

## **Dodo of feniks: het communicatiegeheim in het digitale tijdperk?**

Wilfred Steenbruggen

*Hoe moet het grondrecht op brief-, telefoon- en telegraafgeheim er in het digitale tijdperk uitzien? Hierover wordt al sinds 1997 gediscussieerd. Tot op heden zonder resultaat: men kan het maar niet eens worden over de inhoud en reikwijdte van het nieuwe artikel 13 Grondwet. Twee benaderingen van het grondrecht staan daarbij schijnbaar lijnrecht tegenover elkaar. Zijn beide benaderingen echter wel zo onverzoenlijk? Is er geen concept denkbaar waarin beide benaderingen samenkomen? Dit artikel beoogt deze vragen te beantwoorden.*

### **I Inleiding**

Sinds 1997 wordt in Nederland een discussie gevoerd over hoe aan een grondwettelijk recht op communicatiegeheim in de informatiemaatschappij gestalte moet worden gegeven. De directe aanleiding voor deze discussie vormde een uitspraak van de toenmalige Minister van Justitie dat het briefgeheim, zoals neergelegd in artikel 13 van de Nederlandse Grondwet, geen bescherming aan e-mail biedt.<sup>1</sup> Daarmee werd pijnlijk duidelijk dat artikel 13 Grondwet waarin het brief-, telefoon- en telegraafgeheim zijn neergelegd, niet informatiemaatschappij-proof is.

Verschillende wijzigingsvoorstellen zijn sindsdien gedaan. Verschillende daarvan voorzien in een recht op vertrouwelijke communicatie.<sup>2</sup> Dit recht is echter omstreden. Voorstellen met betrekking tot het recht vertrouwelijk te communiceren, konden op hevige kritiek rekenen, zowel ten aanzien van het object van het recht, de conceptuele uitwerking ervan als de beperkingsmogelijkheden. De discussie wordt getekend door een fundamenteel verschil van mening over wat het object van het communicatiegeheim dient te zijn. Grofweg staan daarbij twee benaderingen van het geheim lijnrecht tegenover elkaar.

De eerste benadering is de 'vertrouwelijke communicatie'-benadering die terug te voeren is op Hofmans proefschrift uit 1995.<sup>3</sup> Voorstanders van deze benadering zijn de Commissie Franken en het kabinet Kok-II. De andere benadering is de 'transport'-benadering die wordt verdedigd door onder meer Dommering<sup>4</sup> en Asscher in zijn recent verschenen proefschrift<sup>5</sup>.

In dit artikel ga ik in op de vraag of beide benaderingen wel zo onverzoenlijk zijn. Dienen in het toekomstige communicatiegeheim niet beide benaderingen samen te komen, om de burger een maximale bescherming te bieden, niet alleen tegenover de overheid, maar ook - steeds meer - tegenover medeburgers?

Ik zal hieronder eerst kort uiteenzetten wat de twee verschillende benaderingen inhouden. Vervolgens ga ik in op de grondslagen van het communicatiegeheim waarbij ik ook zal bekijken hoe deze in beide benaderingen terugkeren. Vervolgens wordt onderzocht of het communicatieproces bij post en telecommunicatie aanknopingspunten voor het communicatiegeheim in het digitale tijdperk biedt. Tenslotte zal ik proberen, om rekening houdende met de grondslagen van het communicatiegeheim, op grond van de gevonden aanknopingspunten een concept voor een communicatiegeheim uiteen te zetten dat beide benaderingen integreert.

### **II Twee benaderingen van het communicatiegeheim**

---

\* Wilfred Steenbruggen is werkzaam als onderzoeker aan het Instituut voor Informatierecht te Amsterdam.

<sup>1</sup> *Aanhangsel Handelingen II* 1997/1998, nr. 1370. Zie ook L.F. Asscher, 'E-mail een ansichtkaart?', *Mediaforum* 1997-7/8, p. 103.

<sup>2</sup> *Kamerstukken II* 1997/1998, 25 443, nrs. 1-2; Commissie Grondrechten in het digitale tijdperk, *Rapport*, Den Haag 2000; *Kamerstukken II* 2000/2001, 27 460, nr. 1.

<sup>3</sup> 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.

<sup>4</sup> Zie bijvoorbeeld E.J. Dommering, *Handboek Telecommunicatierecht. Inleiding tot het recht en de techniek van de telecommunicatie*, Den Haag: Sdu Uitgevers 1999, p. 601 e.v.

<sup>5</sup> 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.

## **Het recht op vertrouwelijke communicatie**

In 1997 diende de regering een wetsvoorstel tot wijziging van artikel 13 Grondwet in waarin de term vertrouwelijke communicatie werd gepresenteerd als de techniekonafhankelijke norm.<sup>6</sup> 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 geobjectiveerde wil heeft dat slechts de geadresseerde kennis neemt van de inhoud van de communicatie. De geobjectiveerde wil moet volgens dit voorstel blijken 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 en was geen lang leven beschoren.<sup>7</sup> Een commissie onder leiding van de Leidse hoogleraar Franken werd vervolgens belast met de opdracht de problematiek rond grondrechten in het digitale tijdperk te onderzoeken en met nieuwe voorstellen te komen.<sup>8</sup> In het rapport van de Commissie Franken keert het concept 'vertrouwelijke communicatie' terug. 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.

In het voorstel van de Commissie Franken wordt niet alleen communicatie die aan een ander ter vervoer wordt toevertrouwd, beschermd, maar ook het gewone gesprek. De bescherming geldt zowel binnen als buiten de transportfase.

Het kabinet publiceerde daarop een standpunt waarin zij de voorstellen van de Commissie grotendeels overnam.<sup>9</sup> 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.

Zowel het voorstel van de Commissie Franken als het voorstel van het kabinet konden weer op hevige kritiek rekenen.<sup>10</sup>

## **Het transportgeheim**

Recht tegenover het recht op vertrouwelijke communicatie staat de benadering van het geheim als transportgeheim. In deze visie verdient communicatie die aan een vervoerder is toevertrouwd, bescherming, omdat juist het aan een ander toevertrouwen een extra kwetsbaarheid voor de communicerende partijen in het leven roept. Dommering c.s. zijn van mening dat niet de inhoud van de communicatie beschermd dient te worden, maar het *communicatiekanaal*. Voor bescherming komt geadresseerde communicatie in aanmerking, beveiliging van de boodschap tegen de nieuwsgierige blikken van derden wordt niet geëist. Omdat deze benadering het kanaal tot uitgangspunt neemt, worden, naast de inhoud, ook de verkeersgegevens beschermd.

De bescherming duurt voort, zolang de communicatie in de handen van een transporteur is. Uit deze focus op het kanaal volgt dat het gewone gesprek buiten het communicatiegeheim valt. Het

<sup>6</sup> *Kamerstukken II* 1996/1997, 25 443, nrs. 1-3.

<sup>7</sup> Zie ook Dommering e.a. 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.

<sup>8</sup> *Stb.* 1999, 101.

<sup>9</sup> *Kamerstukken II* 2000/2001, 27 460, nr. 1.

<sup>10</sup> 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.

gesprek wordt immers niet aan een transporteur toevertrouwd.<sup>11</sup> Het algemene privacyrecht van art. 10 Grondwet heeft hier een aanvullende functie.

Onder het huidige communicatiegeheim wordt *besloten* communicatie tijdens *transport* beschermd. Zowel voorstanders van het concept 'vertrouwelijke communicatie' als die van het 'transport'-concept kiezen hieruit een criterium bij uitsluiting van het andere en leggen dat aan hun concept ten grondslag. Ter discussie staat derhalve eigenlijk welk van deze twee criteria in de toekomst doorslaggevend moet zijn voor bescherming. Om dat te bepalen moeten we mijns inziens nagaan wat de ratio voor een grondrecht op communicatiegeheim is.

### III Wat zijn de grondslagen van het communicatiegeheim?

Van oudsher beschermt het briefgeheim brieven die aan de Staat in zijn hoedanigheid van transporteur worden toevertrouwd. Zoals in het oude artikel 154 Grondwet 1848 tot uitdrukking komt, gaat het daarbij om de bescherming van 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. De achterliggende ratio is dat de burgers er recht op hebben te communiceren met een ontvanger naar keuze, zonder dat iemand anders, waaronder faciliterende derden, hiervan kennis neemt of de communicatie anderszins verstoort. Waar artikel 7 Grondwet de vrijheid gedachten en gevoelens openbaar (*point-to-multipoint*) te uiten beschermt, beschermt artikel 13 van oudsher de vrijheid gedachten en gevoelens in besloten kring (*point-to-point*) te uiten. Artikel 13 en 7 Grondwet zijn derhalve in dit opzicht traditioneel complementair. In dat opzicht is interessant dat Van der Velden de brief omschrijft als een geschreven gesprek en uitroept hoezeer de briefwisseling een maatschappelijke invloed heeft verworven.<sup>12</sup>

Meestal wordt het communicatiegeheim tot de privacyrechten gerekend. Dat is ook de mening van de grondwetgever in 1983 geweest die het communicatiegeheim in de nabijheid van artikel 10, 11 en 12 Grondwet plaatste. De regering was van mening dat het communicatiegeheim, in het bijzonder op de persoonlijke levenssfeer betrekking heeft.<sup>13</sup> Dat het communicatiegeheim een deelaspect van de privacy beschermt, is naar huidig recht dan ook geen onderwerp van discussie.

Het grondrecht heeft echter ook een speciale band met de communicatievrijheid, zoals Asscher en Dommering terecht opmerken.<sup>14</sup> Van oudsher vormen post, en recenter telecommunicatie, een belangrijk middel tot de uitingsvrijheid. Niet alleen privé-communicatie, maar ook openbare communicatie kan via post en telecommunicatie bij het beoogde ontvangerspubliek worden bezorgd.<sup>15</sup>

Het communicatiegeheim lijkt derhalve een hybride karakter te hebben, in die zin dat het zowel aspecten van de communicatievrijheid als de privacy beschermt. De vraag die daarbij opkomt, is hoe het geheim zich tot deze beide andere grondrechten verhoudt. Om vast te stellen wat het object van het communicatiegeheim is, zullen we eerst moeten vaststellen hoe het grondrecht zich tot de beide andere grondrechten verhoudt.

#### **Communicatievrijheid**

Met betrekking tot de vrijheid van meningsuiting worden globaal twee soorten rechtvaardigingen onderscheiden.<sup>16</sup> Enerzijds dient de uitingsvrijheid de mogelijkheden van het individu zichzelf te

<sup>11</sup> Zie bijvoorbeeld Asscher 2002, p. 24.

<sup>12</sup> Aldus P.A. van der Velden, *Het geheim der brieven. Aan de geschiedenis en aan de beginselen van het Staats-en Strafrecht getoetst*, (diss. Utrecht), 's-Gravenhage 1859 in zijn voorrede; zie ook C. Baart de la Faille, *Strafbare schending van geheimen*, Groningen: Huber 1884, p. 41-45; Duynstee 1891, p. 1-22; Hofman 1995, p. 106-108.

<sup>13</sup> *Kamerstukken II 1975/1976*, 13872, nr. 3, p. 39.

<sup>14</sup> L.F. Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, ITeR 26, Deventer: Kluwer 1999, p. 57; Dommering e.a. 2000, p. 47.

<sup>15</sup> Zie bijvoorbeeld R. Herzog, 'Art. 5 Abs. I, II', in: T. Maunz, G. Dürig & R. Herzog, *Grundgesetz. Kommentar*, München: C.H. Beck Verlag (losbladige uitgave), Rd. 79-80.

<sup>16</sup> Vgl. J.A. Peters, *Het primaat van de vrijheid van meningsuiting : vergelijkende aspecten Nederland-Amerika*, Nijmegen: Ars Aequi Libri 1981, p. 13; A.J. Nieuwenhuis, *Over de grens van de uitingsvrijheid. Een*

ontplooiën. De vrijheid te communiceren wordt in dit perspectief gezien als een noodzakelijke voorwaarde voor individuele autonomie. De idee van individuele autonomie veronderstelt een keuzevrijheid voor het individu die nauw verbonden is met een vrije privé-sfeer waarin het individu kan doen en laten wat hij wil.<sup>17</sup>

Een andere grondslag voor een recht op vrijheid van meningsuiting wordt gevormd door het publieke belang dat gediend is bij het ongehinderd plaatsvinden van de discussie. Deze benadering gaat er in wezen van uit dat bij een vrije uitwisseling van meningen de waarheid vanzelf boven komt.<sup>18</sup> Later krijgt deze grondslag een meer politieke component. De vrije uitwisseling van meningen werd opgevat als een kenmerk van en een voorwaarde voor de democratische samenleving. Ook daarbij is de belangrijkste aanname weer dat het vrije debat de beste manier is de waarheid, of, beter, de minst slechte oplossing te vinden. Democratie geeft iedereen het recht om aan het debat deel te nemen. Voor de democratie is het essentieel dat ideeën en opinies getoetst kunnen worden aan andere denkbeelden.

Van de tweede grondslag bestaan overigens verschillende varianten die met elkaar gemeen hebben dat ze gericht zijn op een min of meer algemeen belang, in tegenstelling tot het individuele belang van de eerste grondslag.<sup>19</sup>

Het algemene en het individuele belang komen samen in het model van de *free market place of ideas*. Dit model wordt gekenmerkt door het zelfbeschikkingsrecht van het individu over zijn uitingen waarna de uitingen op een vrije markt verspreid worden.

Ten aanzien van het communicatiegeheim kunnen vergelijkbare rechtvaardigingsgronden worden onderscheiden. Ook het communicatiegeheim beschermt mogelijkheden tot individuele zelfexpressie en ontplooiing en vormt daarmee een voorwaarde voor persoonlijke autonomie. Van autonomie kan immers geen sprake zijn, wanneer een individu niet onafhankelijk kan bepalen wat wel en niet geopenbaard wordt. Hofman noemt daarom vertrouwelijk kunnen communiceren zelfs een basisbehoefte van de mens.<sup>20</sup>

Bovendien dient ook het communicatiegeheim het openbaar debat. Het recht ongestoord te corresponderen maakt het mogelijk in vrijheid een mening te vormen en in een beperkte kring te toetsen, alvorens aan het publieke debat deel te nemen. Het communicatiegeheim dient dus in beginsel dezelfde belangen, individueel en publiek, als de uitingsvrijheid. Hieruit lijkt ook voort te vloeien dat bescherming van het recht ongestoord met een beperkt aantal anderen te kunnen communiceren, een onontbeerlijke voorwaarde is voor het functioneren van het model van de *free marketplace of ideas*.

Zoals Asscher terecht stelt, bestaat er geen echte vrijheid om de *free marketplace of ideas* te betreden, zolang het communicatiekanaal niet beschermd wordt.<sup>21</sup> Wordt de integriteit van het kanaal bedreigd, dan zal dat een *chilling effect* op het openbaar debat hebben. In dat licht bezien is een inbreuk op het geheim een vorm van censuur. Herzog kent deze overeenkomst zelfs zoveel betekenis toe dat hij uit het censuurverbod van art. 5 van het Duitse *Grundgesetz* een afluisterverbod afleidt.<sup>22</sup>

## **Privacy**

Moet vanuit de communicatievrijheid bescherming van het communicatiegeheim worden gezien als pendant van het censuurverbod, het recht op privacy komt tot uiting in het belang van iedere burger beschermd te worden tegen ongewenste kennisname van privé-communicatie.<sup>23</sup> Vooropgesteld zij dat er geen objectief juiste omschrijving van begrip en inhoud van het recht op

---

*rechtsvergelijkende analyse van de regelgeving ten aanzien van pornografie en racistische uitlatingen*, Nijmegen: Ars Aequi Libri 1997, p. 36-37.

<sup>17</sup> Nieuwenhuis 1997, p. 14.

<sup>18</sup> A.J. Nieuwenhuis, *Persvrijheid en Persbeleid*, Amsterdam: Otto Cramwinckel 1991, p. 19-20.

<sup>19</sup> Zie voor een meer gedetailleerde bespreking van de verschillende grondslagen van de uitingsvrijheid De Meij e.a. 2000; Nieuwenhuis 1997.

<sup>20</sup> Hofman 1995, p.1-2.

<sup>21</sup> Asscher 2002, p. 18.

<sup>22</sup> R. Herzog, 'Art. 5 Abs. I, II', in: T. Maunz, G. Dürig & R. Herzog, *Grundgesetz. Kommentar*, München: C.H. Beck Verlag (losbladige uitgave), Rd. 79-80.

<sup>23</sup> A.J. Nieuwenhuis, *Tussen privacy en persoonlijkheidsrecht. Een grondrechtelijk en rechtsvergelijkend onderzoek*, Nijmegen: Ars Aequi Libri 2001, p. 196.

privacy te geven is.<sup>24</sup> Sommigen benadrukken dat privacy een voorwaarde is om in de openbare democratische besluitvorming en gedachtewisseling te participeren.<sup>25</sup> Privacy is in deze visie niet slechts het tegengestelde van openbaarheid, maar ook een voorwaarde voor het behoorlijk functioneren daarvan. Asscher wijst op de overeenkomst tussen deze benadering en de grondslagen van de uitingsvrijheid om zijn benadering van het communicatiegeheim als aspect van de communicatievrijheid te verenigen met de heersende mening dat het communicatiegeheim een privacyrecht is.<sup>26</sup>

Hoewel privacy en communicatievrijheid zeker voor een deel in elkaars verlengde liggen, wordt privacy over het algemeen gezien als een recht waarmee het individu zijn of haar privé-leven afschermt van anderen, inclusief de overheid. Het is dan een recht van het individu tot ongehinderde zelfontplooiing, een recht zelf te beschikken over de gegevens die over het individu in omloop zijn en een recht tot uiting van gedachten en gevoelens zonder tussenkomst van de overheid of anderen.

Gezien bovenstaande valt dus zowel een benadering van het communicatiegeheim vanuit de privacy als vanuit de communicatievrijheid te verdedigen. Leidt het gekozen perspectief automatisch tot een van de boven beschreven concepten van het grondrecht onder uitsluiting van het andere?

#### **IV Hoe verhouden zich deze grondslagen tot de twee onderscheiden benaderingen?**

##### ***De transportbenadering***

Dommering plaatst het communicatiegeheim binnen het privacyrecht in een schema van drie kringen.<sup>27</sup> Daarbij onderscheidt hij de relationele privacy, de informationele privacy en het communicatiegeheim als transportgeheim. De relationele privacy ziet zijns inziens op een niet aan tijd of plaats, maar aan de persoon gebonden fysieke privé-sfeer. Deze privé-sfeer strekt zich uit tot iedere maatschappelijke situatie waarin een individu zich kan bevinden. Deze vorm van privacy beschermt de meest uiteenlopende gedragingen en wordt ook wel omschreven als 'the right to be let alone', aldus Dommering.<sup>28</sup>

De informationele privacy en het communicatiegeheim bieden daarentegen juist bescherming buiten de fysieke privé-sfeer. De informationele privacy geeft het individu een beschikkingsrecht over gegevens die tot zijn persoon herleidbaar zijn, zogenaamde persoonsgegevens. Dit deel van het privacyrecht ziet op de rechten van het individu om de opslag van deze informatie te verhinderen, te beperken of te veranderen en ziet ook op de verplichtingen en beperkingen die gelden voor de personen en instellingen die deze informatie opslaan.

Het communicatiegeheim beschermt volgens Dommering daarentegen communicatieve handelingen die buiten de fysieke privé-sfeer plaatsvinden. Daarbij gaat het dus om communicaties van een individu die ter vervoer aan de zorg van derden worden toevertrouwd. De integriteit van communicatiemiddelen dient gewaarborgd te worden, zodat burgers op deze middelen kunnen vertrouwen.<sup>29</sup> Ook Dommering wijst er echter op dat het geheim als pendant van het verbod op censuur kan worden beschouwd: *Zoals de staat niet vooraf de inhoud van de*

<sup>24</sup> Hoewel daartoe wel pogingen worden ondernomen. Zie bijvoorbeeld voor een recent overzicht van de theorievorming rond het recht op privacy Nieuwenhuis 2001 en P.H. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische uitgevers 2002.

<sup>25</sup> Ruiz, p. 32-36.

<sup>26</sup> Dommering e.a. 1999, p. 601.

<sup>27</sup> Dommering e.a. 2000, p. 49-51.

<sup>28</sup> Dommering e.a. 1999, p. 601-607. De omschrijving van het recht op privacy als 'the right to be let alone' is afkomstig uit het beroemde artikel van Warren en Brandeis in de *Harvard Law Review*. (S. Warren & L.D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 1891/5, p. 193-220.) Aan het eind van de 19<sup>e</sup> eeuw schrijven zij in een vlammend betoog dat het afgelopen moet zijn met het gegluur en bespioneren van de Amerikaanse roddelpers. Met name de komst van de fotojournalistiek, waarmee kan worden binnengedrongen in de 'sacred precincts of private and domestic life' baart hen zorgen. Zij pleiten voor een juridische erkenning van een recht op privacy dat het individu in bescherming neemt tegen de opdringerige roddelbladen. Strikt genomen is gelijkstelling van relationele privacy met *the right to be let alone* niet helemaal juist. Volgens Warren en Brandeis is het recht op privacy namelijk onderdeel van een uitgebreider recht met rust te worden gelaten.

<sup>29</sup> Dommering e.a. 1999, p. 604.

*te openbaren gedachten mag beoordelen, zo mag hij ook niet kennisnemen van gedachten die niet of nog niet voor openbaarmaking zijn bestemd.*<sup>30</sup>

Dommering beschouwt het communicatiegeheim als een transportgeheim. Dit hangt samen met het feit dat hij de bescherming van de relationele privacy beperkt tot een fysieke privé-sfeer. Zijn systematische benadering van de privacy komt terug in het door hem voorgestane object van het communicatiegeheim. Het transport wordt beschermd.

Asscher volgt Dommering in zijn keuze van het object van het grondrecht in de informatiemaatschappij. Asscher benadert het geheim echter niet vanuit de privacy, maar vanuit de communicatievrijheid. Op deze wijze rechtvaardigt hij een afzonderlijk grondrecht op communicatiegeheim als aspect van de niet-openbare communicatievrijheid. In de Nederlandse context wordt niet-openbare communicatie immers niet door artikel 7 Grondwet beschermd. Bezien vanuit de communicatievrijheid bestaat hier een grondwettelijke lacune, die door een grondrecht dat zich op niet-openbare communicatie richt, opgevuld dient te worden.<sup>31</sup> Minder duidelijk is echter waarom hij het object van dit grondrecht tot bescherming van het transport beperkt. Deze beperking is niet zo vanzelfsprekend als Asscher lijkt aan te nemen. Dat voor de burger een extra kwetsbaarheid bestaat, wanneer hij zijn privé-communicatie aan een derde ter vervoer toevertrouwd, is duidelijk. De enkele vaststelling dat die extra kwetsbaarheid bestaat, is echter niet voldoende om communicatie buiten de transportfase uit te sluiten. De kwetsbaarheid van niet-openbare communicatie buiten de transportfase is met de opkomst van nieuwe geavanceerde technologieën zoals richtmicrofoons en TEMPEST<sup>32</sup> aanzienlijk toegenomen. Nu Asscher pleit voor de vertaling van de aan de grondrechten historisch ten grondslag liggende beginselen naar een hedendaagse context, had het voor de hand gelegen ook communicatie waarbij geen gebruik wordt gemaakt van een transportmiddel, onder het communicatiegeheim te scharen, juist vanwege die toegenomen kwetsbaarheid.

Ter rechtvaardiging van de uitsluiting van communicatie buiten de transportfase zou Asscher mijns inziens beter de nadruk hebben kunnen leggen op de verschuiving van beschikkingsmacht. Bij getransporteerde berichten staat iemand de beschikkingsmacht over het bericht af. Bij communicatie buiten de transportfase houdt iemand zelf de beschikkingsmacht over de communicatie en kan derhalve zelf maatregelen nemen om de vertrouwelijkheid van de uiting te beschermen. Dan is er geen tussenpersoon die de verantwoordelijkheid voor de bescherming (mede) overneemt. In deze visie is de ratio van het communicatiegeheim het beschermen van het vertrouwen in communicatiekanalen waaraan berichten worden toevertrouwd.<sup>33</sup>

Uit bovenstaande blijkt dat voorstanders van de transportbenadering het communicatiegeheim zowel vanuit de privacy als de communicatievrijheid benaderen. Welk van deze belangen doorslaggevend is, lijkt daarbij meer een uitdrukking van een persoonlijke voorkeur dan het resultaat van een beargumenteerde en principiële keuze.

### ***De vertrouwelijke communicatie-benadering***

Hofman en in zijn voetsporen Kaspersen, Hofman & Verbeek<sup>34</sup> maken anders dan Dommering geen onderscheid in verschillende privacyaspecten of -sferen. Hierdoor strekt het object van het door hen voorgestane recht op vertrouwelijke communicatie zich ook uit tot het gehele communicatieproces. Voor bescherming is dan niet doorslaggevend of gebruik wordt resp. is gemaakt van een communicatiemiddel, -dienst of -netwerk. Privé-communicatie wordt voor, tijdens en na het transport beschermd, voorzover er maar sprake is van privé-communicatie. Hierdoor wordt ook het mondelinge gesprek onder het communicatiegeheim gebracht. De vraag is dan wat de grenzen zijn van het communicatiegeheim. Waar houdt het communicatiegeheim

<sup>30</sup> Dommering e.a. 1999, p. 603.

<sup>31</sup> Zie ook Nieuwenhuis 2001, p. 160-162.

<sup>32</sup> TEMPEST is een techniek waarmee aan de hand van de door een computerbeeldscherm afgegeven residustraling communicatie kan worden onderschept. Zie over TEMPEST bijvoorbeeld J.P.G.M. Verbeek, T.A. de Roos & H.J. van den Herik, *Interceptie van vertrouwelijke communicatie. De institutionele kansen en bedreigingen van het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel*, IteR 35, Den Haag: Sdu Uitgevers 2000, p. 28-33.

<sup>33</sup> Vgl. ook E.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, p. 56.

<sup>34</sup> R. Kaspersen, J.A. Hofman & J. Verbeek, 'Vertrouwelijkheid van e-mail', in: IteR, nr. 13, Deventer: Kluwer 1999 en Hofman 1995.

op en begint het recht op privacy? Hofman stelt dat sprake is van vertrouwelijke communicatie, wanneer de verzender van een geobjectiveerde wil tot vertrouwelijkheid. Omdat de wil in beginsel subjektintern is, en dus niet voor derden kenbaar, moet de verzender aan derden kenbaar maken dat hij beoogt vertrouwelijk te communiceren. Dat kan hij doen door gebruik te maken van een beveiligde communicatiedienst (of –netwerk) of door zelf beveiligingsmaatregelen te nemen.

Hoewel Hofman daarmee weliswaar een criterium geeft om te bepalen of het communicatiegeheim van toepassing is, laat hij in het midden hoe het grondrecht zich tot andere grondwettelijke rechten, met name communicatievrijheid en privacy, verhoudt. Dat is echter wel problematisch, gezien de zeer ruime definitie van communicatie die aan het recht ten grondslag ligt. Communicatie is namelijk volgens Hofman elke uitwisseling van berichten. Dit omvat volgens hem ook de uitwisseling van berichten tussen niet-menselijke entiteiten.<sup>35</sup> De vraag komt hierbij op in hoeverre daarbij nog van privacybelangen sprake is. Dat niet-menselijke entiteiten ook een recht op privacy zouden hebben, lijkt mij op zijn minst omstreden. Mijns inziens kan de vertrouwelijke communicatie-benadering dan ook niet geheel vanuit het perspectief van de privacy gerechtvaardigd worden.

De hierboven geschetste benaderingen van het communicatiegeheim hebben gemeen dat zij het grondrecht op een eenzijdige wijze benaderen, nl. vanuit ofwel het perspectief van de privacy of het perspectief van de communicatievrijheid. Een dergelijke eenzijdige benadering schiet mijns inziens tekort, enerzijds omdat het gekozen perspectief enigszins arbitrair lijkt en anderzijds omdat deze eenzijdigheid het zicht op de betekenis van het grondrecht voor zowel de privacy als de communicatievrijheid vertroebelt.

## **V De verhouding van het communicatiegeheim tot privacy en communicatievrijheid**

Hoe verhoudt het communicatiegeheim zich tot de communicatievrijheid en de privacy? Nieuwenhuis probeert op deze vraag een antwoord te geven. Deze verhouding bestaat zijns inziens in de volgende ideaaltypische constructie.

*De vrijheid van meningsuiting ziet op een vrijheid van handelen: de overheid maakt inbreuk, indien zij het verbreiden van informatie met een bepaalde inhoud tegengaat. Het communicatiegeheim is een recht zich te verzetten tegen onderzoek en gesnuffel.*

Doorslaggevend in deze benadering is wat de aard van de overheidsbemoedening is. Gaat het om een verbod op het verspreiden van bepaalde informatie, dan is de vrijheid van meningsuiting in het geding. Snuffelt de overheid aan of onderzoekt zij bepaalde informatie, dan staat het communicatiegeheim, als deelaspect van de privacy, voorop.<sup>36</sup>

Tegen deze benadering kan worden ingebracht dat een belangrijke premisse daarvan in de huidige Nederlandse situatie niet houdbaar is. Zoals Nieuwenhuis zelf al aangeeft, wordt namelijk verondersteld dat de uitingsvrijheid zich mede uitstrekt tot niet-openbare communicatie, hetgeen in het huidige Nederlandse recht niet het geval is.<sup>37</sup> Dit zou echter bij een toekomstige Grondwetwijziging wel opgelost kunnen worden. Belangrijker lijkt mij dat deze ideaaltypische constructie niet terug te vinden is in de jurisprudentie van het EHRM over art. 10 EVRM dat zich mede uitstrekt over niet-openbare communicatie. Het Hof heeft weliswaar het verhinderen van correspondentie onder art. 8 beoordeeld, maar gaf tegelijkertijd aan ook art. 10 van toepassing te achten.<sup>38</sup>

Hoewel Nieuwenhuis' benadering haar merites heeft en ons in staat stelt een onderscheid te maken tussen situaties waarin de privacy en die waarin de communicatievrijheid in het geding is, zou ik hier toch voor een andere oplossing willen pleiten.

Mijns inziens vormt het communicatiegeheim namelijk, naast een deelaspect van de privacy, tegelijkertijd een onderdeel van de ruimere communicatievrijheid. Het communicatiegeheim ziet in het bijzonder op de vrijheid in beslotenheid te communiceren. In de Nederlandse context vormt

---

<sup>35</sup> Hofman 1995, p. 2.

<sup>36</sup> Nieuwenhuis 2001, p. 196.

<sup>37</sup> Idem.

<sup>38</sup> Zie bijvoorbeeld EHRM 25 november 1997, *NJB* 1998, 314 (*Georgiades*).

het grondrecht de codificatie van de niet-openbare communicatievrijheid. De transportmiddelen post en telecommunicatie vormen daarbij essentiële middelen tot deze vrijheid.

Waarom zou niet-openbare communicatie expliciete bescherming verdienen? De vrijheid om in beslotenheid met anderen te communiceren is een voorwaarde voor individuele autonomie. Niet-openbare communicatie, d.w.z. de uitwisseling van denkbeelden of andere informatie met een beperkt aantal anderen, is bepalend voor de totstandkoming van de persoonlijkheid en het maatschappelijk functioneren van het individu. De persoonlijkheid van het individu wordt bepaald door allerlei factoren uit zijn omgeving: de taal, maatschappelijke conventies, rollenstructuren, etc. Deze factoren stellen het individu enerzijds in staat om maatschappelijk te functioneren, anderzijds leggen ze hem zekere grenzen op. Grenzen die het individu, al dan niet bewust, in acht neemt bij zijn handelen. De persoonlijkheid van het individu, voorzover niet reeds genetisch bepaald, wordt derhalve bij uitstek vormgegeven door de interactie met zijn directe omgeving. Autonomie, d.w.z. het individu is vrij om keuzes te maken en te handelen volgens zijn opvattingen over het goede leven, is binnen deze grenzen slechts mogelijk, voorzover het individu zelf kan bepalen of, wanneer en hoe de interactie met de ander plaatsvindt. Mijns inziens ziet de vrijheid van niet-openbare communicatie, waarvan het huidige communicatiegeheim slechts een aspect vormt, bij uitstek op deze (relatieve) autonomie.

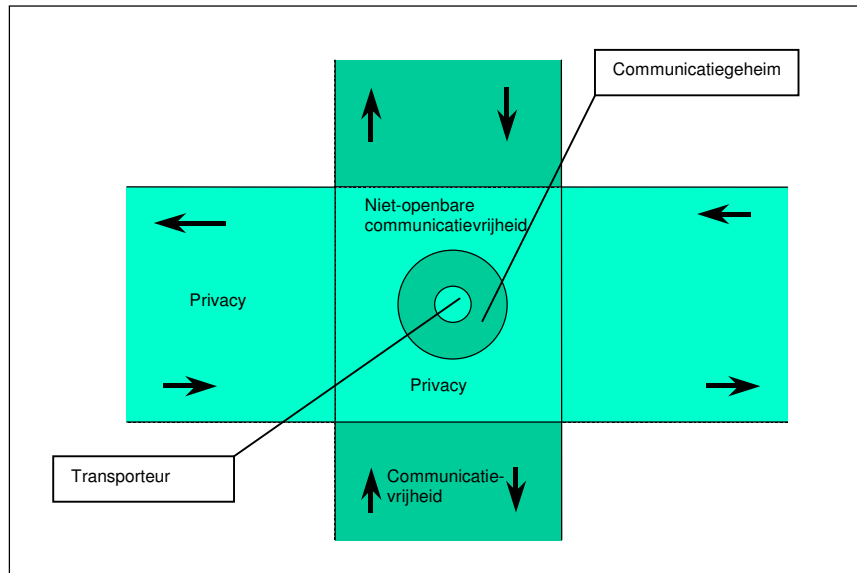
In deze grotere nadruk op de autonomie van de communicerende partijen ligt mijns inziens ook een onderscheid met traditionele noties van de openbare communicatievrijheid. De openbare communicatievrijheid of uitingsvrijheid is in de kern het recht om in vrijheid actief deel te nemen aan het maatschappelijke debat. Dit recht beoogt derhalve burgers in staat te stellen zich te uiten in de publieke sfeer. Het recht op uitingsvrijheid wordt dan ook meestal gerechtvaardigd vanuit het publieke belang. Gewezen kan daarbij worden op het belang van de democratie en waarheidsvinding die samenkomen in de 'free market place of ideas'-benadering. De autonomie van het individu is hierbij ook van belang, maar vormt in dit kader veeleer een middel het ideaal van een werkelijk vrije publieke uitwisseling van meningen en ideeën te bereiken.

In Nederland komt dit treffend tot uitdrukking in het feit dat art. 7 Grondwet is opgebouwd rond het verbod op censuur. Art. 7 verbiedt in beginsel elke voorafgaande toetsing van de inhoud, zij het dat dit verbod onderscheid maakt tussen verschillende communicatiemiddelen. Dit garandeert dat het individu vrij is denkbeelden en andere informatie te openbaren, derhalve in de publieke sfeer te brengen.

Hoewel een zekere overlap niet valt te ontkennen is communicatievrijheid binnen de private sfeer mijns inziens iets wezenlijks anders dan communicatievrijheid in de publieke sfeer. Hiervan vormt art. 13 Grondwet in het Nederlandse constitutionele stelsel een erkenning. Naar huidig recht blijft deze erkenning echter beperkt tot het transport van niet-openbare communicatie.

Dit laat onverlet dat het communicatiegeheim daarnaast en gelijktijdig tevens een onderdeel vormt van het recht op privacy. Het communicatiegeheim heeft daarin echter een bijzonder positie juist vanwege de betekenis van een vrije communicatie voor de persoonlijke autonomie van het individu.

Het grondrecht op communicatiegeheim vormt het kruisvlak van de privacy en de communicatievrijheid. Onderstaand figuur brengt dit voor het geldende recht tot uitdrukking.



De niet-openbare communicatievrijheid bevindt zich op het kruispunt van communicatievrijheid en privacy. Dat betekent dat ook het grondwettelijk communicatiegeheim als onderdeel van de niet-openbare communicatievrijheid zich op dit kruispunt bevindt. Naar huidig recht beschermt art. 13 Gw slechts het niet-openbare transport van communicatie. Bovenstaand figuur brengt dit tot uitdrukking. De transporteur bevindt zich midden op dit kruispunt. Hij heeft immers de beschikking over de aan hem toevertrouwde informatie, zolang het transport voortduurt. Afzender, noch de beoogde ontvanger(s) hebben zicht op hetgeen tijdens het transport plaatsvindt. Dit betekent dat de transporteur een sleutelpositie in het communicatieproces heeft die hem in staat stelt om enerzijds het vrije verloop van het communicatieproces te beïnvloeden, anderzijds kan hij zichzelf of derden toegang verlenen tot de aan hem toevertrouwde informatie en daarmee verbonden gegevens waardoor de privacy van afzender en ontvanger(s) in gevaar komt.

Het gebruik van telecommunicatiediensten is op allerlei maatschappelijke gebieden snel toegenomen. De ubiquiteit van de telecommunicatie leidt ertoe dat allerlei informatiestromen bij de transporteur samenkomen. De transporteur wordt derhalve steeds meer de spin in het web. In dat licht bezien, is het wenselijk dat deze sleutelpositie ten behoeve van zowel de privacy als de communicatievrijheid van de burger met adequate waarborgen is omkleed. Hierin dient het communicatiegeheim te voorzien.

Dat het transport met bijzondere waarborgen dient te zijn omgeven, lijkt duidelijk. Betekent dit echter ook dat de reikwijdte van het communicatiegeheim tot de transportfase beperkt dient te blijven? Mijns inziens niet. Ook communicatie buiten de transportfase is tegenwoordig kwetsbaar. Wanneer we aannemen dat privacy en communicatievrijheid in het communicatiegeheim samenkomen, bestaat principieel geen reden om communicatie buiten de transportfase niet onder dit grondrecht te beschermen.

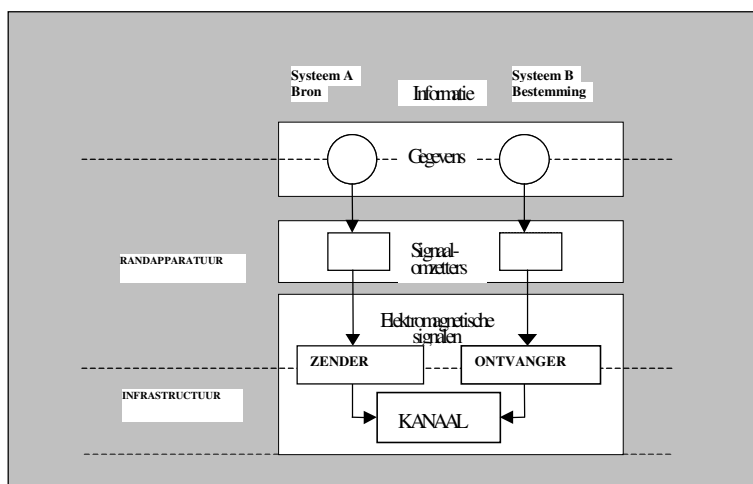
Hoe zou een techniekonafhankelijk concept van het communicatiegeheim uitgaande van bovenstaande kruisvlakbenadering eruit kunnen zien? Ik zal hieronder proberen om een concept van het grondrecht te schetsen dat de huidige bescherming van enkele communicatiemiddelen op een techniekonafhankelijke wijze naar de informatiemaatschappij vertaalt.

## VI Aanknopingspunten voor een nieuw concept

De eerste stap in dit vertalingsproces is een abstractie van de naar huidig recht beschermde specifieke communicatiemiddelen, zodat onthecht van een specifiek communicatiemiddel kan worden bekeken welke eigenschappen onontbeerlijk zijn voor de transmissie, in welke vorm dan ook, van communicatie.

In de communicatiewetenschap wordt bij de beschrijving van het communicatieproces vaak gebruik gemaakt van een model waarin zender, kanaal en ontvanger worden onderscheiden. De

zender verstuurt zijn boodschap over een kanaal naar een ontvanger. De technische werking van een telecommunicatietransmissiesysteem laat zich ook in een dergelijk model omschrijven. Sterk vereenvoudigd zou een telecommunicatietransmissiesysteem er bijvoorbeeld zo uit kunnen zien.<sup>39</sup>



Hierbij dient te worden opgemerkt dat de communicatiewetenschappelijke termen zender en ontvanger in de figuur gevormd worden door bron + zender en bestemming + ontvanger. Ook post kan in een dergelijk model worden beschreven. Post onderscheidt zich dan van telecommunicatie doordat de boodschap niet wordt omgezet in elektromagnetische signalen, maar in zijn geheel wordt overgebracht. De functies van bron en zender vallen derhalve samen, hetzelfde geldt in beginsel voor bestemming en ontvanger. Omdat geen signalen, maar de boodschap zelf wordt overgedragen en tussentijds opgeslagen, hoeft onderweg geen kopie te worden gemaakt.

Bij zowel post als telecommunicatie wordt de boodschap echter door een zender in een bepaalde vorm (al dan niet verpakt) op een bepaald punt in een infrastructuur ingebracht ter aflevering bij een ontvanger.

Het gewone gesprek wijkt van dit model af, nu niet van een met post en telecommunicatie vergelijkbaar kanaal gebruik wordt gemaakt. Het kanaal wordt namelijk bij het gewone gesprek niet door een ander ter beschikking gesteld. Ook hier kan echter een kanaal, d.w.z. een medium waarover een boodschap naar de bestemming wordt overgedragen, onderscheiden worden (de ether). Dat geen gebruik wordt gemaakt van de diensten van een ander heeft wel gevolgen voor het beschermingsregime dat geldt. Wanneer de communicatie aan een ander wordt toevertrouwd, zal de maatschappelijke zorgvuldigheid met zich mee brengen dat de ander zich inspant om de communicatie te bezorgen bij de geadresseerde, zonder dat een derde kennis neemt van de communicatie. Dit zal ik hieronder nog verduidelijken.

Een grondrecht dat de strekking heeft de vrije uitwisseling van gedachten en gevoelens in besloten kring te waarborgen, heeft in theorie drie mogelijke aanknopingspunten, te weten de inhoud (de boodschap kan openbaar zijn of slechts bestemd voor een bepaalde ontvanger), de vorm waarin de boodschap wordt verstuurd (open of besloten) of het communicatiekanaal (open of besloten). Bij alle drie de aanknopingspunten is sprake van enigerlei vorm van adressering. Bij e-mail bijvoorbeeld is er adressering op het niveau van de boodschap (de aanhef), de vorm (het e-mailadres) en het kanaal (het IP-adres).

<sup>39</sup> De figuur is afkomstig uit J.C. Arnbak, J.J. van Cuijlenburg & E.J. Dommering, *Verbinding en ontvlechting in de communicatie. Een studie naar toekomstig overheidsbeleid voor de openbare elektronische informatievoorziening*, Amsterdam: Otto Cramwinckel 1990, p. 7.

We kunnen aan de hand van deze aanknopingspunten het object van een communicatiegeheim in het digitale tijdperk nader vaststellen. Alle aanknopingspunten hebben namelijk bepaalde eigenschappen die van invloed zijn op de reikwijdte van het grondrecht op dat niveau.

Allereerst kunnen we vaststellen dat de communicatie-inhoud geen geschikt aanknopingspunt vormt voor een grondrecht dat de vrijheid om ongestoord te corresponderen beschermen wil. Om te bepalen of een inhoud voor bescherming in aanmerking komt, dient dan namelijk kennis te worden genomen van de inhoud.<sup>40</sup>

De communicatievorm is in beginsel wel een mogelijk aanknopingspunt. Onder vorm versta ik hier de gedaante waarin een boodschap in het kanaal wordt ingebracht. Het huidige briefgeheim vormt eigenlijk het schoolvoorbeeld voor een dergelijke benadering. Doorslaggevend voor bescherming door het briefgeheim is de definitie van brief. Onder het huidige briefgeheim is een brief pas een brief als deze in een envelop zit, dan wel in een daarmee vergelijkbare verpakking. Aan de hand van de vorm (al dan niet verpakt) wordt zo bepaald of de boodschap beschermd wordt.<sup>41</sup> Bij nieuwe media kan een vergelijkbare eis gesteld worden. De functie van de envelop (het bieden van enige mate van beveiliging) wordt dan bijvoorbeeld vervangen door de toepassing van encryptietechnieken.

Het derde aanknopingspunt wordt gevormd door het kanaal waarover het daadwerkelijke transport van communicatie plaatsvindt. Het telefoongeheim knoopt bijvoorbeeld aan bij het gebruikte kanaal. Traditioneel bestaat dat kanaal bij telefonie uit het hiërarchisch opgebouwde circuitgeschakelde telefoonnetwerk. Dit en het feit dat bij telefonie van meet af aan dienstverlening en netwerkbeheer in een hand waren, zorgen ervoor dat het vaste telefoonnetwerk een redelijke mate van beslotenheid kan bieden.

Een eis van beslotenheid is echter op het niveau van het kanaal niet werkbaar meer. Convergentie leidt er namelijk toe dat dienstneutrale netwerken (van netwerken) ontstaan waarbij het netwerk niet langer de aard van het gebruik bepaalt, maar die functie steeds meer wordt overgenomen door protocollen. Dienstverlening en netwerkbeheer zijn gescheiden. Iedere boodschap wordt opgesplitst in pakketjes die langs verschillende trajecten naar de plaats van bestemming worden verzonden en er is geen centrale organisatie, maar een veelheid aan dienstverleners die bij het vervoer zijn betrokken. Hierdoor kunnen pakketjes informatie willekeurige routes volgen over verschillende aan elkaar gekoppelde infrastructuren die elk een ander niveau van beveiliging kunnen hebben. Het criterium van beslotenheid verliest hierdoor zijn bruikbaarheid.

Moeten we hieruit opmaken dat de communicatievorm het enige geschikte aanknopingspunt vormt voor een grondrecht op communicatiegeheim in het digitale tijdperk, zoals in wezen ook door de Commissie Franken wordt voorgesteld? Mijns inziens is dat niet het geval. Op het niveau van het daadwerkelijke transport is de vorm waarin de communicatie wordt verzonden, namelijk niet onderscheidend meer. Op dit niveau zijn er alleen maar digitale pakketjes informatie (0en en 1en), waardoor geen onderscheid gemaakt kan worden tussen open en besloten communicatievormen. Tijdens het transport kan derhalve slechts bij het kanaal worden aangeknoopt. Een techniekonafhankelijk grondrecht kan daarbij geen onderscheid maken tussen open en besloten kanalen. Dit wordt ook steeds meer arbitrair, nu telecommunicatie steeds meer over allerlei verschillende infrastructuren naar de plaats van bestemming wordt geleid.

De techniek dwingt ons derhalve, paradoxaal genoeg, een onderscheid te maken tussen bescherming van *point-to-point*-communicatie in de transportfase en bescherming buiten de transportfase. In de transportfase dient het geheim aan te knopen bij het kanaal, buiten de transportfase vormt de communicatievorm het aanknopingspunt. Dit betekent dat het toekomstige communicatiegeheim eigenlijk uit twee verschillende geheimen zou bestaan, een transportgeheim en een geheim dat ziet op bescherming buiten de transportfase.<sup>42</sup>

---

<sup>40</sup> Nieuwenhuis 2001, p. 33.

<sup>41</sup> Bij brieven gaat het volgens de grondwetgever 1983 om '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' *Kamerstukken II 1975/1976, 13 872, nr. 2, p. 44-46.*

<sup>42</sup> Het Duitse Grundgesetz kent een soortgelijk onderscheid. Art. 10 GG onderscheidt 3 geheimen: het postgeheim, het briefgeheim en het telecommunicatiegeheim. Toen post en telecommunicatie nog een staatsmonopolie waren, vormde het postgeheim een transportgeheim. Tijdens het transport gingen brief- en telecommunicatiegeheim in het postgeheim op. Het postgeheim beschermde alle communicatie, verpakt/ beveiligd of niet, die wordt getransporteerd. Buiten het transport beschermden brief- en telecommunicatiegeheim besloten vormen van communicatie. Tegenwoordig wordt in Duitsland ook wel aangenomen dat het

Deze benadering sluit nauw aan bij het toekomstige Europese regelgevingskader voor de elektronische communicatiesector.<sup>43</sup> Onderdeel van dit kader vormt ook een Europese norm met betrekking tot het communicatiegeheim, neergelegd in art. 5 van de Richtlijn betreffende elektronische communicatie en privacy.<sup>44</sup> Het uitgangspunt van dit nieuwe kader, en derhalve van het communicatiegeheim als onderdeel daarvan, is dat regelgeving uit dient te gaan van zogenaamde dienstenneutrale netwerken. Daartoe verheft het nieuwe kader het begrip elektronische communicatie tot norm. Op het niveau van de transmissie mogen geen verschillende regels gelden voor elektronische communicatiediensten en -netwerken. Het lijkt raadzaam deze benadering ook ten aanzien van het grondrecht op communicatiegeheim te volgen.

## VII Twee geheimen

Ik stel derhalve voor binnen het communicatiegeheim een nadere onderverdeling te maken tussen een transportgeheim, dat ik hier het geheim in enge zin wil noemen, en het geheim buiten transport, het geheim in ruime zin, zodat niet-openbare communicatie in alle fasen van het communicatieproces beschermd wordt. Nu zou ook betoogd kunnen worden dat communicatie buiten de transportfase reeds door het recht op privacy beschermd wordt. Dit betoog verliest echter het verband met de communicatievrijheid uit het oog, op grond waarvan niet valt in te zien dat communicatie buiten de transportfase buiten het communicatiegeheim dient te worden geplaatst. Bovendien verwaarloost deze benadering ten onrechte de toegenomen, en nog toenemende, kwetsbaarheid van communicatie buiten de transportfase. De rechtvaardiging van een sterkere bescherming van niet-openbare communicatie in vergelijking met de privacy ligt mijns inziens juist in de samenkomst van twee fundamentele belangen.

Dat bijvoorbeeld in het EVRM de correspondentie onder het privacyartikel beschermd wordt, is mijns inziens geen tegenargument. Niet alleen wordt correspondentie in de jurisprudentie van het Europese Hof niet uitsluitend onder artikel 8 beschermd, maar onder omstandigheden ook onder artikel 10<sup>45</sup>, het onderscheid tussen artikel 8 en 10 is in de informatiemaatschappij steeds moeilijker te maken.<sup>46</sup> Het systeem van het EVRM noodzaakt, nu het niet voorziet in een bijzondere positie voor een recht op communicatiegeheim, tot een arbitraire differentiatie ten aanzien van *point-to-point*-communicatie in een convergerende omgeving.

Nu belangen van privacy en communicatievrijheid in het informatietijdperk convergeren, kan het communicatiegeheim een belangrijke waarborgfunctie vervullen. In vergelijking met het recht op privacy kan het concept van het geheim namelijk relatief duidelijk worden ingevuld, zoals hieronder zal blijken.

Juist door deze relatieve duidelijkheid biedt het geheim de burger in potentie een sterkere bescherming. Het recht op privacy kan immers 'op zeer uiteenlopende gebieden naar voren komen'.<sup>47</sup> Het weidse concept van de privacy doet afbreuk aan de bescherming die de privacy biedt, aangezien een ruimere definitie over het algemeen tot soepelere beperkingsmechanismen leidt. Mijns inziens verdient het derhalve aanbeveling het communicatiegeheim niet in de privacy te laten opgaan en daardoor te laten uitsterven, maar dient dit grondrecht opnieuw doordacht te worden, zodat het in een fundamenteel gewijzigde context uit zijn as herrijst.

Hoe zouden beide geheimen conceptueel nader kunnen worden vormgegeven?

## VII Een mogelijke conceptuele uitwerking

### ***Het geheim in enge zin: het transportgeheim***

---

telecommunicatiegeheim een transportgeheim is. Zie ook W.A.M. Steenbruggen, 'Mag ik even kijken? Een netwerk kwestie van verantwoordelijkheid', *Computerrecht* 2001-4, p. 173-185.

<sup>43</sup> Zie daarover bijvoorbeeld E.J. Dommering, De nieuwe Brusselse telecommunicatierichtlijnen, *Computerrecht* 2001-1, p. 4-10.

<sup>44</sup> 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, *PbEG* L 201/37 (31.07.2002). Zie W.A.M. Steenbruggen, 'Herziening hoofdstuk 11 Tw: tijd voor een heroverweging?' te verschijnen in *Computerrecht* 2003-1.

<sup>45</sup> Idem noot 38.

<sup>46</sup> HR 26 februari 1999, NJ 1999 (*Antelecom*).

<sup>47</sup> *Kamerstukken II* 1975/1976, 13 872, nr. 3, p. 40-41.

Het transportgeheim beschermt zoals boven weergegeven het communicatiekanaal. De ratio hiervan vormt dat gebruikers slechts ongestoord kunnen communiceren, wanneer zij erop kunnen vertrouwen dat communicatie veilig aan een transporteur ter vervoer kan worden toevertrouwd.

De transporteur heeft in dit kader een bijzondere functie. Boven vergeleek ik het communicatiegeheim met een kruispunt. Om te kunnen communiceren, moet de burger dit kruispunt oversteken. Daarvoor heeft hij de keuze tussen twee verschillende mogelijkheden: hij steekt zelf over of hij maakt gebruik van het openbaar vervoer. In het eerste geval moet hij zelf maatregelen nemen om zich te beschermen, in het tweede geval zal de openbaar vervoerder bepaalde maatregelen ter beveiliging moeten nemen. De overheid heeft de taak deze maatregelen in wet- en regelgeving vorm te geven. Deze maatregelen zouden mijns inziens kunnen bestaan uit bijvoorbeeld beveiliging van de communicatie tegen blikken van derden, het inrichten van het netwerk op een zodanige wijze dat het vervoer van A naar B binnen de afgesproken termijn kan geschieden, het vernietigen van op het netwerk achtergebleven kopieën en het zo spoedig mogelijk wissen van gegevens over het communicatieproces.

Wanneer is het transportgeheim van toepassing? Een mediaspecifiek onderscheid is in het digitale tijdperk nog wel mogelijk – voor post zou bijvoorbeeld een ander regime kunnen gelden dan voor telecommunicatie –, maar zou niet techniekonafhankelijk zijn. Ervan uitgaande dat het grondrecht techniekonafhankelijk dient te zijn, valt dit af.

Door convergentie is ook een eis van beslotenheid op het niveau van het kanaal niet langer bruikbaar. Dit zou immers ook een techniekafhankelijk criterium zijn. Voor bescherming dient derhalve een ander criterium gezocht te worden.

Asscher pleit in zijn proefschrift voor adressering als criterium voor toepasselijkheid van het transportgeheim.<sup>48</sup> Dit criterium heeft mijns inziens op het niveau van het transport geen werkelijk onderscheidende waarde. In de transportfase is namelijk alle informatie geadresseerd. Asscher merkt dit ook op, maar geeft aan dat adressering geen technisch, maar een functioneel criterium zou moeten zijn. Hij werkt dit vervolgens niet uit, waardoor het functionele karakter van het adresseringskarakter in de lucht blijft hangen.

Op het niveau van het transport heeft het adres primair de functie de netwerkllocatie van bestemming aan te duiden.<sup>49</sup> Het geeft dus aan waar de informatie heen moet. Omdat het gaat om een uniek adres, kan de informatie tot een gebruiker of abonnee herleid worden. Met het voorgestelde functionele adresseringscriterium heeft Asscher waarschijnlijk het oog op de identificeerbaarheid van de communicerende partijen. Het een volgt echter niet altijd automatisch uit het ander.

Mijns inziens dient uit het gebrek aan onderscheidend vermogen van adressering de consequentie getrokken te worden dat *alle* informatie die via het kanaal wordt overgedragen, onder het bereik van het transportgeheim valt. Niet alleen telefoongesprekken, e-mailverkeer en vergelijkbare communicatie, maar ook bijvoorbeeld het browsen over Internet wordt dan beschermd onder het transportgeheim. Het kanaal als zodanig wordt beschermd.

Wel dient in dat kader vastgesteld te worden wanneer sprake is van een kanaal. Waar de Commissie Franken stelt dat toepasselijkheid van het recht op vertrouwelijke communicatie kan afhangen van de aard van het kanaal, ontstaan problemen wanneer zij niet aangeeft wanneer sprake is van een kanaal.<sup>50</sup> Mijns inziens gaat het daarbij om (netwerk- of tele)diensten van een of meerdere transporteurs voorzover deze strekken ter aflevering van een door een afzender aangeboden boodschap. Zoals onderstaand figuur<sup>51</sup> duidelijk maakt, kan bij telecommunicatie een onderverdeling worden gemaakt in een viertal lagen. In dit model bevindt zich het kanaal op de niveaus 2 en 3.

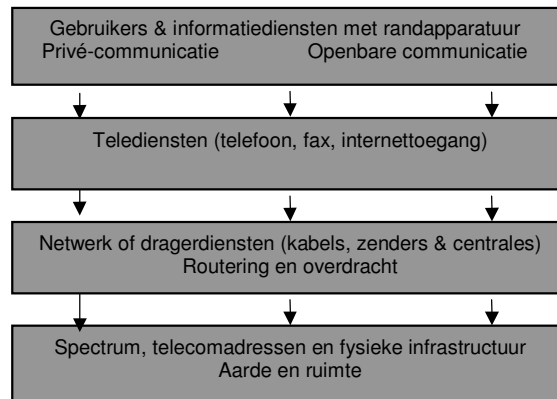
---

<sup>48</sup> Asscher 2002, p. 21 e.v..

<sup>49</sup> Zie ook E.J. Dommering e.a., *Telecommunicatienummers en domeinnamen*, ITeR 15, Deventer:Kluwer 1999.

<sup>50</sup> Rapport Franken 2000, p. 163.

<sup>51</sup> Figuur afkomstig uit Dommering 1999, p. 11.



Om te bepalen of nog sprake is van een kanaal, is de beschikkingsmacht van de transporteur relevant. Het transportgeheim is van toepassing, zolang de communicatie in de macht van de transporteur(s) is, zich op zijn netwerk bevindt. Dat betekent dat ook opgeslagen e-mail op de server van de ISP onder het transportgeheim valt, zelfs al heeft de geadresseerde zijn e-mail opgehaald. Hetzelfde geldt voor het op de voice mail ingesproken bericht.

### ***Inclusief de verkeersgegevens...***

Tegenwoordig is telecommunicatie niet meer denkbaar zonder dat gebruik wordt gemaakt van databanken waarin persoonsgegevens worden gekoppeld met elektronische adresgegevens om de juiste routing en bestemming van een boodschap tot stand te brengen.<sup>52</sup> Steeds vaker treedt een vermenging op van individuele communicatieve handelingen en het waarnemen en vastleggen van persoonsgegevens.<sup>53</sup>

In de voorstellen van het kabinet-Kok II en de Commissie Franken worden verkeersgegevens buiten het communicatiegeheim geplaatst. Ook naar huidig recht vormen de verkeersgegevens geen onderdeel van het geheim. Verkeersgegevens zouden al vallen onder de bescherming van artikel 10 Grondwet.<sup>54</sup> Deze benadering verliest echter de technische realiteit uit het oog. 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 cq. 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 emailprogramma stelt een boodschap samen die voorzien wordt van separate adresinformatie (e-mail adres). Ook technisch is hier een

<sup>52</sup> 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.

<sup>53</sup> 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.

<sup>54</sup> *Kamerstukken II 2000/2001*, 27460, nr. 1, p. 27.

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 bepaald 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](http://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.<sup>55</sup> Naast dit praktische argument is er ook een aantal principiële argumenten om verkeersgegevens onder het bereik van het communicatiegeheim te scharen. Van belang is namelijk wat de aard van het te beschermen rechtsgoed is. Terwijl artikel 10 Grondwet ziet op de bescherming van de persoonlijke levenssfeer, ziet het transportgeheim op de vertrouwelijkheid van het communicatiekanaal. Geheimhouding van verkeersgegevens vormt hiervan een wezenlijk onderdeel. Het gaat er dan ook niet zo zeer om dat verkeersgegevens veel over personen kunnen zeggen, belangrijker is dat het vertrouwen dat de burger in het communicatiekanaal stelt, kan worden aangetast, wanneer verkeersgegevens worden verwerkt voor doelen die niet noodzakelijkerwijs voortvloeien uit het leveren van de dienst. Hierin komt het hybride karakter van het communicatiegeheim naar voren. 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. Het is mijns inziens dan ook zorgwekkend dat het belang van de communicatievrijheid stelselmatig wordt genegeerd bij de discussie over verkeersgegevens.<sup>56</sup>

De uitsluiting van verkeersgegevens is bovendien niet in overeenstemming met de richtlijn elektronische communicatie en privacy. Art. 5 van deze richtlijn draagt Lid-Staten op het vertrouwelijke karakter van openbare elektronische communicatienetwerken en -diensten te waarborgen. Deze bescherming omvat de communicatie, inclusief de gegevens omtrent de communicatie. Verkeersgegevens vormen dus een onderdeel van de beschermde communicatie. Dit uitgangspunt werkt de richtlijn vervolgens uit in art. 6 dat een zeer strikt beschermingsregime voor verkeersgegevens bevat.<sup>57</sup>

### ***Het geheim in ruime zin: bescherming buiten de transportfase***

Zoals boven weergegeven, heeft het geheim in ruime zin betrekking op communicatie buiten de transportfase. Daarbij kan bijvoorbeeld worden gedacht aan een e-mail die wordt opgesteld, maar nog niet verzonden is, de brief die nog niet is gepost en de boodschap die is ingesproken op het antwoordapparaat, maar nog niet gewist. Het aanknopingspunt wordt hier gevormd door de communicatievorm. Deze benadering vormt een voortzetting van het paradigma van de brief.

Op het niveau van de communicatievorm zijn twee criteria voor bescherming denkbaar, te weten adressering en beslotenheid. Laten we even terugkeren naar de metafoor van het kruispunt. Zoals gezegd staan de burger twee mogelijkheden ter beschikking om het gevaarlijke kruispunt van communicatievrijheid en privacy over te steken. Maakt hij gebruik van de diensten van een vervoerder, dan is het transportgeheim van toepassing. In termen van de vertrouwelijke communicatie-benadering blijkt zijn 'redelijke wil tot vertrouwelijkheid' uit het feit dat hij zijn

<sup>55</sup> De nieuwe richtlijn betreffende elektronische communicatie en privacy (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, *PbEG* L 201/37) erkent dit. Art. 6 van deze richtlijn is van toepassing op zowel verkeersgegevens als de inhoud van de communicatie.

<sup>56</sup> Het Cybercrime-verdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2002, 18) wijdt geen woord aan de communicatievrijheid. Ook in het recent uitgelekte voorstel van de Deense EU-voorzitter met betrekking tot een bewaarplicht van tussen een en twee jaar wordt niet gerept over de communicatievrijheid. Meer daarover op <http://www.statewatch.org/news/2002/aug/05datafd1.htm>.

<sup>57</sup> Zie ook W.A.M. Steenbruggen, "Herziening Hoofdstuk 11 Tw. Tijd voor een heroverweging?", te verschijnen in *Computerrecht* 2003-1.

communicatie aan een derde heeft toevertrouwd.<sup>58</sup> Deze derde-transporteur heeft dan ook de plicht maatregelen te nemen ter bescherming van de vertrouwelijkheid van de aan hem toevertrouwde communicatie.

In de fase buiten het transport dient de burger zelf maatregelen te nemen ter bescherming van zijn communicatie, wil hij tenminste aanspraak kunnen maken op de specifieke bescherming van het communicatiegeheim. In dat kader is ook het criterium van de redelijke wil tot vertrouwelijkheid vervuld wanneer een derde uit objectieve feiten en omstandigheden kan opmaken dat de subjectieve wil van de zender gericht is op vertrouwelijkheid (de invulling van het beslotenheids criterium in de 'vertrouwelijke communicatie'-benadering).

Anders dan de vertrouwelijke communicatie-benadering zou ik er niet bij voorbaat van uit willen gaan dat dit criterium altijd veronderstelt dat er sprake is van een technische beveiliging in welke zin dan ook. Dat zou namelijk betekenen dat de beschermenswaardigheid afhankelijk wordt gesteld van de feitelijke bescherming.<sup>59</sup> Mijns inziens kan ook adressering onder omstandigheden voldoende zijn om aan te nemen dat sprake is van een objectieve wil tot vertrouwelijkheid.

Wanneer een burger maatregelen neemt waaruit derden kunnen opmaken dat de communicatie niet voor hen is bestemd, dan dient het recht het vertrouwen van de burger in beginsel te honoreren, hetgeen in casu betekent dat het zwaardere regime van het communicatiegeheim van toepassing is. Dit betekent niet dat communicatie waarbij geen sprake is van zodanige maatregelen, vogelvrij is. In het Nederlandse grondwettelijke systeem kan hier het algemene recht op privacy onder omstandigheden aanvullende bescherming bieden.

### ***Het gewone gesprek***

Mijns inziens dient het geheim in ruime zin ook bescherming te bieden aan het gewone gesprek. Ook hier staan zowel privacy als communicatievrijheid op het spel, wanneer een derde kennis neemt van de inhoud van de communicatie. Bovendien wordt het gewone gesprek steeds kwetsbaarder door de opkomst van steeds geavanceerdere af luister technieken en verdergaande opsporingsbevoegdheden.

Met betrekking tot het gewone gesprek zou ik dan ook willen aansluiten bij het criterium dat op basis van objectieve feiten en omstandigheden voor derden de wens tot vertrouwelijkheid kenbaar moet zijn. Het kabinet Kok-II heeft in zijn kabinetsstandpunt met betrekking tot het voorstel van de Commissie Franken dit criterium zo uitgelegd dat sprake moet zijn van een inbreuk met een technisch hulpmiddel, overigens zonder uit te leggen wat een technisch hulpmiddel precies is.<sup>60</sup>

Ook hier is het aan de communicerende partijen maatregelen te nemen die leiden tot een objectief kenbare wil tot vertrouwelijkheid. Partijen kunnen zich bijvoorbeeld afzonderen, op fluistertoon praten, elkaar briefjes toestoppen, etc. De toepasselijkheid van het geheim afhankelijk te stellen van het middel waarmee inbreuk wordt gemaakt, lijkt mij principieel onjuist, omdat het geheim de strekking heeft de wens tot vertrouwelijkheid van de communicerende partijen te honoreren. Hoe inbreuk wordt gemaakt op de vertrouwelijkheid, is in beginsel irrelevant. Door bescherming afhankelijk te stellen van het inbreukmakende middel wordt het object van het grondrecht op een vrij arbitraire wijze beperkt. De bescherming afhankelijk te stellen van het technische hulpmiddel betekent namelijk dat niet-openbare communicatie die op een andere manier wordt afgeluisterd, bijv. het bekende glas tegen de muur, door middel van infiltratie in een groep, stiekem meeluisteren, niet beschermd is, terwijl ook daarbij een inbreuk op de autonomie van de communicerende partijen wordt gemaakt waarmee zij geen rekening hoeven te houden.

## **VIII Conclusie**

<sup>58</sup> Zie ook A.J. Nieuwenhuis, 'Vertrouwde en virtuele bescherming', *NJCM-Bulletin* 1998-4, p. 427.

<sup>59</sup> Idem noot 18. Zie voorts 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.

<sup>60</sup> *Kamerstukken II* 2000/2001, 27460, nr. 1, p. 40.

De sinds 1997 gevoerde discussie met betrekking tot het communicatiegeheim berust op een fundamenteel verschil van mening over het object van een toekomstig communicatiegeheim. Twee benaderingen staan lijnrecht tegenover elkaar. Beide benaderingen zijn terug te voeren op het huidige communicatiegeheim, dat besloten communicatie tijdens transport beschermt. Omdat de transportbenadering en de vertrouwelijke communicatiebenadering beide een andere keuze maken met betrekking tot wat zij als het doorslaggevende element van het huidige geheim zien, lijken zij onverenigbaar.

De verschillen tussen beide benaderingen komen grotendeels voort uit de verschillende perspectieven van waaruit het communicatiegeheim wordt benaderd. De vertrouwelijke communicatiebenadering benadert het geheim vanuit de privacy en hecht daarom doorslaggevende waarde aan het privé-karakter van de inhoud van de boodschap. De transportbenadering heeft daarentegen meer oog voor de functie van het transport voor de communicatievrijheid.

Boven werd betoogd dat het communicatiegeheim het kruisvlak van communicatievrijheid en privacy vormt. Communicatievrijheid en privacy convergeren in het communicatiegeheim. Dit kruisvlak omvat niet alleen communicatie in de transportfase, maar ook daarbuiten komen communicatievrijheid en privacy samen. Was voorheen redengevend voor beperking van het communicatiegeheim tot de transportfase doorslaggevend dat communicatie tijdens transport extra kwetsbaar is, omdat deze aan een overheidsorgaan moest worden toevertrouwd waardoor de overheid de communicatie kon controleren, zonder dat de communicerende partijen daar enig inzicht in hadden, tegenwoordig zijn particulieren belast met het transport. Dit samen met het feit dat communicatie buiten de transportfase door de opkomst van geavanceerde af luister technieken kwetsbaar is geworden, maakt dat de beperking tot het transport niet langer vanzelfsprekend is. Wordt de kruisvlakbenadering consequent gevolgd, dan dient zowel communicatie tijdens, voor en na het transport te worden beschermd en zelfs wanneer er helemaal geen sprake is van transport. Dit betekent overigens niet dat geen onderscheid kan worden gemaakt tussen de bescherming binnen en buiten het transport.

Wanneer men uitgaat van het transportmodel bij post en telecommunicatie, volgt een onderscheid bescherming binnen en buiten het transport uit de gelaagdheid van het transportmodel. Dit betekent dat een onderscheid gemaakt kan worden tussen een geheim in enge zin dat ziet op het communicatiekanaal en het geheim in enge zin dat ziet op de vertrouwelijkheid van de communicatievorm. Door de technologische ontwikkeling in de telecommunicatie divergeren communicatievorm en -kanaal. In de transportfase dient het communicatiegeheim aan te knopen bij een dienstenneutraal en dus open kanaal. Buiten het transport knoopt het communicatiegeheim aan bij de communicatievorm die gesloten kan zijn. Op deze wijze ontstaat derhalve een tweevoudig regime binnen het communicatiegeheim.

De eigenschappen van het niveau waarop de communicatie zich bevindt, bepalen vervolgens het object van respectievelijk het geheim in enge en in ruime zin. Dat betekent bijvoorbeeld dat alle informatie beschermd wordt zolang deze zich in de beschikkingsmacht van de transporteur bevindt. Ook verkeersgegevens maken hiervan deel uit.

Buiten de transportfase bepalen de eigenschappen van de communicatievorm het object van de bescherming. Hier staat voorop of uit het gedrag van de communicerende partijen blijkt dat zij de communicatie geheim willen houden. Op deze manier kan ook het gesprek beschermd worden. Het algemene recht op privacy heeft een aanvullende werking, voorzover het gaat om een restcategorie van uitingen die naar uit de inhoud blijkt, privacygevoelig zijn.

Het is in de informatiemaatschappij niet noodzakelijk een keuze uit de vertrouwelijke communicatie- of transportbenadering te maken. In de kruisvlakbenadering worden beide verenigd, zodat niet-vertrouwelijke communicatie over de gehele linie beschermd. Op deze wijze treft het communicatiegeheim niet het lot van de dodo, maar herrijst het als glorieuze feniks.