MANUEL KIPER

Warnung vor willkürlichen Anti-Spam-Strategien!

Eine Gerichtsentscheidung, in der das Herausfiltern unerwünschter Werbe-E-Mails als möglicherweise strafbar angesehen wurde, hat erhebliche Aufregung unter Netzverwaltern und IKT-Verantwortlichen ausgelöst. Genau betrachtet, gibt es dafür aber keinen wirklichen Grund ...

Der Bundesgerichtshof hat im Jahr 2004 klargestellt, dass die unerbetene Zusendung von Werbung enthaltenden E-Mails gegen die guten Sitten im Wettbewerb verstößt und eine unzumutbare Belästigung darstellt. Insofern brauchen sich auch Unternehmen die Überflutung der betrieblichen Kommunikationssysteme mit ›Schrott-Mails‹ nicht bieten zu lassen.

Geht es allerdings um Werbe-Mails, die an Mitarbeiter adressiert sind, dann sind auch bei noch so zweifelhaften und zwielichtigen Inhalten einer automatisierten Unterdrückung und Löschung enge rechtliche Grenzen gesetzt, da es sich dabei immer um Eingriffe in gesetzlich geschützte Telekommunikationsvorgänge handelt.

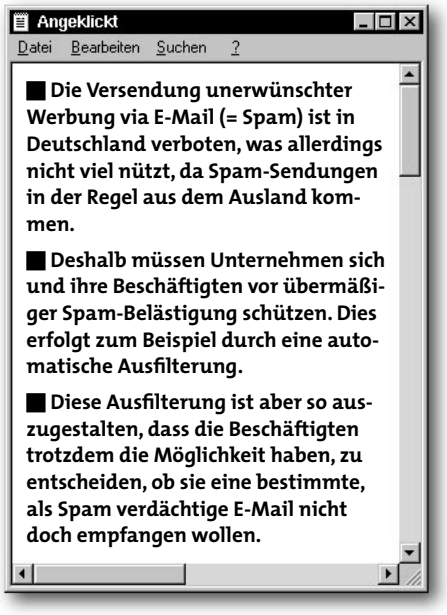
Betriebs- und Personalräte sollten sich zwar nicht gegen ein Herausfiltern von Werbe- und Schrott-Mails wehren, aber doch rechtskonforme Verfahren verlangen, die in einer Betriebsvereinbarung abgesichert werden sollten.

1... Datenschutzrichtlinie für elektronische Kommunikation, Richtlinie 2002/58/EG

2... Gesetz gegen den unlauteren Wettbewerb (UWG) in der Fassung vom 3. Juli 2004

›Spam‹-Versand ist verboten, aber ...

›Spam‹ ist die Abkürzung für ›Spiced Pork And Meat‹ und bezeichnet eigentlich ein in Gelee eingelegtes Frühstücksfleisch. Die Nutzung des Kürzels ausgerechnet für Werbe-Mails geht höchstwahrscheinlich auf einen Monty-Python-Sketch zurück. Darin gibt es in einem Restaurant jede Menge Gerichte – die aber alle Spam-Frühstücksfleisch enthalten, der Begriff ›Spam‹ taucht deshalb immer und überall wieder auf ...



Aber zurück zum elektronischen ›Spam‹: Hierzulande ist die Versendung von Werbe-Mails nur unter sehr eng gefassten Bedingungen erlaubt. Dabei gilt in der EU...[1] und auch in Deutschland...[2] die eher verbraucherfreundliche ›Opt-In‹-Lösung. Das heißt, dass Spam rechtlich nur bei vorheriger Einwilligung des Werbeadressaten zulässig ist. In den USA hingegen gilt das ›Opt-Out‹-Verfahren, wonach der Empfänger vor Werbe-Mails nur dann geschützt ist, wenn er zuvor die Zusendung von Spam aktiv abgelehnt hat (z.B. durch Eintragung in die so genannten Robinson-Listen).

Hier in Deutschland ist seit Juli 2004 nach dem neuen § 7 des UWG (Gesetz gegen den unlauteren Wettbewerb) »eine unzumutbare Belästigung« anzunehmen »bei einer Werbung unter Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post, ohne dass eine Einwilligung der Adressaten vorliegt«.

Hingegen »ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn

- ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder

Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
- der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
- der Kunde der Verwendung nicht widersprochen hat und
- der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.«

Nicht zu Spam-Mails im rechtlichen Sinne zählen damit Werbe-Mails von Unternehmen, mit denen der Empfänger bereits in geschäftlichem Kontakt gestanden hat oder wenn er selbst durch ›schlüssiges Verhalten‹ (also z.B. das Hinterlassen seiner E-Mail-Adresse) einen solchen Kontakt zum Versender aufgenommen hat.

Rechtliche Maßnahmen gegen Spam-Versender

Wird ein Unternehmen durch ›echten‹ Spam belästigt, kann es sich zum Beispiel an die Handelskammer wenden, um gegen den Verursacher eine Klage wegen unlauteren Wettbewerbs anzustrengen.

Gegen Spam aus Deutschland kann auch zivilrechtlich mit einer Abmahnung vorgegangen werden (siehe: ›Die Abmahnung ...‹ in cf 6/03 ab Seite 33). Hierbei wird der Spam-Versender aufgefordert, sich bei Meidung einer Vertragsstrafe zu verpflichten, die Versendung von Spam zu unterlassen. Weigert er sich, kann gerichtlich eine einstweilige Verfügung erlassen werden.

Grundlage für dieses zivilrechtliche Vorgehen ist der Umstand, dass E-Mail-Werbung eine unzulässige Belästigung im Sinne von § 823 und § 1004 BGB darstellt, da sie die Aufmerksamkeit des Betroffenen über Gebühr in Anspruch nimmt und zu einer unzumutbaren Belastung des Gewerbebetriebs gemäß § 823 Abs. 1 BGB führt. Vorformulierte Unterlassungserklärungen werden von Rechtsanwälten angeboten.…[3] Da die meisten unerwünschten Werbe-Mails allerdings aus den USA oder sonstigem Ausland kommen, ist der Rechtsweg gegen Spam vielfach aussichtslos, auch wenn Spam-Versendern in den USA seit dem 1. Januar 2004 bis zu fünf Jahre Freiheitsentzug und bis zu sechs Millionen US-Dollar Geldstrafe drohen.

Eine solche Strafbewehrung für den Spam-Versand sieht das deutsche Recht nicht vor. Die Bundesregierung hat jedoch versucht, mit einem Anti-Spam-Gesetz die Verschleierung von Spam als Ordnungswidrigkeit einzustufen und damit zu verhindern. Dieser im April 2005 vom Kabinett verabschiedete Gesetzentwurf sah Folgendes vor:

»Werden kommerzielle Kommunikationen per elektronischer Post (E-Mail) versandt, darf in der Kopf- und Betreffzeile weder der Absender, noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt insbesondere dann vor, wenn die Kopf- oder Betreffzeile absichtlich so gestaltet ist, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.«…[4] Das Gesetz ist aber (bisher) nicht verabschiedet worden.

Zusammenfassend kann also gesagt werden, dass wohl nur eine Anti-Spam-Strategie durch technische Maßnahmen gegen die Flut von Werbe-Mails wirksam helfen kann.

Achtung: Spam-Filterung kann strafbar sein!

Weltweit sollen bereits 64 Prozent aller E-Mails Spam sein. In Deutschland liegt der Anteil der unerwünschten Spam-E-Mail-Werbung bei 47 Prozent. Ein Unternehmen, das mit Spam bombardiert wird oder der Arbeitgeber, dessen Beschäftigte durch Spam belästigt werden, wird deshalb Strategien entwickeln, um mit diesem Problem fertig zu werden. Hierzu ist der Arbeitgeber sogar verpflichtet – nicht nur um seine betrieblichen Kommunikationsanlagen vor Missbrauch zu schützen, sondern auch um sich schützend vor seine durch E-Mails zum Teil auch sexuell belästigten Beschäftigten zu stellen.

Spam-Filterung bei Providern ⮡ (Internetdienstleistern) und in den Unternehmen selber greift deshalb um sich. Das ist verständlich und notwendig, darf aber nicht ›gutsherrlich‹ vorgenommen werden, sondern hat sich auf die Einwilligung der Betroffenen und auf eine Vereinbarung mit der Interessenvertretung zu stützen – und es muss die rechtlichen Vorgaben beachten.

Unproblematisch ist die Spam-Filterung, soweit es dabei um nicht-personenbezogene E-Mail-Adressen des Unternehmens geht (z.B. info@btq.de). Hier greift das Direktionsrecht. Der Unternehmer oder Dienstherr geht lediglich das Risiko ein, bei automatisierter Spam-Filterung möglicherweise Geschäftspartner oder Kunden zu verprellen oder sich selber wichtige Informationen vorzuenthalten. Da die Filterprogramme aber ›lernfähig‹ sind, lässt sich hier entsprechend behutsam vorgehen.

Unproblematisch ist die Spam-Filterung auch dann, wenn E-Mails strafrechtlich relevante Inhalte oder so genannte ›ausführbare Anhänge‹ ⮡ enthalten, die eine Gefährdung des Unternehmens beispielsweise durch Viren ⮡ heraufbeschwören. Solche E-Mails dürfen oder müssen sogar unterdrückt werden. Sind sie allerdings an personenbezogene E-Mail-Adressen gerichtet (z.B. kiper@btq.de), sollten die herausgefilterten Spam-Mails ›in Quarantäne‹ genommen (also gesondert und geschützt gespeichert) werden, mit einer entsprechenden Information an den Empfänger und möglicherweise auch den Absender.

Dies zeigt schon, dass die Spam-Filterung immer dann rechtlich problematisch wird, wenn es um personenbezogenene E-Mail-Adressen geht.

3… Zu finden beispielsweise unter www.recht-im-internet.de/themen/spam/mustertexte.htm, aus der Kanzlei Jörg Heidrich, die auch für das Bundesamt für Sicherheit in der Informationstechnik (BSI) an der Schrift ›Antispam – Strategien‹ (Mai 2005) beteiligt war

4… Deutscher Bundestag, Drucksache 15/4835 vom 15. 2. 2005, Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz)

Viele Unternehmen und auch Dienststellen vertreten die irrige Auffassung, zwar personenbezogene betriebliche E-Mail-Adressen nutzen zu können, sich zugleich aber durch ein Verbot der privaten Nutzung dieser Adressen beliebige Eingriffe in die betriebliche Netzkommunikation und damit eben auch eine beliebige Spam-Filterung erlauben zu können. Wie kurzschlüssig diese Position ist, wird deutlich, wenn man sich anschaut, wie mit an die Betriebsadresse gerichteten persönlichen Postsendungen (Manuel Kiper c/o BTQ Niedersachsen) oder mit privaten Telefonanrufen an die Dienstnummer umzugehen ist. Diese dürfen keineswegs einfach unterdrückt oder ›gefiltert‹, sondern höchstens im Fall des Übermaßes sanktioniert werden.

Das Bundesverfassungsgericht hat klargestellt…[5], dass allein die Tatsache, dass ein Telefongespräch »in der Sphäre eines Arbeitsverhältnisses« geführt wird, es einer weiteren Person (z.B. dem Personalchef oder dem Abteilungsleiter) keineswegs erlaubt, mitzuhören oder mithören zu lassen. Jeglicher Eingriff in den Telekommunikationsvorgang – und Spam-Filterung ist ein solcher – berührt den Schutzbereich des allgemeinen Persönlichkeitsrechts.

Dabei können aus dem Direktionsrecht zwar Maßnahmen abgeleitet werden, sie müssen aber verhältnismäßig bleiben. Das heißt: Bei Verbot privater Nutzung des betrieblichen E-Mail-Systems bedarf der Einsatz eines Spam-Filters zwar nicht der Einwilligung, aber doch wenigstens der Unterrichtung der einzelnen Beschäftigten über die Tatsache der Filterung. In jedem Fall braucht es aber die Zustimmung des Betriebsrats, da das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 tangiert ist.

Und im Falle personenbezogener betrieblicher E-Mailadressen bei gleichzeitigem Verbot der privaten Nutzung des betrieblichen E-Mail-Systems (siehe: ›Heute schon gemailt und gesurft?‹ in c't 9/05 ab Seite 31) wäre es ein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht, wenn der einzelne Beschäftigte nicht einmal mehr informiert würde, welche E-Mails von welchem Absender an seine Betriebsadresse gegangen und abgefangen worden sind

(um diesen Personen bei Interesse am Kontakt dann eine private E-Mail-Adresse mitteilen zu können) – geschweige denn, dass ihm die Möglichkeit eingeräumt würde, diese E-Mails wiederherzustellen und zu lesen.

Außerdem: Auch wenn bei Verbot privater E-Mail-Nutzung das Telekommunikationsrecht mit dem strengen Post- und Fernmeldegeheimnis des § 88 TKG und der Strafbewehrung möglicher Eingriffe nach dem § 206 StGB nicht gilt, so greift für eingehende private, personenbezogene E-Mails doch der § 303 a StGB!

Dies verkennen zum Teil sogar Datenschutzbeauftragte der Länder. So meinte der Berliner Datenschutzbeauftragte…[6]: Wenn »der Arbeitgeber nicht als Anbieter von Telekommunikationsdiensten gegenüber seinen Beschäftigten agiert« (dies trifft dann zu, wenn die private E-Mail-Nutzung ausdrücklich untersagt wurde), unterläge er »insoweit nicht dem Fernmeldegeheimnis« und dürfe »wie bei herkömmlicher Dienstpost jederzeit die Inhalte kontrollieren und Post ohne dienstlichen Bezug aussortieren und gegebenenfalls löschen«. Dies ist nicht nur unzutreffend, sondern sogar gefährlich:

Werden dabei nämlich ohne Einwilligung persönlich adressierte E-Mails gelöscht, gilt § 303 a StGB mit seiner Strafandrohung für Datenveränderung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat deshalb zutreffend klargestellt, dass »§ 303 a StGB uneingeschränkt auf alle Provider, Unternehmen und Behörden anwendbar ist«.

Der § 303 a StGB besagt: »Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.« Unter Daten werden dabei alle Inhalte verstanden, die »elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden« – also auch E-Mails.

Der Tatbestand der Datenveränderung ist, wie das BSI schreibt, »auf solche Daten beschränkt, an denen und an deren Unversehrtheit ein Dritter ein unmittelbares Interesse besitzt oder besitzen könnte. Ein potentielles Interesse des Empfängers auch bei Spam-Mails ist grundsätzlich«, so das BSI, »angesichts der auch subjektiven Bewertung von Werbemails nicht auszuschließen. Grundsätzlich müssen die Provider und Arbeitgeber bei allen E-Mails zunächst davon ausgehen, dass ihre Kunden oder Arbeitnehmer jede an sie adressierte E-Mail auch erhalten oder es sich selbst vorbehalten wollen, die Nachricht als Spam zu löschen. Eine Ausnahme ist hier allenfalls bei Fällen von Viren-infizierten E-Mails anzunehmen.«

Ausdrücklich und in aller Klarheit formuliert das BSI: »Werden E-Mails also

5… BVerfG-Urteil vom 19. 12. 1991 – 1 BvR 382/85

6… Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit, 31. 12. 2004, ab Seite 54 (www.datenschutz-berlin.de/infomat/dateien/jb/jb04.pdf)

7… Bundesamt für Sicherheit in der Informationstechnik (BSI): ›Antispam – Strategien‹, Bonn, im Mai 2005, ab Seite 55 (www.bsi.de/literat/studien/antispam/antispam.pdf)

vorsätzlich gelöscht oder entsprechend der oberen Darstellung unterdrückt, so ist regelmäßig auch der Straftatbestand des § 303 a StGB bereits erfüllt.«[7] Hier hilft also nur die Einwilligung der Beschäftigten zur Filterung und dazu ein selbstbestimmter Umgang mit Spam.

Noch weitergehend muss die Spam-Filterung das Persönlichkeitsrecht der Beschäftigten wahren, wenn auch die private Nutzung des betrieblichen E-Mail-Systems vom Unternehmen geduldet oder erlaubt wird. Für diesen Fall muss das Unternehmen wie jeder Telekommunikationsanbieter sicherstellen, dass die eingehende elektronische Post ausgeliefert wird oder – im Falle etwa einer Virenwarnung – in ›Quarantäne‹ eingesehen werden kann.

Spam-Filter dürfen also in einem automatisierten Verfahren vermutete Spam-Mails zwar als solche kennzeichnen und vorübergehend zurückhalten, müssen aber in jedem Falle den Adressaten der E-Mail ›Herr des Verfahrens‹ bleiben lassen, ihm also die Entscheidung überlassen, ob er eine E-Mail empfangen und lesen will oder nicht.

Allerdings kann ein Unternehmen die private Nutzung des betrieblichen E-Mail-Systems von der Zustimmung des einzelnen Beschäftigten zu einer zentralen Spam-Filterung und -Unterdrückung gelisteter Spam-Versender abhängig machen. Zusätzlich bedarf dies in jedem Falle aber noch der Zustimmung des Betriebsrats, da das Mitbestimmungsrecht des § 87 Abs. 1 Nr. 6 BetrVG berührt ist.

Auf diesem Hintergrund war deshalb auch nur für manche Beobachter der Beschluss des Oberlandesgerichts (OLG) Karlsruhe vom 10. 1. 2005 (1 Ws 152/04) so überraschend, in der die prinzipielle Strafbarkeit des E-Mail-Ausfilterns bejaht wurde. In diesem Verfahren ging es darum, die Staatsanwaltschaft dazu zu zwingen, einer Verletzung des Post- und Fernmeldegeheimnisses durch Ausfilterung und Unterdrückung persönlich adressierter E-Mails in einer Dienststelle nachzugehen.

Das OLG gab dem Kläger Recht, weil die ausgefilterte Sendung dem Unternehmen »zur Übermittlung anvertraut« war. »Anvertraut ist eine Sendung dann«, so das Gericht weiter, »wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet. Unproblematisch liegt der Gewahrsam an einer E-Mail spätestens dann vor, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht hat und der versendende Mailserver die Daten dem empfangenden Server übermittelt hat [...] Ein Unterdrücken der E-Mail ist dann anzunehmen, wenn durch technische Eingriffe in den technischen Vorgang des Aussendens, Übermittelns oder Empfangens von Nachrichten mittels Telekommunikationsanlagen verhindert wird, dass die Nachricht ihr Ziel vollständig oder unverstümmelt erreicht. [...] Das Tatbestandsmerkmal ›Unterdrücken‹ wird jedenfalls durch eine Ausfilterung der E-Mail erreicht. In diesem Fall findet die Weiterleitung, also das Übermitteln der eingehenden Mail vom Mailserver an den einzelnen Clienten, nicht statt – dies war nach der Schilderung des Anzeigenerstatters der Fall.«

Ob sich in dem vorliegenden Fall der Nachweis einer strafrechtlich erheblichen Verletzung des Post- und Fernmeldegeheimnisses würde führen lassen, ließ sich nach Auffassung des OLG Karlsruhe nicht beurteilen, aber die Staatsanwaltschaft müsse dem Verdacht der Verletzung des Post- und Fernmeldegeheimnisses jedenfalls nachgehen.

Mit ähnlichen Anzeigen müssen somit zukünftig auch Systemverwalter und andere Verantwortliche in Betrieben rechnen, wenn die Spam-Filterung von ihnen nicht gesetzeskonform, sondern willkürlich vorgenommen wird.

Spam-Vermeidung und Anti-Spam-Maßnahmen

Um möglichst wenig Spam ausgesetzt zu sein und andererseits die erwünschte Kommunikation (man spricht hier von ›Ham‹, also ›Schinken‹) durch Anti-Spam-Maßnahmen so minimal wie möglich zu belasten, ist ein Bündel von Maßnahmen nötig:

Hierzu gehört zunächst, den eigenen Rechner durch stets aktuelle Viren-Software zu schützen und ihn damit nicht selber zur missbräuchlichen ›Spam-Schleuder‹ werden zu lassen. Das BSI hat in der schon genannten Schrift für IKT-Administratoren (**www.bsi.de/literat/studien/antispam/antispam.pdf**) eine Reihe weiterer Punkte aufgelistet, um die eigenen Systeme sicher einzurichten und E-Mail-Adressen so zu gestalten, dass eine missbräuchliche Nutzung durch ›Spammer‹ erschwert wird.

Die wesentlichen Anti-Spam-Maßnahmen beruhen allerdings auf einer intelligenten Filterung der eingehenden E-Mails. Ansatzpunkte für eine solche Filterung können die IP-Adresse des sendenden Rechners, die Absenderadresse und der Inhalt einer E-Mail sein. Aber auch das Verhalten des Absenders bei der Zustellung kann Hinweise auf Spam geben.

Zwar können sich Server- und Absenderadressen ändern und professionelle Spammer ihre Spuren verwischen, aber vielfach lässt sich doch eine Unterteilung in ›gute‹ und ›böse‹ Netzserver und ›gute‹ und ›böse‹ Absenderadressen vornehmen. Auf diese Art können auf der Grundlage professioneller Filtersysteme so genannte ›weiße‹ und ›schwarze‹ Listen geführt werden, die ähnlich wie ein Virenschutz täglich aktualisiert werden

und zusätzlich noch nach den betrieblichen Notwendigkeiten korrigiert werden können.

Ein entscheidender Ansatz für Filterung ist natürlich auch die Betreffzeile oder der Inhalt einer E-Mail. Mit Hilfe ›heuristischer‹ (erkennender, lernfähiger) Verfahren lassen sich vermutete Spam-Mails erkennen und als solche markieren (z.B. die häufigen ›Viagra‹-Angebote). Aber auch mit statistischen Methoden lässt sich Spam erkennen, da es sich üblicherweise um Massenversand handelt. Entsprechend oft werden diese Mails mit ihren Inhalten als Spam klassifiziert.

Bei einer neuen Mail lässt sich dann mit statistischen Methoden bestimmter auftretender Wortkombinationen und Vergleich mit bekanntem Spam die vermutliche Spam herausfiltern. Um den legitimen Massenversand erwünschter Werbung nicht an Spam-Filtern scheitern zu lassen, müssen sich seriöse Unternehmen mehr und mehr von Akkreditierungsstellen ihre lauteren Absichten beglaubigen lassen.

Professionelle Anti-Spam-Programme könnten im Prinzip eine Spam-Filterung sogar vorgelagert vornehmen, so dass das Unternehmen durch die Spam-Mails gar nicht erst belastet wird. Da aber die automatisierte Unterscheidung in ›Spam‹ und ›Ham‹ – also in Böse und Gut – nie fehlerfrei läuft, wird die Filterung üblicherweise erst im Betrieb vorgenommen und besteht vorrangig in einer Markierung und gesonderten Anzeige vermuteter Spam-Mails. Bei personenadressierten, zulässigen privaten E-Mails darf die Spam-Filterung im Betrieb höchstens in dieser zurückhaltenden Art ablaufen.

Als Spam verdächtige E-Mails können dann in einem gesonderten Ordner bis zu einem vorher bestimmten Verfallsdatum, bis zu einer bestimmten Menge oder bis zur manuellen Löschung durch den Empfänger abgelegt werden. Damit wird letztlich dem Adressaten oder Bearbeiter der E-Mail eine Hilfestellung gegeben, ohne ihm die Letztentscheidung über Löschen oder Öffnen der herausgefilterten E-Mail abzunehmen. Damit wird auch den weiter vorne beschriebenen gesetzlichen Anforderungen Rechnung getragen.

Einhalten der Mitbestimmung

Auch wenn für Filtermaßnahmen in betrieblichen E-Mail-Systemen die Zustimmung des einzelnen Beschäftigten notwendig ist – insbesondere, wenn die private Nutzung gestattet wurde –, muss vor dem Einsatz von Filtermaßnahmen auch die Zustimmung der Interessenvertretung eingeholt werden.

Das Bundesarbeitsgericht (BAG) hat mit seinem Urteil vom 29. 10. 1997 (5 AZR 508/96) festgestellt, dass das Aufzeichnen des Inhalts eines Telefonats des Arbeitnehmers dessen Einwilligung voraussetzt. Diese kann auch dann nicht stillschweigend als erteilt angenommen werden, wenn der Arbeitnehmer um die Abhörmöglichkeit weiß. Gleiches dürfte für die Inhaltsanalyse und Filterung von E-Mails gelten. In seinen Videoüberwachungs-Urteilen (siehe: ›Videoüberwachung am Arbeitsplatz‹ in cf 2/05 ab Seite 30) hat das BAG klargestellt, dass nicht einmal durch eine Zustimmung des Betriebsrats die heimliche Videoüberwachung der Arbeitnehmer zulässig wird, es sei denn, besondere Sicherheitsinteressen des Arbeitgebers rechtfertigen ausnahmsweise die Überwachung (BAG vom 15. 5. 1991 – 5 AZR 115/800). Alle Eingriffe in das Persönlichkeitsrecht bedürfen der Rechtfertigung, wobei der Grundsatz der Verhältnismäßigkeit gilt (BAG vom 27. 3. 2003 – 2 AZR 51/02).

Damit haben die obersten deutschen Gerichte deutlich gemacht, dass bei technischer Überwachung im Betrieb nicht nur ein Abwägungsprozess zwischen den möglicherweise berechtigten Direktionsinteressen des Arbeitgebers und den Datenschutzinteressen der Beschäftigten vorzunehmen ist. Sie haben vielmehr den Persönlichkeitsschutz des einzelnen Arbeitnehmers so hoch angesiedelt, dass die technische Überwachung und Kontrolle der Beschäftigten immer auf ein verträgliches Maß begrenzt werden muss. Um diesen Abwägungsprozess zu strukturieren, können Betriebs- und Personalräte ihre Beteiligungsrechte nutzen und entsprechende Betriebs-/Dienstvereinbarungen erzwingen.

Betriebsräte haben nach § 80 Abs. 1 Nr. 1 BetrVG die Aufgabe, die Einhaltung der zugunsten der Arbeitnehmer bestehenden Datenschutzregelungen zu kontrollieren. Dies gilt für die Einhaltung des Bundesdatenschutzgesetzes, wenn ausschließlich dienstliche E-Mails zulässig sind, und zusätzlich für die Einhaltung des Post- und Fernmeldegeheimnisses, wenn private E-Mails im Betrieb erlaubt oder geduldet werden.

Als zentrales Instrument der Mitbestimmung greift aber der § 87 Abs. 1 Nr. 6 BetrVG. Hier ist verankert, dass ohne Zustimmung des Betriebsrats technische Einrichtungen nicht eingeführt oder angewendet werden dürfen, wenn sie dazu bestimmt sind, Leistung und Verhalten der Arbeitnehmer zu überwachen. Nach höchstrichterlicher Rechtssprechung ist eine technische Einrichtung immer dann dazu bestimmt, Leistung oder Verhalten zu überwachen, wenn sie objektiv und unmittelbar dazu geeignet ist. Dies gilt unabhängig davon, ob der Betrieb diese Überwachung beabsichtigt und die durch die Datenerfassung gewonnenen Daten auch tatsächlich auswertet. Die Einführung von Filter-Software im Betrieb dürfte somit unstreitig der Mitbestimmung des Betriebsrats unterliegen.

8... abgedruckt in ›Der Personalrat‹ 3/02 ab Seite 107

Spam-Betriebs-/Dienstvereinbarung

Viele Betriebe und Dienststellen haben in der Vergangenheit Vereinbarungen zu E-Mail und Internet oder allgemein zur IKT-Nutzung abgeschlossen, an die bei der Regelung der Spam-Filterung oftmals angeknüpft werden kann. Am Beispiel einer Kommune (Oldenburg/Oldb.) können die Eckpunkte einer solchen Betriebs-/Dienstvereinbarung aufgezeigt werden (siehe info-Kasten rechts).

In Oldenburg existierte bereits eine Dienstvereinbarung zur Einführung und Anwendung von Telekommunikations- und Telediensten, in der es bereits im § 1 hieß: »Filter und Sperrungen bedürfen der Zustimmung der zuständigen Personalvertretung.« Die Stadt Oldenburg plante nunmehr einen verstärkten Virenschutz, Spam-Filterung und E-Mail-Größenbegrenzung mit dem Programm ›GWAVA‹ für Novel-GroupWise, der bei der Stadt Oldenburg etablierten Software.

Die damit mögliche Spam-Filterung war auch aus Sicht der Personalvertretung zweckmäßig. Gleichzeitig bemängelte die Interessenvertretung allerdings, dass das Programm ›GWAVA‹ auch Funktionen enthält, die ausdrücklich dazu bestimmt sind, Beschäftigte zu überwachen und auszuschnüffeln. »The sender and recipient will never know that you caught them discussing an unauthorized topic«, so hieß es auf Seite 91 des englischsprachigen GWAVA-Handbuchs. (»Sender und Empfänger werden niemals erfahren, dass sie bei der Diskussion unerlaubter Themen erwischt wurden.«)

Die Aktivierung solcher Funktionen wollte die Personalvertretung durch eine Dienstvereinbarung unterbinden, die zwischen der Stadt Oldenburg und dem Gesamtpersonalrat im Juni 2005 abgeschlossen wurde (siehe info-Kasten rechts).

Dr. Manuel Kiper, BTQ Beratungsstelle für Technologiefolgen und Qualifizierung im Bildungswerk ver.di in Niedersachsen, Donnerschweer Straße 84, 26123 Oldenburg, fon 0441-8 20 68, **kiper@btq.de**

Internetadressen:

www.drweb.de/email/index.shtml ***(viele Informationen zu Spam und Spamschutz)***

http://service.t-online.de/c/19/82/16/1982160.html ***(Spam- und Virenschutz von T-Online)***

www.spamfighter.com/Lang_DE/Product_Info.asp ***(kostenlose Filtersoftware)***

www.absolit.de/Spam/ ***(55 Tricks, Spam-Filter zu vermeiden, für seriöse E-Mail-Anbieter)***

www.recht-im-internet.de/themen/spam/urteile.htm ***(Gerichtsurteile über unerwünschte E-Mail-Werbung)***

[→] ausführbare Anhänge = unter ›Anhängen‹ (*attachments*) versteht man beliebige Dateien, die zusammen mit einer E-Mail verschickt werden; grob lassen sich dabei zwei Arten von angehängten Dateien unterscheiden: Dateien, die für die Ansicht oder Weiterverarbeitung ein spezielles Computerprogramm brauchen (z.B. Texte) oder Dateien, die selber ein Computerprogramm sind, also als ein solches ›ausgeführt‹ werden können; das Risiko, dass eine ›ausführbare Datei‹ ein Schadprogramm ist oder enthält, ist besonders groß

[→] Client (Kunde, Auftraggeber) = Teil eines Computer-Netzwerks, bestehend aus Verwaltungs-/Steuerungs-Rechnern (Server) und angeschlossenen Arbeitsplatz-Computern (= Clients = ›Kunden‹)

[→] IP-Adresse (IP = Internet Protocol) = Adresse, unter der ein kommunikationsfähiger Computer über das Internet zu erreichen ist

[→] Mailserver = Netzverwaltungsrechner (Server) speziell für die Verwaltung ein- und ausgehender elektronischer Post (E-Mail)

[→] Provider (*provide* = vermitteln, sorgen für) = Anbieter von Telekommunikationsdiensten (Internet-Zugang, Website-Angebot)

[→] Server (Zusteller) = spezielle Computer zur Verwaltung von Netzwerken mit verschiedenen Aufgaben (Netzsteuerung, zentrale Datenspeicherung, Softwarebereitstellung, Postverwaltung)

[→] Virus/Viren = nicht selbstständige Schadprogramme, die zum Funktionieren bestimmte Betriebssystemroutinen oder andere Software brauchen; inzwischen aber oft Sammelbegriff für *alle* Arten von Schadprogrammen