

I know what you did last summer!

Over grenzeloze en ongegeneerde verwerking van verkeersgegevens in de informatiemaatschappij

WILFRED STEENBRUGGEN Gegevens over het communicatiegedrag van de burger worden tegenwoordig op grote schaal in de systemen van telecomoperators en internetproviders vergaard en vastgelegd. Deze gegevens, ook wel verkeersgegevens genoemd, zijn noodzakelijk om de transmissie mogelijk te maken en rekeningen op te stellen.

Mr. drs. W.A.M. Steenbruggen

is werkzaam als onderzoeker bij het Instituut voor Informatierecht te Amsterdam.
E-mail: steenbruggen@jur.uva.nl

De vergaring en verwerking van deze gegevens worden steeds onoverzichtelijker, doordat het aantal verschillende informatiediensten toeneemt en de consument als gevolg van de toenemende mobiliteit van randapparatuur steeds meer en overal waar hij zich bevindt, contact met verschillende netwerken heeft.¹ Steeds meer en steeds vaker worden op allerlei verschillende systemen gegevens achtergelaten. Langzamerhand tekent zich een 24/7 traceerbaarheid van iedere gebruiker af. Zijn interesses, intieme of minder intieme contacten, ja, zijn gehele dagelijks leven kan in de informatiemaatschappij aan de hand van de opgeslagen gegevens worden achterhaald.

In de loop van de jaren zijn de bevoegdheden van justitie en veiligheidsdiensten om gegevens omtrent het telecommunicatieverkeer te vorderen, aanzienlijk uitgebreid. Hoewel oorspronkelijk de bevoegdheid bedoeld was die gegevens te vorderen aan de hand waarvan bepaald kon worden of het zwaardere middel van de telecomtap kon worden ingezet, heeft de bevoegdheid een zelfstandig karakter gekregen. Op de wijze waarop deze bevoegdheid in de Nederlandse rechtsorde is geïntroduceerd en vervolgens vele malen is aangepast aan de wensen van justitie en veiligheidsdiensten valt wel een en ander aan te merken. Momenteel is het veel belangrijker dat na 11 september 2001 in internationaal verband vergaande voorstellen worden gedaan om de bevoegdheden van justitie en veiligheidsdiensten verder te verruimen onder het mom van de noodzakelijke 'war against terrorism'. In dat kader wordt gepleit voor een structurele bewaarplicht voor verkeersgegevens. Telecomaanbieders, waaronder internetproviders, worden in sommige voorstellen verplicht om de ver-



keersgegevens van alle gebruikers van hun diensten en netwerken voor een periode van 1 tot 2 jaar te bewaren.² Voor sommigen is deze termijn zelfs nog te kort.³ Is een dergelijke structurele bewaarplicht wel in overeenstemming met de fundamentele rechten op privacy en het communicatiegeheim?

De instelling van een bewaarplicht betekent dat de transporteur een verlengstuk van justitie en veiligheidsdiensten wordt. Zijn systemen worden een op elk willekeurig moment raadpleegbare databank waarin een schat aan persoonsgegevens is opgeslagen. Met behulp van deze gegevens kan dan een uitermate nauwkeurig en gedetailleerd beeld van het dagelijks leven van iedere burger worden verkregen. Niet alleen kunnen zijn contacten met anderen in kaart worden gebracht, ook zijn interesses, zijn bewegingen. De burger wordt 24 uur per dag 7 dagen per week

Bron: ANP

traceerbaar, identificeerbaar en analyseerbaar aan de hand van zijn communicatiegedrag.

In sommige opzichten zijn telecomaandieners nu reeds een verlengstuk van justitie en veiligheidsdiensten. De transporteur heeft namelijk in de huidige Telecommunicatiewet (Tw) vérgaande verplichtingen tot meewerken opgelegd gekregen. Zo dient hij op eigen kosten zijn telecommunicatienetwerk of -dienst aftapbaar te maken (artikel 13.1 j° 13.6 Tw) en mee te werken aan de uitvoering van een concrete taplast (artikelen 126m en 126t Sv j° 13.2 Tw),⁴ op vordering verkeersgegevens te verstrekken (artikelen 126n en 126u Sv j° artikel 184 Sr) en de gegevens die noodzakelijk zijn om een tap te gelasten of verkeersgegevens te vorderen, te leveren of zelfs te achterhalen door middel van een bestandsanalyse (artikel 13.4 Tw). In het laatste geval bestaat overigens al een (beperkte) bewaarplicht. Artikel 13.4 lid 2 Tw verplicht telecomaandieners verkeersgegevens van gebruikers waarvan zij niet over identificerende gegevens beschikken, voor een termijn van 3 maanden te bewaren.⁵

Tot nog toe heeft de Nederlandse regering telkens aangegeven (nog) niet over te willen gaan tot een ruimere bewaarplicht. De regering heeft echter na 11 september 2001 wel aangekondigd onderzoek te verrichten naar de categorieën gegevens die telecomaandieners bewaren en de belemmeringen die de opsporings- en veiligheidsdiensten ondervinden door de afwezigheid van bewaarplichten van historische verkeersgegevens.⁶ Nu een structurele bewaarplicht niet van de internationale agenda te branden lijkt, is het de hoogste tijd eens te onderzoeken hoe een structurele bewaarplicht voor verkeersgegevens zich ten opzichte van (inter)nationale grondrechtelijke waarborgen ter bescherming van de privacy en het communicatiegeheim verhoudt.

Verkeersgegevens | Voordat we op de fundamenteelrechtelijke waarborgen kunnen ingaan, dient eerst globaal een technisch kader te worden uiteengezet.

Tegenwoordig is telecommunicatie niet meer denkbaar zonder dat gebruik wordt gemaakt van databanken waarin persoonsgegevens worden gekoppeld aan elektronische adresgegevens om de juiste routing en bestemming van een boodschap tot stand te brengen.⁷ Steeds vaker treedt een vermenging op van individuele communicatieve handelingen en het waarnemen en vastleggen van persoonsgegevens.⁸

Bij telefonie kan nog een onderscheid worden gemaakt tussen verkeersgegevens en de inhoud van de getransporteerde informatie; dit hangt samen met het feit dat het transport en de routing c.q. besturing gescheiden zijn. Bij ISDN bijvoorbeeld wordt de scheiding tussen inhoud en verkeersgegevens (technisch gezien) gemarkeerd door de scheiding tussen het spraakkanaal dat de inhoud vervoert en het signaleringskanaal dat boodschappen verstuurt ten behoeve van het vervoeren van die inhoud. Deze signaleringsgegevens zorgen voor het opzetten, instandhouden

en afbreken van het circuit tussen de beller en de ontvanger van een gesprek. Ook wordt de toestand van het netwerk continu gecontroleerd. Signalering zorgt tevens voor het genereren van de informatie (begin- en eindtijd, nummergegevens) die noodzakelijk is voor het factureren.

De opkomst van datatoepassingen die gebaseerd zijn op het Internetprotocol (IP) stelt deze scheiding echter ter discussie. De communicatie die door middel van IP tot stand wordt gebracht, kan nogal wat 'gedaanten' hebben, omdat er een groot aantal diensten is ontwikkeld. E-mail, bijvoorbeeld, is een zeer belangrijke toepassing waarbij de scheiding tussen inhoud en verkeersgegevens inzichtelijk is. De gebruiker van een e-mailprogramma stelt een boodschap samen die voorzien wordt van separate adresinformatie (e-mailadres). Ook technisch is hier een scheiding zichtbaar tussen de boodschap die de inhoud van de te versturen IP-pakketten vormt, en de adresinformatie die in de header van de pakketten terechtkomt.

Kijken we naar een toepassing als websurfen dan wordt de situatie al diffuser. Hierbij haalt een gebruiker door middel van een verzoek de inhoud van een bepaalde webpagina op. De inhoud van deze pagina vormt de communicatie. Teneinde deze communicatie over te brengen toetst de gebruiker een URL in, bijvoorbeeld www.google.com, die ergens in het netwerk wordt vertaald naar het juiste IP-adres. De URL is een verkeersgegeven, maar het IP-adres ook. Complexer wordt het echter bij het gebruik van de zoekmachine. Wanneer de gebruiker een zoekopdracht geeft, wordt de zoekopdracht in de URL opgenomen en naar de zoekmachine gestuurd. De URL is nu niet slechts een verkeersgegeven meer, maar tevens een deel van de inhoud van de communicatie.

De techniek maakt derhalve een strikte scheiding tussen inhoud en verkeersgegevens onmogelijk.⁹ Bovendien is verwerking van verkeersgegevens niet per definitie minder privacygevoelig dan kennisname van de inhoud van communicatie. In het tijdperk van de vaste telefonie waren er slechts weinig verkeersgegevens: aansluitnummers, registratie of een gesprek daadwerkelijk heeft plaatsgevonden en tijdstip en duur van gesprek. Tegenwoordig worden naast deze gegevens nog veel meer gegevens door de verschillende transporteurs verwerkt. Voorbeelden daarvan zijn de aard van de dienst, welke route heeft de communicatie afgelegd, volume, (de meer of minder nauwkeurige) locatie van de gebruiker, (ruwe) gegevens over de inhoud, model en type randapparaat, operating system, bestandsformaat et cetera. Op grond hiervan kunnen door derden uitermate gedetailleerde communicatie- en interesseprofielen van gebruikers worden opgesteld. Hieruit kan informatie worden afgeleid die vaak privacygevoeliger is dan de inhoud van communicatie. Het Wetboek van Strafrecht gaat er traditioneel vanuit dat inhoud privacygevoeliger is dan de gegevens over het telecommunicatieverkeer. Naar aanleiding van het

hiervoor staande kan worden vastgesteld dat dit uitgangspunt herzien, althans aanzienlijk genuanceerd moet worden.

Privacy en communicatiegeheim in Europees verband | Op Europees niveau zijn artikel 8 EVRM en de EU-privacyrichtlijnen van belang. Binnen de Europese Unie zorgt Richtlijn 95/46/EG (Algemene privacyrichtlijn)¹⁰ voor de harmonisatie van de voorwaarden van het recht op bescherming van de persoonlijke levenssfeer die in de rechtssystemen van de lidstaten zijn vastgelegd. Deze richtlijn onderbouwt en versterkt de beginselen die zijn opgenomen in artikel 8 EVRM en in het Verdrag van Straatsburg.¹¹ Richtlijn 97/66/EG (ISDN-richtlijn)¹² specificeert de bepalingen van deze richtlijn voor de telecommunicatiesector. Ik zal hierna eerst artikel 8 EVRM bespreken.

Artikel 8 EVRM | Artikel 8 EVRM garandeert ieder het recht op respect voor zijn privé-leven, [...] en zijn correspondentie. Beperkingen op deze rechten moeten voldoen aan de eisen van het tweede lid, i.e. zij dienen te zijn voorzien bij wet en noodzakelijk in een democratische samenleving in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Het EHRM heeft door middel van een interpretatie van het begrip 'correspondence' in combinatie met het begrip 'private life' nieuwe communicatiemiddelen onder de bescherming van artikel 8 EVRM gebracht. In *Klass* bepaalde het hof op deze wijze voor het eerst dat telefoonverkeer onder artikel 8 beschermd is.¹³ Door de toepassing van deze gecombineerde benadering bij nieuwe communicatiemiddelen wordt tegenwoordig algemeen aangenomen dat artikel 8 EVRM op alle vormen van informatieoverdracht van toepassing is. In *Malone* gaf het hof aan dat ook metering records en in het bijzonder het gekozen telefoonnummer integraal deel uitmaken van de beschermde communicatie.¹⁴ In *P.G. & J.H.* heeft het hof dit recent herhaald.¹⁵ Ook verkeersgegevens worden derhalve onder artikel 8 beschermd. In het laatste arrest merkt het hof evenwel op dat

'Metering which does not per se offend against Article 8 if for example done by the telephone company for billing purposes, is by its very nature to be distinguished from the interception of communications which may be undesirable and unjustified in a democratic society unless justified.'

Uit dit arrest kan worden afgeleid dat verwerking van verkeersgegevens door de telecomaandierder voorzover dit nodig is voor de facturering en, naar men mag aannemen, ten behoeve van de transmissie van de

communicatie, niet in strijd is met artikel 8 EVRM. Verwerking ten behoeve van deze doeleinden is inherent aan de dienstverlening. Daarmee onderscheidt verwerking van verkeersgegevens zich van kennisname van de inhoud. Voorzover de verwerking buiten de genoemde doeleinden treedt, moet de verwerking echter voldoen aan de eisen van artikel 8 EVRM. Bij de toets hieraan hecht het hof in dit arrest veel waarde aan het beperkte kader van de verstrekking aan justitie (de informatie die was verstrekt, bestond slechts uit de telefoonnummers die gebeld waren vanaf een bepaalde locatie in een welomschreven periode). De verstrekking was mogelijk onder de toepasselijke wetgeving, wanneer dit noodzakelijk is ten behoeve van de opsporing van strafbare feiten (een uitzondering op de hoofdregel van anonimisering of verwijdering, neergelegd in de Engelse Telecommunicatiewet). De informatie diende ter ondersteuning van ander bewijs waarbij de tijdstippen van de telefoongesprekken van belang waren. De verstrekking is derhalve niet in strijd met artikel 8 EVRM.

Hoe het hof over verkeersgegevens buiten het beperkte kader van de vaste telefonie zal oordelen, is nog niet geheel duidelijk. Aannemelijk lijkt dat voor verwerking van verkeersgegevens ten behoeve van strafvordering en nationale veiligheid (voorzover verwerking niet noodzakelijk is ten behoeve van de facturering of verlening van de dienst) vergelijkbare eisen als voor de interceptie van communicatie zullen worden gesteld.¹⁶ Dit betekent dat de beperking een wettelijke grondslag moet hebben in de zin van de *Huvig & Kruslin*-uitspraken¹⁷ van het hof. De aanwezigheid van een wettelijke norm of een norm in vaste rechtspraak is niet genoeg. De wettelijke norm dient ook te voldoen aan een aantal kwaliteitseisen. Een onafhankelijke rechter of andere instantie moet de verwerking kunnen controleren. De wettelijke grondslag moet bepalingen bevatten met betrekking tot de duur van de beperking en regels met betrekking tot de delicten waarvoor verkeersgegevens mogen worden verwerkt. De wettelijke regeling moet derhalve nauwkeurig bepalen binnen welke grenzen en op welke wijze de maatregel kan worden toegepast: de doeleinden waarvoor de gegevens mogen worden verwerkt, de tijd dat ze mogen worden bewaard (indien ze mogen worden bewaard) en de toegang ertoe moeten strikt beperkt zijn.

In het kader van de eis dat beperkingen noodzakelijk moeten zijn in een democratische samenleving, toetst het hof of er een dringende noodzaak is voor de opgelegde beperking en of maatregel proportioneel is. In dat kader wordt getoetst of de maatregel geschikt is om het beoogde doel te bereiken en of niet kan worden volstaan met een minder ingrijpende beperking. In het kader van deze toets zullen ook de rechtmatige belangen van de telecomaandierders worden meegenomen. De belasting die een structurele bewaarplicht op hun bedrijfsvoering legt, is aanzienlijk.

Het individu heeft recht op 'een adequate bescher-

ming tegen arbitraire interceptie', stelde het hof in *Malone*. Een adequaat rechtsmiddel dient derhalve tegen een beperking van artikel 8 EVRM open te staan. Elke lidstaat heeft een positieve verplichting hiervoor zorg te dragen.¹⁸ In de *Klass*-uitspraak wordt, evenals in *Leander*¹⁹ de nadruk gelegd op de behoefte aan effectieve garanties tegen misbruik 'gezien het gevaar dat een systeem van geheim toezicht voor de bescherming van de veiligheid van de staat inhoudt voor het ondermijnen of zelfs vernietigen van de democratie, hoewel men zich op de bescherming ervan beroept'. Uit *Klass* volgt dat grootschalig verkennend of algemeen toezicht op communicatie niet door de beugel kan. In deze uitspraak stelt het hof dat de beoordeling van passende en effectieve waarborgen tegen mis-

Adequate waarborgen

bruik van alle omstandigheden van het geval afhangt. Het hof hecht er in casu echter doorslaggevende waarde aan dat het Duitse G-10-Gesetz geen verkennend of algemeen toezicht toestaat en niet in strijd is met artikel 8 EVRM, omdat het voorziet in adequate waarborgen. De Duitse wetgeving voorziet in de volgende waarborgen: het toezicht is beperkt tot gevallen waarin er aanwijzingen zijn om een persoon te verdenken, er kunnen alleen maatregelen worden genomen indien het vaststellen van de feiten met een andere methode geen uitzicht op succes biedt of veel moeilijker is en zelfs dan mag het toezicht alleen op de specifieke verdachte of zijn vermoedelijke contactpersonen betrekking hebben.

Op grond hiervan kan worden geconcludeerd dat een structurele bewaarplicht voor verkeersgegevens waarschijnlijk niet in overeenstemming met artikel 8 EVRM zal zijn. Een dergelijke maatregel lijkt niet proportioneel, al was het alleen maar omdat elke band met een redelijke verdenking van een ernstig strafbaar feit wordt losgelaten. Iedere burger wordt daarmee een potentiële verdachte. Voorts is voor mij de vraag of een dergelijke bewaarplicht efficiënt is, dat wil zeggen geschikt om het beoogde doel te bereiken, en of voor het bereiken van het doel niet met een minder ingrijpend middel volstaan kan worden. Een beperkte bewaarplicht gericht op de verkeersgegevens van een beperkt aantal personen, wanneer er een redelijk vermoeden is van de beraming, voorbereiding van een ernstig strafbaar feit, die voor een beperkte, eventueel verlengbare periode kan worden opgelegd, lijkt eerder in overeenstemming met artikel 8 EVRM.

EU-privacyrichtlijnen | De artikelen 6, 7, 13, 17 leden 1 en 2 van de Algemene privacyrichtlijn en de artikelen 4, 5, 6 en 14 van de ISDN-richtlijn hebben in het bijzonder betrekking op de rechtmatigheid van gegevensverwerking door transporteurs. Deze bepa-

lingen stellen telecomaandieners in staat om gegevens over telecommunicatieverkeer onder bepaalde zeer strikte voorwaarden te verwerken. Beide richtlijnen zijn van toepassing op de verwerking van persoonsgegevens op internet, met inbegrip van verkeersgegevens betreffende abonnees en gebruikers.

Algemene privacyrichtlijn | De Algemene privacyrichtlijn is van toepassing op verkeersgegevens, voorzover deze kunnen worden aangemerkt als persoonsgegevens. Dit is het geval wanneer de gegevens herleidbaar zijn tot een natuurlijk persoon en deze persoon geïdentificeerd kan worden zonder onevenredig veel moeite. Hoewel wellicht niet elk verkeersgegeven als persoonsgegeven gekwalificeerd kan worden,²⁰ zullen de verkeersgegevens waarop een toekomstige bewaarplicht zal zien, wel als persoonsgegevens in de zin van de richtlijn aan te merken zijn. Overigens lijkt aannemelijk dat verkeersgegevens in de meeste gevallen tijdens het gehele verwerkingsproces als persoonsgegevens aangemerkt kunnen worden, omdat er een partij is die de natuurlijke persoon waarop de gegevens betrekking kan hebben, kan identificeren. Bij de bewaarplicht gaat het echter niet om zuiver technische gegevens, maar om gegevens die iets zeggen over wanneer, wat, hoelang, waar et cetera een bepaalde gebruiker communiceert. Een bewaarplicht veronderstelt derhalve dat de gegevens over gebruik van een netwerk of dienst gekoppeld zijn aan identificerende gegevens. Artikel 6 lid 1 sub b van de Algemene privacyrichtlijn bepaalt dat gegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en vervolgens niet mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor de gegevens zijn verzameld. Artikel 6 lid sub e bepaalt dat gegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en vervolgens worden verwerkt. Artikel 13 stelt de lidstaten in staat de reikwijdte te beperken van onder andere artikel 6 lid 1 indien dit noodzakelijk is ter vrijwaring van de veiligheid van de staat, de openbare veiligheid of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

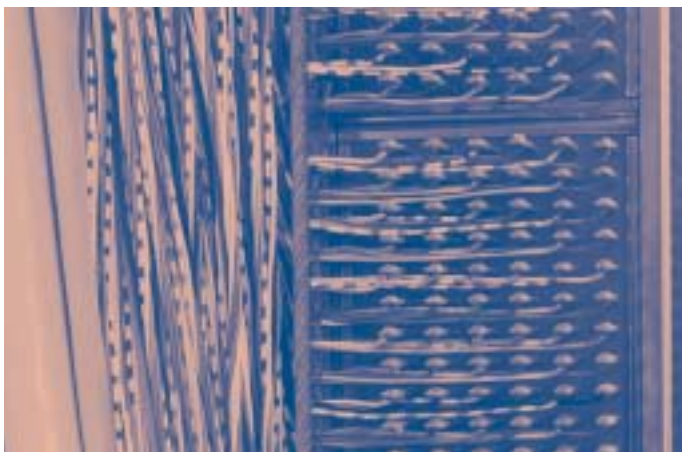
ISDN-richtlijn | De toepassing van de hiervoor genoemde beginselen wordt nader gespecificeerd in de artikelen 5 en 6 lid 2 tot en met 5 van de ISDN-richtlijn. Artikel 5 garandeert het vertrouwelijke karakter van gesprekken via openbare telecommunicatienetwerken en via algemeen beschikbare telecommunicatiediensten. De lidstaten moeten het afluisteren, aftappen of anderszins onderscheppen of controleren van gesprekken door anderen dan de gebruikers verbieden, indien de betrokken gebruikers daarmee niet hebben ingestemd, tenzij sprake is van een uitzondering op grond van artikel 14 lid 1.

Op grond van de ISDN-richtlijn is de algemene regel dat verkeersgegevens na beëindiging van het gesprek meteen moeten worden gewist of geanonimiseerd (artikel 6 lid 1). Artikel 6 lid 2 maakt hierop een uitzondering: bepaalde gegevens mogen voor het opstellen van facturen en voor interconnectiebetalingen worden verwerkt, maar alleen tot aan het einde van de termijn waarbinnen de rekening kan worden betwist. Artikel 14 lid 1 staat de lidstaten toe de reikwijdte te beperken van de in artikel 6 bedoelde rechten en plichten, indien dit noodzakelijk is ter vrijwaring van de veiligheid van de staat en voor het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten als bedoeld in artikel 13 lid 1 van de Algemene privacyrichtlijn.

Omdat de ISDN-richtlijn te sterk op spraaktelefonie is georiënteerd, en daarmee techniekafhankelijk, is in het kader van de 'telecoms review' een nieuwe richtlijn met betrekking tot privacy en elektronische communicatie totstandgekomen.²¹ Dit had heel wat voeten in de aarde, maar op 12 juli 2002 is uiteindelijk de definitieve versie van de richtlijn vastgesteld. De nieuwe Richtlijn privacy en elektronische communicatie moet op 31 oktober 2003 in nationaal recht zijn geïmplementeerd.

De nieuwe richtlijn brengt een aantal wijzigingen ten opzichte van de oude ISDN-richtlijn. De belangrijkste wijzigingen zijn de introductie van een techniekafhankelijke definitie van verkeersgegevens en de regeling van cookies en spam.²² Volgens artikel 2 sub b zijn verkeersgegevens gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering daarvan. Deze definitie maakt ten ene male duidelijk dat het gaat om de gegevens die door de transporteur worden verwerkt ten behoeve van zijn dienstverlening. Artikel 5 van de richtlijn draagt lidstaten op het ver-

Bron: ANP



trouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens te waarborgen. De lidstaten dienen met name het af luisteren, aftappen, opslaan, of anderszins onderscheppen en controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers te verbieden, indien de betrokken ge-

bruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15 lid 1.

Ook onder artikel 6 is de hoofdregel dat verkeersgegevens worden gewist of geanonimiseerd, zodra ze niet meer nodig zijn voor de transmissie van communicatie. Hierop geeft artikel 6 de volgende uitzonderingen. Verkeersgegevens die noodzakelijk zijn voor de facturering en interconnectiebetalingen mogen worden verwerkt tot het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten. Voorts mogen verkeersgegevens worden verwerkt ten behoeve van de marketing van elektronische communicatiediensten of ten behoeve van de levering van toegevoegde waardediensten, wanneer de gebruiker of abonnee waarop de gegevens betrekking hebben, hiervoor zijn uitdrukkelijke toestemming gegeven heeft en zelfs dan alleen voor zolang verwerking noodzakelijk is.

Artikel 15 staat de lidstaten toe de reikwijdte van de in artikel 6 bedoelde rechten en plichten te beperken, indien dat in een democratische samenleving noodzakelijk is ter waarborging van de nationale veiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische communicatiesysteem. Aanknopingspunt hierbij is artikel 8 lid 2 EVRM. Dit betekent dat de noodzakelijkheidseis op dezelfde manier wordt ingevuld als in de jurisprudentie van het EHRM gebeurt. Daartoe kunnen de lidstaten onder meer wetgevingmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren. Artikel 15 geeft duidelijker dan voorheen het geval was aan dat beperkingen op de rechten en plichten van artikel 6 moeten voldoen aan de eisen van artikel 8 lid 2 EVRM.

Op grond van zowel de ISDN-richtlijn als de nieuwe Richtlijn privacy en elektronische communicatie geldt derhalve ten aanzien van verkeersgegevens een telecomspecifieke eis van doelbinding die strikter is dan de doelbinding van de Algemene privacyrichtlijn. Hiermee wordt beoogd op de jurisprudentie van het EHRM ten aanzien van telefonie voort te bouwen. Het Europese regelgevingskader gaat ervan uit dat inhoud en verkeersgegevens onlosmakelijk met elkaar verbonden zijn. Een beperking op de privacy en communicatiegeheim zoals dat voor modernere communicatiemiddelen is uitgewerkt in de EU-richtlijnen, zal derhalve dienen te voldoen aan de eisen van artikel 8 lid 2 EVRM zoals die in de jurisprudentie van het Europese Hof ten aanzien van de interceptie van communicatie zijn gesteld.

Dat artikel 15 van de nieuwe richtlijn nu expliciet stelt dat een bewaarplicht voor een beperkte termijn kan worden opgelegd, betekent derhalve niet dat een generieke bewaarplicht van een tot twee jaar, laat staan langer, kan worden opgelegd. Zoals hiervoor weergegeven in het kader van de bespreking van artikel 8 EVRM dient een dergelijke bewaarplicht te worden opgevat als een vorm van grootschalig verkennend of

algemeen toezicht te worden beschouwd, hetgeen in het kader van artikel 8 EVRM niet is toegestaan.

Een kortere bewaarplicht in individuele gevallen waarbij sprake is van een verdenking van een strafbaar feit, wanneer een andere maatregel dan het opleggen van een bewaarplicht geen uitzicht op succes biedt of veel moeilijker is, en de maatregel alleen op de specifieke verdachte of zijn vermoedelijke contactpersonen betrekking heeft, kan onder omstandigheden wel in overeenstemming zijn met de eisen van 8 EVRM en de beginselen van de EU-richtlijnen. In elk geval zullen ook dan adequate garanties tegen misbruik moeten bestaan, zoals toezicht door een onafhankelijke instantie die, zo nodig, in staat is in te grijpen.

De Grondwet | De Nederlandse Grondwet beschermt van oudsher bepaalde aspecten van privacy, te weten het huisrecht en het briefgeheim. Aan het briefgeheim is in 1983 het telefoongeheim toegevoegd. Uit hetzelfde jaar stamt artikel 10 van de Grondwet dat het recht op eerbiediging van de persoonlijke levenssfeer vastlegt. In het verlengde daarvan bracht de grondwetswijziging een opdracht aan de wetgever om de bescherming van persoonsgegevens ter hand te nemen. Het resultaat is dat de huidige Grondwet in artikel 10 lid 1 het recht op eerbiediging van de persoonlijke levenssfeer in het algemeen vastlegt en in artikel 13 een bijzondere bescherming biedt voor communicatie. Het tweede en derde lid van artikel 10 voorzien in een opdracht aan de wetgever om regels te stellen ten aanzien van persoonsgegevens. De Nederlandse rechter hanteert het uitgangspunt dat de reikwijdten van artikel 8 EVRM en artikel 10 Grondwet min of meer vergelijkbaar zijn. De grenzen die artikel 10 Grondwet aan de mogelijkheid van een bewaarplicht ten aanzien van verkeersgegevens stelt, gaan derhalve zeker niet verder dan de hiervoor in het kader van artikel 8 EVRM en de EU-richtlijnen geschetste. Ik laat artikel 10 Grondwet hier dan ook verder buiten beschouwing.

Artikel 13 | Sinds 1848 is in de Nederlandse Grondwet het grondrecht op briefgeheim opgenomen dat specifiek ziet op de vertrouwelijkheid in de relatie tussen transporteur en de gebruiker van diens diensten. Artikel 154 Grondwet 1848 omschreef het briefgeheim als volgt:

‘Het geheim der aan de post of andere openbare instelling van vervoer toevertrouwde brieven is onschendbaar, behalve op last des rechters, in de gevallen in de wet omschreven’

Tot 1983 veranderde aan deze formulering niets, afgezien van wat komma's en de plaats in de Grondwet.²³ Het grondrecht leidde een vrij ongestoord en onbesproken bestaan. Er was geen discussie over de grondslagen en de betekenis van het grondrecht. Dui-

delijk was dat het grondrecht zich richtte tegen het Staatsbedrijf der PTT; andere openbare instellingen van vervoer waren er niet. Buijs vroeg zich daarom ook vertwijfeld af wat in godsnaam bedoeld kon zijn met ‘openbare instelling van vervoer’.²⁴

In 1983 werd aan het briefgeheim het telefoon- en telegraafgeheim toegevoegd en viel ook de beperking tot het ‘aan het vervoer toevertrouwde’ weg, waardoor het geheim tegenover en binnen iedere overheidsinstelling kon worden ingeroepen. Hiermee werd beoogd ook brieven te beschermen die een andere overheidsinstantie – als voorbeeld diende de gevangenisdirecteur – moesten passeren, alvorens bij de geadresseerde aan te komen. Dit betekent dus niet dat het transportelement als zodanig geen rol meer speelde bij de bepaling van beschermingswaardigheid. Deze uitbreiding vormt louter een erkenning van het feit dat de overheid in haar hoedanigheid van transporteur altijd aan het briefgeheim is gebonden.

De ratio van het grondrecht is, gezien het voornoemde, dat gebruikers slechts ongestoord kunnen communiceren, wanneer zij erop kunnen vertrouwen dat hun communicatie veilig aan een transporteur ter vervoer kan worden toevertrouwd. Het grondrecht op communicatiegeheim is derhalve bij uitstek een grondwettelijke waarborg tegen schending van de vertrouwelijkheid door de transporteur of anderen via de transporteur.

Artikel 13 van de huidige Grondwet verklaart dat het briefgeheim (lid 1) en het telegraaf- en telefoongeheim (lid 2) onschendbaar zijn. Beperkingen van het briefgeheim vereisen een voorafgaande last van de rechter. Ten aanzien van beperkingen van het telefoon- en telegraafgeheim kan worden volstaan met een voorafgaande machtiging door een bevoegd orgaan. Nu voor beide leden een ander beschermingsregime geldt, is het onderscheid tussen de geheimen derhalve uitermate relevant. Op het feit dat het grondwetsartikel hierdoor techniekafhankelijk is geformuleerd, werd ook al snel gewezen.²⁵

Problematisch werd de techniekafhankelijkheid pas echt met de opkomst van nieuwe communicatiemiddelen, zoals e-mail, chat, SMS, et cetera. Onduidelijk is of deze ook beschermd worden onder artikel 13 en, zo ja, onder welk lid.

Bij het huidige briefgeheim gaat het om een:

‘communicatie die plaatsvindt in gesloten enveloppen, althans in een verpakking welke het oogmerk tot uitdrukking brengt dat derden – waaronder de PTT – van de inhoud van de brief geen kennis nemen’.²⁶

Adressering is derhalve niet voldoende. In beginsel beschermen het telefoon- en telegraafgeheim alle communicatie via telefonie of telegrafie. Omdat soms om technische redenen kennis moet worden genomen van de communicatie, heeft het geheim ook de strekking dat informatie (de inhoud) niet verder verspreid

wordt. De verzender moet wel 'het nodige' gedaan hebben om de communicatie geheim te houden. Dat de communicatie geadresseerd is, is ook onder het huidige telefoon- en telegraafgeheim onvoldoende voor bescherming. Ten aanzien van beide geheimen geldt dat de communicatie slechts tijdens het transport beschermd is.

Voorzover het gaat om transmissie van elektromagnetische signalen komt mijns inziens slechts artikel 13 lid 2 Grondwet voor een extensieve interpretatie in aanmerking. Gezien de convergentie die plaatsvindt tussen inhoud en verkeersgegevens en de toegenomen privacygevoeligheid van verkeersgegevens, zou men tevens op grond van een extensieve interpretatie kunnen betogen dat verkeersgegevens onder het in artikel 13 beschermde rechtsgoed dienen te vallen. Dit zou betekenen dat op grond van het huidige artikel een voorafgaande machtiging noodzakelijk is voor het opleggen van een bewaarplicht. Hiermee zou een permanente bewaarplicht niet mogelijk zijn; slechts in incidentele gevallen zou de transporteur een bewaarplicht kunnen worden opgelegd. Daarbij geldt dat slechts die vormen van telecommunicatie zijn beschermd, waarbij de afzender het nodige heeft gedaan om de communicatie geheim te houden. Een aantal communicatiemiddelen zal derhalve buiten de boot vallen. Verkeersgegevens gekoppeld aan het gebruik van die communicatiemiddelen zal hetzelfde lot beschoren zijn.

Onder het huidige artikel is een dergelijke benadering echter überhaupt niet mogelijk. De Grondwetgever was namelijk in 1983 van mening dat verkeersgegevens reeds door artikel 10 beschermd zouden worden. Onder artikel 10 Grondwet worden echter alleen de verkeersgegevens beschermd voorzover zij aangemerkt kunnen worden als persoonsgegevens. Verkeersgegevens die geen betrekking hebben op natuurlijke personen, kunnen niet als zodanig worden aangemerkt. Er bestaat derhalve een zekere lacune in de rechtsbescherming, nog los van de vraag of nieuwe communicatiemiddelen ook onder artikel 13 beschermd kunnen worden.

Het huidige artikel 13 Grondwet stelt derhalve op dit moment in het geheel geen grenzen aan het in het leven roepen van een structurele bewaarplicht voor verkeersgegevens.

In de toekomst? | In 1997 diende de regering een voorstel in tot wijziging van artikel 13 Grondwet waarin de term vertrouwelijke communicatie werd gepresenteerd als techniekonafhankelijke norm.²⁷ Dit nieuwe begrip was afkomstig uit het gelijknamige proefschrift van Hofman. Beschermd worden besloten communicatievormen, zowel binnen als buiten de transportfase. Van beslotenheid in de zin van het grondrecht zou sprake zijn wanneer de verzender een geobjectiverde wil heeft dat slechts de geadresseerde kennisneemt van de inhoud van de communicatie. De geobjectiverde wil moet volgens dit voorstel blij-

ken uit een bepaalde mate van beveiliging. E-mail moest bijvoorbeeld versleuteld zijn, de brief moet in een dichtgeplakte envelop worden verstuurd.

Het voorstel werd bijzonder kritisch ontvangen. Die kritiek richtte zich met name op het criterium van beveiliging – onversleutelde e-mail en gewone faxen zouden namelijk niet beschermd zijn²⁸ – en het feit dat beeldinformatie en verkeersgegevens, dat wil zeggen gegevens die ten behoeve van het transport en de facturering door de transporteur worden verwerkt, van bescherming uitgesloten waren. Verkeersgegevens zouden reeds onder artikel 10 Grondwet vallen, en daarom niet onder artikel 13 Grondwet.

Het voorstel was geen lang leven beschoren. De Tweede Kamer amendeerde lustig, waarna de Eerste Kamer er geen brood meer in zag.

Vervolgens werd een commissie onder leiding van de Leidse hoogleraar Franken belast met de opdracht de problematiek rond grondrechten in het digitale tijdperk te onderzoeken en met nieuwe voorstellen te komen.²⁹ In mei 2000 publiceerde de Commissie-Franken haar rapport.³⁰ Ten aanzien van het nieuwe artikel 13 stelt zij wederom het begrip vertrouwelijke communicatie voor. Van vertrouwelijke communicatie is in de opvatting van de Commissie-Franken sprake wanneer een rechtssubject op grond van zijn wil tot geheimhouding een wijze van communiceren kiest, die hem een 'redelijke verwachting' van vertrouwelijkheid biedt. De vraag wanneer sprake is van een redelijke verwachting, dient te worden beantwoord met behulp van een functioneel vertrouwelijkheids criterium, te weten op basis van feiten en omstandigheden waaruit voor een ander objectief kan worden afgeleid dat de subjectieve wil van de verzender op vertrouwelijkheid is gericht. Dat is een hele mondvol, maar in de praktijk komt het erop neer dat de communicatie een bepaalde mate van beveiliging moet kennen.

Het kabinet publiceerde daarop een standpunt waarin zij de voorstellen van de Commissie grotendeels overnam.³¹ Het recht op vertrouwelijke communicatie geldt in de opvatting van het kabinet echter alleen in de transportfase, voorzover het gaat om communicatie die ter vervoer aan een derde wordt toevertrouwd. Ten aanzien van het live-gesprek geldt de bescherming slechts, voorzover dit met een technisch hulpmiddel wordt afgeluisterd.

Verkeersgegevens worden zowel in het voorstel van de Commissie-Franken als het daaropvolgende kabinetsstandpunt niet onder het grondrecht beschermd. Zij zijn van mening dat de algemene bescherming van artikel 10 Grondwet voor verkeersgegevens volstaat.³² Zowel het voorstel van de Commissie-Franken als het voorstel van het kabinet kon weer op hevige kritiek rekenen.³³ Tot op heden staat de besluitvorming over de wijziging van artikel 13 Grondwet stil. Wordt de hier geschetste lijn door het volgende kabinet voortgezet, dan biedt ook in de toekomst artikel 13 Grondwet geen waarborgen tegen een ongegeneerde vergaring

van verkeersgegevens door justitie en veiligheidsdiensten.

Toch is een discussie mijns inziens hierover van belang, mede gezien de positie van de Nederlandse Grondwet ten opzichte van de internationale rechtsorde. De Nederlandse regering heeft zich in het verleden op het standpunt gesteld dat de grondrechten in de Grondwet een zelfstandige positie ten opzichte van de internationale fundamenteelrechtelijke regeling dienen te hebben, doordat zij op enigerlei wijze de burger een grotere bescherming bieden. Voorzover het gaat om verkeersgegevens is dit echter momenteel niet het geval. Ook de plannen ten aanzien van een wijziging van artikel 13 Grondwet maken deze ambitie niet waar. Dit is verontrustend, omdat nu teruggevallen moet worden op artikel 8 EVRM. Dit artikel beoogt echter slechts minimumwaarborgen ten aanzien van de bescherming van de privacy en het communicatiegeheim te geven. Wordt het minimum de norm?

Conclusie | Een structurele bewaarplicht zoals die in internationaal verband, met name sinds de aanslagen op de Twin Towers, op de agenda staat, kan de toets aan de privacy en het communicatiegeheim van artikel 8 EVRM en de EU-richtlijnen met betrekking tot de bescherming van de persoonlijke levenssfeer en persoonsgegevens, niet doorstaan.

Deze fundamentele rechten verzetten zich tegen het in het leven roepen van een wettelijke plicht voor telecomaandieners de verkeersgegevens van iedere gebruiker standaard voor een periode van 1 tot 2 jaar op te slaan ten behoeve van strafvordering en nationale

veiligheid, terwijl dat niet nodig is in het kader van de dienstverlening. Een dergelijke plicht is een beperking van de privacy en het communicatiegeheim die op voorhand niet proportioneel lijkt. Onder omstandigheden is het denkbaar dat een beperkte bewaarplicht wel in overeenstemming met deze rechten zou zijn. Dan hebben we het over het bewaren van de verkeersgegevens van een beperkte groep personen ten aanzien waarvan het redelijke vermoeden bestaat dat deze een ernstig strafbaar feit beramen, voorbereiden of gepleegd hebben. Ook tegen een dergelijke maatregel moeten adequate waarborgen bestaan, zoals toezicht door een onafhankelijke rechter. Voorts moet de maatregel aan een beperkte termijn gekoppeld zijn, die eventueel verlengd kan worden wanneer dit noodzakelijk is.

Het is voorts opvallend dat de Nederlandse Grondwet ten aanzien van een ongebreidelde vergaring en verwerking van verkeersgegevens geen additionele waarde heeft in vergelijking met de internationale regelingen. Daarmee maakt Nederland de in het verleden uitgesproken ambitie ten aanzien van de grondrechten niet waar. Met betrekking tot de verwerking van verkeersgegevens door justitie en veiligheidsdiensten is het internationale minimum de norm. Gelukkig is zelfs op grond van dat minimum de stelling gerechtvaardigd dat het de staat niets aangaat wat ik vorige zomer deed, zolang er geen sprake is van een redelijke verdenking van een ernstig strafbaar feit.

De links bij dit artikel vindt u op <http://www.javisite.nl>.

Noten

- 1 A.H. Ekker, 'Bewaarplicht verkeersgegevens veroorzaakt digitale boterberg', *I&I* 2002-5, p. 2-3.
- 2 In augustus 2002 lekte een vragenlijst van de Deense EU-voorzitter uit waarin de lidstaten een voorstel werd voorgelegd een structurele bewaarplicht voor minimaal 1 jaar in het leven te roepen, werd voorgelegd. Zie <http://www.statewatch.org/news/2002/aug/05datafd1.htm>. Deze vragenlijst heeft geen juridisch bindende status, maar geeft wel aan dat een dergelijke bewaarplicht nog prominent op de agenda staat.
- 3 In de ontwerpfase van de nieuwe Richtlijn privacy en elektronische communicatie (zie hierna) heeft de Europese Raad van ministers van Justitie (JBZ-Raad) gesproken over een bewaartermijn op basis van een stuk dat de handhavingsbehoefte van een lidstaten benadrukt. 'At present the issue of storage is clearly the weak link in the fight against cybercrime. [...] All the representatives considered that access and on-line service providers should be obliged to store connection data for a minimum period.'; ENFOPOL 38, 8123/01, *Computer Crime - Summary of Replies to the Questionnaire*, 24 april 2001, beschikbaar op <http://www.statewatch.org/news/2001/may/ENFO38.pdf>; zie ook <http://www.statewatch.org/news/2001/may/03Genfopol.htm>. Dit minimum zou dan een jaar moeten zijn, in navolging van de huidige Belgische regeling. Het Verenigd Koninkrijk schijnt toen echter reeds een bewaartermijn van 7 jaar te hebben bepleit. Nederland wees een dergelijke ongeclausuleerde uitbreiding van de mogelijkheden verkeersgegevens te bewaren op dat moment nog af. (*Kamerstukken II* 2000/2001, 21 501-10, nr. 69, p. 4).
- 4 Zie met betrekking tot de bevoegdheden van de veiligheidsdiensten de artikelen 25 tot en met 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2001. Zie ook A.H. Ekker, 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2002-2, p. 77-83.
- 5 De bewaarplicht geldt voor bij AMvB aan te wijzen gegevens. De bedoelde AMvB is het Besluit bijzondere vergaring nummergegevens telecommunicatie van 18 december 2001, *Stb.* 2002, 31, in werking getreden op 1 maart 2002, *Stb.* 2002, 106. De bewaarplicht geldt alleen voorzover de telecomaandieners de gegevens uit zichzelf ver-

- werkt. Voorts gaat het alleen om gegevens die ontstaan wanneer de gebruiker een verbinding opbouwt, dus niet voor locatiegegevens die worden verwerkt als het mobiele toestel stand-by staat.
- 6 *Kamerstukken II 2001/2002, 27 925*, nr. 10, p. 11.
 - 7 Zie J.E.J. Prins, 'Wet bescherming persoonsgegevens. Agenda voor een discussie', in: M. Bauman (red.), *Privacy geregistreerd. Visies op de maatschappelijke betekenis van privacy*, Den Haag: Rathenau Instituut 1998, p. 213-281.
 - 8 Zie E.J. Dommering, 'De Grondwet in de informatiemaatschappij', in: M.C. Burkens e.a. (red.), *Gelet op de Grondwet*, Deventer: Kluwer 1998, p. 110-138.
 - 9 De nieuwe Telecomprivacyrichtlijn (Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEGL 201/37*) erkent dit. Artikel 6 van deze richtlijn is van toepassing op zowel verkeersgegevens als de inhoud van de communicatie.
 - 10 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PbEG 1995 L 281/31*.
 - 11 Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg 28 januari 1981, *Trb.* 1993, 11.
 - 12 Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PbEG 1998 L 24/1*.
 - 13 EHRM 6 september 1978, *AA 1979*, p. 327-334 (*Klass*).
 - 14 EHRM 2 augustus 1984, *NJ 1988*, 534 (*Malone*).
 - 15 EHRM 25 september 2001, n.n.g. (*P.G. & J.H. vs UK*). Raadpleegbaar via <<http://hudoc.echr.coe.int/hudoc/default.asp?Language=en&Advanced=1>>.
 - 16 Zie ook Aanbeveling 2/99 van de artikel 29-Werkgroep betreffende de bescherming van de persoonlijke levenssfeer in het kader van de interceptie van telecommunicatieverkeer. Beschikbaar op <http://www.europa.eu.int/comm/internal_market/en/data-prot/wpdocs/wp18nl.pdf>.
 - 17 EHRM 24 april 1990, *NJ 1991*, 553 (*Huvig & Kruslin*).
 - 18 Zie EHRM 7 juli 1989, *NJ 1991*, 659 m.nt. EJD (*Gaskin*). Dat een effectieve nationale rechtsgang openstaat tegen schendingen van de vrijheidsrechten van het EVRM volgt overigens reeds uit art. 13 EVRM. Zie daarover T. Barkhuysen, *Artikel 13 EVRM: effectieve nationale rechtsbescherming bij schending van mensenrechten*, Lelystad: Koninklijke Vermande, 1998.
 - 19 EHRM 25 februari 1987, *ECHR Series A 1987*, 116 (*Leander*).
 - 20 Zie ook G.N.M. Sciarone-Gorgels, 'Hoofdstuk 11 van de telecommunicatiewet. Rijp voor revisie?', *Privacy en Informatie 1999-5*, p. 196-204.
 - 21 Richtlijn 2002/22/EG van het Europees Parlement en de Raad van 7 maart 2002 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEGL 201/37*.
 - 22 Zie over deze richtlijn en spam het artikel van Gardeniers in dit nummer van JAVI op p. 82. Zie voorts A.R. Lodder en J.P.R. Bergfeld, 'De moeizame strijd tegen spam', *NJB 2002-22*, p. 1057; A.R. Lodder, 'Spam, cookies en 'data retention' in de sector elektronische communicatie: Nieuwe Richtlijn ter vervanging van Richtlijn 97/66/EC inzake privacy en telecom', *Computerrecht 2002-4*, p. 269-270.
 - 23 De geschiedenis van de opeenvolgende grondwetswijzigingen staat uitvoerig beschreven in J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, Zwolle: W.E.J. Tjeenk Willink 1995, p. 105-123; zie voorts P.W.C. Akkermans (red.), *De grondwet. Een artikelsgewijs commentaar*, Zwolle: W.E.J. Tjeenk Willink 1987 p. 273-280; A.J.A. van Dorst, 'Het postgeheim', in: A.K. Koekkoek, W. Konijnenbelt, F.C.L.M. Crijns (red.), *Grondrechten, commentaar op Hoofdstuk 1 van de Grondwet*, Nijmegen: Ars Aequi 1982, p. 279-298.
 - 24 J.T. Buijs, *De Grondwet. Toelichting en kritiek*, Deel II, Arnhem: Gouda Quint 1887, p. 414-417.
 - 25 Idem noot 12.
 - 26 *Kamerstukken II 1975/1976*, 13 872, nr. 2, p. 44-46.
 - 27 *Kamerstukken II 1996/1997*, 25 443, nrs. 1-3.
 - 28 Zie ook E.J. Dommering e.a., *Informatierecht. Fundamentele rechten voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2000, p. 77; E.J. Dommering, 'Geen telefoongeheim op de elektronische snelweg', *Mediaforum 1997-10*, p. 142-147; N.A.M.N. van Eijk, '(G)een recht op vertrouwelijke communicatie: fax en e-mail vogelvrij', *NJB 1997-33*, p. 1554-1555.
 - 29 *Stb.* 1999, 101.
 - 30 Rapport Commissie Grondrechten in het digitale tijdperk, Den Haag: Ministerie van Binnenlandse Zaken 2000.
 - 31 *Kamerstukken II 2000/2001*, 27 460, nr. 1.
 - 32 Zie Commissie-Franken, p. 159.
 - 33 Zie o.a. L.F. Asscher, 'Trojaans hobbelpaard. Een bespreking van het rapport van de commissie grondrechten in het digitale tijdperk', *Mediaforum 2000-7/8*, p. 228-233; E.J. Dommering, 'De nieuwe Nederlandse Constitutie en de informatietechnologie', *Computerrecht 2000-4*, p. 177-185; R.E. de Winter, 'Vernieuwde grondrechten', *NJB 2001-7*, p. 297-299; J.A. de Meij, 'Grondrechten in het digitale tijdperk. Van drukpersvrijheid en briefgeheim naar communicatievrijheid en communicatiegeheim', *NJCM-Bulletin 2001-3*, p. 274-294; F. Kuitenbrouwer, 'Hoe sterk zijn de digitale grondrechten?', *Computerrecht 2000-4*, p. 172-176; en recent L.F. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002.