

# Mag ik even kijken? Een netwerkwestie van verantwoordelijkheid

W.A.M. Steenbruggen<sup>1</sup>

## Inleiding

In mei 2000 richtte het ILOVEYOU-virus wereldwijd grote schade aan. De schade wordt geschat op enkele miljarden gulden. Naast deze schade bij gebruikers genereerde het virus zoveel e-mailverkeer dat netwerken overbelast raakten. Het virus beperkte dus de beschikbaarheid van de dienst. Deze schade had grotendeels voorkomen kunnen worden, wanneer Internet Service Providers (ISP's) verspreiding van e-mails met dit virus zouden zijn tegengegaan door te filteren. Preventief optreden tegen computervirussen door Internet providers is nog geen 'issue'. Op dit moment wordt de verantwoordelijkheid bij de gebruiker gelegd. Hij moet zich zelf maar beschermen. Gezien de ervaringen met de Love Bug is het maar de vraag of dat terecht is. Dit virus bewees dat de gebruiker zich niet altijd kan beschermen. Wellicht zouden Internet providers daarbij een helpende hand moeten toesteken, met name wanneer een virus hun servers platlegt. Het gevaar van computervirussen voor de informatiemaatschappij mag niet onderschat worden. Door convergentie komen steeds meer communicatiemedia in gevaar. De sterk groeiende toename van het Internetgebruik maakt dat de potentiële schade door virussen exponentieel toeneemt.

De heersende mening, zowel in Nederland als in Duitsland, lijkt te zijn dat ISP's niet aansprakelijk kunnen worden gesteld voor de inhoud van e-mail, aangezien het communicatiegeheim hun verbiedt van privé-communicatie kennis te nemen.<sup>2</sup> Het communicatiegeheim is in deze benadering beperkt tot een verbod tot kennisname. In de Duitse grondrechtstheorie wordt echter ook een tweede aspect erkend, te weten een verbod om inlichtingen omtrent de inhoud aan derden te verschaffen dat onder omstandigheden in de plaats van het verbod tot kennisname treedt.

Als ISP's kennis mogen nemen van e-mail, dan kan dat betekenen dat onder omstandigheden een zorgplicht bestaat dat ook te doen. Dit artikel is dan ook toegespitst op de vraag of het communicatiegeheim naar Nederlands en Duits recht beperkt is tot een verbod tot kennisname. Dat betekent dat voornamelijk de constitutionele aspecten van een controle van e-mail aan bod komen. Andere vragen met betrekking tot de aansprakelijkheid van tussenpersonen op het Internet komen gezien het beperkte kader van dit artikel niet aan bod.

Een vergelijking met het Duitse recht ligt vanwege een aantal redenen voor de hand. Allereerst is de grondrechtstheorie in Duitsland veel omvangrijker dan in Nederland, mede omdat Duitsland een constitutioneel hof heeft dat wetten op hun grondwettigheid kan toetsen. Ten tweede kent ook de Duitse grondwet een artikel waarin het communicatiegeheim is gecodificeerd. Dit grondrecht heeft een techniekafhankelijke component en maakt geen onderscheid naar gelang de gebruikte techniek ten aanzien van de mate van bescherming, in tegenstelling tot het Nederlandse grondrecht. Onder het Nederlandse grondrecht is de status van e-mail onduidelijk. Een vergelijking met het Duitse communicatiegeheim kan wellicht wat meer theoretische helderheid omtrent de toelaatbaarheid van een controle van e-mail verschaffen.

## Functie van de aanbieder van e-mail

Gezien het feit dat dit artikel beoogt de belangrijkste drempel voor aansprakelijkheid voor de inhoud van e-mail te onderzoeken, moet voor een juist begrip eerst een klein kader geschetst worden. Er worden verschillende soorten Internet providers onderscheiden. De invloed die een Internet provider kan uitoefenen op de inhoud van de getransporteerde communicatie is afhankelijk van de rol en functie die een provider in het communicatieproces op Internet inneemt. Niet elke Internet provider kan invloed uitoefenen op specifieke boodschappen. We moeten dus nagaan welke positie een aanbieder van e-mail

---

<sup>1</sup> W.A.M. Steenbruggen is werkzaam als projectonderzoeker aan het Instituut voor Informatierecht te Amsterdam. Dit artikel is een bewerking van een afstudeerscriptie.

<sup>2</sup> K.J. Koelman, 'Wat niet weet, wat niet deert: civielrechtelijke aansprakelijkheid van de provider', *Mediaforum* 1998, nr. 7/8, p. 211-212 en C.B. van der Net, *Grenzen stellen op het Internet. Aansprakelijkheid van Internetproviders en rechtsmacht*, Deventer: Gouda Quint 2000, p. 150. Voor Duitsland verwijs ik naar U. Sieber, 'Die rechtliche Verantwortlichkeit im Internet. Grundlagen, Ziele und Auslegung von § 5 TDG und § 5 MDtSV', *MultiMedia und Recht* 1999-2, p. 11 en G. Spindler, 'Verantwortlichkeit von Diensteanbietern nach dem Vorschlag einer E-Commerce-Richtlinie', *MultiMedia und Recht* 1999-4, p. 201.

op Internet inneemt. Als hij namelijk überhaupt niet op specifieke e-mails kan filteren, heeft de in dit artikel ondernomen exercitie weinig zin.

Bij het vaststellen van eventuele aansprakelijkheid van Internet providers voor andermans inhoud speelt ook de mogelijkheid invloed uit te oefenen een rol.

Zo kan een access provider in beginsel niet aansprakelijk zijn voor de inhoud van door hem vervoerde informatie, aangezien hij louter toegang verschaft en niets aan de informatie verandert.<sup>3</sup> Hij stelt geen capaciteit aan gebruikers ter beschikking waarop voor onbepaalde tijd informatie kan worden opgeslagen. Hij heeft derhalve niet de mogelijkheid de inhoud van een individuele e-mail te beïnvloeden. Wel kan hij volgens de huidige stand van de techniek op het gebruikte protocol filteren, maar dat is een paardenmiddel en zal derhalve over het algemeen een ontoelaatbare inbreuk op fundamentele rechten zijn.

Een service provider daarentegen stelt voor onbepaalde tijd capaciteit op zijn server beschikbaar en heeft de mogelijkheid informatie op zijn server te beïnvloeden. Hij kan aansprakelijk zijn voor de inhoud van de informatie, wanneer hij weet dat er onrechtmatige informatie op zijn server staat en deze vervolgens niet verwijdt.<sup>4</sup> Of hij daadwerkelijk aansprakelijk voor de schade is, is daarmee nog niet gezegd. De hier geschetste aansprakelijkheidsregeling heeft mijns inziens het karakter van een voorfilter. Na dit filter zullen andere vragen die het civielrecht ten aanzien van aansprakelijkheid uit onrechtmatige daad stelt, beantwoord moeten worden. Onder meer zal daarbij de omvang van de schade, de voorzienbaarheid en het al dan niet aanwezig zijn van een rechtvaardigingsgrond een rol spelen. Er worden meer rollen onderscheiden, maar de twee bovenstaande zijn voor dit betoog het belangrijkste. We zullen moeten nagaan of de functie van de aanbieder van e-mail louter bestaat uit het bieden van toegang of dat hij meer doet dan dat.

De belangrijkste standaard voor het gebruik van e-mail is het Simple Mail Transfer Protocol (SMTP). Een e-mailadres is opgebouwd in de vorm van een gebruikersnaam@domein. Het domein geeft de netwerkbestemming van het bericht aan. De gebruikersnaam geeft de geadresseerde aan. Het bericht wordt pakketgeschied volgens het TCP/IP-protocol verstuurd. Het Transmission Control Protocol zorgt ervoor dat de te versturen berichten worden opgedeeld in eenheden van gelijke omvang. Deze eenheden worden vervolgens in IP-enveloppen gestopt waarop de plaats van bestemming staat aangegeven. De pakketjes worden dan naar de plaats van bestemming gerouteerd. Daar worden de delen weer samengevoegd. Het SMTP zorgt ervoor dat het betreffende bericht wordt herkend als e-mailbericht, doordat een *Port*-nummer aan het bericht wordt toegekend. Hierdoor weet de computer van bestemming dat het om een e-mailbericht gaat. Meestal wordt het bericht opgeslagen in de mailbox van de geadresseerde. Wanneer deze zich op de server van de provider bevindt, zal, wanneer de e-mail door de geadresseerde wordt opgevraagd, nog een extra handeling moeten plaatsvinden. Er moet wederom een ander *Port*-nummer toegekend worden.

Vaak heeft de eindgebruiker de mogelijkheid om zijn berichten op de server van de provider te laten staan. Hij kan dat meestal in zijn e-mailprogramma instellen. In dat geval stelt een provider dus feitelijk capaciteit beschikbaar.

Een aanbieder van e-mail is gezien het bovenstaande meer dan louter doorgeefluik, hij is een service provider. Dat betekent dat hij in beginsel technisch in staat moet worden geacht op de inhoud van individuele boodschappen te filteren. Daarbij zou gedacht kunnen worden aan een softwarematige oplossing waarbij op specifieke tekstkenmerken gefilterd wordt. Bij het ILOVEYOU-virus zou dat bijvoorbeeld kunnen aan de hand van de Subject-line die Fw: I Love you bevat.

### **Het communicatiegeheim**

Het communicatiegeheim kan een controle van e-mail in de weg staan. Als zodanig heeft het communicatiegeheim ook invloed op de vraag naar de eventuele aansprakelijkheid voor e-mail. Wanneer een ISP geen kennis van e-mail mag nemen, kan hij daarvoor ook niet aansprakelijk gesteld worden. Het communicatiegeheim is neergelegd in art. 13 Grondwet (Gw). Dit artikel beschermt het brief-, telefoon –en telegraafgeheim. Dit artikel is van oudsher tegen de overheid gericht. Post was oorspronkelijk een staatsmonopolie.

---

<sup>3</sup> Zie ook art. 12 van de E-commercerichtlijn (Richtlijn 2000/31/EG van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* 2000 L 178/1).

<sup>4</sup> Rb. 's-Gravenhage 9 juni 1999, *Computerrecht* 1999-4, p. 200-205 m.nt. P.B. Hugenholtz (*Scientology/XS4All*). Vgl. ook art. 14 van de E-commercerichtlijn.

Tegenwoordig hebben particulieren de rol van de overheid bij het transport van privé-communicatie overgenomen. Dit geldt voor post, telefonie, maar ook voor e-mail. Nagegaan dient dus te worden of art. 13 Gw ook tussen burgers onderling zijn werking doet gelden.

In 1983 sprak de regering zich bij de grondwetswijziging uit over de horizontale werking van grondrechten. Zij introduceerde een glijdende schaal met vijf verschillende gradaties van horizontale werking, variërend van directe horizontale werking tot een opdracht aan de wetgever om een nader geformuleerd belang ook in particuliere verhoudingen te verwezenlijken.<sup>5</sup> Een duidelijk antwoord op de vraag hoe individuele grondrechten kunnen doorwerken, werd echter niet gegeven.

De rechtspraak biedt evenmin een consistent beeld. Verhey concludeert dat de glijdende schaal in de praktijk niet zo functioneert. In plaats daarvan kan men een driedeling in de jurisprudentie constateren: uitspraken waarin directe werking van grondrechten wordt aangenomen, die waarin sprake is van indirecte werking en uitspraken waarin van doorwerking op het eerste gezicht niets blijkt, maar waarin het grondrecht impliciet wel een rol bij de privaatrechtelijke rechtsvinding speelde.<sup>6</sup>

Ik wil hier niet te diep ingaan op de horizontale werking, maar ervan uitgaan dat het in art. 13 neergelegde communicatiegeheim zich in elk geval als af te wegen zwaarwegend belang in de open normen van het BW manifesteert.

Onderzocht moet worden of het communicatiegeheim zoals dat in art. 13 Gw uitdrukking heeft gevonden überhaupt e-mail beschermt en zo ja, of dat betekent dat een kennisname ten behoeve van de goede werking van de dienst of ter voorkoming van schade uitsluit.

Artikel 13 noemt e-mail niet. Genoemd worden louter de communicatiemiddelen brief, telefoon en telegraaf. Het briefgeheim wordt beschermd in het eerste lid, de beide andere middelen in het tweede lid. Opvallend is dat beide leden een ander beperkingsregime kennen. Het eerste lid kan beperkt worden in de gevallen bij de wet bepaald op last van de rechter. Het tweede lid daarentegen kan in de gevallen bij de wet bepaald door of met machtiging van degenen die daartoe bij de wet zijn aangewezen. Beide leden kennen geen doelcriteria. Of beperkingen zijn toegestaan die niet uitdrukkelijk aan de competentievoorschriften voldoen, is de vraag. Bij de grondwetsherziening heeft de grondwetgever de leer van de algemene beperkingen afgewezen. Onder algemene beperkingen wordt verstaan

Beperkingen welke niet [...] met het oog op een bepaald grondrecht zijn vastgesteld, maar die veroorzaakt worden doordat een geheel buiten de sfeer van een grondrecht gelegen regeling als neveneffect heeft dat de uitoefening van een grondrecht beperkingen ondergaat.<sup>7</sup>

Beperkingen zonder grondwettelijk fundament zijn echter volgens de regering toch mogelijk. Daarbij onderscheidt zij drie categorieën:

1. De heersende rechtsovertuigingen evolueren zodanig dat bepaalde belemmeringen in een grondrecht, zonder tot een beperkingsclausule herleidbaar te zijn, algemeen aanvaard worden.
2. In de praktijk komen rechtsinstellingen tot ontwikkeling die weliswaar strijdig zijn met de letter van een grondrecht, maar die een gevestigde en algemeen aanvaarde plaats in het rechtsbestel innemen.
3. Een grondrechtsartikel moet op redelijke wijze uitgelegd worden; als een overheidsmaatregel een grondrecht naar de letter genomen beperkt, maar wanneer intrekking van die maatregel in flagrante strijd zou zijn met wat algemeen als redelijk wordt aangemerkt, dan zal zo'n maatregel niet licht ongrondwettig worden geacht. Daarbij kan de eis van proportionaliteit en van het rekening houden met maatschappelijke en persoonlijke belangen een rol spelen.

Daarbij dient te worden bedacht dat grondrechten sowieso redelijk moeten worden uitgelegd. Sinds 1983 blijkt dat wetgever en rechter wel ongeschreven beperkingen aanvaardden of hun toevlucht zoeken in een restrictieve interpretatie. In plaats van strikte toepassing van het grondwettelijke systeem wordt steeds

---

<sup>5</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, p. 131.

<sup>6</sup> L.F.M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy*, Zwolle: W.E.J. Tjeenk Willink 1995, p. 131.

<sup>7</sup> A.K. Koekkoek, W. Konijnenbelt, 'Het raam van hoofdstuk 1 van de herziene Grondwet', in: A.K. Koekkoek, W. Konijnenbelt & F.C.L.M. Crijns (red.), *Grondrechten. Commentaar op hoofdstuk 1 van de herziene Grondwet*, Nijmegen: Ars Aequi Libri 1982, p. 24.

meer een belangenafweging *in concreto* toegepast.<sup>8</sup> Daarmee ontwikkelt de grondrechtelijke beperkingsmethodiek zich in de richting van een noodzakelijkheidstoetsing à la het EVRM.<sup>9</sup> Door grondrechtsinterpretatie kunnen grondrechten beperkt worden. Anders dan bij geschreven beperkingsclausules die de feitelijke bescherming bepalen, wordt in dat geval de potentiële beschermingsomvang door middel van een restrictieve interpretatie of door het aannemen van ongeschreven beperkingen beperkt.

In art. 13 lid 1 Gw is het begrip ‘brief’ bepalend voor de grondwettelijke bescherming. Doorgaans worden brieven als communicatie in ruime zin opgevat. Daarbij gaat het om

een communicatie die plaatsvindt in gesloten enveloppen, althans in een verpakking welke het oogmerk van de afzender tot uitdrukking brengt, dat derden [...] van de inhoud van de brief geen kennis kunnen nemen.<sup>10</sup>

De communicatie moet op een vaste informatiedrager zijn vastgelegd en gesloten zijn. De Hoge Raad bepaalde in 1994 dat gegevens die in een zakcomputer zijn opgeslagen geen brief zijn, wanneer het niet gaat om *mededelingen, gericht tot een of meer anderen dan de gebruiker* gaat.<sup>11</sup> Of adressering daarmee het uitsluitende of slechts een aanvullend criterium is geworden, is niet duidelijk. Adressering kan mijns inziens slechts een aanvullend criterium zijn om tussen privé- en massa-communicatie te onderscheiden. Daarna dient nog bepaald te worden of het briefgeheim de communicatie beschermt. In art. 13 wordt immers een onderscheid tussen verschillende vormen van privé-communicatie gemaakt. Het tweede lid van artikel 13 beschermt het telefoon –en telegraafgeheim. Omdat op dit geheim soms door de vervoerder om technische redenen inbreuk moet worden gemaakt, heeft het telefoongeheim ook de strekking dat informatie niet verder verspreid wordt. Blijkbaar kent het telefoon –en telegraafgeheim een aantal aspecten. In eerste instantie geldt een verbod tot kennisname. Is kennisname echter noodzakelijk om technische redenen, om stringen te verhelpen, dan geldt een verbod informatie aan derden te verstrekken. Zou e-mail onder art. 13 lid 2 Gw beschermd worden, dan kan in beginsel een kennisname ten behoeve van de goede werking van de dienst, analoog aan dat van het telefoon –en telegraafgeheim zijn toegestaan. Wanneer de beschikbaarheid van de dienst op het spel staat, zou een ISP van de inhoud van e-mail kennis kunnen nemen. Bij de Love Bug stond inderdaad die beschikbaarheid op het spel. Hierop kom ik later terug.

Een andere eis voor bescherming op grond van art. 13 lid 2 Gw is een bepaalde mate van beveiliging.<sup>12</sup> Degene die zich van deze media bedient, moet ervoor zorgen dat van een geheim te houden communicatie sprake kan zijn.<sup>13</sup>

E-mail wordt in geen van beide leden genoemd. Qua techniek lijkt e-mail het meest op de telegraaf. De telegraaf werkt grof gezegd als volgt. Met behulp van een telegraafstoestel wordt de tekst van een telegram omgezet in elektronische pulsen, die via een kabel naar een centrale verzonden worden. Daar wordt het bericht in zijn geheel ontvangen en opgeslagen, vervolgens wordt bepaald wat de volgende centrale op de route is en tenslotte wordt het telegram naar die centrale doorgezonden. Tijdens het transport worden dus telkens kopieën gemaakt. Omdat de getransporteerde eenheid een bericht is, wordt dit berichtschakelen of *message switching* genoemd.<sup>14</sup> De vergelijking met het pakketgeschakelde transport van e-mail ligt voor de hand. E-mail zou dus in beginsel onder het telefoon –en telegraafgeheim gebracht kunnen worden.

Dit betekent niet noodzakelijkerwijs dat de ILOVEYOU-mail door het telefoon –en telegraafgeheim beschermd zou worden. De maker van de *Love Bug* heeft er het nodige aan gedaan om de e-mail met het virus een zo groot mogelijk publiek te laten bereiken. Hij heeft het virus zo ontworpen dat het zichzelf verzond naar alle adressen in een adresboek. Van een geheim te houden communicatie kan dan geen sprake zijn. Bij het ILOVEYOU-virus was op een vrij eenvoudige wijze vast te stellen dat sprake was van een automatisch doorgezonden e-mail aan de hand van de subject line in de header. Deze bevatte immers Fw: I Love You.

---

<sup>8</sup> Verhey, p. 28.

<sup>9</sup> Zie ook F.H. Kistenkas, ‘Naar een grondrechtelijke evenredigheidstoets’, *Gem.st* 1991, nr. 6925, p. 377 e.v.

<sup>10</sup> *Kamerstukken II 1975/1976*, 13872, nr. 2, p. 44-46.

<sup>11</sup> HR 29 maart 1994, *Delikt en Delinkwent* 1993, 314; L.F. Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie*, Deventer: Kluwer 1999, p.71.

<sup>12</sup> E.J. Dommering e.a., *Informatierecht. Fundamentele rechten voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2000, p. 79.

<sup>13</sup> *Kamerstukken II 1975/1976*, 13872, nr. 3, p. 46.

<sup>14</sup> Dommering e.a. 2000, p. 87.

Of het huidige artikel 13 e-mail beschermt, is onzeker. Deze onzekerheid wordt veroorzaakt door de techniekafhankelijke formulering van het grondrecht en versterkt wordt doordat de mate van bescherming van de gebruikte techniek afhankelijk is. Een adequate bescherming van e-mail lijkt op basis van het huidige artikel niet mogelijk.

## EVRM

Art. 94 Gw bepaalt dat binnen het Koninkrijk geldende wettelijke voorschriften niet toegepast worden, indien dit niet verenigbaar is met een ieder verbindende bepalingen van verdragen en besluiten van volkenrechtelijke organisaties. Het Europees Verdrag tot Bescherming van de Rechten van de Mens (EVRM) bevat een algemene norm inzake de bescherming van de persoonlijke levenssfeer, namelijk art. 8. Dit artikel is een ieder verbindende bepaling in de zin van art. 94 Gw. Het is dus van belang of filteren van e-mail onder 8 EVRM toegestaan is en zo ja, onder welke voorwaarden.

In de jurisprudentie van Europese Hof en de Europese Commissie voor de Rechten van de Mens is art. 8 zodanig uitgelegd dat niet alleen briefverkeer, maar ook telefoonverkeer<sup>15</sup> en andere communicatievormen onder de bescherming van art. 8 vallen. Het Hof verbond de begrippen "correspondence" en "private life" met elkaar. Hierdoor wordt niet langer slechts besloten, maar ook niet-besloten communicatie beschermd. Bovendien heeft het EHRM bepaald dat ook zakelijke correspondentie door art. 8 beschermd wordt.<sup>16</sup>

Art. 8 heeft niet alleen een negatieve dimensie. De staat dient ook een adequaat wettelijk kader te scheppen voor bescherming in horizontale verhoudingen. Ten aanzien van het element 'private life' is dit uitdrukkelijk door het Hof erkend.

Although the object of art. 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference; in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.<sup>17</sup>

Een positieve verplichting kan ook ten aanzien van het 'correspondence'-element worden aangenomen. Doorslaggevend lijkt te zijn of zonder handelend optreden van de staat nog sprake is van een effectieve bescherming.<sup>18</sup>

Door de koppeling van 'correspondence' met 'private life' kan ook e-mail aanspraak maken op bescherming door art. 8 EVRM. Beperkingen moeten voldoen aan de eisen van het tweede lid. Zo moeten ze voorzien zijn bij wet en noodzakelijk in een democratische samenleving ter bescherming van een reeks van doeleinden.

Op de wettelijke basis voor het filteren van e-mail kom ik nog terug. De eis dat een beperking noodzakelijk moet zijn in een democratische samenleving valt uiteen in eisen van subsidiariteit en proportionaliteit. Een beperking moet geschikt en gerechtvaardigd zijn om het gestelde doel te bereiken en niet verder gaan dan strikt noodzakelijk is.

Aan de eisen van art. 8 lid 2 EVRM zou kunnen worden voldaan door middel van een gedragscode voor ISP's waarin een onafhankelijk orgaan, bijvoorbeeld de Registratiekamer, aangewezen wordt als instantie die beoordeelt of het filteren van virus bevattende e-mails noodzakelijk en proportioneel is. In zijn afweging zou dit orgaan onder meer moeten betrekken of het virus een zodanig grote schade aan zal richten dat filteren in de rede ligt. Het filteren mag slechts gedurende een korte tijd gebeuren, bijvoorbeeld totdat adequate anti-virussoftware voorhanden is. Bij minder schadelijke virussen zou een waarschuwing meer voor de hand liggen. Verderop in dit artikel kom ik terug op hoe een concrete uitwerking eruit zou kunnen zien.

---

<sup>15</sup> EHRM 6 september 1978, AA 1979, p. 327-334 (*Klass*). Zie ook Dommering e.a. 2000, p. 103.

<sup>16</sup> EHRM 16 december 1992, NJ 1994, 559 (*Niemitz*), m.nt. E.J. Dommering.

<sup>17</sup> EHRM 7 juli 1989, NJ 1991, 659 (*Gaskin*) m.nt. E.J. Dommering.

<sup>18</sup> Zie ook EHRM 13 juni 1979, NJ 1980, 462 (*Marckx*). Het effectiviteitsbeginsel wordt ook in andere situaties toegepast. Zie bijvoorbeeld *Klass* met betrekking tot het slachtoffervereiste van art. 25 EVRM. Zie verder ook E.A. Alkema, 'The third Party Applicability or "Drittwirkung" of the European Convention on Human Rights', *Protecting Human Rights: The European Dimension* (Wiarda-bundel), Keulen 1988.

## De toekomst van het grondwettelijk communicatiegeheim

Het heeft weinig zin een zorgplicht voor de ISP op basis van de huidige wetgeving te construeren, als in de toekomst het communicatiegeheim een kennisname door de ISP verbiedt. We moeten dus de toekomst van het communicatiegeheim onderzoeken.

### Wetsvoorstel 25443

De techniekafhankelijke formulering van het huidige art. 13 bracht de regering er in 1997 toe, een wijzigingsvoorstel in te dienen.<sup>19</sup> Daarin werd de term ‘vertrouwelijke communicatie’ als techniekafhankelijke norm geïntroduceerd. Dit begrip is afkomstig uit het gelijknamige proefschrift van Hofman.<sup>20</sup> Vertrouwelijke communicatie is volgens Hofman de uitwisseling van berichten, waarbij sprake is van een (geobjectieerde) wil tot vertrouwelijkheid.<sup>21</sup> Buitenstaanders moet het objectief duidelijk zijn dat het om vertrouwelijke communicatie gaat. Hofman stelt als criterium de beslotenheid van de communicatievorm (de fysieke gedaante waarin de communicatie in een bepaald geval is gegoten) of het communicatieproces (feitelijk transport van het bericht) voor.<sup>22</sup> Wanneer eenvoudig van de communicatie kennis kan worden genomen, geniet deze geen bescherming. Volgens de regering betekende dit dat onversleutelde e-mail en ‘gewone’ faxen geen grondwettelijke bescherming genieten.<sup>23</sup> Dit leidde tot vernietigende kritiek.<sup>24</sup> De voornaamste bezwaren vormden de koppeling aan de stand der techniek, doordat bescherming afhangt van de feitelijke beschermingsmogelijkheden, en de verwarring tussen norm en feit, omdat beschermingswaardigheid met het risico van inbreuk verward wordt. Ook de Tweede Kamer was kritisch. Het voorstel werd ingetrokken. Tegelijkertijd werd de commissie ‘Grondrechten in het digitale tijdperk’ ingesteld, die de taak had met techniekafhankelijke wijzigingsvoorstellen te komen.<sup>25</sup> In mei 2000 bracht de commissie Franken haar rapport uit.

### Voorstel commissie ‘Grondrechten in het digitale tijdperk’

Het voorstel van de commissie ‘Grondrechten in het digitale tijdperk’ voor een nieuw artikel 13 Gw luidt:

1. Ieder heeft het recht vertrouwelijk te communiceren.
2. Dit recht kan bij de wet worden beperkt, op last van de rechter, of, indien de beperking in het belang van de nationale veiligheid plaatsvindt, met machtiging van een bij de wet aangewezen minister.
3. Degene van wie dit recht wordt beperkt, wordt van die beperking zo spoedig mogelijk in kennis gesteld. In bij de wet te bepalen gevallen kan in het belang van de strafvordering of in het belang van de nationale veiligheid de kennisgeving worden uitgesteld. Indien het belang van de nationale veiligheid zich blijvend tegen de kennisgeving verzet, kan, in bij de wet te bepalen gevallen, de kennisgeving achterwege worden gelaten.
4. De wet stelt regels ter bescherming van de vertrouwelijkheid van communicatie.

Er valt heel wat op dit voorstel af te dingen. In de eerste plaats komt de commissie weer met ‘vertrouwelijke communicatie’ op de proppen, inclusief zijn parlementaire geschiedenis. Een recht op vertrouwelijke communicatie veronderstelt volgens de commissie een rechtssubject, dat op grond van zijn wil tot geheimhouding een wijze van communiceren verkiest die hem een *redelijke verwachting van vertrouwelijkheid* biedt. Toepassing van het criterium ‘redelijke verwachting van vertrouwelijkheid’

<sup>19</sup> *Kamerstukken II 1997/1998*, 25 443.

<sup>20</sup> *Kamerstukken II 1997/1998*, 25 443, nr. 3.

<sup>21</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, p. 45.

<sup>22</sup> Hofman 1995, p. 47.

<sup>23</sup> Volgens de regering zou gewone e-mail met een Ansichtkaart te vergelijken zijn.

<sup>24</sup> N.A.N.M van Eijk, ‘(G)een recht op vertrouwelijke communicatie: fax en email vogelvrij?’, *NJB* 1997, nr. 33, p. 1554-1555; E.J. Dommering, ‘Geen telefoongeheim op de elektronische snelweg’, *Mediaforum* 1999-10, p. 142-147; A.J. Nieuwenhuis, ‘Vertrouwde en virtuele bescherming’, *NJCM-Bulletin* 4, 1998, p. 423-437; L.F. Asscher, ‘E-mail een Ansichtkaart?’, *Mediaforum* 1997-7/8, p. 103.

<sup>25</sup> *Kamerstukken I 1998/1999*, 25443, nr. 40a.

betekent in feite dat de bescherming die het huidige grondrecht biedt, het risico loopt te verwateren. In beginsel laat dit criterium het immers toe dat bescherming afhangt van willekeurige maatschappelijke belangen. Daarnaast betekent het voorkomen van een dergelijk maatschappelijk belang niet dat het grondrecht beperkt wordt, maar dat het grondrecht niet van toepassing is. In dat geval wordt het potentiële bereik van het grondrecht dus ingeperkt. Hierdoor verliest de grondrechtelijke waarborg aan waarde. In horizontale verhoudingen zal het voorgestelde grondrecht des te eerder aan kracht inboeten. De commissie stelt dat een redelijke verwachting van vertrouwelijkheid aanwezig is op het moment dat voor een ander objectief duidelijk is dat de subjectieve wil van de verzender op vertrouwelijkheid is gericht. Daarvoor stelt de commissie de volgende criteria voor:

1. de aard van het gebruikte kanaal (besloten)
2. adressering
3. de aard van de communicatie (gesloten envelop, encryptie, opschriften als vertrouwelijk of andere uiterlijke kenmerken die op vertrouwelijkheid duiden)<sup>26</sup>

Bij e-mail kan de aard van het gebruikte kanaal reeds beslissend zijn. Wat bedoelt de commissie Franken met kanaal? E-mail kan via satelliet, telefoonlijn, etherfrequentie en kabel overgebracht worden. Deze kanalen zijn niet naar hun aard vertrouwelijk, zoals Asscher terecht stelt.<sup>27</sup> Doelt de commissie misschien op het gebruikte protocol? Dat zou weer een techniekafhankelijke benadering zijn en dat was nu juist niet de bedoeling. Voorts zou dit een uiterst beperkte opvatting van e-mail opleveren, omdat ook van andere protocollen gebruik kan worden gemaakt.<sup>28</sup>

Adressering is in elk geval niet voldoende. Adressering moet gepaard gaan met een van de andere criteria om aan te nemen dat er sprake is van een objectieve wil tot vertrouwelijkheid. De grondwettelijke bescherming van e-mail hangt weer af van een bepaalde mate van beveiliging.

Het verbod om inlichtingen omtrent de inhoud van de communicatie aan derden te verstrekken, zal onder het nieuwe voorstel verwateren. Wanneer het onvermijdelijk is dat van de communicatie wordt kennisgenomen, is per definitie de verwachting van vertrouwelijkheid niet meer redelijk.

De reikwijdte van het grondrecht op vertrouwelijke communicatie is niet beperkt tot de transportfase. Ook directe communicatie, het 'live'-gesprek, wordt onder het voorstel beschermd, voorzover er sprake is van een objectief kenbare wil tot vertrouwelijkheid. Dat is bijvoorbeeld het geval wanneer mensen fluisteren of zich afzonderen. De commissie verliest hier uit het oog dat het communicatiegeheim ziet op *privé-communicatie die aan een transporteur is toevertrouwd*. Het beschermt de vertrouwelijkheid van de dienst. De commissie haalt dus twee concepten door elkaar. Voorts zal een uitbreiding zoals de commissie voorstaat tot een grote overlapping met het algemene privacyrecht leiden.<sup>29</sup> Hierdoor zal het communicatiegeheim verwateren.

Een positief aspect is de opdracht aan de wetgever de bescherming van vertrouwelijke communicatie in horizontale verhoudingen te waarborgen. Het voorgestelde artikel 13 kent dus horizontale werking. Inmiddels heeft het kabinet zijn standpunt bepaald over het voorstel van de commissie 'Grondrechten in het digitale tijdperk'.<sup>30</sup> Het kabinetsstandpunt is grotendeels in overeenstemming met het voorstel, maar wijkt in een belangrijk opzicht daarvan af. Stelde de commissie nog voor de bescherming van de vertrouwelijke communicatie te laten voortduren tot het moment waarop de geadresseerde daadwerkelijk kennis heeft genomen van het bericht, het kabinet wenst de bescherming te beperken tot de transportfase. Dit doet inderdaad meer recht aan de aard van het communicatiegeheim.

Echter, ook in het kabinetsstandpunt is een geadresseerde ansichtkaart niet beschermd. Ten aanzien van het 'live'-gesprek meent het kabinet dat deze alleen onder de reikwijdte van het voorgestelde art. 13 valt, wanneer de inbreuk daarop plaatsvindt met behulp van een technisch hulpmiddel.<sup>31</sup> Over een verbod, inlichtingen te verstrekken, laat het kabinet zich niet uit.

Of in de toekomst e-mail beschermd zal zijn, blijft onduidelijk. Het grotendeels door het kabinet overgenomen voorstel van de commissie 'Grondrechten in het digitale tijdperk' scheidt daaromtrent geen duidelijkheid. De rechtsontwikkeling zal het moeten uitwijzen.

De ILOVEYOU-mail zal mijns inziens geen aanspraak kunnen maken op bescherming door het recht op vertrouwelijke communicatie. De mail is niet vertrouwelijk in de zin van dit nieuwe grondrecht. Als

---

<sup>26</sup> Commissie grondrechten in het digitale tijdperk, Rapport, Den Haag 2000, p. 163.

<sup>27</sup> L.F. Asscher, 'Trojaans hobbelpaard. Een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk', *Mediaforum* 2000-7/8, p. 232.

<sup>28</sup> Als voorbeeld noem ik het HTTP waarvan bij webmail gebruik wordt gemaakt.

<sup>29</sup> Asscher 2000, p. 232.

<sup>30</sup> *Kamerstukken II* 2000/2001, 27460, nr. 1.

<sup>31</sup> *Kamerstukken II* 1999/2000, 27460, nr. 1, p. 24.

eenmaal bekend is dat een virus zichzelf verspreidt en te herkennen is op bijvoorbeeld de in de subject line opgenomen woorden Fw: I love you, dan is per definitie geen sprake meer van een objectief kenbare wil tot vertrouwelijkheid van de afzender. Voor andere virussen die zich op een vergelijkbare wijze verspreiden, zal mutatis mutandis hetzelfde gelden.

### **Andere relevante bepalingen**

Het communicatiegeheim komt ook in enkele lagere nationale regelingen aan bod. De belangrijkste zullen hieronder de revue passeren.

### **18.13 Tw en vergelijkbare technieken**

Art. 18.13 van de Telecommunicatiewet bepaalt dat aanbieders van openbare telecommunicatiediensten bij hun bedrijfsvoering het belang van de bescherming van het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken in acht nemen. Dit artikel verwijst naar een amendement op het voorstel tot wijziging van art. 13 Gw, wetsvoorstel 25443. Zoals boven uiteengezet, is dit nooit aangenomen. Ook in het voorstel van de commissie ‘Grondrechten in het digitale tijdperk’ komt het geheim van daarmee vergelijkbare technieken niet terug. Art. 18.13 Tw heeft dus eigenlijk in deze formulering geen bestaansrecht meer. Het artikel werpt een aantal vragen op. Ten eerste wat zijn daarmee vergelijkbare technieken en ten tweede welk regime is van toepassing. Met art. 18.13 Tw heeft de Kamer buiten twijfel willen stellen, dat ook e-mail onder dezelfde bescherming als brieven, telefoon en telegraaf valt.<sup>32</sup>

Voor e-mail zou het regime van het telefoon –en telegraafgeheim het eerst in aanmerking komen, zoals reeds beargumenteerd.

### **De goede werking van de dienst**

In bepaalde gevallen is kennisname van telecommunicatie toegestaan. In het Wetboek van Strafrecht is art. 139c de centrale af luisterbepaling.

Art. 139c lid 2 sub 3 Wetboek van Strafrecht staat aftappen ten behoeve van de goede werking van een openbaar telecommunicatienetwerk toe. Het onderscheppen van virus bevattende e-mail is een maatregel ten behoeve van de goede werking van openbare telecommunicatienetwerken, met name indien een virus zoveel verkeer genereert dat de servers van ISP's plat liggen. Dit artikel was oorspronkelijk bedoeld om het de aanbieder van een telecommunicatienetwerk mogelijk te maken de lijnwaliteit van telefoonverbindingen te controleren en om na te gaan of bepaalde verbindingen wel tot stand kwamen. Een telecommunicatienetwerk is een ruimer begrip dan telefoonnetwerk. Aangenomen mag derhalve worden dat een controle ter waarborging van de beschikbaarheid van de telecommunicatiedienst door art. 139c wordt toegestaan. In veel gevallen zal een virus slechts de gebruikers treffen en niet de beschikbaarheid van de dienst bedreigen. Een controle op basis van art. 139c lid 2 Sr zal in dat geval niet tot de mogelijkheden behoren. Wordt de beschikbaarheid van de dienst wel bedreigd, dan zal er wel een bevoegdheid tot kennisname bestaan.

Hoewel in de huidige Telecommunicatiewet een dergelijke bevoegdheid niet meer expliciet opgenomen is, kende de vroegere telecommunicatiereggeving wel een vergelijkbare regeling. Zo bepaalde art. 14bis van de Telefoon –en Telegraafwet 1904<sup>33</sup> dat van telefonische of telegrafische berichten kennis mocht worden genomen door daartoe gemachtigd personeel ten behoeve van een goede werking van de dienst. Bij deze bevoegdheid – die met betrekking tot de telegrafie terugging op de artikelen 6 en 8 van de Telegraafwet van 1852 – ging het oorspronkelijk om telegraafverkeer via postkantoren en niet-automatisch telefoonverkeer. De Memorie van Antwoord<sup>34</sup> verklaarde echter dat hoewel controle op het automatisch telefoon –en telexverkeer grotendeels automatisch gebeurt, handmatige observatie daarnaast noodzakelijk blijft om euvels als slechte verstaanbaarheid en ruis, echo en dergelijke in de lijn op te sporen, alsmede om storingen te kunnen verhelpen.

---

<sup>32</sup> Dommering e.a. 2000, p. 75.

<sup>33</sup> Wet van 11 januari 1904 betreffende aanleg, exploitatie en gebruik van telegrafien en telefonen. *Stb.* 1904, nr. 7.

<sup>34</sup> *Kamerstukken II* 1985/1986, 19335, nr. 3, p. 1 en nr. 5, p. 4.

Een bepaling als art. 14bis T&T-wet was ook nog in de Wet op de Telecommunicatievoorzieningen<sup>35</sup> opgenomen, in art. 6. Art. 6 lid 1 bepaalde dat van gegevens die met gebruikmaking van aan de houder van de concessie opgedragen diensten of van vaste verbindingen getransporteerd werden, slechts ten behoeve van een goede uitvoering van de dienst kennis mag worden genomen door het daartoe door de houder van de concessie gemachtigde personeel, belast met de uitvoering van de opgedragen diensten en van de zorg voor vaste verbindingen. Het tweede lid verklaart het eerste lid van overeenkomstige toepassing op de infrastructuurvergunninghouder. De ratio was dat de mogelijkheid moet bestaan de kwaliteit van verbindingen te bewaken. Artikel 6 lid 1 WTV, ingevolge art. 13t WTV van overeenkomstige toepassing op de houders van een vergunning voor mobiele telecommunicatie, was echter niet van toepassing op de aanbieder van toegevoegde waardediensten, waaronder e-mail. In de Telecommunicatiewet vinden we hiervan geen spoor meer terug. Ook art. 18.13 was in eerste instantie niet opgenomen. Dit gebeurde pas na aandringen van de Tweede Kamer. Waarschijnlijk is de uitzondering ten behoeve van de goede werking van de dienst gewoon vergeten. De bepaling in het Wetboek van Strafrecht bleef echter gehandhaafd. Hoewel er plannen zijn om deze bepaling te verwijderen, kan worden aangenomen dat de uitzondering ten behoeve van de goede werking van de dienst nog steeds geldt.<sup>36</sup> Historisch en systematisch is een beperking ten behoeve van de goede werking van de dienst namelijk onlosmakelijk met het communicatiegeheim verbonden. Eigenlijk is deze kennisname geen beperking, maar inherent aan dat geheim. Daarbij verwijs ik ter vergelijking op de Duitse leer van de *inherente beperkingen*.<sup>37</sup> De geschiedenis van telefoon –en telegraaf is zodanig dat de technologische onvolmaaktheid het noodzakelijk maakte dat bij storingen, ruis e.d. kennisgenomen werd van de inhoud van de communicatie. Een verbod inlichtingen aan derden te verschaffen, biedt dan aanvullende bescherming. Nieuwe tijden brengen nieuwe (onvoorziene) problemen, ook ten aanzien van de beschikbaarheid van de dienst. Een beperkte uitleg van ‘de goede werking van de dienst’, in de zin dat de bevoegdheid slechts mag worden gebruikt om de lijnkwaliteit van telefoonverbindingen te controleren of na te gaan of verbindingen tot stand komen, is techniekafhankelijk en doet geen recht aan de soms razendsnelle technische ontwikkelingen op het gebied van de telecommunicatie. Nieuwe media hebben hun eigen vormen van storing. Bij pakketschakeling wordt geen gegarandeerde verbinding opgebouwd zoals bij telefonie. Zou ‘de goede werking van de dienst’ zo uitgelegd moeten worden als hierboven aangegeven, dan is niet goed begrijpelijk dat art. 139c lid 2 Sr spreekt van openbare telecommunicatienetwerken en niet van openbare telefoonnetwerken. Mijns inziens is de bevoegdheid van art. 139c lid 2 Sr dus ook van toepassing op nieuwe telecommunicatiemiddelen. Een interessante vraag die gesteld kan worden, is of van deze bevoegdheid reeds gebruikt kan worden gemaakt in een stadium dat slechts bekend is dat het virus netwerken kan lamleggen. Mijns inziens is dat onder omstandigheden mogelijk. Naar dit middel van preventieve kennisname mag echter niet te snel worden gegrepen. De rechtszekerheid is ermeê gediend, wanneer de Telecommunicatiewet uitdrukkelijk voorziet in een beperking op het communicatiegeheim ten behoeve van de beschikbaarheid van de dienst. Gezien het bovenstaande kan echter worden verdedigd dat in het communicatiegeheim een dergelijke ongeschreven beperking reeds geïncorporeerd is.

### **Voorkomen van schade**

Dat ook het voorkomen van schade bij gebruikers een zelfstandig belang is dat interceptie van vertrouwelijke communicatie kan rechtvaardigen, kan uit art. 2 lid 3 van de Postwet 1988 afgeleid

---

<sup>35</sup> Wet van 26 oktober 1988 houdende regels met betrekking tot voorzieningen voor telecommunicatie, *Stb.* 1988, 520.

<sup>36</sup> Op dit moment ligt namelijk een wetsvoorstel bij de Tweede Kamer waarin art. 139c lid 2 sub 3 wordt geschrapt. Volgens de MvT bij dit voorstel (*Kamerstukken II* 2000/2001, 27576, nr. 3, p. 10) is deze uitzondering niet in overeenstemming met art. 5 j° 14 van de ISDN-richtlijn (Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PbEG* 1998 L 24/1). De ISDN-richtlijn verwijst echter naar de nationale constituties van de lidstaten en het EVRM voor de invulling van de reikwijdte van art. 5 van deze Richtlijn. Nu de nationale constituties de reikwijdte van de bescherming bepalen, is het maar de vraag of art. 139c lid 2 sub 3 Sr in strijd is met de ISDN-richtlijn.

<sup>37</sup> Ook in Nederland zijn ongeschreven beperkingen wel aanvaard sinds de grondwetsherziening van 1983. Zie daarover Verhey 1992, p. 26-29.

worden. Deze bepaling stelt expliciet dat de houder van de concessie het postvervoer weigert, indien dit strijdig is met de wet of gevaar oplevert voor personen of zaken. Het gaat hierbij om een absolute weigeringsplicht. Art. 2 lid 3 Postwet ziet op bombrieven en met ziekten verspreidende virussen besmette post. Wanneer het vermoeden bestaat dat een aan de post ter bezorging toevertrouwd pakket een bom bevat, zal deze bepaling met zich mee brengen dat dit pakket niet bezorgd mag worden. Ook dit moet gezien worden als een beperking van het communicatiegeheim, immers ook een bombrief is een vertrouwelijke boodschap die ter bezorging aan een vervoerder wordt toevertrouwd. Het voorkomen van schade is hier een zodanig groot belang dat een beperking van het onschendbare briefgeheim gerechtvaardigd is. Het gaat hierbij om letsel- en zaakschade, schade die naar zijn aard als ernstiger gewaardeerd wordt dan de vermogens- en immateriële schade die over het algemeen bij computervirussen te verwachten is.

Gezien de ontwikkeling richting informatiemaatschappij en het toenemende belang van informatiediensten en de toenemende afhankelijkheid daarvan is wellicht ook het voorkomen van schade aangericht door elektronische equivalenten van bombrieven wenselijk. Op dit moment bestaat echter op het gebied van telecommunicatie geen analoge bevoegdheid. Ik zie daartoe momenteel ook de noodzaak niet, hoe paradoxaal dat misschien ook mag klinken in het licht van het hiervoor gestelde. Mijns inziens is een kennisname van e-mail pas gerechtvaardigd op het moment dat de beschikbaarheid van de dienst wordt bedreigd. Als daarvoor kennisname is toegestaan, dan kan als accessoir belang de bescherming van de rechten van gebruikers worden meegenomen in de beslissing welke maatregelen moeten worden genomen om verdere verspreiding van computervirussen tegen te gaan.

### **Het communicatiegeheim in Duitsland**

Ter ondersteuning van mijn stelling dat een beperking ten behoeve van de beschikbaarheid van de dienst onlosmakelijk met het communicatiegeheim verbonden is, zal ik het Duitse communicatiegeheim nader onder de loep nemen.

#### **Algemeen**

Vooropgesteld dient te worden dat, indien een wetstekst op meerdere manieren kan worden geïnterpreteerd, de grondwetsconforme uitleg voorrang heeft. Wetgever, bestuur en rechtsprekende organen zijn krachtens art. 1 lid 3 *Grundgesetz* (GG) direct aan de grondwettelijke grondrechten gebonden. Op art. 1 lid 3 GG is ook de horizontale werking van grondrechten gebaseerd. Het *Bundesverfassungsgericht* sprak zich in *Lüth*<sup>38</sup> uit over de mogelijkheid van horizontale werking. Het verwierpt de mogelijkheid van directe horizontale werking. Grondrechten kunnen echter wel indirect werken. Ook moet de staat de waarden van de Grondwet in horizontale verhoudingen vorm geven.<sup>39</sup> Bij een beperking van een grondrecht wordt ingegrepen in het object van het grondrecht. Een ingreep is alleen toegestaan, indien deze berust op een wettelijke grondslag, dat wil zeggen een wet in formele zin. Bij verschillende grondrechten zijn beperkingsclausules met of zonder doelcriteria opgenomen. Deze geven aan in welke gevallen en op welke grondslag het betreffende recht kan worden beperkt. Ook art. 19 GG bevat een aantal waarborgen. Zo mag een wet die een grondrecht beperkt niet slechts voor een individueel geval gelden. Voorts moet een dergelijke wet het desbetreffende grondrecht met artikelnummer noemen. Daarnaast bevat art. 19 lid 2 GG de zogenaamde *Wesengehaltsgarantie*: het te beperken grondrecht mag in geen geval in zijn kern worden aangetast. De jurisprudentie heeft uit deze garantie een aantal nadere voorwaarden afgeleid.<sup>40</sup> De beperking moet voldoen aan de *Grundsatz der Verhältnismäßigkeit* en het *Übermaßverbot*<sup>41</sup>. Dat wil zeggen dat de getroffen maatregel geschikt moet zijn voor het nagestreefde doel, zij moet noodzakelijk zijn en zij mag de getroffen burger niet overmatig belasten.<sup>42</sup> In beginsel moeten beperkingen ook in horizontale verhoudingen aan eisen van proportionaliteit en subsidiariteit voldoen.

Tenslotte noem ik nog de zogenaamde inherente beperkingen. De interpretatie van het object van een grondrecht kan meebrengen dat men – op grond van met name historische of systematische argumenten – van oordeel is dat een bepaald feit of een bepaalde handeling niet beschermd is. Deze benadering is

<sup>38</sup> BVerfG 15 januari 1958, *BVerfGE* 7, 198 (*Lüth-Urteil*).

<sup>39</sup> Zo ook L. Gramlich, 'Art 10 GG nach der zweiten Postreform 1994', *Computer und Recht* 1996-2, p.110.

<sup>40</sup> BVerfG 15 december 1965, *BVerfGE* 19, 343.

<sup>41</sup> T. Maunz & R. Zippelius, *Deutsches Staatsrecht*, München: C.H. Beck Juristischer Verlag 1994, p. 148.

<sup>42</sup> Hofman 1995, p. 304

vooral aanvaard bij grondrechten die geen geschreven beperkingsclausules met of zonder doelcriteria kennen. Of grondrechten die wel een geschreven beperkingsclausule kennen, ook aan inherente beperkingen onderworpen kunnen zijn, is omstreden. Hoewel het *Bundesgerichtshof* en het *Bundesverwaltungsgericht* inherente beperkingen ook wel voor deze grondrechten aanvaard hebben, heeft het constitutionele hof, het *Bundesverfassungsgericht*, deze benadering in zijn *Fangschaltungsentscheidung*<sup>43</sup>, waarover later meer, nadrukkelijk verworpen.

## Art. 10 GG

Net als in Nederland wordt ook in Duitsland het communicatiegeheim tot de privacyrechten gerekend.<sup>44</sup> Daarbij wordt echter ook erkend dat het communicatiegeheim tevens een aspect van de communicatievrijheid beschermt. Het Duitse communicatiegeheim is neergelegd in art. 10 GG. Sinds 1949 luidt art. 10 GG als volgt:

- (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
- (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Het communicatiegeheim bevat drie elementen: een briefgeheim, een postgeheim en een telecommunicatiegeheim. Het tweede lid bevat de beperkingsclausule.

## Postgeheim

Het postgeheim beschermt communicatie die door de post wordt vervoerd. Beschermd zijn niet alleen brieven, maar ook briefkaarten, gedrukte stukken, pakjes en pakketten. De bescherming begint op het moment dat een stuk aan de post wordt toevertrouwd en duurt voort totdat het de invloedssfeer van de post verlaat, meestal door bezorging bij de geadresseerde.<sup>45</sup> Ook stukken die zich op het postkantoor in de postbus van de geadresseerde bevinden, worden door het postgeheim beschermd.<sup>46</sup>

Het geheim heeft twee bestanddelen: enerzijds een verbod tot het verstrekken van inlichtingen omtrent de inhoud van de communicatie en begeleidende omstandigheden, het zogenaamde *Auskunftsverbot*, en anderzijds een verbod tot kennisname, het *Eindringeverbot*. Naar de heersende leer maakt een verbod om stukken (tijdelijk) aan het postverkeer te onttrekken geen deel uit van het postgeheim.<sup>47</sup>

Systematisch is dit juist: het stuiten van communicatie is een inbreuk op de communicatievrijheid, niet op het communicatiegeheim. Hofman signaleert in de Duitse literatuur een verschil van mening over de vraag of de bescherming van het verbod tot kennisname ook betrekking heeft op niet-gesloten stukken. Het woord impliceert mijns inziens een zekere mate van beslotenheid. Dat zou betekenen dat voor overtreding van dit verbod meer vereist is dan een enkele blik op de inhoud van de communicatie. Op briefkaarten zou dit verbod naar zijn aard niet van toepassing kunnen zijn. Dit laat uiteraard de toepassing van het inlichtingenverbod onverlet.

Onduidelijk is of het postgeheim ook van toepassing is op het telecommunicatieverkeer of dat het telecommunicatiegeheim als *lex specialis* dient te worden opgevat. Men neemt wel aan dat het postgeheim alleen op fysiek verkeer van toepassing is, terwijl het telecommunicatiegeheim het non-fysieke berichtenverkeer beschermt.

Op de bescherming van het postgeheim kunnen in ieder geval de afzender en de post zelf aanspraak maken.<sup>48</sup> Of ook de geadresseerde zich op het postgeheim kan beroepen, is omstreden. De

<sup>43</sup> BVerfG 25 maart 1992, NJW 1992, 1875 (*Fangschaltungsentscheidung*).

<sup>44</sup> Zie over de verhouding van het communicatiegeheim tot de algemene privacy BVerfG 31 januari 1973, BVerfGE 34, 238 (*Tonbandbeschluss*).

<sup>45</sup> Hofman 1995, p. 313.

<sup>46</sup> BVerfG 15 maart 1988, BVerfGE 79, 110.

<sup>47</sup> Hofman, p.316-317.

<sup>48</sup> W. Schmitt Glaeser, 'Schutz der Privatsphäre', Rn. 67, in J. Isensee & P. Kirchhof, *Handbuch des Staatsrechts der Bundesrepublik Deutschland*, Deel VI, Heidelberg: C.F. Müller Juristischer Verlag 1992, p. 43-107.

geadresseerde kan in elk geval aanspraak maken op bescherming door het algemene persoonlijkheidsrecht, voorzover hij een zelfstandig privacybelang heeft.

### **Briefgeheim**

Het briefgeheim beschermt het briefverkeer buiten het bereik van de post tegen kennisname door de overheid. Het briefgeheim biedt voor en na de transportfase bescherming. Tijdens de transportfase gaat het in het postgeheim op.<sup>49</sup> Onder brief wordt verstaan *irgendeine an Stelle des mündlichen Verkehrs von Person zu Person erfolgende Mitteilung in beliebiger Schrift –und Vervielfältigungsart*.<sup>50</sup> Het moet in elk geval gaan om een vaste informatiedrager en de inhoud van de communicatie moet als mededeling, als alternatief voor een mondeling gesprek kunnen worden opgevat. Pakjes, pakketten, kranten en dergelijke vallen niet onder het beschermingsbereik van het briefgeheim, omdat deze geen of niet alleen mededelingen in de zin van bovengenoemde definitie omvatten.

Of naast de hiervoor genoemde voorwaarden brieven nog gesloten moeten zijn om aanspraak op bescherming te kunnen maken, is omstreden. Het constitutionele hof heeft zich nog niet over deze vraag uitgesproken. Het *Bundesgerichtshof* en het *Bundesverwaltungsgericht* hebben dat echter wel gedaan. Zij stelden beide de eis van geslotenheid. Zo overwoog het *Bundesgerichtshof* in 1990 dat, hoewel in staat te zijn met anderen te communiceren voor de mens een groot belang is en daarbij indirecte communicatie een steeds belangrijker rol speelt, dit bereik tegelijkertijd zeer kwetsbaar is. Reeds de schijn van een inbreuk op de vertrouwelijkheid schaadt de onbevangenheid van de communicatie. Een buitenstaander dient hier in elk geval rekening mee te houden wanneer de wens om anderen van de communicatie uit te sluiten, waarneembaar tot uitdrukking komt en voorzorgsmaatregelen tegen een toevallige kennisname door een derde getroffen zijn. Dat is het geval bij gesloten poststukken. In het dichtplakken van de envelop wordt de wens tot vertrouwelijkheid zichtbaar uitgedrukt.<sup>51</sup>

De eis van geslotenheid betekent dat het briefgeheim slechts een verbod tot kennisname van de inhoud inhoudt. Het verbod inlichtingen aan derden te verstrekken, is beperkt tot de nadere omstandigheden van het briefverkeer, onder de voorwaarde dat het om gesloten brieven gaat.<sup>52</sup> Ten aanzien van briefverkeer dat door de Duitse PTT wordt verzorgd, gaat het briefgeheim in het postgeheim op. Dan blijft ook de ongesloten 'brief' dus maximaal beschermd. In gevallen dat het briefverkeer door een andere instantie verzorgd wordt, geniet de ongesloten 'brief' geen bescherming van post, -of briefgeheim. In dat geval zal het algemene privacyrecht een aanvullende functie vervullen.

### **Telecommunicatiegeheim**

Toen post en telecommunicatie uitsluitend door de Duitse PTT werden verzorgd, was omstreden of het telecommunicatiegeheim een zelfstandige positie naast het postgeheim had. Zo werd wel aangenomen dat in de transportfase het telecommunicatiegeheim in het postgeheim opging.<sup>53</sup> Slechts buiten de transportfase of wanneer de telecommunicatie door een ander overheidsorgaan dan de PTT werd verzorgd, had het een zelfstandige functie. Door privatisering en liberalisering heeft het telecommunicatiegeheim een zelfstandige plaats naast het postgeheim ingenomen.

Het telecommunicatiegeheim omvat enerzijds een verbod tot kennisname van door middel van telecommunicatie overgebrachte boodschappen, voorzover de kennisname niet functioneel is voor de verzorging van de dienst. Anderzijds is het verboden aan derden inlichtingen te verstrekken over begeleidende omstandigheden, de verkeersgegevens.

Het lijkt erop dat naast de afzender ook de ontvanger aanspraak op bescherming van het telecommunicatiegeheim kan maken. In zijn *Fangschaltungsentscheidung*<sup>54</sup> overwoog de constitutionele rechter dat, ook al geldt het telecommunicatiegeheim niet tussen de gespreksdeelnemers onderling, dit

<sup>49</sup> W. Schmitt Glaeser, 'Schutz der Privatsphäre', Rn. 62.

<sup>50</sup> B. Pieroth & B. Schlink, *Grundrechte. Staatsrecht II*, Heidelberg: C.F. Müller Juristischer Verlag 1985, p. 197; Hofman 1995, p. 317.

<sup>51</sup> BGH 20 februari 1990, *JR* 1991, 67.

<sup>52</sup> Of verkeersgegevens ook onder het briefgeheim vallen, is omstreden. Ten aanzien van *Post –en Fernmeldegeheimnis* heeft het *Bundesverfassungsgericht* expliciet aanvaard dat deze ook verkeersgegevens omvatten. Voor het *Postgeheimnis* verwijs ik naar BVerfG 20 juni 1984, *BVerfGE* 67, 157 en voor het *Fernmeldegeheimnis* naar BVerfG 25 maart 1992, *NJW* 1992, 1875 (*Fangschaltungsentscheidung*).

<sup>53</sup> Schmitt Glaeser Rn. 64;

<sup>54</sup> BVerfG 25 maart 1992, *NJW* 1992, 1875.

niet betekent dat geen sprake is van inbreuk op dat geheim, wanneer de PTT na toestemming van één van de gespreksdeelnemers kennisneemt van de inhoud van een gesprek.

In een telefoongesprek zijn de posities niet duidelijk te onderscheiden. Toch zou bovenstaande overweging van het constitutionele hof een grotere betekenis kunnen hebben. Hofman wijst bij zijn bespreking van het postgeheim namelijk op een arrest van het *Bundesgerichtshof* uit 1990, waarin het hof een doorslaggevende betekenis toekent aan het feit dat een postrechtelijke gebruikersverhouding alleen tussen afzender en post bestaat.<sup>55</sup> Zou ook bij een telefoongesprek de contractuele verhouding doorslaggevend zijn, dan kan alleen degene die voor het gesprek betaalt, aanspraak maken op bescherming door het telecommunicatiegeheim.

Het telecommunicatiegeheim beschermt de vertrouwelijkheid van alle door middel van telecommunicatie overgedragen boodschappen. Het is niet beperkt tot traditionele telecommunicatiemiddelen, zoals telefoon en telegraaf, maar omvat ook nieuwe technologieën. In die zin is het een dynamisch en techniekonafhankelijk grondrecht.

Of communicatie besloten moet zijn, om aanspraak op bescherming te maken, is de vraag. Gramlich stelt dat e-mail versleuteld moet zijn, om door het telecommunicatiegeheim beschermd te worden, want *was für den Brief der Verschluss, wäre für TK-Dienstleistungen die Verschlüsselung*.<sup>56</sup> Ruiz wijst er echter op dat, hoewel een provider toegang tot de inhoud van de boodschappen kan hebben en mogelijk zelfs een kopie op zijn server heeft gemaakt, e-mail niet in open zicht van de provider ligt en derhalve onder het beschermingsbereik van art. 10 GG valt.<sup>57</sup> Gezien de ontwikkeling van het telecommunicatiegeheim lijkt Ruiz' benadering beter in de geest van art. 10 GG te passen.

Bij de hierboven geschetste ontwikkeling past een verbod om inlichtingen aan derden te verschaffen dat wanneer het onvermijdelijk is, kennis van de inhoud van de vervoerde communicatie te nemen, het verbod tot kennisname aanvult. Bij het postgeheim zijn beide verboden met betrekking tot de inhoud erkend en is de vertrouwelijkheid van de dienst maximaal gegarandeerd.

### **Beperkingsmogelijkheden**

De eerste zin van art. 10 lid 2 GG bepaalt dat de grondrechten van het eerste lid slechts bij wet mogen worden beperkt. Concreet komt dit erop neer dat beperkingen altijd een grondslag in een wet in formele zin moeten hebben. Wanneer de beperking één van de doelen neergelegd in de tweede zin van het tweede lid dient, dan kan de wet bepalen dat notificatie niet vereist is en mag in plaats van de rechter een door de volksvertegenwoordiging aangewezen orgaan de rechtmatigheid van de beperking controleren. De wet bedoeld in de tweede zin van het tweede lid is het zogenaamde *G-10 Gesetz*.<sup>58</sup> Aangezien deze wet hier niet van belang is, volsta ik met deze constatering.

Geldt het vereiste dat beperkingen terug te voeren moeten zijn op een wet in formele zin nu absoluut, zijn inherente beperkingen uitgesloten? Voor 1992 was de heersende leer dat inherente beperkingen mogelijk waren, met name ten aanzien van de zogenaamde *betriebsbedingte Maßnahmen*.<sup>59</sup> Dat gold in een uitspraak uit 1984 omschrijft het *Bundesverwaltungsgericht* deze als volgt:

Betriebsbedingt und somit keine verbotenen Eingriffe in das Postgeheimnis sind Maßnahmen, ohne die eine sachgerechte Abwicklung des Postdienstes nicht möglich ist, die insbesondere die Beförderungsinteressen der Betroffenen nicht durchkreuzen, sondern sie gerade wahrnehmen.<sup>60</sup>

Hoewel deze beperking op het eerste gezicht op de boven door mij gesignaleerde beperking ten behoeve van de goede werking van de dienst lijkt, zijn *betriebsbedingte Maßnahmen* veel ruimer. Het *Bundesverwaltungsgericht* heeft als zulke maatregelen onder meer aangemerkt de bestelling op een ander adres bij de afwezigheid van de geadresseerde, het openen van onbestelbare stukken en het vaststellen van de inhoud van beschadigde stukken. Zelfs heeft het in *Patentex*<sup>61</sup> het vaststellen van het

---

<sup>55</sup> Hofman 1995, p. 316.

<sup>56</sup> Gramlich 1996, p. 112.

<sup>57</sup> Ruiz 1997, p. 156.

<sup>58</sup> *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* van 13 augustus 1968, *BGBL.* I 949.

<sup>59</sup> Voor een overzicht zie Hofman 1995, p. 328-329.

<sup>60</sup> BVerwG 25 april 1984, *NJW* 1984, 2111.

<sup>61</sup> BVerwG 27 maart 1958, *BVerwGE* 6, 299 (*Patentex*).

feit of een niet-gesloten stuk aanstootgevende inhoud bevat, als noodzakelijk in het kader van de bedrijfsvoering aangemerkt.

In zijn *Fangschaltungsentscheidung*<sup>62</sup> heeft de constitutionele rechter echter de toelaatbaarheid van inherente beperkingen ten aanzien van art. 10 GG expliciet afgewezen. Het bepaalde daarin dat de potentiële bescherming van een grondrecht niet mag afhangen van een bij de overheid bestaande behoefte of noodzaak tot beperking.

E-mail geniet in Duitsland door de dynamische interpretatie van het telecommunicatiegeheim grondwettelijke bescherming. Beperkingen op het communicatiegeheim moeten herleidbaar zijn tot een wet in formele zin. In een concreet, individueel geval kan een beperking op het communicatiegeheim toegestaan zijn wanneer andere grondrechtelijke belangen dit rechtvaardigen. Dan hoeft er geen wettelijke basis voor de beperking te zijn. Overigens is ook geen wettelijke basis vereist, wanneer de communicatiepartners hun toestemming voor de beperkende handeling geven.

Voor het antwoord op de vraag of de ISP toch kennis mag nemen van e-mail ten behoeve van de goede werking van de dienst of om schade te voorkomen, zal de toepasselijke Duitse wetgeving moeten worden onderzocht.

### Het telecommunicatiegeheim in de Duitse Telecommunicatiewet

De Nederlandse Telecommunicatiewet voorziet niet in een beperking op het communicatiegeheim ten behoeve van de goede werking van de dienst of het telecommunicatienetwerk. Historisch en systematisch vormt een dergelijke beperking echter een noodzakelijk en vanzelfsprekend complement op het communicatiegeheim. Aangenomen kan derhalve worden dat deze beperking zich in Nederland als inherente beperking op het communicatiegeheim doet gelden. In Duitsland is de situatie anders. Uit de eerder besproken *Fangschaltungsentscheidung* van het constitutionele hof volgt dat inherente beperkingen op het brief-, post –en telecommunicatiegeheim niet toegestaan zijn. Beperkingen moeten dus een expliciete grondslag in een wet in formele zin hebben. Aangezien e-mail door het telecommunicatiegeheim beschermd wordt, moet onderzocht worden of de Duitse telecommunicatiereggeving voorziet in een beperking, die een kennisname ten behoeve van de goede werking van de dienst toestaat.

Voor bovengenoemde uitspraak ging de Duitse wetgever er klaarblijkelijk van uit dat *betriebsbedingte Maßnahmen* als inherente beperkingen fungeerden, dus voorzag de toenmalige telecommunicatiereggeving niet in een formeel-wettelijke grondslag. In 1995 werd in het *Gesetz über Fernmeldeanlagen*<sup>63</sup> (FAG), de directe voorganger van het huidige Telecommunicatiewet (*Telekommunikationsgesetz* -TKG), een expliciete grondslag voor *betriebsbedingte Maßnahmen* opgenomen.

Het derde lid van art. 10 FAG gaf aanbieders van openbare telecommunicatiediensten de bevoegdheid kennis te nemen van de communicatie, wanneer dit ten behoeve van de goede werking van de dienst nodig is. Daarbij gold een notificatieplicht.

In hoofdstuk 11 TKG<sup>64</sup> vinden we de tegenwoordig geldende regeling. Art. 85 TKG vormt de centrale bepaling en luidt, voorzover hier van belang, als volgt:

1. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre nähere Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
2. Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig, Telekommunikationsdienste erbringt oder daran mitwirkt. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
3. Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu erschaffen. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit diese Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

[...]

<sup>62</sup> BVerfG 25 maart 1992, NJW 1992, 1875 (*Fangschaltungsentscheidung*).

<sup>63</sup> *Gesetz über Fernmeldeanlagen vom 14. Januar 1928*, RGBl. I, p. 8.

<sup>64</sup> *Telekommunikationsgesetz vom 25. Juli 1996*, BGBl. I, p. 1120.

De wetgever heeft de directe gebondenheid van particuliere aanbieders van telecommunicatiediensten aan het telecommunicatiegeheim verzekerd door letterlijk het grondwettelijke geheim over te nemen. Gebonden aan het communicatiegeheim en de andere bepalingen van het elfde deel van het TKG is een ieder die in het kader van een beroep of bedrijf telecommunicatiediensten aanbiedt. Daarbij is irrelevant of het aanbod openbaar of gericht op het maken van winst is.<sup>65</sup>

Het begrip telecommunicatie is niet beperkt tot spraaktelefonie, maar omvat boodschappen van welke aard dan ook die door middel van telecommunicatie-inrichtingen verzonden, overgedragen of ontvangen kunnen worden.<sup>66</sup> Een telecommunicatie-inrichting zijn technische inrichtingen of systemen die als berichten identificeerbare elektromagnetische of optische signalen kunnen verzenden, sturen of controleren. Een telecommunicatie-inrichting is dus wat anders dan een telecommunicatienetwerk. Immers, dat is het gekoppelde geheel van inrichtingen die bovengenoemde handelingen kunnen verrichten. Het technische proces van het ontvangen en doorsturen van e-mailberichten via Internet in de vorm van datapakketjes is in elk geval voorzover het de technische afwikkeling op het niveau van transportprotocollen betreft, telecommunicatie in de zin van de Duitse Telecommunicatiewet. In beginsel geldt een verbod tot kennisname, aangevuld met een verbod, aan derden inlichtingen over het communicatieproces te verschaffen. Als kennisname van de inhoud onvermijdelijk is, treedt volgens § 85 lid 3 TKG het verbod tot kennisname terzijde en levert een verbod inlichtingen te verstrekken aanvullende bescherming. Dit is opvallend, gezien de bij het grondwettelijke telecommunicatiegeheim gesignaleerde discussie over de eis van beslotenheid. Het geheim van § 85 TKG beschermt besloten en niet-besloten communicatievormen. Vooropgesteld dat voor de interpretatie van grondrechten wettelijke bepalingen niet beslissend mogen zijn, is dit mijns inziens toch een duidelijke aanwijzing dat het telecommunicatiegeheim zich steeds meer ontwikkelt tot een grondrecht dat de vertrouwelijkheid van de dienst beschermt.

De bescherming van het telecommunicatiegeheim wordt nader geconcretiseerd door uitzonderingsbepalingen. In eerste instantie zijn dat de uitzonderingen die in de Telecommunicatiewet opgenomen zijn, meer in het bijzonder in § 89-92 TKG. Daarbij is in het kader van dit onderzoek § 89 TKG het meest van belang.

Dit artikel bevat gedetailleerde voorschriften met betrekking tot gegevens die over het communicatieproces door de dienstverlener vergaard worden. Enerzijds bevat het artikel een machtiging voor een verordening waarin bepaalde in het artikel genoemde zaken nader geregeld moeten worden, anderzijds ook zelfstandige bepalingen die onafhankelijk van de uit te vaardigen verordening reeds gelden.<sup>67</sup> Art. 89 lid 5 TKG bepaalt dat de exploitant van een telecommunicatie-inrichting kennis mag nemen van bestaande verbindingen om verkeer om te leiden of storingen in het netwerk tegen te gaan. Dit mag niet verder gaan dan in het kader van de bedrijfsvoering noodzakelijk is. Maakt de exploitant gebruik van deze bevoegdheid, dan moet dat aan de gespreksdeelnemers kenbaar gemaakt worden. In § 85 TKG is een uitzondering op het verbod tot kennisname opgenomen, voor het geval dat kennisname onvermijdelijk is om de dienst überhaupt te leveren. Hieronder wordt blijkens § 89 lid 5 TG ook een kennisname ten behoeve van de goede werking van de dienst begrepen. Een kennisname om storingen te voorkomen of te verhelpen, dient de beschikbaarheid van het communicatiemiddel. Maatregelen in dienst van de beschikbaarheid van een communicatiemiddel zijn eigenlijk een logische aanvulling op het communicatiegeheim. Zonder dienst valt er niets geheim te houden. Niet alleen is in het TKG een bevoegdheid tot kennisname opgenomen, deze bevoegdheid wordt in § 87 lid 1 sub 3 TKG aangevuld met een plicht, passende technische en organisatorische maatregelen te nemen om storingen die de werking van telecommunicatienetwerken aanzienlijk beperken, op te heffen. Deze plicht staat naast de in het eerste lid van hetzelfde artikel opgenomen plicht, technische en organisatorische maatregelen te nemen om het communicatiegeheim en persoonsgegevens te beschermen. De plicht geldt echter alleen voor degene die een telecommunicatie-inrichting exploiteert. Aangenomen kan worden dat bij ernstige storingen, de aanbieder niet alleen de bevoegdheid, maar zelfs de plicht heeft om kennis van de inhoud te nemen, zodat de oorzaak van de storing vastgesteld en deze vervolgens opgeheven kan worden.

---

<sup>65</sup> U. Wuermeling & S. Felixberger, 'Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz', *Computer und Recht* 1997-4, p.231.

<sup>66</sup> § 3 lid 16 TKG.

<sup>67</sup> De verordening bedoeld in art. 89 TKG is de opvolger van de huidige *Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen* (*Telekommunikationsdienstunternehmen-Datenschutz-Verordnung* - TDSV) die van net voor het TKG stamt. Op 20 november 2000 heeft de *Bundesrat* de nieuwe TDSV aangenomen.

De Duitse OPTA (RegPT) is met het toezicht belast. In § 91 TKG zijn de bevoegdheden van de toezichthouder op de telecommunicatiemarkt ten aanzien van dit deel vastgelegd. De RegPT kan aanwijzingen geven of andere geschikte maatregelen treffen, om naleving te verzekeren. Uit dien hoofde kan de RegPT inlichtingen vorderen, gebouwen betreden en onder omstandigheden bedrijven stilleggen. Ook mag de RegPT uit hoofde van zijn toezichthoudende taak ten aanzien van dit deel van het TKG kennis van de inhoud van privé-communicatie nemen. Aan het citeergebod van art. 19 GG wordt in § 91 lid 5 TKG voldaan. Uiteraard moeten bij de uitoefening van de bevoegdheid de beginselen van proportionaliteit en subsidiariteit in acht worden genomen.

### **Filteren in de praktijk**

Hoe zou gezien het bovenstaande filteren er in de praktijk kunnen uitzien? Voordat ik daarop inga, wil ik nogmaals vooropstellen dat het filteren van virus bevattende e-mail slechts een optie is op het moment dat de beschikbaarheid van de e-maildienst bedreigd wordt. Is dit niet het geval, dan heeft de ISP geen bevoegdheid om kennis te nemen van de inhoud van boodschappen.

De beschikbaarheid van de dienst wordt bedreigd, wanneer een virus zoveel e-mailverkeer genereert dat e-mailservers platliggen. Op het moment dat e-mailservers platliggen, mag de ISP kennis nemen van de inhoud van e-mail. Het kan echter gewenst zijn al proactief op te treden.

Het communicatiegeheim sluit een routinematige controle van verbindingen niet uit, wanneer dit noodzakelijk is om de kwaliteit van die verbindingen te waarborgen. Ten aanzien van e-mail kan deze bevoegdheid analoog toegepast worden. In de praktijk betekent dit dat de ISP op het moment dat hij afweet van het bestaan van een virus dat servers kan platleggen, hij in beginsel zijn servers op de aanwezigheid van dat virus mag controleren. Naarmate daarbij de voorzienbare schade groter wordt, zal des te eerder een plicht ontstaan van deze bevoegdheid gebruik te maken.

Deze maatregel moet echter gezien de eisen van art. 8 EVRM proportioneel zijn. Bij virussen die geringe schade aanrichten bij gebruikers en dienstverleners, ligt een inhoudelijke controle niet in de rede. Een ISP kan niet de plicht worden opgelegd ten allen tijde elke e-mail op virussen te controleren. Een dergelijke algemene verplichting wordt verboden door art. 15 van de E-commercerichtlijn.<sup>68</sup> Bovendien zou een dergelijke vergaande controle over het algemeen niet voldoen aan eisen van proportionaliteit en subsidiariteit.

Of een virus een dermate grote schade kan aanrichten, dat filteren noodzakelijk is ter bescherming van de rechten van anderen, kan een ISP niet altijd beoordelen. Dit alleen al omdat er ook valse viruswaarschuwingen, *hoaxes*, in omloop zijn.<sup>69</sup> Eventuele maatregelen die de ISP neemt, moeten berusten op juiste en volledige informatie. Op basis van die informatie kan de dreiging worden beoordeeld. Wanneer de ISP een virusmelding krijgt, zal hij de betrouwbaarheid van de informatie moeten kunnen verifiëren. In dat verband verdient het aanbeveling dat de ISP's gezamenlijk een verdragscode opstellen. In deze gedragscode kan een nationaal, liever nog internationaal, onafhankelijk expertisecentrum aangewezen worden dat in staat is de gevaren van een virus adequaat en snel te beoordelen. Wellicht is hiervoor de Registratiekamer of OPTA de geschikte instantie.<sup>70</sup>

Als deze instantie een virus als zodanig gevaarlijk kwalificeert dat filteren de enige manier is om de dreiging te neutraliseren, zouden de ISP's gezamenlijk tot filteren van de e-mails op hun servers over kunnen gaan. Het filteren zou dan net zolang moeten voortduren, totdat anti-virussoftware de gebruiker kan beschermen en de gebruiker kennis heeft verkregen van het bestaan van het virus en hij weet welke beschermingsmogelijkheden er zijn. In de praktijk moet daarbij waarschijnlijk gedacht aan een periode van enkele dagen.

Wanneer de instantie het filteren noodzakelijk acht, zal de ISP in beginsel de plicht hebben het virus van zijn servers te verwijderen, tenzij dat redelijkerwijs niet van hem gevraagd kan worden, omdat dat technisch en/ of organisatorisch ondoenlijk is.

Richt een virus minder grote schade aan, of verspreidt het zich minder snel, dan kan wellicht volstaan worden met het verzenden van een viruswaarschuwing aan de individuele afnemers.

---

<sup>68</sup> Richtlijn 2000/31/EG van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* 2000 L 178/1

<sup>69</sup> Als voorbeeld kan het *sulfnbk.exe*-virus worden genoemd. Zie daarvoor <http://www.netkwesties.nl/editie15/artikel3.html>

<sup>70</sup> In dat verband kan ook gewezen worden op het recente initiatief van de Belgische toezichthouder op de telecommarkt. Het BIPT heeft op haar website ([www.bipt.be](http://www.bipt.be)) een lijst van gevaarlijke virussen staan die telkens geupdate wordt.

Dat de beoordeling van de virusdreiging in handen wordt gelegd bij een centrale instantie biedt een aantal voordelen. Ten eerste is daardoor een gecoördineerde en dus effectievere aanpak mogelijk. Bovendien wordt de individuele ISP verlost van de tijdrovende en kostbare taak elke virusmelding te verifiëren. Tenslotte wordt de privacy van gebruikers op deze manier beter gewaarborgd. De kans op willekeurige inbreuken op het communicatiegeheim wordt namelijk kleiner.

## **Conclusies en aanbevelingen**

Door de techniekafhankelijke formulering van art.13 Gw is e-mail niet zomaar onder één van de daar genoemde geheimen te brengen. E-mail lijkt door de pakketgeschakelde transporttechniek het meest op de telegraaf. Van telefoon –en telegraafgeheim zou dus in eerste instantie de meeste bescherming te verwachten zijn. Omdat de mate van grondwettelijke bescherming afhankelijk is van de gebruikte techniek, is het, nu e-mail niet expliciet genoemd wordt, uiterst onwaarschijnlijk dat e-mail in de Nederlandse grondwet bescherming vindt.

Of dit in de toekomst anders is, is vooralsnog niet duidelijk. Wetsvoorstel 25443 eiste een bepaalde mate van beveiliging voor grondwettelijke bescherming. Gewone e-mail zou niet afdoende beveiligd zijn. Het voorstel van de commissie ‘Grondrechten in het digitale tijdperk’ overtuigt niet echt. Ook het daarop volgende kabinetsstandpunt neemt niet alle onduidelijkheid weg.

Zou e-mail wel bescherming genieten, dan geldt nog niet in alle gevallen een verbod tot kennisname. Kennisname kan om technische redenen noodzakelijk blijken te zijn. Dan heeft het communicatiegeheim de strekking dat de informatie niet verder verspreid wordt. Een absoluut verbod tot kennisname zou een goede werking van de dienst onmogelijk maken.

De bevoegdheid tot kennisname ten behoeve van de goede werking van de dienst is nu alleen in art. 139c Sr te vinden. In de Telecommunicatiewet wordt met geen woord over deze bevoegdheid gerept. Waarom is niet geheel duidelijk. De rechtszekerheid zou ermee gediend zijn, wanneer wederom een dergelijke bevoegdheid in de Telecommunicatiewet wordt opgenomen. Ik stel dan ook voor een dergelijke bevoegdheid bij de eerstvolgende wetswijziging op te nemen. Deze zou er als volgt uit kunnen zien.

Een aanbieder van telecommunicatiediensten –en/ of netwerken mag kennis nemen van de inhoud van de door hem getransporteerde communicatie, voorzover dit noodzakelijk is om de beschikbaarheid van de dienst te waarborgen. Indien hij gebruik maakt van deze bevoegdheid, is het hem verboden de aldus verkregen kennis omtrent de inhoud aan derden te verstrekken, behoudens voorzover de wet hem daartoe verplicht.

Voor het Duitse recht geldt eigenlijk het omgekeerde verhaal. In Duitsland wordt e-mail beschermd door het telecommunicatiegeheim van art. 10 GG.

Het postgeheim is de meest centrale bepaling van art. 10 GG. Het beschermt besloten en niet-besloten communicatie. Dat is mogelijk, doordat het ten aanzien van de inhoud twee aspecten kent, te weten een verbod tot kennisname en een verbod inlichtingen aan derden te verschaffen. Het beschermt alleen tijdens de transportfase, wat erop neerkomt dat de bescherming ophoudt op het moment dat het stuk de invloedssfeer van de post verlaat.

Brief –en postgeheim beschermen alleen communicatie op vaste informatiedragers. Het telecommunicatiegeheim beschermt daarentegen het non-fysieke berichtenverkeer. Ook het telecommunicatiegeheim kan in een inlichtingenverbod en een verbod tot kennisname worden onderscheiden. Het is een dynamisch grondrecht dat op alle vormen van telecommunicatie, waaronder e-mail, van toepassing is.

Een bevoegdheid tot kennisname ten behoeve van de goede werking van de dienst maakt in Duitsland geen deel uit van het telecommunicatiegeheim. Beperkingen op art. 10 GG moeten dus voldoen aan de eisen van art. 10 lid 2.

Aangezien een bevoegdheid tot kennisname in bepaalde gevallen toch noodzakelijk werd geacht, heeft de Duitse wetgever deze expliciet in de Duitse Telecommunicatiewet opgenomen.

De ISP heeft een dus bevoegdheid tot kennisname, wanneer de beschikbaarheid van de dienst bedreigd wordt. In dat geval zou hij e-mails met virussen in beginsel kunnen filteren. Daargelaten of hij civielrechtelijk aansprakelijk gesteld kan worden, wanneer hij dit nalaat, wil ik toch benadrukken dat er omstandigheden kunnen rijzen waarin filteren uitermate wenselijk is. Ik stel dan ook voor dat de ISP's gezamenlijk een gedragscode opstellen waarin een onafhankelijk virusmeldpunt wordt opgericht. Een onafhankelijk orgaan, bijvoorbeeld de Registratiekamer, zou dan moeten beoordelen of maatregelen

genomen moeten worden tegen de verdere verspreiding van computervirussen. Dit orgaan zou onder meer het volgende in zijn oordeel kunnen betrekken:

- De snelheid van verspreiding
- De potentiële bedreiging van de beschikbaarheid van de dienst
- De beschikbaarheid van adequate anti-virussoftware
- De verwachte omvang van de schade bij gebruikers

Wellicht kan volstaan worden met het sturen van een waarschuwing per e-mail naar de afnemers van de ISP's. Is dat niet het geval, dan zou het orgaan de bevoegdheid moeten hebben de ISP's te verplichten gedurende een korte tijd te filteren op basis van objectieve kenmerken van de gevaarlijke e-mail.