## IV. Ausblick

Die Umsetzung der Enforcement-Richtlinie steht unmittelbar bevor. Man darf gespannt sein, inwiefern die vorgesehenen neuen Mechanismen zur Rechtsdurchsetzung im Urheberrecht eine Veränderung der bisherigen Praxis mit sich bringen werden. Dies wird auch davon abhängen, wie die Gerichte mit den neuen Instrumentarien umgehen werden. Sowohl der I. Zivilsenat des BGH als auch der EuGH sind weiterhin mit einer erheblichen Zahl urheberrechtlicher Verfahren befasst, so dass auch für das Jahr 2008 mit einer maßgeblichen Fortbildung des Urheberrechts gerechnet werden darf, auch wenn ein gewisser Anteil der beim BGH noch anhängigen Verfahren Fragen der Gerätevergütung nach altem Recht betreffen.

Von Rechtsanwalt und Fachanwalt für Arbeitsrecht Olaf C. Sauer, Hamburg

Der Autor ist Rechtsanwalt in der Anwaltssozietät DAMM & MANN, Hamburg. Mehr über den Autor erfahren Sie auf S. XII.

# Der Einsatz von Spamfiltern am Arbeitsplatz – Eine kritische Analyse

Im Vorfeld der diesjährigen Computermesse CEBIT empfahl die Arbeitsgemeinschaft Informationstechnologie des Deutschen Anwaltsvereins (DAVIT), dass Unternehmen im Arbeitsvertrag oder in einer Betriebsvereinbarung die private Nutzung von E-Mails am Arbeitsplatz ausdrücklich regeln sollten. Die in zahlreichen Unternehmen übliche Filterung der elektronischen Post verstoße ohne wirksame Zustimmung gegen das Post- und Fernmeldegeheimnis. Diese Empfehlung nimmt der Autor zum Anlass, die rechtlichen Probleme im Zusammenhang mit der Nutzung von Spamfiltern am Arbeitsplatz genauer zu betrachten und eine praktische Handhabung der – sicherlich unverzichtbaren – Nutzung solcher Spamfilter kritisch zu analysieren.

## I. Einführung

Der Einsatz von Spamfiltern am Arbeitsplatz ist obligatorisch. Die Flut von Spams, die nicht zurückgeht, sondern im Gegenteil immer weiter ausufert, wäre nicht anders zu beherrschen. Am Arbeitsplatz kann der Einsatz von Spamfiltern allerdings rechtlich insbesondere deshalb problematisch sein, wenn der Arbeitgeber als direkter Vertragspartner des Providers zwar in den Einsatz des Spamfilters eingewilligt haben mag, eine ausdrückliche Einwilligung des Arbeitnehmers als eigentlichem Nutzer des E-Mail-Programms allerdings fehlt. Denkbar ist auch, dass der Arbeitgeber selbst alle technischen Einrichtungen für eine E-Mail-Nutzung hat, die er dem Mitarbeiter zur dienstlichen oder gar privaten Nutzung zur Verfügung stellt, der Arbeitgeber es dann aber unterlässt, eine ausdrückliche Einwilligung für den Einsatz eines Spamfilters von seinen Mitarbeitern einzuholen. Es stellt sich insoweit die Frage, ob der Arbeitgeber sich in derartigen Fällen durch den Einsatz von Spamfiltern am Arbeitsplatz aufgrund eines Verstoßes gegen das Post- und Fernmeldegeheimnis strafbar machen kann.

## II. Begriffsherkunft

Zunächst ein kurzer Rückblick auf die Herkunft des Begriffes „Spam": Ursprünglich war der Begriff „Spam" die Markenbezeichnung eines Dosenfleisches („Spam" = spiced ham"). Dosenfleisch war überall erhältlich und deren Qualität oft minderwertig, daher verwendete man den Begriff zunehmend im Sinne eines Synonyms für überflüssige Dinge. Zu dieser Bedeutungswandlung des Wortes „Spam" trug bei, dass die Comedian-Gruppe Monty Python in einem Sketch aus dem Jahre 1970 das Wort „Spam" ständig wiederholend ironisch verwendete, da eine Speisekarte eines Bistros ausschließlich „Spam" – Gerichte aufwies. Die erste „Spam" im Sinne einer „überflüssigen" E-Mail soll Herr Tuerk 1978 versendet und dadurch einen Umsatz für das angebotene Produkt von 12-14 Millionen Dollar erzielt haben.[1] Die Freude des Spamversenders ist das Leid des Spamempfängers. Kürzlich hat das US-Bundesgericht zwei bekannte Spamversender, Sanford Wallace und Walter Rines, für die Versendung von Spams an das Internetportal „MySpace" zu $ 230 Mio. USD verurteilt.[2] Spamfilter versuchen nun durch unterschiedlichste Methoden, unerwünschte Spams von erwünschten Nachrichten zu unterscheiden. Die einfachste Form einer Filterung ist die Durchsuchung der Nachricht nach bestimmten Signalwörtern in schwarzen Listen („Blacklists"). Erscheint das Wort in der Nachricht, wird die Nachricht als Spam ausgesondert. Komplexere, heute gebräuchliche Filter weisen einer Nachricht aufgrund verschiedener Merkmale eine Wahrscheinlichkeit für das Vorliegen eines Spams zu. Derartige Merkmale können beispielsweise sein, dass eine E-Mail auf html-Seiten verweist, sie selbstextrahierende Programme enthält (bspw. Dateien mit den Endungen exe, bat, com), sie typische Spam-Formate oder bestimmte Begriffe aufweist etc. Erreicht oder überschreitet die Nachricht anhand dieser Merkmale einen festgelegten Wert („Score"), wird sie von dem Filter als Spam ausgesondert. Das Problem bei einer derartigen Filterung stellt in erster Linie nicht die Entfernung unerwünschter Spams dar, sondern die fehlende Weiterleitung tatsächlich erwünschter Nachrichten („false positives"). Wenn der Arbeitnehmer deshalb aufgrund einer beispielsweise besonders strengen

1 Vgl. Spiegel-Online, „Der erste Spammer verdiente zwölf Millionen Dollar – mit einer E-Mail" vom 1. 5. 2008; Tagesschau vom 3. 5. 2008, http://www.tagesschau.de/schlusslicht/spam2.html (Stand: 20. 6. 2008).

2 Vgl. Spiegel-Online, „230 Millionen Dollar Entschädigung für MySpace wegen Spam-Flut", http://www.spiegel.de/netzwelt/web/0,1518,553116,00.html (Stand: 20. 6. 2008).

Filterung durch den Arbeitgeber wünscht, dass seine E-Mails nicht bzw. jedenfalls nicht in dieser Weise gefiltert werden, stellt sich die Frage nach der Rechtmäßigkeit des Einsatzes von Spamfiltern durch den Arbeitgeber.

## III. Kann der Einsatz von Spamfiltern strafbar sein?

### 1. Beschluss des OLG Karlsruhe vom 10. 1. 2005

Spätestens nach einem im Jahre 2005 ergangenen Beschluss des OLG Karlsruhe[3] wird in der Fachliteratur intensiv darüber diskutiert, ob der Einsatz von Antispam-Software strafbar sein kann. Was war Hintergrund des Beschlusses? Ein Diplom-Informatiker zeigte den Dekan seiner Universität an. Der Dekan habe ihm das Privileg entzogen, die Kommunikationseinrichtungen der Fakultät zu benutzen. Danach habe er mit Dozenten, anderen Wissenschaftlern und Freunden an der Fakultät nicht mehr per E-Mail kommunizieren können. Die entsprechenden E-Mails seien ausgefiltert worden. Die Filterung soll zum Beispiel solche E-Mails gesperrt haben, in deren Absenderadresse sein Name vorgekommen sei. Die Sperrung habe zum anderen E-Mails betroffen, die von Fakultätskollegen an ihn gesendet worden seien, d. h. bei denen er Empfänger gewesen, auf dem Verteiler gestanden oder im Betreff erwähnt worden sei. Die Fakultätskollegen seien weder zuvor befragt noch informiert worden.[4] Das OLG Karlsruhe war der Auffassung, die Staatsanwaltschaft habe zu Unrecht von der Einleitung eines Ermittlungsverfahrens abgesehen. Es liege ein hinreichender Verdacht der Verletzung des Post- und Fernmeldegeheimnisses (§ 206 Abs. 2 Nr. 2 StGB) vor. Die E-Mails seien der Universität i. S. d. § 206 Abs. 2 Nr. 2 StGB anvertraut gewesen. Unter Hinweis auf *Heidrich/Tschoepe*[5] vertrat das OLG Karlsruhe die Ansicht, ein Gewahrsam an einer E-Mail liege spätestens dann vor, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht und der versendende Mailserver die Daten dem empfangenden Server übermittelt habe. Das Tatbestandsmerkmal des Unterdrückens der E-Mail sei anzunehmen, wenn durch Eingriffe in den technischen Vorgang des Aussendens, Übermittelns oder Empfangens von Nachrichten mittels TK-Anlagen verhindert wird, dass die Nachricht ihr Ziel vollständig oder unverstümmelt erreicht.[6] Das Tatbestandsmerkmal „Unterdrücken" werde jedenfalls durch eine Ausfilterung der E-Mail erreicht. In diesem Fall finde die Weiterleitung, also das Übermitteln der eingehenden Mail vom Mailserver an den Empfänger nicht statt. Ein Einverständnis, das dem Tatbestandsmerkmal einer „unbefugten" Unterdrückung entgegenstehen würde, könne nur dann von Bedeutung sein, wenn es von allen an dem konkreten Fernmeldeverkehr Beteiligten erteilt wird. Unter Umständen könne es zwar nach den allgemeinen Rechtfertigungsgründen gerechtfertigt sein, eine E-Mail herauszufiltern, wenn eine E-Mail mit Viren behaftet sei, sodass bei deren Verbreitung Störungen oder Schäden der TK- und Datenverarbeitungssysteme eintreten. Anhaltspunkte für eine solche Rechtfertigung fehlten allerdings. Die weiteren Ermittlungen hätten demgemäß festzustellen, ob es einen konkreten Anlass gegeben habe zu befürchten, dass die E-Mails eine Störung oder einen Schaden in dem TK-System der Universität hätten auslösen können.

### 2. Meinungen in der Literatur

Die Entscheidung wurde in der Literatur überwiegend dahingehend interpretiert, dass bei jedem Einsatz eines Spamfilters die Gefahr eines strafrechtlich relevanten Verhaltens bestehen kann. Man warnte davor, einen Spamfilter ohne eine Einwilligung des Nutzers einzusetzen. Ein Provider müsse beim Einsatz eines Spamfilters für eine Einwilligung des Nutzers sorgen. Auch ein Arbeitgeber könne sich strafbar machen, wenn er ohne Einwilligung seiner Arbeitnehmer Spamfilter in seinem Unternehmen einsetze. Andernfalls seien die Straftatbestände der §§ 206 Abs. 2 Nr. 2 StGB bzw. 303 a StGB verletzt. Hierzu im Einzelnen:

#### *a) Strafbarkeit des Einsatzes von Spamfiltern aus § 206 Abs. 2 Nr. 2 StGB*

Der Einsatz von Spamfiltern könnte gem. § 206 Abs. 2 Nr. 2 StGB strafbar sein. Das setzt voraus, dass der Arbeitgeber ein Unternehmen ist, das eine ihm anvertraute Sendung unterdrückt.

aa) Es stellt sich zunächst die Frage, ob der Arbeitgeber ein Unternehmen im Sinne des § 206 StGB ist. Das setzt voraus, dass er geschäftsmäßig Telekommunikationsdienste erbringt. Gestattet der Arbeitgeber seinen Mitarbeitern die private Nutzung seiner Telekommunikationseinrichtung, fungiert er als Diensteanbieter im Sinne von § 3 Nr. 6 TKG. Denn das Tatbestandsmerkmal der „geschäftsmäßigen Nutzung" ist weit auszulegen und erfasst jede Betätigung, die nicht ausschließlich hoheitliche Ziele verfolgt.[7] Ein geschäftsmäßiger Telekommunikationsdienst erfordert ferner keine Gewinnerzielungsabsicht. Es genügt, wenn ein Drittbezug hergestellt wird in der Weise, dass der Anbieter die Telekommunikationseinrichtung nicht nur für interne Zwecke unterhält. Ein solcher Drittbezug liegt nach ganz überwiegender Auffassung bei der Erlaubnis einer privaten E-Mail-Korrespondenz durch den Arbeitgeber vor, wobei auch eine stillschweigende Duldung der Privatnutzung ausreicht.[8] Der Arbeitgeber ist daher bei einer ausdrücklichen oder stillschweigenden Duldung der privaten Nutzung des E-Mail-Programmes durch seine Arbeitnehmer ein Unternehmen im Sinne des § 206 Abs. 2 Nr. 2 StGB. Demgegenüber ist bei einem Verbot der privaten Nutzung dienstlicher E-Mail-Programme eine Strafbarkeit gem. § 206 Abs. 2 Nr. 2 StGB mangels Unternehmereigenschaft von vornherein ausgeschlossen.[9]

bb) Umstritten ist ferner die Frage, ob eine E-Mail eine Sendung im Sinne des § 206 StGB sein kann. Dies wird zum Teil verneint, weil eine E-Mail keine verschlossene Sendung sei. § 206 Abs. 2 Nr. 1 StGB erfordere eine „verschlossene" Sendung. Der Tatbestand des § 206 Abs. 2 Nr. 2 StGB beziehe sich ausdrücklich auf dieses Tatbestandsmerkmal und verlange daher ebenfalls das Vorlie-

3 OLG Karlsruhe, 10. 1. 2005 – 1 Ws 152/04, K&R 2005, 181.
4 OLG Karlsruhe, 10. 1. 2005 – 1 Ws 152/04, K&R 2005, 181.
5 *Heidrich/Tschoepe*, MMR 2004, 75, 77.
6 Unter Hinweis auf: *Schönke/Schröder*, Strafgesetzbuch, 27. Aufl. 2006, § 206 Rn. 20; *Heidrich/Tschoepe*, MMR 2004, 75 ff., 78.
7 Herrschende Meinung, vgl. *Altenhain*, in: Münchener Kommentar, StGB, Bd. 3, 2003, § 206, Rn. 13.
8 U. a. *Büchner*, in: BK-TKG, 3. Aufl. 2006, § 85 Rn. 4; *Hoeren*, NJW 2004, 3513; 17. Tätigkeitsbericht der Hessischen Landesregierung, RDV 2005, 132, 133; jeweils m. w. N.
9 *Köcher*, DuD 2005, 165.

gen einer „verschlossenen Sendung".[10] Dieser Auffassung ist entgegenzuhalten, dass die Voraussetzung des „Verschlossenseins" einer Sendung im Sinne des § 206 Abs. 2 Nr. 1 StGB vor dem Hintergrund des Schutzzweckes der Norm erforderlich ist; diese schütze nämlich vor einer Öffnung oder der Kenntnisnahme der Sendung. § 206 Abs. 2 Nr. 2 StGB sichert demgegenüber jede „Übermittlung" der Sendung, die ein „Verschlossensein" der Sendung gerade nicht erfordert. Es ist folgerichtig nach der – wohl überwiegend vertretenen Auffassung – jeder Gegenstand unabhängig von seiner Verkörperung und der „Verschlossenheit" eine Sendung im Sinne des § 206 Abs. 2 Nr. 2 StGB.[11]

cc) Folgt man der Auffassung, dass auch eine E-Mail eine „Sendung" gem. § 206 Abs. 2 Nr. 2 StGB sein kann, ist fraglich, wann eine E-Mail gem. § 206 Abs. 2 Nr. 2 StGB „anvertraut" ist. Dies ist wohl dann der Fall, wenn die Sendung wie vorgesehen in den Verkehr gelangt und der versendende Mailserver dem empfangenen Server die Daten übermittelt hat[12]. Richtig ist wohl konsequenterweise dann, dass eine E-Mail nicht wie vorgesehen in den Verkehr gelangt ist, wenn ihr die technischen Grundlagen zur Versendung an einen Adressaten fehlen[13], sie also völlig wahllos verschickt wird. Eine Ausfilterung solcher völlig wahllos versendeter Spams verletzt daher schon mangels eines Anvertrautseins der Sendung nicht § 206 Abs. 2 Nr. 2 StGB. Darüber hinaus ist der Auffassung zuzustimmen, dass solche E-Mail-Sendungen nicht im Sinne des § 206 Abs. 2 Nr. 2 StGB anvertraut sind, wenn sie bewusst zur Verbreitung von unerwünschter Werbung oder sonstigen Zuschriften verschickt werden. Denn ein Versender solcher E-Mails kann nicht in schutzwürdiger Weise darauf vertrauen, dass seine Spam-E-Mails ihren Empfänger erreichen[14]. Es verbleiben nach allem allerdings jedenfalls diejenigen E-Mail-Sendungen innerhalb einer gestatteten oder geduldeten Privatkorrespondenz, die der Versender nicht als Spam verschickt und der Filter dennoch (fälschlicherweise) als Spam ausfiltert („false positive"). Jedenfalls solche Sendungen sind im Sinne des § 206 Abs. 2 Nr. 2 StGB anvertraut. Eine fälschliche Unterdrückung ordnungsgemäß versandter E-Mails lässt sich aber bei dem Einsatz von Spamfiltern am Arbeitsplatz nicht vermeiden.

dd) Der Tatbestand des § 206 StGB verlangt indes außerdem, dass die anvertraute Sendung „unbefugt" unterdrückt wurde. Bei dem Tatbestandsmerkmal handelt es sich um ein allgemeines Rechtswidrigkeitsmerkmal.[15] Eine Einwilligung schließt demzufolge als Einverständnis bereits die Tatbestandsmäßigkeit aus.[16] Berechtigt zu einer Einwilligung in die Löschung der E-Mail ist der Empfänger der E-Mail.[17] Dies ist zunächst der Arbeitgeber. Der Arbeitgeber wird in aller Regel in die Spamfilterung durch den Provider entweder ausdrücklich oder jedenfalls konkludent dadurch einwilligen, dass er das E-Mail-Programm in Kenntnis der vorgesehenen Filterung nutzt. Der Arbeitnehmer jedoch hat keine eigenen vertraglichen Beziehungen zum Provider. Er selbst kennt den Provider und den eingesetzten Spamfilter im Zweifel nicht. Gleiches gilt, wenn der Arbeitgeber zwar die technische Umgebung (als Provider) stellt – und dem Mitarbeiter zur privaten Nutzung überlässt –, er den Arbeitnehmer allerdings nicht ausreichend über einen Spamfiltereinsatz aufklärt und erst recht keine ausdrückliche Einwilligung zum Einsatz des eingesetzten Filters einholt. Es ist sehr fraglich, ob in derartigen Fällen ein die Tatbestandsmäßigkeit ausschließendes Einverständnis des Arbeitnehmers zur Filterung seiner privat verschickten E-Mails durch einen Spamfilter unterstellt werden kann. Fehlt es an einer ausdrücklichen Einwilligung des Arbeitnehmers, was vor allem bei der schlichten stillschweigenden Duldung der Privatnutzung der Fall ist, wird von einigen Stimmen in der Literatur pauschal die Gefahr eines strafrechtlich relevanten Verhaltens des Arbeitgebers konstatiert. Allenfalls für potentiell virenbehaftete E-Mails könnte eine konkludente Einwilligung des Arbeitnehmers angenommen werden.[18] Diese auf potentiell virenbehaftete begrenzte Annahme einer konkludenten Einwilligung ist zwischenzeitlich meines Erachtens überholt. Jeder Nutzer weiß heutzutage, dass die Verwendung von E-Mail-Programmen ohne den Einsatz von Spamfiltern technisch de facto nicht mehr möglich ist. Ferner bleiben meines Erachtens bei einer derart pauschalen Betrachtungsweise außerdem die spezifischen Gegebenheiten des Arbeitsverhältnisses außer acht. Denn eine ausdrückliche bzw. stillschweigende Duldung der Privatnutzung von E-Mail-Programmen kann in einem Arbeitsverhältnis grundsätzlich nur im Rahmen des existierenden technischen Systems des Arbeitgebers erfolgen. Ein Recht auf private Nutzung der TK-Anlage besteht unbestritten nicht. Der Arbeitnehmer kann also – auch bei einer ausdrücklich oder stillschweigend geduldeten – Privatnutzung des E-Mail-Programms vom Arbeitgeber nicht eine „spamfilterfreie" TK-Anlage verlangen. Um einen Vergleich zu bemühen: Erhalten Arbeitnehmer Dienstwagen auch zum privaten Gebrauch, ist die Nutzung auf das zur Verfügung gestellte Fahrzeug beschränkt. Der Arbeitnehmer willigt in diesem Fall konkludent ein, in ein Dieselfahrzeug kein Benzin einzufüllen. Er ist zur Verwendung des Dieselkraftstoffes angesichts seiner Schadensabwendungspflicht sogar verpflichtet.[19] Der Arbeitnehmer geht schließlich aufgrund der allgemein bekannten Vielzahl von Spamattacken davon aus, dass ein E-Mail-Programm des Arbeitgebers selbstverständlich eine Filterung aller E-Mails vorsehen muss; jeder Arbeitnehmer der einen Computer nutzt, wird sich der Problematik uferlos eingehender Spamsendungen bewusst sein. Es wäre heute lebensfremd anzunehmen, einem Arbeitnehmer sei bei der Nutzung der TK-Anlage des Arbeitgebers nicht bekannt, dass ein ungefilterter E-Mail-Zugang in kurzer Zeit dazu führen würde, dass der E-Mail-Verkehr im Unternehmen zusammenbricht. Nutzt der Arbeitnehmer also in Kenntnis dieser Umstände die IT-Umgebung des Arbeitgebers zur privaten Nutzung des E-Mail-Programmes, nimmt er die Filterung seiner privaten E-Mail-Korrespondenz jedenfalls konkludent in Kauf. *Stenzel*[20] ist in diesem Zusammen-

10 *Schönke/Schröder* (Fn. 6), § 206 Rn. 20.
11 *Schönke/Schröder* (Fn. 6), § 206, Rn. 20; *Schmidl*, DuD 2005, 269; *Spindler/Ernst*, CR 2004, 437, 439, jeweils m. w. N.
12 *Schmidl*, DuD 2005, 269; *Hoyer*, in: Systematischer Kommentar StGB, Losebl.-Ausg., § 206 Rn. 26.
13 Sog. RFC (Requests For Comments )-Konformität, vgl. erläuternd u. a. http://www.heise.de/glossar/entry/d21c51387a35bd3c (Stand: 19. 6. 2008); *Heidrich/Tschoepe*, MMR 2004, 75, 77.
14 *Schmidl*, DuD 2005, 270.
15 *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 206 Rn. 9.
16 *Schönke/Schröder* (Fn. 6), § 206 Rn. 11.
17 *Kitz*, CR 2005, 450, 453; *Köcher*, DuD 2005, 163, 165.
18 Vgl. u. a. *Hoeren*, NJW 2004, 3513; *Schmidl*, DuD 2005, 267, 271; *Heidrich/Tschoepe*, MMR 2004, 75, 78, jeweils mit weiteren Nachweisen.
19 ErfK-*Preis*, 8. Aufl. 2008, § 611 BGB Rn. 744.
20 *Stenzel*, MMR 8/2004, S. X.

hang beizupflichten: Es wäre eine „sonderbare Friktion, unerwünschte E-Mail-Werbung zivilrechtlich als unzumutbare, rechtswidrige Belästigung einzustufen, aus strafrechtlicher Sicht jedoch anzunehmen, der Adressat sei mit der Abhilfe (z. B. mittels Spam-Filter der Providers) nicht einverstanden".[21]

Auch der Beschluss des OLG Karlsruhe[22] steht dieser Auffassung nicht entgegen. In der vom OLG Karlsruhe zu bewertenden besonderen Fallgestaltung hatte der Arbeitgeber bewusst einen Mitarbeiter von der Kommunikation ausgeschlossen und den Spamfilter offenbar zielgerichtet auf diesen Mitarbeiter eingestellt. Dass eine solche zielgerichtete Filterung über eine übliche, vom Arbeitnehmer als Selbstverständlichkeit zur Gefahrenabwehr hinzunehmende Spamfilterung hinausgeht und nicht von seiner konkludenten Einwilligung umfasst sein kann, liegt auf der Hand. Jedenfalls solange der Arbeitgeber die Filterung der E-Mails auf den üblichen (vom Arbeitnehmer zu erwartenden) Rahmen beschränkt, ist meines Erachtens allerdings eine konkludente Einwilligung des Arbeitnehmers anzunehmen.

ee) Der Einsatz eines Spamfilters kann überdies nach den allgemeinen Grundsätzen des rechtfertigenden Notstandes straffrei bleiben. Ob überhaupt ein allgemeiner Rechtfertigungsgrund bei § 206 StGB eingreifen kann, ist zwar umstritten.[23] Ein allgemeiner Rechtfertigungsgrund durch Notstand liegt nach der auch vom OLG Karlsruhe vertretenen Auffassung (vgl. III. 1.) jedoch jedenfalls dann vor, wenn die ausgefilterte E-Mail Viren und/oder sonstige schädliche Programme enthält.[24] Auch insoweit ist meines Erachtens zu berücksichtigen, dass inzwischen angesichts der in den letzten Jahren nochmals explosionsartig angestiegenen Spamflut die Unterhaltung einer TK-Anlage grundsätzlich sinnvollerweise nur möglich ist, wenn der Verwender einen ausreichend effektiven Spamschutz einsetzt. Eine Eingrenzung des rechtfertigenden Notstandes auf ersichtlich schädliche, virenbehaftete E-Mails greift daher zu kurz; denn eine ungehinderte Spamflut kann heute technisch in gleicher Weise schädlich für eine TK-Anlage sein wie ein Virus. Das bestätigen anschaulich die immer wieder notwendigen Abschaltungen von E-Mail-Servern, wenn der Provider der einsetzenden Spamflut nicht Herr wird. Unter diesem Gesichtspunkt ist der Einsatz eines marktüblichen Spamfilters als gebotenes und damit verhältnismäßiges Verhalten des Arbeitgebers nach den allgemeinen Grundsätzen des rechtfertigenden Notstandes gerechtfertigt.

*b) Strafbarkeit des Einsatzes von Spamfiltern aus § 303 a StGB*

Neben einer möglichen Strafbarkeit aus § 206 Abs. 2 Nr. 2 StGB kommt eine Strafbarkeit gem. § 303 a StGB in Betracht, wenn Daten durch die Filterung rechtswidrig gelöscht, unterdrückt, unbrauchbar gemacht oder verändert werden. E-Mails sind Daten, die im Sinne des § 202 a Abs. 2 StGB – auf den § 303 a StGB unmittelbar verweist – „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden". Der Bestimmtheitsgrundsatz aus Art. 103 Abs. 2 GG gebietet es, dass nicht jede Datenveränderung strafrechtlich relevant sein kann. Infolgedessen müssen die Daten fremd sein. Dies ist dann der Fall, wenn eine andere Person ein unmittelbares Recht auf Verarbeitung, Löschung oder Nutzung hat.[25] Erst wenn also eine private Nachricht im „Postfach" des Arbeitnehmers liegt, ist eine Löschung der E-Mail ohne oder gegen den Willen des Arbeitnehmers tatbestandlich gem. § 303 a StGB relevant.[26] Allerdings bedürfte eine Löschung der ausdrücklich bzw. stillschweigend geduldeten privaten Korrespondenz des Arbeitnehmers wiederum einer rechtfertigenden (konkludenten) Einwilligung oder eines rechtfertigenden Notstandes. Hierzu verweisen wir auf die Ausführungen zu § 206 Abs. 2 Ziff. 2 StGB.[27]

## IV. Zusammenfassung und praktische Hinweise zur Verwendung von Spamfiltern am Arbeitsplatz

Nach allem ist nach den hier dargestellten Grundsätzen bei der Verwendung von Spamfiltern am Arbeitsplatz auf Folgendes zu achten:

1. Verbietet der Arbeitgeber die private Nutzung der betrieblichen E-Mail-Programme, ist eine Strafbarkeit gem. § 206 Abs. 2 Nr. 2 StGB und § 303 a StGB nach der wohl überwiegenden Auffassung ausgeschlossen. Der Arbeitgeber erbringt schon keine geschäftsmäßigen Post- oder Telekommunikationsdienste gegenüber seinem Arbeitnehmer im Sinne des § 206 Abs. 1 StGB. Da die Daten rein dienstlicher E-Mails außerdem im Sinne des § 303 a StGB dem Arbeitgeber „gehören", werden durch eine Filterung durch den Arbeitgeber ferner keine fremde Daten gelöscht oder unterdrückt, so dass der Arbeitgeber sich auch nicht gem. § 303 a StGB strafbar macht.

2. Wenn der Arbeitgeber die private Nutzung der betrieblichen E-Mail-Programme ausdrücklich bzw. stillschweigend duldet – oftmals lässt sich in einem Unternehmen mit einer modernen IT-Umgebung eine Privatnutzung nicht ernsthaft verbieten – ist Folgendes zu beachten:

a) Es ist grundsätzlich empfehlenswert, eine ausdrückliche Einwilligung des Arbeitnehmers durch eine arbeitsvertragliche und/oder betriebliche Vereinbarung einzuholen. Eine ausdrückliche Einwilligung hat nicht nur den Vorteil, dass die Gefahr eines ggf. strafrechtlich relevanten Verhaltens dadurch vermieden wird. Der Arbeitgeber ist bei einer ausdrücklichen Regelung zudem auch in der Lage, die Grenzen der privaten Nutzung eindeutig festzulegen. Aus Sicht des Arbeitgebers sollte er in einer solchen ausdrücklichen Einwilligung im Arbeitsvertrag oder arbeitsvertraglichen Ergänzungen jede Form der Filterung möglichst weitgehend erfassen. Für einen zukünftig vorbehaltenen Widerruf einer gestatteten Privatnutzung sollte er unter Berücksichtigung der Entscheidung des BAG vom 11. 10. 2006[28] konkrete Widerrufsgründe nennen. Der Einsatz eines marktüblichen Spamfilters ist darüber hinaus nach der hier vertretenen Auffassung grundsätzlich nicht mit strafrechtlichen Risiken verbunden. Der

21 Zu der Problematik im Zusammenhang mit Kontrollmöglichkeiten bei privater Internetnutzung am Arbeitsplatz vgl. *Rath/Karner*, K&R 2007, 446.
22 OLG Karlsruhe, 10. 1. 2005 – 1 Ws 152/04, K&R 2005, 181 m. w. N.
23 *Fischer* (Fn. 15), § 206 Rn. 9.
24 OLG Karlsruhe, 10. 1. 2005 – 1 Ws 152/04, K&R 2005, 181; 17. Tätigkeitsbericht der Hessischen Landesregierung, RDV 2005, 132, 133; *Schmidl*, DuD 2005, 269, 271, jeweils m. w. N.
25 *Fischer* (Fn. 15), § 303 a, Rn. 4.
26 *Fischer* (Fn. 15), § 303 a, Rn. 7.
27 S.o. Ziff. 3 lit. a.
28 BAG, 11. 10. 2006 – 5 AZR 721/05, NZA 2007, 87.

Arbeitnehmer willigt regelmäßig (konkludent) in den Gebrauch eines marktüblichen Spamfilters – auch hinsichtlich seiner privaten E-Mail-Korrespondenz – allein schon dadurch ein, dass er in Kenntnis der heute notwendigen und selbstverständlichen Spamfilterung das System des Arbeitgebers nutzt. Ferner ist der Einsatz marktüblicher Spamfilter nach der hier vertretenen Auffassung in gleicher Weise gerechtfertigt wie der Einsatz von Virenfiltern. Allerdings ist zu empfehlen, den Arbeitnehmer auf die Nutzung des Spamfilters vorsorglich deutlich hinzuweisen. Denn jedenfalls dann kann der Arbeitnehmer nicht mehr behaupten, er habe vor der Nutzung der IT-Anlage des Arbeitgebers nichts von einer Spamfilterung gewusst. Es reicht meines Erachtens ein allgemeiner Hinweis, in etwa: „Wir nutzen zum Schutz unserer TK-Anlage einen Spamfilter, derzeit ... Der Spamfilter wird an den jeweils aktuellen Stand der Technik angepasst. Bitte beachten Sie, dass generell jede E-Mail-Korrespondenz anhand dieses Filters überprüft wird." Alternativ kann eine sog. Quarantänelösung eingesetzt werden. Die vermeintlichen Spam-E-Mails werden nicht gelöscht, sondern in einem gesonderten Ordner bereitgehalten.[29] Nicht ohne ausdrückliche Zustimmung des Arbeitnehmers erlaubt ist demgegenüber auch nach der hier vertretenen Auffassung eine darüber hinausgehende, insbesondere zielgerichtete Filterung der privaten E-Mail-Korrespondenz des Arbeitnehmers durch den Arbeitgeber.

b) Zu beachten ist außerdem: Besteht im Unternehmen ein Betriebsrat und ist eine Privatnutzung von E-Mails gestattet, ist der bloße providergestützte Einsatz von Viren- und Spamfiltern nach überwiegender und zutreffender Auffassung nicht mitbestimmungspflichtig. Dies jedenfalls dann, wenn der Scan automatisiert abläuft und ein Kontrollvorgang durch den Arbeitgeber ausgeschlossen ist.[30]

Wenn der Einsatz des Spamfilters demgegenüber durch besondere technische Gegebenheiten objektiv[31] geeignet ist, eine technische Überwachung des Mitarbeiterverhaltens durch den Arbeitgeber zu ermöglichen, sei es durch Protokolldateien[32], sei es dass der Arbeitgeber selbst als Provider alle technischen Mittel als Provider zur Verfügung stellt oder aus sonstigen Gründen die Nutzung kontrollieren kann[33], hat der Betriebsrat ein Mitbestimmungsrecht. In diesem Fall sollte der Arbeitgeber sowohl die Grenzen der Privatnutzung des Arbeitnehmers als auch den Einsatz von Spamfiltern in einer Betriebsvereinbarung regeln.

29 *Lenhardt*, DuD 2003, 487, 489.
30 *Fitting*, Betriebsverfassungsgesetz, 24. Aufl. 2008, § 87 Rn. 245; *Beckschulte*, DB 2007, 1526.
31 BAG, 29. 6. 2004, AP Nr. 41 zu § 87 BetrVG 1972 Überwachung.
32 *Lenhardt*, DuD 2003, 487, 489.
33 *Rath/Karner*, K&R 2007, 446, 448.

Von Wiss. Mitarb. Miriam Ballhausen und Wiss. Mitarb. Rechtsanwalt Jan Dirk Roggenkamp, Universität Passau
Mehr über die Autoren erfahren Sie auf S. XI, XII.

# Personenbezogene Bewertungsplattformen

Welches Handy soll ich kaufen, welches Buch ist lesenswert? Häufig geben Bewertungen im Internet den Ausschlag bei Kaufentscheidungen. In den USA bereits seit langem gang und gäbe, etablieren sich zunehmend Bewertungsplattformen, auf denen nicht nur Produkte und Dienstleistungen, sondern auch Personen bewertet werden können. Sehr zum Unmut der Datenschutzbeauftragten und natürlich der betroffenen Personen selbst. Erste Bußgeldbescheide sind bereits erlassen, eine ganze Reihe Verfahren vor den Gerichten anhängig. Der folgende Beitrag beleuchtet das Phänomen dieser – auch „Social Scoring Plattformen" genannten – personenbezogenen Bewertungsplattformen.

## I. Typologie der Bewertungsplattformen

Bewertungsplattformen sind so unterschiedlich wie ubiquitär. Eine erste grobe Typologisierung der verschiedenen, hinter den Plattformen stehenden Geschäftsmodelle lässt sich anhand des jeweiligen Bewertungsgegenstands vornehmen. Zunächst ist zwischen Produkt- und Personenbewertungsplattformen zu unterscheiden. Erstere sind hinreichend bekannt und Gegenstand juristischer Erörterungen gewesen.[1] Inzwischen findet sich in jedem größeren Online-Shop ein Feature, mittels welchem Kunden (und teilweise auch jedermann) eine „Rezension"[2] verfassen können, die mit einer Vergabe von null bis fünf Sternchen gekrönt wird, und gewissermaßen als Fazit des „Rezensenten" für die mehr oder weniger ausführliche Beschreibung der Erfahrungen und Eindrücke in Bezug auf den Bewertungsgegenstand gilt. Vergleichsweise neu[3] auf dem deutschsprachigen Internetmarkt sind Personen- beziehungsweise personenbezogene Bewertungsplattformen.[4] Diese lassen sich in drei – in der Regel ineinander übergehende – Kategorien einteilen.

### 1. Dienstleistungsbewertungen

Dienstleistungsbezogene Bewertungsplattformen beziehen sich ausschließlich auf eine konkrete Tätigkeit des Erbringers einer Dienstleistung. Die Bewertung der hinter der Dienstleistung stehenden Person ist sekundär und be-

1 Vgl. z. B. *Schmitz/Laun*, MMR 2005, 208 – 213.
2 So die Bezeichnung des Online-Buchhändlers amazon.de – eine Reminiszenz an die Ursprünge als reiner Online-Buchladen.
3 So wurde die Produktbewertungsplattform ciao.de bereits 1999 gelauncht.
4 Bisweilen auch „Social Scoring"-Plattformen genannt, vgl. *Scherzer*, jurisPR-ITR 13/08, Anm. 2; *Krieg*, jurisPR-ITR 13/08, Anm. 3; *Hecht*, Freilaw 2/2008, S. 1.