00451/06/DE
WP 118

Stellungnahme 2/2006 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post

Angenommen am 21. Februar 2006

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe c und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14 -

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

Die Artikel-29-Datenschutzgruppe ist sich der zunehmenden Verbreitung verschiedener Online-Kommunikationsdienste einschließlich gebührenfreier internetbasierter E-Mail-Dienste und damit zusammenhängender Dienste bewusst. Mit der Ausweitung der elektronischen Kommunikationsdienste kommen Bedenken hinsichtlich des Schutzes des Kommunikationsgeheimnisses auf, insbesondere angesichts der Praxis, Nachrichten zu prüfen, um Werbemüll (Spam) und Viren zu beseitigen und festgelegte Inhalte zu ermitteln.

Der Artikel-29-Datenschutzgruppe ist bekannt, dass die meisten Internetdienstanbieter (Internet Service Providers - ISP) und Anbieter von Diensten elektronischer Post (E-Mail-Anbieter) Filtersysteme verwenden, um Netze und Geräte zu schützen, in selteneren Fällen auch, um Nachrichten aus geschäftlichen Gründen zu prüfen. Die Artikel-29-Datenschutzgruppe ist jedoch der Ansicht, dass die Verwendung solcher Filtersysteme in einigen Fällen unter Umständen nicht mit den nachstehend beschriebenen Datenschutzvorschriften in Einklang steht. Dies könnte unter anderem darauf zurückzuführen sein, dass die Anwendung der Rechtsvorschriften auf diese neue Art von Dienstleistungen nicht immer klar ist.

Mit der vorliegenden Unterlage sollen vor allem Leitlinien zur Frage der Vertraulichkeit von elektronischen Nachrichten und speziell zum Filtern von Online-Nachrichten gegeben werden. Insbesondere soll der Frage nachgegangen werden, ob das Scannen von Nachrichten, wie es von den ISP und E-Mail-Anbietern üblicherweise zu verschiedenen Zwecken vorgenommen wird, ein Abfangen von Nachrichten darstellt und ob und wie ein solches Abfangen gerechtfertigt sein kann.

Zu diesem Zweck werden in der vorliegenden Unterlage unter anderem die Bestimmungen zur Vertraulichkeit elektronischer Nachrichten gemäß Artikel 5 Absatz 1 der Richtlinie 2002/58/EG über den Schutz der Privatsphäre in der elektronischen Kommunikation sowie andere einschlägige Bestimmungen, die Teil des gemeinschaftlichen Besitzstandes und der zu seiner Umsetzung erlassenen innerstaatlichen Rechtsvorschriften sind, untersucht.

II. RECHTLICHER RAHMEN FÜR DEN DATENSCHUTZ UND DEN SCHUTZ DER PRIVATSPHÄRE IN DER ELEKTRONISCHEN KOMMUNIKATION

A) Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten

Die Vertraulichkeit der Kommunikation wird durch die internationalen Übereinkommen über Menschenrechte, insbesondere die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten („EMRK“) und die Verfassungen der Mitgliedstaaten gewährleistet. Sie wird außerdem durch die beiden nachstehend beschriebenen EU-Richtlinien garantiert.

---

[1] ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

Artikel 8 der EMRK gewährt jedermann das Recht auf Achtung seines Privatlebens und seiner Korrespondenz und legt fest, unter welchen Voraussetzungen Eingriffe in die Ausübung dieses Rechts zulässig sind. Der Europäische Gerichtshof für Menschenrechte („Gerichtshof“) hat Artikel 8 mehrfach auf normale postalische Mitteilungen angewandt.

Das Abfangen, Öffnen, Lesen und verzögerte Zustellen von Briefen oder das Behindern der Versendung von Briefen wurden allesamt als Verstoß gegen Artikel 8 der EMRK[2] gewertet. Aus der Rechtsprechung der Kommission und des Europäischen Gerichtshofs für Menschenrechte kann geschlossen werden, dass elektronische Nachrichten mit größter Wahrscheinlichkeit unter Artikel 8 der EMRK fallen, da die Begriffe „Privatleben“ und „Korrespondenz“ beide auf sie zutreffen[3]. Kommunikationspartner, die elektronische Post austauschen, können berechtigterweise erwarten, dass ihre Nachrichten nicht von Dritten, seien es öffentliche oder private Stellen, kontrolliert werden.

Das Recht auf Achtung der „Korrespondenz“ beinhaltet nicht nur die Vertraulichkeit, sondern auch das Recht, Korrespondenz zu versenden und zu empfangen[4]. Daraus kann geschlossen werden, dass ein generelles Verbot der Versendung oder des Empfangs von elektronischer Post im Widerspruch zu Artikel 8 der EMRK steht.

Jeder, der der gerichtlichen Zuständigkeit eines der Vertragsstaaten der EMRK untersteht, hat ein Recht auf Achtung seines Privatlebens und seiner Korrespondenz. Dies schließt alle an einer Kommunikation beteiligten Parteien ein. In der Rechtssache A gegen Frankreich (1993) befand der Gerichtshof, dass das Aufzeichnen eines Telefongesprächs mit der Zustimmung nur einer der Parteien einen Eingriff in das Recht der anderen an der Kommunikation beteiligten Partei auf Achtung der Korrespondenz darstelle.

Nach der EMRK können die Vertragsstaaten der Menschenrechtskonvention Maßnahmen zum rechtmäßigen Abfangen von Korrespondenz einschließlich elektronischer Nachrichten oder andere für diese Zwecke erforderliche Maßnahmen ergreifen, soweit sie mit der EMRK in Einklang stehen, so die Auslegung durch den Europäischen Gerichtshof für Menschenrechte in seiner Rechtsprechung. Abfangen kann dabei definiert werden als Kenntnisnahme vom Inhalt privater Kommunikation zwischen zwei oder mehreren Teilnehmern und/oder von zugehörigen Verkehrsdaten, einschließlich der mit der Nutzung elektronischer Kommunikationsdienste verbundenen Verkehrsdaten, durch einen Dritten, was eine Verletzung des Rechts einer Einzelperson auf Schutz der Privatsphäre und Vertraulichkeit der Korrespondenz darstellt. Aus diesem Grund sind Abfangmaßnahmen abzulehnen, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Artikel 8 Absatz 2 der EMRK durch den Europäischen Gerichtshof für Menschenrechte ergeben:

Sie müssen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen.

---

[2] In der Rechtssache Niemitz (1992) befand der Gerichtshof, dass Briefe, die bereits an den Adressaten ausgeliefert wurden, unter Artikel 8 der EMRK fallen. In dieser Entscheidung stellte der Gerichtshof zudem fest, der Schutz gelte nicht nur für private Mitteilungen, sondern auch für geschäftliche Korrespondenz. In den Rechtssachen Klass (1978), Malone (1984) und Huvig (1990) erklärte der Gerichtshof, dass auch Telefongespräche unter Artikel 8 fallen. Für andere Kommunikationsmittel ist die Rechtssache Mersch der Kommission (1985) maßgeblich; die Kommission vertrat hier die Ansicht, das Abhören von Nachrichten jeglicher Art verstoße gegen Artikel 8.

[3] Untermauert wird diese Schlussfolgerung durch die Tatsache, dass eine Kontrolle von E-Mail-Nachrichten in den meisten Staaten verboten ist und dass sowohl auf internationaler als auch auf nationaler Ebene spezifische Befugnisse zum Abfangen von E-Mail-Nachrichten geschaffen wurden.

[4] In Erwägungsgrund 43 zum Urteil Golder (1975) heißt es: *„Jemanden schon an der Möglichkeit des brieflichen Verkehrs zu hindern, bedeutet den radikalsten „Eingriff“ (Art. 8 Abs. 2) in die Ausübung des „Rechts auf Achtung des Briefverkehrs“; es ist nicht vorstellbar, dass ein solcher Eingriff nicht unter Art. 8 fällt, während dies bei einer einfachen Kontrolle unbestritten so ist.“* Auch die Nichtweiterleitung eingegangener Post stellt einen Eingriff dar (Schöneberger & Durmaz, 1988).

In privaten Beziehungen ist für die Anwendung der Konventionsrechte jedoch der Grundsatz der positiven Verpflichtungen der Vertragsparteien maßgeblich. Die Vertragsparteien sind nicht nur dazu verpflichtet, von Eingriffen in Rechte abzusehen, sondern auch dazu, positive Maßnahmen zu treffen, um sicherzustellen, dass diese Rechte tatsächlich ausgeübt werden können, und zwar nicht nur gegenüber der Staatsgewalt, sondern auch im Bereich der persönlichen Beziehungen der Einzelnen untereinander. Dies beinhaltet auch die Verpflichtung, einen angemessenen Rechtsrahmen für die Ausübung dieser Rechte zu schaffen.

In Artikel 6 Absatz 2 des Vertrags über die Europäische Union wird ausdrücklich festgestellt, dass die Union die Grundrechte, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben, achtet. Nach Artikel 52 Absatz 3 der EU-Charta haben die in der Charta enthaltenen Rechte die gleiche Bedeutung und Tragweite, wie sie ihnen in der EMRK verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.

B) Besondere Bestimmungen zur Vertraulichkeit elektronischer Nachrichten

Wie vorstehend erwähnt, wird die Vertraulichkeit der Kommunikation auch durch zwei EU-Richtlinien gewährleistet. Bei der Prüfung der Frage der Vertraulichkeit der Kommunikation sind die Bestimmungen dieser Richtlinien in Verbindung sowohl mit der EMRK als auch mit der vorstehend dargelegten Rechtsprechung des Gerichtshofs für Menschenrechte auszulegen.

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Datenschutzrichtlinie“) gilt als Querschnittsregelung für den Schutz der Persönlichkeitsrechte. Was die Verarbeitung personenbezogener Daten anbelangt, so verweist die Datenschutzrichtlinie auf das in Artikel 8 der EMRK verankerte Recht auf Privatsphäre[5]. Das Recht auf Empfang und Weitergabe von Informationen wird ebenfalls als Teil des in Artikel 10 der EMRK garantierten Rechts auf Informationsfreiheit anerkannt[6]. Darüber hinaus bestimmt Erwägungsgrund 47, dass die Person, von der eine elektronische Nachricht mit personenbezogenen Daten stammt, als die für diese Daten verantwortliche Person anzusehen ist, während der E-Mail-Anbieter in der Regel als Verantwortlicher für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind, gilt.

Gegenstand der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation („Datenschutzrichtlinie für elektronische Kommunikation“) ist die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze in der Gemeinschaft. Die Bestimmungen dieser Richtlinie spezifizieren und ergänzen die Datenschutzrichtlinie. Die Vertraulichkeit der Kommunikation wird insbesondere durch Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation geschützt, der wie folgt lautet:

---

[5] Erwägungsgrund 10: „Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und –freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre“.

[6] Erwägungsgrund 37: „Für die Verarbeitung personenbezogener Daten zu journalistischen, literarischen oder künstlerischen Zwecken, insbesondere im audiovisuellen Bereich, sind Ausnahmen von bestimmten Vorschriften dieser Richtlinie vorzusehen, soweit sie erforderlich sind, um die Grundrechte der Person mit der Freiheit der Meinungsäußerung und insbesondere der Freiheit, Informationen zu erhalten oder weiterzugeben, die insbesondere in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und der Grundfreiheiten garantiert ist, in Einklang zu bringen.“

„Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen … gesetzlich dazu ermächtigt sind."

Und in Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation heißt es: *„Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten."*

Relevant ist auch die Richtlinie über den elektronischen Geschäftsverkehr (E-Commerce-Richtlinie), insbesondere die Bestimmungen zur Haftung der Anbieter von E-Mail-Diensten und Internetdiensten, denen zufolge die Mitgliedstaaten den Diensteanbietern keine Überwachungspflichten allgemeiner Art auferlegen dürfen. Eine solche Verpflichtung wäre ein Verstoß gegen die Informationsfreiheit und gegen die Vertraulichkeit der Korrespondenz (Artikel 15 der E-Commerce-Richtlinie[7]).

III. SCANNEN DER INHALTE ELEKTRONISCHER POST

Vor diesem rechtlichen Hintergrund erhebt sich die Frage, ob das Scannen von Nachrichten, das bei ISP und E-Mail-Anbietern zu den unterschiedlichsten Zwecken üblich ist, mit dem EU-Recht vereinbar ist.

Die meisten ISP und E-Mail-Anbieter scannen die elektronische Post. Sie tun dies routinemäßig unter anderem zu folgenden Zwecken: Spamfilterung, Virenerkennung, Suche und Rechtschreibprüfung sowie Weiterleitung, automatische Antwort, Kennzeichnung dringender Nachrichten, Umwandlung eingehender E-Mails in Textnachrichten für Mobiltelefone, automatisches Sichern und Ablegen in Ordnern, Umwandlung von Text-URLs in anklickbare Links.

Nachstehend werden die rechtlichen Rahmenbedingungen für das Filtern zu folgenden Zwecken untersucht: (A) zum Erkennen von Viren, (B) zum Filtern von Spam und (C) zum Erkennen festgelegter Inhalte.

A) Filtern von elektronischer Post zum Erkennen von Viren

Mit Virenscannen wird das Verfahren der Untersuchung von Dateien auf bekannte Viren bezeichnet. Zuweilen schließt sich an das Virenscannen eine Virenbeseitigung an, bei der das aufgefundene Virus aus der Datei entfernt wird, sodass diese gefahrlos benutzt werden kann. Ein solches Scannen findet im Allgemeinen dann statt, wenn die elektronische Post auf den Servern des E-Mail-Anbieters eingeht. Die meisten E-Mail-Anbieter haben das Virenscannen in ihren Leistungskatalog aufgenommen, um sich selbst und die Nutzer vor schädlichen Viren zu schützen. Dabei wird das Scannen zumeist automatisch gestartet und kann von den Nutzern nicht abgeschaltet werden.

Bei der Bewertung der Rechtsgrundlagen für diese Praxis ist die Artikel-29-Datenschutzgruppe zu der Auffassung gelangt, dass die Einrichtung und Anwendung von Filtersystemen seitens der Anbieter von elektronischen Diensten zum Zwecke der

[7] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

Virenerkennung durch die in Artikel 4 der vorstehend genannten Datenschutzrichtlinie für elektronische Kommunikation festgelegte Verpflichtung der Betreiber, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten, gerechtfertigt sein könnte.

Da die Versendung virenbehafteter elektronischer Post (neben der Beschädigung sonstiger, in der Endeinrichtung der Nutzer gespeicherter Dokumente und Software) zum Systemzusammenbruch beim E-Mail-Anbieter führen und somit die Übermittlung weiterer elektronischer Nachrichten beeinträchtigen kann, ist die Artikel-29-Datenschutzgruppe der Ansicht, dass die Vornahme einer solchen Filterung eine Sicherheitsmaßnahme zum Schutz des Systems des für die Datenverarbeitung Verantwortlichen (des E-Mail-Anbieters) darstellt, zu der der Anbieter elektronischer Dienste, wie oben ausgeführt, gemäß Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation verpflichtet ist.

Nach Auffassung der Artikel-29-Datenschutzgruppe kann die Verwendung von Filtern für die Zwecke von Artikel 4 mit Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation vereinbar sein.

Die Artikel-29-Datenschutzgruppe möchte aber betonen, dass Maßnahmen wie die oben genannten mit den allgemeinen Grundsätzen des Gemeinschaftsrechts in Einklang stehen müssen.

Des Weiteren ist die Artikel-29-Datenschutzgruppe der Ansicht, dass die Einrichtung von Filtersystemen durch die Anbieter elektronischer Dienste auch als Maßnahme betrachtet werden kann, mit der die Anbieter die Erfüllung des Dienstleistungsvertrags mit ihren Kunden sicherstellen, die erwarten, E-Mails mit einem gewissen Maß an Sicherheit empfangen und versenden zu können. Somit lässt sich die von E-Mail-Anbietern bei der Anwendung von Filtersystemen vorgenommene Datenverarbeitung auch nach Artikel 7 Buchstabe b der Datenschutzrichtlinie rechtfertigen, demzufolge eine Verarbeitung von Daten erfolgen darf, wenn sie *„erforderlich [ist] für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist.“*

Da sich also, wie vorstehend dargelegt, das Virenfiltern mit der Gewährleistung der Sicherheit der Dienste gemäß Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation und/oder mit der reinen Vertragserfüllung gemäß Artikel 7 Buchstabe b der Datenschutzrichtlinie unbeschadet der Vertraulichkeit der Kommunikation rechtfertigen lassen könnte, erinnert die Artikel-29-Datenschutzgruppe daran, dass die Anbieter von elektronischen Diensten auf die Einhaltung der folgenden Regeln achten müssen:

a) Die Inhalte der E-Mail-Nachrichten und der beigefügten Anhänge müssen geheim gehalten werden und dürfen außer an den (die) Empfänger an niemanden weitergegeben werden.

b) Wenn ein Virus entdeckt wird, muss die installierte Software hinreichende Garantien hinsichtlich der Geheimhaltung bieten.

c) Erfolgt ein Scannen auf Viren in Form einer inhaltlichen Überprüfung, so sollte sie automatisch und lediglich für diesen Zweck stattfinden, d. h. die Inhalte dürfen für keinen anderen Zweck analysiert werden.

Über das Filtern sollten auch Informationen bereitgestellt werden (siehe nachstehenden Abschnitt zu diesem Thema).

B) Filtern von elektronischer Post zum Aussortieren von Werbemüll (Spam)[8]

ISP und E-Mail-Diensteanbieter wenden verschiedene Verfahren an, um zu verhindern, dass unerbetene elektronische Nachrichten (nicht notwendigerweise nur Werbe-E-Mails), also Werbemüll (*Spam*), ihre beabsichtigten Adressaten erreicht.

Eines dieser Verfahren ist die Aufstellung so genannter „Schwarzer Listen" („Blacklisting"), bei der die IP-Adressen bestimmter Server und bestimmten ISP zugeordnete dynamische IP-Bereiche auf die Schwarze Liste gesetzt werden[9]. Auf dieses Verfahren wird in der vorliegenden Stellungnahme nicht weiter eingegangen.

Das Herausfiltern von Werbemüll ist eine notwendige Praxis geworden. Würden die Anbieter von E-Mail-Diensten die elektronische Post nicht auf Spam filtern, so würde Spam einen immer größeren Teil der bei ihnen eingehenden Post ausmachen, die Systeme wären wahrscheinlich sehr langsam und ineffizient und die E-Mail-Dienste für die Nutzer praktisch unbrauchbar. Dies würde natürlich Unzufriedenheit bei den Kunden hervorrufen und die Möglichkeit, einen vertrauenswürdigen und zuverlässigen E-Mail-Dienst anzubieten, mit ziemlicher Sicherheit einschränken.

Wenngleich Werbemüll als solcher wohl weniger eine Bedrohung für die Sicherheit der Dienste der E-Mail-Anbieter als vielmehr für die allgemeine Leistungsfähigkeit des Netzes und insbesondere des E-Mail-Dienstes darstellt, kann sie doch nichtsdestoweniger der Grund dafür sein, dass ein Anbieter von elektronischen Diensten nicht mehr in der Lage ist, den eigentlichen E-Mail-Dienst zu erbringen. Die Datenschutzgruppe ist der Auffassung, dass Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation, in dem verlangt wird, dass die Betreiber von elektronischen Kommunikationsdiensten geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Sicherheit ihrer Dienste zu gewährleisten, zwar auf die Sicherheit der E-Mail-Dienste und Netzdienste *als solche* abzielt, aber auch auf die allgemeine Leistungsfähigkeit der E-Mail- und Netzdienste. Die Sicherheit elektronischer Dienste ist insofern kritisch, als sie sich auf die Leistungen des Anbieters auswirkt. Die Artikel-29-Datenschutzgruppe vertritt daher die Auffassung, dass Artikel 4 auch auf diese Situation anwendbar sein könnte. Anders ausgedrückt, Bedrohungen der allgemeinen Leistungsfähigkeit der E-Mail-Dienste und Netzdienste können es rechtfertigen, dass die Anbieter von Internetdiensten und E-Mail-Diensten zum Schutz gegen Spam Filterungen vornehmen. Zieht man in Betracht, welche Folgen Spam sogar dann hat, wenn der Spam-Versender pro Tag nur wenige Informationen per elektronische Post verschickt, diese Informationen jedoch an eine sehr große Zahl von Empfängern adressiert, so verstärkt dies das Argument zugunsten der Anwendung von Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation, denn sogar in solchen Fällen kann die Versendung einer derart begrenzten

---

[8] Das im März 2005 von der Spam-Taskforce erstellte OECD-Dokument „Anti Spam Regulations" (Anti-Spam-Vorschriften) (DSTI/CP/ICCP/SPAM(2005)1) beschreibt den Begriff „Spam" folgendermaßen: *„Spam" ist ein gängiger Begriff, der in den internationalen Medien und in politischen Erklärungen verschiedener Länder verwendet wird, für den es indessen keine gemeinsame Definition gibt. Obgleich sie im Großen und Ganzen das Gleiche meinen, definieren die einzelnen Länder „Spam" jeweils so, wie es für ihre lokale Gegebenheiten am relevantesten ist. Eine wesentliche Voraussetzung für die Konzeption einer Anti-Spam-Politik ist, dass eindeutig verstanden und definiert wird, was unter Spam zu verstehen ist, und dass zwischen dem Versenden von unverlangten Werbesendungen („Spamming") und rechtmäßigen Verfahren unterschieden wird. "*

[9] Bei der Anwendung dieser Technik nimmt der E-Mail-Anbieter keine Filterung vor, er blockiert lediglich (d. h. verweigert die Annahme von) E-Mails, die von den auf der Schwarzen Liste stehenden Servern oder IP-Bereichen kommen, ohne ihren Inhalt zu überprüfen. Diese Praxis des Blacklisting stellt zwar grundsätzlich einen geringeren Eingriff in die Privatsphäre dar als das inhaltliche Filtern, es kann sich indessen die Frage nach der Redefreiheit und dem Recht auf freie Meinungsäußerung sowie nach dem in Artikel 8 der EMRK verankerten und vom Gerichtshof genauer ausgelegten Recht auf Freiheit der Korrespondenz und auf freien Empfang von Korrespondenz stellen.

Zahl von E-Mails den Internetverkehr blockieren und die Zuverlässigkeit, Sicherheit und Effizienz der E-Mail-Dienste im Allgemeinen ernsthaft beeinträchtigen. Darüber hinaus ist die Datenschutzgruppe aus den gleichen Gründen auch der Ansicht, dass eine solche Filterung auf der Grundlage von Artikel 7 Buchstabe b der Datenschutzrichtlinie gerechtfertigt sein könnte, mit der Begründung, dass eine Spamfilterung notwendig ist, um den E-Mail-Anbieter in die Lage zu versetzen, den Dienstleistungsvertrag ordnungsgemäß auszuführen, dessen Vertragspartei die betroffene Person, also der Empfänger der elektronischen Post, ist.

Besorgt ist die Artikel-29-Datenschutzgruppe hingegen über die Tatsache, dass das Filtern zuweilen zu „falschen Treffern" führt, d. h. rechtmäßige und „erwünschte" Mitteilungen als Spam eingestuft und daher nicht zugestellt werden. Die Datenschutzgruppe ist der Ansicht, dass das Filtern und Zurückhalten von mutmaßlich unerwünschten eingegangenen Nachrichten nicht nur zu einem Eingriff in die Redefreiheit, sondern auch zu einem Verstoß gegen Artikel 10 der EMRK führen und somit einen Eingriff in die private Kommunikation darstellen kann[10].

Unbeschadet der Anwendung von Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation und zum Schutz des in Artikel 10 der EMRK verankerten Grundsatzes der Kommunikationsfreiheit sowie der in Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation festgeschriebenen und durch Artikel 8 der EMRK anerkannten Vertraulichkeit der Kommunikation empfiehlt die Datenschutzgruppe den Anbietern von elektronischen Diensten daher aus den oben dargelegten Gründen dringend, sich nach den folgenden Empfehlungen zu richten, die in erster Linie darauf abzielen, den Empfängern von elektronischer Post eine Kontrolle über die grundsätzlich an sie gerichteten Nachrichten zu geben:

a) Die Artikel-29-Datenschutzgruppe unterstützt die Vorgehensweise, bei der die Teilnehmer eines Dienstes zum einen die Möglichkeit erhalten, sich gegen das Scannen ihrer E-Mails zum Schutz vor Werbemüll zu entscheiden, zum anderen die Möglichkeit, als Spam eingestufte E-Mails zu prüfen, um sich zu vergewissern, ob es sich tatsächlich um Spam handelte, und schließlich noch die Möglichkeit, zu entscheiden, welche „Art" von Spam ausgefiltert werden soll. Die Datenschutzgruppe begrüßt im Übrigen das Vorgehen einiger E-Mail-Anbieter, die ihren Teilnehmern eine einfache Möglichkeit anbieten, ihre Entscheidung rückgängig zu machen und ihre elektronische Post wieder scannen zu lassen, um Spam auszufiltern.

b) Die Artikel-29-Datenschutzgruppe unterstützt außerdem die Entwicklung von Filtersystemen, die die Endnutzer entweder in der Endeinrichtung oder auf Servern Dritter oder auf dem E-Mail-Server des Anbieters installieren oder konfigurieren können und die es ihnen ermöglichen, zu kontrollieren, welche Mitteilungen sie erhalten möchten und welche nicht, auch um die Kosten für das Herunterladen unerwünschter elektronischer Post zu senken, wie in Erwägungsgrund 44 der Richtlinie 2002/58 dargelegt. Die Datenschutzgruppe befürwortet ferner die Suche nach anderen, möglicherweise weniger stark in die Privatsphäre eingreifenden Instrumenten zur Bekämpfung von Spam.

Zusätzlich zu den vorstehenden Ausführungen erinnert die Artikel-29-Datenschutzgruppe die Anbieter von E-Mail-Diensten, die elektronische Post auf Werbemüll filtern, an ihre Verpflichtung gemäß Artikel 10 der Datenschutzrichtlinie, die Teilnehmer in deutlicher und unmissverständlicher Weise über ihre Spam-Politik zu unterrichten, wie weiter unten in Abschnitt IV dieser Stellungnahme ausgeführt. Der E-Mail-Anbieter muss außerdem die Vertraulichkeit der gefilterten E-Mails gewährleisten, die für keine anderen Zwecke verwendet werden sollten.

[10] Wie vom Gerichtshof anerkannt, siehe Schöneberger & Durmaz, 1988.

C) Filtern von elektronischer Post zum Erkennen festgelegter Inhalte

Die Artikel-29-Datenschutzgruppe stellt fest, dass einige E-Mail-Anbieter sich das Recht auf Durchsuchen und sogar Beseitigen von festgelegten Inhalten vorbehalten[11]. Hierbei kann es sich beispielsweise um mutmaßlich illegale oder vom Empfänger, also dem Nutzer des jeweiligen Dienstes, nicht gewünschte Inhalte handeln. Das für diese Art des Filterns verwendete Verfahren entspricht weitgehend dem Verfahren zum Auffinden von Viren und Spam.

Anders als das Virenfiltern kann das Filtern von elektronischer Post zum Erkennen festgelegter Inhalte, auch wenn es sich um mutmaßlich illegale Inhalte handelt, nicht als notwendige technische und organisatorische Maßnahme zur Gewährleistung der Sicherheit von E-Mail-Diensten im Sinne von Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation betrachtet werden. Dem E-Mail-Anbieter droht keine Beeinträchtigung bzw. kein Erliegen seines Kommunikationsdienstes aufgrund des in der elektronischen Post enthaltenen Materials. Daher lässt sich das Scannen zum Zweck der Auffindung solchen Materials nicht damit rechtfertigen, dass der E-Mail-Anbieter die Sicherheit seines Dienstes gewährleisten muss. Die Artikel-29-Datenschutzgruppe ist auch besorgt darüber, dass die Anbieter von elektronischen Diensten, wenn sie solche Filterverfahren anwenden, zu Zensoren privater E-Mail-Kommunikation werden, indem sie beispielsweise Nachrichten sperren, deren Inhalte vielleicht völlig legal sind, was grundsätzliche Fragen im Zusammenhang mit der Redefreiheit, der Freiheit der Meinungsäußerung und der Informationsfreiheit aufwirft. Die Datenschutzgruppe möchte betonen, dass die Diensteanbieter keine allgemeine Verpflichtung zur Überwachung festgelegter oder mutmaßlich schädlicher Inhalte haben, dass diese Art der Dienstleistung jedoch, wie nachstehend genauer ausgeführt, vom Provider durchaus als Dienst mit Zusatznutzen angeboten werden kann.

Die Datenschutzgruppe ist daher der Auffassung, dass es gemäß Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation E-Mail-Anbietern untersagt ist, Nachrichten und die damit verbundenen Verkehrsdaten zu filtern, zu speichern oder auf andere Weise abzufangen, um eventuelle festgelegte Inhalte zu ermitteln, es sei denn, sie haben die Einwilligung der betroffenen Nutzer der Dienste oder sind gemäß Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation, die durch Rechtsvorschriften der Mitgliedstaaten umgesetzt wurde, gesetzlich zu solchen Überwachungsmaßnahmen ermächtigt.

---

[11] Siehe die AGB von Yahoo: Yahoo! überprüft und kontrolliert Inhalte grundsätzlich nicht, behält sich jedoch das Recht vor, Inhalte, die über die Services zugänglich sind, zurückzuweisen oder an einem anderen Ort innerhalb der Services zu veröffentlichen. Eine rechtliche Verpflichtung hierzu besteht nicht. Dies gilt insbesondere für Inhalte, die gegen diese AGB verstoßen oder aus sonstigen Gründen zu beanstanden sind. Sie müssen die Risiken, die mit der Nutzung von Inhalten verbunden sind, allein bewerten und tragen, einschließlich der Risiken, die sich daraus ergeben, dass Sie auf die Richtigkeit, Vollständigkeit oder Brauchbarkeit von Inhalten für Ihre Zwecke vertrauen. Insoweit erkennen Sie an, dass Sie nicht auf Inhalte, die von Yahoo! geschaffen oder von Dritten Yahoo! zur Verfügung gestellt werden, insbesondere Inhalte in Yahoo! Message Boards, Yahoo! Clubs, oder den sonstigen Bereichen der Services, vertrauen dürfen. Yahoo! ist berechtigt, Inhalte zu speichern und an Dritte weiterzugeben, soweit dies gesetzlich vorgeschrieben oder nach pflichtgemäßem Ermessen notwendig und rechtlich zulässig ist, um a) gesetzliche Bestimmungen oder richterliche oder behördliche Anordnungen zu erfüllen, b) diese AGB durchzusetzen, c) auf die Geltendmachung einer Rechtsverletzung durch Dritte zu reagieren, d) Ihren Anforderungen an den Kundendienst zu entsprechen oder e) die Rechte, das Eigentum oder die persönliche Sicherheit von Yahoo!, seinen Nutzern oder der Öffentlichkeit zu wahren.

IV. INFORMATIONSPFLICHT

Zusätzlich zu Artikel 5 der Datenschutzrichtlinie für elektronische Kommunikation muss die Verarbeitung personenbezogener Daten zwecks Kenntnisnahme des Inhalts privater Mitteilungen und/oder der mit ihnen verbundenen Verkehrsdaten auch verschiedenen Anforderungen der Datenschutzrichtlinie genügen.

Unter anderem ist in der Datenschutzrichtlinie die Verpflichtung festgeschrieben, die Betroffenen über die Verarbeitung ihrer persönlichen Daten zu informieren. Insbesondere sind die für die Datenverarbeitung Verantwortlichen nach Artikel 10 *„Information der betroffenen Person“* verpflichtet, Personen, bei denen personenbezogene Daten erhoben werden, bestimmte Auskünfte zu erteilen, zu denen die Identität des für die Verarbeitung Verantwortlichen sowie die Zweckbestimmungen der Datenverarbeitung gehören. Darüber hinaus bestimmt Artikel 6 Absatz 1 Buchstabe a der Datenschutzrichtlinie, dass die Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen, wodurch der Verpflichtung der für die Verarbeitung Verantwortlichen Nachdruck verliehen wird, die Bedingungen der Verarbeitung personenbezogener Daten völlig transparent zu machen.

Was das Filtern zwecks Erkennen von Viren und Werbemüll (*Spam*) anbelangt, so hält die Artikel-29-Datenschutzgruppe die Vorgehensweise der E-Mail-Anbieter, die Unterrichtung der Teilnehmer in die Vertragsbedingungen aufzunehmen, für angemessen.

Darüber hinaus müssen E-Mail-Anbieter auch Artikel 4 der Datenschutzrichtlinie für elektronische Kommunikation beachten, nach dem die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste die Teilnehmer über besondere Risiken der Verletzung der Netzsicherheit unterrichten müssen. Liegt das Sicherheitsrisiko außerhalb des Wirkungsbereichs möglicher Abhilfemaßnahmen des Diensteanbieters, so sollte dieser seine Nutzer und Teilnehmer über Maßnahmen informieren, die sie selbst zum Schutz der Sicherheit ihrer Kommunikation treffen können.

V. SONSTIGE MIT DER ELEKTRONISCHEN POST ZUSAMMENHÄNGENDE DIENSTE

Die Artikel-29-Datenschutzgruppe nimmt zur Kenntnis, dass eine neue Art von Softwareprodukten und Dienstleistungen wie beispielsweise der so genannte Dienst *„Did they read it?“* („Wer hat wann meine E-Mail gelesen?“) entstanden ist, die darauf abzielen, das Öffnen elektronischer Post zu verfolgen.

Diese Art von Service ermöglicht dem Teilnehmer, festzustellen, a) ob eine vom Teilnehmer verschickte E-Mail vom Empfänger/von den Empfängern gelesen wurde, b) wann sie gelesen wurde, c) wie oft sie gelesen (oder zumindest geöffnet) wurde, d) ob sie an andere weitergeleitet wurde und e) wenn ja, auf welchen E-Mail-Server an welchem Standort. Schließlich lässt sich damit auch feststellen, welche Art von Webbrowser und Betriebssystem der E-Mail-Empfänger verwendet.

Die Datenverarbeitung erfolgt stillschweigend, d. h. die E-Mail-Empfänger, bei denen die Daten abgerufen werden, erhalten keine Benachrichtigung über die Datenverarbeitung. Außerdem haben die E-Mail-Empfänger keine Möglichkeit, den vorstehend beschriebenen Informationsabruf zu akzeptieren oder abzulehnen. Alles in allem haben die Empfänger von elektronischer Post bei diesen neuen Produkten anders als bei den klassischen E-Mail-Systemen mit Bestätigungsfunktion keinerlei Möglichkeit, die Verarbeitung der Bestätigungsinformationen und ihre Weitergabe an den Softwarenutzer zu akzeptieren oder abzulehnen.

Die Artikel-29-Datenschutzgruppe spricht sich mit allem Nachdruck gegen eine solche Datenverarbeitung aus, bei der persönliche Daten über das Verhalten von Nachrichtenempfängern aufgezeichnet und weitergegeben werden, ohne dass die betreffenden Empfänger zweifelsfrei ihre Einwilligung hierzu gegeben hätten. Die stillschweigend vorgenommene Datenverarbeitung verstößt gegen die in Artikel 10 der Datenschutzrichtlinie niedergelegten Grundsätze des Datenschutzes, die Loyalität und Transparenz bei der Erhebung personenbezogener Daten verlangen.

Eine Datenverarbeitung, die darin besteht, vom Empfänger einer E-Mail Informationen darüber einzuholen, ob er die Nachricht gelesen und ob er sie an Dritte weitergeleitet hat, darf nur stattfinden, wenn der Empfänger der E-Mail zweifelsfrei seine Einwilligung gegeben hat. Eine solche Datenverarbeitung ist durch keine andere Rechtsgrundlage gerechtfertigt. Daher verstößt die stillschweigende Datenverarbeitung gegen die in Artikel 7 der Datenschutzrichtlinie verankerten Datenschutzgrundsätze, nach denen die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben haben muss.

VI. SCHLUSSFOLGERUNG

Da hinsichtlich der Rechtmäßigkeit des Filterns elektronischer Post Unsicherheit herrscht und seitens der Beteiligten um Leitlinien nachgesucht wurde, hält die Datenschutzgruppe die Veröffentlichung der vorliegenden Stellungnahme für angebracht.

Die Artikel-29-Datenschutzgruppe möchte die Anbieter von elektronischen Diensten ermutigen, die in dieser Stellungnahme enthaltenen Anleitungen und Empfehlungen bei der Erbringung ihrer Leistungen zu berücksichtigen. Im Rahmen ihrer Politik der Technologieförderung, die auch Erfordernisse des Datenschutzes und des Schutzes der Privatsphäre beim Aufbau von Infrastruktur- und Informationssystemen einschließlich Endeinrichtungen beinhaltet, möchte die Datenschutzgruppe die Entwickler von E-Mail-Software auffordern, datenschutzkonforme Systeme zu konzipieren und zu entwickeln, die so beschaffen sind, dass die Verarbeitung personenbezogener Daten auf das absolut notwendige Mindestmaß begrenzt wird, das zu dem mit der Verarbeitung verfolgten Ziel in einem angemessenen Verhältnis steht.

Geschehen zu Brüssel am 21. Februar 2006

Für die Datenschutzgruppe

Der Vorsitzende
Peter Schaar