vermoedelijke) globale inhoud van een bericht, omdat gewoonlijk een bericht van postzegelverzamelaar@aanbieder.nl over postzegels zal gaan, en een bericht van janwilseks@aanbieder.nl gewoonlijk iets met seks te maken zal hebben. Omdat het om een zwakke tekenrelatie gaat, kunnen dit soort emailadressen als verkeersgegevens en niet als inhoud worden behandeld. Sommige emailadressen wijzen echter op de kern van de vermoedelijke

communicatie, zoals jaikkomnaarpetersfeestje@yahoo.com, in welk geval het emailadres (vergelijkbaar met een emailonderwerpregel) een afbeelding wordt van de inhoud. Het zou in dat geval dan ook als inhoud moeten worden behandeld. (Dat roept wel de vraag op of het praktisch mogelijk is een onderscheid te maken *binnen* een bepaalde categorie, zoals emailadressen. Op die vraag kom ik in hoofdstuk 6 terug.)

Samenvattend kan men de volgende conceptuele typologie van verkeersgegevens maken, ten behoeve van de afbakening tussen verkeersgegevens en inhoud:

| **classificeringsvraag** | **inhoud?** | **voorbeelden** |
|---|---|---|
| 1. *Onder wiens verantwoordelijkheid valt het gegeven?* | | |
| a. communicatiepartner(s) | ja | sms-bericht<br>emailonderwerpregel<br>URL van zoekmachine na "?": zoeken-op=grondwet |
| b. transporteur, en het gegeven biedt geen inzicht in inhoud | nee | locatiegegeven mobiele telefoon<br>URL van zoekmachine tot en met "?": http://www.rijksoverheid.nl/zoeken? |
| c. transporteur, en het gegeven biedt mogelijk zicht op de inhoud | bepalen aan hand van vraag 2 | |
| 2. *Op welke manier verwijst het verkeersgegeven naar de inhoud?* | | |
| a1. afbeelding (regel) | ja | geautomatiseerd toetsmenu: "toets nu uw BSN in"<br>berichtspecifiek emailadres:[175] jaikkomnaarpetersfeestje@yahoo.com<br>berichtspecifiek informatienummer: 0906-BLOWJOB |
| a2. afbeelding (uitzondering: zwak verband) | nee | inhoudspecifiek emailadres:[176] petersfeestje@yahoo.com<br>inhoudspecifiek informatienummer: 0900-NOTARIS |
| b1. diagram (regel) | ja | patroon van webaanmelding + emailbevestiging |
| b2. diagram (uitzondering: zwak verband) | nee | |
| c1. metafoor (regel) | nee | telefoonnummer 144 ("red een dier") |

[175] Met 'berichtspecifiek' bedoel ik dat het verkeersgegeven dusdanig concreet is dat het een indicatie geeft niet alleen van het vermoedelijke onderwerp maar ook van de vermoedelijke strekking van een bericht.

[176] Met 'inhoudspecifiek' bedoel ik dat het verkeersgegeven concreet genoeg is om het vermoedelijke onderwerp aan te duiden, maar niet concreet genoeg om de strekking van berichten uit af te leiden.

| classificeringsvraag | inhoud? | voorbeelden |
|---|---|---|
| c2. metafoor (uitzondering: sterk verband) | ja | telefoonnummer 112 + locatie + tijdstip presentmelding bij Internetapplicaties |
| d1. index (regel) | ja | geautomatiseerd telefoonkeuzemenu: "voor inentingen, toets 3"<br>URL met (min of meer) vaste inhoud: http://nl.wikipedia.org/wiki/Uniform_Resource_Locator<br>URL met flexibele inhoud + tijdstip: http://www.nu.nl/ op maandag 12 januari om 13:52 |
| d2. index (uitzondering: koppeling niet te maken) | nee | URL met flexibele inhoud zonder datum/tijd: http://www.nu.nl/ |
| e1. symbool (regel) | nee | informatienummer: 144, 0906-1234<br>poortnummer voor financiële of medische applicatie<br>emailadres met inhoudelijke component: postzegelverzamelaar@aanbieder.nl |
| e2. symbool (uitzondering: sterk verband) | ja | contextspecifiek locatiegegeven (gekoppeld aan toegevoegdewaardedienst): sms van restaurant X aan mobiel Y in de buurt van X |

**Tabel 1. Een conceptuele typologie van verkeersgegevens**

Een voordeel van deze typologie is dat het houvast biedt om op basis van inhoudelijke argumenten een verkeersgegeven al dan niet als inhoud te classificeren. Een nadeel is dat het ook een onderscheid maakt in verkeersgegevens als telefoonnummers en emailadressen, afhankelijk van de mate waarin die inzicht bieden in de inhoud van communicatie, terwijl de rechtspraktijk tot nu toe gegevens als nummers integraal behandelt als verkeersgegevens. De classificering van verkeersgegevens tot nu toe is dan ook meer functioneel dan conceptueel van aard.

## 4.2. Een functionele typologie

De rechtspraktijk kent verschillende opsommingen van typen verkeersgegevens. De twee belangrijkste zijn de aanwijzing van verkeersgegevens die kunnen worden gevorderd en de aanwijzing van verkeersgegevens die telecommunicatieaanbieders moeten bewaren.

Het Besluit vorderen gegevens telecommunicatie wijst de volgende typen gegevens aan als verkeersgegevens:

a. 'de naam, het adres en de woonplaats van de gebruiker;
b. de nummers van de gebruiker;
c. de naam, het adres, de woonplaats en het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen, of van de natuurlijke persoon

of rechtspersoon die heeft getracht met de gebruiker verbinding tot stand te brengen;

d. de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, dan wel, ingeval er geen verbinding tot stand is gekomen, de datum en het tijdstip waarop is getracht verbinding met de gebruiker tot stand te brengen (…);
e. de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende de geografische positie van de randapparatuur van een gebruiker ingeval van een verbinding of poging daartoe;
f. de nummers van de randapparatuur waarvan de gebruiker gebruik maakt of heeft gemaakt;
g. de soorten diensten waarvan de gebruiker gebruik maakt of heeft gemaakt evenals de daarbij behorende gegevens;
h. de naam, het adres en de woonplaats van degene die de rekening betaalt voor de openbare telecommunicatiediensten en telecommunicatienetwerken die de gebruiker ter beschikking heeft of heeft gehad, indien deze een ander is dan de gebruiker.'[177]

Op basis van de Wet bewaarplicht telecommunicatiegegevens, moeten telecomaanbieders de diverse typen gegevens bewaren, die grotendeels neerkomen op naam- en adresgegevens, nummers, type dienst, datum/tijdgegevens, en (bij mobiele telefonie) locatiegegevens.[178]

Anton Ekker heeft een classificering van verkeersgegevens gemaakt die deze gegevens groepeert naar het object van het verkeersgegeven: communicatiegedrag algemeen, routering en vorm en omvang.[179] Deze classificering biedt een antwoord op de klassieke vragen: wie, wat, waar, wanneer en hoe? Ze kunnen daarom worden samengenomen in de volgende typologie:

| **object van het gegeven** | **type verkeersgegeven** | **vragen** |
|---|---|---|
| communicatiegedrag algemeen | duur<br>tijdstip (begin, eind), datum<br>locatie eindapparatuur<br>type dienst | wanneer<br><br>waar<br>wat |
| routering | adres/nummer verzender<br>adres/nummer ontvanger | wie |
| vorm en omvang | volume (omvang)<br>gebruikte protocol<br>formaat | wat<br>hoe |

**Tabel 2. Typologie naar object van verkeersgegevens**

177 Art. 2 Besluit vorderen gegevens telecommunicatie, *Stb.* 2004, 394.
178 Zie Bijlage behorende bij art. 13.2a Telecommunicatiewet, ingevoerd bij Wet bewaarplicht telecommunicatiegegevens, *Stb.* 2009, 333.
179 Ekker 2003, p. 45.

De waarom-vraag komt hierin niet aan de orde. Deze hangt samen met een tweede classificering van Ekker, naar het doel van de verwerking: transmissie, facturering, of toegevoegdewaardedienst. Dit lijkt op de drie functies die Fischer onderscheidt, maar de derde categorie (toegevoegdewaardediensten bij Ekker, dienstbeheer bij Fischer) verschilt. Ekkers indeling is gebaseerd op Richtlijn 2002/58/EG, die een toegevoegdewaardedienst definieert als een 'dienst die de verwerking vereist van verkeersgegevens of locatiegegevens anders dan verkeersgegevens, en die verder gaat dan hetgeen nodig is voor het overbrengen van een communicatie of de facturering ervan'.[180]

Een typologie naar doel van verwerking is bruikbaarder dan bovenstaande typologie naar object van verkeersgegevens, als het gaat om het afbakenen van verkeersgegevens tegenover inhoud. Over het algemeen bieden verkeersgegevens die worden verwerkt ten behoeve van facturering of dienstbeheer namelijk geen zich op de inhoud. De voorbeelden in de grijze gebieden betreffen namelijk verkeersgegevens die worden verwerkt voor transmissie of voor een toegevoegdewaardedienst.[181] De gegevens uit het Besluit vorderen gegevens telecommunicatie kunnen aan de hand van deze doelen dan als volgt worden gegroepeerd:

| **doel van verwerking (aanbieder)** | **type verkeersgegeven** | **inhoud?** |
|---|---|---|
| transmissie | tijdstip (begin, eind), datum<br>nummer verzender<br>nummer ontvanger<br>locatie eindapparatuur (cel-ID)<br>gebruikte protocol<br>formaat | mogelijk |
| facturering | duur<br>volume (omvang)<br>soort dienst<br>NAW-gegevens betaler | nee |
| dienstbeheer | NAW-gegevens gebruiker<br>nummers van gebruiker | nee |
| toegevoegdewaardedienst | verfijnde locatiegegevens | mogelijk |

**Tabel 3a. Typologie van verkeersgegevens naar doel van verwerking (aanbieder)**

[180] Art. 2 onder g Richtlijn 2002/58/EG.

[181] Merk op dat zelfgekozen emailadressen onder 'nummers van de gebruiker' vallen in tabel 3, maar alleen iets over de inhoud van communicatie vertellen als zij zijn gebruikt bij een concrete communicatie; ze vallen dus alleen in het grijze gebied als het een 'nummer verzender' betreft bij een transmissie, maar niet als het om 'nummers van de gebruiker' in de zin van het dienstbeheer gaat.

Deze typologie bekijkt de verkeersgegevens vanuit de functionaliteit van de transporteur. Men kan echter ook een ander perspectief hanteren, namelijk voor welke functie de overheid verkeersgegevens zou willen verwerken. Volgens het WODC-onderzoek naar het gebruik van de telefoon- en Internettap in de opsporing, vraagt de politie vooral historische verkeersgegevens op.[182] Daarbij kunnen de volgende doelen worden onderscheiden:[183]

- voorfase van aftappen: onderzoeken welk nummer het best kan worden getapt (welk nummer wordt het meest gebruikt; is er capaciteit om de hoeveelheid communicatie uit te luisteren);
- opsporingsinformatie:
    - in kaart brengen van netwerken (wie belt met wie);
    - met wie stond het slachtoffer in contact;
    - met wie heeft een getuige contact gehad;
- bewijsinformatie, bijvoorbeeld:
    - vaststellen contact tussen verdachte en slachtoffer;
    - locatiegegevens.

Deze doelen zullen grotendeels overeenkomen met die van inlichtingen- en veiligheidsdiensten, met de kanttekening dat bewijsinformatie bij deze diensten geen rol speelt.

Voor de verschillende doelen zijn verschillende typen verkeersgegevens het meest relevant. Om te bekijken welke nummers het beste afgetapt kunnen worden en om netwerken in kaart te brengen, zijn voor nummergegevens en NAW-gegevens nodig, alsmede wellicht duur en omvang, gebruikte protocol en soort dienst. Deze laatste informatie is daarbij alleen op geaggregeerd niveau nodig: het zal niet nodig zijn om deze gegevens per afzonderlijke communicatie te weten te komen. Voor andersoortige opsporingsinformatie en voor bewijsdoeleinden zijn juist wel gegevens per afzonderlijke communicatie wenselijk, en daarbij kan het sneller voorkomen dat verkeersgegevens zicht bieden op de inhoud van communicatie. Dit kan worden vertaald in een volgende typologie:

| **doel van verwerking (overheid)** | **type verkeersgegeven** | **inhoud?** |
|---|---|---|
| voorfase aftappen (op welk(e) nummer(s) is een tap wenselijk?)<br><br>of<br><br>netwerken in kaart brengen | nummer verzender<br>nummer ontvanger<br>gebruikte protocol (geaggregeerd)<br>formaat (geaggregeerd)<br>duur (geaggregeerd)<br>volume (geaggregeerd)<br>soort dienst (geaggregeerd)<br>NAW-gegevens betaler<br>NAW-gegevens gebruiker<br>nummers van gebruiker | nee |

[182] Odinot e.a. 2012, p. 115.
[183] Vgl. ibid., p. 111-115.

| | | |
|---|---|---|
| contact slachtoffer, getuigen als opsporingsinformatie<br><br>of<br><br>bewijsinformatie | nummer verzender<br>nummer ontvanger<br>tijdstip (begin, eind), datum<br>duur<br>volume<br>gebruikte protocol<br>formaat<br>soort dienst<br>locatie eindapparatuur (cel-ID)<br>verfijnde locatiegegevens | mogelijk |

**Tabel 3b. Typologie van verkeersgegevens naar doel van verwerking (overheid)**

Feitelijk komt deze typologie neer op een simpel criterium: hangen verkeersgegevens samen met een concrete communicatiehandeling, of houden ze in meer algemene zin verband met gebruik van communicatiemiddelen? Gegevens die niet samenhangen met een concrete communicatiehandeling, zoals welke emailadressen iemand gebruikt of een geaggregeerd overzicht van hoe vaak iemand met een bepaald nummer belt, bieden geen zicht op inhoud van concrete communicatie. Gegevens die wel samenhangen met een concrete communicatiehandeling bieden mogelijk wel zicht op de inhoud van die specifieke communicatie.

De typologieën naar doel van de verwerking (tabel 3a en 3b) bieden enig houvast om verkeersgegevens van inhoud af te bakenen. Bepaalde categorieën verkeersgegevens kunnen worden uitgesloten van inhoud, zoals verkeersgegevens die worden verwerkt voor facturering of dienstbeheer, of limitatief opgesomde (en voor dit doel geaggregeerde) verkeersgegevens die de overheid nodig heeft voor het in kaart brengen van netwerken of in de voorfase van aftappen. Voor de overige categorieën biedt deze indeling evenwel geen afbakeningscriterium: het zal afhankelijk van de context en de precieze invulling zijn of de desbetreffende verkeersgegevens als inhoud zouden moeten worden behandeld. Dat komt omdat functionele typologieën te maken hebben met de functies die verkeersgegevens hebben voor de aanbieder of de overheid, maar geen onderscheid maken in de beschermwaardigheid van gegevens, zoals de eerdere conceptuele typologie deed. Beschermwaardigheid van verkeersgegevens kan echter niet alleen worden bekeken vanuit een abstract-theoretisch perspectief ontleend aan de semiotiek, maar ook vanuit de ratio van bescherming van verkeersgegevens, wat leidt tot een teleologische typologie.

## 4.3. Een teleologische typologie

Fischer maakt een onderscheid in verkeersgegevens dat gebaseerd is op een verschil in potentiële privacygevoeligheid. Hij bouwt daarbij voort op het model van Bordewijk & Van Kaam dat vier typen communicatiepatronen onderscheidt:

1. *conversatie*: individueel geïnitieerd en inhoud afkomstig van een individu (bijvoorbeeld telefoongesprek);
2. *registratie*: geïnitieerd door een centrale instantie en inhoud afkomstig van een individu (bijvoorbeeld telemarketing);
3. *consultatie*: individueel geïnitieerd en inhoud afkomstig van een centrale instantie (bijvoorbeeld *video-on-demand*);
4. *allocutie*: geïnitieerd door een centrale instantie en inhoud afkomstig van een centrale instantie (bijvoorbeeld televisie-uitzending).

Volgens Fischer is bij conversatie en registratie qua privacygevoeligheid de inhoud belangrijker dan de verkeersgegevens. Bij consultatie en allocutie kantelt het perspectief: daar is de inhoud minder gevoelig, maar het feit dat een individu die inhoud tot zich neemt is wel potentieel privacygevoelig.[184] Eenzelfde kanteling vindt volgens Fischer plaats bij locatiegegevens: eenvoudige locatiegegevens zijn nodig voor het afwikkelen van mobiele telecommunicatie, waarbij de inhoud van het verkeer gevoeliger is dan de globale locatie, maar bij toegevoegdewaardediensten worden de verfijnde (veel preciezere) locatiegegevens potentieel privacygevoeliger dan de inhoud van de communicatie.[185] Aldus komt Fischer tot een onderscheid in twee typen verkeersgegevens:

> - 'Type I traffic data: regular traffic data. These are traffic data relating to the traffic patterns conversation and registration, except for any high-resolution location data;
>
> - Type II traffic data: special traffic data relating to the traffic patterns consultation and allocution, plus any high-resolution location data.
>
> Type II traffic data deserve more protection than Type I. Also, the scope of protection of Type I traffic data is a priori thinner than the communication content to which it relates.'[186]

Met andere woorden: Fischers type I-gegevens zijn a priori minder beschermwaardig dan inhoud van communicatie (hoewel ze in bijzondere gevallen wel ex post even of meer privacygevoelig kunnen blijken). Type II-gegevens zouden meer beschermd moeten worden dan type I-gegevens, waarbij Fischer overigens in het midden laat of het beschermingsniveau hetzelfde zou moeten zijn als dat van inhoud van communicatie of een sui generis-beschermingsniveau.

Arno Smits stelt ook een onderscheid voor in verkeersgegevens naar privacygevoeligheid. Hij kijkt daarbij primair naar surfgegevens. Volgens Smits is een IP-adres of domeinnaam (overheid.nl) vergelijkbaar met een klassiek

---

184 Fischer 2010, p. 36-38.
185 Ibid., p. 38.
186 Ibid., p. 36.

adresgegeven en dus een verkeersgegeven, maar is een volledige URL privacygevoeliger en niet vergelijkbaar met het oude begrip verkeersgegeven. Daarom zou een scheiding gemaakt moeten worden tussen deze twee typen.[187] Ook Ekker verwijst naar een onderscheid in privacygevoeligheid. Omdat gegevens over mobiele communicatie privacygevoeliger zijn dan verkeersgegevens die samenhangen met vaste communicatie, 'kan men betogen dat sommige verkeersgegevens meer bescherming verdienen dan andere.'[188] Het gaat dan vooral om locatiegegevens, die bij mobiele telefonie privacygevoeliger zijn dan bij vaste telefonie. Het is daarom een mogelijkheid om locatiegegevens apart te behandelen, of om een onderscheid te maken tussen verkeersgegevens behorend bij mobiele telefonie en verkeersgegevens behorend bij vaste telefonie. Dat kan men uitbreiden met verkeersgegevens behorend bij Internet, waarbij de meeste grijze gebieden bestaan en die, vooral voor wat betreft surfgegevens, volgens een breed gedragen visie in de literatuur meer bescherming behoeven dan klassieke verkeersgegevens.

Hierbij moet worden aangetekend dat de auteurs die een onderscheid naar privacygevoeligheid voorstellen, geen criterium of operationalisering expliciteren op basis waarvan iemand kan bepalen wanneer een gegeven meer of minder privacygevoelig is. Het onderscheid is bij hen meer een intuïtief onderscheid dat aan de hand van voorbeelden wordt geïllustreerd. Voor de rechtspraktijk biedt dat wellicht weinig houvast, omdat een abstract geformuleerd onderscheid in privacygevoeligheid steeds moet worden toegepast op concrete gevallen. Wellicht kan men daarom aanknopen bij onderscheiden die elders in de wetgeving worden gehanteerd, zoals het onderscheid tussen 'gewone' persoonsgegevens en gevoelige persoonsgegevens,[189] of een onderscheid tussen het maken van een geringe inbreuk op de persoonlijke levenssfeer en het maken van een meer dan geringe inbreuk op de persoonlijke levenssfeer waarbij 'een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven'.[190] De wetgever kan echter ook in de toelichting een nadere omschrijving geven van wat privacygevoeligheid inhoudt in de telecommunicatiesfeer, die in de rechtsontwikkeling via jurisprudentie dan verder kan uitkristalliseren, zoals dat normaliter gaat met open normen in het recht.

Hoe men ook precies het begrip privacygevoeligheid omschrijft of invult, de literatuur geeft aan dat vooral Internetgegevens en locatiegegevens als privacygevoelig worden beschouwd. Een typologie zou daarom kunnen zijn:

- type A: verkeersgegevens behorend bij post en telefonie, met uitzondering van locatiegegevens bij mobiele telefonie; dit zijn de klassieke verkeersgegevens die onder het bestaande beschermingsregime vallen;

---

187 Smits 2006, p. 397, 399.
188 Ekker 2003, p. 45.
189 Zie art. 16 Wbp.
190 *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26-27.

- type B: locatiegegevens bij mobiele telefonie en verkeersgegevens behorend bij Internet; dit zijn nieuwe typen verkeersgegevens die meer juridische bescherming nodig hebben dan type A.

Belangrijk om op te merken is echter dat de genoemde auteurs pleiten voor een onderscheid tussen bepaalde typen verkeersgegevens, waarbij de meer privacygevoelige gegevens meer bescherming verdienen, vanuit een algemeen privacybelang. De argumentatie voor het onderscheid tussen type I en II, of type A en B, is niet ingegeven door het belang van het correspondentiegeheim als zodanig – de vrijheid om privé te communiceren zonder dat de overheid meeluistert. De teleologie in deze typologieën is dus het belang van privacy in het algemeen en niet per se het correspondentiegeheim in het bijzonder.

Toch kan de discussie over een onderscheid in verkeersgegevens naar privacygevoeligheid niet geheel tot artikel 10 Gw – het algemene privacyrecht – worden verengd. Ten eerste is dat zo omdat de discussie in de literatuur vaak in het kader van artikel 13 Gw wordt gevoerd, vanwege het substantiële verschil in de *checks and balances* in beide grondwetsartikelen. Artikel 10 Gw biedt in formele zin nauwelijks juridische bescherming, omdat de wetgever bij of krachtens de wet privacyinbreuken kan invoeren, waarbij de Grondwet geen eis stelt ten aanzien van eventueel toezicht. Dit in tegenstelling tot artikel 13 Gw, waarbij de wetgever alleen bij (maar niet krachtens) de wet inbreuken kan invoeren en waarbij de inbreuk voor een belangrijk deel onderworpen is aan rechterlijk toezicht. Dit levert een vanzelfsprekende druk op om verkeersgegevens onder de werking van artikel 13 Gw te brengen, vanwege de privacygevoeligheid die verkeersgegevens in het huidige communicatielandschap kenmerkt.

Ten tweede kan de discussie over beschermingsniveaus van verkeersgegevens niet verengd worden tot artikel 10 Gw, omdat er wel degelijk een samenhang bestaat tussen de privacygevoeligheid van verkeersgegevens en de ratio van het correspondentiegeheim: de wetenschap dat (privacygevoelige) verkeersgegevens als surfgegevens of locatiegegevens voor andere doelen dan communicatietransport worden gebruikt, zou burgers kunnen belemmeren om vrijelijk hun communicatiekeuzes te maken. Zij zouden bijvoorbeeld minder snel bepaalde informatie op Internet op zoeken of op bepaalde locaties hun telefoon aanzetten, omdat derden dan een onwenselijk scherp inzicht zouden kunnen krijgen in hun privégedrag. Om die reden past het in de systematiek van de privacygrondrechten om verkeersgegevens onder de werking van artikel 13 Gw te brengen,[191] en daarbij een onderscheid te maken binnen verkeersgegevens naar privacygevoeligheid. De minder gevoelige gegevens – afhankelijk van de gekozen typologie, type I of type A – zouden dan op een lager niveau worden beschermd dan de meer gevoelige gegevens – type II of type B. Deze laatste categorieën zouden dan, vanuit de

[191] Vgl. par. 2.2 en de eerste alinea van par. 2.4.

ratio van het correspondentiegeheim en het mogelijk verkillend effect van kennisneming van deze gegevens op de privécommunicatievrijheid van burgers, aanspraak kunnen maken op hetzelfde beschermingsniveau als inhoud van communicatie.

## 4.4. Conclusie

In dit hoofdstuk zijn diverse typologieën van verkeersgegevens gepresenteerd die zouden kunnen helpen bij de beantwoording van de vraag welke verkeersgegevens onder de bescherming van artikel 13 Gw zouden moeten vallen gezien de ratio van het correspondentiegeheim. Hiermee is de derde onderzoeksvraag naar classificatie van de grijze gebieden beantwoord. Het blijkt dat er geen eenvoudig afbakeningscriterium is aan de hand waarvan een logische typologie kan worden geformuleerd die eenduidig verkeersgegevens indeelt in gegevens die niet en gegevens die wel dusdanig samenhangen met inhoud van communicatie dat zij onder artikel 13 Gw zouden moeten vallen. Dat viel ook te verwachten: als er wel een eenduidig en afdoende afbakeningscriterium zou zijn, dan zou dat in de literatuur al wel zijn geformuleerd en zou er geen diepteonderzoek nodig zijn geweest naar de afbakening tussen verkeersgegevens en inhoud.

Wat wel mogelijk blijkt, is om typen verkeersgegevens te ordenen aan de hand van bepaalde criteria, waarmee het afbakeningsprobleem wordt verkleind of in elk geval meer inzichtelijk wordt gemaakt. Zo kunnen verkeersgegevens worden ingedeeld naar de manier waarop zij mogelijk samenhangen met inhoud, volgens het semiotische onderscheid in soorten tekenrelaties. Verkeersgegevens die een afbeelding of diagram vormen van de inhoud of die indexicaal verwijzen naar inhoud, hebben over het algemeen een nauwer verband dan verkeersgegevens die metaforisch of symbolisch verwijzen naar inhoud. Dit biedt een zinvol materieel criterium om een scheidslijn tussen beschermingsniveaus van verkeersgegevens en inhoud te trekken. Het is wel een vrij abstract criterium dat veel interpretatie vergt. Bovendien leidt het tot een onderscheid binnen bepaalde categorieën verkeersgegevens, zoals telefoonnummers en emailadressen, dat weliswaar inhoudelijk hout snijdt maar ver afstaat van de juridische werkelijkheid waarin nummers en adressen als één categorie worden behandeld.

Een indeling naar het doel van de verwerking kan wel worden gebruikt om bestaande juridische categorieën verkeersgegevens te classificeren. Dat leidt tot twee mogelijke typologieën – een vanuit het perspectief van doelen van de aanbieder en een vanuit het perspectief van doelen van de overheid – waarbij bepaalde typen niet met inhoud samenhangen en dus als pure verkeersgegevens kunnen worden behandeld. Bij gebrek aan een materieel criterium kunnen de verkeersgegevens van de andere typen echter moeilijk worden beoordeeld.

Een derde mogelijkheid is om verkeersgegevens in te delen naar privacygevoeligheid, vanuit de gedachte dat artikel 13 Gw een bijzonder privacygrondrecht is en dus beoogt om de privacy van burgers te beschermen. In deze benadering gaat het dan niet zo zeer om het aanvullend beschermen van bepaalde categorieën verkeersgegevens omdat ze samenhangen met de inhoud, maar omdat ze privacygevoeliger zijn dan andere categorieën. Omdat de privacygevoeligheid van verkeersgegevens wel samenhangt met de ratio van het correspondentiegeheim – kennisneming ervan kan een verkillend effect hebben op de vrijheid om privé te communiceren – kunnen de meer privacygevoelige categorieën verkeersgegevens onder artikel 13 Gw worden beschermd, mogelijk op hetzelfde niveau als inhoud.

Omdat geen van de typologieën een ideale afbakening oplevert, is het nodig om nader te analyseren of een combinatie van criteria en typologieën mogelijk is die de voordelen van de diverse indelingen bundelt.

# 5. Synthese: de beschermwaardigheid van verkeersgegevens onder artikel 13 Gw

Uit de literatuur komt naar voren dat de ratio van het correspondentiegeheim is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Die vrijheid impliceert dat artikel 13 Gw de vertrouwelijkheid van het communicatieproces beschermt, en het correspondentiegeheim zou dan ook de gegevens moeten beschermen die samenhangen met dat proces. Dat wil niet zeggen dat verkeersgegevens aanspraak zouden moeten maken op hetzelfde beschermingsniveau als inhoud, omdat er een zeker kwalitatief verschil kan bestaan tussen verkeersgegevens en inhoud, vergelijkbaar met het verschil tussen het correspondentiegeheim in ruime zin en dat in enge zin.

Zoals geconcludeerd in hoofdstuk 2 is de 'inhoud' van communicatie dat deel van de communicatie dat valt onder de verantwoordelijkheid van de verzender (en niet van de transporteur). Gelet op de ratio van bescherming door artikel 13 Gw gaat het niet alleen om de letterlijke en volledige inhoud, maar ook om gegevens die de strekking weergeven van (een deel van) de inhoud. Hierdoor ontstaat een afbakeningsprobleem: wanneer geven gegevens die primair onder de verantwoordelijkheid van de transporteur vallen (als samenhangend met het transport) voldoende zicht op de strekking van (een deel van) de inhoud van communicatie om aanspraak te kunnen maken op het beschermingsniveau van de inhoud van communicatie?

Zoals blijkt uit de analyse van de grijze gebieden[192] is dit een complexe vraag die zich niet makkelijk laat beantwoorden. Binnen de grijze gebieden vallen allerlei voorbeelden te geven van zowel gegevens die iets meer neigen naar pure verkeersgegevens als gegevens die iets meer neigen naar inhoud. De eenvoudigste oplossing voor dit afbakeningsprobleem is om, zoals Jan Smits aanbeveelt op basis van zijn technische analyse, verkeersgegevens integraal onder artikel 13 Gw te brengen en collectief te behandelen als inhoud.[193] Het collectief onderbrengen van verkeersgegevens onder inhoud voorkomt dat er steeds weer bij technische ontwikkelingen bepaald moet worden of bepaalde gegevens nu wel of niet voldoende zicht geven op de inhoud van communicatie om ze als inhoud te behandelen. Dat is een groot voordeel gezien de technische turbulentie die het telecommunicatielandschap, met steeds nieuwe applicaties en zich steeds ontwikkelende protocollen, kenmerkt.[194]

---

[192] Zie hfd. 3 van dit deel en vooral Deel 1.

[193] Ibid. Zie ook Hes 2003, p. 18. Vgl. ook Asscher en Ekker 2003, p. 104: 'Zowel in de discussie over de technische aspecten van verkeersgegevens als in de juridische debatten worden vraagtekens geplaatst bij de wénselijkheid om nog onderscheid te maken tussen de inhoud van communicatie en de verkeersgegevens.'

[194] Zie Deel 1; Hes 2003, p. 18: 'Ook zou de dynamiek in de technologie kunnen leiden

Hoewel er vanuit analytisch oogpunt veel voor die benadering te zeggen valt, kunnen er vanuit juridisch-praktisch en politiek perspectief bezwaren tegen worden gemaakt. De wetgeving en praktijk zijn eraan gewend geraakt om verkeersgegevens op redelijk laagdrempelige wijze te verwerken en om deze anders te behandelen dan inhoud. Het integraal onderbrengen van verkeersgegevens onder inhoud zou een systeembreuk in de lagere wetgeving betekenen. Daar is niets op tegen als die systeembreuk vanuit grondwettelijk oogpunt gewenst is, integendeel: de Grondwet moet leidend zijn voor lagere wetgeving en niet omgekeerd. Het is echter niet zeker dat het afschaffen van het onderscheid momenteel vanuit een grondwettelijke ratio aan de orde is. Het argument om verkeersgegevens integraal onder inhoud te scharen lijkt vooralsnog vooral gelegen in het praktische probleem een geschikt afbakeningscriterium en werkbare afbakeningsprocedure te formuleren, en niet zozeer in een intrinsieke ratio om alle verkeersgegevens op dezelfde wijze als communicatie-inhoud te behandelen. Er bestaat nog steeds, tot op zekere hoogte, een kwalitatief verschil tussen verkeersgegevens en inhoud, dat globaal gesproken gepaard gaat met een, tot op zekere hoogte, verschil in aanspraak op juridische bescherming. Met andere woorden, het afbakeningsprobleem zou vermoedelijk niet door het paardenmiddel van het compleet afschaffen van een onderscheid moeten worden opgelost.

De vraag is echter wat dan wel een geschikt afbakeningscriterium is. Zoals in hoofdstuk 2 en 4 betoogd, is het primaire onderscheid gebaseerd op de vraag onder wiens verantwoordelijkheid de gegevens vallen:

- inhoud is datgene wat onder verantwoordelijkheid van de verzender valt;
- verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen.

Sommige van de verkeersgegevens vallen weliswaar onder verantwoordelijkheid van de transporteur, maar kunnen de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender. In dat geval zouden zij als inhoud moeten worden behandeld. Voor het bepalen van wanneer verkeersgegevens de strekking weergeven van (een deel van) de inhoud, kan in eerste instantie een negatieve benadering worden gevolgd. Het is mogelijk gegevens aan te wijzen die in elk geval niet (of nauwelijks) zicht geven op de strekking van communicatie.

Dat is in de eerste plaats het geval bij gegevens die niet samenhangen met een concrete communicatiehandeling, waaronder gebruikersgegevens en geaggregeerde verkeersgegevens vallen. Deze gegevens kunnen bijvoorbeeld worden gebruikt om netwerken van (potentiële) verdachten in kaart te brengen of om te bepalen welke telecommunicatienummers het beste kunnen worden afgetapt (zie typologie 3b in hfd. 4). Het omvat met name gegevens die veelal relevant zijn voor facturering of dienstbeheer in plaats van voor

tot een continue herdefinitie van de scheidslijn tussen inhoud en verkeersgegevens en derhalve aan voortdurend "achterlopende" wetgeving.'

transmissie van een specifieke communicatie (zie typologie 3a in hfd. 4).

Voor wat betreft gegevens die wel samenhangen met een concrete communicatiehandeling, kunnen ten tweede ook gegevens worden uitgesloten die de 'klassieke' verkeersgegevens vormen waar het juridische beschermingsregime voor verkeersgegevens uit is voortgekomen: de verkeersgegevens behorend bij post en telefonie,[195] met uitzondering van locatiegegevens bij mobiele telefonie (een type verkeersgegeven dat historisch gezien niet bekend was bij de ontwikkeling van het juridische regime rond verkeersgegevens, en dat van een andere aard is dan klassieke adresgegevens). Weliswaar kunnen in sporadische uitzonderingsgevallen dit type 'klassieke' gegevens (wie belt wanneer met wie) ook zicht bieden op de strekking van de inhoud van communicatie (bijvoorbeeld als iemand het nummer 0906-2569562 belt, wat een naamnummer is voor 0906-BLOWJOB), maar dat is zo zeldzaam dat deze categorie wel generiek als verkeersgegevens en niet als inhoud kan worden behandeld.

Hiermee is het probleemgebied in elk geval nader ingeperkt, namelijk tot verkeersgegevens behorend bij concrete communicatiehandelingen die samenhangen met Internet of locatiegegevens bij mobiele telefonie. Dit zijn gegevens waar de grijze gebieden het meest grijs zijn: of zo'n verkeersgegeven onder inhoud valt hangt erg af van het concrete gegeven (postzegelverzamelaar@aanbieder.nl biedt geen zicht op de strekking van een concreet bericht, jaikkomnaarpetersfeestje@yahoo.com biedt wel zicht op de vermoedelijke strekking van een concreet bericht) alsook van de context (bijvoorbeeld of de overheid het gegeven in verband kan brengen met andere gegevens die in samenhang zicht bieden op de inhoud van communicatie).

Voor dit probleemgebied zou de afbakening gezocht kunnen worden in de semiotische relatie tussen verkeersgegeven en inhoud. Een vuistregel is dat als het verkeersgegeven verwijst naar de inhoud als een afbeelding, een diagram, een index, een sterke metafoor of een sterk symbool, het als inhoud moet worden beschouwd; in de andere gevallen (een zwakke afbeelding, contextloze index, gewone metafoor of gewoon symbool) kan het als verkeersgegeven worden behandeld. Deze afbakening zou vanwege de contextspecificiteit eigenlijk op het niveau van concrete verkeersgegevens gemaakt moeten worden, maar dat zou een grote detaillering vergen van alle mogelijke subcategorieën van verkeersgegevens in het onderhavige probleemgebied. De wetgever is gewend te werken met globale categorieën verkeersgegevens, zoals 'adres', 'nummer' of 'tijdstip'. Het is in beginsel mogelijk om voor elk grijs gebied een meer categorische afweging te maken, afhankelijk van de vraag of de categorie verkeersgegeven *meestal* wel of *meestal* niet verband houdt met de strekking van communicatie. Zo biedt een zelfgekozen emailadres meestal geen zicht op de strekking van een concrete communicatie (het is meestal een symbool in plaats van een afbeelding van de vermoedelijke inhoud), terwijl

[195] Zie art. 100 lid 2-3 Sv-1926, zie daarover Koops 2002, p. 108-112.

een URL meestal wel direct verband houdt met de inhoud van communicatie (het is meestal een index, waarbij de koppeling met specifieke inhoud van een geconsulteerde webpagina te maken valt).

Mogelijk blijft dan nog een restverzameling over van categorieën verkeersgegevens die even vaak wel als niet zicht bieden op de strekking van communicatie, maar die restverzameling is wellicht voldoende klein om op basis van een andersoortige belangenafweging een keuze te maken of de desbetreffende categorie verkeersgegevens als verkeersgegevens of als inhoud moet worden behandeld.

Samenvattend komt de hier beschreven afbakening neer op het volgende stroomschema:

1. Valt het gegeven onder verantwoordelijkheid van de communicatiepartner(s)?
   Zo ja -> inhoud. Zo nee -> verkeersgegeven maar mogelijk (ook) inhoud. Ga naar vraag 2.
2. Biedt het verkeersgegeven mogelijk zicht op de inhoud?
   Zo nee -> verkeersgegeven. Zo ja -> mogelijk inhoud. Ga naar vraag 3.
3. Houdt het verkeersgegeven verband met een concrete communicatiehandeling?
   Zo nee -> verkeersgegeven. Zo ja -> mogelijk inhoud. Ga naar vraag 4.
4. Is het een verkeersgegeven behorend bij telefonie (maar geen locatiegegeven)?
   Zo ja -> verkeersgegeven. Zo nee -> mogelijk inhoud. Ga naar vraag 5.
5. Heeft het verkeersgegeven een sterke relatie met de inhoud? Er is een sterke relatie als het verkeersgegeven semiotisch een afbeelding, diagram, index, sterke metafoor of een sterk symbool is van de inhoud.
   Zo ja -> inhoud. Zo nee -> verkeersgegeven.

De volgende tabel illustreert hoe de verschillende categorieën verkeersgegevens via dit stroomschema kunnen worden geclassificeerd.

| **antwoord**<br>**classificeringsvraag** | **ja** | **nee** |
|---|---|---|
| *1. Valt het gegeven onder verantwoordelijkheid van de communicatiepartner(s)?* | Inhoud<br>sms-bericht<br>emailonderwerpregel<br>telefoonkeuzemenu<br>URL van zoekmachine na "?": zoeken-op=grondwet | *Ga naar vraag 2.* |

| **antwoord classificeringsvraag** | **ja** | **nee** |
|---|---|---|
| *2. Biedt het verkeersgegeven mogelijk zicht op de inhoud?* | *Ga naar vraag 3.* | Verkeersgegeven<br>contextloos<br>locatiegegeven mobiele telefoon<br>URL van zoekmachine tot en met "?": http://www.google.com/search?<br>toegewezen emailadres |
| *3. Houdt het verkeersgegeven verband met een concrete communicatiehandeling?* | *Ga naar vraag 4.* | Verkeersgegeven<br>geaggregeerde verkeersgegevens |
| *4. Is het een verkeersgegeven behorend bij post of telefonie (maar geen locatiegegeven)?* | Verkeersgegeven<br>*telefonie:*<br>nummer verzender<br>nummer ontvanger<br>tijdstip (begin, eind), datum<br>duur<br>soort dienst<br>*post:*<br>adres verzender<br>adres ontvanger<br>datum<br>volume<br>soort dienst | *Ga naar vraag 5.* |
| *5. Heeft het verkeersgegeven een sterke relatie met de inhoud? Semiotisch: is het een afbeelding, diagram, index, sterke metafoor, sterk symbool?* | Inhoud<br>*afbeelding*<br>[dit zijn gegevens die vrijwel altijd onder vraag 1 al als inhoud zijn gekwalificeerd, zoals emailonderwerpregel]<br>*diagram*<br>patroon van webaanmelding + emailbevestiging<br>*sterke metafoor*<br>presentmelding<br>*index*<br>URL<br>*sterk symbool*<br>contextrijk locatiegegeven | Verkeersgegeven<br>*symbool*<br>poortnummer<br>Internetprotocol<br>zelfgekozen emailadres<br>contextarm<br>locatiegegeven |

**Tabel 4. Stroomschema voor classificering van verkeersgegevens**

Uit het schema blijkt dat URL's en locatiegegevens op diverse plaatsen terugkomen. Aangezien een URL uiteindelijk als een index fungeert en daarmee over het algemeen gekoppeld kan worden aan de inhoud van een webpagina, kunnen URL's integraal als inhoud worden gekwalificeerd. Locatiegegevens blijven echter afhankelijk van de context.

De classificatie kan vervolgens ook worden gegroepeerd naar verschillende soorten communicatie (zoals de Wet bewaarplicht telecommunicatiegegevens verschillende categorieën hanteert van telefonie, email en Internet[196]). Op basis van de hierboven gegeven argumentatie en toepassing van het stroomschema, zou ik de verschillende typen gegevens als volgt classificeren als inhoud dan wel als verkeersgegevens:

| **beschermingsregime**<br><br>**soorten communicatie** | **inhoud** | **verkeersgegevens** |
|---|---|---|
| post | | adres verzender<br>adres ontvanger<br>datum<br>volume<br>soort dienst |
| telefonie | sms-bericht<br>telefoonkeuzemenu (toonkiezen)<br>contextrijk locatiegegeven | nummer verzender<br>nummer ontvanger<br>tijdstip (begin, eind), datum<br>duur<br>soort dienst<br>contextloos of contextarm locatiegegeven |
| Internet: email | emailonderwerpregel | emailadres verzender<br>emailadres ontvanger<br>tijdstip (begin, eind), datum<br>volume |
| Internet: overig | URL's<br>patroon van webaanmelding + emailbevestiging<br>presentmelding | poortnummer<br>Internetprotocol<br>geaggregeerde verkeersgegevens |

**Tabel 5. Classificatie van typen verkeersgegevens naar beschermingsregime**

Hiermee is een antwoord geformuleerd op de vierde onderzoeksvraag, namelijk welke typen verkeersgegevens beschermwaardig zijn onder artikel 13 Gw omdat zij 'inhoud' betreffen: dat geldt voor de gegevens in de kolom 'inhoud'.[197] De tabel moet echter niet worden gezien als een uitputtende

[196] Zie noot 178.

[197] Daarbij moet worden aangetekend dat er goede systematische redenen zijn om alle verkeersgegevens onder artikel 13 Gw te brengen, dus ook die in de rechterkolom van

opsomming, noch als een definitief antwoord. Met name voor wat betreft Internet zijn er vele soorten gegevens die moeilijk te vangen zijn onder simpele noemers; daarvoor zijn de protocollen en applicaties te divers.[198] De tabel geeft ook geen definitief antwoord omdat er verschillen kunnen ontstaan door de combinatie van gegevens; wanneer men alle verkeersgegevens heeft behorend bij iemands Internetgebruik over een periode van een paar uur 'is het vrij gemakkelijk geworden de inhoud van al die verschillende (internet) activiteiten te duiden, zonder daadwerkelijk de inhoud te kennen'.[199] Ook kan de combinatie van verkeersgegevens uit de rechterkolom – die dus in beginsel niet onder het beschermingsregime van inhoud vallen – met gegevens uit andere bronnen een dusdanige context opleveren dat de verkeersgegevens dan wel de inhoud van communicatie weerspiegelen.[200] Daarnaast moet ook onder ogen worden gezien dat door convergentie langzamerhand het onderscheid verdwijnt tussen telefonie, email en (overig) Internet.[201] Om deze redenen is nog een nadere reflectie nodig.

Tabel 5. Die kolom betreft dan verkeersgegevens die binnen artikel 13 Gw met een lichtere beperkingsclausule zouden kunnen worden beschermd.

198 Zie Deel 1.

199 Deel 1, par. 5 > p. 94.

200 Zie par. 3.11.

201 Zie Deel 1, o.a. bijlage 4.

# 6. Reflectie

## 6.1. Eerste reflectie: afbakeningscriteria en onderscheid telefonie, email, Internet

In het voorgaande is een inhoudelijke analyse gegeven van de afbakening tussen verkeersgegevens en inhoud. Dat heeft een tamelijk complex beeld opgeleverd. Hoewel het mogelijk is om verkeersgegevens volgens het in het vorige hoofdstuk gepresenteerde stroomschema te classificeren (zoals in Tabel 5 is gedaan), is het de vraag of het juridisch en technisch haalbaar is om een dergelijk classificeringsmodel in wetgeving en praktijk te hanteren. Daarom luidt het tweede onderdeel van de hoofdonderzoeksvraag: in hoeverre zijn de beschermwaardige typen verkeersgegevens juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit?

In beginsel is een tweeledig afbakeningscriterium te formuleren dat juridisch voldoende abstractieniveau heeft en dat inhoudelijk goed werkt om de kern van het onderscheid tussen inhoud en verkeersgegevens te duiden. Het **hoofdcriterium** is **onder wiens verantwoordelijkheid de gegevens vallen**: **inhoud is datgene wat onder verantwoordelijkheid van de verzender valt**; verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Het **nevencriterium** is dat **verkeersgegevens** die (juridisch-)technisch onder het begrip verkeersgegevens vallen, onder artikel 13 Gw **als inhoud moeten worden behandeld wanneer zij de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender**.

De operationalisering van dit laatste criterium levert echter complicaties op. Zoals hoofdstuk 5 laat zien, zijn er diverse argumentatiestappen nodig om grijze gebieden volgens dit criterium uiteindelijk in te delen naar het beschermingsregime van inhoud of van verkeersgegevens. Enig houvast kan worden gevonden in de semiotische duiding van de manier waarop verkeersgegevens samenhangen met inhoud. Dat is evenwel een vrij abstracte exercitie die de nodige interpretatie vergt, en bovendien contextafhankelijk blijkt. De typen verkeersgegevens waarmee de wetgever tot nu toe gewoon is te werken – zoals 'nummer', 'adres' of 'cel-ID' – kennen in de technische werkelijkheid allerlei verschijningsvormen, waardoor deze soms meer en soms minder de strekking van communicatie-inhoud blootgeven. Met name bij Internetcommunicatie ontstaat een zeer complex beeld van wat verkeersgegevens wel of niet over communicatie-inhoud kunnen zeggen.

Wil men verkeersgegevens juridisch afbakenen van inhoud op een manier die verenigbaar is met de technische realiteit, dan suggereert de technische analyse van Jan Smits voor wat betreft Internetcommunicatie dat door de dynamiek en diversiteit van Internetprotocollen, verkeersgegevens niet

zinvol meer te scheiden zijn van inhoud.[202] Om het correspondentiegeheim niet uit te hollen, zouden daarom alle Internetgerelateerde verkeersgegevens onder het beschermingsregime van communicatie-inhoud moeten vallen. Voor (klassieke) telefonie valt de scheiding echter wel eenvoudiger te maken, evenals vermoedelijk voor email. Het afbakeningsprobleem zou daarom op dit moment opgelost kunnen worden door het bovengenoemde tweeledige criterium te hanteren, waarbij het nevencriterium als volgt wordt toegepast:

- verkeersgegevens behorend bij telefonie die onder het beschermingsregime van verkeersgegevens vallen worden limitatief opgesomd (zoals in de rechterkolom in Tabel 5); de overige telefoniegerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
    - locatiegegevens bij mobiele telefonie vormen een sui generis-categorie; hiervoor dient de wetgever een zelfstandige keuze te maken, omdat het voor deze te contextafhankelijk is om te bepalen of zij de strekking van communicatie-inhoud weergeven;
- verkeersgegevens behorend bij email die onder het beschermingsregime van verkeersgegevens vallen worden limitatief opgesomd (zoals in de rechterkolom in Tabel 5); de overige emailgerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
- verkeersgegevens behorend bij Internet (met uitzondering van email) vallen onder het beschermingsregime van inhoud.

## 6.2. Nadere reflectie: alles is Internet, (dus) alles wordt inhoud

Het is de vraag of de in de vorige subparagraaf geschetste benadering voldoende duurzaam is. De Grondwet zelf hoeft niet tot in detail de afbakening van verkeersgegevens en inhoud te duiden; de tekst van artikel 13 Gw zou vermoedelijk alleen de term 'post- en telecommunicatiegeheim' bevatten en de toelichting zou op hoofdlijnen een afbakening langs bovenstaande lijnen kunnen bevatten. De toelichting bij het Grondwetsartikel is echter wel leidend voor de interpretatie van het grondrecht in de toekomst. Nu kan het makkelijk een jaar of tien kan duren voordat een nieuwe grondwetsbepaling in werking treedt[203] en men zou willen dat de bepaling vervolgens ook ten minste enkele decennia meegaat. Daarom moet de toelichting bij de grondwetswijziging voldoende helder zijn om voor de komende decennia de wetgever (en wie weet op termijn ook de rechter) richting te geven aan wat op welk niveau beschermwaardig is aan telecommunicatie.

Voor een begrip van wat 'enkele decennia' betekent in termen van technologische ontwikkeling, is het zinvol te bedenken hoe de ontwikkeling van telecommunicatie in de afgelopen decennia heeft plaatsgevonden. Sinds

---

[202] Ibid., p. 48-50.

[203] Vergelijk de vorige wijziging: de tekst van het huidige art. 13 Gw werd eind 1976 door de Tweede Kamer vastgesteld en trad grotendeels in 1988 in werking.

de lancering van het wereldwijde web in 1991 heeft Internetcommunicatie fundamentele transformaties ondergaan, met onder andere de opkomst van sociale media / web 2.0, mobiel Internet, cloud computing en allerlei toepassingen die door breedbandverbindingen en eindgebruikersoftware (*peer-to-peer*-programma's, apps) mogelijk zijn gemaakt. Deze transformaties waren 25 jaar geleden moeilijk te voorzien, en de gevolgen ervan voor hoe telecommunicatie plaatsvindt waren in geen enkel opzicht te overzien. Het valt nu niet te voorzien hoe de ontwikkeling van het Internet zich in de komende dertig jaar zal doorzetten, maar het valt wel te voorspellen dat er zich onvoorspelbare transformaties zullen voordoen. En dit alles gaat gepaard met een aanzienlijke technologische turbulentie in de protocollen en standaarden die met de ontwikkelingen in infrastructuur en applicaties gemoeid zullen zijn.

Het is zeer de vraag of een indeling in telefonie, email en "overig Internet" hout snijdt. Het onderscheid is nu al aan het vervagen en zal op de middellange termijn weinig of geen relevantie meer hebben. De klassieke telefonie-infrastructuur van circuitgeschakelde telefoonnetten en GPS-mobiele telefonie raken snel uitgefaseerd; vrijwel alle telefonie is tegenwoordig al pakketgeschakeld. Waar wetgeving nu categorieën hanteert van 'telefonie over een vast of mobiel netwerk' en 'internettelefonie', wordt miskend dat vaste en mobiele telefonie nu ook al grotendeels via pakketgeschakelde infrastructuren worden afgehandeld. Daarbij is het de vraag hoe het begrip 'telefonie' in de toekomst geduid moet worden.[204] Gesprekken worden nu al via verschillende protocollen via Internet getransporteerd en het lijkt niet erg zinvol om verschillende protocollen in te delen in 'klassieke' telefonie of 'Internettelefonie' afhankelijk van waar ze het meest op lijken. Daarbij is het de vraag wat de ratio is van aparte categorieën 'telefonie' of 'email', als communicatie via Internet allerlei vormen kan aannemen, met niet alleen verschillende protocollen maar ook uiteenlopende functionaliteiten (allerlei vormen van mens-mens-, mens-machine- en machine-machine-communicatie) en formaten (tekst, spraak, beeld, multimedia). 'Email' is geen intrinsieke categorie vanuit de ratio van het correspondentiegeheim, nu een sms-bericht en een chatbericht in een online spel dezelfde functionaliteit hebben voor gebruikers als een korte email. 'Telefonie' is geen intrinsieke categorie vanuit de ratio van het correspondentiegeheim, nu 'telefoons' computers zijn geworden waarmee je even goed 'klassiek' kunt bellen ('mobiele telefonie') als Skypen ('Internettelefonie') of Whatsappen ('Internettelefonie' of overig 'Internet'?), en tegelijkertijd telefoongesprekken in het sociale verkeer vaak een uitwisselbare functie hebben met andere vormen van communicatie (als chatten, sms'en en Facebooken).

Kortom, nu alle communicatie pakketgeschakeld wordt en daarmee van Internetprotocollen gebruik maakt, heeft een categorie 'Internetcommunicatie' geen onderscheidende waarde meer. De categorieën

---

[204] Zie ook Deel 1, par. 5.

'telefonie' en 'email' hebben geen eeuwigheidswaarde wanneer alles over Internet gaat en allerlei communicatievormen in elkaar overvloeien. Wanneer alles over Internet gaat, in complexe en uitwisselbare patronen, is de consequentie ook dat alles wat met telecommunicatie te maken heeft – vanuit de in hoofdstuk 5 geschetste argumentatie – inhoud wordt.

Misschien zouden we dan ook moeten constateren dat het begrip 'verkeersgegevens' zijn langste tijd gehad heeft. In de historische ontwikkeling van telecommunicatie zijn gegevens die nodig zijn voor het transport van berichten op een zeker moment 'losgekomen' van de boodschap, waardoor ze ook voor andere doeleinden dan enkel transport gebruikt konden worden.[205] Met de komst van mobiele telefonie en vooral Internet zijn er steeds nieuwe soorten verkeersgegevens bijgekomen, die op complexe manieren samenhangen met het berichtverkeer. Bij Internetcommunicatie valt weliswaar nog wel een conceptueel onderscheid te maken tussen verkeersgegevens en de inhoud van communicatie, maar dat conceptuele onderscheid verliest sterk aan relevantie als het gaat om het secundaire gebruik voor bijvoorbeeld marketing- of opsporingsdoeleinden (naast het pure transport) van de gegevens. Verkeersgegevens zijn dermate verknoopt met communicatiepatronen, dat het vaak mogelijk is dat kennis van de verkeersgegevens gepaard gaat met kennis van de strekking van wat er wordt gecommuniceerd.

De conclusie zou dan ook kunnen zijn dat, wanneer de categorieën 'telefonie' en 'email' achterhaald raken nu alle communicatie in complexe patronen en met een grote diversiteit aan applicaties en protocollen over Internet wordt getransporteerd, alle communicatie Internetcommunicatie is. Vanuit de hiervoor genoemde redenering dat verkeersgegevens behorend bij Internet als inhoud moeten worden beschermd, is dan de conclusie dat verkeersgegevens en inhoud altijd samenvallen vanuit de ratio van het correspondentiegeheim.

Wanneer het onderscheid tussen verkeersgegevens en inhoud van communicatie wegvalt in de wolk van Internetcommunicatie, blijft overigens wel een ander onderscheid staan dat gebruikt zou kunnen worden om de reikwijdte van het correspondentiegeheim te omschrijven. Dat is een onderscheid tussen communicatiegerelateerde gegevens (inhoud en verkeersgegevens) en gebruikersgegevens.[206] Communicatiegerelateerde gegevens zijn gegevens die samenhangen met concrete communicatiehandelingen. Deze raken de vrijheid om vertrouwelijk te kunnen communiceren en zouden daarom in-

---

[205] Zie ibid., hoofdstuk 3.

[206] Dit onderscheid sluit aan op de functionele typologie naar doel van de verwerking (vanuit het aanbiedersperspectief), zie tabel 3b in par. 4.2. Gebruikersgegevens kunnen worden gezien als de gegevens die worden gegenereerd en verwerkt voor facturering en dienstbeheer, terwijl communicatiegerelateerde gegevens de gegevens zijn die worden gegenereerd en verwerkt voor transmissie van communicatie of voor toegevoegdewaardediensten.

tegraal onder artikel 13 Gw moeten vallen. Gebruikersgegevens zijn gegevens over iemands telecommunicatiegebruik in meer algemene zin, die niet samenhangen met een concrete communicatie; het zijn gegevens die iets zeggen over de gebruiker in plaats van over de communicatie. Daaronder vallen de identificerende gegevens die op basis van artikel 126na/ua/zi Sv kunnen worden gevorderd,[207] zoals NAW-gegevens, de soorten diensten en de telefoonnummers en emailadressen die iemand in gebruik heeft, alsook factuurgegevens. Vaste IP-adressen zijn vergelijkbaar met klassieke adresgegevens en zijn daarom ook gebruikersgegevens; dynamische IP-adressen kunnen echter dermate snel wisselen (ook binnen enkele minuten) dat zij sneller met concrete communicatiehandelingen in verband kunnen worden gebracht, zodat dynamische IP-adressen eerder als verkeersgegevens (en dus communicatiegerelateerde gegevens) zouden moeten worden beschouwd dan als gebruikersgegevens.[208] Naast de identificerende en factuurgegevens zouden ook geaggregeerde verkeersgegevens (welk volume wordt gebruikt over periode X door aansluiting Y? met welke telefoonnummers heeft telefoonnummer A contact over periode X?) onder het begrip 'gebruikersgegevens' kunnen worden geschaard, omdat door de aggregatie de koppeling met concrete communicatiehandelingen verdwijnt.[209] Deze gegevens raken de vrijheid vertrouwelijk te communiceren niet of nauwelijks, omdat ze niet samenhangen met concrete communicatiehandelingen en dus niet met spe-

---

[207] Art. 126na Sv geeft (evenals de parallelle artikelen 126ua en 126zi Sv) opsporingsambtenaren de bevoegdheid om 'gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst' te vorderen. Merk op dat gebruikersgegevens ook kunnen worden gevorderd op basis van art. 126n/u/zh Sv, de bevoegdheid die gemakshalve vaak wordt aangeduid als de bevoegdheid tot het vorderen van verkeersgegevens. Die aanduiding is niet helemaal correct, omdat art. 126n/u/zh zowel verkeersgegevens als gebruikersgegevens omvat ('een vordering (…) gegevens te verstrekken over een gebruiker van een communicatiedienst [oftewel gebruikersgegevens, BJK] en het communicatieverkeer met betrekking tot die gebruiker [oftewel verkeersgegevens, BJK]'). Omdat bij een vordering verkeersgegevens justitie ook bijna altijd de gebruikersgegevens nodig heeft, zijn deze twee categorieën samengenomen in één artikel.

[208] Vgl. BVerfG 24 januari 2012, 1 BvR 1299/05 (beschikbaar op http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html), §116, waarin het Duitse constitutioneel hof bepaalde dat dynamische IP-adressen onder de reikwijdte van het Duitse correspondentiegeheim vallen (dat zowel inhoud als verkeersgegevens beschermt), hetzij omdat ze nauw met concrete telecommunicatiehandelingen verbonden zijn, hetzij omdat de aanbieder voor de identificatie van een specifiek dynamisch IP-adres de daarbijbehorende verbindingsdata moet inzien en daarmee raakt aan concrete communicatiehandelingen.

[209] Daarbij is wel van belang dat de aggregatie dusdanig moet zijn dat de geaggregeerde gegevens niet meer terug te herleiden zijn tot concrete communicatiehandelingen, ook niet als de geaggregeerde gegevens in verband worden gebracht met andere gegevens die de overheid tot haar beschikking heeft of kan krijgen.

cifieke keuzes om gebruik te maken van een communicatiemiddel. Daarom vallen gebruikersgegevens niet onder de reikwijdte van artikel 13 Gw. Een onderscheid tussen communicatiegerelateerde gegevens (waaronder zowel inhoud als verkeersgegevens vallen) en gebruikersgegevens zou voor de langere termijn een bruikbaarder afbakeningscriterium kunnen bieden dan een onderscheid tussen (niet inhoudgerelateerde) verkeersgegevens en inhoud van communicatie.

## 6.3. Nog nadere reflectie: waarom communicatie(inhoud) beschermen?

De reflectie zou nog een stap verder moeten gaan. Dit rapport bevat, conform de opdracht, een zoektocht naar een antwoord op de vraag wanneer verkeersgegevens onder artikel 13 Gw beschermd zouden moeten worden omdat zij inhoud van communicatie betreffen. Ik weet niet zeker of dat de meest relevante vraag is die de grondwetgever zich zou moeten stellen vanuit het perspectief van het wenselijke grondwettelijke beschermingsniveau van verkeersgegevens of, in meer algemene zin, van communicatiegerelateerde gegevens. De analyse in dit rapport en in de aanpalende technische analyse laat namelijk zien dat verkeersgegevens niet alleen vaak – in grotere of kleinere mate – verknoopt zijn met inhoud van communicatie, maar vooral dat het sterk contextafhankelijk is welk inzicht verkeersgegevens bieden in het communicatiegedrag van burgers. Het maakt niet alleen uit welke infrastructuur en welke protocollen er worden gebruikt, en dus welke typen verkeersgegevens precies worden verwerkt, maar vooral ook welke hoeveelheid gegevens iemand beschikbaar heeft om analyses op los te laten. En, zoals in de literatuur al vaker is betoogd, die analyses zijn inmiddels niet meer primair privacygevoelig omdat zij inzicht bieden in wat er precies wordt gecommuniceerd, maar omdat zij inzicht bieden in communicatiegedrag en vooral ook in gedragspatronen in het algemeen.

De consequentie van deze argumentatie is niet alleen dat verkeersgegevens een sterk niveau van juridische bescherming behoeven omdat zij, met name als zij over een bepaalde periode en voor meerdere communicatiemiddelen beschikbaar zijn, een scherp inzicht kunnen bieden in de persoonlijke levenssfeer van burgers. De consequentie is ook dat de noodzaak van bescherming van *inhoud* van communicatie ten opzichte van andere aspecten van communicatie – en van het persoonlijke leven in het digitale tijdperk in het algemeen – opnieuw doordenking behoeft. In de negentiende eeuw was er een bijzondere reden om aan de overheid als postvervoerder toevertrouwde brieven te beschermen tegen kennisneming door de overheid. In de twintigste eeuw lag het voor de hand om deze bescherming te extrapoleren naar telefonie (de telegrafie laat ik even buiten beschouwing), omdat naast de brief de telefoon het enige middel was waarmee burgers op afstand onderling vertrouwelijk contacten konden onderhouden en het

daarbij onwenselijk was dat de overheid zo maar zou kunnen meeluisteren. In de eenentwintigste eeuw lijkt het voor de hand te liggen deze bescherming van inhoud van communicatie nu op dezelfde manier door te trekken naar Internetcommunicatie.

De ontwikkeling van Internetcommunicatie moet echter wel in perspectief worden geplaatst. Ten eerste is de functie van Internetcommunicatie veel uitgebreider en diverser dan communicatie via brief of telefoon ooit geweest is. Het gaat lang niet meer alleen om het communiceren met andere mensen of instanties, maar ook om het opslaan in de cloud van materiaal (muziek, boeken, foto's, documenten) dat vroeger in de beschermde muren van het huis lag opgeslagen. Het gaat ook om communicatie van sensoren of apparaten die via het Internet der dingen aan huis of lichaam zijn verbonden. Ten tweede is de hoeveelheid communicatie geëxplodeerd. Waar men vroeger per dag hooguit enkele brieven schreef en enkele telefoongesprekken voerde, worden nu honderden of duizenden communicatiehandelingen verricht – elke handeling op het web genereert berichtentransport. Ten derde betekent de ontwikkeling van *data mining* en profilering dat er uit grote hoeveelheden data allerlei verbanden kunnen worden afgeleid. De combinatie van deze drie aspecten betekent dat Internetcommunicatie steeds meer en steeds indringender inzicht biedt in de persoonlijke levenssfeer, ook zonder dat kennis wordt genomen van de *inhoud* van al die communicatie.

Daar komt bij dat burgers kwetsbaar zijn geworden nu we in een tijdperk komen waarin de locatie waar gegevens opgeslagen liggen, irrelevant wordt.[210] Gegevens die men opslaat in de cloud (zonder dat men deze deelt met anderen) zijn kwetsbaarder voor kennisneming door anderen dan gegevens die men thuis opslaat. Het is in dat licht begrijpelijk dat het wetsontwerp-2012 voorstelt om ook cloud-opslag onder het correspondentiegeheim te brengen,[211] maar conceptueel gezien is een cloud-opslagdienst geen nieuwe vorm van telecommunicatie (relationele privacy) maar een nieuwe vorm van materiaalopslag (ruimtelijke privacy). Het zou daarom, vanuit de ratio van de verschillende dimensies van privacybescherming, eerder passen om het huisrecht (art. 12 Gw) te actualiseren tot een meer locatieonafhankelijk, digitaal 'huis'recht dat ook extern opgeslagen maar vanuit het huis beschikbare gegevens beschermt die men van oudsher binnen het huis bewaarde.

De kwetsbaarheid voor kennisneming door anderen van vertrouwelijke gegevens in het 'locatieloze' tijdperk uit zich op vergelijkbare wijze ook in draagbare computers (laptops, tablets, smartphones) waarop men grote

---

210 Koops e.a. 2012b.

211 Door de keuze voor een telecommunicatiegeheim 'verkrijgen ook e-mail, communicatie via de sociale media, *opslag van persoonlijke bestanden in de 'cloud'* en de zoekvraag om informatie op internet via een zoekmachine bescherming onder artikel 13'. Wetsvoorstel wijziging artikel 13 Grondwet, 1 oktober 2012, p. 8 (cursivering toegevoegd).

hoeveelheden gegevens meedraagt die van oudsher alleen of vooral thuis werden bewaard. Er bestaat een groot verschil in rechtsbescherming voor burgers tegenover kennisneming door de overheid van gegevens die zijn opgeslagen op hun computer, afhankelijk van het feit of de computer in het huis staat (art. 97/110 j° 125i Sv) of op een andere plaats dan een woning die wordt doorzocht (art. 96c j° 125i Sv), of in een auto ligt die door de politie wordt onderzocht (art. 96b j° 125i Sv), dan wel door iemand bij zich wordt gedragen wanneer hij wordt aangehouden (art. 95 Sv). In de laatste twee gevallen mag elke politieambtenaar de computer in beslag nemen en onderzoeken, terwijl bij de woning dat alleen is toegestaan met toestemming van de rechter-commissaris. Het is sterk de vraag of een dergelijk verschil in rechtsbescherming van computergegevens nog gerechtvaardigd is in het mobiele tijdperk.

Nu is het vraagstuk van digitale kwetsbaarheid als zodanig niet het onderwerp van het huidige rapport, maar de uitstap naar opgeslagen gegevens toont aan dat waar vroeger gegevensopslag niet als bijzondere categorie expliciet hoefde te worden beschermd omdat het van nature grotendeels onder het huisrecht viel, gegevensopslag in het huidige mobiele en Internettijdperk niet langer onder het (huidige) huisrecht valt, waardoor een lacune in de rechtsbescherming is ontstaan.

Het feit dat Internetcommunicatie een steeds indringender inzicht biedt in de persoonlijke levenssfeer ook zonder kennisneming van inhoud, en het feit dat naast communicatie ook gegevensopslag vragen oproept over grondwettelijke bescherming, betekenen dat de grondwetgever zich moet afvragen of er nog voldoende reden is om inhoud van communicatie als een zelfstandige categorie met meer egards te behandelen dan andere vormen van privacygevoelige gegevens in het digitale tijdperk. Is voor de komende decennia de verbijzondering van privacy in bescherming van lichaam, huis en communicatie(inhoud) nog wel de meest voor de hand liggende indeling als we kijken naar de verknooptheid van Internet met het menselijk gedrag in al zijn facetten? Zijn de meest bijzondere bedreigingen voor de burger nog steeds dat de overheid fysiek het lichaam aantast, fysiek het huis binnendringt of de inhoud van vertrouwelijke communicatie beluistert?

Internetcommunicatie is niet langer een fenomeen dat zich uitsluitend in de relationele privacy van het correspondentiegeheim laat vangen; het is verknoopt met alle aspecten van wat burgers zijn en doen. Voor de kortere termijn heeft het wellicht nog zin om communicatie-inhoud – met inbegrip van verkeersgegevens die nauw verband houden met die inhoud – bijzondere bescherming te bieden ten opzichte van andere vormen van digitale kwetsbaarheid. Voor de langere termijn – en dat is een termijn die past bij het perspectief van de grondwetgever – lijkt het mij echter ook noodzakelijk om de systematiek van de privacygrondrechten over de hele linie opnieuw te doordenken, om effectief tegenwicht te bieden aan alle nieuwe vormen waarin de overheid zicht kan krijgen op de persoonlijke levenssfeer van burgers.

# 7. Samenvatting en conclusies

In dit rapport staat de volgende vraag centraal: welke typen verkeersgegevens moeten juridisch beschermwaardig worden geacht onder artikel 13 Gw, gelet op de ratio en functie van het correspondentiegeheim (zoals ik artikel 13 Gw in dit rapport aanduid), en in hoeverre zijn deze typen juridisch af te bakenen op een manier die verenigbaar is met de technische realiteit? Bij de beantwoording van deze vraag is, vanuit de nadruk die in het wetsontwerp-2012 ligt op de inhoud van communicatie als het te beschermen object onder artikel 13, vooral gekeken of het mogelijk is om een geschikte afbakening te ontwerpen tussen verkeersgegevens en inhoud.

Uit de literatuur komt naar voren dat de ratio van het correspondentiegeheim is gelegen in de vrijheid om vertrouwelijk te kunnen communiceren. Deze ratio wordt in de literatuur op een meer consistente manier beargumenteerd en doorgetrokken dan in de wetgevingsvoorstellen van de afgelopen decennia. Deze voorstellen stellen op hoofdlijnen dat het correspondentiegeheim de vertrouwelijkheid van communicatie beschermt (en daarmee beperkt is tot de inhoud van communicatie) maar bevatten ook regelmatig formuleringen die samenhangen met de vrijheid om vertrouwelijk te kunnen communiceren (en daarmee de vertrouwelijkheid van het communicatieproces in bredere zin aanduiden). Het valt daarom aan te bevelen dat de grondwetgever bij een nieuw wetsvoorstel een meer systematische uitwerking geeft van wat volgens hem de ratio van het correspondentiegeheim is in relatie tot de inhoud van communicatie en het communicatieproces in bredere zin.

Los van de vraag of verkeersgegevens, als onderdeel van het communicatieproces, als zodanig wel of niet beschermwaardig onder artikel 13 Gw worden geacht, is de vraag wat er precies onder 'verkeersgegevens' en 'inhoud' moet worden verstaan. Onder de 'inhoud' van communicatie kan worden verstaan dat deel van de communicatie dat valt onder de verantwoordelijkheid van de verzender of ontvanger (en niet van de transporteur). Verkeersgegevens zijn gegevens die vallen onder de verantwoordelijkheid van de transporteur (als transporteur). Gelet op de ratio van bescherming door artikel 13 Gw vallen onder inhoud ook (verkeers)gegevens die de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender of ontvanger.

Uit de literatuur en uit de aan dit rapport aanpalende technische analyse van Jan Smits komen diverse grijze gebieden naar voren tussen verkeersgegevens en inhoud. Sommige van deze grijze gebieden betreffen gegevens die technisch gesproken als verkeersgegevens kunnen worden gekwalificeerd, maar die duidelijk onder de verantwoordelijkheid van de verzender of ontvanger vallen en dus inhoud betreffen (sms-bericht, emailonderwerpregel). Bij de meeste grijze gebieden gaat het echter om gegevens die (deels) onder de

verantwoordelijkheid van de transporteur vallen, maar die in meer of minder sterke mate zicht bieden op de (strekking van de) inhoud van communicatie. Soms bestaat er een sterk of rechtstreeks verband met inhoud (bijvoorbeeld bij surfgegevens), vaak gaat het om een zwakker of indirecter verband (bijvoorbeeld bij emailadressen, informatienummers of poortnummers). Soms kan echter uit deze laatste gegevens ook de strekking van communicatie worden afgeleid, zeker als verkeersgegevens over lange tijd beschikbaar zijn en/of gecombineerd worden met andere gegevens.

Vallen de gegevens uit de grijze gebieden op een dusdanige wijze te groeperen dat zij volgens een voldoende scherp criterium kunnen worden geclassificeerd als wel of geen inhoud betreffend? De analyse in dit rapport heeft geen eenvoudig afbakeningscriterium opgeleverd aan de hand waarvan een logische typologie kan worden geformuleerd die eenduidig verkeersgegevens indeelt in gegevens die wel en gegevens die niet volgens het beschermingsregime van inhoud onder artikel 13 Gw beschermd moeten worden. Wel is het mogelijk om typen verkeersgegevens te ordenen aan de hand van bepaalde criteria, waarmee het afbakeningsprobleem wordt verkleind of in elk geval meer inzichtelijk wordt gemaakt. Zo kunnen verkeersgegevens worden ingedeeld naar de manier waarop zij mogelijk samenhangen met inhoud, volgens het semiotische onderscheid in soorten tekenrelaties. Verkeersgegevens die een afbeelding of diagram vormen van de inhoud of die indexicaal verwijzen naar inhoud, hebben over het algemeen een nauwer verband dan verkeersgegevens die metaforisch of symbolisch verwijzen naar inhoud. Dit biedt een zinvol materieel criterium, maar het is wel vrij abstract en vergt de nodige interpretatie. Een tweede mogelijkheid is een indeling naar het doel van de verwerking, waarmee bestaande juridische categorieën verkeersgegevens kunnen worden geclassificeerd en waarbij bepaalde typen gegevens uitgesloten kunnen worden omdat zij niet met inhoud samenhangen. Een derde mogelijkheid is om verkeersgegevens in te delen naar privacygevoeligheid; omdat kennisneming van verkeersgegevens een verkillend effect kan hebben op de vrijheid om privé te communiceren, kunnen de meer privacygevoelige categorieën verkeersgegevens onder artikel 13 Gw worden beschermd, mogelijk op hetzelfde niveau als inhoud.

Geen van deze drie typologieën levert een ideale of eenduidige afbakening op, maar zij kunnen wel worden gecombineerd. Dat levert een stroomschema op van vijf vragen:

1. Valt het gegeven onder verantwoordelijkheid van de communicatiepartner(s)?
   Zo ja -> inhoud. Zo nee -> ga naar vraag 2.
2. Biedt het verkeersgegeven mogelijk zicht op de inhoud?
   Zo nee -> verkeersgegeven. Zo ja -> ga naar vraag 3.
3. Houdt het verkeersgegeven verband met een concrete communicatiehandeling?
   Zo nee -> verkeersgegeven. Zo ja -> ga naar vraag 4.
4. Is het een verkeersgegeven behorend bij telefonie (maar geen locatiegegeven)?
   Zo ja -> verkeersgegeven. Zo nee -> ga naar vraag 5.

5. Heeft het verkeersgegeven een sterke relatie met de inhoud? Er is een sterke relatie als het verkeersgegeven semiotisch een afbeelding, diagram, index, sterke metafoor of een sterk symbool is van de inhoud. Zo ja -> inhoud. Zo nee -> verkeersgegeven.

Aan de hand hiervan kunnen in beginsel alle categorieën verkeersgegevens worden ingedeeld naar inhoud of (pure) verkeersgegevens. In Tabel 5 in hoofdstuk 5 is een overzicht gegeven van wat deze classificatie oplevert voor concrete categorieën, waarbij een onderscheid gemaakt kan worden tussen telefonie, email en (overig) Internet. Bij Internetcommunicatie (buiten email) blijkt daarbij een complex beeld te bestaan wat verkeersgegevens wel of niet over communicatie-inhoud kunnen zeggen, zodat het moeilijk is om subcategorieën te definiëren die integraal als puur verkeersgegeven kunnen worden beschouw. Vaak zal de combinatie van verschillende gegevens het nodige suggereren over wat er is gecommuniceerd. Bovendien is het, aldus de technische analyse van Jan Smits, door de dynamiek en diversiteit van Internetprotocollen nauwelijks werkbaar om verkeersgegevens zinvol te scheiden van inhoud. Om die reden zouden verkeersgegevens bij Internetcommunicatie (met uitzondering van email) integraal als inhoud moeten worden behandeld.

Op een iets hoger abstractieniveau (dat wenselijk is voor de grondwetgever), kan de afbakening die volgt uit het stroomschema als volgt in meer algemene zin worden samengevat. In beginsel is een tweeledig afbakeningscriterium te formuleren dat juridisch voldoende abstractieniveau heeft en dat inhoudelijk goed werkt om de kern van het onderscheid tussen inhoud en verkeersgegevens te duiden. Het **hoofdcriterium** is onder wiens verantwoordelijkheid de gegevens vallen: inhoud is datgene wat onder verantwoordelijkheid van de verzender valt; verkeersgegevens zijn gegevens die onder verantwoordelijkheid van de transporteur (als transporteur) vallen. Het **nevencriterium** is dat verkeersgegevens die (juridisch-)technisch onder het begrip verkeersgegevens vallen, onder artikel 13 Gw als inhoud moeten worden behandeld wanneer zij de strekking weergeven van (een deel van) datgene wat valt onder de verantwoordelijkheid van de verzender. Het nevencriterium kan daarbij als volgt worden toegepast:[212]

- verkeersgegevens behorend bij telefonie die onder het beschermingsregime van verkeersgegevens vallen, kunnen limitatief worden opgesomd (bijvoorbeeld: nummer verzender/ontvanger, datum/tijdstip/duur, soort dienst); de overige telefoniegerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
    - locatiegegevens bij mobiele telefonie vormen een sui generis-categorie die te contextafhankelijk is om in te delen naar inhoud/

[212] Hierbij laat ik verkeersgegevens behorend bij post buiten beschouwing, omdat deze geen reguleringsprobleem opleveren. De huidige wetgeving in de Postwet en het Wetboek van Strafvordering zou gewoon kunnen worden gehandhaafd.

verkeersgegevens; hiervoor dient de wetgever een zelfstandige keuze te maken;

- verkeersgegevens behorend bij email die onder het beschermingsregime van verkeersgegevens vallen, kunnen limitatief worden opgesomd (bijvoorbeeld: emailadres verzender/ontvanger, datum/tijdstip, volume); de overige emailgerelateerde verkeersgegevens vallen onder het beschermingsregime van inhoud;
- verkeersgegevens behorend bij Internet (met uitzondering van email) vallen integraal onder het beschermingsregime van inhoud.

Voor dit moment lijkt dit een indeling te bieden die recht doet aan de ratio van het correspondentiegeheim, voldoende abstractieniveau heeft vanuit het perspectief van de (grond)wetgever, en in de technisch-juridische werkelijkheid uitvoerbaar zou moeten zijn.

Bij deze conclusie passen echter twee kanttekeningen. De categorieën 'telefonie' en 'email' raken achterhaald nu alle communicatie in complexe patronen en met een grote diversiteit aan applicaties en protocollen over Internet wordt getransporteerd. Vrijwel alle communicatie is tegenwoordig Internetcommunicatie. Naast de technische convergentie van infrastructuren en diversificatie van protocollen, vindt er ook een sociale convergentie plaats van 'gesprekken' en 'berichtenverkeer', en tegelijkertijd een diversificatie aan communicatievormen van mens tot mens, mens tot machine, en machine tot machine. Vroeg of laat zullen in dit communicatielandschap 'telefonie' en 'email' geen bijzonder betekenisvolle categorieën meer zijn, waardoor het hiervoor gesuggereerde aanwijzen van verkeersgegevens behorend bij telefonie en email een zinloze of eindeloos complexe exercitie wordt in historisch-analogisch redeneren. In het Internettijdperk verliest het conceptuele onderscheid tussen verkeersgegevens en inhoud sterk aan relevantie als het gaat om het secundaire gebruik (naast het pure transport) van de gegevens. De conclusie zou dan moeten luiden dat, wanneer alle communicatie over Internet gaat, verkeersgegevens en inhoud altijd samenvallen vanuit de ratio van het correspondentiegeheim, en dat het historisch gegroeide begrip 'verkeersgegevens' zijn langste tijd gehad heeft om het gebruik van communicatiegerelateerde gegevens te reguleren.[213]

In plaats van een onderscheid tussen verkeersgegevens en inhoud van communicatie, zou dan een onderscheid tussen gebruikersgegevens en communicatiegerelateerde gegevens gehanteerd kunnen worden om de reikwijdte van het correspondentiegeheim te omschrijven. Communicatiegerelateerde

---

[213] Voor verkeersgegevens bij post zou een uitzondering kunnen worden gemaakt, omdat de infrastructuren van post (fysieke pakketjes die in de fysieke brievenbus worden afgeleverd) en telecommunicatie (digitale pakketjes die via elektronische signalen worden afgeleverd) – voor zover het gaat om de infrastructuur van transport – niet convergeren.

gegevens zijn gegevens die samenhangen met concrete communicatiehandelingen en raken daarom direct de vrijheid om vertrouwelijk te kunnen communiceren; deze vallen integraal onder artikel 13 Gw. Gebruikersgegevens zijn gegevens over het telecommunicatiegebruik in meer algemene zin: het betreft gegevens over de gebruiker, zoals welke telefoonnummers, emailadressen en IP-adressen iemand in gebruik heeft en factuurgegevens; ook geaggregeerde verkeersgegevens zouden onder het begrip 'gebruikersgegevens' kunnen worden geschaard. Deze gegevens raken de vrijheid vertrouwelijk te communiceren niet of nauwelijks, omdat ze niet samenhangen met concrete keuzes om gebruik te maken van een communicatiemiddel, en vallen daarom buiten de reikwijdte van artikel 13 Gw. Een onderscheid tussen communicatiegerelateerde gegevens en gebruikersgegevens zou voor de langere termijn een bruikbaarder afbakeningscriterium kunnen bieden dan een onderscheid tussen (niet inhoudgerelateerde) verkeersgegevens en inhoud van communicatie.

Tot slot moet echter ook een tweede kanttekening worden geplaatst, namelijk dat Internetcommunicatie niet langer een fenomeen is dat zich uitsluitend in de relationele privacy van het correspondentiegeheim laat vangen. Het Internet is verknoopt met alle aspecten van wat burgers zijn en doen, en dat zal met de ontwikkeling van het Internet der dingen alleen maar toenemen. Internetcommunicatie biedt een steeds indringender inzicht in de persoonlijke levenssfeer, ook zonder dat kennis wordt genomen van inhoud; daarnaast zijn inmiddels ook opgeslagen gegevens (die losstaan van communicatie in de zin van relationele privacy) kwetsbaar voor kennisneming door derden. Informatie- en communicatietechnologie roept aldus vragen op over grondwettelijke bescherming van niet alleen de relationele privacy, maar ook de ruimtelijke en lichamelijke privacy. Het is daarom de vraag of er nog voldoende reden is om inhoud van communicatie als een zelfstandige categorie met meer egards te behandelen dan andere vormen van privacygevoelige gegevens in het digitale tijdperk. Voor de kortere termijn heeft het wellicht nog zin om communicatie-inhoud – met inbegrip van verkeersgegevens die nauw verband houden met die inhoud – bijzondere bescherming te verlenen ten opzichte van andere vormen van digitale kwetsbaarheid. Voor de langere termijn – en dat is een termijn die past bij het perspectief van de grondwetgever – is het ook noodzakelijk om de systematiek van de privacygrondrechten over de hele linie opnieuw te doordenken, om effectief tegenwicht te bieden aan alle nieuwe vormen waarin de overheid zicht kan krijgen op de persoonlijke levenssfeer van burgers.

# Bijlage

## Wetsvoorstel wijziging artikel 13 Grondwet (Internetconsultatieversie), 1 oktober 2012

### Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon en telegraafgeheim

### VOORSTEL VAN WET

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

### ARTIKEL I

Er bestaat grond het hierna in de artikelen II en III omschreven voorstel tot verandering in de Grondwet in overweging te nemen.

### ARTIKEL II

Artikel 13 van de Grondwet komt te luiden:

### Artikel 13

1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.

2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, met machtiging van een of meer bij de wet aangewezen ministers.

3. De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.

(…)

# MEMORIE VAN TOELICHTING

## I. ALGEMEEN DEEL

### 1. Inleiding

#### 1.1 Algemeen

Dit wetsvoorstel strekt ertoe de reikwijdte van de onschendbaarheid van het brief-, telefoon- en telegraafgeheim dat in artikel 13 Grondwet (hierna: artikel 13) is neergelegd, uit te breiden naar alle communicatiemiddelen. In de praktijk voldoet de huidige grondwettelijke bepaling niet langer; de modernisering van artikel 13 zal moeten leiden tot een techniekonafhankelijke benadering van de reikwijdte. De directe aanleiding voor onderhavig voorstel tot wijziging van artikel 13 is gelegen in het rapport van de Staatscommissie Grondwet van november 2010 en de daaropvolgende kabinetsreactie.[214] De Staatscommissie Grondwet ging in het tweede deel van haar rapport, waarin de grondrechten centraal staan, onder meer in op het vraagstuk van grondrechten in het digitale tijdperk. Zij adviseerde een aantal grondrechten aan te passen in verband met de ontwikkelingen in de informatietechnologie. Het kabinet oordeelde in reactie op het advies van de Staatscommissie Grondwet dat de huidige techniekafhankelijke en limitatieve formulering van de beschermde communicatiemiddelen de normatieve betekenis van artikel 13 aan de wetgever en rechter in de weg staat. Zij leidt tot netelige interpretatievraagstukken en het risico van inconsistentie in de uitleg en de beoogde en gewenste rechtsbescherming. Dit probleem wordt versterkt doordat de formulering van artikel 13 ver achter loopt bij de verwante verdragsrechten waarin de laatste jaren nieuwe ontwikkelingen, normen en formuleringen zijn uitgekristalliseerd. Het onderhavige voorstel is aangekondigd in een brief[215], waarover ook is beraadslaagd in beide kamers van de Staten-Generaal.[216]

#### 1.2 Achtergrond en noodzaak

Sinds de jaren 90 van de vorige eeuw wordt een politieke en juridische discussie over modernisering van artikel 13 Grondwet gevoerd. Deze discussie kan niet los worden gezien van de ontwikkelingen in de digitale samenleving. Informatiestromen en communicatie vinden heden ten dage hun weg

---

214 Kamerstukken II 2011/12, 31 570, nr. 20.
215 Kamerstukken II 2011/12, 31 570, nr. 21.
216 Handelingen I 2011/12, nr. 18, item 3, blz. 3-29; item 5, blz. 31-47 en Kamerstukken II 2011/12, 31 570, nr. 22 en nr. 23.

via zeer diverse elektronische communicatiemiddelen. Deze digitalisering is reeds enkele decennia gaande en heeft onder meer geleid tot vergaande veranderingen in de wijze waarop communicatie in de samenleving gestalte krijgt. Maar ook nieuwe elektronische communicatiemiddelen hebben geleid tot ingrijpende wijzigingen in communicatiepatronen en informatiestromen in de samenleving. Stelden traditionele media zoals kranten, radio en tv slechts enkelen in staat te communiceren met velen en bepaalden die enkelen wat noodzakelijke en wenselijke informatie was - de nieuwe elektronische communicatiemiddelen stellen velen in staat zelf informatie te zoeken en te distribueren. Waar de oude technologie voorzag in identieke informatie voor het gehele publiek, openen de nieuwe communicatiemiddelen vele wegen voor velen om toegang te krijgen tot en het verspreiden van een ongelimiteerde hoeveelheid informatie. Deze digitalisering heeft de ontwikkeling van een informatiesamenleving, ook iSamenleving genoemd, verder voortgestuwd.[217] Kenmerkend voor de informatiesamenleving is onder meer dat informatie een eigenstandige economische waarde vertegenwoordigt. Het beheren, genereren, overdragen en gebruik van informatie is een wezenlijke factor van betekenis in de informatiesamenleving – ook voor de wijze waarop en de mate waarin wordt gecommuniceerd. Die veranderingen – toename van het aanbod van informatie en van het aantal communicatiemiddelen - hebben onherroepelijk gevolgen voor het communicatiegeheim dat artikel 13 beoogt te beschermen. De gedigitaliseerde informatiesamenleving stelt ons voor nieuwe vragen waar het gaat om privé, ofwel vertrouwelijk, te kunnen communiceren, met name in de gevallen waarin de tekst van het huidige artikel 13 nog niet voorziet in adequate bescherming van nieuwe communicatiemiddelen. De behoefte om privé te kunnen communiceren is in de gedigitaliseerde informatiesamenleving onverminderd groot. Artikel 13 beschermt privé-communicatie nu enkel wanneer deze plaatsvindt per brief, telefoon of telegraaf. De hoge vlucht die het gebruik van elektronische communicatiemiddelen heeft genomen in de digitale informatiesamenleving noodzaakt derhalve tot het heroverwegen van de reikwijdte van artikel 13 Grondwet.

Het huidige artikel 13 beschermt het brief-, telefoon- en telegraafgeheim. Communicatie met behulp van andere middelen worden niet door deze grondwetsbepaling beschermd. De opsomming van artikel 13 is daarmee anachronistisch: bijna niemand communiceert meer via de telegraaf, andere communicatiemiddelen hebben daarentegen een plaats verworven in de maatschappij die het belang van communicatie per brief minst genomen overtreffen. Nieuwe communicatiemiddelen en -technieken lijken enkel op gekunstelde wijze – door extensieve interpretatie – en dan nog slechts tot op zekere hoogte onder artikel 13 te brengen. In dit verband kan worden gewezen op de reden die de grondwetgever in 1983 aanvoerde om – naast het

---

[217] WRR-rapport *iOverheid* (2011), p. 32 e.v.

aloude briefgeheim – ook het telefoon- en telegraafgeheim constitutionele bescherming te bieden: de regering was "van mening dat naast de briefwisseling ook de communicatie door middel van telefoon en telegraaf een belangrijke plaats in het maatschappelijk verkeer heeft verworven en in verband met het privé-karakter ervan onder de grondrechten moet worden opgenomen".[218] Indien het criterium is dat communicatie privé moet zijn, ongeacht het middel of de techniek met behulp waarvan wordt gecommuniceerd, is duidelijk dat elektronische vormen van communicatie niet langer onbesproken kunnen blijven. In deze zin sluit onderhavig voorstel naadloos aan bij hetgeen de grondwetgever in 1983 voor ogen had. De mate van bescherming die artikel 13 biedt, is op dit moment afhankelijk van het gebruikte middel: communicatie per brief is op grondwettelijk niveau beter beschermd dan communicatie per telefoon. Dat doet geen recht aan één van de belangrijkste kenmerken van de digitale samenleving, te weten convergentie van communicatiemiddelen. Eén en hetzelfde communicatiemiddel wordt immers in toenemende mate gebruikt voor verschillende vormen van communicatie. Een voorbeeld is het gebruik van e-mail- en internetfuncties via mobiele telefoons, of het opvragen van audio- en videodiensten via het internet. Een verschil in bescherming louter vanwege een onderscheid van het gebruikte communicatiemiddel is dan ook niet langer gerechtvaardigd. Gelet op deze omstandigheden is modernisering van artikel 13 noodzakelijk en dringend gewenst.

Bij de voorbereiding van het onderhavige voorstel zijn naast het rapport van de Staatscommissie Grondwet 2010 ook eerdere adviezen, regeringsvoorstellen, alsmede kritiek daarop van betekenis geweest. Zo hebben wij ons rekenschap gegeven van de voorstellen die de regering in 1999 heeft ingetrokken, terwijl deze aanhangig waren in de Eerste Kamer[219], het daaropvolgende rapport van de Commissie Grondrechten in het Digitale Tijdperk (commissie-Franken)[220], de adviezen van de Raad van State naar aanleiding van de regeringsvoorstellen uit 2001[221], en kritiek vanuit de wetenschap op de eerdere voorstellen. Tot slot is vermeldenswaardig het in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties uitgebrachte rapport *Constitutional Rights and New Technologies*, een internationaal-vergelijkend onderzoek met betrekking tot grondrechten en nieuwe technologieën in België, Frankrijk, Duitsland, Zweden, Canada en de Verenigde Staten, dat in 2007 aan de Tweede Kamer is aangeboden.[222]

---

[218] Kamerstukken II 1975/76, 13 872, nr. 3, blz. 44.

[219] Kamerstukken II 1996/97, 25 443 nr. A.

[220] Rapport Grondrechten in het digitale tijdperk, Kamerstukken II 2000/01, 27 460, nr. 1, bijlage 1.

[221] Gepubliceerd in: *De grondwetsherziening 2006, Naar een nieuwe grondwet*. Documentatiereeks deel 39, SDU Uitgevers 2006, blz. 431-472 (artikel 7 Grondwet), blz. 475-495 (artikel 10 Grondwet) en blz. 499-536 (artikel 13 Grondwet).

[222] Kamerstukken II 2006/07, 27 460, nr. 5.

Een bezinning op adequate bescherming van het communicatiegeheim kan zich niet beperken tot uitsluitend de Nederlandse Grondwet. Op het internationale vlak tekent zich sinds 2000 een aantal scherpe contouren af met betrekking tot de bescherming van het communicatiegeheim in het digitale tijdperk. Op het moment dat de commissie-Franken in 2000 haar rapport uitbracht en in de eerste jaren nadien was er in internationaalrechtelijk opzicht nog weinig materiaal voorhanden met betrekking tot het vraagstuk van het brief- en telecommunicatiegeheim. Daarin is inmiddels het nodige veranderd. Mede naar aanleiding van de kritische overwegingen van de Raad van State ten aanzien van de in 2001 ingediende wetsvoorstellen[223] heeft Nederland zich vanaf 2004 in Europees verband hard gemaakt voor de totstandkoming van een richtinggevende uitspraak van de Raad van Europa. Aan een dergelijke uitspraak bestond behoefte vanwege de in sterke mate toenemende betekenis van de digitalisering en informatisering voor de Nederlandse Grondwet en voor de toekomstige visie op regelgeving van de Raad van Europa ter zake. Die inspanningen resulteerden destijds in de – op het niveau van de Raad van Europa vastgestelde - eerste *Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society* van 13 mei 2005.[224] De verklaring stelt voorop dat de grondrechten – waaronder het recht op respect voor privé-leven en correspondentie – dezelfde bescherming verdienen in een digitale omgeving als in een niet-digitale omgeving. Beperking van het respect voor correspondentie mag niet plaatsvinden vanwege het enkele feit dat de correspondentie geschiedt in een digitale vorm. Ook nadien zijn er in de Raad van Europa nog vele verklaringen en aanbevelingen tot stand gekomen met het perspectief op de naleving van mensenrechten in de digitale informatiesamenleving.[225]

Vanuit het mondiale perspectief valt wat betreft de ontwikkelingen op het mensenrechtelijk terrein na het laatste wetsvoorstel van de regering in 2001 het volgende te melden. Hiervoor werd reeds gewezen op de Verklaring van het Comité van Ministers van de Raad van Europa van 2005. Deze verklaring kwam opnieuw in mondiaal perspectief aan de orde bij gelegenheid van de *World Summit on the Information Society*, die onder auspiciën van de Verenigde Naties in november 2005 plaatsvond. In de slotverklaring van die top zijn "freedom of expression and the free flow of information" erkend als "essential" voor de informatiesamenleving. Recent nam de

---

223 Zie: *De grondwetsherziening 2006, Naar een nieuwe grondwet*. Documentatiereeks deel 39, SDU Uitgevers 2006, blz. 499-536 (artikel 13 Grondwet).

224 CM (2005)56.

225 Zie bijvoorbeeld aanbeveling CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines en aanbeveling CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet. Op 15 maart 2012 aanvaardde het Comité van Ministers van de Raad van Europa de Internet Governance Strategy 2012-2015, CM(2011)175 final

VN-mensenrechtenraad de Resolutie "on the promotion, protection and enjoyment of human rights on the Internet" aan, waarin de Raad stelt dat de rechten die mensen offline hebben ook online beschermd moeten worden.[226] Aldus is ook het belang van de gelding en bescherming van de grondrechten in een digitale samenleving op mondiaal niveau erkend. Wij zien hierin vanuit internationale hoek steun voor het - ook al eerder door Nederlandse kabinetten beleden - uitgangspunt dat *online* en *offline* in beginsel zoveel mogelijk dezelfde normen moeten gelden.[227] Dit adagium blijkt overigens niet altijd onverkort en eenvoudig toepasbaar. Voortschrijdend inzicht noopt tot enige nuancering van dit uitgangspunt; naarmate het ICT-recht tot verdere wasdom komt, is aandacht voor de concrete belangen die achter de rechtsnormen schuilgaan, van groot belang gebleken. Hieraan moet blijvend aandacht worden besteed. De eigenheid van de vraagstukken in de *online* wereld is immers niet altijd één op één te transponeren in de *offline* wereld.[228]

Tot slot kan betekenis van de wetgeving die in het kader van de Europese Unie tot stand is gekomen, nauwelijks worden overschat. Het EU-Handvest van de Grondrechten ziet in het algemeen op bescherming van het communicatiegeheim. De secundaire EU-wetgeving ziet tot in detail op bescherming van het elektronisch communicatiegeheim. Die ontwikkeling werd eind jaren '90 van de vorige eeuw ingezet en is al vergaand uitgekristalliseerd. Deze wetgeving heeft ook in de Nederlandse rechtsorde zijn beslag gekregen. Dit internationale juridische kader wordt nader toegelicht in paragraaf 5 van de toelichting. Daarnaast zullen in de paragrafen 2, 3 en 4, die een toelichting geven op concrete onderdelen van het onderhavige voorstel, indien relevant ook specifieke verwijzingen naar internationale verdragsbepalingen, aanbevelingen en jurisprudentie worden opgenomen.

## 1.3 Doelstelling

Het voorstel vervangt de onschendbaarheid van het brief-, telefoon- en telegraafgeheim door het recht op het brief- en telecommunicatiegeheim. Het heeft tot doel de huidige grondwettelijke bescherming die nu ziet op communicatie per brief, telegraaf of telefoon, uit te breiden naar alle huidige en toekomstige communicatiemiddelen. Het wetsvoorstel strekt aldus tot modernisering van het huidige artikel; met dit voorstel wordt gestreefd naar een volledig techniekonafhankelijke bescherming. Doordat niet langer enkel wordt gerefereerd aan specifieke communicatiemiddelen, maar wordt gekozen voor een specifieke (briefgeheim) en een generieke bescherming (telecommunicatiegeheim) verkrijgen ook e-mail, communicatie via de sociale

---

[226] A/HRC/20/L.13 (5 juli 2012).
[227] Kamerstukken II 1999/00, 27 460, nr. 1, blz. 11
[228] *Overheden over internationalisering en ICT-recht*, J.E.J. Prins, E.J. Koops e.a., 2000, p. 85.

media, opslag van persoonlijke bestanden in de 'cloud' en de zoekvraag om informatie op internet via een zoekmachine bescherming onder artikel 13. Het voorstel bevat een verruiming van de reikwijdte van artikel 13 tot alle telecommunicatie, ongeacht het middel of de techniek die is gebruikt om te communiceren, en brengt deze, voor zover het om de inhoud gaat, in het tweede lid onder hetzelfde niveau van bescherming als nu voor het briefgeheim geldt, namelijk dat beperking slechts mogelijk is met een voorafgaande machtiging van de rechter. Indien de beperking in het belang van de nationale veiligheid plaatsvindt, volstaat een machtiging van een bij de wet aangewezen minister. Tot slot is een algemene regelingsopdracht voor de wetgever opgenomen met het oog op de mogelijk veranderende betekenis van het brief- en telecommunicatiegeheim in horizontale verhoudingen en in toekomstige technologische en maatschappelijke ontwikkelingen.

(…)

2.3 Verkeersgegevens

Bij communicatie met gebruikmaking van daartoe bestemde kanalen ontstaan gegevens die niet zien op de gecommuniceerde boodschap als zodanig, maar die betrekking hebben op de overdracht of op de opslag van het bericht. Te denken valt bijvoorbeeld aan gegevens over tijdstip, plaats, duur van en betrokken nummers bij een telefoongesprek en gegevens over tijdstip, adressering en omvang van een e-mailbericht. Zij zien niet op de inhoud van de communicatie en worden hierna aangeduid als 'verkeersgegevens'.

Opgemerkt zij dat de juridische definitie van verkeersgegevens op de diverse rechtsterreinen op verschillende wijzen wordt vastgesteld. Artikel 126n Wetboek van Strafvordering omschrijft deze gegevens als (bij algemene maatregel van bestuur aangewezen) "gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker". Dergelijke gegevens, die thans in het Besluit vorderen gegevens telecommunicatie zijn aangewezen als verkeersgegevens, hebben geen betrekking op de inhoud van telecommunicatie en vallen derhalve niet onder de werking van artikel 13. Verkeersgegevens kennen in de EU-Richtlijnen die zien op elektronische communicatienetwerken en -diensten een eigen, reeds vastgelegde betekenis.[229] In deze betekenis omvatten verkeersgegevens die gegevens, die worden verwerkt voor het overbrengen van communicatie over een elektronisch

[229] Art. 5, eerste lid, van de ePrivacyrichtlijn luidt: 'Tot verkeersgegevens behoren onder meer gegevens met betrekking tot de routering, de duur, het tijdstip of het volume van een communicatie, het gebruikte protocol, de locatie van de eindapparatuur van de verzender of de ontvanger, het netwerk waarop de communicatie begint of eindigt en het begin, het einde of de duur van de verbinding'. Er is geen sprake van een gesloten lijst van gegevens die hiertoe behoren.

communicatienetwerk of voor de facturering ervan. Verkeersgegevens worden ook wel "inhoudloze transmissiegegevens" genoemd.[230] Voor zover verkeersgegevens tevens persoonsgegevens zijn, worden deze beschermd door artikel 10 Grondwet. Bezien vanuit het hiervoor beschreven rechtens te beschermen belang vallen verkeersgegevens, omdat het geen inhoud van de communicatie betreft, buiten de reikwijdte van artikel 13.

Verkeersgegevens geven op zich geen inzicht in de inhoud van de communicatie, maar wel in andere aspecten die verband kunnen houden met de inhoud van de communicatie.[231] Verkeersgegevens kunnen bovendien naar hun aard raken aan de telecommunicatievrijheid. Met instemming wordt op dit punt verwezen naar de opmerking van de Raad van State ter zake van metagegevens in zijn advies op het wetsvoorstel uit 2001: "De strekking van artikel 13 is dat burgers zonder inmenging vertrouwelijk met elkaar kunnen communiceren. Zou iemand weten of vermoeden dat de overheid weet welke telefoongesprekken hij voert, dan zou dat voor hem reden kunnen zijn om bepaalde gesprekken niet meer te voeren. Dit doorbreekt de vertrouwelijkheid van de communicatie op zichzelf niet, maar raakt wel de vrijheid van (tele)communicatie."[232] De Commissie Franken en de meerderheid van de Staatscommissie Grondwet wilden verkeersgegevens niet binnen de reikwijdte van artikel 13 brengen.[233]

In dit wetsvoorstel is het standpunt van de beide commissies gevolgd en zijn verkeersgegevens niet onder de reikwijdte van artikel 13 gebracht. De reden daarvan is dat zij niet de inhoud van de telecommunicatie betreffen en dat een andersluidende keuze tot gevolg zou hebben dat voor inzage in verkeersgegevens steeds een rechterlijke machtiging nodig zou zijn, hetgeen gelet op de aard van deze gegevens te vergaand zou zijn.

Aandacht verdient evenwel dat de inhoud van telecommunicatie in technische zin soms ook als een verkeersgegeven wordt gezien. Zo wordt het onderwerp van een e-mail in technische zin wel tot de verkeersgegevens betreffende die e-mail gerekend. Maar in juridische zin valt het onderwerp van een e-mail onder de reikwijdte van artikel 13 omdat dat onderwerp betrekking heeft op de inhoud van de e-mail. Een ander voorbeeld is een sms-bericht: technisch gezien is een dergelijk bericht in zijn geheel een verkeersgegeven, maar juridisch gezien omvat een sms-bericht – naast verkeersgegevens – tevens de inhoud van communicatie. De conclusie is dat aan de bescherming

---

230 A.H.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen 2006, p. 4 en 5.

231 L.F. Asscher en A.H. Ekker, *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam 2003.

232 W01.01.0467/I, p. 6 en 7. In dezelfde zin de Registratiekamer (voorganger van het College Bescherming Persoonsgegevens) in zijn reactie op het rapport van de commissie-Franken: (vindplaats).

233 Rapport Staatscommissie Grondwet, p. 89. De minderheid wenste verkeersgegevens wel onder de reikwijdte van artikel 13 te brengen, zie p. 88 van het rapport.

van artikel 13 niet kan afdoen dat gegevens die de inhoud van de telecommunicatie betreffen in technische zin als een verkeersgegeven worden beschouwd. Verkeersgegevens die niet mede betrekking hebben op de inhoud van telecommunicatie vallen echter buiten de reikwijdte van artikel 13.

(…)

# Over de auteurs

Prof. dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT, het Tilburg Institute for Law, Technology, and Society van de Universiteit van Tilburg. Van 2005-2010 was hij lid van De Jonge Akademie, een onderdeel van de Koninklijke Nederlandse Akademie van Wetenschappen.

Koops doet onderzoek naar regulering en technologie, in het bijzonder strafrechtelijke onderwerpen als opsporingsbevoegdheden en privacy, computercriminaliteit, cryptografie en DNA. Hij is ook geïnteresseerd in andere onderwerpen binnen technologieregulering, zoals identificatie, dataprotectie, digitale grondrechten, regulering door techniek, de maakbare mens, en regulering van bio-, nano- en neurotechnologie. Van 2004-2009 leidde hij een VIDI-onderzoeksprogramma over recht, technologie en schuivende machtsverhoudingen.

Koops studeerde wiskunde en algemene literatuurwetenschap in Groningen. Hij promoveerde in 1999 in de rechtswetenschappen op een onderzoek naar regulering van cryptografie. Koops is co-redacteur van zeven boeken over technologieregulering, *Emerging Electronic Highways* (1996), *ICT Law and Internationalisation* (2000), *Starting Points for ICT Regulation* (2006), *Cybercrime and Jurisdiction* (2006), *Constitutional Rights and New Technologies* (2008), *Dimensions of Technology Regulation* (2010) en *Engineering the Human* (2013). Hij publiceerde diverse boeken en vele artikelen over recht en technologie. Zijn webpublicatie *Crypto Law Survey* wordt wereldwijd beschouwd als een standaardbron over cryptografie-regulering.

Prof. dr. mr. J.M. (Jan) Smits (1953) startte in 1972, na het behalen van het HBS-diploma, de studie rechten aan de KUB. Na "omzwervingen" op de rechtswinkel en wetenschapswinkel rondde hij in 1982 zijn studie rechten af met het behalen van de meesterstitel. Na drie jaar als wetenschappelijk medewerker te hebben gewerkt aan de Juridische Faculteit van de KUN ging hij in 1985 als universitair docent naar Juridische Informatica aan de Utrechtse Universiteit. Tegelijk met deze overstap verscheen zijn eerste boek: 'Het recht uitgedaagd door de computer'. In Utrecht maakte hij zes jaar deel uit van een onderzoeksgroep die met behulp van technieken uit de kunstmatige intelligentie een methodologie ontwikkelde voor het bouwen van juridische kennissystemen. Verschillende publicaties getuigen van de neerslag van dit onderzoek. Tegelijkertijd bekwaamde hij zich verder op het terrein van zowel het nationale als internationale telecommunicatierecht. Het onderzoek op dit terrein resulteerde in zijn dissertatie in 1990 onder de titel: *Legal aspects of implementing international telecommunication links; institutions, regulations and instruments*. Op 1 september 1992 werd hij (deeltijd)hoogleraar Recht & Techniek aan de Technische Universiteit Eindhoven. Samen met Bekkers

schreef hij in 1998 *Mobile Communications: Standards, Regulation, and Applications*, in 1999 gevolgd door *Digital Video Broadcasting: Technology, standards, and regulation*, dit keer samen met De Bruin, beide uitgegeven bij Artech House. In 2001 verscheen met diverse auteurs *Advances in Network and Distributed Systems Security*. Vanaf hetzelfde jaar één van de auteurs van Tekst & Commentaar Telecommunicatie- en Privacyrecht. Zijn recente onderzoek heeft vooral betrekking op de relatie tussen vernieuwing van (telecom)infrastructuren en de rol van het EU-recht hierbij, zoals meer specifiek de rol van Diensten van Algemeen Economisch Belang.

Een aantal jaren was hij lid van de Mediaraad, en tevens van het Stichtingsbestuur van de Stichting Informatiediensten code (Stic), toezichthouder gebruik van 0800/0900-nummers.

Vanaf september 2003 tot begin 2013 was hij lid van de Wetenschappelijk Technische Raad van de Stichting Surf. Tevens is hij zelfstandig gevestigd telecommunicatieconsultant en (mede-)oprichter van 2knowit BV.

Ir. F. J. van der Kroon (1962) MBA is na zijn studie Luchtvaart- en Ruimtevaarttechniek aan de TU Delft (1989) in de telecommunicatie-industrie gaan werken (Alcatel). In die tijd is hij opgeleid tot Cisco Certified Internetworking Expert (1993) en heeft hij zijn MBA behaald aan de University of Bradford (1998). Van 2009 tot en met 2011 heeft hij bij het Lectoraat Ondernemen en Innoveren van De Haagse Hogeschool onderzoek gedaan naar en gepubliceerd over de innovatiekracht van bedrijven. Sinds 2012 is hij partner bij 2knowit.

# Literatuurlijst


Agre, P.E. (1998), 'Introduction', in: P.E. Agre en M. Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, MA / London: The MIT Press, p. 1-28.

Article 29 Working Party (2000), *Privacy on the Internet*, Brussels, Article 29 Data Protection Working Party, 21 November 2000.

Asscher, L. (2000), 'Trojaans hobbelpaard. Een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk', *Mediaforum*(7/8), p. 228-233.

Asscher, L. (2003), *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam, Otto Cramwinckel.

Asscher, L.F. en A.H. Ekker (red.) (2003), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever.

Bekkers, R.N.A. en J.M. Smits (1997), *Mobiele Telecommunicatie; Regulering, standaarden en toepassingen*, Deventer, Kluwer.

Blok, P. (2002), *Het recht op privacy*, Den Haag, Boom Juridische uitgevers.

Bordewijk, J.L. en B. Van Kaam (1982), *Allocutie. Enkele gedachten over communicatievrijheid in een bekabeld land*, Baarn, Bosch & Keuning NV.

Castellani, A., N. Bui, P. Casari, M. Zach and M. Zorzi, 'Architecture and Protocols for the Internet of Things: A Case Study', *8th IEEE International Conference on Pervasive Computing and Communications Workshops* (PERCOM Workshops), Mannheim, 29 March-2 April 2010, p. 678-683.

Commissie Grondrechten in het digitale tijdperk (2000), *Rapport*, Den Haag, mei 2000.

Dommering, E.J. (1997), 'Geen telefoongeheim op de elektronische snelweg', *Mediaforum*(10), p. 142-147.

Dommering, E.J. (red.) (2000), *Informatierecht: fundamentele rechten voor de informatiesamenleving*, Amsterdam, Otto Cramwinckel.

Dorst, A.J.A. van (1982), 'Het postgeheim', in: A.K. Koekkoek, W. Konijnenbelt en F.C.L.M. Crijns (red.), *Grondrechten. Commentaar op Hoofdstuk 1 van de herziene Grondwet*. Nijmegen: Ars Aequi, p. 279-297.

Ekker, A.H. (2003), 'Publiekrechtelijke bescherming van verkeersgegevens', in: L.F. Asscher en A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel, p. 41-58.

Fischer, J.C. (2010), *Communications Network Traffic Data. Technical and Legal Aspects*, diss. Eindhoven, TU/e.

Hes, R. (2003), 'Verkeersgegevens in nieuwe generaties telecommunicatiesystemen', in: L.F. Asscher en A.H. Ekker (red.), *Verkeersgegevens.*

*Een juridische en technische inventarisatie*. Amsterdam: Otto Cramwinckel, p. 12-40.

Hes, R. (2003), 'Verkeersgegevens in nieuwe generaties telecommunicatiesystemen', in: L.F. Asscher en A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever, p. 12-40.

Hildebrandt, M. (2008), 'Profiling and the Identity of the European citizen', in: M. Hildebrandt en S. Gutwirth (red.), *Profiling the European Citizen*, s.l., Springer, p. 303-326.

Hildebrandt, M. en S. Gutwirth (red.) (2008), *Profiling the European Citizen. Cross-disciplinary perspectives*, s.l., Springer.

Hofman, J.A. (1995). *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, diss. Amsterdam (VU), Zwolle, W.E.J. Tjeenk Willink.

Koops, B.J. (2002), *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer, Kluwer.

Koops, B.J. (2003), 'Verkeersgegevens en strafrecht: een agenda voor discussie', in: : L.F. Asscher en A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*. Amsterdam: Otto Cramwinckel, p. 59-92.

Koops, B.J., G. Bodea, G. Broenink e.a. (2012a), *Juridische scan openbronnonderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg/Delft, TILT/TNO, juli 2012.

Koops, B.J., R. Leenes, P. De Hert en S. Olislaegers (2012b), *Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing* Tilburg / Den Haag, TILT / WODC.

Lindenberg, K. (2002), *Van ORT tot ORO. Een verzameling van de werken die hebben geleid tot het Oorspronkelijk Regeringsontwerp van een nieuw Wetboek van Strafvordering (1914)*, Groningen, Rijksuniversiteit Groningen.

MacGillavry, E.C. (2004). *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven*, diss. Groningen, Nijmegen, Wolf Legal Publishers.

Mediaraad (1993), *Advies van de Mediaraad inzake herstructurering van het beleid betreffende de informatievoorziening*, Den Haag, Mediaraad.

Odinot, G., D. De Jong, J.B.J. Van der Leij e.a. (2012), *Het gebruik van de telefoon- en internettap in de opsporing*, Meppel, Boom Lemma.

Patijn, A. (2004), 'Verplichte opslag van verkeersgegevens?', *Computerrecht* (2), p. 134-138.

Smits, A.H.H. (2006). *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen, Wolf Legal Publishers.

Smits, J.M. (1993), 'Telecommunicatieprivacy en regelgeving: nood of

deugd? Een beschouwing naar aanleiding van een Ontwerp-Richtlijn van de EG', *Mediaforum* (5), p. 50-53.
Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, 2010.
Steenbruggen, W. (2009), *Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk*, Amsterdam, Otto Cramwinckel.
Studiecommissie VMC (1999), 'Preadvies inzake een nieuwe tekst voor de artikelen 7 en 13 van de Grondwet', *Mediaforum* (11/12), p. 1-8.