CyLaw-Report IV

CyLaw-Report IV : „E-Mail-Filter I“

Entscheidung des OLG Karlsruhe vom 10.01.2005 – Az.: 1 Ws 152/04 -

Das FÖR[1] an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) ist verantwortlich für das SicAri-Teilprojekt[*] "Cyberlaw“[2]. Mit den CyLaw-Reports soll das rechtswissenschaftliche Diskursangebot L.O.S. (Legal Open Source), das bisher nur Rechtsquellen (SicAri-Cyberlaw) enthält, um Rechtsprechung ergänzt werden. Die CyLaw-Reports-Idee ist es, auch Nicht-Juristen an grundlegender und/oder aktueller Cyberlaw-Rechtsprechung und juristischer Methodik fokusssiert teilhaben zu lassen. Fragestellungen, die spezielles juristisches Wissen voraussetzen werden mit dem Kürzel „FEX“ (Für Experten) gekennzeichnet. Hintergrundwissen wird unter der Überschrift „FÖR-Glossar“ ergänzt. Aus Gründen der Präsentationsstrategie wird zwischen „clear cases“, die eine relativ einfache rechtliche Prüfung erfordern, und „hard cases“, die eine vertiefte Diskussion erfordern, unterschieden. In keinem Falle ist mit den CyLaw-Reports die Übernahme von Haftung verbunden.
Die Entscheidung des OLG Karlsruhe wurde ausgewählt, weil sie – soweit ersichtlich – die erste Entscheidung zur Filterung von E-Mails ist.

Gliederung:

[*] Die Arbeiten am CyLaw-Report werden im Rahmen des Projektes SicAri vom Bundesministerium für Bildung und Forschung gefördert.

A. E-Mail-Filterung – „Clear Case"

I. Sachverhalt

Der Unternehmer X bietet seinen Mitarbeitern an, Kommunikationseinrichtungen wie insbesondere Internet und E-Mail zu privaten wie zu geschäftlichen Zwecken zu nutzen. Um sein System vor schädlichen Programmen (Viren) zu schützen, hat X eine Filter-Software installiert. Virenbehaftete E-Mails werden nach dem Eingang auf dem Server des X von der Filter-Software erkannt, ausgefiltert und gelöscht. Mitarbeiter M nutzt das Angebot des X. M meint, X dürfe nicht einfach fremde E-Mails löschen. Dies sei sogar strafbar.

II. Strafbarkeit des X wegen Verletzung des Fernmeldegeheimnisses

X könnte sich durch die Verwendung der Filter-Software wegen Verletzung des Fernmeldegeheimnisses, insbesondere durch Unterdrückung der Sendung (§ 206 Abs. 2 Nr. 2 Strafgesetzbuch), strafbar machen.

§ 206 StGB [Verletzung des Post- oder Fernmeldegeheimnisses]
(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt
1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.
(3) Die Absätze 1 und 2 gelten auch für Personen, die
1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mir dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.
(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

1. Tatbestandmäßigkeit (Objektiver Tatbestand)

a. Unternehmen, das geschäftsmäßig Telekommunikationsdienste erbringt

X muss mit seinem Unternehmen „geschäftsmäßig Telekommunikationsdienste erbringen“, um als Täter des Delikts in Frage zu kommen.

Eine Legaldefinition bietet § 3 Nr. 30 Telekommunikationsgesetz (TKG).

§ 3 TKG [Begriffsbestimmungen]
Im Sinne dieses Gesetzes ist oder sind
(…)
10. „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht;
(…)

Das Unternehmen des X bietet Telekommunikationsdienste an. Dies geschieht auch nachhaltig, denn das Angebot ist auf Dauer angelegt. Auf eine Gewinnerzielungsabsicht kommt es gerade nicht an. Die Mitarbeiter sind schließlich auch Dritte in diesem Sinne. Dieses Merkmal liegt nur dann nicht vor, wenn die Telekommunikationsdienste ausschließlich für den betrieblichen Eigenbedarf bestimmt sind. Sobald auch eine private Nutzung durch die Mitarbeiter erfolgt, ist dies nicht mehr der Fall. Die Arbeitnehmer sind als Dritte anzusehen.

b. zur Übermittlung anvertraute Sendung

- **Sendung**

Es muss zunächst eine Sendung vorliegen. Fraglich ist, ob dies zwingend ein körperlicher Gegenstand wie etwa ein Brief sein muss oder ob auch nichtkörperliche Sendungen wie hier eine E-Mail von der Vorschrift erfasst sind.

Gegen eine Geltung der Norm auch für E-Mails könnte der Wortlaut von § 206 Abs. 2 Nr. 1 StGB sprechen, der verschlossene Sendungen nennt. Eine E-Mail kann aber nicht wie ein Brief verschlossen werden. Dem entspräche bei der E-Mail noch am ehesten eine Verschlüsselung. Verschlossenheit und Verschlüsselung können aber nicht gleichgesetzt werden. Ein Brief kann nämlich sowohl verschlossen als auch verschlüsselt im Sinne von chiffriert werden. Dies zeigt, dass beides wesentlich verschieden ist. Bei der E-Mail gibt es eben nur die Möglichkeit der Verschlüsselung und nicht die des Verschließens.

Für eine Geltung des § 206 Abs. 2 Nr. 2 StGB auch für E-Mails spricht hingegen, dass § 206 Abs. 2 Nr. 2 StGB im Gegensatz zu Nr. 1 gerade nicht von verschlossenen, sondern nur von zur Übermittlung anvertrauten Sendungen spricht. Außerdem verbliebe § 206 Abs. 2 Nr. 2 im Telekommunikationssektor kaum ein Anwendungsbereich, wenn dieser sich nur auf körperliche Sendungen bezöge. Schließlich ist auch die herkömmliche Telekommunikation nichtkörperlich.

Danach könnte in einer E-Mail eine Sendung in diesem Sinne gesehen werden.

- **„zur Übermittlung“**

Diese Sendung soll auch durch X an den jeweiligen Adressaten übermittelt, also weitergeleitet werden.

- **„anvertraut“**

Schließlich wird die Sendung dem X auch anvertraut. Anvertraut ist eine Sendung immer dann, wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet. Die an M gerichteten E-Mails werden zunächst vom Server des X angenommen und befinden sich daher im Gewahrsam des X.

c. "Unterdrücken"

Die Sendungen des M müssten von X unterdrückt werden. Voraussetzung hierfür ist, dass die Sendung dem ordnungsgemäßen Post- oder Telekommunikationsverkehr entzogen wird. Dies ist hier der Fall. Die E-Mails des M werden von der Filter-Software ausgefiltert und gelöscht.

d. Unbefugt

X muss dabei auch unbefugt handeln. Das Merkmal unbefugt könnte etwa nicht vorliegen, wenn der Betroffene in die Verwendung der Filter-Software eingewilligt hat. Dies hat M aber nicht getan.

In der Position des X könnte man aber bei virenbehafteten E-Mails davon ausgehen, dass keiner der Mitarbeiter solche E-Mails erhalten möchte. Der Mitarbeiter müsste zur Vermeidung von Schäden die E-Mails nach Erhalt sowieso löschen. Daher könnte man ein Einverständnis der Mitarbeiter unterstellen.[3]

2. Tatbestandsmäßigkeit (Subjektiver Tatbestand)

Das Handeln des X muss auch vorsätzlich erfolgen. Davon kann bei der willentlichen Installation einer Filter-Software ausgegangen werden.

3. Rechtswidrigkeit

Die Handlung des X muss auch rechtswidrig sein. Die Rechtswidrigkeit könnte nach Ansicht des OLG Karlsruhe[4] entfallen, wenn eine andere gesetzliche Vorschrift, die sich ausdrücklich auf Telekommunikationsvorgänge bezieht, das Verhalten des X erlaubt. Die Maßnahmen des X könnten zum technischen Schutz seines E-Mail-Systems erlaubt sein (§ 109 Abs. 1 Nr. 2 TKG).

§ 109 [Technische Schutzmaßnahmen]
(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze
1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen.

Durch schädliche Programme, die in E-Mails enthalten sind, wie Viren oder Würmer kann es zu unerlaubten Zugriffen kommen. Daher könnte die Ausfilterung von virenbehafteten E-Mails als durch § 109 Abs. 1 Nr. 2 TKG gerechtfertigt angesehen werden. Die Ausfilterung verhindert unter Umständen gewichtige Schäden und beeinträchtigt demgegenüber das Interesse der Adressaten der E-Mails nur geringfügig. Die Filtermaßnahme kann daher als „angemessene technische Vorkehrung“ und folglich als gerechtfertigt angesehen werden.[5]

4. Schuld

Würde man die Verwendung des E-Mail-Filters nicht als gerechtfertigt ansehen, läge auch ein schuldhaftes Handeln des X vor, da schuldausschließende Gründe nicht ersichtlich sind.

5. Ergebnis

X macht sich nach hier vertretener Auffassung nicht strafbar wegen Verletzung des Fernmeldegeheimnisses (§ 206 Abs. 2 Nr. 2 StGB). Entweder schließt die vermutete Einwilligung der Betroffenen bereits die Verwirklichung des Tatbestandes aus oder die Handlung des X ist gerechtfertigt durch § 109 Abs. 1 Nr. 2 TKG.

III. Strafbarkeit des X wegen Datenveränderung

X könnte sich durch das Löschen der E-Mails wegen Datenveränderung strafbar machen (§ 303a StGB). Zwar hat das OLG Karlsruhe in seiner Entscheidung diesen Straftatbestand nicht geprüft. Wegen der Parallelität in den Voraussetzungen – die Tathandlung ist jeweils das Unterdrücken von Daten – liegt eine Prüfung jedoch nahe.

§ 303a StGB [Datenveränderung]
(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 202a StGB [Ausspähen von Daten]
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

1. Tatbestandsmäßigkeit (Objektiver Tatbestand)

a. Daten

Bei den E-Mails muss es sich um Daten im Sinne des § 202a Abs. 2 StGB handeln. E-Mails sind Daten. Diese werden auch „nicht unmittelbar wahrnehmbar gespeichert“, da sie nur mit technischen Hilfsmitteln und nicht allein mit den menschlichen Sinnen wahrnehmbar sind. E-Mails sind damit Daten (§ 202a Abs. 2 StGB).

b. Fremdheit der Daten?

- Fraglich ist, ob § 303a Abs. 1 StGB die Veränderung jeglicher Daten erfasst. Dann wäre auch das Löschen eigener Daten am eigenen Computer strafbar. Man könnte argumentieren, dass dieses Ergebnis offensichtlich unsinnig wäre. Sinn und Zweck des § 303a StGB könnte darin gesehen werden, Daten vor der Löschung oder Veränderung durch dazu nicht berechtigte Personen zu schützen (teleologische Auslegung). Dies dient dem Interesse des Berechtigten an der Erhaltung seiner Daten – sowohl hinsichtlich ihrer Existenz als auch ihrer Integrität. Für diese Auffassung könnte auch die systematische Auslegung sprechen. § 303a StGB folgt auf § 303 StGB, der die Sachbeschädigung unter Strafe stellt.

§ 303 StGB [Sachbeschädigung]
(1) Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

§ 303 StGB regelt nur die Beschädigung oder Zerstörung von Sachen. Daten sind keine körperlichen Gegenstände und daher nicht vom Begriff „Sache“ erfasst. § 303a StGB ergänzt § 303 StGB also nur. Die Sachbeschädigung (§ 303 StGB) bezieht sich aber eindeutig nach dem Wortlaut nur auf fremde Sachen. Wegen der

Parallelität der Vorschriften könnte sich § 303a StGB ebenfalls nur auf fremde Daten beziehen.

- Würde man dieser Auffassung folgen, dann müssten die Daten für X fremd sein. Die E-Mails stammen von Dritten. Die E-Mails werden von diesen Dritten erstellt und dann versandt. Mit der Versendung könnte die Verfügungsbefugnis der Absender aufhören, da sie die Daten aus ihrem Bereich entlassen und weggeschickt haben.[6] Entsprechend könnte dies auf Empfängerseite zu sehen sein: Mit dem Empfang der E-Mail hätte der M Verfügungsbefugnis erlangt.
- Es stellt sich dann die Frage, wann ein Empfänger eine E-Mail empfangen hat. Dies könnte in dem Zeitpunkt der Fall sein, in dem die E-Mail in die Mailbox des Empfängers gelangt. Dafür könnte zum einen eine systematische Auslegung sprechen. § 206 StGB könnte § 303a StGB nämlich insoweit ergänzen, als die Zwischenphase des Transports der Daten von § 206 StGB geschützt wäre.
- Die E-Mails gelangen in vorliegenden Fall gar nicht in die Mailbox des M, X filtert sie schon vorher aus. Folgte man der eben dargestellten Auffassung, dann hätten zu diesem Zeitpunkt weder die Absender noch Empfänger M eine Verfügungsbefugnis über die Daten. Die Daten wären nicht fremd für X – auch wenn X sich nach § 206 StGB strafbar machen kann.

2. Ergebnis

X würde sich damit nicht wegen Datenveränderung strafbar machen. Sieht man dies anders und hält die Daten doch für fremd, dann könnte eine Einwilligung des M vorliegen, virenbehaftete E-Mails auszufiltern. Liegt eine solche nicht vor oder kann sie nicht vermutet werden, dann käme außerdem ebenfalls eine Rechtfertigung als technische Schutzmaßnahme in Betracht.

Im Ergebnis liegt nach hier vertretener Auffassung keine Strafbarkeit wegen Datenveränderung vor.

B. E-Mail-Filterung – "Hard Case"

I. Sachverhalt

Der Sachverhalt ist an die Entscheidung des OLG Karlsruhe vom 10.01.2005[7] angelehnt.

> Die Hochschule H bietet ihren Mitarbeitern an, Kommunikationseinrichtungen wie insbesondere Internet und E-Mail zu privaten wie zu geschäftlichen Zwecken zu nutzen. Auch der externe Mitarbeiter M nutzt diese Möglichkeit. Der Leiter des Hochschulrechenzentrums U setzt, ohne seine Mitarbeiter zu informieren, ein E-Mail-Filtersystem ein, das M als nicht vertrauenswürdigen Absender ansieht. Dies hat zur Folge, dass die E-Mails des M zwar zunächst vom Mail-Server des U angenommen, dann aber unternehmensintern ausgefiltert und nicht an die vorgesehenen Empfänger ausgeliefert werden. M erhält dann eine Fehlermeldung. Die vorgesehenen Empfänger der Mails erhalten keine Benachrichtigung.

II. Strafbarkeit des U wegen Verletzung des Fernmeldegeheimnisses

U könnte sich durch die Verwendung der Filter-Software wegen Verletzung des Fernmeldegeheimnisses durch Unterdrückung der Sendung (§ 206 Abs. 2 Nr. 2 StGB), strafbar gemacht haben.

1. Tatbestandsmäßigkeit (Objektiver Tatbestand)

a. Unternehmen, das geschäftsmäßig Telekommunikationsdienste erbringt

Die Hochschule H muss ein Unternehmen sein, das geschäftsmäßig Telekommunikationsdienste erbringt, damit U Täter des Delikts sein kann. Ein „geschäftsmäßiges Erbringen von Telekommunikationsdiensten" liegt vor (siehe oben unter A III 1).

H muss auch ein Unternehmen darstellen. Dies könnte im Hinblick auf die hoheitliche Tätigkeit der H zweifelhaft sein. Ausgehend vom Zweck der Norm, sowohl das subjektive Recht auf Geheimhaltung wie den Anspruch auf Übermittlung einer Sendung zu schützen, könnte der Unternehmensbegriff aber weit auszulegen sein. Davon ausgehend wäre jede Betätigung im geschäftlichen Verkehr, die nicht ausschließlich hoheitlich erfolgt oder auf eine rein private Tätigkeit beschränkt ist, als Unternehmen anzusehen. Durch das Angebot der H an ihre Mitarbeiter, die Telekommunikationsdienste auch privat zu nutzen, liegt keine ausschließlich hoheitliche Tätigkeit mehr vor. H ist daher nach hier vertretener Auffassung Unternehmen.

„Betätigt sich aber die Universität nicht ausschließlich hoheitlich, sondern stellt ihre TK-Anlage unterschiedlichen Nutzergruppen (Mitarbeitern der Universität, Vereinen, außenstehenden Dritten) zur Verfügung, so ist eine Abgrenzung zwischen dienstlichen, wissenschaftlichen und Studienzwecken, privaten und auch wirtschaftlichen Zwecken nicht mehr möglich. Dadurch aber wird die Universität auch außerhalb ihres hoheitlichen Aufgabengebiets tätig und nimmt wie jeder beliebige Dritte am geschäftlichen Verkehr teil, sodass für diesen Betätigungsbereich auch die Maßstäbe gelten müssen, wie für jedermann, der auf diesem Gebiet geschäftlich tätig wird.“[8]

U als Leiter des Rechenzentrums der H kann sich also aus § 206 Abs. 2 StGB strafbar machen.

b. zur Übermittlung anvertraute Sendung

Die E-Mails des M stellen Sendungen dar (siehe oben unter A III 2).

„Der Begriff Sendung i.S.v. § 206 Abs. 2 Nr. 2 StGB erstreckt sich auch auf unkörperliche Gegenstände, da § 206 Abs. 2 Nr. 2 StGB nicht - wie § 206 Abs. 2 Nr. 1 StGB - auf verschlossene Sendungen beschränkt ist. Tatobjekte des § 206 Abs. 2 Nr. 2 StGB sind daher nicht nur unverschlossene Postsendungen, sondern auch jede Form der dem Fernmeldegeheimnis unterliegenden Telekommunikation.“[9]

Diese wurden U auch zur Übermittlung anvertraut. Die Sendungen sollten durch U als Leiter des Rechenzentrums der H an den jeweiligen Adressaten übermittelt, also weitergeleitet werden. Da die E-Mails des M zunächst vom Mail-Server des Hochschulrechenzentrums angenommen werden, befinden sie sich im Gewahrsam des U und sind damit „anvertraut“.

„Unproblematisch liegt der Gewahrsam an einer E-Mail spätestens dann vor, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht

hat und der versendende Mailserver die Daten dem empfangenden Server übermittelt hat.“[10]

c. “Unterdrücken“

Ein „Unterdrücken“ liegt vor, wenn die Sendung dem ordnungsgemäßen Post- oder Telekommunikationsverkehr entzogen wird. Dies ist hier geschehen. Die E-Mails des M wurden von der Filter-Software ausgefiltert und nicht an die bestimmungsgemäßen Empfänger weitergeleitet. Gleichgültig ist dabei, ob U die E-Mails des M letztlich löscht oder ob er sie archiviert etc. Nicht nur die Vernichtung einer Sendung stellt ein Unterdrücken dar, sondern bereits das längere Zurückhalten einer Sendung, wenn dies zu einer Verzögerung der Zustellung führt. Diese Schwelle wurde hier eindeutig überschritten.

„Soweit auch die Auffassung vertreten wird, dass ein Unterdrücken bei einer E-Mail nicht das Zerstören oder Beschädigen der Nachricht, also ihr Löschen, Verstümmeln oder Verkürzen ist, sondern nur ihr vollständiges oder vorübergehendes Zurückhalten oder Umleiten an eine andere Adresse greift dies zu kurz; denn letztlich kann es keinen Unterschied machen, wie verhindert wird, dass die Nachricht ihren Empfänger erreicht, nämlich ob dies durch Zurückhalten oder Umleiten der E-Mail oder durch deren Löschung oder sonstige Verstümmelung geschieht.“[11]

d. Unbefugt

Auch ein unbefugtes Handeln des U liegt vor, denn M hat nicht in die Verwendung der Filtersoftware eingewilligt. Für ein vermutetes Einverständnis des M ist bei objektiv ungefährlichen E-Mails kein Raum. Ein solches vermutetes Einverständnis mit der Ausfilterung kann nur bei tatsächlich von Viren betroffenen E-Mails in Betracht kommen.

2. Tatbestandsmäßigkeit (subjektiver Tatbestand)

Im Hinblick auf die willentliche Installation der Filter-Software kann von einem vorsätzlichen Handeln des U ausgegangen werden.

3. Rechtswidrigkeit

Die Maßnahmen des U könnten nach Ansicht des OLG Karlsruhe[12] zum technischen Schutz seines E-Mail-Systems erlaubt sein (§ 109 Abs. 1 Nr. 2 TKG). IT-Sicherheit kann damit den Einsatz von Filter-Software rechtfertigen.

Von M muss ein unerlaubter Zugriff auf das E-Mail-System des U erfolgt oder befürchtet worden sein. Ein solcher unerlaubter Zugriff könnte im Zusammenhang mit Viren, Würmern oder sonstigen schädlichen Programmen befürchtet werden. Die E-Mails des M enthielten aber keine derartigen Programme.

Die Maßnahme des U könnte dann trotzdem als gerechtfertigt erscheinen, wenn es irgendwelche Anhaltspunkte dafür gab, dass die E-Mails des M solche Programme oder Viren etc. enthielten. Auch dies war aber nicht der Fall. Die rein subjektive Einschätzung von U, der M sei nicht (mehr) vertrauenswürdig, kann ohne einen entsprechenden Tatsachenhintergrund die Unterdrückungshandlung nicht rechtfertigen.

> „U.U. kann es daher gerechtfertigt sein, eine E-Mail herauszufiltern, z.B. dann, wenn eine E-Mail mit Viren behaftet ist, sodass bei deren Verbreitung Störungen oder Schäden der TK- und Datenverarbeitungssysteme eintreten. Irgendwelche dementsprechenden Anhaltspunkte aber, die zu einem Herausfiltern der E-Mails (…) berechtigt hätten, fehlen, sodass in diesen Fällen ein „Herausfiltern“ der E-Mails unbefugt erfolgte.“[13]

Das Verhalten des U war daher rechtswidrig.

4. Schuld

U hat auch schuldhaft gehandelt. Ihm war zwar möglicherweise nicht klar, dass die Verwendung von Filter-Software strafbar sein kann, diese Unkenntnis allein reicht aber nicht, sein Verhalten zu entschuldigen. U hätte sich besser informieren müssen.

5. Ergebnis

U hat sich wegen Verletzung des Fernmeldegeheimnisses strafbar gemacht (§ 206 Abs. 2 Nr. 2 StGB).

C. Schlussfolgerungen aus der Entscheidung des OLG Karlsruhe

Aus der Entscheidung des OLG Karlsruhe ergeben sich folgende Schlussfolgerungen:

- Eine Universität kann ein Unternehmen im Sinne des § 206 Abs. 1 StGB darstellen. Dies ist im Bereich von Telekommunikationsdiensten dann der Fall, wenn diese auch zur privaten Nutzung angeboten werden. Die Universität nimmt dann wie jedes andere Unternehmen am Geschäftsverkehr teil.
- Eine E-Mail stellt eine Sendung im Sinne des § 206 Abs. 2 Nr. 2 StGB dar.
- Diese Sendung ist einem Unternehmen „anvertraut“ und befindet sich in dessen Gewahrsam, wenn der versendende Server die Daten an den empfangenden Server übermittelt hat.
- Ein „Unterdrücken“ im Sinne der Vorschrift liegt sowohl bei einer Löschung oder Vernichtung der Sendung wie auch bei einer sonstigen Verhinderung des Zugangs der Sendung vor.
- Eine Rechtfertigung von Filterungsmaßnahmen kommt grundsätzlich nach § 109 Abs. 1 Nr. 2 TKG in Betracht. Dies allerdings nur, wenn es tatsächliche Anhaltspunkte dafür gibt, dass eine E-Mail mit Viren oder sonstigen schädlichen Programmen behaftet ist. Die generelle Einstufung der E-Mails eines Absenders als gefährlich kann daher nicht als gerechtfertigt angesehen werden.

[1] Informationen zu FÖR (Fachgebiet Öffentliches Recht) finden Sie unter http://www.bwl.tu-darmstadt.de/jus4/?FG=jus.
[2] Cyberlaw (in einer öffentlich-rechtlichen Betrachtung) ist ein Oberbegriff für Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace und der Cyberworld befassen.
[3] Anders könnte dies z.B. bei Spam-Mails zu sehen sein: Bei Spam kann man eventuell nicht einfach unterstellen, dass sich der Empfänger nicht für die transportierte Werbebotschaft interessiert.
[4] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (180).
[5] Das OLG Karlsruhe lässt offen, ob daneben auch ein Rückgriff auf die allgemeinen strafrechtlichen Rechtfertigungsgründe, insbesondere auf den rechtfertigenden Notstand, möglich wäre.

> **§ 34 StGB [Rechtfertigender Notstand]**
> Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

Auch hier müssen die widerstreitenden Interessen gegeneinander abgewogen werden: einerseits das Interesse an einem reibungslosen Funktionieren des Computersystems des X und andererseits das Interesse der Mitarbeiter, an sie gerichtete E-Mails auch tatsächlich zu erhalten. Das Ausfiltern virenbehafteter E-Mails könnte auch im Rahmen des § 34 StGB mit paralleler Argumentation als gerechtfertigt angesehen werden.
[6] FEX: Man könnte folgende Überlegung anstellen: Würde man eine weiter andauernde Verfügungsbefugnis der Absender bejahen, dürfte niemand empfangene E-Mails löschen, da der Absender immer noch Rechte daran hätte.
[7] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178.
[8] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (180).
[9] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (180).
[10] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (180).
[11] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (180).
[12] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (180).
[13] Beschluss des OLG Karlsruhe vom 10.01.2005, Az.: 1 Ws 152/04, MMR 2005, 178 (181).

Prof. Dr. Viola Schmid, LL.M. (Harvard) - **schmid@jus.tu-darmstadt.de**