



EEN GRONDRECHT OP VERTROUWELIJKE COMMUNICATIE

Kort geleden werd er een voorstel tot wijziging van artikel 13 van de Grondwet aan de Tweede Kamer aangeboden. Dat artikel zegt in zijn huidige versie dat het briefgeheim en het telegraaf- en telefoongeheim onschendbaar zijn. De grondwetgever vindt echter dat het recht niet aan de techniek moet worden gebonden, reden waarom er wordt voorgesteld er een recht op vertrouwelijke communicatie van te maken. De koppeling van de bescherming aan het begrip 'vertrouwelijk' levert echter een aanzienlijke beperking van de grondwettelijke bescherming op. Dit artikel analyseert de consequenties. Tevens wordt stilgestaan bij de effecten van de privatisering op de grondwettelijke bescherming van brief- en telefoongeheim. Maar eerst wordt de vraag gesteld om wat voor soort grondrecht het nu eigenlijk gaat.

1. De voorgestelde wijziging

Artikel 13 Gw zou volgens het ontwerp¹ moeten gaan luiden:

1. Het recht op vertrouwelijke communicatie is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die door de wet zijn aangewezen.
2. De wet stelt regels ter bescherming van vertrouwelijke communicatie.
3. Degene wiens recht op vertrouwelijke communicatie wordt beperkt, wordt van die beperking in kennis gesteld. Bij wet kunnen uitzonderingen worden gesteld op de eerste volzin, voor gevallen waarin het belang van de staat zulks dringend vordert.

De Memorie van Toelichting stelt dat de huidige tekst van artikel 13 niet meer correspondeert met de nieuwe ontwikkelingen van de communicatiemiddelen: "Dit geldt niet alleen voor post en telecommunicatie (e-mail, sealfax), voor verschillende typen van telecommunicatie onderling (telefoon, fax, datacommunicatie), maar ook voor directe communicatie (gesprekken van mond tot mond) enerzijds en telecommunicatie anderzijds. Men denke bij dit laatste bijvoorbeeld aan de mogelijkheid van videoconferencing en interactieve Videotex." De aandachtige lezer die deze zin voorzichtig savouereert, zal bij 'sealfax' nog wel op de gedachte komen dat het niet gaat om zeehondenfax, maar om een vorm van in de praktijk nauwelijks voorkomende (in Australië, en misschien ook wel in Antarctica, gesignaleerde) vorm van verzegelde ontvangst van faxen (bij ontvangst worden ze in een enveloppe opgeborgen) die het Ministerie van Binnenlandse Zaken heeft ontdekt om, zo zal hierna blijken, de fax buiten het briefgeheim te plaatsen. Maar met de merkwaardige manier waarmee met het begrip telecommunicatie wordt omgesprongen zal de lezer geen raad weten. Datacommunicatie is 'telecommunicatie onderling' en interactieve Videotex is 'telecommunicatie anderzijds'. Dat kan niet goed aflopen, denkt de lezer, bij herlezing van dit terminologische en taalkundige monstrem. De Memorie van Toelichting vervolgt dat het noodzakelijk is om een techniek-onafhankelijke benadering te kiezen. Daarom dat er voor wordt gekozen alle vertrouwelijke communicatie te beschermen. Er wordt aangeknoopt bij het proefschrift van J.A.Hofman, *Vertrouwelijke Communicatie*². Communicatie is vertrouwelijk wanneer er een

¹ TK 1996-1998, 25443, nrs. 1-2.

² Door ondergetekende besproken in *Mediaforum* 1996-2, 26-27; de noodlottige misverstanden die

'geobjectiveerde wil' van vertrouwelijkheid is. Het daarop volgende stuk van de Memorie van Toelichting is te fantastisch om het niet integraal te citeren³:

"Bij het verzenden van gegevensdragers in gesloten verpakkingen, het verzenden van beveiligde computerberichten over het datanetwerk en het verzenden van gesloten faxen (sealfax) is in objectieve termen sprake van een wil die gericht is op geheimhouding van de communicatie. Dit is tevens het geval wanneer men buiten gehoorafstand van derden een telefoongesprek voert via openbare telecommunicatienetten, in beginsel met inbegrip van alle niet kabelgebonden delen daarvan. Anderzijds zijn vormen van telecommunicatie waarbij beveiligingsvoorzieningen als versleuteling, het gebruik van compressietechnieken (sic!) of het pakketgewijs verzenden van digitale gegevens (sic!) ontbreken, evenals briefkaarten, gewone faxen en niet versleutelde computerberichten die via computernetwerken worden getransporteerd, communicatievormen die zonder of met een geringe inspanning voor derden toegankelijk zijn. Dit heeft tot gevolg dat bij gebruik van die communicatie-middelen niet op geheimhouding mag worden gerekend en bij een geobjectiveerde wilsconstructie men tot de conclusie moet komen dat de wil van de communicerenden niet op geheimhouding is gericht."

Het is verleidelijk om de wijze waarop ten departemente van de grondwetgever de telecommunicatietechniek door elkaar wordt gehaspeld aan een nadere analyse te onderwerpen (ik heb bijvoorbeeld met sicjes in het citaat aangegeven hoe verzendtechnieken zoals compressie en pakketschakeling worden verward met berichtbeveiliging). Maar laat ik mij tot de hoofdzaak beperken: voortaan is alleen zeehondenfax nog grondwettelijk beschermd. Het normale elektronische berichtenverkeer dat breed in zwang is gekomen (fax, e-mail), wordt met een gebaar buiten de grondwet geplaatst, terwijl er ook van het telefoongeheim niet veel overblijft, omdat de communicatie over de lijn niet is versleuteld (dat willen ze op het Ministerie van Justitie, waar de encryptietechnologie een voorwerp van zorg is, trouwens niet hebben). De passage over het telefoongesprek buiten gehoorafstand van derden is overigens van een grote bizarheid: wie een telefoongesprek voert met het telefoonapparaat op de speaker zodat anderen kunnen meeluisteren (in het zakelijk verkeer een veel voorkomend verschijnsel), verspeelt zijn telefoongeheim. Maar er is meer. Daartoe tracteer ik de lezer nogmaals op een fantastisch citaat:

"Onder het begrip communicatie dient in dit kader uitsluitend geschreven (tekst, tekens, protocollen, enz.) en auditieve (geluid) communicatie te worden verstaan. Beeldinformatie valt in beginsel niet onder het communicatiebegrip. Wel kan dit type informatie onder de bescherming van artikel 10 van de grondwet vallen. Hoewel uit beeldinformatie wel interactie tussen personen met een bepaalde inhoud of betekenis kan worden afgeleid, zijn beelden toch minder informatieverschaffend dan geschreven of gesproken communicatievormen. De bovenstaande hoofdregel lijdt slechts in de volgende gevallen uitzondering: indien beelden worden opgenomen en eventueel bewaard, met het oogmerk deze tot geschreven of auditieve communicatie te herleiden -bijvoorbeeld door middel van liplezen- dan wel wanneer reeds zonder dit oogmerk gemaakte beelden daadwerkelijk herleid worden tot vertrouwelijke communicatie. In beide gevallen is tevens sprake van een vertrouwelijke communicatie."

De fotootjes die met een brief worden meegestuurd vallen dus niet meer onder het briefgeheim, tenzij er familieleden met geheimzinnige grijnzen op staan waaruit familieleden aan de andere kant van de Oceaan door middel van liplezen geheime boodschappen weten te ontcijferen. Hoe zou een communicatiewetenschapper tegen deze passage aankijken? Droeg hij een hoed hij zou hem vertwijfeld opeten. En hoe zit het precies met het streven artikel 13 van de Gw het digitale tijdperk binnen te loodsen, het tijdperk immers waarin er alleen bits over de lijn gaan of worden opgeslagen, of het nu beeld, schrift of geluid is?

aan dit proefschrift ten grondslag liggen en die in dit ontwerp doorwerken heb ik daar bestreden.

³ TK 1996-1997, 254443, nr.3, 2.

Een grondwetsvoorstel dat wordt gepresenteerd als een versterking van het brief- en telefoongeheim en een aanpassing van deze rechten aan het digitale tijdperk blijkt in feite die rechten geheel uit te hollen. Tot beter begrip van wat hier allemaal is fout gegaan, ga ik eerst terug in de geschiedenis en sta ik stil bij het rechtskarakter van dit grondrecht. Daarna zal ik ingaan op de beperkingsclausules van het ontwerp en op de horizontale werking van het grondrecht waarover het ontwerp ook een aantal gedachten bevat.

2. Wat houdt het grondrecht in?

2.1. Bescherming van het communicatiekanaal

Artikel 13 van de huidige grondwet verklaart onomwonden dat het briefgeheim (lid 1) en het telegraaf- en telefoongeheim (lid 2) onschendbaar zijn. Het tweede lid dateert van de wijziging van 1983, daarvoor kenden wij alleen het briefgeheim dat vanaf 1848 (toen het in de Gw kwam) onveranderlijk luidde: "Het geheim der aan de post of andere openbare instelling van vervoer toevertrouwde brieven is onschendbaar, behalve op last de rechters, in de gevallen in de wet omschreven." Dat is een mooi artikel dat we nog aan Thorbecke te danken hebben, want in het Parlement was er niet veel animo voor de bescherming van het briefgeheim op constitutioneel niveau.⁴ Pogingen om het briefgeheim uit te breiden tot de telegraaf en de telefoon hadden geen succes. Pas in 1983 werden de telegraaf (waaronder de toen in opkomst zijnde telex werd begrepen) en de telefoon toegevoegd, en viel ook de beperking tot het "aan het vervoer toevertrouwde" weg, waardoor het geheim tegenover en binnen iedere overheidsinstelling kon worden ingeroepen. Daarbij werd het voorbeeld van de post voor gedetineerden en de gevangenisdirecteur gegeven.

Het brief- en telefoongeheim wordt doorgaans tot het privacyrecht gerekend. Dat is nog terug te vinden in de plaatsing van artikel 13 bij het huisrecht (artikel 12), en de regels omtrent privacy en persoonlijke integriteit (de artikelen 10 en 11). Het EVRM noemt in artikel 8 de bescherming van het privéleven, het huis en de privécorrespondentie in één adem. Artikel 17 van het BuPo heeft dezelfde structuur. Het is de vraag of dit wel juist is. Het brief- en telefoongeheim zijn communicatierechten, die de vrije en ongestoorde communicatie van gedachten en gevoelens met door de verzender van de boodschap zelf gekozen personen garanderen. Dat is voor de vrijheid van meningsuiting net zo wezenlijk als het in het openbaar ongestoord kunnen uiten van zijn gedachten. Wie de regering wil bestrijden wil in het geheim telefonisch kunnen overleggen met vertrouwelingen over de toespraak die hij ongecensureerd via de media wil uitspreken. Afluisteren tijdens verkiezingscampagnes is net zo bedreigend voor de democratie als het niet toelaten van de oppositie tot de televisie. Nu kan men zeggen dat dat bij het privégesprek zonder gebruikmaking van communicatiemiddelen ook het geval is, maar dat mist naar mijn mening toch het punt 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 communicatiekanaal: het brief- en postgeheim zijn in hun essentie klassieke onthoudingsrechten, die op de beheerders van netten en aanbieders van informatietransportdiensten

⁴ De geschiedenis van de opeenvolgende grondwetswijzigingen staat uitvoerig beschreven in het in de tekst geciteerde proefschrift van Hofman, 105-123; zie voorts P.W.C. Akkermans (red.), *De grondwet, een artikelgewijs commentaar* (Zwolle 1987, 1e druk), 273-280; A.J.A van Dorst, Het Postgeheim, in: A.K. Koekoek, W. Konijnenbelt, F.C.L.M. Crijns (red.), *Grondrechten, commentaar op Hoofdstuk ! van de Grondwet* (Nijmegen 1982), 279-298.

de plicht leggen zich te onthouden van een inmenging in de verzonden boodschap. Of zoals ze sinds jaar en dag bij de PTT zeggen: de boodschappers hebben geen boodschap aan de boodschap. Ook als men het brief- en telefoongeheim onder het privacyrecht brengt als 'een bijzonder aspect van de privacy'⁵, is het van groot belang het als een apart recht met daaraan gekoppelde onthoudingsplicht te behandelen. Het Ontwerp laat zien hoe gevaarlijk het is om dat niet te doen. Ik verwijs naar het geciteerde voorbeeld van het telefoongesprek dat binnen gehoorsafstand van derden wordt gevoerd. Het gaat bij het voeren van een telefoongesprek niet om het meeluisteren van personen aan de kant van degene die het gesprek voert of beluistert, maar om het niet mogen meeluisteren door degene die het gesprek transporteert (op dat meeluisteren aan het begin en het einde van de lijn kom ik nog terug onder 2.4.). Bij de concrete vormgeving rijzen een paar belangrijke vragen, samen te vatten in drie aspecten: de communicatietechniek, welke vorm van communicatie valt er onder (en zijn er in dat verband bijzonder beveiligingseisen te stellen?), en de reikwijdte van de gelding van het recht. Op deze drie aspecten ga ik thans in.

2.2. De communicatietechniek: brief, telegraaf, telefoon en hoe nu verder?

Wij hebben het tot 1983 met het briefgeheim moeten stellen. Sedert 1983 zijn het telegraaf- en telefoongeheim aan de catalogus van artikel 13 toegevoegd. Maar sindsdien zijn er nieuwe ontwikkelingen zoals het antwoordapparaat, de fax, voicemail en e-mail, die zich alle daardoor kenmerken dat de gesproken of geschreven boodschap wordt vastgelegd en door de geadresseerde op een door hem gekozen moment wordt 'opgehaald'. Valt dat nog onder een 'brief', een 'telegraaf' of een 'telefoon'? Het is het klassieke dilemma van de jurist die met een nieuw technisch fenomeen wordt geconfronteerd: gaan wij legistisch (naar de letter) of teleologisch (naar de geest) te werk? Het EHRM heeft er nooit een probleem van gemaakt om onder de 'correspondence' van artikel 8 EVRM ook het telefoongeheim te begrijpen.⁶ Ook in de Nederlandse doctrine treffen een vergelijkbare benadering aan.⁷ Het verst gaat daarin D.H.M. Meuwissen⁸: "De opsomming van de communicatiemiddelen in artikel 13 kan niet als limitatief, maar moet als enuntiatief worden uitgelegd. Het gaat er tenslotte om dat het beginsel dat aan artikel 13 ten grondslag ligt in een analoge (extensieve) interpretatie tot zijn recht komt." Ik kan daar geheel in meegaan, hetgeen betekent dat ook informatie die over telecommunicatienetten (telefoon, kabel, draadloos of niet) wordt vervoerd en bij ontvangst (en soms ook onderweg) eerst wordt opgeslagen of op een vaste informatiedrager wordt zichtbaar gemaakt (zoals bij de fax) onder artikel 13 valt. Daarbij heeft de Grondwetgever van 1983 het wel lastig gemaakt omdat het beperkingsregime van artikel 13 lid 2 Gw (telegraaf en telefoon) door een onduidelijke discussie in de Tweede Kamer (waarover hierna in par. 3) niet hetzelfde is als bij het briefgeheim. Als men het begrip 'brief' beperkt tot het transport van een vaste informatiedrager (papier, tape) over land, zee of door de lucht (zoals de meeste commentatoren kennelijk doen), ontstaan willekeurige verschillen waardoor de fax, die een elektronische transportfase kent onder het telefoongeheim valt (of beter nog onder het telegraafgeheim, omdat de fax met haar papieren output in de eindfase nog het meest op het telegram of de telex lijkt), maar de diskette die over de post wordt verzonden onder het briefgeheim. Dat is op zich een goed argument om naar een niet techniekgebonden bepaling te gaan, maar dan wel een andere dan door de regering voorgesteld.

⁵ C.A.J.M. Kortmann, *Constitutioneel Recht* (Deventer 1997, 3e druk), 412.

⁶ De zaak Klass, 6 september 1978, series A, vol. 28, AA 28 (1979), 327-334, met noot van E.A. Alkema.

⁷ Akkermans a.w. noot.. ,278, en daar aangehaalde literatuur.

⁸ D.H.M. Meuwissen *Grondrechten* (Utrecht/Antwerpen 1984), 178.

2.3. Welke communicatie; beveiligingseisen?

Het ontwerp acht de geobjectiveerde wil tot vertrouwelijkheid het beslissende criterium. Naar mijn mening is dit het verkeerde criterium, en kan men, aanknopend bij het door Bordewijk en Van Kaam ontwikkelde communicatieschema, beter als kenmerk nemen of de communicatie van de zender tot een of meer identificeerbare ontvangers is gericht, of, m.a.w. de informatie is *geadresseerd*.⁹ Dergelijke definities treft men ook in de literatuur aan als het gaat om de vraag om het begrip 'brief' nader te bepalen. Adressering is ook het kenmerk van het telefoongesprek, omdat de opbeller contact zoekt met het in cijfers gestelde adres van de opgebelde (die door opname in het telefoonboek van dat nummer zijn privacy in zoverre heeft prijsgegeven; caller identification is een manier om dat prijsgeven van privacy te corrigeren, en heeft dus niets te maken met de privacy van de beller zoals velen denken, *but I digress*). En dat geldt ook voor de conference call, omdat alle deelnemers vooraf zijn geadresseerd, maar niet voor de babbelbox waarbij iedere anonieme inbeller kan meebabbelen in het groepsgesprek. Ook de e-mail box en de fax kennen identificeerbare adres-santen, hetgeen weer niet het geval is met het elektronische bulletin-board, waar iedere zender voor iedereen toegankelijke berichten kan 'ophangen'.

Het privé karakter van de communicatie ligt dus in de adressering van de boodschap en niet in de inhoud van de communicatie; adressering impliceert dat de boodschap niet voor een ander adres (individu of instelling) is bestemd, en zeker niet voor degene die de boodschap transporteert.

⁹ Dit is wat J.L. Bordewijk en B. van Kaam, *Allocutie, enkele gedachten over communicatievrijheid in een bekabeld land* (Baarn 1982), 30 'conversatie' noemen, een dialoog tussen een of meer partijen die ten opzichte van elkaar in een gelijke positie verkeren, dit in tegenstelling tot de verkeerspatronen waarbij er informatie-uitwisseling tussen een openbaar informatiebestand en een individu plaats vindt, zonder dat het individu dat samenstelling van het bestand actief kan beïnvloeden.

Moeten er aan het geadresseerde bericht nadere beveiligingseisen worden gesteld, om in aanmerking te komen voor bescherming? Uit de geschiedenis van de Gw en de daarop gevolgde commentaren blijkt dat de 'geobjectiveerde wil van vertrouwelijkheid' niet uit de lucht is komen vallen. De verwarring tussen het privé karakter van de geadresseerde boodschap en *het risico* dat, ondanks adressering, derden van die boodschap kunnen kennisnemen, heeft zich al vroeg in het Nederlandse constitutionele denken genesteld. Dit komt mijns inziens, omdat men gefocust is gebleven op de brief en men niet voldoende is blijven onderscheiden tussen de bescherming van het communicatiekanaal en de communicatie zelf. In het regeringsvoorstel van 1976¹⁰ wordt het kunnen kennisnemen van de inhoud van het bericht tot een element van het grondrecht verheven. Het briefgeheim bestaat omdat de "communicatie plaatsvindt in een gesloten enveloppe, althans een verpakking die het oogmerk van de afzender tot uitdrukking brengt dat derden - waaronder de PTT - van de inhoud van de brief geen kennis kunnen nemen". Dat zou bij het open aangeboden telegram, waarbij de postbeambte altijd van de inhoud kennis moet nemen, anders zijn. Bij de telefoon zou dat probleem zich niet meer voordoen, want, "gezien de automatisering van het telefoonverkeer waardoor gewoonlijk geen tussenkomst van derden meer nodig is, benadert het telefoongeheim wat het geheimhoudingsaspect betreft het briefgeheim." De Grondwetgever van 1983 gaat op dit spoor verder door te verklaren dat de draadloze telefoon buiten het telefoongeheim valt, omdat iedereen in het ontvanggebied van de zender zou kunnen meeluisteren. In 1997 antwoordt de Minister van Justitie op een kamervraag over e-mail dat deze buiten de grondwettelijke bescherming zou vallen omdat deze, net als een Ansichtkaart, door derden gemakkelijk kan worden gelezen.¹¹ En het ontwerp gooit het ontbreken van een technische beveiliging en het kunnen kennisnemen door derden op een grote hoop door alle berichten die tijdens het transport niet technisch beveiligd zijn, of waarvan derden voor of na het transport kunnen kennisnemen buiten de bescherming van het grondrecht te plaatsen.

In deze gedachtengang worden norm en feit door elkaar gehaald. Wie een geadresseerd bericht verzendt beoogt een boodschap te verzenden die alleen voor de adressant is bestemd. Bij de uitvoering van dat voornemen kan de verzender meer of minder voorzorgsmaatregelen nemen. Wie geld verstuurt zal dat waarschijnlijk aangetekend doen of bijzondere eisen stellen aan de doorzichtigheid van de enveloppe. Een fax die niet door een ander mag worden gelezen zal vooraf telefonisch worden aangekondigd, zodat de geadresseerde bij het ontvangapparaat staat op het moment dat deze binnenkomt. Soms kiezen de gebruikers van een kwetsbaar kanaal geheimtaal om de risico's te beperken (zoals bijvoorbeeld bij de mobiele telefoon). Een brief die naar een grote organisatie wordt verstuurd, maar aldaar door een persoon moet worden gelezen, bevat op de enveloppe het opschrift 'persoonlijk en vertrouwelijk'. Wie persoonlijk wil telefoneren doet de deur van zijn kamer dicht en kiest een tijdstip van telefoneren waarop hij verwacht dat de geadresseerde alleen op zijn kamer is. Maar het achterwege laten van voorzorgsmaatregelen betekent niet dat de norm dat de boodschap niet voor anderen is bestemd, niet geldt! En dat is zeker niet zo in de transportfase. Het toevoegen van een beveiligingseis koppelt de bescherming van het grondrecht bovendien aan de stand van de techniek: de afschaffing van de telefoniste maakt het mogelijk het telefoongeheim in te voeren, en de ontwikkeling van de encryptietechnologie leidt daarentegen weer tot afschaffing. Dat is dus precies het tegengestelde van hetgeen het ontwerp beoogde te bereiken.

De beperking van het brief- en telefoongeheim, zodat e-mail er buiten valt heeft bovendien gevaarlijke neveneffecten op de discussie over de vraag of de access provider tot het Internet aansprakelijk kan worden gesteld voor de inhoud van de informatie die via zijn dienstverlening toegankelijk is voor derden. Als het geoorloofd is om van de inhoud van de e-mail boxen die onder zijn beheer staan kennis te nemen, is het nog maar een stap om te zeggen dat hij ook voor de inhoud

¹⁰ Wetsontwerp 11051, besproken en geciteerd bij Van Dorst, a.w. noot 4, 282-283.

¹¹ Aanhangsel TK, 1995/1996, 1370, waarover L.F. Asscher, in: *Mediaforum* 1997-7/8, 103.

daarvan verantwoordelijk kan worden gesteld.¹² De inperking van de gelding van het brief- en telefoongeheim valt niet samen met de vraag of het geoorloofd is van de inhoud van verstuurde berichten kennis te nemen, waartegen bepalingen van het Wetboek van strafrecht waken (138a, 139a-139f, 201, 441 Sr). Toch kunnen ook hier ongewenste neveneffecten optreden als het gaat om de vraag of overtreding van deze strafbare feiten ook daadwerkelijk tot strafbare gedragingen leiden. Ik signaleer deze neveneffecten zonder ze hier verder in detail te analyseren.

Wanneer is er sprake van een inbreuk op geadresseerde informatie? Men zou hier in navolging van het Duitse recht de laagdrempelige eis van het nemen van een hindernis, waaronder reeds valt het openen van een niet dichtgeplakte enveloppe valt, kunnen hanteren.¹³ Zelfs het lezen van een ansichtkaart is al het nemen van een hindernis omdat het de postbeambte dwingt de routine van het sorteren of bestellen te doorbreken.

2.4. Wat omvat het brief, etc. geheim?

Een lastige vraag is waar het briefgeheim, etc., precies begint en ophoudt en hoever het zich uitstrekt tijdens het transport. In Nederland is die vraag nog iets ingewikkelder geworden, omdat bij de laatste wijziging van de Gw het brief- en telefoongeheim geheel losgekoppeld is van het transport: brief- en telefoongeheim zijn, kortweg, 'onschendbaar'. Bij dat laatste gaat het dan vooral om de onschendbaarheid van de brief, omdat alles wat zich als brief aandient alleen met een rechterlijke last kan worden geopend. Sommigen zien daarin een onpraktische beperking.¹⁴

Ik zou voor de analyse van dat vraagstuk willen terugkeren naar de gedachte dat het een communicatierecht is, zo men wil een bijzonder aspect van de privacy, dat het waard is afzonderlijk te regelen. Dat betekent dat wij ons concentreren op de bescherming van het communicatiekanaal voor de verzending van geadresseerde boodschappen. De vraag valt uiteen in twee delen: waar begint en eindigt het communicatiekanaal en welke handelingen moeten wij tijdens verzending, transport, en ontvangst nog aan het transportgeheim (zoals ik het vooruitlopend op paragraaf 5 maar vast noem) toerekenen?¹⁵

De eerste vraag raakt met name de opslag van de boodschap, al of niet in elektronische vorm, aan verzend- en ontvangstzijde. Naar mijn mening valt de opslagfase van de verzendgerede of ontvangen boodschap onder het brief- of telefoongeheim. In België en Duitsland wordt eveneens verdedigd om de (elektronische) postbus onder het transportgeheim te brengen.¹⁶ Moet daarop de beperking worden gesteld dat de werking van het grondrecht ophoudt op het moment dat de ontvangen boodschap is gelezen? Voor de werking van het transportgeheim, dunkt mij wel, en dat zou betekenen dat de mailserver die de postbusfaciliteit aanbiedt, de verplichting heeft al de opgehaalde berichten uit zijn computer te verwijderen. Ik ben mij ervan bewust dat er tal van grensvragen overblijven. Een moeilijk grensgevallen, die ik hier noem, vormt de bezorgde maar nog niet geopende brief. Het hangt dunkt mij af van de functionele, organisatorische relaties binnen het

¹² Zie daarover o.a. E.J. Dommering, *Internet, een juridische plaatsbepaling van een nieuw communicatieproces*, in: *Computerrecht* 1996/6, 210-221.

¹³ Hofman a.w. noot 2, 370.

¹⁴ Zie over dit probleem met name Van Dorst, a.w. noot 4, 296.

¹⁵ Ik leg het accent dus op datgene wat Van Dorst, a.w. noot 4, 289, zonder duidelijke argumentatie 'het postgeheim in ruime zin' noemt.

¹⁶ Zie L.F. Asscher, a.w. noot 5 en Jos Dumortier, Rebecca Vanhecke en Stephanie Missotten, *Laat de Belgische wetgeving gerechtelijk aftappen van privécommunicatie via GSM of Internet toe?*, in: *Computerrecht* 1997/4, 145-149.

besteladres of de brief dan geacht moet worden de eindbestemming te hebben bereikt. Bij kantoren, waar brieven centraal worden geopend is dat doorgaans het geval op het moment dat de brief is afgeleverd aan het kantooradres.¹⁷ Maar bij brieven aan gedetineerden is dat bepaald niet zo. En binnen gezinsrelaties? Sommigen behandelen dit probleem als een kwestie van het al of niet toekennen van horizontale werking aan het recht, aangezien het laatste stukje van het communicatiekanaal (de niet geopende brief op het gangtafeltje thuis) in de privésfeer ligt.¹⁸ Erg overtuigend is dat argument niet. Als de ouder een voor de dochter bestemd telefoongesprek aanneemt, wordt dat gesprek toch ook doorverbonden? Op het moment dat het grondrecht in de nieuwe geprivatiseerde verhoudingen van de post- en telecommunicatie moet werken, valt deze redengeving al helemaal weg. Men zal toch begin en eindpunt van het communicatiekanaal moeten vaststellen.

Tijdens transport en opslag worden er privacygevoelige gegevens gegenereerd die worden vastgelegd. Bij het telecommunicatiebedrijf dat het transport verzorgt zijn dat de verkeersgegevens met betrekking tot de abonnee, bij het bedrijf dat de postbusfaciliteit aanbiedt zijn dat inloggegevens. De Memorie van Toelichting van het Ontwerp, p. 3, stelt dat deze buiten het begrip vertrouwelijke communicatie vallen. Over deze vraag heeft een interessante discussie tussen de Raad van State en de regering plaats gehad, omdat de Raad onder verwijzing naar de zaak Malone¹⁹ er op had gewezen dat deze gegevens wel degelijk onder het telefoongeheim kunnen worden begrepen.²⁰ In antwoord op die kritiek stelt de Memorie van Toelichting echter dat ze onder omstandigheden als persoonsgegevens kunnen worden aangemerkt die binnen de sfeer van artikel 10 Gw vallen. Dat maakt de bescherming tot een wassen neus, omdat zij als geïsoleerde persoonsgegevens dikwijls geen deel uit zullen maken van een persoonsregistratie en de daarvoor geldende beschermingsregels. 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 opgebeldde 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 *Auskunftsverbot* (als pendant van het *Eindringeverbot*), het verbod feiten mee te delen over de omstandigheden van verzending.²¹ Hetgeen betekent dat ze alleen binnen de beperkingen van het transportgeheim aan derden kunnen worden verstrekt. Artikel 125f Sv gaat ten onrechte van een andere gedachte uit.

Alles wat buiten de sfeer valt van de verzending en wat daaraan is toe te rekenen, blijft de bescherming van het algemene privacyrecht genieten. Dat zijn dus het lezen van geopende brieven die voor een ander zijn bestemd, afluisteren van het telefoongesprek binnen gehoorsafstand, het tapen van gesprekken, teletelers, richtmicrofoons enz. (strafbaar gesteld in artikel 139a, 139b Sr en 139f, en civielrechtelijk aan te pakken via een onrechtmatige daadsactie en het portretrecht).

3. Beperkingen

Bij de laatste Grondwetswijziging is er het nodige te doen geweest over de formulering van de beperkingen. Het briefgeheim stelde als eis dat de beperking moet steunen op een wet en slechts bij rechterlijke last kon plaatsvinden. De regering vond in verband met de verrichtingen van de BVD die laatste eis een hinderlijke beperking en wilde deze in het aanvankelijke ontwerp schrappen. Er

¹⁷ Vgl. Van Dorst a.w. noot 4, naar aanleiding van het begrip 'misbruik' in 139c lid 2 Sr.

¹⁸ C.A.J.M. Kortmann, *De Grondwetsherzieningen 1983 en 1987*, (Deventer 1997), 103.

¹⁹ EHRM 2 augustus 1984 (Series A, nr. 82).

²⁰ TK 1996-1997, 25443 B, 2.

²¹ Hofman, a.w. noot 4, 371.

was nota bene het communistische (hetgeen bij nader doordenken niet zo merkwaardig is) kamerlid Bakker voor nodig om daar bezwaar tegen te maken. In de woeling van het parlementaire debat bleef vervolgens de oude regel van het briefgeheim gehandhaafd, maar verviel de beperking van de rechterlijke last voor het telegraaf- en telefoongeheim. Daarmee werd op constitutioneel niveau een ongewenst onderscheid in beschermingsniveau geïntroduceerd. De regering probeert nu andermaal het vereiste van de rechterlijke last uit het artikel te krijgen, wederom met hetzelfde argument. Inmiddels is het niet alleen de BVD, maar zijn het 'de inlichtingen- en bewakingsdiensten'.²² Ditmaal was het de Raad van State die daarover viel, onder verwijzing naar de beslissing van het EHRM in de zaak Klass.²³ De regering antwoordt daarop in de bewuste passage met het argument dat uit de uitspraak in die zaak zou volgen dat de eis van rechterlijke machtiging niet zou gelden. Het Hof drukt zich in die zaak echter aanmerkelijk voorzichtiger uit, ik citeer de bewuste rechtsoverweging 56: "The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge". Vervolgens onderzoekt het Hof in detail de 'checks and balances' die zijn neergelegd in de parlementaire controle, de notificatieplicht en de mogelijkheid van rechterlijke controle achteraf. De uitkomst van dat onderzoek is dat het Duitse systeem van controle op de Veiligheidsdienst (waar het in casu om ging) door de beugel kon. Op grond van deze uitspraak, die trouwens door Van Dijk en Van Hoof is bestreden,²⁴ is mijns inziens alleen te verdedigen dat in uitzonderingsgevallen verbandhoudende met de nationale veiligheidsdienst met een politieke controle kan worden volstaan, mits die voldoende 'checks and balances' bevat, en, achteraf een rechterlijke controle mogelijk is. De hoofdregel van het eerste lid zou dus hoogstens een uitzonderingsbepaling voor de nationale veiligheidsdienst kunnen zijn. Bovendien moeten die wettelijke procedures aan vrij zware kwaliteitseisen voldoen, zoals de Huvig en Kruslinzaken leren.²⁵ Regering en Raad van State verschilden ook van mening over de beperking van de notificatieplicht in het derde lid. Het vastleggen van een notificatieplicht is op zichzelf een grondwettelijk novum dat kan worden toegejuicht, maar de beperking daarvan 'in het belang van de staat' is veel te ruim. Een meer uitgewerkte beperkingsclausule toegesneden op artikel 8 lid 2 EVRM, zoals de Raad van State verlangde, is gewenst.

Zoals men kan overwegen een uitzonderingsbepaling voor de veiligheidsdienst op te nemen, die voldoet aan de eisen van proportionaliteit en rechterlijke controle (achteraf), zo verdient het ook overweging om voor het omgaan met 'verkeersgegevens' een apart regime te ontwerpen, omdat de rechterlijke last vooraf uiteraard niet kan werken. Dat is nu bijvoorbeeld gebeurd in artikel 139c 3e Sr. De opdracht aan de wetgever zal ook hier waarborgen voor proportionaliteit en rechterlijke controle moeten bevatten. Zo lijkt, naar analogie van persoonsregistratie (voorzover verzamelingen verkeersgegevens daar al niet rechtstreeks onder zouden vallen) een doelbinding noodzakelijk en ligt ook een beperking in de tijd met daaraan de plicht de gegevens te vernietigen voor de hand.

4. Horizontale werking

De Memorie van Toelichting geeft als toelichting op het tweede lid dat de privatisering van de post- en telecommunicatie er toe noopt dat de Grondwet "een opdracht aan de wetgever bevat er in te voorzien dat ook in horizontale verhoudingen het recht op vertrouwelijke communicatie wordt

²² TK 1996-1997, 25443, 3, 4.

²³ Zie noot..

²⁴ P. van Dijk en G.J.H. van Hoof, *De Europese Conventie in theorie en praktijk*, (Nijmegen 1990, derde druk), 658-660.

²⁵ EHRM 24 april 1990, Series A 176, NJ 1991, 532, m.nt. EJD.

gegarandeerd". De grondwetgever snijdt dit probleem terecht aan. De nieuwe Telecommunicatiewet liberaliseert de data- en telefoondiensten, maar bekommert zich nauwelijks om het telefoongeheim. Bij e-mail bestaan in het geheel geen garanties. De dienstverleners komen ook niet voort uit een traditie waarin het telefoongeheim iets heiligs is.

De gelding van het grondrecht is tot aan de privatisering nooit problematisch geweest omdat het grondrecht rechtstreeks tegen de PTT als staatsbedrijf kon worden ingeroepen. De ambtenaren, werkzaam bij de PTT, hadden ook een strafrechtelijk gesanctioneerde plicht het brief- en telefoongeheim te respecteren (372-374 bis Sr). Door de privatisering werkt deze constructie niet meer.²⁶

In de literatuur bestaat geen eenstemmigheid of het post- en telefoongeheim als grondrecht horizontale werking toekomt, dat wil zeggen: gelding heeft in verhoudingen tussen particulieren en particuliere instellingen.²⁷ Bij het algemene privacyrecht is dat door de HR expliciet erkend in de zaak van de Edamse Bijstandsmoeder, al is niet helemaal duidelijk of de HR het grondrecht ook *direct* toepasselijk heeft geacht.²⁸ De onzekerheid *hoe* grondrechten in private verhoudingen doorwerken (direct of indirect via privaatrechtelijke beginselen) is trouwens in de Nederlandse literatuur een punt van discussie gebleven, zoals Alkema in zijn overzicht van 1995 heeft laten zien.²⁹

Het is merkwaardig dat de Memorie van Toelichting in het geheel niet rept over de vraag of het grondrecht direct of indirect werking heeft in private verhoudingen, temeer daar de keuze voor het begrip 'vertrouwelijke communicatie' toch bij uitstek een horizontaal karakter aan het recht verleent. Hoe dit ook zij, het is duidelijk dat er veel voor te zeggen is die werking in wettelijke bepalingen nader gestalte te geven. De grondwetgever zou daarvoor preciezer indicaties moeten geven dan een blanco volmacht aan de wetgever. Het nagenoeg gelijktijdig ingediende wetsontwerp Telecommunicatiewet doet bijvoorbeeld niets met het onderwerp. Juist bij de algehele liberalisatie van het verkeer over telecommunicatienetten, openbaar of niet, was er dringend behoefte geweest aan een algemene 'geen boodschap aan de boodschap' bepaling, en had een aanpassing overwogen moeten worden van de desbetreffende bepalingen in het Wetboek van Strafrecht.

Conclusie

De Grondwetgever heeft een belangrijk onderwerp aangepakt, maar naar mijn mening op de verkeerde manier. Het gaat om afdoende garanties in te bouwen ter waarborging van het communicatiegeheim in een tijdperk dat de post- en telecommunicatie-infrastructuur en daarover aangeboden diensten geprivatiseerd zijn, en de digitale informatietechnologie bezig is zich diep in te graven in de samenleving.

De uitwerking van het begrip 'vertrouwelijke communicatie' bergt het niet denkbeeldige risico in zich dat een belangrijk nieuw medium als Internet dat, naar verwachting, na de eerste anarchistische fase, juist op het gebied van individuele transacties en communicaties zijn verdere expansie zal vinden, geen 'telegraaf- en telefoongeheim' meer zal kennen. Is het naïviteit of opzet van de overheid? Is dit

²⁶ Van der Pot-Donner, *Handboek van het Nederlandse Staatsrecht* (Zwolle 1995, 13e druk), 306.

²⁷ C.A.J.M. Kortmann *De Grondwetwijzigingen 1983 en 1987* (Deventer 1987), 103; positiever Van Dorst, a.w. noot 4, 290-297.

²⁸ HR 8 januari 1987 *NJ* 1987, 928, m.nt. EAA, *Computerrecht 1987/.....*, m.nt.E.J. Dommering; zie voor een analyse van deze jurisprudentie L.F.M. Verhey *Horizontale werking van grondrechten, in het bijzonder het recht op privacy* (Zwolle, 1992), 290-297.

²⁹ E.A.A. Alkema, De reikwijdte van fundamentele rechten, in: *Handelingen Nederlandse Juristenvereniging 1995-I* (Zwolle 1995), 22-32.

een nieuwe poging van de overheid een communicatiemedium dat zich aan de staatsmacht onttrekt, onder controle te krijgen?

De bepaling bereikt ook niet de beoogde technische neutraliteit. Door een beschermingsniveau als aanknopingspunt te nemen verschiet zij telkens van kleur, al naar gelang de stand van de techniek, en roept zij nieuwe onzekerheden op. Als een e-mail boodschap straks met een druk op de knop ook voor de gemiddelde gebruiker kan worden geencrypteerd, valt zij dan wel onder het communicatiegeheim? Het getuigt ook niet van veel begrip voor de digitale techniek door beeld in beginsel niet tot het communicatiegeheim te rekenen.

Ook op het gebied van het stelsel van beperkingen is het ontwerp een stap terug. Het ontwerp lijkt thans de volledige winst te willen nemen die door de interventie van de Tweede Kamer in 1983 maar gedeeltelijk (namelijk alleen op het gebied van het telegraaf- en telefoongeheim) kon worden geïncasseerd.

Op het gebied van de horizontale werking verschaft het geen behoorlijke waarborgen.

Waarom moest dit Ontwerp in haast aan de Tweede Kamer worden gepresenteerd, zonder een gedegen discussie (met participatie uit wetenschappelijke kring) over onderwerpen als de effecten van de, mede door de enorme ontwikkeling van de informatietechnologie gevoede, privatisering en de internationalisering van de rechtsorde op de vormgeving van de grondrechten? En hoe zat het ook weer met de openbare discussie over de juridische aspecten van de elektronische snelweg?

Moeten er weer in allerlei amendementen in elkaar worden geflanst om erger te voorkomen? In 1983 is dat ook niet goed afgelopen. Daarvoor is de Grondwet toch een te kostbaar bezit? Of deelt ook deze in de algehele verwording van de wet: ooit een uitdrukking van de geschreven rede, thans een instrument van belangenbehartiging en tijdsgebonden verdeel- en heerspolitiek?