

# Stop bugging me!

## Wilfred Steenbruggen

*Computervirussen vormen een steeds grotere bedreiging voor de informatiemaatschappij. Via het internet kunnen virussen in korte tijd wereldwijd enorme schade aanrichten. De overheid vindt vooralsnog dat gebruikers dit zelf maar moeten oplossen. De digitale zelfredzaamheid van gebruikers schiet echter te vaak tekort. Ligt hier een taak voor de Internet Service Providers?*

Melissa, Anna Kournikova, ILOVEYOU, deze namen klinken vrij onschuldig, maar de schijn bedriegt. Alledrie zijn het computervirussen die de afgelopen jaren wereldwijd voor miljarden gulden schade hebben aangericht. Nu we dichterbij de informatiemaatschappij komen, beginnen computervirussen een steeds grotere bedreiging te vormen. Daarvoor zijn een aantal redenen. Computervirussen hebben door de verschijnselen convergentie<sup>1</sup> en internationalisering van telecommunicatienetwerken een steeds groter bereik.<sup>2</sup> Ook is het economisch goed informatie belangrijk in waarde gestegen, waardoor tevens de potentiële schade toeneemt. De 'interconnectedness' van netwerken maakt het mogelijk dat virussen zich razendsnel verspreiden. Bovendien zijn virussen relatief makkelijk te produceren.

Alle genoemde virussen konden zichzelf reproducen en verspreiden. Het ILOVEYOU-virus verspreidde zich bijvoorbeeld als volgt. Een gebruiker krijgt een e-mail met als *subject* 'ILOVEYOU'. Aan die e-mail bevindt zich een attachment met de titel loveletter.txt. Als de gebruiker de attachment opent, begint het virus zijn werk. Het downloadt een schadelijk programma van een website, dat vervolgens een aantal bestanden op de harde schijf wist. Daarna stuurt het virus zichzelf door naar alle adressen in het adresboek van het e-mailprogramma. De geadresseerde denkt dat het bericht van een bekende komt, opent de attachment en het spel begint van voren af aan. Naast schade bij gebruikers veroorzaakte het ILOVEYOU-virus ook een uitval van e-mailservers. Het genereerde zoveel verkeer dat servers van internet providers dit niet aankonden. De beschikbaarheid van het communicatiemiddel e-mail kwam dus in het gedrang.

Tot nu toe propageert de overheid een eigen verantwoordelijkheid van de eindgebruiker ten opzichte van computervirussen. Uit de ILOVEYOU-case valt echter af te leiden dat deze benadering tekortschiet. De digitale zelfredzaamheid van gebruikers laat te wensen over. Voor dergelijke netwerkproblemen dient een netwerkoplossing gevonden te worden. Een oplossing zou kunnen zijn Internet Service Providers onder omstandigheden een zorgplicht op te leggen om verspreiding van e-mails met virussen te voorkomen.

Verspreiding van virussen kan namelijk voor een groot deel verhinderd worden, wanneer Internet Service Providers e-mails die zich in de mailboxen op hun servers bevinden, filteren. Het filteren zou op basis van specifieke tekstenmerken kunnen gebeuren. Een andere efficiënte maatregel zou kunnen zijn afnemers per e-mail voor een specifiek virus te waarschuwen. Hieronder zal ik proberen uit te werken hoe dit in de praktijk zou kunnen functioneren. Daarvoor zal ik allereerst het relevante juridische kader schetsen.

### Aanbieder van e-mail

Een internet provider is niet zonder meer aansprakelijk voor de inhoud van de via zijn systemen getransporteerde informatie. Aansprakelijkheid voor de inhoud van informatie op het internet is verbonden met de mogelijkheid op die inhoud invloed en controle uit te oefenen. Afhankelijk van de rol die een tussenpersoon in het communicatieproces inneemt, kan die mogelijkheid verschillen. Zo kan een *access provider* niet aansprakelijk zijn voor de inhoud van door hem vervoerde informatie, aangezien hij alleen toegang verschaft en niets aan de informatie verandert.<sup>3</sup> De dienst die hij verleent, bestaat uit het verschaffen van toegang en niet uit het beschikbaar stellen van

opslagcapaciteit. Opslag van informatie vindt alleen plaats, voorzover en zo lang dat voor transportdoeleinden noodzakelijk is. Theoretisch zou hij de communicatie op het gebruikte protocol kunnen filteren, maar niet op de inhoud van een individuele boodschap.

Een *service provider* daarentegen heeft wel de mogelijkheid de inhoud van de via zijn systemen getransporteerde informatie te controleren en beïnvloeden. Omdat hij voor onbepaalde tijd servercapaciteit aan zijn afnemers ter beschikking stelt, kan hij makkelijker de rechtmatigheid van de informatie controleren. Daarom wordt aangenomen dat hij aansprakelijk kan zijn voor de inhoud van de informatie, wanneer hij weet dat er onrechtmatige informatie op zijn server staat en deze vervolgens niet prompt verwijdert.<sup>4</sup>

Vanwege de onderscheiden regimes is het van het grootste belang vast te stellen wat voor positie een e-mail provider nu eigenlijk inneemt. Anders gezegd: is hij een access of een service provider? De belangrijkste standaard voor het gebruik van e-mail is het Simple Mail Transfer Protocol (SMTP). Het SMTP zorgt ervoor dat het getransporteerde 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, die zich normaliter op de server van de provider bevindt. Op het moment dat de geadresseerde zijn e-mail ophaalt, zal wederom een *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 zelf 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 een doorgeefluik. Hij is een service provider. In beginsel geldt voor hem het bijbehorende aansprakelijkheidsregime.

### **Communicatiegeheim**

Wanneer een ISP e-mail filtert, kan dat een inbreuk op het communicatiegeheim opleveren.<sup>5</sup> Dit fundamentele recht biedt in eerste instantie bescherming tegenover de overheid. Dit wordt ook wel *verticale werking* genoemd. Na de Tweede Wereldoorlog is de gedachte opgekomen dat burgers zich ook tegenover medeburgers op grondrechten zouden moeten kunnen beroepen. Ter onderscheiding van de eerdergenoemde verticale werking wordt dit ook wel *horizontale werking* genoemd. Omdat ISP's meestal particuliere bedrijven zijn, is de vraag of het communicatiegeheim hen verbiedt e-mail te filteren, een vraag naar de horizontale werking van dit geheim.

Het communicatiegeheim beschermt privé-communicatie die ter bezorging aan een transporteur is toevertrouwd. In beginsel mag de transporteur geen kennis nemen van de door hem vervoerde privé-communicatie. Een zorgplicht van de ISP voor de inhoud van e-mail wordt daarom ook in de juridische literatuur afgewezen.<sup>6</sup> Dit argument tegen een zorgplicht gaat echter niet onverkort op.

In bijzondere gevallen staat het communicatiegeheim kennisname van getransporteerde privé-communicatie namelijk wel degelijk toe. Wanneer kennisname onvermijdelijk is om de goede werking van de dienst te waarborgen, geldt geen verbod op kennisname. In dat geval wordt het communicatiegeheim gewaarborgd door een verbod om inlichtingen aan derden over de inhoud van de communicatie te verschaffen.

Het communicatiegeheim wordt onder meer in art. 13 van de Grondwet en art. 8 van het Europees Verdrag voor de Rechten van de Mens beschermd. Kan een burger zich op deze rechten tegenover een andere burger beroepen? Ten aanzien van art. 8 EVRM heeft de Hoge Raad expliciet erkend dat het horizontale werking heeft.<sup>7</sup> Met betrekking tot art. 13 Gw is dat minder duidelijk. Bij de grondwetsherziening van 1983 is echter erkend dat grondrechten ook in verhoudingen tussen burgers onderling kunnen werken. Over de wijze waarop die doorwerking dan zou moeten plaatsvinden werd geen duidelijkheid gegeven. Dit kan volgens de regering van geval tot geval verschillen. Ik ga er hier van uit dat het communicatiegeheim in elk geval in een rechterlijke belangenafweging als zwaarwegend belang moet worden meegenomen.

### **Bescherming communicatiemiddelen**

In art. 13 Gw wordt het brief-, telefoon- en telegraafgeheim beschermd. Het briefgeheim geniet de meeste bescherming. Beperkingen op dit geheim zijn mogelijk op last van de rechter in de gevallen bij wet voorzien. Bij beperking van het telefoon- en telegraafgeheim is echter geen rechterlijke last vereist. De wet kan bepaalde personen aanwijzen die een beperking mogen gelasten. De grondwettelijke waarborg is bij het telefoon- en telegraafgeheim dus minder groot.

Kortom, enkel deze drie communicatiemiddelen worden genoemd, waarbij een onderscheid naar communicatiemiddel ten aanzien van de graad van bescherming wordt gemaakt. Daaruit kunnen we afleiden dat de bescherming van e-mail – hoewel ook een privé-communicatiemiddel – niet automatisch uit de bewoordingen van het grondwetsartikel volgt.

Wellicht kan e-mail door een wijdere interpretatie onder een van de genoemde geheimen geschaard worden. E-mail valt in elk geval niet onder de noemer brief. Bij de grondwetsherziening van 1983 is door de regering immers gesteld dat een brief ‘een communicatie [is] 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>8</sup> Bovendien zou deze communicatie op een vaste informatiedrager moeten zijn vastgelegd. Aan deze criteria voldoet e-mail niet.

Kan e-mail dan onder het telefoon- of telegraafgeheim worden gebracht? Qua techniek lijkt e-mail het meest op de telegraaf. E-mail zou dan echter wel moeten voldoen aan de eis van een bepaalde mate van beveiliging.<sup>9</sup> Degene die zich van telefoon of telegraaf bedient, moet er namelijk voor zorgen dat van een geheim te houden communicatie sprake kan zijn.<sup>10</sup>

Het is niet geheel duidelijk wat de exacte reikwijdte van deze eis is, laat staan of e-mail daaraan voldoet. Dat de toenmalig minister van Justitie, Winnie Sorgdrager, in 1997 stelde dat onversleutelde e-mail evenals een ansichtkaart niet beschermd zou zijn, maakt het niet duidelijker.<sup>11</sup> Deze vergelijking snijdt echter geen hout. Enerzijds omdat een ISP aanzienlijk wat tijd en moeite moet investeren om kennis te nemen van een individuele e-mail,<sup>12</sup> terwijl de postbode bij de bezorging van een ansichtkaart in een oogopslag tezamen met het adres de boodschap kan lezen. Anderzijds verliest Sorgdrager uit het oog dat ten aanzien van het briefgeheim duidelijk een eis van beslotenheid wordt gesteld, terwijl bij telefoon- en telegraafgeheim ook communicatie waarbij kennisname onvermijdelijk is voor het uitvoeren van de dienst, nog beschermd wordt. Ondertussen is echter wel zoveel verwarring geschapen, dat voor een adequate grondwettelijke bescherming van e-mail weinig goeds meer te verwachten valt van het huidige artikel.

Daarom worden er pogingen ondernomen om art. 13 Grondwet techniekonafhankelijk te formuleren, zodat e-mail evenals andere nieuwe communicatiemiddelen in de toekomst wel grondwettelijke bescherming kent.<sup>13</sup>

Ook al zou e-mail wel bescherming genieten, dan geldt nog niet in alle gevallen een verbod tot kennisname. Kennisname kan namelijk 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 dienstverlening onmogelijk maken. Een bevoegdheid tot kennisname wanneer dit noodzakelijk is voor de goede uitvoering van de dienst maakt dus deel uit van het communicatiegeheim.

In elk geval is de vraag of e-mail grondwettelijk beschermd wordt, niet geheel doorslaggevend. E-mail wordt namelijk wel door andere regelgeving beschermd. In de verhouding ISP-gebruiker wordt e-mail zelfs op dezelfde voet als het telefoon- en telegraafgeheim beschermd. 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. Ook ISP's zijn aanbieders van openbare telecommunicatiediensten en dus aan deze bepaling gebonden. Zoals gezegd is e-mail qua techniek het best vergelijkbaar met de telegraaf. E-mail zou op basis van dit

artikel dezelfde bescherming als telefoon en telegraaf verkrijgen. De Tweede Kamer wilde met art. 18.13 Tw echter buiten twijfel stellen, dat ook e-mail beschermd wordt.<sup>14</sup>

### **Recht op privacy**

Artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) bepaalt dat eenieder recht heeft op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Tezamen vormen deze rechten het recht op privacy. In het arrest *Klass* bepaalde het Europees Hof voor de Rechten van de Mens (EHRM) dat ook telefoonverkeer onder de bescherming van artikel 8 viel. Het Hof kiest daarbij niet voor een wijdere interpretatie van het begrip correspondentie, maar kiest voor een combinatie van privé-leven en correspondentie.<sup>15</sup> In het arrest *Malone* gaf het Hof aan dat ook *metering records* en in het bijzonder het gekozen telefoonnummer integraal deel uitmaken van de beschermde communicatie.<sup>16</sup> Over e-mail bestaan nog geen expliciete uitspraken. Toch is aannemelijk dat ook e-mail door art. 8 beschermd zal worden. Hofman ziet in de zaak *Mersch e.a./Luxemburg* zelfs een uitbreiding van de bescherming tot alle vormen van communicatie.<sup>17</sup> Volgens Hofman heeft de bescherming van artikel 8 EVRM zich gaandeweg uitgestrekt van schriftelijke correspondentie, via telefoonverkeer en radiografische communicatie, tot de vertrouwelijke communicatie als geheel.<sup>18</sup> De door het EHRM ondernomen koppeling van correspondentie en privé-leven maakt dit inderdaad in beginsel mogelijk. Ik ga er hier dan ook van uit dat e-mail onder de bescherming van art. 8 EVRM valt.

Artikel 8 lid 2 EVRM bevat een getrapte beperkingsclausule. De eerste vereiste, namelijk dat een beperking een wettelijke basis dient te hebben, komt naar voren in de arresten *Kruslin* en *Huvig*. Deze eis omvat meer dan de aanwezigheid van een wettelijke norm of een norm in vaste rechtspraak. De wettelijke basis dient ook te voldoen aan bepaalde kwaliteitseisen, de *rule of law*. Deze houden onder meer in de mogelijkheid van controle door een onafhankelijke rechter, bepalingen met betrekking tot de duur van het afluisteren en regels met betrekking tot de delicten waarbij mag worden afgeluisterd.<sup>19</sup> Er moeten dus waarborgen zijn tegen misbruik van de beperkingen. In *Klass* zegt het Hof met zoveel woorden dat als een inbreuk op het communicatiegeheim niet bekend wordt gemaakt aan degene die wordt afgeluisterd, en daardoor dus niet getoetst kan worden door de rechter, 'Article 8 could to a large extent be reduced to a nullity'.<sup>20</sup>

Een van de belangrijke voorwaarden die het EHRM stelt aan interceptie is dat er een effectief rechtsmiddel bestaat. Bij geheime interceptie zijn de waarborgen tegen misbruik nog belangrijker dan bij maatregelen waarvan de afgeluisterde op de hoogte is. Om de toegang tot rechterlijke controle open te houden is een systeem van notificatie wenselijk, al mag het onder omstandigheden beperkt worden.<sup>21</sup> Het individu heeft recht op 'adequate bescherming tegen arbitraire interceptie'.<sup>22</sup>

Het EHRM spreekt zich principieel uit vóór rechterlijke toetsing van inbreuken op het communicatiegeheim, maar geeft aan dat dat niet in alle gevallen noodzakelijk zal zijn, 'in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge'.<sup>23</sup>

Het is nog niet geheel duidelijk hoe het EHRM zal omgaan met andere (nieuwere) elektronische communicatiemiddelen. Worden alleen 'closed channel communications' beschermd of ook 'open channel communications'? Interessant in dat verband is een uitspraak van de Commissie over radiocommunicatie via de 27 MHz-band: 'the transmission of information or ideas via the technical medium used by the applicants constitutes a transmission of information or ideas that might be regarded as being carried out by correspondence within the meaning of article 8'.<sup>24</sup> In die zaak werd de vraag of het ging om besloten communicatie of niet, dus niet maatgevend geacht voor de vraag of er bescherming was door artikel 8 EVRM. Dit is ook systematisch juist, aangezien het Hof de begrippen correspondentie en privé-leven aan elkaar gekoppeld heeft. Over het algemeen wordt aangenomen dat het EHRM te zijner tijd met behulp van verdragsdynamische interpretatie ook e-mail onder artikel 8 zal verstaan.

Wanneer e-mail inderdaad door art. 8 EVRM beschermd wordt, zal het filteren van e-mails met virussen als een beperking van het recht op privacy van art. 8 beschouwd moeten worden. Het filteren zal dan moeten voldoen aan de eisen die het tweede lid aan beperkingen stelt.

### **Filteren in de praktijk**

Het communicatiegeheim staat dus niet altijd in de weg als het gaat om aansprakelijkheid voor computervirussen. Op de vraag of ISP's ook daadwerkelijk aansprakelijk gesteld kunnen worden voor de schade van computervirussen die via hun systemen verspreid worden, zal hier geen eenduidig antwoord gegeven kunnen worden.

Het filteren van virus bevattende e-mail is in elk geval slechts een optie 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 dat laatste gebeurt, mag de ISP kennis nemen van de inhoud van e-mail. Het kan echter gewenst zijn al in een eerder stadium 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 het volgende. Op het moment dat de ISP afweet van het bestaan van een virus dat servers kan platleggen, mag hij in beginsel zijn servers op de aanwezigheid van dat virus 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 elke e-mail op virussen te controleren. Een dergelijke algemene plicht wordt verboden door art. 15 van de E-commercerichtlijn.<sup>25</sup> Bovendien zou een dergelijke vergaande controle over het algemeen niet voldoen aan eisen van proportionaliteit en subsidiariteit. Deze beginselen eisen dat beperkingen gerechtvaardigd zijn door een achterliggend belang. Een beperkende maatregel moet geschikt zijn om haar doel te bereiken en mag niet verder gaan dan strikt noodzakelijk is.

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>26</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 de geschikte instantie.

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.

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.

### **Hoe nu verder?**

Nu het communicatiegeheim niet altijd een kennisname verbiedt, kan een ISP in beginsel aansprakelijk zijn voor de schadelijke inhoud van e-mail. Met name wanneer de beschikbaarheid van communicatiediensten door een computervirus wordt bedreigd, mag de ISP kennis nemen van de inhoud van e-mail. In dat geval zou ook een plicht tot filteren kunnen ontstaan. Deze ontstaat des te eerder, naarmate de potentiële schade toeneemt.

Omdat het optreden van een individuele ISP weinig zoden aan de dijk zet, is een gecoördineerde aanpak de aangewezen manier om daadwerkelijk de verspreiding van schadelijke computervirussen tot een minimum te beperken. De gezamenlijke ISP's zouden in een gedragscode een centrale onafhankelijke instantie kunnen belasten met de coördinatie van het anti-virusbeleid. Deze instantie dient de schadelijkheid van virussen tegen de privacy beperkende aspecten van filtermaatregelen af te wegen. Op deze manier kan gewaarborgd worden dat op het communicatiegeheim niet willekeurig en ongerechtvaardigd inbreuk wordt gemaakt. Bovendien is een gecoördineerde aanpak veel efficiënter. Afhankelijk van de ernst van de dreiging zou een door de instantie te instigeren maatregel kunnen verschillen van het filteren van e-mail met bepaalde eigenschappen, dan wel het informeren van de gebruikers. De eerste maatregel moet in duur beperkt zijn.

Het gezamenlijk optreden van ISP's zou een effectieve netwerkoplossing kunnen zijn om het virusprobleem binnen de perken te houden. Of deze oplossing ook wenselijk en noodzakelijk is, hangt echter van toekomstige ontwikkelingen af.

1. Convergentie is het proces waarbij eens van elkaar gescheiden vormen van communicatie samensmelten en de grenzen tussen verschillende communicatietechnologieën vervagen. Een voorbeeld is het gebruik van kabel voor andere diensten dan omroep, zoals telefonie. Zie J.C. Arnbak, J.J. van Cuijlenburg en E.J. Dommering, *Verbinding en ontvlechting in de communicatie. Een studie voor toekomstig overheidsbeleid in de openbare elektronische informatievoorziening*, Amsterdam: Otto Cramwinckel Uitgever 1990.

2. Ook WAP-telefoons zijn niet meer veilig.

3 Art. 12 van 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.

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

5. Ik gebruik de term communicatiegeheim als techniekonafhankelijke en ruimere omschrijving van het constitutionele brief-, telefoon –en telegraafgeheim.

6. K.J. Koelman, 'Wat niet weet, wat niet deert: civielrechtelijke aansprakelijkheid van de provider', *Mediaforum* 1998, nr. 7/8, p. 211-212; C.B. van der Net, *Grenzen stellen op het Internet*.

*Aansprakelijkheid van internet-providers en rechtsmacht*, Deventer: Gouda Quint 2000, p. 54. Ook in Duitsland is dit de heersende leer. Zie daarvoor U. Sieber, 'Die rechtliche Verantwortlichkeit im Internet. Grundlagen, Ziele und Auslegung von § 5 TDG und § 5 MDStV', *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.

7. HR 9 januari 1987, *Computerrecht* 1987-2, p. 110-115 (*Bespiede bijstandsmoeder*) m. nt. E.J. Dommering.
8. *Kamerstukken II* 1975/1976, 13872, nr. 2, p. 44-46.
9. E.J. Dommering e.a., *Informatierecht. Fundamentele rechten voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2000, p. 79.
10. *Kamerstukken II* 1975/1976, 13872, nr. 3, p. 46.
11. Zie ook L.F. Asscher, 'E-mail een ansichtkaart?', *Mediaforum* 1997-7/8, p. 103.
12. De e-mail moet gelokaliseerd worden, uitgesorteerd en uiteindelijk geopend en gelezen.
13. Zie de voorstellen van de Commissie Franken (Rapport Commissie 'Grondrechten in het digitale tijdperk', Den Haag 2000), het daaropvolgende kabinetsstandpunt (*Kamerstukken II* 2000/2001, 27460, nr. 1) en de mijns inziens terechte kritiek op deze voorstellen (o.a. L.F. Asscher, 'Trojaans hobbelpaard', *Mediaforum* 2000-7/8, p. 228-233; E.J. Dommering, 'De Nederlandse Constitutie en de informatietechnologie', *Computerrecht* 2000-4, p. 177-185)
14. Dommering e.a 2000, p. 75.
15. J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van vertrouwelijke communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, Zwolle: W.E.J. Tjeenk Willink 1995, p. 70-72; EHRM 6 september 1978 (*Klass*); R.A. Lawson & H.G. Schermers, *Leading cases of the European Court of Human Rights*, Nijmegen: Ars Aequi 1997, p. 66-67.
16. EHRM 2 augustus 1984 (*Malone*), *NJ* 1988, 534; Hofman 1995, p. 70-71; A.J. Nieuwenhuis, 'Vertrouwde en virtuele bescherming', *NJCM-Bulletin* 1998, p. 429.
17. Hofman 1995, p. 71-72.
18. Hofman 1995, p. 72.
19. EHRM 24 april 1990 (*Kruslin en Huvig*), *NJ* 1991, 523; Lawson en Schermers 1997, p. 373-375.
20. *Klass*, par. 36.
21. Nieuwenhuis 1998, p. 433.
22. EHRM 2 augustus 1984 (*Malone*), *NJ* 1988, 534; Hofman 1995, p. 75-77.
23. *Klass*, para 56.
24. ECRM 13 mei 1982 (*X en Y/ België*). Geciteerd bij Hofman 1995, p. 71.
25. 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
26. Als voorbeeld kan het sulfnbk.exe-virus worden genoemd. Zie daarvoor <http://www.netkwesties.nl/editie15/artikel3.html>

Mr. drs. W.A.M. Steenbruggen is werkzaam als projectonderzoeker bij het Instituut voor Informatierecht aan de Universiteit van Amsterdam.