Rechtliche Zulässigkeit von Blacklisting und Greylisting

A. BEDEUTUNG DES GUTACHTENS FÜR IT-VERANTWORTLICHE UND DIE HOCHSCHULLEITUNG

Spam und mit Schadsoftware behaftete E-Mails machen seit Jahren einen großen Anteil des weltweiten E-Mail-Verkehrs aus. Derzeit wird angenommen, dass ca. 95 % aller E-Mails solch unerwünschte Inhalte enthalten. Im Fall einer Übertragung all dieser E-Mails auf den E-Mail-Server des Adressaten, würden die Systeme unmittelbar überlastet werden. Die E-Mails würden infolgedessen nur unter erheblicher Zeitverzögerung zugestellt werden können. Wenn derartige Verzögerungen vermieden werden sollen, müssten die Betreiber von E-Mail-Servern ihre Systeme kontinuierlich aufrüsten, wobei erhebliche Kosten entstehen würden.

Um diese Situation zu entschärfen, gibt es technische Filtermethoden, die bereits vor der Übertragung der E-Mail auf den Empfänger-Server ansetzen. Diese frühzeitige Filterung verhindert die Überlastung der technischen Systeme und trägt dazu bei, dass eingehende E-Mails zeitnah an den Adressaten zugestellt werden können. Zwei hierfür häufig angewendete Verfahren sind das Blacklisting und das Greylisting, welche im folgenden Gutachten rechtlich untersucht werden. Beim Blacklisting wird die IP-Adresse des Versender-Servers mit einer Datenbank abgeglichen. Enthält die Datenbank diese IP-Adresse, wird die E-Mail unabhängig von deren Inhalt abgeblockt. Dem Versender-Server wird hierüber eine Benachrichtigung geschickt, damit ggf. ein zweiter Zustellversuch unternommen werden kann. Ist die IP-Adresse nicht in der Datenbank enthalten, wird die E-Mail auf den Empfänger-Server übertragen und dort ggf. lokal auf ihren Spam-Gehalt untersucht. Beim Greylisting hingegen wird jede E-Mail zunächst abgeblockt. Wird dann von einem korrekt konfigurierten E-Mail-Server ein zweiter Zustellversuch von derselben E-Mail-Adresse an denselben Adressaten unternommen, wird die E-Mail angenommen. Ausgangspunkt ist hierbei die Hypothese, dass Spam-Versender im Gegensatz zu seriösen Versender-Servern keine zweiten Zustellungsversuche unternehmen.

Rechtliche Probleme bei diesen Verfahren können sich vor allem im Datenschutzrecht und im Strafrecht ergeben. Ebenso muss die Vereinbarkeit mit dem Fernmeldegeheimnis beachtet werden und es stellt sich die Frage, ob der Provider aufgrund des Nutzungsverhältnisses verpflichtet ist, jegliche E-Mails zuzustellen. In dem folgenden Gutachten (Punkt B) werden diese Fragen rechtlich bewertet und die Forschungsstelle Recht kommt zu dem Ergebnis, dass sowohl Black- als auch Greylisting rechtlich zulässig sind, soweit der Provider sich an zuverlässige Anbieter dieser Verfahren wendet. Zu Bedenken ist jedoch, dass es bisher kaum gerichtliche Entscheidungen zu dieser Thematik gibt. Im Anschluss an das Gutachten (Punkt C) folgt eine kurze Übersicht über die Ergebnisse der einzelnen untersuchten Problempunkte.

B. GUTACHTEN

I. Rechtliche Zulässigkeit von Blacklisting

Ob Blacklisting zulässig ist, richtet sich in erster Linie nach denjenigen rechtlichen Vorschriften, die die Beachtung von Datenschutz und Fernmeldegeheimnis sicherstellen sollen. Dabei ist der Zeitpunkt relevant, zu dem die IP-Adresse des Versender-Servers mit der Blacklist abgeglichen werden soll: Die früheste Möglichkeit (1.) für diesen Abgleich besteht, sobald die Verbindung zum Empfänger-Server aufgebaut ist, aber noch keine weiteren Daten auf den Empfänger-Server übertragen wurden. Die zweite Möglichkeit (2.) setzt erst zu einem späteren Zeitpunkt an, wenn bereits der Envelope vom Empfänger-Server zur Kenntnis genommen worden ist. Dieser Zeitpunkt bietet sich vor allem dann an, wenn in Kombination zu der Blacklist auch ein Whitelisting betrieben wird, das die Kenntnis von den beteiligten E-Mail-Adressen voraussetzt. Zudem sind die Pflichten aus dem Nutzungsverhältnis bei der Verwendung von Blacklists zu beachten.

1. Blacklisting bei Verbindungsaufbau

Beim Blacklisting zu diesem Zeitpunkt kennt der Empfänger-Server lediglich die IP-Adresse des Versender-Servers und gleicht diese mit einer Blacklist ab.

a. Datenschutz

Die folgenden Ausführungen entsprechen unter Umständen nicht der ab dem 25. Mai 2018 geltenden Rechtslage. Dem hier zur Verfügung gestellten Text liegt die Rechtslage vor Geltung der Verordnung (EU) 2016/679, bekannt unter ihrem Kurztitel EU-Datenschutz-Grundverordnung (DS-GVO), zugrunde. Die Verordnung gilt ab dem 25. Mai 2018 verbindlich in allen Mitgliedsstaaten der Europäischen Union und verdrängt grundsätzlich alle nationalen Regelungen zum Datenschutzrecht.
Für den Regelungsbereich der elektronischen Kommunikation soll die DS-GVO durch die E-Privacy-Verordnung ergänzt und präzisiert werden. Diese befindet sich jedoch noch in der Beratungsphase und wird nicht rechtzeitig zum 25. Mai 2018 in Kraft treten. Es ist nicht auszuschließen, dass die E-Privacy-Verordnung für die hier dargestellten Sachverhalte wiederum neue Regelungen bereithält.
Die Forschungsstelle Recht im DFN beobachtet diese Entwicklungen und passt die datenschutzrechtlichen Ausführungen entsprechend an. Bis dahin bitten wir um Ihre Geduld.

Dem Datenschutz unterliegen „personenbezogene Daten“. Hierunter versteht man „Einzelangaben über persönliche oder sachliche Verhältnisse“ einer bestimmten oder bestimmbaren natürlichen

Person, § 3 Abs. 1 BDSG. Beim Blacklisting wird die IP-Adresse des Versender-Servers auf Protokollebene, also noch vor Übermittlung der Nachricht und der beteiligten E-Mail-Adressen, erfasst und dem Anbieter der Blacklist zum Abgleich mit dessen Datenbank übermittelt.

Nur wenn sich aus der IP-Adresse des Versender-Servers Informationen ergeben, die Aufschluss über Umstände eines Menschen geben, dessen Identität sich sofort oder mittels anderer Quellen feststellen lässt, ist Datenschutzrecht zu beachten. Beim Blacklisting bei Verbindungsaufbau wird nur die IP-Adresse des Versender-Servers erfasst und verarbeitet. Zwar wird vertreten, dass IP-Adressen generell als personenbezogene Daten anzusehen sind und dies auch für die IP-Adressen des Versender-Servers gilt.[1] Bei dieser Sichtweise wird allerdings übersehen, dass es allein anhand der IP-Adresse des Versender-Servers nicht möglich ist, einen Rückschluss auf die an dem Kommunikationsvorgang beteiligten Menschen (Absender oder Empfänger) zu ziehen. Nur der Versender-Server kann identifiziert werden. Dies lässt keinen Rückschluss auf eine Einzelperson zu und daher liegt kein personenbezogenes Datum vor. Das bedeutet, dass beim Blacklisting das Datenschutzrecht gar nicht erst Anwendung findet. Es bedarf somit weder einer Einwilligung durch den Empfänger noch einer gesetzlichen Erlaubnis oder einer Rechtfertigung.

b. Fernmeldegeheimnis nach dem Telekommunikationsgesetz

Der Anwendungsbereich des Fernmeldegeheimnisses, § 88 TKG, erstreckt sich nicht nur auf personenbezogene Daten, sondern auf sämtliche Kommunikationsdaten. Dies sind alle Informationen, die entweder Inhalt der Kommunikation sind (z.B. Text einer E-Mail oder Inhalt eines Telefongesprächs) oder Aufschluss über deren nähere Umstände geben (z.B. Zeitpunkt oder Beteiligte der Kommunikation).[2]

Die IP-Adresse des Versender-Servers ist nicht Gegenstand dessen, was der Versender dem Empfänger mitteilen wollte, weshalb sie eindeutig nicht Inhalt der Kommunikation ist. Teils wird sie jedoch als Umstand der Kommunikation angesehen.[3] Diese generelle Einordnung von IP-Adressen verkennt jedoch, dass IP-Adressen von E-Mail-Servern keinen Aufschluss über die Beteiligten der Kommunikation geben. „Beteiligte der Kommunikation“ sind nur diejenigen, die auf die Vertraulichkeit der

[1] So argumentiert etwa *Heidrich*, CR 2009, 168, 172 f., der zwar auf die Problematik der IP-Adressen von Mail-Servern eingeht, nicht jedoch zu dem Ergebnis kommt, dass diese von den IP-Adressen der Nutzer unterschieden werden müssen.

[2] *Ellinghaus* in: Arndt/Fetzer/Scherer, Telekommunikationsgesetz, § 88, Rn. 13 f.

[3] *Heidrich*, CR 2009, 168, 173, nach dessen Ansicht IP-Adressen generell als Verkehrsdaten dem Fernmeldegeheimnis unterliegen.

Kommunikation vertrauen dürfen, also Absender und Empfänger.[4] Der Versender-Server wird als technischer Übermittler tätig und ist daher selbst kein Beteiligter. Er betreibt den Kommunikationsdienst rein technisch und gibt nur fremde Daten weiter, auf deren Inhalt er keinen Einfluss und an deren Vertraulichkeit er selbst kein Interesse hat. Im Gegenteil ist er verpflichtet, die Daten unverändert und ohne Ansehung des Inhalts zu übermitteln. Darüber hinaus ist, einer allgemeineren Definition folgend, als Umstand der Kommunikation all das zu verstehen, was den jeweiligen Telekommunikationsvorgang individualisierbar macht.[5] Die Kenntnis der Tatsache, dass eine E-Mail über einen bestimmten Versender-Server verschickt wurde, ermöglicht keine Zuordnung der Kommunikation zu bestimmten Personen, sodass der Vorgang gerade nicht individualisierbar ist. Die Erfassung der IP-Adresse des Versender-Servers ist daher fernmelderechtlich unbedenklich.

c. Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB (Verletzung des Post- oder Fernmeldegeheimnisses)

Das Fernmeldegeheimnis wird strafrechtlich durch § 206 Abs. 2 Nr. 2 StGB geschützt. Danach liegt eine Strafbarkeit vor, wenn ein Unternehmen, welches geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, eine ihm zur Übermittlung anvertraute Sendung unterdrückt. Die wesentlichen Voraussetzungen sind also zum einen die „Unterdrückung" einer Sendung durch ein Telekommunikationsunternehmen und zum anderen, dass diese Sendung dem Unternehmen „zur Übermittlung anvertraut" worden ist. Unter dem Begriff des „Unternehmens" ist auch eine Hochschule als E-Mail-Provider zu verstehen, soweit die Privatnutzung zugelassen ist oder geduldet wird.[6] Unter dem Begriff des „Unterdrückens" versteht man, dass die Nachricht in vorschriftswidriger Weise dem Übertragungsvorgang entzogen, aus ihm entfernt oder von ihm ferngehalten wird, unabhängig davon, ob dies dauernd oder vorübergehend geschieht.[7] Wenn der Zustellvorgang bewusst unterbrochen und die E-Mail durch das Blacklisting endgültig abgewiesen und dem Zugriff des Empfängers dadurch vorenthalten wird, ist eine Unterdrückung zu bejahen. Allerdings muss die Sendung (E-Mail) dem Unternehmen vorher „zur Übermittlung anvertraut" worden sein, damit eine Strafbarkeit des „Unterdrückenden" vorliegen kann. Anvertraut ist die Sendung, wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet.[8] Unproblematisch liegt

[4] So wohl auch *Bock* in: Beck'scher TKG-Kommentar 3. Auflage 2006, § 88, Rn. 19.

[5] *Bock* in: Beck'scher TKG-Kommentar 3. Auflage 2006, § 88, Rn. 14.

[6] *OLG Karlsruhe*, Beschluss v. 10.01.2005 – 1 Ws 152/04; *Heidrich*, MMR 2005, 181, 181; *Cornelius/Tschoepe*, K&R 2005, 269, 269. Andere Ansicht (allerdings ohne Berücksichtigung des Urteils des OLG Karlsruhe): *Fischer,* Strafgesetzbuch, 55. Aufl. 2008, § 206, Rn. 2, der öffentlich-rechtliche Körperschaften (Universitäten) nicht als Unternehmen sieht.

[7] Vgl. *OLG Karlsruhe*, Beschluss v. 10.01.2005 – 1 Ws 152/04; *Heidrich*/*Tschoepe*, MMR 2004, 75, 77.

[8] *Heidrich/Tschoepe*; MMR 2004, 75, 77; *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 206, Rn. 12.; *Lenckner* in: Schönke/Schröder, Strafgesetzbuch, 27. Auflage, Rn. 17.

der Gewahrsam an einer E-Mail spätestens dann vor, wenn die Anfrage zur Übermittlung von Daten den Empfänger-Server des Unternehmens erreicht und der Versender-Server die Daten dem Empfänger-Server übermittelt hat.[9] Beim Blacklisting bei Verbindungsaufbau wird nur die IP-Adresse des Versender-Servers angenommen, die beiden beteiligten Server sind zu diesem Zeitpunkt im Anmeldeverfahren aber noch nicht im Zustand der Nachrichtenübermittlung. Der Empfänger-Server kann bereits in diesem Moment entscheiden, ob er die Kommunikation mit dem Versender-Server zulässt. Gute Argumente sprechen deshalb dagegen, dass bereits die Kenntnisnahme der IP-Adresse des Versender-Servers ausreicht, um ein Anvertrauen der gesamten Nachricht zu bejahen. Der Versender hat keinen Einfluss auf die IP-Adresse des Versender-Servers. Sie ist nicht Teil dessen, was er dem Empfänger mitteilen möchte, und sie lässt auch keine Rückschlüsse auf die Kommunikation zu. Des Weiteren wird sie bereits in der „Begrüßungsphase" und somit noch vor dem Austausch des eigentlichen Nachrichteninhalts übermittelt. Dies entspricht auch dem Ablauf nach dem gängigen technischen Protokoll (SMTP). Die IP-Adresse des Versender-Servers ist weder Teil noch Umstand der Telekommunikation, da sie nur Aufschluss über den Versender-Server gibt, welcher jedoch kein „Beteiligter" ist. Eine Annahme der „Sendung" als solcher kann hierin nicht gesehen werden. Deshalb ist das Kriterium des „Anvertrauens" nicht erfüllt, eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB scheidet aus.[10]

Sollte die Privatnutzung ausgeschlossen sein und auch nicht geduldet werden, ist die Hochschule ohnehin kein Diensteanbieter im Sinne des TKG und auch kein „Unternehmen" nach § 206 StGB. Eine Strafbarkeit nach dieser Vorschrift entfällt dann in jedem Fall.[11]

d. Strafbarkeit nach § 303a StGB (Datenveränderung)

Selbst wenn das Fernmeldegeheimnis nicht betroffen ist, kann dennoch eine strafbare Datenveränderung nach § 303a StGB gegeben sein. Das ist der Fall, wenn Daten rechtswidrig gelöscht, unterdrückt, unbrauchbar gemacht oder verändert werden. Unter „Daten" sind sämtliche Arten von elektronischen Daten zu verstehen, unabhängig von Personenbezug oder Übertragungsvorgang.[12] Der § 303a StGB ist in Verbindung mit § 303 StGB (Sachbeschädigung) zu verstehen.[13] Diese Vorschrift

[9] *OLG Karlsruhe*, Beschluss v. 10.01.2005 – 1 Ws 152/04; *Heidrich*/*Tschoepe*, MMR 2004, 75, 77; *Heidrich*, CR 2009, 168, 169; *Heidrich*, MMR 2005, 181, 181.

[10] *Heidrich*, CR 2009, 168, 169; *Heidrich*, MMR 2005, 181, 182. Andere Ansicht: *Heidrich/Tschoepe*; MMR 2004, 75, 77 f.; *Cornelius/Tschoepe*, K&R 2005, 269, 270.

[11] *Heidrich/Tschoepe*; MMR 2004, 75, 76.

[12] Vgl. die Legaldefinition in § 202a Abs. 2 StGB.

[13] *Wieck-Noodt* in: Münchener Kommentar zum StGB, 1. Auflage 2006, § 303a Rn. 1.

setzt die Verletzung fremden Eigentums voraus. Nun kann zwar an Daten an sich kein Eigentum erlangt werden, trotzdem ist die Reichweite der Vorschrift so einzuschränken, dass nicht alle Daten (also etwa auch eigene) erfasst werden, sondern nur solche, die einer fremden Person zugeordnet sind und über die diese Person verfügungsberechtigt ist.[14] Der Schutzzweck der Vorschrift ist daher zu sehen im Interesse des Verfügungsberechtigten an der jederzeitigen Zugriffsmöglichkeit auf die unversehrten Daten.[15] Das Abblocken der angebotenen E-Mails kann insofern ein „Unterdrücken" darstellen, als dass sie dem Empfänger vorenthalten und dessen Zugriff entzogen werden.[16] Das setzt voraus, dass der Empfänger die Verfügungsbefugnis über diese Daten hat. Aus dem Rechtsverhältnis, welches dem E-Mail-Dienst zu Grunde liegt, ergibt sich eine Verfügungsbefugnis für alle Daten (E-Mails), die der Empfänger-Server für seinen Empfänger angenommen hat und vorhält.[17] Der Empfänger erlangt also erst dann Verfügungsbefugnis über die E-Mail, wenn diese vollständig, also inklusive Header und Body, auf den Empfänger-Server übertragen worden ist; teilweise wird sogar das Einstellen der E-Mail in das Postfach des Empfängers verlangt. Eine reine Adressierung an den Empfänger reicht dagegen für eine Verfügungsbefugnis desselben nicht aus.[18] Bis zur Übertragung der Datei hat der Versender bzw. der Versender-Server die Verfügungsbefugnis.[19] Wird die Annahme verweigert, werden die Daten nicht gelöscht, sondern es wird lediglich eine Unzustellbarkeitsmitteilung versandt. Der Versender wird hierdurch darüber informiert, dass er weiterhin die Verfügungsbefugnis hat. Die Verfügungsbefugnis kann also bis zur endgültigen Annahme nur beim Versender oder beim Versender-Server liegen.[20] Stellt man darauf ab, ob der Versender auf die Daten noch Einfluss hat, ist mit dem Absenden der E-Mail die Verfügungsbefugnis auf den Versender-Server übergegangen. Andererseits spricht für einen Verbleib der Verfügungsbefugnis beim Versender, dass der Versender-Server nur aufgrund rechtlicher Verpflichtungen gegenüber dem Versender tätig wird und der Versender faktisch Herr über die Nachricht bleibt.[21] Für die Beurteilung der Rechtmäßigkeit des Blacklistings beim Verbindungsaufbau muss dies jedoch nicht entschieden werden, da der Empfänger jedenfalls noch nicht verfügungsbefugt ist und ihm dementsprechend die Verfügungsbefugnis auch

---

[14] *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 303a, Rn. 4; *Wieck-Noodt* in: Münchener Kommentar zum StGB, 1. Auflage 2006, § 303a Rn. 9 m.w.N.; *Weidemann* in: Beck'scher Online –Kommentar StGB, § 303a, Rn. 5; *Stree* in: Schönke/Schröder, Strafgesetzbuch, 27. Auflage 2006, § 303a, Rn. 3; *Jüngel/Schwan/Neumann*, MMR 2005, 820, 821.

[15] *Wieck-Noodt* in: Münchener Kommentar zum StGB, 1. Auflage 2006, § 303a Rn. 2 m.w.N.; *Heidrich/Tschoepe*; MMR 2004, 75, 79.

[16] *Stree* in: Schönke/Schröder, Strafgesetzbuch, 27. Auflage 2006, § 303a, Rn. 4; *Weidemann* in: Beck'scher Online –Kommentar StGB, § 303a, Rn. 9.

[17] *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 303a, Rn. 7.

[18] *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 303a, Rn. 7.

[19] *Jüngel/Schwan/Neumann*, MMR 2005, 820, 822 f.; *Heidrich*, CR 2009, 168, 169 f.

[20] *Heidrich*, CR 2009, 168, 170.

[21] *Jüngel/Schwan/Neumann*, MMR 2005, 820, 821 f.

nicht entzogen werden kann. Dem Versender oder dem Versender-Server wird diese ebenfalls nicht durch das Abweisen der E-Mail entzogen,[22] da sich dadurch die Zugriffsmöglichkeiten auf die E-Mail nicht verändern. Die Daten liegen – genau wie vor dem Abweisen – in unveränderter Form beim Versender-Server.

Diese Argumentation wurde bisher noch nicht durch die Rechtsprechung behandelt und auch in der juristischen Literatur hat sich noch keine eindeutige Meinung herausgebildet. Daher ist es theoretisch denkbar, dass ein Gericht, sofern es überhaupt zu einem Verfahren kommt, anders entscheidet. Wenn sich der Provider für den Fall weiter absichern möchte, dass ein Gericht die Verfügungsbefugnis des Empfängers bejaht, kann er eine Einwilligung des Empfängers in die Maßnahme einholen.[23]

e. Zulässigkeit nach dem Nutzungsverhältnis

Unabhängig von Datenschutz, Fernmeldegeheimnis oder Strafrecht sind E-Mail-Provider durch Vertrag oder durch das Nutzungsverhältnis dazu verpflichtet, die E-Mails an die adressierten Nutzer zuzustellen. Hiervon sind nicht nur die möglichen „false positives“ umfasst, sondern grundsätzlich auch Spam-Mails, zumal der Empfänger zumindest theoretisch das Interesse am Erhalt einer solchen E-Mail haben könnte.[24] Gerade im Hochschulbereich können solche Spams im Einzelfall aus einem legitimen Interesse heraus zu Forschungszwecken erwünscht sein.[25] Wenn der Provider nun mittels einer Black- oder Greylist E-Mails abweist und somit eine Zustellung verweigert, stellt sich die Frage, ob er hierdurch eine Vertragsverletzung begeht und Schadensersatzansprüchen ausgesetzt sein kann.

Die zivilrechtliche Schadensersatzhaftung wegen einer Vertragsverletzung ergibt sich aus §§ 280 ff. BGB.[26] Diese Vorschriften gelten entsprechend für öffentlich-rechtliche Nutzungsverhältnisse.[27] Das dafür erforderliche Schuldverhältnis ist in dem Benutzungsverhältnis zwischen Provider und Nutzer zu sehen. Allerdings müsste der Provider mit dem Einsatz einer Blacklist bei Verbindungsaufbau eine Pflichtverletzung begangen haben, damit er schadensersatzpflichtig ist. Die Hauptpflicht des Vertrages ist sicherlich, dass der Provider dazu verpflichtet ist, dem Nutzer die an ihn adressierten E-Mails zuzustellen. Dieser Pflicht kommt der Provider mit dem Abweisen der E-Mail – sei es nun

[22] So im Ergebnis *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 303a, Rn. 7.

[23] *Wieck-Noodt* in: Münchener Kommentar zum StGB, 1. Auflage 2006, § 303a Rn. 17 m.w.N.

[24] *Heidrich*, CR 2009, 168, 170; *Hoeren*, NJW 2004, 3513, 3515; *Heidrich*, MMR 2005, 181, 182; *Spindler/Ernst*, CR 2004, 437, 440.

[25] *Hoeren*, NJW 2004, 3513, 3515.

[26] *Heidrich*, CR 2009, 168, 171; *Spindler/Ernst*, CR 2004, 437, 444.

[27] *Schulze*/Dörner/Ebert, Kommentar zum BGB, 5. Auflage 2007, § 280, Rn. 3.

eine Spam-E-Mail oder einer „false positive" – nicht nach. Gleichzeitig hat der Provider aber dafür zu sorgen, dass seine Systeme funktionsfähig bleiben und dass der E-Mail-Betrieb ordnungsgemäß vonstattengehen kann. Diese Pflicht ergibt sich zum einen aus dem Nutzungsverhältnis selbst, auf Grund dessen der Provider einen effektiven und leistungsfähigen Dienst zu erbringen hat. Zum anderen gibt es auch im TKG (z.B. in § 109 Abs. 2 für öffentliche Anbieter) die Pflicht, die Systeme gegen Störungen zu schützen. Bei einem eingehenden Spam-Aufkommen von ca. 95 Prozent aller E-Mails wären die Server schnell überlastet und hätten voraussichtlich nach kurzer Zeit keinen Speicherplatz für erwünschte E-Mails (vgl. B. II. a.). Gleichzeitig würde die Zustellung aller eingehenden E-Mails eine Zeitverzögerung des Zugangs der E-Mail im Postfach des Nutzers mit sich bringen. Ausgegangen werden kann, je nach Leistungsfähigkeit der Systeme, von einem Zeitraum von bis zu zwei Tagen. Gerade bei drängenden geschäftlichen bzw. dienstlichen, aber auch bei manchen privaten E-Mails ist eine solche Verzögerung natürlich äußerst unerwünscht. Selbst wenn – bei nicht erfolgendem Blacklisting – die Nutzer die in ihren Postfächern eingehenden E-Mails in kurzen Abständen überprüfen und Spam-Nachrichten löschen, ändert dies nichts am Umfang der beim Empfänger-Server selbst eingehenden Nachrichten. Bereits an dieser Stelle und damit vor Zustellung an den Nutzer käme es zu Überlastungen des Systems und damit zu den genannten Verzögerungen. Wenn den Empfänger-Server also die Pflicht trifft, einen effektiven und zeitnahen E-Mail-Dienst zu erbringen, muss er auch dafür sorgen (dürfen), dass Verzögerungen vermieden werden. Entscheidend für eine Zulässigkeit ist also, welche Pflichten den Empfänger-Server hinsichtlich der Spam-Abwehr treffen. Zur Bestimmung dieser Pflichten kann auf die ergänzende Vertragsauslegung zurückgegriffen werden, wenn eine Regelungslücke im Vertrag besteht, die nicht durch gesetzliche Vorschriften gelöst werden kann.[28] Wenn die Nutzungsordnungen keine Regelung für das Blacklisting bei Verbindungsaufbau enthalten, liegt hierin eine ausfüllungsbedürftige Regelungslücke, es sei denn, auf diese Regelung wurde bewusst verzichtet.[29] Es ist nicht davon auszugehen, dass sich Empfänger und Empfänger-Server in Kenntnis der Sachlage bei Vertragsschluss dazu entschlossen haben, den Fall der für einen effektiven Dienst erforderlichen Spam-Filterung bewusst nicht zu regeln. Die so entstandene Regelungslücke ist daher unbeabsichtigt und ausfüllungsbedürftig. Auch das Gesetz enthält keine speziellen Vorschriften für E-Mail-Dienste, sondern nur allgemeine Grundsätze, die so spezielle Fragen wie eine Spam-Filterung nicht regeln. In diesen Fällen muss der hypothetische Wille der Parteien ermittelt werden. Dabei ist darauf abzustellen, was die Parteien bei einer Interessenabwägung nach Treu und Glauben verein-

[28] Dazu grundsätzlich: *BGH*, 9, 273, 277 f.; *Jauernig*, BGB, 13. Auflage 2009, § 157, Rn. 2; Palandt*/Ellenberger*, Bürgerliches Gesetzbuch, 69. Auflage 2010, § 157, Rn. 2,4; *Busche* in: Münchener Kommentar zum BGB, 5. Auflage 2006, § 157, Rn. 37; *Roth* in: Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Januar 2003, § 157, Rn. 11.

[29] *Jauernig*, BGB, 13. Auflage 2009, § 157, Rn. 2; Palandt*/Ellenberger*, Bürgerliches Gesetzbuch, 69. Auflage 2010, § 157, Rn. 3; *Roth* in: Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Januar 2003, § 157, Rn. 15.

bart hätten, wenn sie den nicht geregelten Fall bedacht hätten.[30] Sowohl der Empfänger-Server als auch der Empfänger der E-Mail werden ein objektives Interesse daran haben, dass Spam-Mails abgewehrt werden. Auf Grund der geringen Fehlerquote ist die Beeinträchtigung des Empfängers durch zumindest mögliche „false positives" als sehr gering einzuschätzen. Dem steht ein starkes Interesse beider Parteien gegenüber, die Belastung der Systeme gering zu halten und damit einen zuverlässigen und schnellen E-Mail-Dienst zu gewährleisten. Auf Grund des überwiegenden Interesses zu Gunsten der Spam-Abwehr ergibt sich nach ergänzender Vertragsauslegung eine Einschränkung der Zustellungspflicht dahingehend, dass nicht alle dem Empfänger-Server angebotenen E-Mails angenommen und weitergeleitet werden müssen, sondern dass zuvor eine geeignete und zuverlässige Filtermethode anzuwenden ist. Mit der Nutzung eines Blacklisting-Dienstes verstößt der Empfänger-Provider daher nicht gegen eine Vertragspflicht und macht sich dementsprechend nicht schadensersatzpflichtig. Einer Einwilligung des Nutzers bedarf es nach Ansicht der Forschungsstelle Recht deshalb nicht.[31]

Allerdings ist darauf hinzuweisen, dass sich der Empfänger-Server an einen zuverlässigen Listenbetreiber wenden muss, der die Gefahr von „false positives" möglichst weitgehend ausschließt bzw. fehlerhafte Einträge in seiner Liste zeitnah zurücknehmen kann. Anderenfalls könnte sich der Provider wiederum einer Pflichtverletzung schuldig machen, wenn er unzuverlässige Listen verwendet. Um dies zu verhindern, ist der Provider ggf. dazu gezwungen, den Anbieter der Blacklist zu wechseln, falls sich dieser als unzuverlässig herausstellt.[32]

Auch wenn nach Ansicht der Forschungsstelle Recht eine Einwilligung des Nutzers in die Gesamtmaßnahme nicht erforderlich ist, können die E-Mail-Provider im Rahmen der nächsten Änderung der Benutzungsordnung eine Klausel bezüglich der Spamfilterung aufnehmen, um Unklarheiten für die Zukunft zu vermeiden. Dabei sollte der Nutzer auch darüber informiert werden, dass eine absolut zuverlässige Bewertung technisch nicht möglich ist und eine E-Mail fälschlicherweise als Spam deklariert werden kann.

---

[30] Palandt*/Ellenberger,* Bürgerliches Gesetzbuch, 69. Auflage 2010, § 157, Rn. 7; *Busche* in: Münchener Kommentar zum BGB, 5. Auflage 2006, § 157, Rn. 46; *Roth* in: Staudingers Kommentar zum Bürgerlichen Gesetzbuch, Januar 2003, § 157, Rn. 30.

[31] *Spindler/Ernst*, CR 2004, 437, 440 ff. lehnten im Jahr 2004 noch eine Filterpflicht ab, merken aber an, dass dies in Zukunft anders zu sehen sein könnte, wenn das Angebot von Spam-Filtern Bestandteil der verkehrsüblichen Schutzpflicht des Providers ist.

[32] *Heidrich*, CR 2009, 168, 170 f.; *Spindler/Ernst*, CR 2004, 437, 444 f.

f. Mitbestimmungsrecht des Personalrats

Ob bei der Einführung von Blacklisting der Betriebs- bzw. Personalrat mitbestimmungsberechtigt ist, richtet sich sowohl nach den Landespersonalvertretungsgesetzen als auch dem Betriebsverfassungsgesetz (BetrVG). Welches Gesetz zu beachten ist, hängt von der Rechtsform des Arbeitgebers ab. Handelt es sich um eine Dienststelle der öffentlichen Verwaltung, gelten die jeweiligen Landespersonalvertretungsgesetze; für alle nichtöffentlichen Stellen, die privatrechtlich ausgestaltet sind, gilt das BetrVG.[33] Beispielsweise ist in § 72 Abs. 3 Nr. 1 des Landesvertretungsgesetzes Nordrhein-Westfalen (LPVG NRW) ausdrücklich festgelegt, dass die Einführung und Anwendung technischer Einrichtungen, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten bestimmt sind, der Mitbestimmung des Personalrats unterliegen. Identisch mit dem Wortlaut dieser Regelung ist § 87 Abs. 1 Nr. 6 BetrVG, der ein solches Mitbestimmungsrecht für den Betriebsrat vorsieht. Sinn und Zweck des Blacklistings ist allerdings nicht die Überwachung der Mitarbeiter. Vielmehr dient das Blacklisting der Abwehr von Spam-Nachrichten, um die Stabilität des Empfänger-Servers und die Effektivität des E-Mail-Dienstes zu gewährleisten. In § 72 Abs. 3 Nr. 1 LPVG NRW a.F. hieß es noch, dass die Maßnahme zur Überwachung „geeignet“ sein muss. Dem Wortlaut zu Folge kam es demnach nicht auf die Absicht des Empfänger-Servers an, sondern nur auf die theoretische Möglichkeit der Überwachung. In der heutigen Fassung wurde das Wort „geeignet“ durch „bestimmt“ ersetzt, was zunächst dafür spricht, dass die subjektive Absicht des Dienststellenleiters und nicht mehr bloß die generelle Eignung zur Überwachung maßgeblich sein soll. Aufschluss für die begriffliche Änderung kann die Entstehungsgeschichte bieten. Das LPVG NRW sollte grundlegend novelliert werden und an das bewährte und in seinen Grundstrukturen unverändert gebliebene Bundespersonalvertretungsgesetz angepasst werden. Insofern wurde die Formulierung des § 75 Abs. 3 Nr. 17 BPersVG einfach wörtlich in § 72 Abs. 3 Nr. 1 LPVG NRW übernommen.[34] In der Rechtsprechung herrscht zu § 75 Abs. 3 Nr. 17 BPersVG jedoch weitgehend Einigkeit, dass der Begriff „bestimmt“ objektiv-final betrachtet werden muss.[35] Mitbestimmungspflichtig ist also auch die Einführung solcher technischen Einrichtungen, die lediglich objektiv geeignet sind, den Beschäftigten zu überwachen, ohne dass der Dienststellenleiter bei der Einführung und Anwendung subjektiv die Absicht haben muss, die technische Einrichtung zu diesem Zweck einzusetzen.[36] Maßgeblich ist der Schutzzweck der Norm.[37] Das Mitbestimmungsrecht des Personalrats soll sicherstellen, dass die Beeinträchtigungen und Gefahren

[33] *Koch* in: Erfurter Kommentar zum ArbR, 10. Auflage 2010, § 1 BetrVG, Rn. 6; *Ricardi*, Betriebsverfassungsgesetz, 12. Auflage 2009, § 1 BetrVG, Rn. 1.

[34] http://www.im.nrw.de/inn/doks/lpvg_begruendung.pdf (zuletzt abgerufen am 3.5.2010).

[35] *BVerwG*, B. v. 26.9.2006, Az. 6 PB 10/06 (zur Auslegung des Mitbestimmungstatbestands); *LAG Baden-Württemberg*, B. v. 308.2006, Az. 12 TaBV 7/04; *Hamburgisches OVG*, B. v. 28.2.2000, Az. 8 Bf 338/99 PVL.

[36] *BVerwG*, B. v. 26.9.2006, Az. 6 PB 10/06; *Hamburgisches OVG*, B. v. 28.2.2000, Az. 8 Bf 338/99 PVL.

[37] *BVerwG*, B. v. 26.9.2006, Az. 6 PB 10/06.

für den Schutz der Persönlichkeit des Beschäftigten am Arbeitsplatz, die von der Technisierung der Verhaltens- und Leistungskontrolle ausgehen, auf das erforderliche Maß beschränkt bleiben. Aufgrund dessen ist die Einbeziehung des Personalrats nur dann entbehrlich, wenn die technische Einrichtung nach ihrer Konstruktion überhaupt nicht zur Überwachung geeignet ist oder es zur Überwachung einer technischen Änderung der Anlage bedarf.[38] Darüber hinaus ist eine Zustimmung des Personalrats nur dann einzuholen, wenn eine Maßnahme neu eingeführt oder eine bestehende Maßnahme wesentlich erweitert wird, für die bereits eine Zustimmung vorliegt.[39] Die Daten, die beim Betrieb eines E-Mail-Dienstes anfallen, können durchaus dazu verwendet werden, die Leistung und das Verhalten der Mitarbeiter zu überwachen, selbst wenn der Dienst nicht zu diesem Zweck bestimmt ist. Technisch ist es möglich, aus den anfallenden Daten die Beteiligten der Kommunikation zur Kenntnis zu nehmen, die Anzahl und die Zeitpunkte der Kontakte zwischen den Beteiligten, und sogar den Inhalt der E-Mail. Insofern war der Personalrat bereits bei Einführung des E-Mail-Dienstes mitbestimmungsberechtigt. Beim Blacklisting bei Verbindungsaufbau ist eine solche Überwachung hingegen nicht möglich. Nur die IP-Adresse des Versender-Servers wird zur Kenntnis genommen. Aus ihr sind keinerlei Informationen ersichtlich, die Aufschluss über die Beteiligten des Kommunikationsvorgangs geben können. Insofern ist der Personalrat bei Einführung dieser Maßnahme nicht mitbestimmungsberechtigt.

g. Informationspflichten

Um im Falle eines „false positives“ einen erneuten Zustellversuch zu ermöglichen, ist es erforderlich, den Versender-Sender in Form einer Unzustellbarkeitsquittung zu informieren. In dieser sollte der Grund der Abweisung angegeben werden. Nur so kann der Versender aktiv werden, wenn er irrtümlich für einen Spam-Versender gehalten wird, und sich wieder von der Blacklist löschen lassen. Ein Nachteil dieser Benachrichtigung ist natürlich, dass die Absender richtigerweise als Spam klassifizierter E-Mails von der Existenz der E-Mail-Adresse erfahren und sich ggf. auf den Spamfilter einstellen. Allerdings wird die Beeinträchtigung für die Beteiligten durch eine Benachrichtigung erheblich verringert, sodass die Bekanntgabe der Existenz der E-Mail-Adresse in Kauf zu nehmen ist und eine Benachrichtigung dementsprechend vorzunehmen ist.[40] Diese Benachrichtigungspflicht ergibt sich zwar nicht unmittelbar aus dem Gesetz. Allerdings würde ohne eine entsprechende Information an den Versender-Server dieser (bzw. der Versender) nicht wissen, dass die E-Mail nicht zugestellt wurde

[38] *BVerwG*, B. v. 26.9.2006, Az. 6 PB 10/06.

[39] *BVerwG*, B. v. 13.8. 1992, Az. 6 P 20/91; *Kaiser* in: Richardi/Dörner/Weber, Personalvertretungsrecht, 3. Auflage 2008, § 75 Rn. 546.

[40] *Spindler/Ernst*, CR 2004, 437, 438.

und dass er tätig werden muss, damit ein erneuter Zustellversuch erfolgreich sein kann. Es könnte daher passieren, dass eine fälschlicherweise abgelehnte seriöse E-Mail verloren geht. Um einen möglichst ausgewogenen Interessenausgleich zu gewährleisten, ist daher eine Unzustellbarkeitsquittung zuzustellen. Die rechtliche Grundlage hierfür bildet letztlich die ergänzende Vertragsauslegung (siehe B. I. 1. e.), bei der die mutmaßlichen Interessen der Parteien miteinander in Einklang gebracht werden müssen. Der Empfänger hat ein Interesse daran, dass „false positives" erneut zugestellt werden können, während eine entsprechende Information des Versender-Servers durch den Empfänger-Server diesen kaum belastet.

Eine Informationspflicht des Empfängers hinsichtlich der einzelnen Abweisung besteht nicht. Es wäre widersinnig, eine hohe Anzahl von Spam-Mails abzublocken, dem Nutzer daraufhin aber genau dieselbe Anzahl von Mails zu schicken mit der Nachricht, dass eine E-Mail geblockt wurde. Der durch die Spam-Abwehr erzielte Effekt der Systementlastung und erhöhten Übersichtlichkeit für den Nutzer wäre damit wieder aufgehoben. Auch für eine Übersichtsmail über die Anzahl der in einem bestimmten Zeitraum als Spam abgelehnten E-Mails besteht kein Bedürfnis. Dem Empfänger könnte ohnehin nur die IP-Adresse des Versender-Servers mitgeteilt werden, die aber über den Versender in aller Regel nichts aussagt. Zudem dürfte auf Grund des enormen Spam-Aufkommens eine solche Zusammenfassung äußerst unübersichtlich und ihr Nutzen für den Empfänger sehr gering sein.[41]

2. Blacklisting nach Kenntnisnahme des Envelopes

Zu diesem Zeitpunkt kennt der Empfänger-Server nicht nur die IP-Adresse des Versender-Servers, er hat vielmehr auch Kenntnis vom Inhalt des Envelopes, also dem alphanumerischen Namen des Versender-Servers, der E-Mail-Adresse des Absenders und der E-Mail-Adresse des Empfängers der E-Mail. Zu beachten ist hierbei, dass nur die E-Mail-Adresse des Empfängers verbindlich ist, die anderen Daten können leicht gefälscht werden und sind daher nicht als zuverlässig anzusehen. Ferner ist wichtig, dass auch beim Blacklisting nach Kenntnisnahme des Envelopes nur die bei Verbindungsaufbau erhobene IP-Adresse des Versender-Servers mit der Blacklist abgeglichen wird, nicht die Daten des Envelopes. Der spätere Zeitpunkt beruht vor allem auf dem Grund, dass neben dem Blacklisting auch ein Whitelisting betrieben werden kann, für das die Daten des Envelopes erforderlich sind.

a. Datenschutz

[41] Anders noch *Spindler/Ernst*, CR 2004, 437, 439, die eine Benachrichtigung aufgrund der vertraglichen Verpflichtung für erforderlich halten.

Die folgenden Ausführungen entsprechen unter Umständen nicht der ab dem 25. Mai 2018 geltenden Rechtslage. Dem hier zur Verfügung gestellten Text liegt die Rechtslage vor Geltung der Verordnung (EU) 2016/679, bekannt unter ihrem Kurztitel EU-Datenschutz-Grundverordnung (DS-GVO), zugrunde. Die Verordnung gilt ab dem 25. Mai 2018 verbindlich in allen Mitgliedsstaaten der Europäischen Union und verdrängt grundsätzlich alle nationalen Regelungen zum Datenschutzrecht.
Für den Regelungsbereich der elektronischen Kommunikation soll die DS-GVO durch die E-Privacy-Verordnung ergänzt und präzisiert werden. Diese befindet sich jedoch noch in der Beratungsphase und wird nicht rechtzeitig zum 25. Mai 2018 in Kraft treten. Es ist nicht auszuschließen, dass die E-Privacy-Verordnung für die hier dargestellten Sachverhalte wiederum neue Regelungen bereithält.
Die Forschungsstelle Recht im DFN beobachtet diese Entwicklungen und passt die datenschutzrechtlichen Ausführungen entsprechend an. Bis dahin bitten wir um Ihre Geduld.

Wie beim Blacklisting bei Verbindungsaufbau wird beim Blacklisting nach Kenntnisnahme des Envelopes lediglich die IP-Adresse des Versender-Servers mit der Blacklist abgeglichen. Die Übermittlung dieser Adresse ist datenschutzrechtlich nicht zu beanstanden, da es sich hierbei nicht um eine Übermittlung personenbezogener Daten handelt (vgl. B. I. 1. a.). Es werden aber auch die E-Mail-Adressen von Absender und Empfänger aus dem Envelope zur Kenntnis genommen, die Aufschluss darüber geben, wer an dem Kommunikationsvorgang beteiligt ist. Diese stellen personenbezogene Daten dar, zumindest wenn die dahinterstehende Person erkennbar oder zu ermitteln ist,[42] sodass die datenschutzrechtliche Zulässigkeit dieser Kenntnisnahme und der weiteren Verwendung zu hinterfragen ist.

Sofern die Hochschule am Arbeitsplatz die private Nutzung des dienstlichen E-Mail-Accounts erlaubt, ist sie in rechtlicher Hinsicht als „Diensteanbieter von Telekommunikationsdiensten“ nach § 3 Nr. 6 TKG anzusehen, da die Hochschule insofern Dienste für Dritte anbietet und daher gem. § 3 Nr. 10 TKG die Dienste geschäftsmäßig erbringt.[43] Der Diensteanbieter muss im Sinne von § 3 Nr. 6 TKG die besonderen datenschutzrechtlichen Vorschriften der §§ 91 ff. TKG beachten. Bei den Daten des Envelopes handelt es sich um dem Fernmeldegeheimnis unterliegende Verkehrsdaten nach § 3 Nr. 30 TKG, also Daten, die sich jeweils auf einen konkreten Telekommunikationsvorgang beziehen.[44] Die datenschutzrechtliche Zulässigkeit des Erhebens und Verwendens bestimmt sich nach § 96 Abs. 1 TKG, wonach die Daten erhoben und verwendet werden dürfen, soweit dies für die Erbringung des Dienstes – also für die Zustellung der E-Mail – erforderlich ist. Die Kenntnisnahme der Daten des Envelopes durch den Empfänger-Server erfüllt diese Voraussetzungen. Sie sind zum Auf-

[42] *Schmitz* in: Hoeren/Sieber, Handbuch Multimedia-Recht, 21. Ergänzungslieferung 2008, Teil 16.4, Rn. 55.
[43] *Fetzer* in: Arndt/Fetzer/Scherer, TKG, § 3, Rn. 42.
[44] *Fetzer* in: Arndt/Fetzer/Scherer, TKG, § 3, Rn. 3.

bau des Telekommunikationsdienstes erforderlich, da der Diensteanbieter ohne die E-Mail-Adressen die jeweilige E-Mail nicht an den Empfänger weiterleiten könnte. Da zudem eine Weiterleitung dieser Daten an Dritte nicht stattfindet, sondern nur die IP-Adresse des Versender-Servers übermittelt wird, werden die E-Mail-Adressen nicht zu einem anderen als dem der Erhebung zu Grunde liegenden Zweck verwendet. Datenschutzrechtliche Probleme ergeben sich folglich nicht. Allerdings ist zu beachten, dass die Daten – soweit sie nicht mehr gebraucht werden – unverzüglich zu löschen sind, § 96 Abs. 1 Satz 3 TKG.[45] Wird die E-Mail aufgrund des Blacklistings blockiert, werden die Daten des Envelopes nicht mehr für die Erbringung des Dienstes benötigt. Insofern ist die Erhebung der Daten zulässig, diese müssen aber gelöscht werden, wenn die E-Mail nicht angenommen wird oder zugestellt worden ist.

Ist die private Nutzung des E-Mail-Accounts hingegen ausgeschlossen, ist der Arbeitgeber kein „Diensteanbieter“ im Sinne des Telekommunikationsgesetzes mehr, sodass die besonderen Vorschriften des Datenschutzes im TKG keine Anwendung finden. Daher muss die Zulässigkeit der Erhebung der Daten des Envelopes anhand allgemeiner Datenschutzvorschriften bestimmt werden.[46] Nach den für Hochschulen einschlägigen Landesdatenschutzgesetzen ist die Erhebung und Speicherung der Daten möglich, sofern dies zur Aufgabenerfüllung erforderlich ist (vgl. z.B. §§ 12, 13 DSG NRW). Zur Erbringung eines E-Mail-Dienstes ist es erforderlich, die E-Mail-Adressen der beteiligten Kommunikationspartner zur Kenntnis zu nehmen. Sofern auch bei Ausschluss der Privatnutzung die Daten des Envelopes gelöscht werden, wenn die E-Mail aufgrund des Blacklistings abgewiesen wird, ist die Kenntnisnahme und vorläufige Speicherung datenschutzrechtlich nicht zu beanstanden.

b. Fernmeldegeheimnis nach dem Telekommunikationsgesetz

Nach § 88 Abs. 1 TKG sind solche Informationen geschützt, die im Rahmen eines Kommunikationsvorganges anfallen, also entweder deren Inhalt oder aber deren nähere Umstände darstellen. Hierzu gehören die Informationen über die Beteiligten der Kommunikation, also auch die E-Mail-Adressen, die im Envelope enthalten sind.[47] Das Fernmeldegeheimnis ist also beim Blacklisting nach Kenntnisnahme des Envelopes zu beachten.

Der Telekommunikationsanbieter darf sich gem. § 88 Abs. 3 TKG die Kenntnis über die Daten des Envelopes nur verschaffen, wenn sie für die geschäftsmäßige Erbringung der Dienste erforderlich ist,

[45] *Büttgen* in: Scheuerle/Mayen, TKG, 2. Auflage 2008, § 96, Rn. 9; *Robert* in: Beck`scher TKG-Kommentar, 3. Auflage 2006, § 96, Rn. 11.

[46] *Heidrich*, CR 2009, 168, 173.

[47] *Bock* in: Beck`scher TKG-Kommentar, 3. Auflage 2006, § 88, Rn. 13.

und er darf die Daten nur verwenden (also etwa speichern oder übermitteln), soweit es für diesen Zweck auch erforderlich ist. Die Kenntnisnahme und zeitweise Speicherung wurde bereits im Rahmen der datenschutzrechtlichen Beurteilung als erforderlich zur Erbringung des Dienstes qualifiziert (vgl. B. I. 2. a.). Verwendet werden die E-Mail-Adressen der Kommunikationsbeteiligten nicht für das Blacklisting, sondern nur für die Zustellung der E-Mail und damit für die Erbringung des Dienstes, soweit die E-Mail nicht aufgrund des Blacklistings blockiert wird. Denn für das Blacklisting nach Kenntnisnahme des Envelopes wird nur die IP-Adresse des Versender-Servers benötigt, welche dem Fernmeldegeheimnis nicht unterfällt (vgl. B. I. 1. b.). Insofern verstößt das Blacklisting nach Kenntnisnahme des Envelopes nicht gegen die Vorgaben des Fernmeldegeheimnisses nach dem TKG.

c. Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB (Verletzung des Post- oder Fernmeldegeheimnisses)

Voraussetzung für eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB ist, dass die E-Mail, die nach Kenntnisnahme des Envelopes geblockt und damit unterdrückt wird, zuvor dem Empfänger-Server „zur Übermittlung anvertraut“ worden ist. Dem Empfänger-Server sind sowohl die IP-Adresse des Versender-Servers, als auch die Inhalte des Envelopes bekannt. Dennoch ist die E-Mail zu diesem Zeitpunkt dem Empfänger-Server entsprechend der unter B.I.1.c. vorgenommenen Argumentation noch nicht „zur Übermittlung anvertraut“. Ein Anvertrauen liegt erst vor, wenn die Sendung im Machtbereich des Empfänger-Servers angekommen ist. Bisher ist aber nur der Envelope angenommen worden. Er gehört weder zum Header noch zum Body, welcher der eigentliche Nachrichteninhalt ist, sondern enthält nur Adressinformationen. Die beiden beteiligten Server befinden sich noch in der „Begrüßungsphase“, die Phase der eigentlichen Übermittlung hat hingegen noch nicht begonnen. Diese Stufen sind auch nach dem SMTP (also dem gängigen E-Mail-Protokoll) getrennt. Solange Header und Body noch nicht übertragen wurden, sprechen daher überzeugende Gründe dafür, dass ein Anvertrauen noch nicht vorliegt.[48] Allerdings wird auch vertreten, dass § 206 StGB das Fernmeldegeheimnis umfassend schützt und damit neben dem Inhalt bereits die Umstände der Kommunikation erfasst.[49] Die E-Mail ist mit dem Absenden aus dem eigenen Kontrollbereich entlassen und befindet sich bis zur vollständigen Ankunft beim Empfänger im besonders anfälligen und damit schutzbedürftigen Übertragungsvorgang. Daher ließe sich sagen, dass ein Unterdrücken im Übertragungsvorgang einen Gesetzesverstoß darstellt und bereits das Annehmen und Unterdrücken von Kommunikationsumständen ausreicht, um ein Anvertrauen zu bejahen.[50] Dagegen spricht aber, dass § 206 Abs. 2 StGB – anders als Abs. 1 – gerade auf die Sendung als solche abstellt, nicht auf einzelne Um-

[48] *Heidrich*, MMR 2005, 181, 181 f.

[49] *Lenckner* in: Schönke/Schröder, StGB, § 206, Rn. 6.

[50] Vgl. *Heidrich/Tschoepe*, MMR 2004, 75, 77.

stände. Das Anvertrauen im Sinne von Abs. 2 Nr. 2 bezieht sich daher auf die gesamte Sendung.[51] Erst wenn sie vollständig angenommen wird, geht die Verantwortlichkeit für die Sendung und den weiteren Kommunikationsvorgang auf den Empfänger-Server über. Daher muss die Sendung auch gerade dem unterdrückenden Unternehmen (Empfänger-Server) anvertraut worden sein, nicht ausreichend ist das Absenden und damit das Anvertrauen an irgendein an der Kommunikation beteiligtes Unternehmen, also etwa den Versender-Server. Aus diesem Grund ist die Forschungsstelle Recht der Ansicht, dass bei der Frage, ob die E-Mail dem Empfänger-Server anvertraut wurde, nicht auf die Übermittlung des Envelopes, sondern vielmehr auf die Übermittlung der Nachricht (Header und Body) abzustellen ist. Folglich liegt beim Blacklisting nach Kenntnisnahme des Envelopes kein Anvertrauen im Sinne des § 206 Abs. 2 Nr. 2 StGB vor. Diese Fallkonstellation wurde allerdings noch nicht von der Rechtsprechung behandelt.

d. Strafbarkeit nach § 303a StGB (Datenveränderung)

Im Rahmen des § 303a StGB ist entscheidend, ob die Daten, die abgewiesen werden, dem Zugriff des Verfügungsbefugten entzogen oder vorenthalten werden. (vgl. B. I. 1. d.) Im Wesentlichen kann dabei auf das zum Blacklisting bei Verbindungsaufbau Gesagte (vgl. B. I. 1. d.) zurückgegriffen werden. Der Empfänger erlangt nach Ansicht der Forschungsstelle Recht die Verfügungsbefugnis erst, wenn die gesamte Nachricht vom Empfänger-Server angenommen worden ist. Wenn nur der Envelope angenommen und die restliche, eigentliche Nachricht (Header und Body) abgewiesen wird, hat der Empfänger noch keine Verfügungsbefugnis erlangt. Diese verbleibt beim Versender oder beim Versender-Server und wird durch das Blacklisting nach Kenntnisnahme des Envelopes nicht entzogen oder anderweitig beeinträchtigt, zumal eine Unzustellbarkeitsmitteilung den Versender-Server darüber informiert, dass die Verfügungsbefugnis bei ihm verbleibt. Auch für diese Form des Blacklistings gibt es weder Rechtsprechung noch einheitliche Literatur, allerdings kann mit guten Argumenten von einer Rechtmäßigkeit dieser Maßnahme ausgegangen werden, die mit einer Einwilligung des Empfängers weiter abgesichert werden kann.

[51] So wohl auch *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 206, Rn. 15, der – allerdings für das Tatbestandsmerkmal „Unterdrücken“ – das Zurückhalten der „(Gesamt-)Sendung (Datei)“ oder eines wesentlichen Teils verlangt.

e. Zulässigkeit nach dem Nutzungsverhältnis

Beim Blacklisting nach Kenntnisnahme des Envelopes ergeben sich keine Unterschiede zum Blacklisting bei Verbindungsaufbau bezüglich der Pflichten aus dem Nutzungsverhältnis (vgl. B. I. 1. e.).

f. Mitbestimmungsrecht des Personalrats

Der Betriebs- bzw. Personalrat war bei Einführung des E-Mail-Dienstes als solchem mitbestimmungsberechtigt (vgl. B. I. 1. f.). Im Gegensatz zum Blacklisting bei Verbindungsaufbau kann der Empfänger-Server nun aber aus den Daten des Envelopes erkennen, wer an der Kommunikation beteiligt war. Insofern wäre eine Überwachung der Mitarbeiter aufgrund dieser Daten möglich. Dennoch ist der Personalrat beim Blacklisting nach Kenntnisnahme des Envelopes nicht mitbestimmungsberechtigt. Zum einen werden nur die Daten zur Kenntnis genommen, die der Empfänger-Server ohnehin zur Erbringung des Dienstes benötigt. Es fallen also keine weiteren Daten an. Zum anderen besteht eine Mitbestimmungsberechtigung nur, wenn die bestehende technische Maßnahme wesentlich erweitert wird (vgl. B. I. 1. f.). Durch den Abgleich der IP-Adresse des Versender-Servers wird dieses Datum nicht nur für die reine E-Mail-Zustellung verwendet, sondern noch für einen weiteren Zweck (Spam-Abwehr). Dies stellt zwar eine Erweiterung dar, welche aber nicht als wesentlich anzusehen ist. Die IP-Adresse ermöglicht keinen Rückschluss auf die Beteiligten und die Möglichkeit der Überwachung auf Grund der Daten des Envelopes besteht ohnehin schon durch den E-Mail-Dienst an sich. Das Gefährdungspotential wird somit nicht wegen der Verwendung einer Blacklist gesteigert. Der Personalrat ist also nicht erneut mitbestimmungsberechtigt.

g. Informationspflichten

Wie beim Blacklisting bei Verbindungsaufbau ist es erforderlich, den Versender-Server in Form einer Unzustellbarkeitsquittung über die Abweisung und deren Grund zu informieren. Eine Informationspflicht des Empfängers hinsichtlich der einzelnen Abweisung besteht nicht (vgl. B. I. 1. g.).

II. Rechtliche Zulässigkeit von Greylisting

a. Datenschutz

Die folgenden Ausführungen entsprechen unter Umständen nicht der ab dem 25. Mai 2018 geltenden Rechtslage. Dem hier zur Verfügung gestellten Text liegt die Rechtslage vor Geltung der Verordnung

(EU) 2016/679, bekannt unter ihrem Kurztitel EU-Datenschutz-Grundverordnung (DS-GVO), zugrunde. Die Verordnung gilt ab dem 25. Mai 2018 verbindlich in allen Mitgliedsstaaten der Europäischen Union und verdrängt grundsätzlich alle nationalen Regelungen zum Datenschutzrecht.
Für den Regelungsbereich der elektronischen Kommunikation soll die DS-GVO durch die E-Privacy-Verordnung ergänzt und präzisiert werden. Diese befindet sich jedoch noch in der Beratungsphase und wird nicht rechtzeitig zum 25. Mai 2018 in Kraft treten. Es ist nicht auszuschließen, dass die E-Privacy-Verordnung für die hier dargestellten Sachverhalte wiederum neue Regelungen bereithält.
Die Forschungsstelle Recht im DFN beobachtet diese Entwicklungen und passt die datenschutzrechtlichen Ausführungen entsprechend an. Bis dahin bitten wir um Ihre Geduld.

Beim Greylisting werden wie beim Blacklisting nach Kenntnisnahme des Envelopes zusätzlich zu der IP-Adresse des Versender-Servers auch die E-Mail-Adressen von Absender und Empfänger (Envelope) zur Kenntnis genommen. Wenn die Hochschule die private Nutzung des dienstlichen E-Mail-Accounts erlaubt, ist sie Diensteanbieter nach dem Telekommunikationsgesetz und muss sich an die datenschutzrechtlichen Vorschriften der §§ 91 ff. TKG halten. Die Daten des Envelopes sind Verkehrsdaten nach § 3 Nr. 30 TKG, sodass ihre Erhebung und Verwendung zum Zwecke der Übermittlung und Zustellung der E-Mail nach § 96 Abs. 1 TKG zulässig ist (vgl. B. I. 2. a.).

Anders als beim Blacklisting werden die Daten des Envelopes für die Spamabwehr eingesetzt, indem sie vorübergehend gespeichert und mit den Envelopes später eingehender E-Mails abgeglichen werden. Diese Verwendung der Daten dient nicht unmittelbar der Erbringung des E-Mail-Dienstes, sondern einem anderen Zweck (Spam-Abwehr). Dementsprechend ist sie von der Erlaubnis des § 96 Abs. 1 TKG nicht mehr umfasst. Einschlägig ist in diesem Fall vielmehr § 100 TKG.[52] Zweck des § 100 Abs. 1 TKG ist das Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen. Eine Störung liegt dann vor, wenn durch ein unbeabsichtigtes Ereignis der bestimmungsgemäße Gebrauch der TK-Anlage beeinträchtigt oder unmöglich gemacht wird.[53] Durch das massenhafte Aufkommen von unerwünschten E-Mails kann die Funktionsfähigkeit des Mailservers erheblich beeinträchtigt werden. Nach einem Statusbericht zur Bekämpfung von Spam in Europa geht die europäische Agentur für Internetsicherheit davon aus, dass weniger als 5 Prozent aller E-Mails erwünscht sind. Ca. 95 Prozent sind demnach Spam-Nachrichten, die im Wege von Filtermethoden aussortiert werden müssen, damit es nicht zu einer Überlastung der E-Mail-Systeme

[52] Andere Ansicht: *Heidrich*, CR 2009, 168, 172, der im Rahmen von § 100 TKG nur die Nutzung der Kundendaten des TK-Anbieters für rechtmäßig ansieht. Bei dieser Auslegung wird jedoch übersehen, dass § 100 TKG sowohl Daten von Teilnehmern als auch von Nutzern umfasst und somit auch Daten Dritter in den Anwendungsbereich des § 100 TKG fallen.

[53] *Fetzer* in: Arndt/Fetzer/Scherer, TKG, § 3, Rn. 5.

kommt.[54] Ohne Filterung vor Annahme der E-Mails würden die Systeme des Empfänger-Servers überlastet. Dies hätte zur Folge, dass E-Mails erheblich verzögert zugestellt oder sogar endgültig abgelehnt werden müssten. Zwar kann der Empfänger-Server seine Kapazitäten entsprechend anpassen. Bei dem ständigen Anstieg des Spam-Aufkommens würde jedoch schnell die Grenze der Unverhältnismäßigkeit überschritten, wobei sich diese Grenze nicht eindeutig bestimmen lässt. Jedenfalls sind im Rahmen der Verhältnismäßigkeit unter Umständen auch die Berufs- und Eigentumsfreiheit des Empfänger-Servers zu beachten, welche betroffen sein können, wenn er seine Kapazitäten ständig erweitern muss, um das immer weiter steigende Spam-Aufkommen bewältigen zu können.[55] Damit liegt zumindest eine erhebliche Beeinträchtigung der für den E-Mail-Dienst erforderlichen TK-Anlage vor, eine Störung ist also gegeben.

Das Greylisting ist geeignet, das Spam-Aufkommen zu verringern und diese Störungsquelle zu beseitigen. Allerdings muss die Speicherung und Verwendung der Daten zur Erreichung dieses Zwecks auch erforderlich sein. Eine Maßnahme ist erforderlich, wenn kein milderes Mittel gleicher Eignung zur Verfügung steht, wenn also kein anderes Mittel verfügbar ist, das in gleicher (oder sogar besserer) Weise geeignet ist, den Zweck zu erreichen, dabei aber den Betroffenen weniger belastet.[56] Wird aus Server-IP, Mailadresse des Absenders sowie Mailadresse des Empfängers ein Hashwert gebildet, ist es nicht mehr ohne Weiteres möglich, Versender und Adressat der E-Mail zu identifizieren. Die Beeinträchtigung der Betroffenen wird auf diese Art so gering wie möglich gehalten. Zugleich bleibt das Greylisting ebenso effektiv wie bei der unveränderten Verwendung des Envelopes, und die Umwandlung in Hashwerte stellt regelmäßig auch keinen unverhältnismäßigen technischen oder finanziellen Aufwand für den Empfänger-Server dar. Die Verwendung von Hashwerten ist daher ein zumutbares milderes Mittel als die Speicherung der unverschlüsselten Daten. Sofern dies beachtet wird, ist das Greylisting nach Ansicht der Forschungsstelle Recht nach § 100 Abs. 1 TKG datenschutzrechtlich zulässig.

Ist die private Nutzung des E-Mail-Accounts ausgeschlossen, ist nicht mehr der Datenschutz nach dem TKG anzuwenden, sondern die allgemeinen Datenschutzvorschriften, insbesondere die Landesdatenschutzgesetze für die Hochschulen (vgl. B. I. 2. a.). Durch Greylisting kann das Spam-Aufkommen wesentlich vermindert werden, wodurch eine Stabilität des Mailservers herbeigeführt wird. Im Rahmen der allgemeinen Datenschutzgesetze ist eine Abwägung zwischen den Interessen

---

[54] http://www.enisa.europa.eu/media/press-releases/prs-in-german/spam21012010de (zuletzt abgerufen am 03.05.2010).

[55] Andere Ansicht: *Heidrich*, CR 2009, 168, 172, der im Rahmen einer vergleichbaren Argumentation bzgl. § 109 Abs. 2 TKG im normalen Spamaufkommen keine unzumutbare Belastung der Systeme versteht.

[56] Allgemein zur Verhältnismäßigkeit bzw. Erforderlichkeit *Di Fabio* in: Maunz/Dürig, Grundgesetz, 56. Ergänzungslieferung 2009, Art. 2, Rn. 45.

des Empfänger-Servers und denen des Empfängers vorzunehmen. Auf Grund der hohen Zuverlässigkeit und geringen Fehlerquote des Greylistings fällt diese Abwägung im Regelfall zu Gunsten des Empfänger-Servers aus, der so seine Systeme schützt und gleichzeitig – auch im Interesse des Empfängers – die Effektivität des E-Mail-Dienstes gewährleistet.[57] Außerdem sind die Eingriffsvoraussetzungen insgesamt geringer als bei Anwendbarkeit des TKG. Wenn also bereits nach dem TKG das Greylisting zulässig ist, dann gilt dies erst recht bei Ausschluss der Privatnutzung und Anwendbarkeit der Landesdatenschutzgesetze. Zu beachten ist auch hier, dass die Verwendung von Hashwerten ein milderes Mittel gegenüber der Verwendung der E-Mail-Adressen in ihrer ursprünglichen Form darstellt und daher vorzunehmen ist, solange dies keinen unverhältnismäßigen Aufwand erfordert.

b. Fernmeldegeheimnis nach dem Telekommunikationsgesetz

Als Diensteanbieter sind die Hochschulen auch an das Fernmeldegeheimnis gebunden, § 88 TKG (vgl. B. I. 1. b.). Die Speicherung und der Abgleich der E-Mail-Adressen fallen unter dessen Schutzbereich, da mit den Adressen der Beteiligten Umstände über die Kommunikation bekannt werden. Gem. § 88 Abs. 3 S. 2 TKG dürfen Kenntnisse über diese Umstände nur für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes der technischen Systeme verwendet werden. Für die Erbringung des Dienstes selbst sind die Speicherung und Verwendung der Daten des Envelopes zum Zwecke der Spam-Abwehr zunächst nicht erforderlich, denn an sich können und müssen die Daten nach Weiterleitung oder Ablehnen der E-Mail gelöscht werden. Allerdings führt das erhebliche Spam-Aufkommen zu starken Beeinträchtigungen des E-Mail-Dienstes, wenn keine Filtermaßnahmen ergriffen werden (vgl. B. I. 1. e.). Eine effektive Erbringung des Dienstes wäre nicht möglich, da es zu deutlichen Verzögerungen in der Mail-Zustellung käme, wohingegen gerade bei E-Mails erwartet wird, dass eine zeitnahe Zustellung als wesentlicher Bestandteil des Dienstes erfolgt. Dementsprechend ist eine angemessene und möglichst wenig beeinträchtigende Spam-Abwehr für die Erbringung des Dienstes erforderlich.

Zudem erlaubt § 88 Abs. 3 S. 1 und 2 TKG eine Verwendung der Daten zum Schutz der technischen Systeme. Dazu gehört auch die Verwendung zur Sicherstellung eines geregelten Kommunikationsablaufs.[58] Ohne Filterung kann es dazu kommen, dass die Systeme überlastet werden und teilweise oder vollständig ausfallen. Natürlich kann die Kapazität der Systeme erweitert werden. Angesichts der Spam-Zunahme dürfte diese Aufrüstung allerdings einen unverhältnismäßigen Aufwand erfor-

[57] Andere Ansicht: *Heidrich*, CR 2009, 168, 173, der die Interessen des Versenders als überwiegend ansieht.

[58] *Bock* in: Beck'scher TKG-Kommentar, 3. Auflage 2006, § 88, Rn. 29; danach seien auch Viren- und Spamfilter unter bestimmten Umständen ausdrücklich zulässig.

dern, der von den Anbietern nicht verlangt werden kann (vgl. B. II. a.). Da das Fernmeldegeheimnis der Nutzer (gerade bei einer Verwendung von Hashwerten, vgl. B. II. a.) nur sehr am Rande betroffen ist, sprechen gute Argumente dafür, dass auch unter dem Gesichtspunkt des Schutzes der technischen Systeme das Greylisting verhältnismäßig und nach § 88 Abs. 3 TKG gerechtfertigt ist. Das Fernmeldegeheimnis wird durch diese Maßnahme folglich nicht verletzt.

c. Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB (Verletzung des Post- oder Fernmeldegeheimnisses)

Wie beim Blacklisting nach Kenntnisnahme des Envelopes ist Voraussetzung für eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB, dass im zumindest vorübergehenden Blockieren der E-Mail im Rahmen des Greylistings ein Unterdrücken liegt. Wenn eine E-Mail dauerhaft abgewiesen wird, liegt jedenfalls ein Unterdrücken der E-Mail vor (vgl. B. I. 1. c.). Beim Greylisting kann es aber sein, dass die E-Mail nur vorübergehend nicht angenommen und zu einem späteren Zeitpunkt dem Empfänger zugestellt wird, sodass sich hierbei die Frage stellt, ob eine reine Verzögerung ebenfalls ein Unterdrücken darstellt. Denn teilweise wird eine relevante Verzögerung verneint, wenn sie nur wenige Minuten beträgt.[59] Beim Greylisting kann – je nach Einstellung des Versender-Servers – die Verzögerung aber auch mehrere Stunden bis Tage dauern. Außerdem ist die Verzögerung in jedem Fall absichtlich durch den Empfänger-Server herbeigeführt und nicht rein technisch bedingt. Ein Unterdrücken liegt also stets vor.

In jedem Fall muss die Nachricht für eine Strafbarkeit zusätzlich dem Empfänger-Server „zur Übermittlung anvertraut“ worden sein. Da nach obiger Argumentation (B. I. 2. c.) aber noch kein „Anvertrauen“ vorliegt, solange noch nicht Header und Body der E-Mail übermittelt sind, entfällt die Strafbarkeit nach § 206 Abs. 2 Nr. 2 StGB.

d. Strafbarkeit nach § 303a StGB (Datenveränderung)

Im Rahmen des § 303a StGB gilt das Gleiche wie beim Blacklisting nach Kenntnisnahme des Envelopes (vgl. B. I. 2. d.).

[59] Bei „längerem Zurückhalten“ eine Unterdrückung bejahend *Fischer*, Strafgesetzbuch, 55. Aufl. 2008, § 206, Rn. 15, m.w.N.; ebenso für „vorübergehendes Entziehen“ *Lenckner* in: Schönke/Schröder, Strafgesetzbuch, 27. Auflage, Rn. 17.

e. Zulässigkeit nach dem Nutzungsverhältnis

Beim Greylisting ergeben sich keine Unterschiede zum Blacklisting bezüglich der Pflichten aus dem Nutzungsverhältnis (vgl. B. I. 1. e.).

f. Mitbestimmungsrecht des Personalrats

Beim Greylisting speichert der empfangende Mailserver den Envelope, sofern die eingehende E-Mail eine unbekannte Kombination aus Versender-Server und E-Mail-Adressen enthält. Anders als beim Blacklisting nach Kenntnisnahme des Envelopes werden diese Daten insgesamt neben der E-Mail-Zustellung auch für das Greylisting verwendet. Diese Daten werden für einen gewissen Zeitraum gespeichert. Die Aussagekraft der so gespeicherten Daten ist jedoch dieselbe wie die der ohnehin erfassten Informationen aus dem E-Mail-Dienst. Insofern besteht, wie beim Blacklisting nach Kenntnisnahme des Envelopes, keine erhöhte Gefahr der Überwachung und damit keine wesentliche Erweiterung der Maßnahme (vgl. B. I. 2. f.). Der Personalrat ist also nicht mitbestimmungsberechtigt.

g. Informationspflichten

Der Empfänger-Server muss dem Versender-Server eine Fehlermeldung übermitteln, aufgrund derer der Versender-Server einen erneuten Zustellversuch unternimmt. Dies ist ohnehin technische Grundvoraussetzung für das Greylisting und daher zwingend notwendig, auf eine rechtliche Pflicht kommt es daher nicht an (für sie würde allerdings das Gleiche gelten wie für die Informationspflicht im Rahmen des Blacklisting, siehe B. I. 1. g.).

Den Empfänger über jede abgewiesene E-Mail zu informieren widerspräche der Idee des Greylistings, da hierbei generell jede E-Mail, egal ob Spam oder Nicht-Spam, zunächst abgewiesen wird.

C. ERGEBNIS

Blacklisting nach Verbindungsaufbau

Eine technisch mögliche Variante des Blacklistings ist das Blacklisting nach Verbindungsaufbau. Bei dieser Variante wird vom Empfänger-Server nur die IP-Adresse des Versender-Servers angenommen und mit einer Blacklist abgeglichen.

Die IP-Adresse des Versender-Servers stellt kein personenbezogenes Datum dar, Datenschutzvorschriften finden aus diesem Grund keine Anwendung.

Mit der Erhebung der IP-Adresse und ihrer weiteren Verwendung zum Abgleich mit einer Blacklist wird auch nicht in das Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz (TKG) eingegriffen, denn es wird weder über den Inhalt noch über die näheren Umstände der Kommunikation Aufschluss gegeben.

Es sprechen gute Argumente dafür, dass das Blacklisting nach Verbindungsaufbau nicht strafbewehrt ist. Im Rahmen des § 206 Abs. 2 Nr. 2 StGB, Unterdrückung einer anvertrauten Sendung, lässt sich argumentieren, dass beim Verbindungsaufbau zwischen Versender- und Empfänger-Server noch kein Teil der Sendung (E-Mail), also weder Envelope noch Header und Body, übertragen wurde und damit die E-Mail noch nicht anvertraut ist. Dies ergibt sich aus dem technischen Protokoll zur E-Mail-Übertragung (SMTP). Einer nach § 303a StGB strafbaren Datenunterdrückung kann entgegengehalten werden, dass die E-Mail dem Verfügungsbefugten zu keinem Zeitpunkt entzogen wird. Mangels Übertragung der E-Mail liegt die Verfügungsberechtigung noch nicht beim Betreiber des Empfänger-Servers bzw. beim Empfänger, sondern unverändert beim Betreiber des Versender-Servers bzw. beim Versender. Unabhängig von einer genaueren Zuordnung gilt, dass in die Verfügungsbefugnis nicht eingegriffen wird, denn die E-Mail liegt weiterhin bei dem Versender-Server, sodass sich insofern die Situation nach dem Abweisen nicht von derjenigen vor der Abweisung unterscheidet. Der Betreiber des Versender-Servers kann vielmehr nach wie vor über die E-Mail verfügen. Diese Bewertung durch die Forschungsstelle Recht ist derzeit gerichtlich weder abgelehnt noch bestätigt.

Auch aus dem Nutzungsverhältnis wird sich häufig keine Pflicht des Betreibers des Empfänger-Servers ergeben, sämtliche E-Mails, also auch Spam und mit Schadsoftware behaftete, anzunehmen und dem Empfänger zuzustellen. Filtermaßnahmen sind unabdingbar für die technisch ordnungsgemäße Erbringung eines E-Mail-Dienstes, denn nur so können die technischen Systeme vor Überlastung und Versagen durch das massenhafte Aufkommen von Spam-Mails geschützt werden. Weist die Vereinbarung über das Nutzungsverhältnis eine entsprechende Regelungslücke auf, ist nach Auffassung der Forschungsstelle Recht im Rahmen einer ergänzenden Auslegung von einer Zulässigkeit der

Ausfilterung auszugehen. Auch diese Auffassung ist derzeit gerichtlich weder abgelehnt noch bestätigt.

Blacklisting nach Verbindungsaufbau unterfällt nicht der Mitbestimmung des Personal- bzw. Betriebsrates, da bei dieser Maßnahme keine personenbezogenen Daten verarbeitet werden und sie somit nicht zur Überwachung der Nutzer geeignet ist.

Der Empfänger muss über die Ablehnung einer E-Mail nicht informiert werden. Dem Versender-Server hingegen ist eine Unzustellbarkeitsquittung zuzustellen, aus der der Grund der Ablehnung hervorgeht.

Blacklisting nach Kenntnisnahme des Envelopes

Eine weitere Variante des Blacklistings ist das Blacklisting nach Kenntnisnahme des Envelopes. Auch hier erfolgt ein Abgleich der IP-Adresse des Versender-Servers mit der Blacklist. Die Maßnahme greift aber später im Protokollablauf, sodass es zusätzlich zur Übertragung des Envelopes mit E-Mail-Adressen von Sender und Empfänger und damit zur Kenntnisnahme und kurzzeitigen Speicherung personenbezogener Daten kommt.

Da die Daten des Envelopes für die Zustellung der E-Mail benötigt und auch nur für diese Zwecke zur Kenntnis genommen werden, ist die Speicherung datenschutzrechtlich nach § 96 Abs. 1 TKG zulässig.

Blacklisting nach Kenntnisnahme des Envelopes verstößt nicht gegen das Fernmeldegeheimnis. Zwar liefern die Daten des Envelopes Kenntnis über die näheren Umstände der Kommunikation, dies ist aber nach § 88 Abs. 3 Satz 1 TKG zulässig, da die Kenntnis der Daten für die geschäftsmäßige Erbringung des E-Mail-Dienstes erforderlich ist.

Auch beim Blacklisting nach Kenntnisnahme des Envelopes sprechen gute Argumente gegen eine strafrechtliche Relevanz. Zwar wird bei dieser Maßnahme mit der Übertragung des Envelopes ein erster Schritt zur Übermittlung der E-Mail gemacht. Da § 206 Abs. 2 StGB aber auf die Sendung als solche abzielt ist, sprechen gute Gründe dafür, dass für ein Anvertrautsein der E-Mail die Übertragung von Header und Body vorauszusetzen ist. Hinsichtlich der nach § 303a StGB strafbaren Datenunterdrückung kann auf die Ausführungen zum Blacklisting nach Verbindungsaufbau verwiesen werden.

In Bezug auf die Pflichten des Betreibers des Empfänger-Servers aus dem Nutzungsverhältnis gilt das zum Blacklisting nach Verbindungsaufbau Gesagte.

Auch beim Blacklisting nach Kenntnisnahme des Envelopes ist der Personal- bzw. Betriebsrat nicht mitbestimmungsberechtigt. Zwar bieten die Informationen im Envelope die Möglichkeit zur Überwachung der Beschäftigten, jedoch nicht über den notwendigerweise bereits vorhandenen E-Mail-Dienst hinaus.

Hinsichtlich der Informationspflichten ergeben sich keine Unterschiede zum Blacklisting nach Verbindungsaufbau.

Greylisting

Beim Greylisting wird in der Annahme, dass Spam-Versender anders als „seriöse“ Mail-Versender nur einen Zustellversuch unternehmen, vom Empfänger-Server der erste Zustellversuch jeder E-Mail abgelehnt. Um die Zustellung der E-Mail beim zweiten Zustellversuch zu ermöglichen, werden beim ersten Zustellversuch Daten des Envelopes und damit personenbezogene Daten erhoben und gespeichert. Anders als beim Blacklisting nach Kenntnisnahme des Envelopes werden die Daten auf dem Empfänger-Server aber nicht nur für die Zustellung der E-Mail, sondern auch zum Zweck der Feststellung des zweiten Zustellversuchs und damit für die Spam-Abwehr verwendet.

Wegen dieser Zweckänderung sind auf das Greylisting andere datenschutzrechtliche Normen als auf das Blacklisting nach Kenntnisnahme des Envelopes anwendbar. Hier ergibt sich die datenschutzrechtliche Rechtmäßigkeit bei Zulassung der Privatnutzung des E-Mail-Dienstes aus § 100 Abs. 1 TKG, andernfalls aus den einschlägigen Regelungen im Bundesdatenschutzgesetz (BDSG) und in den Landesdatenschutzgesetzen. Dabei ist jedoch eine Pseudonymisierung mindestens der E-Mail-Adressen erforderlich, da sie den Betreiber des E-Mail-Dienstes nicht übermäßig, den Nutzer jedoch deutlich weniger belastet.

Greylisting verstößt nicht gegen das Fernmeldegeheimnis. Zwar liefern die Daten des Envelopes Kenntnis über die näheren Umstände der Kommunikation, dies ist aber nach § 88 Abs. 3 Satz 1 TKG zulässig, da die Kenntnis für die geschäftsmäßige Erbringung des Dienstes erforderlich ist. Ausschlaggebendes Argument ist auch hier der für die Diensterbringung unabdingbare Schutz der technischen Systeme vor Überlastung und Versagen durch das massenhafte Aufkommen von Spam-Mails.

Auch beim Greylisting sprechen gute Argumente gegen eine strafrechtliche Relevanz. Die Argumente zu § 206 Abs. 2 Nr. 2 StGB sind dieselben wie beim Blacklisting nach Kenntnisnahme des Envelopes. Hinsichtlich der nach § 303a StGB strafbaren Datenunterdrückung kann auf die Ausführungen zum Blacklisting nach Verbindungsaufbau verwiesen werden.

In Bezug auf die Pflichten des Betreibers des Empfänger-Servers aus dem Nutzungsverhältnis gilt das zum Blacklisting nach Verbindungsaufbau Gesagte.

Beim Greylisting ist der Personal- bzw. Betriebsrat aus denselben Gründen wie beim Blacklisting nach Kenntnisnahme des Envelopes nicht mitbestimmungsberechtigt.

Der Empfänger muss über die Ablehnung einer E-Mail nicht informiert werden. Dem Versender-Server wird eine Fehlermeldung zugestellt, dies ist dem Greylisting inhärent. Nur so kann der Versender-Server, soweit er richtig konfiguriert ist, einen erneuten Zustellversuch vornehmen.