

# **Rechtliche Rahmenbedingungen für Provider beim Filtern, Scannen und Löschen von Spam, Späh- und Schadsoftware**

## **Gutachten**

**eco – Verband der deutschen Internetwirtschaft e.V.**

**Verfasser: RA Ivo Ivanov**

## INHALTSVERZEICHNIS

<b>I. EINLEITUNG</b>	<b>4</b>
<b>II. ANSPRÜCHE DES PROVIDERS GEGEN DEN VERBREITER VON SPAM, SPYWARE ODER MALWARE.</b>	<b>4</b>
<b>III. TECHNISCHE MAßNAHMEN DER PROVIDER</b>	<b>6</b>
<i>1. Blacklists</i>	6
<i>2. Dateianhänge</i>	7
<i>3. Header-Analyse</i>	7
<i>4. Text-Analyse</i>	7
<b>IV. RECHTLICHE GRUNDLAGEN</b>	<b>8</b>
<i>1. Strafrechtliche Risiken</i>	9
a. Verletzung des Post- und Fernmeldegeheimnisses (§ 206 StGB)	9
aa. „Sendung“. Die E-Mail als Brief	9
bb. „Zur Übermittlung anvertraut“	11
cc. „Unbefugte Unterdrückung“	13
aaa. Tatbestandsausschließendes Einverständnis des Kunden in dem Vertrag mit dem Provider	14
bbb. Mutmaßliches Einverständnis des Kunden in das Filtern bzw. Blocken	17
dd. Rechtswidrigkeit	18
aaa. Rechtfertigung nach dem TKG	18
bbb. Rechtfertigung nach den allgemeinen Rechtfertigungsgründen	20
b. Datenunterdrückung (§ 303a StGB)	21
c. Ausspähen von Daten (§ 202a StGB)	23
d. Zwischenergebnis	23
<i>2. Datenschutzrechtliche Relevanz</i>	23
a. Eingriff in Datenschutzrechte	24
b. Rechtfertigung des Eingriffs in Datenschutzrechte	25
c. Zwischenergebnis	27
<i>3. Zivilrechtliche Überlegungen</i>	27
a. Pflicht zur Filterung	28
b. Recht zur Filterung	29
c. Lösungsrechte und Benachrichtigungspflichten	30
d. Umgang mit Blacklists	32
<b>V. BEWERTUNG EINZELNER KONSTELLATIONEN UND FRAGEN AUS DER PRAXIS</b>	<b>33</b>

<i>1. Muss der Provider auf Informationen von „außen“ über die in seinem System angesiedelten Botnetze oder die über seine Systeme verbreiteten Phishing-E-Mails reagieren?</i>	33
<i>2. Wann liegt „Kenntnis“ von dem Missbrauch im vorgenannten Sinne vor?</i>	34
<i>3. Wer kann „Kenntnis“ von dem Missbrauch verschaffen?</i>	35
<i>4. Welche Maßnahmen sind zu ergreifen?</i>	35
<i>5. Darf prophylaktisch nach Botnetzen gesucht werden?</i>	36
<b>VI. ZUSAMMENFASSENDE RECHTLICHE BEWERTUNG DER ABWEHRMAßNAHMEN</b>	<b>38</b>
<i>1. Zentrale Blockierung durch Blacklists</i>	38
<i>2. Filtern durch Analyse des Headers</i>	39
<i>3. Filtern durch Analyse des E-Mail-Textes oder des E-Mail-Anhanges</i>	39
<i>4. Löschen von E-Mails bzw. Mailanhängen</i>	40
<b>VII. AUSBLICK</b>	<b>41</b>

## I. Einleitung

Immer stärker wächst in der Gesellschaft das Bewusstsein, welche große Bedeutung den modernen elektronischen Kommunikationsnetzen und –diensten im Alltag zukommt – im Berufsleben wie auch zu Hause. Sollen die angebotenen Dienste in breitem Umfang genutzt werden, bedarf es vertrauenswürdiger, sicherer und zuverlässiger Technologien. Die Europäische Kommission hat in ihrer Mitteilung vom 15. November 2006 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen den privaten Sektor aufgefordert, Sicherheitslücken in Netzen und Informationssystemen, die zur Verbreitung von Spam und Schadsoftware genutzt werden können, zu schließen und weiterhin verstärkt auf Filterlösungen zu setzen<sup>1</sup>.

Das vorliegende Gutachten setzt sich mit den rechtlichen Fragen auseinander, die das Bekämpfen der Verbreitung von unerwünschter elektronischer Werbung (*Spam*), Spähsoftware (*Spyware*) und Schadsoftware (*Malware*) durch die Provider aufwirft.

## II. Ansprüche des Providers gegen den Verbreiter von Spam, Spyware oder Malware.

Benutzt ein Spammer zur Versendung der E-Mails unberechtigt fremde Mail-Server, so kommen seitens des Providers Unterlassungs- und Schadensersatzansprüche in Betracht. Die Nutzung fremder Ressourcen und Rechnerkapazitäten stellt eine rechtswidrige und

---

<sup>1</sup> Vgl. unter:

[http://ec.europa.eu/information\\_society/policy/ecomms/doc/info\\_centre/communic\\_reports/spam/com\\_2006\\_0688\\_f\\_de\\_acte.pdf](http://ec.europa.eu/information_society/policy/ecomms/doc/info_centre/communic_reports/spam/com_2006_0688_f_de_acte.pdf).

schuldhafte Eigentumsverletzung im Sinne des § 823 Abs. 1 BGB jedenfalls dann dar, wenn der Mail-Server infolge des erhöhten E-Mail-Aufkommens nicht mehr bestimmungsgemäß funktioniert. Der Missbrauch des Mail-Servers kann auch einen Anspruch wegen betriebsbezogenen Eingriffs in den ausgeübten und eingerichteten Gewerbebetrieb des Server-Betreibers auf Schadensersatz (§ 823 Abs. 1 BGB) sowie Unterlassen (§§ 823 Abs. 1, 1004 BGB analog) begründen. Es kommen auch in Betracht Ansprüche wegen vorsätzlich sittenwidriger Schädigung (§ 826 BGB) sowie aus § 823 Abs. 2 BGB, wenn Straftatbestände verwirklicht werden, die auch den Schutz des Providers bezwecken, beispielsweise das Erschleichen von Leistungen (§ 265a StGB), eine Datenveränderung (§ 303a StGB), Computersabotage (§303b StGB) oder eine Störung von Telekommunikationsanlagen (§ 317 StGB).

Darüber hinaus können auch Abwehransprüche aus Markenrecht geltend gemacht werden. Denn häufig benutzen Spammer gefälschte Absenderangaben und missbrauchen dazu vermehrt auch tatsächlich existierende Domains (z.B. [xy@hotmail.com](mailto:xy@hotmail.com), [xy@gmx.de](mailto:xy@gmx.de), [xy@web.de](mailto:xy@web.de), [xy@freenet.de](mailto:xy@freenet.de) etc.), deren Bezeichnungen in den meisten Fällen den Schutz von eingetragenen Marken genießen. Damit wird unter anderem versucht, die Abwehrmaßnahmen von Mailhosts zu konterkarieren, die bei eintreffenden E-Mails die Absender-Domain verifizieren und anderenfalls als Spam markieren. Es existieren mittlerweile Gerichtsurteile<sup>2</sup>, die die unberechtigte Verwendung der Marke eines Internetdienstleisters, die u.a. für Werbung und Marketing eingetragen ist, zur Bildung von E-Mail-Absenderadressen für Spam-E-Mails als markenrechtsverletzend angesehen und einen Unterlassungs- sowie Schadensersatzanspruch des Providers gegen den Versender zugesprochen haben.

---

<sup>2</sup> Vgl. OLG Karlsruhe, CR 2007, 105.

Die Durchsetzung der vorgenannten Ansprüche scheitert jedoch oft an der Anonymität der meistens in außereuropäischen Ländern sitzenden Versender, die damit für die deutsche Justiz kaum greifbar sind und an dem unverhältnismäßigen Rechercheaufwand. Die mögliche Lösung heißt daher: Filtersoftware, deren Einsatz jedoch oft ein erhebliches rechtliches Risiko für den Provider begründen kann.

### III. Technische Maßnahmen der Provider

Die Maßnahmen der Provider reichen von der Blockierung von Absenderadressen über die automatische Abweisung von E-Mails von offenen Relays oder Filtermaßnahmen bis zur Markierung nach Spam-Wahrscheinlichkeit und nachfolgender Zustellung oder auch Löschung.

Bevor eine rechtliche Beurteilung stattfinden kann, sind zunächst die verschiedenen technischen Möglichkeiten der Gestaltung und des Einsatzes von Filtersoftware darzustellen. Dabei ist zu unterscheiden, je nachdem ob der Einsatz beim Kunden selbst (client-based) oder beim Provider (server-based) erfolgt. Die unten benannten Techniken stellen die zur Zeit gängigsten dar, können dabei auch miteinander kombiniert werden, was in der Regel auch geschieht.

#### **1. Blacklists**

Der Absender kann anhand einer Blacklist als bereits bekannter Spammer identifiziert und seine Nachricht beim Eingang aussortiert werden. Dabei kann die komplette Domain des Absenders bzw. dessen IP-Adresse(n) schon beim Verbindungsaufbau blockiert werden. Das Blockieren einer ganzen Domain oder einer IP-Range führt natürlich oft dazu, dass auch die E-Mails anderer Nutzer derselben Absenderdomain verloren gehen.

Solange eine solche Blacklist von jedem Kunden individuell erstellt werden kann, erscheint es aus Sicht des Providers tatsächlich und auch rechtlich unproblematisch, da der Kunde selbst entscheiden kann und darf, wen er blockiert und wen nicht.

Entsteht hingegen die Blacklist auf Veranlassung des Providers oder gar auf Grund von Hinweisen Dritter, kann dies problematisch sein, denn der eine Adressat mag E-Mails einer bestimmten Firma für unerwünscht halten, für den anderen sind sie möglicherweise wichtige Kundenpost. Grundsätzlich sind Provider bereits vertraglich verpflichtet, E-Mails – und damit eigentlich auch SPAM-Mails – zuzustellen.

## **2. Dateianhänge**

E-Mail-Anhänge werden als häufiges Trägermedium für Computerviren im Rahmen einer Filterung auf bekannte, schädliche Strukturen untersucht. Oftmals wird bei Entdeckung nicht die gesamte E-Mail vernichtet, sondern allein der Anhang abgetrennt. Dadurch wird eine Kenntnisnahme vom Inhalt der E-Mail durch den Empfänger ermöglicht und diese nicht verändert. Allerdings existieren mittlerweile auch Viren, die in den HTML-Code einer so genannten formatierten Nachricht eingebunden und dort aktiviert werden können. Um diese Schädlinge aufzuspüren, genügt das Scannen des Anhangs nicht. Es erfordert vielmehr das Durchsuchen des Nachrichtentextes selbst.

## **3. Header-Analyse**

Filterprogramme untersuchen oft auch den E-Mail-Header auf Unstimmigkeiten. Werden solche aufgedeckt, kann davon ausgegangen werden, dass E-Mail-Adressen ge- oder verfälscht wurden.

## **4. Text-Analyse**

Schließlich lassen sich E-Mails auch auf anstößige oder eindeutig werbebezogene Textbausteine scannen. Dies geschieht zunächst im

Betreff aber auch innerhalb der Nachricht selbst. Um nach einschlägigen Schlagwörtern innerhalb des Textes zu suchen muss das Filterprogramm allerdings „Kenntnis“ vom Inhalt der Nachricht nehmen und sie (virtuell) öffnen. Gespeichert oder für den Provider und seine Mitarbeiter lesbar abgelegt werden die geöffneten Mails dabei jedoch nicht.

#### IV. Rechtliche Grundlagen

Nicht alle Abwehrmethoden sind rechtlich unbedenklich. Zu differenzieren ist zunächst, wonach gesucht wird: Spam oder Spyware und Malware. Des Weiteren ist zu differenzieren zwischen der Durchsuchung auf Merkmale (Filterung) und den weiteren Schritten wie dem Löschen, Blockieren, oder Umleiten in spezielle Ordner. Bei der Beurteilung der Zulässigkeit einzelner Maßnahmen sind die widerstreitenden Belange abzuwägen. Dabei kommen auf Seiten der Kunden vor allem das Telekommunikationsgeheimnis, das Persönlichkeitsrecht sowie das Datenschutzrecht zum Tragen. Die unterschiedlichen Schutzziele der Virenabwehr und der Spam-Bekämpfung stecken den Rahmen für zulässige Maßnahmen ab. Deshalb können zur Virenabwehr weiter reichende Maßnahmen zulässig sein, weil es sich dabei um notwendige Maßnahmen des Datenschutzes und der Datensicherheit zur Abwehr akuter Gefährdungen der Daten und der TK-Infrastruktur handelt, während die Bekämpfung von Spam zumeist dem Schutz vor Belästigung und Ressourcenverbrauch dient.

## **1. Strafrechtliche Risiken**

Einschlägige Strafnormen sind 206 Abs. 2 Nr. 2 StGB („Verletzung des Post- und Telekommunikationsgeheimnisses“) und § 303a Abs. 1 StGB („Datenveränderung“).

### **a. Verletzung des Post- und Fernmeldegeheimnisses (§ 206 StGB)**

Nach § 206 Abs. 2 Nr. 2 StGB macht sich nämlich strafbar, wer als Inhaber oder Beschäftigter eines Post- oder Telekommunikationsunternehmens *unbefugt* eine ihm zur Übermittlung *anvertraute Sendung* unterdrückt. Als Telekommunikationsunternehmen sind alle Provider anzusehen, die E-Mail-Dienste anbieten, und zwar auch dann, wenn für diese Dienste kein Entgelt anfällt<sup>3</sup>.

#### **aa. „Sendung“. Die E-Mail als Brief**

Im strafrechtlichen Schrifttum ist streitig, ob eine E-Mail eine *anvertraute „Sendung“* im Sinne des § 206 Abs. 2 Nr. 2 StGB sein kann<sup>4</sup>

Einerseits wird unter Hinweis auf das Erfordernis der „Verschlossenheit“ in § 206 Abs. 2 Nr. 1 StGB vertreten, dass es sich um eine körperliche, verschließbare Sendung handeln muss und daher § 206 Abs. 2 Nr. 2 StGB auf E-Mails nicht angewendet werden kann.<sup>5</sup>

---

<sup>3</sup> Sieber in Hoeren/Sieber, Handbuch Multimediarecht, Kap 19, Rz. 532; Heidrich/Tschoepe, MMR 2004, 75 (76).

<sup>4</sup> Vgl. Tröndle/Fischer, 54. Auflage 2007, § 206, Rdnr. 13.

<sup>5</sup> Vgl. Lackner/kühl, StGB, 25. Aufl. 2004, § 206, Rdnr. 8; Träger in LK-StGB, 11 Aufl. 2005, § 206 Rdnr. 22.

Andererseits wird betont, dass sich § 206 Abs. 2 Nr. 2 StGB eine solche Einschränkung nicht entnehmen lässt mit der Folge, dass auch die Unterdrückung von E-Mails den Straftatbestand erfüllen kann<sup>6</sup>. Dieser Auffassung ist auch die Rechtsprechung gefolgt<sup>7</sup>.

Die besseren Argumente sprechen für die Auffassung, die die Tauglichkeit der E-Mail als Tatobjekt im Sinne des § 206 Abs. 2 Nr. 2 StGB bejaht. Denn § 206 Abs. 2 Nr. 2 StGB erstreckt sich gemäß § 206 Abs. 3 Nr. 2 StGB auch auf Telekommunikationsdienstleistungen. Da Abs. 2 Nr. 1, wie sogleich gezeigt wird, im TK-Sektor keine Rolle spielt, muss sich dies auf die Nr. 2 beziehen, da sonst die Erwähnung der Telekommunikation überflüssig wäre.

Die E-Mail-Sendung stellt also ein geeignetes Tatobjekt im Sinne des § 206 Abs. 2 Nr. 2 StGB dar.

Eine Strafbarkeit wegen unbefugter Kenntnisnahme vom Inhalt einer Sendung (§ 206 Abs. 1 Nr. 1 StGB – verbietet das Öffnen verschlossener Sendungen) kommt selbst dann, wenn man beim Filtern überhaupt eine Kenntnisnahme bejahen wollte – was kaum möglich sein wird – nicht in Betracht, da sich die Nr. 1 ausschließlich auf „verschlossene Sendungen bezieht. Eine solche liegt aber bei E-Mails nicht vor, auch nicht bei verschlüsselter Post.<sup>8</sup>

---

<sup>6</sup> Tröndle/Fischer, 54. Aufl. 2007, § 206, Rdnr. 13, Lenckner in Schönke/Schröder, StGB, 27. Aufl. 2006, § 206, Rdnr. 20, Heidrich/Tschoepe, MMR 2004, 75 (77), Sieber in Hoeren/Sieber, Handbuch Multimediarecht, Kap. 12.1, Rdnr. 45; Spindler/Ernst, CR 2004, 437 (439).

<sup>7</sup> Vgl. OLG Karlsruhe, Beschl. V. 10.1.2005 – 1 Ws 152/04, CR 2005, 288.

<sup>8</sup> Lenckner in Schönke/Schröder, StGB, § 206, Rdnr. 18.

## **bb. „Zur Übermittlung anvertraut“**

§ 206 Abs. 6 Abs. 2 Nr. 2 setzt des weiteren voraus, dass die Sendung dem Übermittler „zur Übermittlung anvertraut ist“. Dies liegt vor, wenn die Sendung wie vorgesehen in den Verkehr gelangt und der versendende Mailserver dem empfangenden Server die Daten übermittelt hat<sup>9</sup>.

Hier stellen sich zwei Fragen:

(1) Sind E-Mails mit Spam, Spähsoftware (*Spyware*) und Schadsoftware (*Malware*) „wie vorgesehen in den Verkehr gelangt“?

Zu (1): Viren, wie mittlerweile auch der größte Anteil der Spam-E-Mails werden in zunehmendem Maße ohne Kenntnis und Wollen des Inhabers automatisiert von ungesicherten oder ihrerseits selbst infizierten Rechnern (Botnetze) versandt. Durch das Fernmeldegeheimnis werden jedoch alle tatsächlichen Teilnehmer am Fernmeldeverkehr – also z.B. nicht nur die berechtigten Inhaber von Fernmeldeanschlüssen geschützt<sup>10</sup>. Beim Merkmal des „Anvertrautseins“ ist daher nicht auf die subjektive Absicht des Absendenden, sondern nur auf objektive Kriterien abzustellen, sodass RFC-konform versandte E-Mails ebenso als „auf vorschriftsmäßige Weise in den Verkehr gelangt“ einzuordnen sind.

---

<sup>9</sup> OLG Karlsruhe, Beschl. V. 10.1.2005 – 1 Ws 152/04, CR 2005, 288; Kitz, CR 2005, 450 (451).

<sup>10</sup> Lencker in Schönke/Schröder, StGB, § 206, Rdnr. 6.

(2) Ab wann darf man von einer Übermittlung der Daten an den empfangenden Server und somit einem „Anvertrautsein“ im obigen Sinne ausgehen?

Zu (2): Eine Übermittlung der Daten und somit ein „Anvertrauen“ liegt dann eindeutig vor, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Providers erreicht hat und der versendende Server die Daten dem empfangenen Server übermittelt hat, wenn also die E-Mails erst angenommen und quittiert werden, und erst dann providerintern ausgefiltert werden. Denn ein Wechsel in der Verantwortung für den Mailtransport liegt in dem Moment vor, wo der empfangende Server den Erhalt der E-Mail an den Absender-Client bestätigt. Also im Rahmen des Simple Mail Transfer Protocol (SMTP): mit dem Ende der DATA-Phase nach Übertragung der Kopfzeilen (Header) und des eigentlichen Inhalts.

Umstritten ist, ob das Blockieren bereits vor Datenübertragung, etwa auf der Basis von Blacklists, wo eine Verweigerung der Annahme aller E-Mails von den auf diesen Listen geführten IP-Adressen stattfindet, ebenfalls tatbestandsrelevant im Rahmen des § 206 Abs. 2 Nr. 2 StGB ist. Der Vorgang kann in etwa mit der Maßnahme aus dem Bereich der klassischen Telefonie verglichen werden, bei der alle eingehenden Telefonanrufe einer bestimmten Vorwahl blockiert werden.

Eine Auffassung nimmt ein „Anvertrauen“ der Sendung auch in dem Fall von Blacklistblocking auf IP-Ebene an und bejaht die Tatbestandsmäßigkeit von § 206 Abs. 2 Nr. 2 StGB. Denn bei diesem Ansatz sei zumindest ein Bestandteil der eigentlichen Sendung, nämlich die IP-Nummer des Absenders im Header, bereits in den Bereich des empfangenen Mailservers gelangt und ihm damit zur weiteren Übermittlung anvertraut.<sup>11</sup> Das Tatbestandsmerkmal des

---

<sup>11</sup> Cornelius/Tschoepe, K&R 2005, 269, (270).

Anvertrautseins bei der Verwendung von Blacklists entfiere jedoch, sofern die E-Mail nach dem Blocken an den Versender zurückgeschickt wird, also „gibounced“ wird und hierbei wieder in den Einflussbereich des Absenders gelangt.

Nach der Gegenauffassung<sup>12</sup> wird der das Tatbestandsmerkmal „zur Übertragung anvertraut“ auf den Zeitpunkt nach der vollständigen Übertragung der Nachricht beschränkt, technisch also nach Ende der DATA-Phase. Dies hat zur Folge, dass eine Filterung anhand der IP-Adresse (technisch nach dem MAIL FROM Befehl) nicht unter den Straftatbestand des § 206 StGB fallen würde.

Aufgrund der so dargestellten Divergenz in den rechtlichen Auffassungen und der damit verbundenen Rechtsunsicherheit empfiehlt es sich, die Einwilligung des Kunden – wie dies im Nachfolgenden zu erörtern sein wird – einzuholen sowie die geblockten E-Mails zu bouncen, d.h. an den Absender als unzustellbar zurückzusenden.

### **cc. „Unbefugte Unterdrückung“**

Unterdrückt ist die Sendung, wenn der Täter verhindert, dass sie ihr Ziel vollständig oder unverstümmelt erreicht, und zwar auf jedwede Weise, auch durch Löschen<sup>13</sup>. Unterdrücken ist dann bei einer E-Mail gegeben, wenn die Datei in der Übermittlungs-, Zwischenspeicherungs- und Auslieferungsphase gelöscht, fehlgeleitet oder zurückgehalten wird oder wenn wesentliche Teile entfernt oder durch andere ersetzt werden.<sup>14</sup> Damit kann insbesondere auch die so genannte Quarantäne-Lösung, bei der die E-Mail auf vom übrigen System getrennte (externe oder interne) Server umgeleitet wird als Unterdrückung angesehen

---

<sup>12</sup> Heidrich, MMR 2005, 181, Anm. zu OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04.

<sup>13</sup> OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04, CR 2005, 288; Lencker in Schönke/Schröder, StGB, § 206, Rdnr. 20; Heinrich/Tschoepe, MMR 2004, 75 (77).

<sup>14</sup> Tröndle/Fischer, StGB, 54. Aufl. 2007, § 206, Rdnr. 15.

werden. Ein Unterdrücken in Form der Verzögerung liegt hierin nur dann nicht, wenn der Adressat auf die gesonderten Server jederzeit unmittelbaren Zugriff hat.

Das Merkmal „unbefugt“ und somit die Strafbarkeit kann durch eine Einwilligung des Kunden in das Filtern bzw. Blocken von unerwünschten bzw. schädlichen E-Mails entfallen. Diese kann ausdrücklich aber auch konkludent erklärt werden.

### ***aaa. Tatbestandsausschließendes Einverständnis des Kunden in dem Vertrag mit dem Provider***

Es ist umstritten, ob allein die Einwilligung des Empfängers in die Unterdrückung der E-Mail ausreicht, um den Straftatbestand auszuschließen oder nicht vielmehr auch die Einwilligung des Absenders erforderlich ist.

Nach einer Auffassung sei der Tatbestand des § 206 Abs. 2 Nr. 2 StGB nur dann ausgeschlossen, wenn sowohl der Absender als auch der Empfänger der E-Mail einer Filterung zugestimmt hat.<sup>15</sup> Dies wird damit begründet, dass § 206 Abs. 2 Nr. 2 StGB (auch) das Fernmeldegeheimnis schütze<sup>16</sup>. Das Fernmeldegeheimnis wiederum schützt alle an der Telekommunikation beteiligten<sup>17</sup> – bei der E-Mail sowohl den Absender als auch den Empfänger.

Nach einer anderen Auffassung ist der Tatbestand von § 206 Abs. 2 Nr. 2 StGB bereits dann nicht erfüllt, wenn nur der Empfänger einer E-Mail in deren Löschung oder anderweitigen Nichtzustellung einwilligt.<sup>18</sup>

---

<sup>15</sup> Heidrich/Tschoepe, MMR 2004, 75 (78); Cornelius/Tschoepe, K & R 2005, 269 (270); Schmidl, MMR 2005, 343 (346).

<sup>16</sup> OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04, CR 2005, 288.

<sup>17</sup> BVerfG, CR 1992, 431, Lenckner in Schönke/Schröder, StGB, 27. Aufl. 2006, § 206, Rdnr. 12.

<sup>18</sup> Härting, CR 2007, 311 (316), Kitz, CR 2005, 450 (453), Spindler/Ernst, CR 2004, 437 (439).

Die besseren Argumente sprechen für die zweite Ansicht. Zwar hat das BVerfG hinsichtlich der so genannten Einwilligungformel ausgeführt, dass ein Eingriff in das Fernmeldegeheimnis aus Art. 10 GG nur „im Einverständnis mit beiden Kommunikationspartnern“ ausscheide<sup>19</sup>. Als Maßstab für eine strafrechtliche Einwilligung lässt sich die Aussage des BVerfG jedoch nur dort heranziehen, wo tatsächlich Absender und Empfänger in ihren Interessen als Träger des Grundrechts aus Art. 10 GG betroffen sind. Das ist bei allen Handlungen der Fall, die den Schutzbereich des Post- und Fernmeldegeheimnisses beeinträchtigen.

In § 206 Abs. 2 Nr. 2 StGB geht es nicht um den Schutz vertraulicher Kommunikationen. Wenn die E-Mail-Sendungen unterdrückt werden, gelangt hierdurch weder die vertrauliche Kommunikation zwischen zwei Personen zur Kenntnis eines Dritten, noch realisiert sich die Gefahr der heimlichen Überwachung fremder Kommunikation. Der Sinn des § 206 Abs. 2 Nr. 2 StGB liegt daher nicht im Schutz des Fernmeldegeheimnisses.<sup>20</sup> § 206 Abs. 2 Nr. 2 StGB schützt nur (1) das Interesse des Betroffenen an dem ordnungsgemäßen Umgang mit der Sendung (Individualinteresse) und (2) das öffentliche Vertrauen in die Sicherheit und Zuverlässigkeit des Post- und Telekommunikationsverkehrs (Allgemeininteresse). Als strafwürdig sieht § 206 Abs. 2 Nr. 2 StGB nicht das Mithören bzw. Mitlesen fremder Kommunikation an, sondern die Verweigerung der Beförderung bzw. Übermittlung und somit die Verletzung einer vertraglichen Verpflichtung. § 206 Abs. 2 Nr. 2 StGB verstärkt also die vertragliche Beförderungspflicht des Telekommunikationsunternehmens.

Wenn aber der Empfänger-Provider durch die Einwilligung seines Kunden in das Filtern bzw. Blocken der schädlichen sowie unerwünschten E-Mails von der vertraglichen Verpflichtung der

---

<sup>19</sup> BVerfG, CR 1992, 431.

<sup>20</sup> Vgl. Lackner/Kühl, StGB, 25. Aufl. 2004, § 206 Rdnr. 8.

Zustellung befreit worden ist, kann es schon aus logischen Gesichtspunkten nicht richtig sein, den Empfänger-Provider strafrechtlich zu einer Beförderung für verpflichtet zu erachten, die er zivilrechtlich nicht ausführen muss oder gar darf.

Soweit das Individualinteresse an dem ordnungsgemäßen Umgang mit der E-Mail-Sendung betroffen ist, kann und muss jeder einwilligen, dessen diesbezügliches Interesse die entsprechende Filterhandlung des Providers beeinträchtigt. Aus Sicht des Empfängers umfasst dieses Interesse sicherlich, dass der Provider dem Empfänger an ihn gerichtete Sendungen zustellt und nicht eigenmächtig unterdrückt. Ein Aussortieren bedarf also in jedem Fall der Einwilligung des Empfängers. Ob auch der Absender mit einer Unterdrückung seiner E-Mail einverstanden sein muss, hängt davon ab, wie weit aus seiner Sicht das Interesse an einem ordnungsgemäßen Umgang mit der Sendung reicht. Grundsätzlich darf er davon ausgehen, dass seine Sendung dem Empfänger zugestellt wird. Allerdings obliegt es dem Empfänger zu entscheiden, ob er von der Sendung Kenntnis nimmt oder sie unbesehen zurückschickt oder vernichtet. Dies ist ein Ausfluss seines allgemeinen Persönlichkeitsrechtes aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG in der Gestalt des Rechtes auf informationelle Selbstbestimmung. Dieses Recht verwirklicht der Provider auf Geheiß seines Kunden. Seinen eigenen ordnungsgemäßen Umgang mit der Sendung stellt der Provider damit, dass – auch aus Absendersicht – nicht in Frage, denn er weicht nicht eigenmächtig von seinem grundsätzlichen Zustellungsauftrag ab. Deshalb sind von § 206 Abs. 2 Nr. 2 StGB geschützte Individualinteressen des Absenders dann nicht betroffen, wenn der Provider dem Empfänger einer Sendung auf dessen eigenen Wunsch hin nicht zustellt ggf. vernichtet. Aus diesem Grund ist auch das durch § 206 Abs. 2 Nr. 2 StGB geschützte Allgemeininteresse in Form des öffentlichen Vertrauens in die Sicherheit und Zuverlässigkeit des

Telekommunikationsverkehrs nicht beeinträchtigt. An der grundsätzlichen Funktionsfähigkeit der Telekommunikationssysteme dürfen nämlich keine Zweifel aufkommen, so lange der Provider nicht eigenmächtig Sendungen unterdrückt, sondern nur auf Geheiß des Empfängers dessen Rechte aus Art. 2 Abs. 1 GG wahrnimmt.

Insgesamt bleibt daher festzuhalten: ist die Zustellung von Spam-Mails, Spyware und/oder Malware vertraglich ausgeschlossen, kommt eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB wegen des tatbestandsausschließenden Einverständnisses des Empfängers nicht in Frage. Gänzlich unbeachtlich ist somit, ob der Absender mit der Löschung einverstanden ist. Ist es dem Empfänger jederzeit möglich, die übersandte E-Mail ungelesen zu löschen, so darf er dies auch seinem Provider überlassen.

### ***bbb. Mutmaßliches Einverständnis des Kunden in das Filtern bzw. Blocken***

Falls eine vertragliche Regelung hinsichtlich der Einwilligung des Kunden in das Filtern bzw. Blocken von unerwünschten bzw. schädlichen E-Mails fehlt, wird man auf eine Rechtfertigung des Provider-Verhaltens durch Annahme einer mutmaßlichen Einwilligung zurückgreifen müssen.<sup>21</sup> Dabei ist regelmäßig davon auszugehen, dass der Kunde mit einer Löschung von virenbehafteten Anhängen, aber auch von virenbehafteten E-Mails insgesamt einverstanden ist.<sup>22</sup>

Bei den Spam-E-Mails müssen die Provider davon ausgehen, dass ihre Kunden jede an sie interessierte E-Mail auch erhalten bzw. sich selbst vorbehalten wollen, die Nachricht als Spam zu löschen. Weder aus dem Gesichtspunkt des Handelns im Interesse des Betroffenen (Prinzip der

---

<sup>21</sup> Heidrich/Tschoepe, MMR 2004, 75 (79); Spindler/Ernst, CR 2004, 437 (439).

<sup>22</sup> Spindler/Ernst, CR 2004, 437 (439).

Geschäftsführung ohne Auftrag), noch aus dem Prinzip des fehlenden schutzwürdigen Eigeninteresses lässt sich eine mutmaßliche Einwilligung zum Unterdrücken von Spamsendungen ableiten<sup>23</sup>.

## **dd. Rechtswidrigkeit**

Das Tatbestandsmerkmal des „unbefugten“ Handelns hat in § 206 Abs. 2 Nr. 2 StGB eine Doppelfunktion: Zum einen scheidet ein unbefugtes Handeln mit einem Einverständnis des Betroffenen – wie bereits dargelegt – aus, zum anderen ist es als Hinweis darauf gedacht, dass die Rechtfertigungsgründe eine besondere Rolle spielen.

### ***aaa. Rechtfertigung nach dem TKG***

Eine Befugnis und Verpflichtung zumindest zur Löschung virenbehafteter E-Mails könnte sich aus § 109 Abs. 1 Nr. 2 TKG ergeben. Danach hat der Betreiber von Telekommunikationsanlagen angemessene, technische Vorkehrungen zum Schutz der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu schaffen. Derartige Störungen können unzweifelhaft durch Viren oder Würmer entstehen, die sich per E-Mail verbreiten. Des Weiteren kommt § 109 Abs. 2 Satz 1 TKG als Rechtfertigungsgrund in Betracht. Nach dieser Norm sind Betreiber von Telekommunikationseinrichtungen verpflichtet, angemessene technische Vorkehrungen und Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, zu treffen. Nach § 109 Abs. 2 Satz 4 TKG ist dies dann der Fall, wenn die hierzu erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und ein Richtungen für die Allgemeinheit steht. Vor dem Hintergrund der Gefahren, die

---

<sup>23</sup> Vgl Spindler/Ernst, CR 2004, 437 (440).

virenverseuchte Internetpakete für die gesamte Infrastruktur eines Diensteanbieters mit sich bringen, steht das automatisierte Scannen sowie Blocken in einem gebotenen Verhältnis zu dem ggf. vorliegenden Eingriff in die Telekommunikation. Da § 109 TKG in den beiden soeben aufgezeigten Alternativen eine Verpflichtung zum Ergreifen von Schutzmaßnahmen statuiert<sup>24</sup>, ist das Löschen virenbehafteter E-Mails aufgrund der damit verbundenen Gefahr für die Infrastruktur gerechtfertigt.<sup>25</sup>

Nach einigen Stimmen in der Literatur soll eine Rechtfertigung für die Löschung von Spam wegen der restriktiven Auslegung des § 109 TKG aufgrund des damit verbundenen Eingriffs in das Fernmeldegeheimnis ausscheiden.<sup>26</sup>

Nach hiesiger Auffassung lässt dies in dieser Allgemeinheit so nicht vertreten.

Ob eine Rechtfertigung auch bei der Unterdrückung von „normalen“ Spam-E-Mails erkannt werden kann, hängt von den Umständen des Einzelfalls, insbesondere von der Erheblichkeit der Beeinträchtigung der Infrastruktur ab. Vor dem Hintergrund der enorm hohen absoluten Anzahl an Spam-E-Mails und des stetigen Anstiegs des Spam-Aufkommens, das im Einzelfall eine ernsthafte Gefahr für die Infrastruktur der Diensteanbieter begründet, können auch Filtermaßnahmen gegen Spam-E-Mails nach § 109 TKG gerechtfertigt sein.<sup>27</sup> Letztendlich sind die Provider gesetzlich in der Pflicht, ihre Systeme vor dem Kollaps zu schützen. Wenn der Diensteanbieter einen Spam-Filter anbietet, kann dies oft zur Erbringung des Telekommunikationsdienstes erforderlich sein, da man vom Provider

---

<sup>24</sup> Bock in Beck'scher TKG-Kommentar, § 88, Rdnr. 7.

<sup>25</sup> Vgl. OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04, CR 2005, 288; Cornelius/Tschoepe, K & R 2005, 269, 270.

<sup>26</sup> Heidrich/Tschoepe, MMR 2004, 75 (78).

<sup>27</sup> Vgl. Bock in Beck'scher TKG-Kommentar, § 88, Rdnr. 7.

nicht verlangen kann, dass er sich an der Verbreitung dieser Inhalte, die seine Systeme belasten, beteiligt und ein Schutz vor der Belastung ohne eine (automatisierte) Verarbeitung der E-Mail langfristig nur geringe Erfolgchancen verspricht.<sup>28</sup> Dies ist gerade der Fall<sup>29</sup>, wenn es um die Abwehr von z.B. *Denial of Service Attacks* oder erheblichem Spam-Aufkommen geht, da diese generelle Abwehrmaßnahmen erfordern. Dementsprechend ist im Bereich des Datenverkehrs die Filterung nach bestimmten IP-Adressen zur Vermeidung von Spam-Sendungen, die von diesen IP-Adressen ausgehen, oder sog. Support-Scans, die zur Vorbereitung von Hacking-Maßnahmen an Netzknoten des Datenübertragungsnetzes auf IP-Protokoll-Basis genutzt werden, zulässig, wenn die Anonymisierung und das Verhältnismäßigkeitsprinzip berücksichtigt werden<sup>30</sup>.

### **bbb. Rechtfertigung nach den allgemeinen Rechtfertigungsgründen**

In der Literatur ist umstritten, ob und wann neben spezialgesetzlichen Rechtfertigungsgründen auch die des allgemeinen Rechts – hier insbesondere § 34 StGB – eingreifen können<sup>31</sup>. Grund hierfür ist § 88 Abs. 3 Satz 3 TKG, wonach eine Verletzung des Fernmeldegeheimnisses nur dann zulässig ist, „soweit oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf TK-Vorgänge bezieht“.

Während eine Meinung die Anwendung des Notstandes nach § 34 StGB ablehnt, da sich diese Vorschrift nicht ausdrücklich auf TK-

---

<sup>28</sup> Bock in Beck'scher TKG-Kommentar, § 88, Rdnr. 26.

<sup>29</sup> Vgl. die Ausführungen hierzu unten unter Ziffer V. 5.

<sup>30</sup> Vgl. Wittern, in Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 100, Rdnr. 11.

<sup>31</sup> Vgl. zur Übersicht Tröndle/Fischer, StGB, 54. Aufl. 2007, § 206, Rdnr. 9.

Vorgänge bezieht<sup>32</sup>, will eine andere Ansicht die die allgemeinen Rechtfertigungsgründe zumindest dann heranziehen, wenn besondere Fallgestaltungen vorliegen, die außerhalb des Rahmens des § 88 TKG liegen.<sup>33</sup>

Der zweiten Meinung ist nach hiesiger Auffassung der Vorrang zu geben. § 88 Abs. 3 Satz 3 TKG ist im Zusammenhang mit Satz 1 zu sehen. Der Anwendungsbereich ist also nur dann eröffnet, wenn es gerade um die Verschaffung und Verwendung der Kenntnisse vom Inhalt und den näheren Umständen der Telekommunikation geht. In einer Konstellation, in der es nicht primär um die Verschaffung und Verwendung dieser Kenntnisse geht, muss ein Rückgriff auf die allgemeinen Rechtfertigungsgründe prinzipiell möglich sein, soweit keine spezielleren eingreifen.<sup>34</sup> Allerdings ist eine solche (ungeregelte) Fallgestaltung in der Praxis schwer vorstellbar. So kann sich ein Provider, der Maßnahmen zur Abwehr eines Angriffs mit Computerviren und unter bestimmten Umständen von Spam-E-Mails ergreift, auf die Vorschrift des § 109 TKG berufen.

#### ***b. Datenunterdrückung (§ 303a StGB)***

Der Tatbestand der Datenunterdrückung nach § 303a Abs. 1 Alt. 2 StGB ist grundsätzlich ebenfalls einschlägig, wenn E-Mails unterdrückt werden. Das Merkmal des „Unterdrückens“ entspricht den o.g. Ausführungen zu § 206 Abs. 3 StGB.

Rechtswidrig geschieht dies dann, wenn der Provider eine fremde Rechtsposition, also das Verfügungsrecht über die Daten, verletzt. Dieses Verfügungsrecht ist Schutzgegenstand von § 303a StGB.

---

<sup>32</sup> Lencker, in: Schönke/Schröder, StGB, § 206, Rdnr. 14, Lackner/Kühl, StGB, § 206, Rdnr. 15.

<sup>33</sup> Tröndle/Fischer, StGB, 54. Aufl. 2007, § 206, Rdnr. 9; Cornelius/Tschoepe, K & R 2005, 269 (270).

<sup>34</sup> Vgl. OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04, CR 2005, 288; Cornelius/Tschoepe, K & R 2005, 269, 270.

Anders als § 206 Abs. 2 Nr. 2 StGB schützt § 303a StGB also nur Individualinteressen.<sup>35</sup>

Die Strafbarkeit kann auch hier durch Einwilligung des Interessensträgers, also des hinsichtlich der Daten Berechtigten, beseitigt werden. Dies ist im Zeitpunkt des Filterns bzw. Blockens der Empfänger der Sendungen. Eine Einwilligung des Absenders ist auch hier wie bei § 206 Abs. 2 Nr. 2 StGB nicht erforderlich. Denn ursprünglich ist der Absender allein Verfügungsberechtigt über die Daten gewesen. Er hat jedoch dann aber eine Kopie seiner Originaldaten zielgerichtet aus seinem Einflussbereich entsenden lassen, um sie in die Verfügungsgewalt des Empfängers zu transportieren. Durch entsprechende Einschaltung des Providers als Bote für die Einigungserklärung der Annahme und als Geheißperson für die Übergabe, kann der Empfänger schon vor der Zustellung, also noch auf Serverebene, die Daten seiner ausschließlichen Verfügung unterwerfen. Damit braucht auch insoweit nur er der Löschung bzw. dem Blocken der E-Mail durch den Provider zuzustimmen, um eine Strafbarkeit des Providers nach § 303a Abs. 1 Alt. 2 StGB auszuschließen.

Diese Einwilligung sollte sinnvollerweise in dem Providervertrag mit dem Kunden enthalten sein.

Ist dies nicht der Fall, gelten die oben bei § 206 Abs. 2 Nr. 2 StGB dargestellten Grundsätze für ein mutmaßliches Einverständnis.

Auch die Ausführungen zu einer Rechtfertigung des Providers nach § 109 TKG sind entsprechend zu berücksichtigen.

---

<sup>35</sup> Lackner/Kühl, StGB, § 303a, Rdnr. 4; Tröndle/Fischer, StGB, 54. Aufl. 2007, § 303a, Rdnr. 9.

### *c. Ausspähen von Daten (§ 202a StGB)*

Der Tatbestand des Ausspäehens von Daten (§ 202a StGB) wird bei der E-Mail-Filterung bzw. Blocken nicht einschlägig sein, da es zum einen schon an einem Verschaffen von Daten fehlt, zum anderen aber auch für den Provider keine besondere Sicherung der E-Mail besteht<sup>36</sup>. Das virtuelle Öffnen der E-Mail zwecks Scannings des Textes bzw. des Anhangs ist kein Verschaffen von Daten, selbst wenn die Software auf ein Schlagwort trifft, zumal der Provider selbst nicht erkennen könnte, welches Schlagwort sich in der E-Mail befindet. Der Täter des § 202 a StGB muss die Daten entweder lesen oder abspeichern, so dass sie später gelesen werden können.<sup>37</sup> Beides ist in der Konstellation des Scannings oder der Filterung nicht der Fall.

### *d. Zwischenergebnis*

Beim Filtern bzw. Blocken von E-Mails kommt eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB sowie § 303 a StGB des Providers in Betracht. Die Strafbarkeit entfällt, wenn der Kunde, also der Adressat der Sendungen in den jeweiligen Maßnahmen im Voraus einwilligt. Eine Einwilligung des Absenders ist nicht erforderlich. Das Unterdrücken von virenverseuchten E-Mails sowie unter gewissen Umständen von Spam-E-Mailings kann nach § 109 Abs. 1 Nr. 2 bzw. Abs. 2 Satz 1 TKG gerechtfertigt sein.

## **2. Datenschutzrechtliche Relevanz**

Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn sie gesetzlich erlaubt oder vom Betroffenen gestattet sind (z.B. § 4 Abs. 1 BDSG, § 3 Abs. 1 TDDSG):

---

<sup>36</sup> Spindler/Ernst, CR 2004, 437 (439). m.w.N.

<sup>37</sup> Ernst in: Hacker, Cracker & Computerviren 2004, Rdnr. 234 f.

- *Erheben* ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG),
- *Verarbeiten* ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten (§ 3 Abs. 5 BDSG),
- *Nutzen* ist jede weitere Verwendung der Daten (§ 3 Abs. 5 BDSG).

Ein Verstoß dagegen stellt gemäß § 43 Abs. 2 BDSG eine Ordnungswidrigkeit und beim Vorliegen vom Vorsatz eine Straftat (§ 44 BDSG) dar.

#### *a. Eingriff in Datenschutzrechte*

Durch den Einsatz von Filter- und Blockadesystemen bei der Bekämpfung von Spam-E-Mails und schädlichen Datensendungen könnten datenschutzrechtliche Belange betroffen sein. Es ist fraglich, ob beim Einsatz von E-Mail-Filterprogrammen die vorgenannten datenschutzrechtlich relevanten Verletzungsformen – Erhebung, Verarbeitung, Nutzung von personenbezogenen Daten – einschlägig sind. Erforderlich für eine Erhebung wäre ein zielgerichtetes Beschaffen.<sup>38</sup> Daran fehlt es, obwohl bei der Analyse die E-Mail oft geöffnet werden muss, weil nur ein Abgleich des Mailinhalts mit einer Stichwortliste erfolgt und kein Auslesen von personenbezogenen Daten aus der E-Mail stattfindet.<sup>39</sup> Auch eine Speicherung findet – außerhalb des Arbeitsspeichers – nicht statt. Nichtsdestotrotz lässt sich eine sonstige Verwendung von Daten im Sinne einer datenschutzrechtlich relevanten Nutzung nach § 3 Abs. 5 BDSG nicht gänzlich ausschließen. Insbesondere steht der Umstand, dass die Abwehrmaßnahmen der Provider in nahezu allen Fällen automatisch durchgeführt werden, der Anwendung des Datenschutz- und des Datenschutzstrafrechts nicht entgegen.<sup>40</sup>

---

<sup>38</sup> Gola/Schomerus, BDSG, § 3, Rdnr. 28, Simitis, BDSG, § 3, Rdnr. 126, 130.

<sup>39</sup> Vgl. Spindler/Ernst, CR 2004, 437 (440).

<sup>40</sup> Simitis, BDSG, 5. Aufl. 2003, § 1, Rdnr. 69.

Es ist auch nicht anzuzweifeln, dass in den gescannten und gefilterten Sendungen personenbezogene Daten enthalten sind, wenn die Sendungen - wie dies sehr oft der Fall ist – an natürliche Personen gerichtet sind. Allerdings gilt dann, wenn die Daten in der Filtersoftware nicht einer Person zugeordnet werden, dass diese mangels Bestimmbarkeit datenschutzrechtlich keine Rolle spielt<sup>41</sup>. Dies gilt erst recht, wenn es sich bei den E-Mail-Daten überhaupt nicht um die Daten natürlicher Personen handelt. Diese sind allein hinsichtlich der Daten, die dem Telekommunikationsgeheimnis unterfallen, durch das TKG geschützt.

Alles in einem Im Ergebnis kann ein datenschutzrechtlich relevanter Eingriff aber nicht ausgeschlossen werden.

#### ***b. Rechtfertigung des Eingriffs in Datenschutzrechte***

Eine datenschutzrechtliche Rechtfertigung ergibt sich im Falle von Filtern und Blocken von unerwünschten und/oder schädlichen E-Mails aus § 100 Abs. 1 (Störungsbekämpfung) und Abs. 3 Satz 1 TKG (Missbrauchbekämpfung).<sup>42</sup> Diese Norm gestattet die Erhebung und Verwendung von Bestands- und Verkehrsdaten zum Aufdecken und zum Unterbinden von Störungen (Abs. 1) sowie rechtswidriger Inanspruchnahme der Infrastruktur des Providers (Abs. 3). Der Diensteanbieter ist demnach berechtigt, seine gesamten Datenbestände nach solchen Daten auszuwerten, die konkrete Indizien für eine missbräuchliche Inanspruchnahme des Dienstes enthalten. Diese breite Eingriffsbefugnis nach der jetzigen Fassung des § 100 Abs. 3 Satz 1 TKG ist damit zu begründen, dass sich der Wortlaut der Norm im Rahmen der TKG-Novellierung im Jahre 2004 entscheidend verändert hat. Im Rahmen der Novellierung ist das Merkmal „im

---

<sup>41</sup> Tinnefeld, in : Rossnagel, Handbuch Datenschutzrecht, Kap. 4.1, Rdnr. 18 ff.

<sup>42</sup> Vgl. LG Köln, Urteil vom 12.09.2007, Az.: 28 O 339/07 - JurPC Web-Dok. 164/2007, Abs. 51 ff.

Einzelfall“ weggefallen. Damit sollen von der jetzigen Eingriffsbefugnis nicht nur Störungen und Gefahren erfasst sein, die im Einzelfall auftreten, sondern gegebenenfalls auch Störungen oder Fehler, die bei einer größeren Anzahl von Teilnehmern und Nutzern oder einer Vielzahl von Fällen auftreten. Dies ist gerade der Fall, wenn es um die Abwehr von z.B. *Denial of Service Attacks* oder erheblichem Spam-Aufkommen geht, da diese generelle Abwehrmaßnahmen erfordern. Dementsprechend ist im Bereich des Datenverkehrs die Filterung nach bestimmten IP-Adressen zur Vermeidung von Spam-Sendungen, die von diesen IP-Adressen ausgehen, oder sog. Support-Scans, die zur Vorbereitung von Hacking-Maßnahmen an Netzknoten des Datenübertragungsnetzes auf IP-Protokoll-Basis genutzt werden, zulässig, wenn die Anonymisierung und das Verhältnismäßigkeitsprinzip berücksichtigt werden<sup>43</sup>.

Diese breite Eingriffsbefugnis, die in erheblichem Maß auch Daten unbeteiligter Dritter einbezieht und damit datenschutzrechtlich besonders sensibel ist, wird gemäß § 100 Abs. 3 Satz 2 TKG generell auf die Daten beschränkt, die nicht älter als sechs Monate sind.

Zwar tritt bei der Filterung von E-Mails das Problem hinzu, dass diese einen Doppelcharakter besitzen und die Inhalte eigentlich den datenschutzrechtlichen Regelungen des Telemediendienstegesetzes (TMG) unterfallen. Dort jedoch fehlt eine entsprechende Regelung. Die Anwendung des TMG und dort insbesondere des § 15 TMG (Nutzungsdaten) im Bezug auf die Inhaltsdaten wird dann angenommen, wenn Daten betroffen sind, die der Nutzer und der Anbieter online austauschen, um die durch den Teledienst begründeten Leistungs- und Rechtsverhältnisse zu erfüllen<sup>44</sup>. Dies ist vorliegend nicht der Fall, da die Inhaltsdaten (z.B. E-Mail im Header oder Body der

---

<sup>43</sup> Vgl. Wittern, in Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 100, Rdnr. 11.

<sup>44</sup> Schmitz, in: Spindler/Schmitz/Geis, TDDSG, § 3, Rdnr. 8.

E-Mail), die bei der Filter-Analyse des E-Mail-Verkehrs ggf. erfasst werden, nicht von den Beteiligten ausgetauscht werden, um einen Telemediendienst zu erfüllen. Die Zulässigkeit des Zugriffs auf Inhaltsdaten richtet sich daher im vorliegenden Fall nicht nach dem TMG, sondern nach den allgemeinen Regeln des BDSG und des TKG<sup>45</sup>.

In diesem Zusammenhang ist auch auf die Pflicht der TK-Provider zur Implementierung technischer Schutzmaßnahmen gemäß § 109 TKG hinzuweisen.

Es sollte auch beachtet werden, dass die für Filterzwecke zulässigerweise ausgelesenen Daten in keinem Fall anderweitig verwendet werden dürfen (vgl. § 31 BDSG) – etwa um dem Kunden auf die Inhalte der E-Mail bezogene Werbung zukommen zu lassen.

### *c. Zwischenergebnis*

Nach alledem ist der Einsatz von E-Mail-Filtern gegen Viren und Spam datenschutzrechtlich grundsätzlich zulässig.<sup>46</sup> Zu beachten ist jedoch stets das Gebot der Datensparsamkeit des § 3a BDSG sowie die Anonymisierung und das Verhältnismäßigkeitsprinzip.

## **3. Zivilrechtliche Überlegungen**

Der Absender hat einen vertraglichen Anspruch gegen seinen E-Mail-Provider auf Beförderung der von ihm versandten E-Mails. Ebenso ist der Empfänger-Provider zur Beförderung von E-Mails verpflichtet, die auf dem Account eines Kunden eingehen. Beim E-Mail-Provider-

---

<sup>45</sup> Bitzer, in: Rossnagel, recht der Multimediendienste, § 3 TDDSG, Rdnr. 13.

<sup>46</sup> Schaar, Datenschutz im Internet, 2002, Rdnr. 630; Rossnagel, recht der Multimediendienste, Kap. 6.4., Rdnr. 35; Spindler/Ernst, CR 2004, 437 (440); Wittern, in Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 100, Rdnr. 2.

Vertrag gehört die Beförderung der E-Mails zu den Hauptpflichten des Providers.<sup>47</sup> In diesem Zusammenhang ist fraglich, ob der Provider im Sinne einer nebenvertraglichen Schutzpflicht bzw. Verkehrssicherungspflicht gehalten ist, eingehende E-Mails von vornherein auf Viren zu prüfen und auch Spam-E-Mails vom Kunden fern zu halten.

#### *a. Pflicht zur Filterung*

Ein wichtiger Faktor bei der Konkretisierung der vertraglichen Schutzpflichten ist die Beherrschbarkeit von Gefahren und das berechnete Vertrauen auf den Schutz vor solchen Gefahren durch die Diensteanbieter<sup>48</sup>. Maßgeblich ist ferner, ob entsprechende Sicherungsmaßnahmen in der Praxis bereits eingesetzt werden oder sogar bereits als verkehrszüblich bezeichnet werden können<sup>49</sup>.

Legt man die genannten Kriterien zugrunde, dürfte der Kunde regelmäßig darauf vertrauen, dass die Systeme des Providers mit entsprechenden Sicherungsmaßnahmen ausgestattet sind, die einen Zugriff Dritter auf die E-Mail-Accounts verhindern und der Provider grundlegende Anforderungen an die Sicherheit seiner Server und der dort gespeicherten Daten seiner Kunden gegenüber Ausspähsversuchen oder Missbrauch seitens Dritter einhalten muss.<sup>50</sup> Demgemäß zählt ein automatisierter Virenschutz – der natürlich nicht alle Eingriffe abwehren kann – zu den vertraglichen Nebenpflichten eines E-Mail-Providers.<sup>51</sup> Aufgrund des enorm angestiegenen Spam-Aufkommens in den letzten Jahren und der damit verbundenen allgemeinen Bedrohung für die

---

<sup>47</sup> Stadler in Hoeren/Sieber, Handbuch Multimediarecht, Kap. 12.1., Rdnr. 45.

<sup>48</sup> Wagner, in: Münch/Komm, 2004, BGB, § 823, Rdnr. 273; J. Hager, in Staudinger, 1999, BGB, § 823, Rdnr. E 27.

<sup>49</sup> Vgl. Spindler/Ernst, CR 2004, 437 (441).

<sup>50</sup> Kommarnizki, in Hoeren/Sieber, Handbuch Multimedia-Recht, 12 Rdnr. 72; Ernst Vertragsgestaltung im Internet, 2003, Rdnr. 588.

<sup>51</sup> Ernst Vertragsgestaltung im Internet, 2003, Rdnr. 588.

Kapazitäten und die Funktionsweise eines E-Mail-Services dürfte auch von einer Verpflichtung der Provider auszugehen sein, einen Spam-Filter zu verwenden, zumal das Angebot von Spam-Filtern mittlerweile zum Standardbestandteil der meisten Dienstleistungsangeboten gehört und somit verkehrsblich ist.

Sollte der Provider die vorgenannten Filterpflichten in seinen AGB ausschließen oder einschränken wollen, würde die jeweilige Klausel der Inhaltskontrolle unterliegen. Will der Provider daher seine Filterpflichten ausschließen, kann er dies nicht zuletzt im Hinblick auf das Transparenzgebot in § 307 Abs. 3 BGB allenfalls in einer klar formulierten Leistungsbeschreibung tun, die dem Kunden von vornherein klar vor Augen führt, dass er nur einen E-Mail-Dienst ohne Virencheck und Spam-Filterung erhält.

#### ***b. Recht zur Filterung***

Wie bereits dargestellt, ergibt sich eine Pflicht zur Filterung, zumindest betreffend die virenverseuchten E-Mails und großen, systemgefährdenden Spam-Wellen aus § 109 TKG, wonach die Provider gehalten sind, technische Maßnahmen zum Schutze der Systemsicherheit einzusetzen. Daraus resultiert auch eine zivilrechtliche Berechtigung, entsprechende Filtersysteme einzusetzen. Darüber hinaus wurde bereits erörtert, dass auch von einer mutmaßlichen Einwilligung des Kunden in die Filterung von Viren auszugehen ist.

Beim Einsatz von Spam-Filtern ist dagegen die Rechtslage etwas anders: Der Provider kann nicht von vornherein davon ausgehen, dass der Kunde eine Filterung aller seiner E-Mails wünscht. Gerade um die strafrechtlichen Risiken zu minimieren ist es erforderlich, mit dem Vertragsabschluss auch die Einwilligung des Kunden in das Löschen bzw. Blocken von Spam-E-Mails einzuholen. In diesem Zusammenhang

hat der Provider bei der Gestaltung seiner Verträge zu beachten, dass die mit einem Einverständnis verbundene datenschutzrechtlich relevante Einwilligung in die Löschung von E-Mails den Anforderungen des § 4a BDSG (Schriftlichkeit, drucktechnische Hervorhebung etc) bzw. im elektronischen Einwilligungsverfahren den Anforderungen des § 94 TKG (bewusste und eindeutige Erteilung, Protokollierungspflicht etc) genügt.

Auf der Absenderseite ist wiederum geboten, den Transport von Spam- und Viren-E-Mails auszuschließen, da der Kunde, der eine E-Mail versendet, im Normalfall erwarten wird, dass alle von ihm versandten E-Mails auch tatsächlich befördert werden, selbst wenn es sich um Spam- oder Viren-E-Mails handelt. Eine solche Ausschlussklausel dürfte im Allgemeinen auch einer Inhaltskontrolle nach § 307 BGB standhalten. Denn es liegt kein Regelfall einer unangemessenen Benachteiligung des Vertragspartners vor: Es fehlt an einer gesetzlichen Regelung, von der abgewichen wird (§ 307 Abs. 2 Nr. 1 BGB), und auch die Erreichung des Vertragszwecks ist durch ein Verbot der Versendung von Spam- und Viren-E-Mails nicht gefährdet / § 307 Abs. 2 Nr. 2 BGB). Es widerspricht auch nicht Treu und Glauben (§ 307 Abs. 1 Satz 1 BGB), wenn der Provider eine solche Verwendung ausschließt. Denn der Provider hat ein nachvollziehbares und keineswegs treuwidriges Interesse daran, nicht an Handlungen mitzuwirken, die rechtswidrig sind. Wenn sich der Provider durch entsprechende AGB-Klauseln dagegen schützt, Erfüllungsgehilfe eines Spammers oder Virenversenders zu werden, liegt hierin keine unredliche und unangemessene Benachteiligung des versendenden Kunden vor.

### ***c. Lösungsrechte und Benachrichtigungspflichten***

Von der Pflicht bzw. dem Recht zur Filterung ist das Recht zum Löschen der indizierten E-Mail zu unterscheiden.

Insofern stellt sich die Frage, ob der Provider die virenverseuchten bzw. als Spam erkannten Spam-E-Mails ohne weiteres löschen kann oder (zwischen-)speichern muss, und dem Kunden eine entsprechende Nachricht zu übersenden hat. Dabei ist zu berücksichtigen, dass grundsätzlich die alleinige Verfügungsbefugnis über die E-Mails beim Nutzer liegt.<sup>52</sup>

Wie zu verfahren ist, hängt in erster Linie von der vertraglichen Vereinbarung mit dem Kunden und insbesondere davon ab, ob und wie dieser in die Löschung der herausgefilterten E-Mails eingewilligt hat. Wenn eine entsprechende Einwilligung vorliegt, die bei den virenverseuchten E-Mails auch gemutmaßt werden darf, so darf die Löschung nach dem Inhalt der Einwilligung erfolgen. Dabei ist zu berücksichtigen, dass eine generelle Einwilligung in die Löschung nicht vorab erteilt werden kann, da der Provider die Befugnis hätte, sämtliche nach seiner Auffassung verdächtigen E-Mails zu löschen.

Liegt eine Einwilligung in die Löschung nicht vor, so ist der Kunde zwingend vorher zu benachrichtigen. Dies entspricht der strafrechtlichen Wertung. Insbesondere im Bereich der Spam-E-Mails, wo die Gefahr der Löschung von „normalen“ E-Mails, die falsch als Spam markiert wurden, sehr präsent ist, darf der Provider nicht ohne vorherige Benachrichtigung (vermeintliche) Spam-E-Mails löschen. Dem Kunden ist dann eine angemessene Frist bis zur Löschung zu gewähren, ihn auf die bevorstehende Löschung hinzuweisen und ihm Zugang zu der indizierten E-Mail zu ermöglichen.

Es wird auch die Pflicht des Providers bejaht, sein Mail-System so zu konfigurieren, dass an den Absender einer virenverseuchte E-Mail die Nachricht übermittelt wird, dass die E-Mail wegen Virenverseuchung

---

<sup>52</sup> Hoeren, NJW, 2004, 3513 (3516).

gelöscht wird.<sup>53</sup> Auch diese Pflicht entspringt den nebenvertraglichen Schutz- und Treuepflichten dem Kunden gegenüber, da ansonsten die Gefahr besteht, dass Kommunikationspartner des Kunden ohne deren Wissen E-Mails virenverseucht abgesandt haben und die Nachrichten verloren gegangen sind<sup>54</sup>. Nur auf diese Weise kann der Partner des Kunden und damit der Kunde selbst die Chance erhalten, E-Mails nach vorheriger Kontrolle nochmals zu versenden.

#### *d. Umgang mit Blacklists*

Bleibt die Entstehung und Pflege der für seinen Account zuständigen Spam-Blacklists dem Kunden selbst überlassen, entstehen keine Rechtsprobleme.

Wird die Pflege vom Provider durchgeführt, sind einige Regeln zu beachten:

- ◆ Die Aufnahme von Absenderadressen darf nicht willkürlich möglich sein.
- ◆ Die sorgfältige Auswahl und Überwachung der Informationsquellen muss gewährleistet sein.
- ◆ Angesichts der hohen Missbrauchsgefahr besteht eine Pflicht zur Einführung von Prüfkriterien.
- ◆ Die stetige Pflege während der Vertragslaufzeit ist zwingend.
- ◆ Jede Änderung von Kriterien ist dem Kunden bekannt zu geben.

Bei einer Verletzung der vorgenannten Pflichten könnte sich der Provider gegenüber seinem Kunden einem Anspruch auf Schadensersatz neben der Leistung aus §§ 280 Abs. 1 S. 1, 282, 241 Abs. 2 BGB ausgesetzt sehen. Darüber hinaus kann auch eine Haftung des Providers aus wettbewerbsrechtlichen Gesichtspunkten wegen gezielter Behinderung (§§ 3, 4 Nr. 10 UWG) bzw. wegen eines Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb (§ 823 Abs. 1

---

<sup>53</sup> Spindler/Ernst, CR 2004, 437, 443; Hoeren, NJW, 2004, 3513 (3516).

<sup>54</sup> Spindler/Ernst, CR 2004, 437, 443.

BGB) gegenüber unberechtigterweise eingetragenen Dritten in Frage kommen. Dies bestätigt die aktuellste Rechtsprechung. Mit Urteil vom 27.09.2007 (Az.: 7 O 80/07) verurteilte das Landgericht Lüneburg den Betreiber eines gewerblich genutzten Mailservers mit verschiedenen E-Mail-Konten von Kunden dazu, es zu unterlassen, die E-Mails eines absendenden Mailservers mittels einer sogenannten Blacklist auf IP-Basis (DNS Blacklist) zu blockieren. Ein solches Verhalten wertete das Gericht als absichtliche Behinderung des Absenders und somit als wettbewerbswidrig. Dies soll auch dann gelten, wenn über die geblockte IP des Mailservers unerwünschte E-Mails (Spam) versandt werden. Mailserver-Betreiber dürfen sich der Urteilsbegründung zufolge nur in „begrenzten Ausnahmefällen“ mittels IP-Blacklisting vor Spam schützen.

## V. Bewertung einzelner Konstellationen und Fragen aus der Praxis

### ***1. Muss der Provider auf Informationen von „außen“ über die in seinem System angesiedelten Botnetze oder die über seine Systeme verbreiteten Phishing-E-Mails reagieren?***

Nach dem derzeitigen Stand in der Rechtsprechung des Bundesgerichtshofes (BGH) <sup>55</sup> gelten die Privilegierungen des Telemediengesetzes (TMG) nicht für Ansprüche auf Beseitigung der rechtswidrigen Handlung (Störung). Der Provider ist demnach gehalten, ab Kenntnis vom Missbrauch seiner Systeme zum Versand von rechtswidrigen E-Mails über Botnetze, tätig zu werden, um den Missbrauch zu beenden.

---

<sup>55</sup> Vgl. zuletzt BGH, Urteil vom 19.04.07, Az.: I ZR 35/04 (Internetversteigerung II)

## **2. Wann liegt „Kenntnis“ von dem Missbrauch im vorgenannten Sinne vor?**

Auslöser für Maßnahmen seitens des Providers soll nach Auffassung des BGH<sup>56</sup> die Kenntnis des Hostproviders über das Vorliegen *einer klaren Rechtsverletzung* sein. Unstreitig ist es erforderlich, dass die Kenntnis sich nicht nur auf die Handlung als solche (Versenden von E-Mails) sondern auch auf die Rechtswidrigkeit dieser Handlung (Versenden von Spam-E-Mails) erstreckt.<sup>57</sup> Darüber hinaus ist die Kenntnis von einer konkreten rechtswidrigen Handlung erforderlich. Das bedeutet, dass dem Anbieter genaue Informationen über eine konkrete IP-Adresse vorliegen, die am Botnetz beteiligt ist und über die rechtswidrige E-Mails versandt werden. Eine allgemeine Mitteilung an den Anbieter, dass sich in seinem System verschiedene (Botnetz)Rechner befinden, die an der Verbreitung von Spam-E-Mails beteiligt sind, ohne dass diese Rechner näher gekennzeichnet werden, kann nicht die Kenntnis begründen.

Hier besteht für den Hostprovider erhebliche Unsicherheit dahingehend, ab wann vom Vorliegen einer hinreichend klaren Rechtsverletzung auszugehen ist. Bei allgemein verbreiteten und bekannten Spam-E-Mails „mittlerer Art und Güte“ (z.B. Werbe-E-Mails für Potenz- oder Körperteilverlängerungsmittel) mag die Rechtswidrigkeit eindeutiger feststellbar sein. In anderen Situationen ist dies jedoch nicht immer der Fall.

Bis zum Zeitpunkt einer formellen Abmahnung, die substantiiert die Legitimation (Vollmacht), den Verstoß und Beweise vorlegt, befindet sich der Provider in einer Vielzahl von Fällen in einer haftungsrechtlichen Zwickmühle, wonach er entweder gegenüber dem

---

56 BGH, Urteil vom 11.03.2004, Az.: I ZR 304/01 (Rolex-Ricardo / Internetversteigerung I), JurPC Web-Dok. 265/2004, Abs. 1 - 49; bestätigt durch BGH, Urteil v 19.04.2007 – I ZR 35/04 – Rolex-eBay / Internetversteigerung II).

<sup>57</sup> Vgl. Spindler/Schmitz/Geis, § 11 TDG, Rdnr. 12.

Kunden auf Schadensersatz wegen Nichterfüllung oder aber seitens des Verletzten in Anspruch genommen werden kann.

In der Praxis sollte daher darauf geachtet werden, dass Tatsachen, also nachprüfbare Umstände vorliegen, die erhebliche und begründete Bedenken nach einer gewissenhaften Prüfung gegen die Rechtmäßigkeit aufkommen lassen. Sobald dies der Fall ist, liegt Kenntnis im vorgenannten Sinne vor.

### **3. Wer kann „Kenntnis“ von dem Missbrauch verschaffen?**

Es ist unerheblich, wer dem Provider die Kenntnis von der rechtswidrigen Handlung verschafft hat und wie dies geschah. Jedermann – sowohl Nutzer, Geschädigter als auch jeder andere, insbesondere in- und ausländische Behörden, kommen als Informanten in Betracht.

### **4. Welche Maßnahmen sind zu ergreifen?**

Der Umfang der Maßnahmen richtet sich danach, was dem Provider technisch möglich und wirtschaftlich zumutbar ist. Welche Maßnahmen diesen Kriterien entsprechen, ist Frage des Einzelfalles und lässt sich nicht verallgemeinern.

Hierbei ist jedoch zu berücksichtigen, dass die Maßnahmen so durchzuführen sind, dass unbeteiligte Kunden möglichst nicht davon betroffen sind. So dürfte die Ausschaltung eines ganzen virtuellen Rootservers nicht angebracht sein, wenn sich dadurch zwar die rechtswidrige Verbreitung der Spam-E-Mails unterbinden ließe, davon jedoch andere, daran nicht beteiligte Kunden-Sektionen betroffen wären.

### **5. Darf prophylaktisch nach Botnetzen gesucht werden?**

Vor dem Hintergrund der enorm hohen absoluten Anzahl an Spam-E-Mails und des stetigen Anstiegs des Spam-Aufkommens, insbesondere durch die Verbreitung von Botnetzen, das im Einzelfall eine ernsthafte Gefahr für die Infrastruktur der Diensteanbieter begründet<sup>58</sup> und oft zu erhebliche Störungen an den Provider-Systemen führt, können vorbeugende Maßnahmen gegen die Verbreitung von Viren bzw. Spam-E-Mails über Botnetze nach § 109 TKG gerechtfertigt sein.<sup>59</sup> Letztendlich sind die Provider gesetzlich in der Pflicht, ihre Systeme vor dem Kollaps zu schützen. Denn (präventive) Maßnahmen gegen die alltägliche Gefahr, die von Botnetzen ausgeht, sind zur Erbringung des Telekommunikationsdienstes erforderlich. Der Schutz vor der Systembelastung ohne eine (automatisierte) Verarbeitung des E-Mail-Verkehrs verspricht langfristig nur geringe Erfolgschancen.<sup>60</sup>

Die damit verbundene Auswertung von Verkehrsdaten ist nach § 100 Abs. 1 (Störungsvermeidung) bzw. Abs. 3 Satz 1 TKG (Missbrauchbekämpfung) gerechtfertigt sein.<sup>61</sup>

Nach § 100 Abs. 1 TKG darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. Wie bereits mehrfach dargelegt, führt die massive Verbreitung von Spam-Mails über Botnetze oft zu erheblichen Störungen an der Funktionalität der E-Mail-Server. Demnach sind technische Maßnahmen, die bezwecken, diese Störungen zu erkennen, einzugrenzen und zu beseitigen nach § 100 Abs. 1 TKG zulässig. Dies gilt gerade im präventiven Bereich. Denn es

---

<sup>58</sup> Vgl. beispielhaft: Online-Meldung des Heise-Verlages vom 25.05.2007 unter dem Titel „Mailserver ächzen unter Spam-Last“, im Internet abrufbar unter: <http://www.heise.de/newsticker/meldung/90241>

<sup>59</sup> Vgl. Bock in Beck'scher TKG-Kommentar, § 88, 3. Auflage 2006, Rdnr. 7.

<sup>60</sup> Bock in Beck'scher TKG-Kommentar, § 88, 3. Auflage 2006, Rdnr. 26.

<sup>61</sup> Vgl. hierzu die Ausführungen oben unter: IV, 2, b.

entspricht der - soweit ersichtlich - herrschenden Meinung in der Literatur<sup>62</sup>, dass § 100 Abs. 1 TKG im Unterschied zu der früher geltenden Norm des § 9 Abs. 1 TDSV 2000 nicht mehr voraussetzt, dass im Einzelfall tatsächlich Störungen und Fehler oder konkrete Anhaltspunkte dafür vorliegen müssen. Somit ist auch eine vorsorgliche, präventive Datenverarbeitung und Erhebung zur Erkennung von Fehlern oder Störungen demnach grundsätzlich zulässig.<sup>63</sup> Die präventive Erhebung und Verwendung der Daten darf jedoch nicht unbegrenzt stattfinden. Zur Störungsbeseitigung besteht eine durch die Grundsätze der Verhältnismäßigkeit, Erforderlichkeit und der Zweckbindung eingeschränkte Erhebungsbefugnis. Insbesondere sind die Daten unverzüglich zu löschen, wenn keine Störungen oder Fehler auftraten.

Falls - entgegen der hier vertretenen Auffassung - die Verbreitung von Viren- und Spam-E-Mails über Botnetze als nicht dafür geeignet angesehen wird, Störungen an den E-Mail-Systemen der Provider zu verursachen, wäre eine allgemeine präventive Auswertung aller Daten unter dem Deckmantel der Suche nach Botnetzen grundsätzlich nicht zulässig. Denn nach der Regelung des § 100 Abs. 3 TKG, die hier einschlägig wäre, ist die allgemeine präventive Auswertung der Daten ohne irgendeinen, konkreten Anhaltspunkt nicht erlaubt.<sup>64</sup> Nach § 100 Abs. 3 TKG dürfen Maßnahmen gegen die rechtswidrige Inanspruchnahme der Systeme dann ergriffen werden, wenn tatsächliche Anhaltspunkte vorliegen. Demnach lässt sich jedoch ein sogenanntes Frühwarnsystem einrichten, das allerdings erst mit der personenbezogenen Auswertung von Daten beginnen darf, wenn eine missbräuchliche Leistung möglich erscheint. Es lässt sich auch eine

---

<sup>62</sup> Vgl. Kleszczewski in: Berliner Kommentar zum Telekommunikationsgesetz, § 100 Rz.8; Wittern in Beck'scher TKG-Kommentar, 3. Auflage 2006, § 100, Rdnr.1 und 6.

<sup>63</sup> Vgl. AG Bonn, Urteil v. 05.07.2007 - Az.: 9 C 177/07; Kleszczewski in: Berliner Kommentar zum Telekommunikationsgesetz, § 100 Rz.8; Wittern in: Beck'scher TKG-Kommentar, 3. Auflage 2006, § 100 Rdnr. 1 und 6.

<sup>64</sup> Wittern in Beck'scher TKG-Kommentar, 3. Auflage 2006, § 100, Rdnr.10.

sogenannte „Rasterauswertung“ von Verbindungsdaten vornehmen. Der Provider ist demnach berechtigt, seine gesamten Datenbestände, die nicht älter sind als sechs Monate (§ 100 Abs. 3 Satz 2 TKG) nach solchen Daten auszuwerten, die konkrete Indizien für eine missbräuchliche Inanspruchnahme des Dienstes enthalten. Geeignete Filterkriterien können eine stark erhöhte oder ansteigende Nutzungsfrequenz oder Verbindung über ungewöhnlich lange Zeiträume sein. Im Bereich des Datenverkehrs ist bei der Bekämpfung von Botnetzen die Filterung nach Support-Scans zulässig, die zur Vorbereitung von Hacking-Maßnahmen an Netzknoten des Datenübertragungsnetzes auf IP-Protokoll-Basis und zur Ausforschung von verwundbaren Systemen genutzt werden. Auch hier ist jedoch das Verhältnismäßigkeitsprinzip mit seinen drei Säulen der Erforderlichkeit, Geeignetheit und Angemessenheit der Maßnahme zu beachten

*Schließlich sollte folgendes berücksichtigt werden:* Aufgrund des mit solchen Maßnahmen einhergehenden weitreichenden Eingriffes in Datenschutzbelange unbeteiligter Dritter ist eine Information der Bundesnetzagentur oder des Bundesbeauftragten für den Datenschutz über die Einführung oder Änderungen des Filterverfahrens vorgeschrieben (§ 100 Abs. 3 Satz 5 TKG).

## VI. Zusammenfassende rechtliche Bewertung der Abwehrmaßnahmen

### **1. Zentrale Blockierung durch Blacklists**

Ohne vorherige Zustimmung des Nutzers zu diesem Vorgehen ist eine zentrale Blockierung rechtlich problematisch. Das Zurückschicken oder Löschen von E-Mails ohne vorherige Nutzereinwilligung kann insbesondere eine strafbare Unterdrückung der Sendung nach § 206 Abs. 2 Nr. 2 StGB oder auch als Datenunterdrücken nach § 303a Abs. 1 Alt. 2 StGB darstellen.

Bei virenverseuchten E-Mails oder bei massiven Spam-Wellen kann das Verhalten auch ohne besondere Einwilligung nach § 109 TKG gerechtfertigt sein, da der Provider danach verpflichtet ist, geeignete Schutzmaßnahmen für die Systemsicherheit zu ergreifen. Die datenschutzrechtliche Erlaubnis zu der Verwendung der hierfür erforderlichen Bestands- und Verkehrsdaten ergibt sich aus § 100 Abs. 1 bzw. Abs. 3 TKG.

Die Pflege und Verwaltung der Blacklist ist für den Provider mit zahlreichen Verpflichtungen verbunden, betreffend unter anderem die Auswahl der Informationsquellen und die Einhaltung von Kontrollmechanismen. Die Verletzung dieser Pflichten kann Unterlassungs- und Schadensersatzansprüche gegen ihn seitens der Kunden oder unberechtigt eingetragenen Dritten begründen.

## ***2. Filtern durch Analyse des Headers***

Vor dem Hintergrund des Fernmeldegeheimnisses, das Inhalte wie auch Verbindungsdaten vor Kenntnisnahme schützt, ist eine Filterung allenfalls zulässig, wenn sie automatisiert erfolgt und eine Kenntnisnahme durch Administratoren ausgeschlossen ist. Unbedenklich ist insoweit die Praxis im automatisierten Verfahren einer E-Mail eine (Punkt-)Bewertung ihrer Spam-Wahrscheinlichkeit zuzuordnen und diese Bewertung an den E-Mail-Header anzufügen. Die Verwendung von Verbindungsdaten ohne die Einwilligung kann nach den restriktiv auszulegenden Voraussetzungen des § 100 TKG gerechtfertigt sein.

## ***3. Filtern durch Analyse des E-Mail-Textes oder des E-Mail-Anhanges***

Unbedenklich ist ein Virenscanning von ein und ausgehenden E-Mails, solange es automatisiert abläuft und keine Kenntnisnahme des Kontrollvorganges oder -ergebnisses, etwa durch Administratoren, stattfindet. Allerdings muss das Inhalts-Scanning auf fest definierte

Virensignaturen begrenzt bleiben und darf ein Scanning nach frei wählbaren Stichworten nicht zulassen. Ohne ausdrückliche Einwilligung der Nutzer verbietet sich eine inhaltliche, stichwortbasierte Kontrolle von E-Mails als unzulässige Inhaltskontrolle aus datenschutzrechtlichen Gründen und als strafbare Verletzung des Telekommunikationsgeheimnisses. Bei virenverseuchten E-Mails kann das Verhalten auch ohne besondere Einwilligung nach § 109 TKG gerechtfertigt sein, da der Provider danach verpflichtet ist, geeignete Schutzmaßnahmen für die Systemsicherheit zu ergreifen.

Im Allgemeinen gilt, dass nur derartige Filterlösungen, die auf einer umfassenden vorherigen Einwilligung des Nutzer beruhen und ihm die eigene Entscheidung überlassen, bei welchem Schwellenwert er welche Aktion unternimmt, datenschutzrechtlich, zivil- und strafrechtlich unbedenklich sind.

#### ***4. Löschen von E-Mails bzw. Mailanhängen***

Grundsätzlich liegt die alleinige Verfügungsbefugnis über E-Mails beim Nutzer des Maildienstes. E-Mails dürfen diesem nicht – auch nicht zeitweilig – vorenthalten werden und auch nur entsprechend dem Vertrag mit dem Nutzer gelöscht werden. Ansonsten besteht beim Löschen von E-Mails ohne Einbeziehung des Nutzers nicht nur das Risiko einer Vertragsverletzung, sondern vor allem auch eine Strafbarkeit wegen der unbefugten Unterdrückung der Sendung nach § 206 Abs. 2 Nr. 2 StGB sowie einer Datenveränderung durch Unterdrücken bzw. Unbrauchbarmachen von Daten, die für den E-Mail-Empfänger bestimmt sind. Ohne die Einwilligung des Nutzers kann das Löschen von virenverseuchten E-Mails oder deren Anhängen aus Gründen der gebotenen Aufrechterhaltung der Systemsicherheit nach § 109 TKG gerechtfertigt sein.

## VII. Ausblick

Bei allen Maßnahmen gegen Spam, Spyware oder Malware sind die widerstreitenden Interessen sorgfältig abzuwägen. Auf der einen Seite muss die Datensicherheit gewährleistet und die IT-Systeme vor Schäden durch Viren oder Spamflut geschützt werden. Über das berechnete Eigeninteresse des Providers am Schutz seiner Systeme hinaus treffen ihn vertragliche und gesetzliche Pflichten, das Fernmeldegeheimnis und den Schutz personenbezogener Daten technisch und organisatorisch sicherzustellen sowie das informationelle Selbstbestimmungsrecht der am Datenverkehr Beteiligten nicht außer Acht zu lassen. Vor dem Hintergrund der nach wie vor bestehenden Rechtsunsicherheit empfiehlt der eco Verband den Betreibern von E-Mail-Serverdienstleistungen eine möglichst große Transparenz gegenüber ihren Kunden zu pflegen. Dies setzt voraus, dass die Kunden vertraglich über die Art und den Umfang der Maßnahmen zur Spam-Abwehr informiert werden. Wie bereits im Jahre 2004 im Rahmen des Anti-Spam-Task-Force Whitepaper vom eco Verband empfohlen<sup>65</sup>, ist der Betreiber von E-Mail-Servern gut beraten, sich das vorherige ausdrückliche Einverständnis seiner Kunden in die jeweiligen Anti-Spam-Maßnahmen zu sichern.

Dezember 2007

eco - Verband der deutschen Internetwirtschaft e. V.

---

<sup>65</sup> Vgl. unter: <http://www.eco.de/initiativen/1463.htm>