28. Jahrgang
Heft 21
25. Mai 2007/S. 985

Zeitschrift für Wirtschaftsrecht ZIP

Aufsätze

Mark C. Hilgard[*)]

Archivierung und Löschung von E-Mails im Unternehmen

Kaum einem Unternehmen gelingt es, seinen Datenbestand so zu optimieren, dass es nur nützliche E-Mails archiviert, alle überflüssigen E-Mails aber löscht. Der Beitrag zeigt die gesetzlichen Archivierungsfristen für E-Mails auf und beschäftigt sich mit den Rechtsfolgen gezielter und automatischer Löschungsaktionen. Er beleuchtet zudem einige Anforderungen an ein Dokumentenmanagementprogramm.

I. Einführung

1. Die Speicherung von E-Mails

Unternehmen speichern Dokumente, und insbesondere E-Mails, nicht wegen gesetzlicher Anforderungen, sondern um Vorgänge zu dokumentieren. Sie wollen geschäftliche Vorfälle festhalten und die Dokumentation, falls notwendig, zu Beweiszwecken verwenden können. Sie bewahren E-Mails daher im eigenen Interesse auf, um ggf. den Nachweis bestimmter Vorfälle führen zu können. Für das umsichtige Unternehmen ist prinzipiell alles archivierungsbedürftig, was in einem Streitfall nutzbar gemacht werden kann. Gerade wenn Rechtsstreitigkeiten, Produkthaftungs- oder Gewährleistungsansprüche drohen, will sich ein Unternehmen durch Speicherung der Daten, Geschäftsdokumente und E-Mails absichern. Die Datenmenge wächst beständig an, das Datenarchiv droht zu platzen.

2. Das Löschen von E-Mails

Erfahrungsgemäß neigt der Umgangston in E-Mails dazu, schnell zu eskalieren. E-Mails sind, weil einfach zu versenden, ein ideales Mecker- und Beschwerdemedium. Schnell geschrieben, werden sie dank beliebig langer Speichermöglichkeit leicht zum elektronischen Elefantengedächtnis eines Unternehmens.[1)] Insofern können in diesem „E-Giftschrank" viele Mittelchen gefunden werden, die gegen alle möglichen Personen, etwa gegen den Absender, aber natürlich auch gegen das Unternehmen, verwendet werden können. Dies legt den Gedanken nahe, den E-Giftschrank regelmäßig zu leeren („Was ich nicht mehr weiß, macht mich nicht mehr heiß.").

Das wachsende E-Mail-Aufkommen belastet auch die IT-Systeme der Unternehmen ganz erheblich. Nach einer Vergleichsstudie des Speicherherstellers Hitachi Data Systems[2)] verbrauchen E-Mails bereits durchschnittlich mehr als 10 % der Speicherkapazität. Löschungsaktionen liegen daher auch aus technischen Gründen nahe.

Gegen ein Anwachsen der Datenmengen gibt es verschiedene Rezepte. Dokumente sollen jedoch nicht irgendwelchen unkontrollierten Löschaktionen zum Oper fallen. So gibt es Versuche, die Kapazität der Mailboxen („Postfächer") auf eine bestimmte Anzahl von Megabytes pro Mitarbeiter zu begrenzen und den Anwender somit indirekt zu zwingen, überschüssige E-Mails zu löschen.[3)] Oder es wird unternehmensseitig vorgegeben, E-Mails sofort in bestimmten Ordnern – etwa projektbezogen – abzulegen. Andere wiederum versuchen, die Diskussion einzelner Themen in ein Forum auszulagern, in dem die E-Mails sodann ausgetauscht werden. Aus diesem Grund liegt es für ein Unternehmen ebenfalls nahe, alle, den Großteil oder jedenfalls einen erheblichen Teil von E-Mails nach Ablauf bestimmter Zeiträume („Vernichtungszyklen")[4)] automatisch zu löschen.

Automatische oder gezielte Löschaktionen können also sowohl unter hygienischen als auch unter technischen Aspekten

*) *Dr. iur., Rechtsanwalt und Partner in der Sozietät Mayer, Brown, Rowe & Maw LLP, Frankfurt/M.*

1) Instruktiv die Beispiele in Wirtschaftswoche Nr. 24 v. 9. 6. 2005, S. 47 ff. und bei *Braun*, DatenschutzPraxis, Oktober 2005, S. 12.

2) Zitiert nach Wirtschaftswoche Nr. 24 v. 9. 6. 2005, S. 49.

3) Dies kann allerdings dazu führen, dass die Mitarbeiter eigene persönliche E-Mail-Archive auf den PCs oder Netzwerklaufwerken einrichten. Der Sinn der Mailboxbeschränkung wird damit konterkariert.

4) Unternehmen, die ihre E-Mails aus den beschriebenen Gründen grundsätzlich nach Ablauf einer bestimmten Frist löschen, können keineswegs sicher sein, dass die E-Mails auch wirklich spurlos verschwunden sind. Abgesehen davon, dass gerade brisante E-Mails oft – etwa von Angestellten – „zur Sicherheit" als Kopie gespeichert werden, tauchen Spuren in Sicherungsdateien auf dem eigenen Rechner, im Mail-Server oder beim Empfänger auf. Software zur Löschung von Daten vernichtet oft zwar eine beträchtliche Anzahl von Sektoren, löscht aber nicht alle Daten. Fachleute vertreten teilweise die Auffassung, wer absolute Sicherheit wolle, solle die Platte physisch zerstören. Zudem werden E-Mails oft unkontrolliert an eine Vielzahl von Empfängern weitergeleitet.

sinnvoll sein. Wie aber sind sie rechtlich zu bewerten? In den USA sind unqualifizierte Löschaktionen mit horrenden Strafen bedroht. So wird es nach dem Sarbanes Oxley Act mit bis zu 20 Jahren Gefängnis und 1 Mio. US-$ Geldbuße geahndet, wenn E-Mails gelöscht oder verfälscht werden, die als Beweismaterial in einem Betrugsverfahren dienen könnten.[5] Wie sieht es mit der Zulässigkeit solcher Löschaktionen in Deutschland aus? Stehen in Deutschland lediglich die gesetzlichen Aufbewahrungsfristen für Handelsdokumente und steuerlich relevante Unterlagen einer Löschung entgegen? Welche Konsequenzen hat die Löschung aufbewahrungspflichtiger E-Mails?

Mit den gesetzlichen Vorgaben, präventiven und reaktiven forensischen Maßnahmen und praktischen Implikationen rund um die Löschung von E-Mails durch ein Unternehmen befasst sich der vorliegende Beitrag.

II. Die Aufbewahrungsfristen für E-Mails

1. Beweisfunktion

Mit E-Mails werden Nachrichten oder Informationen über das Internet versandt. Die Änderung der §§ 126, 127 BGB und die Einführung der elektronischen Signatur durch das Signaturgesetz haben elektronische zunehmend den papiergebundenen Informationen rechtlich gleichgestellt.[6]

Gemäß Art. 5 Abs. 1 lit. b der SigRL[7] sollen elektronische Dokumente, die mit einer qualifizierten Signatur versehen sind, in gerichtlichen Verfahren als Beweismittel zugelassen werden. Elektronische Dokumente können daher jetzt in allen Gerichtszweigen als Beweismittel (Augenscheinobjekte[8]) eingesetzt werden. Damit steigt ihr Beweiswert. Um dem Empfänger einer elektronischen Erklärung den Beweis zu erleichtern, dass diese von der in der qualifizierten Signatur ausgewiesenen Person stammt, ordnet § 371a ZPO einen Beweis des ersten Anscheins an. Auch in Schiedsverfahren finden sich immer öfter Dokumente nur in elektronischer Form.[9]

2. Handels- und steuerrechtliche Aufbewahrungsfristen

Für die Aufbewahrung von E-Mails bestehen in Deutschland keine speziellen gesetzlichen Fristen. Vielmehr gelten dieselben gesetzlichen Aufbewahrungsfristen wie für Dokumente in Papierform, also jene gesetzlichen und regulatorischen Anforderungen, welche auch als „Compliance-Anforderungen" bezeichnet werden. Vor dem Gesetz ist alles aufbewahrungspflichtig, was für eine betriebliche Überprüfung und die Transparenz der Unternehmensverhältnisse bedeutsam ist. Ob und, wenn ja, wie lange E-Mails aufzubewahren sind, richtet sich also nach ihrem Inhalt. So sind beispielsweise E-Mails, die als Handels- oder Geschäftsbrief zu qualifizieren sind oder steuerlich relevante Daten enthalten, 6 Jahre aufzubewahren. E-Mails mit rein privatem Inhalt unterliegen hingegen überhaupt keiner Aufbewahrungsfrist.

Einschlägig sind damit die *handelsrechtlichen* Aufbewahrungsfristen des § 257 HGB, welche auf die zuverlässige Dokumentation der Geschäfte zwischen Kaufleuten hinwirken, sowie die *steuerrechtlichen* Aufbewahrungspflichten des § 147 AO, welche auf die Transparenz und Prüfbarkeit der Steuererklärung abzielen. Danach unterliegen einer 10-jährigen Aufbewahrungsfrist: Handelsbücher/Bücher, Inventar, Jahresabschlüsse, Lageberichte, Eröffnungsbilanz, Konzernabschlüsse, Konzernlageberichte, Arbeitsanweisungen, sonstige Organisationsunterlagen, Buchbelege. Einer 6-jährigen Aufbewahrungsfrist unterliegen empfangene Handels- oder Geschäftsbriefe, Wiedergabe der abgesandten Handels- oder Geschäftsbriefe und sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind. Ergänzt werden die Vorschriften des § 257 HGB bzw. § 147 AO durch Ziffer 7 der Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)[10], welche die Aufbewahrungsfrist der Verfahrensdokumentation zur DV-Buchführung regelt. Die Verfahrensdokumentation gehört zu den Arbeitsanweisungen und sonstigen Organisationsunterlagen i. S. d. § 257 Abs. 1 HGB bzw. § 147 Abs. 1 AO und ist daher grundsätzlich 10 Jahre aufzubewahren. Teile der Verfahrensdokumentation, denen ausschließlich Belegfunktion zukommt (z. B. die Dokumentation zur DV-Verkaufsabrechnung, aus der sich die Buchungen zu den Forderungen ergeben), sind grundsätzlich nur 6 Jahre aufzubewahren. Verkürzt ausgedrückt: Geschäftliche E-Mails müssen 6 Jahre lang aufbewahrt werden.

Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahrs, in dem die aufzubewahrende E-Mail empfangen oder abgesandt wurde. Bei per E-Mail abgeschlossenen Verträgen beginnt die Aufbewahrungsfrist mit dem Ende des Jahres, in dem der Vertrag endet.

Gemäß § 147 Abs. 3 Satz 2 AO läuft die steuerrechtliche Aufbewahrungsfrist nicht ab, soweit und solange die betreffenden E-Mails für Steuern von Bedeutung sind, für welche die Festsetzungsfrist, in der Regel 1 bis 4 Jahre, noch nicht abgelaufen ist.

Um Unsicherheiten bei der Feststellung abzumindern, wann Unterlagen vernichtet werden dürfen, sieht das BMF-Schreiben vom 25. 10. 1977 vor, dass Unterlagen nach Ablauf der in der AO genannten oder in anderen Steuergesetzen zugelassenen kürzeren Aufbewahrungsfristen nur noch aufzubewahren sind, wenn und soweit sie erforderlich sind für eine begonnene Außenprüfung, für eine vorläufige Steuerfestsetzung nach § 165 AO, für anhängige steuerstraf- oder bußgeldrechtliche Ermittlungen, für ein schwebendes oder aufgrund einer Außenprüfung zu erwartendes Rechtsverfahren oder zur Begründung von Anträgen des Steuerpflichtigen.

Bei der elektronischen Archivierung von E-Mails muss sichergestellt sein, dass die Daten mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar ge-

5) Der Sarbanes Oxley Act gilt zwar nur in den USA, hat aber drastische Auswirkungen auf den internationalen Rechtsverkehr; international agierende deutsche Unternehmen kommen gar nicht daran vorbei, sich mit diesem Gesetz und seinen Auswirkungen auf ihr Geschäft auseinanderzusetzen.

6) Verträge können – soweit nicht Schriftform vorgeschrieben ist – auch per E-Mail abgeschlossen werden. Auch elektronische Willenserklärungen sind echte Willenserklärungen.

7) RL 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen v. 13. 12. 1999, ABl EG Nr. 1113 v. 19. 1. 2000.

8) §§ 371, 371a ZPO, § 91 Abs. 1 Satz 1 VwGO, §§ 71 ff. StPO, § 81 Abs. 1 Satz 2 SGO sowie § 83 Abs. 1 ArbGG.

9) Vgl. hierzu etwa *Gebhardt*, IDR 2005, 30, 36.

10) BMF-Schreiben v. 9. 11. 1993, BStBl I 1995, 738,

macht werden, während der Aufbewahrungsfrist verfügbar sind, jederzeit innerhalb angemessener Frist lesbar gemacht und für die Besteuerung maschinell ausgewertet werden können.[11] Verstöße gegen die Archivierungspflichten von Handelsbriefen, einschließlich E-Mails, werden durch § 283b Abs. 1 Nr. 2 StGB (Verletzung der Buchführungspflicht) mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe geahndet.

3. Weitere materiellrechtliche Aufbewahrungspflichten

Neben den allgemeinen handels- und steuerrechtlichen Aufbewahrungspflichten bestehen für bestimmte Geschäftsaktivitäten auch spezialgesetzliche Aufbewahrungsfristen. So müssen etwa Banken bestimmte Transaktionen dokumentieren und die entsprechenden Dokumente vorhalten;[12] auch die Bestimmungen des Geldwäschegesetzes sehen Dokumentationspflichten vor, die natürlich nur Sinn machen, wenn die entsprechende Dokumentation über einen bestimmten Zeitraum aufzubewahren – und damit zugänglich – ist.

Daneben gibt es Aufbewahrungspflichten, die sich als Reflexwirkung aus anderen Pflichten ergeben. Derjenige, der von einem anderen aus materiellrechtlichen Gründen die Herausgabe oder Einsichtnahme[13] in Dokumente verlangen kann, hat einen Anspruch darauf, dass der andere diese Dokumente auch tatsächlich bis zur Herausgabe oder Einsichtnahme aufbewahrt. Diese Aufbewahrungspflichten beruhen nicht unmittelbar auf dem Gesetz, sondern auf zivilrechtlichen oder öffentlich-rechtlichen Verpflichtungen. Es muss betont werden, dass ein materiellrechtlicher Anspruch auf Herausgabe oder Vorlegung der Daten in Konkurrenz zu den gesetzlichen Aufbewahrungsfristen steht. Bei Ablauf gesetzlicher Aufbewahrungsfristen stellt sich also stets auch die Frage, ob Dritte eigene Rechte an diesen Daten haben, welche zu einer Aufbewahrungspflicht führen und damit gleichfalls einer Vernichtung entgegenstehen könnten.

4. Zwischenergebnis

Es kann damit festgehalten werden, dass E-Mails nicht gelöscht werden dürfen, solange sie aus handels- oder steuerrechtlichen oder spezialgesetzlichen Gründen aufbewahrt werden müssen.

III. Löschen von Daten nach Ablauf der Aufbewahrungsfrist als Beweisvereitelung?

Wie ist es rechtlich zu beurteilen, wenn E-Mails, die nicht (mehr) aufbewahrungspflichtig, aber beweisrelevant sind oder möglicherweise zu einem späteren Zeitpunkt werden können, entweder systematisch – etwa aufgrund eines Document Retention Plan (dazu unten V) – oder gezielt (etwa im Hinblick auf eine zukünftig drohende streitige Auseinandersetzung[14]) gelöscht werden: Liegt eine strafbare Beweisvereitelung vor?

1. Die zivilrechtliche Seite

Die ZPO enthält keine Regeln für Beweisvereitelung.[15] Nach herrschender Definition liegt eine Beweisvereitelung vor, „wenn eine Partei dem beweispflichtigen Gegner die Beweisführung vorwerfbar unmöglich macht oder erschwert, indem sie vorhandene Beweismittel vernichtet oder sonstwie deren Benutzung verhindert".[16]

Diese Definition ergibt sich aus dem im Zivilrecht herrschenden Beibringungsgrundsatz, wonach die Parteien – und zwar nur sie – darüber entscheiden können, welchen Tatsachenstoff sie dem Gericht unterbreiten.[17] Die zivilprozessuale Konsequenz einer Vereitelung des Beweises ist eine dem Vereiteler nachteilige Beweiswürdigung.[18] Wenn allerdings völlig offen ist, ob das vernichtete Beweismittel überhaupt Relevanz gehabt hätte, bleibt die Tat zivilprozessual ohne Folgen.

2. Die strafrechtliche Seite

§ 274 Abs. 1 Nr. 2 StGB regelt die Beseitigung beweiserheblicher Daten. Danach wird mit Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe bestraft, wer „beweiserhebliche Daten (§ 202a Abs. 2 StGB), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht, einem anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert".

Der objektive Tatbestand des § 274 Abs. 1 Nr. 2 StGB wirft damit zwei Fragen auf: Sind E-Mails, die nicht mehr aufbewahrt werden müssen, an denen aber vielleicht irgendwann einmal jemand ein Interesse haben *könnte*, „beweiserheblich"? Und was bedeutet „nicht oder nicht allein verfügen dürfen" für den Täter?

2.1 Beweiserhebliche Daten

Wenden wir uns zunächst der ersten Frage zu. § 274 StGB verweist auf die Definition beweiserheblicher Daten in § 202a Abs. 2 StGB. Anders als § 269 StGB (der ebenfalls den Terminus „beweiserhebliche Daten" gebraucht, einen Verweis auf § 202a Abs. 2 StGB jedoch nicht enthält) beschränkt sich § 274 StGB also allein auf den Schutz von Daten, welche „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden".

Zur Bestimmung des Merkmals der Beweiserheblichkeit solcher Daten ist auf § 269 Abs. 1 StGB zurückzugreifen. „Beweiserheblich"[19] sollen nach der Regelungsabsicht des Gesetz-

11) Die Finanzverwaltung darf auch digitale Unterlagen prüfen; die Form der Speicherung und Vorlage ist Teil des Prozesses, welcher von einem Dokumentenmanagementsystem erfasst werden muss.

12) Vgl. dazu etwa die MaRisk.

13) Ein solches Recht kann sich z. B. aus § 810 BGB ergeben.

14) Schließlich können sich Dokumente oder E-Mails, die als die eigenen Prozesschancen nicht fördernd eingestuft werden, irgendwann einmal als vorlagepflichtig herausstellen.

15) Normen, die einen Beweisvereitelungssachverhalt erfassen, sind etwa §§ 427, 441 Abs. 3 Satz 3, §§ 444, 453 Abs. 2, § 454 Abs. 1 ZPO.

16) BGH ZIP 1985, 312 = NJW 1986, 59, 60, dazu EWiR 1985, 219 *(Gerhardt)*; OLG Köln VersR 1992, 356.

17) Die Parteien entscheiden, welcher Tatsachenstoff in den Prozess eingeführt wird; das Gericht darf seinem Urteil nur solche Tatsachen zugrunde legen, die von den Parteien vorgetragen worden sind; BVerfG NJW 1979, 1925, 1927; BGH NJW 1981, 574; BGH NJW 1989, 3161, 3162. Das Gericht darf Tatsachen, die die Parteien nicht vorbringen, grundsätzlich nicht berücksichtigen, BGH MDR 1978, 567; *Baumbach/Lauters/Albers/Hartmann*, ZPO, 65. Aufl., 2007, Grdz. § 128 Rz. 23.

18) BGH GRUR 1995, 697, dazu EWiR 1995, 1019 *(Bacher)*.

19) Beweiserheblich sind Daten, wenn die verkörperte Erklärung bestimmt und geeignet ist, für ein Rechtsverhältnis Beweis zu erbringen; *Cramer*, in: Schönke/Schröder, StGB, 27. Aufl., 2006, § 269 Rz. 9. Als beweiserhebliche Daten werden solche angesehen, die i. S. d. § 269 StGB urkundengleiche Beweisfunktion haben (a. A. *Lenckner-Winkelbauer*, CR 1986, 824, 827).

gebers nur solche Daten sein, die „dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden".

Beweiserhebliche Daten sollen danach die Verwendung von Urkunden ersetzen.[20] Aus dem Zweck der Vorschrift, wonach nur solche Daten in Betracht kommen, die im Falle ihrer Wahrnehmbarkeit tauglicher Urkundeninhalt sein können, wird geschlossen, dass die verkörperte Erklärung bestimmt und geeignet sein muss, für ein Rechtsverhältnis Beweis zu erbringen.[21] Man wird daher davon ausgehen müssen, dass alle E-Mails, die ausgedruckt als „Urkunde" angesehen würden, gleichfalls „beweiserhebliche Daten" i. S. d. § 274 Abs. 1 Nr. 2 StGB sind. Ob sie zu irgendeinem Zeitpunkt von prozessualer Bedeutung sind oder werden können, spielt keine Rolle.

2.2 Verfügungsbefugnis

Damit kommen wir zur zweiten Frage: Vertreten wird entsprechend dem Schutzzweck des § 274 StGB, „verfügen dürfen" bezeichne das *Beweisführungsrecht*, also das Recht, mit den Daten im Rechtsverkehr Beweis zu erbringen.[22] Damit stellt sich die Frage, wann das Interesse eines Dritten am unveränderten Bestand der Daten zu einem Recht zur Beweisführung erstarkt und damit die alleinige Verfügungsbefugnis des Dateninhabers einschränkt. Bereits oben unter II 3 wurden solche Aufbewahrungspflichten, welche sich als Reflexwirkung aus anderen Pflichten ergeben, dargestellt.

2.2.1 Vorlagepflicht aus materiellrechtlichen Gründen

Eine alleinige Verfügungsbefugnis soll nicht mehr vorliegen, wenn der Inhaber der Daten vorlegungspflichtig ist[23] bzw. wenn sich in einem konkreten Rechtsstreit ein Beweisführungsinteresse der Gegenpartei erkennbar manifestiert hat, beispielsweise durch die Aufforderung, die Daten vorzulegen.[24] In diesem Falle stehe eben auch dem Dritten ein Verfügungsrecht zu, mit der Konsequenz, dass der Inhaber der Daten bei eigenmächtiger Löschung den objektiven Straftatbestand des § 274 StGB verwirklicht.

Es gibt auch Entscheidungen, wonach ein ausschließliches Verfügungsrecht des Dateninhabers nicht mehr besteht, wenn ein Dritter Anspruch auf Vorlegung der Urkunde hat.[25] Andererseits sollen gesetzliche Vorlegungspflichten für § 274 Abs. 1 Nr. 1 StGB einem ausschließlichen Verfügungsrecht nur dann entgegenstehen, wenn sie die „Rechnungslegung im weiteren Sinne und nicht allein (in der Regel bußgeldrechtlich abgesicherte) öffentlich-rechtliche Überwachungsmaßnahmen erleichtern sollen".[26]

Ein alleiniges Verfügungsrecht steht dem Besitzer der Daten sicherlich nicht zu, wenn ein Dritter von ihm aus materiellrechtlichen Gründen die Herausgabe oder die Vorlegung der Daten verlangen kann. Demgemäß statuiert etwa § 422 ZPO bei Bestehen einer materiellrechtlichen Pflicht auch eine prozessuale Vorlagepflicht, die zum Entfallen einer alleinigen Verfügungsbefugnis über die Daten führt.

2.2.2 Vorlagepflicht aus prozessualen Gründen

Der durch die ZPO-Reform vom 27. 7. 2001 zum 1. 1. 2002 überarbeitete § 142 ZPO ermöglicht es dem Gericht, einer Partei die Vorlage solcher Daten aufzugeben, die die beweisbelastete Partei materiellrechtlich gerade nicht herausverlangen kann (§ 422 ZPO). Hierzu gehören auch E-Mails.[27]

Es herrscht weitgehend Einigkeit darüber, dass elektronische Dokumente, die in einem Computerspeicher existieren, keine Urkunden i. S. d. § 142 ZPO darstellen: Zum einen fehlt es an der schriftlichen Verkörperung der im elektronischen Dokument enthaltenen Gedankenäußerung. Darüber hinaus fehlt ihnen die Verkehrsfähigkeit. Der hohe Beweiswert der Urkunde liegt in der jederzeitigen Möglichkeit der Einsichtnahme. Dies ist bei elektronischen Speicherverfahren nicht gegeben, da regelmäßig ein hoher technischer Aufwand erforderlich ist, den Inhalt des Dokuments sichtbar zu machen. Weiterhin spricht gegen die Qualifizierung des elektronisch gespeicherten Dokuments als Urkunde dessen Unzuverlässigkeit. Die Fälschung eines solchen Dokuments, ohne Spuren zu hinterlassen, erscheint relativ leicht möglich. Eine E-Mail – auch wenn sie ausgedruckt wird – stellt daher keine Urkunde im beweisrechtlichen Sinne dar, sondern lediglich ein Augenscheinobjekt von wesentlich geringerer Beweiskraft.

„Sonstige Unterlagen" i. S. d. § 142 ZPO sind jedoch auch alle Gegenstände, die sich im Besitz einer Partei oder eines Dritten befinden und eine Ähnlichkeit zu Urkunden aufweisen, soweit sie ebenfalls die Aufzeichnung einer Information darstellen, also insbesondere Bild-, Daten- oder Tonträger, selbst wenn ihr gedanklicher Inhalt nicht ohne technische Hilfsmittel sinnlich wahrnehmbar ist. Damit lassen sich elektronische Dokumente unter den Begriff der „sonstigen Unterlagen" subsumieren.[28]

Ist die durch einen Beschluss nach § 142 ZPO *prozessual* eingeschränkte Verfügungsmacht des Dateninhabers derjenigen vergleichbar, welche aufgrund eines materiellrechtlichen Anspruchs eines Dritten eingeschränkt ist? Bei der Beantwortung dieser Frage muss berücksichtigt werden, dass die Anordnung der Datenvorlage nach § 142 ZPO eine Ermessensentscheidung ist, die eine Abwägung aller Umstände des Einzelfalls erfordert. Da man nicht davon ausgehen kann, dass sich das Ermessen des Gerichts regelmäßig auf null reduzieren wird, kann mithin das Verfügungsrecht des Inhabers der Daten allenfalls ab dem Zeitpunkt prozessual eingeschränkt sein, ab dem eine entsprechende Datenvorlage durch das Gericht *angeordnet* wird. Es kommt also nicht darauf an, ob dem Vernichter die Notwendigkeit der Daten zur Beweisführung durch den Dritten „bereits erkennbar sein musste", wie dies vielfach

20) *Tröndle/Fischer*, StGB, 52. Aufl., 2004, § 269 Rz. 3.
21) *Cramer* (Fußn. 19), § 269 Rz. 9.
22) *Cramer* (Fußn. 19), § 274 Rz. 5; ebenso *Holznagel*, Recht der IT-Sicherheit, 2003, § 7 Rz. 29.
23) *Cramer* (Fußn. 19), § 274 Rz. 5; BGHSt 29, 192; BayObLG NJW 1980, 1057; *Tröndle/Fischer* (Fußn. 20), § 274 Rz. 2; OLG Celle NJW 1966, 557; BayObLG NJW 1968, 1896.
24) *Cramer* (Fußn. 19), § 274 Rz. 5; ebenso *Holznagel* (Fußn. 22), § 7 Rz. 29.
25) OLG Celle NJW 1966, 557; BayObLG NJW 1968, 1896.
26) Vgl. etwa OLG Düsseldorf NJW 1985, 1232.
27) Ablehnend *Stein/Jonas*, ZPO, 22. Aufl., 2005, § 142 Rz. 15 mit dem Argument, sie seien keine „Unterlagen" i. S. d. § 142 ZPO, da sie in § 371 Abs. 1 Satz 2 ZPO eindeutig als Augenscheinobjekte behandelt würden. Die Vorlage elektronischer Dokumente sei daher nach § 144 ZPO zu beurteilen.
28) Vgl. im Einzelnen *Kraayvanger/Hilgard*, Die Justiz 2003, 572.

postuliert wird.[29] Vor einer gezielten Anordnung ist die Löschung der Daten vielmehr ohne weiteres zulässig. Da gegen die Vorlageanordnung kein spezieller Rechtsbehelf zur Verfügung steht, kommt es auf die „Rechtskraft" einer solchen Anordnung nicht an.

Damit bleibt festzuhalten, dass das Verfügungsrecht des Inhabers von Daten, welche evtl. gemäß § 142 ZPO aufgrund einer Ermessensentscheidung eines Zivilgerichts vorgelegt werden müssen, jedenfalls bis zu einem entsprechenden Vorlagebeschluss nicht eingeschränkt ist. Eine Vernichtung bzw. Löschung dieser Daten *vor* Erlass des Beschlusses ist nur dann tatbestandsauslösend i. S. d. § 274 StGB, wenn dem Gericht gar keine andere Wahl bleibt, als die Vorlage der Daten anzuordnen. Ein solcher Fall erscheint bei der gegenwärtigen Praxis kaum denkbar. Vorlagebeschlüsse ergehen nicht aus heiterem Himmel, sondern aufgrund schlüssigen Tatsachenvortrags der beweisbelasteten Partei. Dass ein solcher Vortrag jedoch zwingend zum Erlass eines entsprechenden Vorlagebeschlusses nach § 142 ZPO führt, ist kaum vorstellbar.

Als Ergebnis ist damit festzuhalten, dass das Gericht gemäß § 142 ZPO die Vorlage elektronischer Dokumente wie z. B. E-Mails fordern kann. Bis zum Erlass eines solchen Beschlusses ist die Vernichtung von E-Mails ohne Bestehen eines materiellrechtlichen Herausgabeanspruchs nicht als Beweisvereitelung oder Urkundenunterdrückung strafbar.

2.3 Der subjektive Tatbestand des § 274 StGB

Aus dem Vorstehenden wird ersichtlich, dass die Löschung von E-Mails relativ schnell den objektiven Tatbestand des § 274 Abs. 1 Nr. 2 StGB erfüllen kann. Es lohnt sich daher, auch einen Blick auf die subjektive Seite des Tatbestands zu richten.

Neben der Kenntnis einer Einschränkung des eigenen Verfügungsrechts (also etwa eines gerichtlichen Vorlagebeschlusses) erfordert die Beweisvereitelung auf subjektiver Seite einen doppelten Schuldvorwurf. Das Verschulden muss sich sowohl auf die Zerstörung bzw. Entziehung der Daten als Beweisobjekt beziehen („Wollen der Vernichtungshandlung"), als auch auf die Beseitigung seiner Beweisfunktion, also darauf, die Beweislage des Gegners in einem (gegenwärtigen oder zukünftigen) Prozess nachteilig zu beeinflussen.[30] Der Dateninhaber muss in der Absicht handeln, einem anderen Nachteil zuzufügen, wobei die Schädigung durchweg nicht das einzige Motiv zu sein braucht. Als Nachteil ist jede Beeinträchtigung fremder Rechte (auch Beweisführungsrechte[31]) zu verstehen, etwa die Verschlechterung der Beweislage[32]. Absicht der Nachteilszufügung bedeutet unbedingten Vorsatz.[33]

IV. Die Aufbewahrungs- und Herausgabepflichten für E-Mails in den USA

Hier ist nicht der Ort, um amerikanische Aufbewahrungsfristen aufzuzeigen. Höchst bedeutsam ist jedoch, dass in den USA jede Partei im Vorfeld eines Zivilprozesses verpflichtet ist, der Gegenseite auf Anforderung Unterlagen herauszugeben, welche in einem bevorstehenden Verfahren als „potentially relevant and discoverable" qualifiziert werden. Nicht selten geht es dabei um Hunderttausende von Seiten Papier, und die Gefahr, auf diese Weise Geschäftsgeheimnisse an einen Wettbewerber zu verlieren, war schon bisher groß.

Durch den umfassenden Einsatz von E-Mails, die mehr und mehr herkömmliche Korrespondenz und auch Telefonate ersetzen, ist das Verfahren mittlerweile aber noch komplizierter geworden. So ist jede E-Mail prozessrechtlich ein separates Dokument, und an einem einzigen Tag kann das E-Mail-System eines Unternehmens Tausende solcher Dokumente hervorbringen, welche prozessrelevant sein können. Rechtsfragen um die Herausgabe von Daten haben sich daher unter der Bezeichnung „Electronic Discovery" oder „E-Discovery"[34] als ein eigenes Rechtsgebiet herauskristallisiert. Wie sollen, etwa im Fall einer Produkthaftungsklage, Kopien aller dieses Produkt betreffenden E-Mails gesammelt, analysiert und sodann vorgelegt werden? Führt die Pflicht zur Aufbewahrung relevanter Dokumente dazu, dass ein Angestellter seine E-Mails nicht mehr löschen darf? Muss ein Unternehmen E-Mails, die vor Monaten gelöscht wurden, wiederherstellen? Wie soll es Millionen von E-Mails durchsuchen, um die wichtigen von den belanglosen zu trennen? Und welche gerichtlichen Sanktionen drohen, wenn es versäumt, seine E-Mails in einer E-Discovery offenzulegen?[35]

War ein amerikanisches Beweisermittlungsverfahren schon bisher ein schwieriges und teures Unterfangen, so hat die E-Discovery Aufwand und Risiken für Unternehmen erheblich erhöht. Sie müssen nun damit rechnen, dass sie alle relevanten E-Mails offenbaren müssen.[36] E-Discovery eröffnet Klägern eine neue Dimension von Informationen, insbesondere den Zugriff auf interne Kommunikationsvorgänge beklagter Unternehmen.[37]

Bislang fehlt es selbst in den Vereinigten Staaten noch an hinreichenden rechtlichen Regeln zur E-Discovery.[38] Erst seit dem 1. Dezember 2006 fallen elektronisch gespeicherte Informationen in die Kategorie vorzulegender Dokumente.[39] Die Gerichte stellen unterschiedliche Anforderungen an die

29) Vgl. BGH NJW 1960, 821; BGH NJW 1963, 389; BGH NJW 1976, 1315, 1316.
30) BGH VersR 1995, 952, 954; BGH NJW 1994, 1594, 1595; *Musielak/Foerste*, ZPO, 5. Aufl., 2007, § 286 Rz. 65; MünchKomm-*Prütting*, ZPO, 2. Aufl., 2000, § 286 Rz. 81; BGH NJW 2004, 2221.
31) BGHSt 29, 192.
32) RGZ 22, 285; RGHRR 1936 Nr. 1026.
33) OLG Hamburg NJW 1964, 736, 737.
34) In England besteht mit der „E-Disclosure" ein ähnliches Konzept; vgl. etwa *Sautter*, New Law Journal 2005, 1618.
35) Hingewiesen sei etwa auf den Fall Morgan Stanley, in dem ein Award in Höhe von 1,45 Mrd. US-$ erging; der Fall involvierte die Nichtvorlegung von E-Mails und falsche Angaben über die vorzulegenden Informationen (vgl. dazu etwa „Don't Hit Delete", International Bar News, Oktober 2005, S. 8). *Bücking/Weber* weisen in Computerwoche.de vom 17. 11. 2005 darauf hin, dass ein Zivilprozess allein schon deshalb verloren werden kann, weil eine Partei beweispflichtige Tatsachen, welche elektronisch dokumentiert sein müssten, nicht rechtzeitig findet.
36) „This is one of the greatest legal risks US companies face today" – so die Union Bank of California, zitiert nach International Bar News, Oktober 2005, S. 8. Zu den Grundlagen vgl. auch *Gebhardt*, IDR 2005, 30.
37) Vgl. etwa *Hess*, AG 2005, 897, 904.
38) Der schon zitierte Sarbanes Oxley Act sowie die entsprechenden Anwendungsvorschriften und -richtlinien dürften wohl den größten Einfluss auf Datenmanagementprogramme haben.
39) Vgl. FRCP 34(a); hierzu eingehend etwa *Allman*, FCLR Sept. 2006; *Allman*, Northwestern Journal of Technology and Intellectual Property, 2006, Vol. 5, No. 1.

Pflicht zur Aufbewahrung und Herausgabe elektronischer Dokumente und kommen teilweise zu sehr drastischen und damit fragwürdigen Lösungen.[40] Auch die Parteien äußern oft exzessive, nur schwer erfüllbare Beweisverlangen. Insofern sind vorbeugende Löschungsaktionen eine nahe liegende Verlockung, die aber schon wegen der in den USA wesentlich strengeren Beweisvereitelungsvorschriften im Falle eines gerichtlichen Beschlusses („rechtzeitig" – sprich: sofort) gestoppt werden müssen. Wie bereits eingangs ausgeführt, wird oftmals der Bestand an verfügbaren Daten schon vorbeugend zeitabhängig in bestimmten Vernichtungszyklen reduziert, um die Zahl herauszugebender Dokumente zu limitieren.

Eine Gruppe von Rechtsexperten und Beratern hat sich darangesetzt, die Regelungslücken im Bereich der E-Discovery zu schließen und Regeln im Umgang mit der E-Discovery aufzustellen. Diese Fachleute haben sich unter dem Dach der „Sedona Conference" – einer gemeinnützigen Organisation – in verschiedenen Working Groups[41] zusammengetan und einen Leitfaden vorgelegt. Die „Sedona Principles"[42] sollen als „Benchmark" im Umgang mit elektronischen Dokumenten in Beweisermittlungsverfahren dienen und versuchen dabei, z. B. den Begriff der „Angemessenheit" zu bestimmen, denn nach einem Kernsatz amerikanischen Beweisrechts muss eine Partei nur diejenigen Informationen – gleich, ob auf Papier oder in elektronischer Form – herausgeben, die sie nach „angemessener" Prüfung als für die streitige Frage möglicherweise erheblich einstuft. Was bei elektronischen Dokumenten angemessen ist, hängt jedoch sowohl vom Verständnis der elektronischen Technik als auch von der Anwendung des jeweiligen Rechts ab. Ist das Herausgabeverlangen einer Partei unangemessen, kann das Gericht es auf Antrag beschneiden und so den Gegner vor unangemessenen Belastungen und Ausgaben schützen.

Die Auswirkungen der E-Discovery werden auch hierzulande immer stärker spürbar. Die deutsche Justiz verweigert sich zwar zu Recht Ersuchen US-amerikanischer Gerichte nach Durchführung einer pre-trial discovery;[43] zunehmend ist jedoch zu beobachten, dass Unternehmen, welche etwa einem in den USA ansässigen Konzern angehören,[44] bereit sind, solchen Ersuchen auch ohne Einschaltung deutscher Institutionen stattzugeben und die angeforderten Informationen vorzulegen.[45]

V. Dokumentenmanagementprogramm

Die vorstehenden Ausführungen legen es für ein Unternehmen und dessen Rechtsberater nahe, schon bei der Speicherung, aber insbesondere auch für die Löschung von E-Mails Maßnahmen zu ergreifen, die sowohl der technischen Seite und den gesetzlichen Bestimmungen als auch präventiven und reaktiven forensischen Zielen Rechnung tragen. Mit anderen Worten: Die Archivierung und Löschung von Daten, wie z. B. E-Mails, muss professionalisiert, d. h. systematisiert werden. Dieses System wird im Folgenden als DRP („Document Retention Plan", „Dokumentenmanagementprogramm" oder „Records Management") bezeichnet. Ein DRP sollte „good corporate practice" bzw. „best corporate practice" entsprechen. Gerade Firmen, die von einem Prozess betroffen sein können, sollten – nicht nur angesichts der Entwicklung von Prozessen in den USA – ihr System zur Aufbewahrung elektronisch gespeicherter Informationen auch auf die Anforderungen einer E-Discovery hin überprüfen.

In Anbetracht der Komplexität, des Umfangs und der Verbreitung von geschäftlichen Informationen auf elektronischen Übermittlungswegen ist es ein anspruchsvolles Unterfangen, ein DRP zu verwirklichen. Wie dem Verfasser aus der Praxis geläufig ist, wird mit der Aufstellung eines DRP das Ziel angestrebt, den unstrukturierten E-Mail-Verkehr fachlich zu organisieren, archivierungspflichtige bzw. archivierungswürdige E-Mail-Vorgänge ordnungsgemäß zu speichern und gleichzeitig den gesetzlichen und regulatorischen Anforderungen gerecht zu werden. Weitere organisatorische und technische Maßnahmen sind zu treffen, um dem Datenschutz Rechnung zu tragen. Auf dem Markt[46] werden verschiedene E-Mail-Archivlösungen angeboten. Diese müssen eine Unterstützung bei der Einhaltung von Aufbewahrungsfristen bereitstellen und die Unveränderbarkeit von gespeicherten Objekten gewährleisten. Die sachgerechte – automatische oder gezielte – Löschung von Daten ist dabei nur eine von vielen Anforderungen, die an einen DRP gestellt werden.[47] Hier ist jedoch nicht der Ort, in Details zu gehen. DRP ist also ein wichtiges Medium, um in einem Unternehmen Effizienzsteigerungen durchzusetzen. Insofern werden mit einem DRP wesentlich mehr als archivarische Fragen angegangen, die regelmäßig ein größeres Team erfordern.

Allein die Trennung aufbewahrungspflichtiger E-Mails von solchen, die ohne weiteres vernichtet werden dürfen, stellt sich als anspruchsvoll heraus, wie sich am Beispiel von steuerrelevanten E-Mails zeigt. Die Löschung ist natürlich untrennbar mit der Archivierungsmethode verbunden, so dass beide Aspekte gleichzeitig zu lösen sind.

---

40) Beschreibung der wichtigsten Verfahren etwa bei *Gebhardt*, IDR 2005, 30, 31 ff.

41) Der Verfasser ist Mitglied der WG 6, welche sich schwerpunktmäßig mit „International Electronic Information Management, Discovery and Disclosure" beschäftigt.

42) Die „Sedona Principles: Best Practices Recommendation & Principles Addressing Electronic Document Production" sind im Internet zugänglich unter www.thesedonaconference.org. Aus dem Vorstehenden erklärt sich auch, warum die Einführung und Überwachung von Dokumentenmanagementprogrammen in den USA sehr oft auf Prozessrecht spezialisierten Anwälten obliegt.

43) Eine Beweisaufnahme in Deutschland richtet sich nach den Vorschriften des Haager Übereinkommens vom 18. 3. 1970 über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen (HBÜ). Die Bundesrepublik Deutschland hat von der in Art. 23 HBÜ eingeräumten Möglichkeit, einen Vorbehalt zu erklären, Gebrauch gemacht; demgemäß werden auf eine pre-trial discovery of documents gerichtete Rechtshilfeersuchen nicht erledigt. Vgl. hierzu etwa *Kraayvanger/Hilgard*, Die Justiz 2003, 572; *Reufels/Scherer*, IPRax 2005, 456; *Wazlawik*, IPRax 2004, 396; *Bimboese/Reufels*, IDR 2004, 189; *Schütze*, RIW 2004, 162.

44) Hier werden die Daumenschrauben außerhalb Deutschlands angelegt. Hierzu etwa *Klinger*, RIW 2007, 108, 109 f.

45) Die Versuche, US-amerikanische Wertvorstellungen auch in der deutschen Rechts- und Wirtschaftsordnung durchzusetzen, stehen im Zentrum des transatlantischen Justizkonflikts. Hierzu instruktiv *Hess*, AG 2005, 897. Zur US-amerikanischen Beweishilfe bei nicht amerikanischen Verfahren vgl. *Kraayvanger/Richter*, RIW 2007, 177.

46) Enterprise-Content-Management-Markt (ECM-Markt).

47) Es ist ein verbreiteter Irrglaube, dass E-Mails mit einem Klick auf die Delete-Taste auf Nimmerwiedersehen im digitalen Orkus verschwinden: „E-Mails are forever", vgl. etwa den gleichnamigen Artikel im Handelsblatt v. 30. 9. 2005, S. 8.

Gerade bei der Diskussion um steuerrelevante Daten, die entsprechend der AO und den GDPdU in einer Steuerprüfung auswertbar und über die Aufbewahrungsfrist von sechs oder zehn Jahren bereitgestellt werden müssen, spielen E-Mails eine wichtige Rolle. Da die Außenprüfung auf E-Mails mit steuerlich relevantem Inhalt zugreifen darf, sind diese getrennt von nicht steuerrelevanten oder gar privaten E-Mails aufzubewahren. Je nach Unternehmensprofil werden insbesondere datenschutzrechtliche Aspekte eine eindeutige Trennung zwischen prüfungspflichtigen und vom Zugriff auszuschließenden Unternehmensdaten erforderlich machen. Eine fehlende Trennung dürfte dazu führen, dass bei der Suche nach einer bestimmten Mail der gesamte E-Mail-Verkehr, also einschließlich sensibler oder datenschutzrechtlich bedenklicher elektronischer Mitteilungen, einer Prüfung unter Einsatz moderner Suchfunktionen unterzogen werden muss. Eine Separierung empfiehlt sich weiter, um den Aufwand für die gesetzlich vorgeschriebene Archivierung so gering wie möglich zu halten. Ansonsten müssten nämlich auch jene Daten vorgehalten werden, die steuerlich nicht relevant sind.

Die Separierung erfordert, dass der Steuerpflichtige die aufbewahrungspflichtigen Datenbestände im EDV-System zunächst identifiziert. Im Grunde besteht hier kein Unterschied zu steuerlich relevanten Unterlagen in Papierform.[48)]

E-Mails sind insbesondere daraufhin zu prüfen, ob sie Handelsbriefe darstellen. Demgegenüber sind Eröffnungsbilanzen, Jahresabschlüsse und Konzernabschlüsse in analoger Form aufzubewahren, so dass sie sich von vornherein nicht als Inhalt für E-Mails eignen. Zudem muss die Archivierung von E-Mails ggf. in einer Betriebsvereinbarung mit Regeln zum Umgang von privaten und geschäftsrelevanten E-Mails geklärt werden.

Aus dem Vorstehenden ergibt sich als weitere Anforderung an einen DRP, dass eine automatisierte elektronische Archivierung aller Daten zur Durchsetzung oder Abwehr von Ansprüchen vorgenommen wird, und zwar möglichst protokolliert, mit Index und kurzfristigen Zugriff erlaubend. Gleichzeitig muss das Persönlichkeits- und Datenschutzrecht der Mitarbeiter beachtet werden, deren E-Mail-Input und -Output gescannt und archiviert wird.

Selbstverständlich müssen nicht nur allgemeine praktische Bestimmungen beachtet werden, sondern auch die Vielzahl derjenigen Vorschriften, welche spezifisch auf das jeweilige Unternehmen und seine Branche Anwendung finden. Dies kann eine sehr große Herausforderung darstellen. Eine entsprechende betriebliche Policy zum Umgang mit E-Mails muss nicht nur erarbeitet, sondern im Unternehmen dann auch gelebt und ihre Einhaltung kontrolliert werden. Dies bedeutet weit mehr als die deutliche Trennung von Privat- und Geschäfts-Mails.

VI. Resümee

Das Löschen von E-Mails nach Ablauf der gesetzlichen Aufbewahrungsfrist ist nur in Ausnahmefällen – nämlich wenn Dritte ein materielles oder prozessuales Recht daran haben – strafbar.

Die Verwaltung von E-Mails ist eine zunehmend anspruchsvolle und komplexe Aufgabe, insbesondere für Unternehmen, die in mehreren Jurisdiktionen tätig sind. Gerade wenn – oft untereinander nicht vereinbare – Vorschriften verschiedener Länder über Aufbewahrung, Speicherung, Vorlage und Löschung aufeinanderprallen, stellt die Errichtung eines einheitlichen Programms eine außerordentliche Herausforderung dar, die jedoch ganz erhebliche Effizienzsteigerungen verspricht. Letztlich kann das Bestehen eines DRP entscheidend für den Erfolg oder Misserfolg einer E-Discovery sein.

48) Die Filterung steuerlich relevanter E-Mails kann durch die Definition spezifischer technischer Ordnungskriterien, wie etwa „steuerrelevant" und „steuerlich nicht relevant" erleichtert werden.

Thorsten Graeber)/Gerhard Pape**)*

Der Sonderverwalter im Insolvenzverfahren

Die im Gesetz nicht geregelte Figur des Sonderinsolvenzverwalters hat in der letzten Zeit zunehmend an Bedeutung gewonnen. Dies gilt sowohl für Fälle, in denen der bestellte Verwalter verhindert ist, als auch für Verfahren, in denen es darum geht, Ansprüche gegen den amtierenden Verwalter zu verfolgen, der sich einerseits – etwa bei dem Vorwurf, er habe sich eine Verletzung insolvenzspezifischer Pflichten zuschulden kommen lassen – nicht selbst in Anspruch nehmen kann, andererseits aber auch nicht „auf Verdacht" entlassen werden darf. Ziel des nachfolgenden Beitrags ist es, einige der zahlreichen Zweifelsfragen zu klären, die sich um diese Form der Verwaltung ranken.

I. Zulässigkeit der Bestellung eines Sonderinsolvenzverwalters

Die Bestellung eines Sonderverwalters ist in der Insolvenzordnung nicht geregelt. § 77 RegEInsO sah noch eine ausdrückliche Regelung für den Fall der tatsächlichen oder rechtlichen Verhinderung des eigentlichen Verwalters vor. Im weiteren Lauf des Gesetzgebungsverfahrens wurde mit der Erwägung, das Institut der Sonderinsolvenzverwaltung könne wie im bis-

*) *Dr. iur., Richter am AG, Potsdam*
**) *Dr. iur., Richter am OLG, Göttingen*