Max W. Mosing, Die e-mail-Nutzung im Lichte der anwaltlichen Verschwiegenheitspflicht, AnwBl 2001, 440

63. Jahrgang, Heft 9

Österreichisches

ANWALTSBLATT

Organ des Österreichischen Rechtsanwaltskammertages

September 2001

Abhandlungen

Mag. Max W. Mosing, Wien*)

Die e-Mail-Nutzung im Lichte der anwaltlichen Verschwiegenheitspflicht

In der anwaltlichen Praxis ist zumindest für jene Anwälte/innen, deren Kanzlei international ausgerichtet ist, das e-Mail immer mehr zu einem unverzichtbaren Kommunikationsmittel geworden. Nicht selten ist der elektronisch übertragene Postanfall bereits bei weitem umfangreicher als herkömmliche postalische Nachrichten. Die generelle Umstellung auf den elektronischen Rechtsverkehr auch im Umgang mit Behörden und Gerichten („e-Government") wird hier das ihrige zur Beschleunigung diese Prozesses tun. Mit der Verwendung dieser neuen Kommunikationsmittel entstehen aber auch neue Risiken aus rechtlicher und vor allem standesrechtlicher Sicht, die es zu erörtern und zu lösen gilt. Während einerseits grundlegende Interessen der Mandanten zu berücksichtigen sind (Geheimnisschutz, Schutz vor Manipulationen etc), stehen aber auch Standesinteressen (Einfachheit der Kommunikation, Schutz vor ausufernden Haftungsfolgen) zur Diskussion. Die folgende Abhandlung dient als einführende internationale und nationale Darstellung in den Themenkreis und soll eine informierte Diskussion sowie die stärkere Vertretung standrechtlicher Anliegen in dieser Diskussion ermöglichen. Die Basisarbeit für diesen Artikel wurde im Rahmen des postgruadellen Universitätslehrgangs für Informationsrecht und Rechtsinformation geleistet.

Grundsatz jedes anwaltlichen Handelns ist „Eifer, Treue und Gewissenhaftigkeit".[1] „Vornehmste Berufspflicht des Rechtsanwaltes ist die Treue zu seiner Partei."[2] Die Treuepflicht des Rechtsanwaltes wird in § 9 Abs 2 RAO um die Verschwiegenheitspflicht erweitert. Die Verschwiegenheit ist „unabdingbare Voraussetzung für die Ausübung"[3] und grundlegende Pflicht des Rechtsanwaltsberufs.[4] Bei der Euphorie, aber auch den unliebsamen Nebenerscheinungen, die das Internet und seine Dienste in den letzten Jahren mit sich gebracht haben, stellt sich die Frage, welche Konsequenzen die althergebrachten Pflichten auf die Nutzung dieser neuen Techniken haben könnten. Gerade die e-Mail-Nutzung könnte mit einer anwaltlichen Pflicht kollidieren: der Verschwiegenheitspflicht. Die anwaltliche Pflicht zur Verschwiegenheit umfasst nämlich neben dem Mitteilungs- und Verwertungsverbot auch eine aktive Geheimhaltungspflicht.[5] Das Mitteilungs- und Verwertungsverbot untersagt die Weitergabe von Geheimnissen und „Informationsprodukten",[6] wobei der Geheimnisbegriff[7] die allgemeine Unzugänglichkeit der Information,[8] den Geheimhaltungswillen[9] und das objektive Geheimhaltungsinteresse voraussetzt. Aufgrund der aktiven Geheimhaltungspflicht hat der Rechtsanwalt darüber hinaus auch Maßnahmen zu treffen, die verhindern, dass ein unberechtigter Dritter zu Geheimnissen oder Informationsprodukten Zugang erlangt. Bei der anwaltlichen Tätigkeit unterliegen sämtliche schriftliche oder elektronische Aufzeichnungen, aber auch sonstige Mitteilungen im Rahmen der Erfüllung des vom Klienten erteilten Auftrages, dem obgenannten Geheimnisbegriff iVm der Verschwiegenheitspflicht und bilden daher der Geheimhaltungspflicht unterliegende „Informationsprodukte". Somit sind Gegenstand der Berufsverschwiegenheit nach § 9 RAO sämtliche Informationen und Kenntnisse des Rechtsanwaltes über persönliche, betriebliche und wirtschaftliche Angelegenheiten seines Klienten einschließlich der Tatsache, dass eine bestimmte Person oder ein bestimmtes Unternehmen Klient des Anwaltes ist.[10] All diese Informationen darf der Anwalt also nach dem Mitteilungs- und Verwertungsverbot nicht weitergeben und hat sie aufgrund der aktiven Geheimhaltungspflicht gegen Zugriff Dritter zu schützen: sämtliche Unterlagen (Handakte, Terminkalender usw) sind so zu verwahren, dass sie für Unbeteiligte nicht eingesehen werden können.

Übersendet der Rechtsanwalt Nachrichten mittels e-Mail,[11] eine auch unter Anwälten[12] immer beliebtere Kommunikationsform, so hat er sich die Sicherheitsfrage (auch) im Zusammenhang mit der Verschwiegenheitspflicht zu stellen.[13] Der Rat der Anwaltschaften

*) Mag. *Max W. Mosing* ist juristischer Mitarbeiter der Kanzlei Alix Frank Rechtsanwälte KEG.

1) § 9 RAO.

2) § 10 RL-BA.

3) *Feil Erich / Wennig Fritz,* Anwaltsrecht[2] (Linde, Wien 1999) 74.

4) Vgl *Fichtenbauer Peter,* Die Verschwiegenheitspflicht des Rechtsanwaltes als Vertragsverfasser, AnwBl 1993, 69 (69); *Strigl Richard,* Anmerkung zu OBDK 10. 5. 1993, 13 Bkd 4/92 (AnwBl 1994/4615) AnwBl 1994/4615.

5) *Prohaska-Marchried Martin,* Geheimnisschutz berufsmäßiger Parteienvertreter: Berufsgeheimnisse und ihre Anerkennung im Zivilprozess, Strafprozess, Verwaltungsverfahren, Abgabeverfahren, Finanzstrafverfahren und Kartellverfahren der EU-Kommission (Manz, Wien 1998) 27.

6) Vgl *Prohaska-Marchried,* Geheimnisschutz 8.

7) Vgl § 1 DSG, Art 20 Abs 3 B-VG, § 11 UWG, §§ 122 ff, 255 StGB ua.

8) Vgl *Wessely Wolfgang,* Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612 (612); *Bertel Christian / Schweighofer Klaus,* Österreichisches Strafrecht: Besonderer Teil II[4] (Springer, Wien-New York 1999) 243.

9) Vgl OGH 25. 2. 1992, 4 Ob 114/91 EvBl 1992/58 = JBl 1992, 599 = ÖBl 1992, 21 = RdW 1992, 210.

10) Vgl *Prohaska-Marchried,* Geheimnisschutz 31; vgl aber die Möglichkeit der Einwilligung durch den Klienten gem § 45 Abs 3 lit e RL-BA.

11) „Electronic Mail" = „elektronische Briefe".

12) Vgl *Thiele Clemens,* Die Benutzung von E-Mail zur Klientenkommunikation, AnwBl 1999, 634 (634).

13) Vgl *Gassauer-Fleissner Christian,* Geheimhaltung, Offenbarung und Veröffentlichung von Daten in Informationsnetzen, ecolex 1997, 102 (103); *Prohaska-Marchried,* Geheimnisschutz 30 f.

der Europäischen Union (CCBE) hat einen „Guidance for European Lawyers" zum Thema „Electronic Communication and the Internet" veröffentlicht.[14]) Darin wird den Anwälten „empfohlen", keine vertraulichen Informationen in nicht-verschlüsselten e-Mails ohne die ausdrückliche Zustimmung des Klienten zu versenden.

Die US-amerikanische Anwaltsvereinigung (ABA) hat ebenfalls eine Richtlinie zum Thema „Protecting the Confidentiality on Unencryted E-Mail"[15]) herausgegeben, nach der – quasi diametral zur CCBE – unverschlüsselte e-Mails über das Internet nicht den Model Rules of Professional Conduct (1998) widersprechen. Das ABA-Komitee führte in der Begründung aus, dass „[. . .] mail services often reserve the right to inspect the contents of any letters or packages handled by the service"[16]) und schließt daraus, dass bei e-Mails – trotz der auch im Bericht angesprochenen Risken – die Gefahr der nicht genehmigten Zugriffe mit denen des Post- und auch Sprachtelefonverkehrs vergleichbar sei. Für ein weiteres Argument, das als ausschlaggebend für die Entscheidung angeführt wird, wurde nicht auf die technische Sicherheit oder die Praxis abgestellt, sondern rein auf die gesetzlichen Verbote der unberechtigten Zugriffe,[17]) die in den USA für Briefe und auch für e-Mails bestehen.[18]) Aus dem gesetzlichen Verbot wurde vom ABA-Komitee auf eine allgemeines Vertrauen in die Verschwiegenheit/Privatheit („expectation of privacy") geschlossen. Auch wenn es, wie auch das ABA-Komitee feststellte, tatsächliche Gefahren des unberechtigten Zugriffs gibt, verhindert dieses Vertrauen, dass der Anwalt einen Bruch seiner Verschwiegenheitspflicht begeht.

Es wurde – allerdings vor der Veröffentlichung des CCBE-Guidance – die Meinung vertreten, dass die ABA-RL auch die Lage in Ö darstelle.[19]) Um dies zu prüfen, hat man den Grundgedanken des ABA-Komitees auf die Rechtslage in Ö anzuwenden; das Komitee ging davon aus, dass wenn die e-Mail(-Übertragung) grundsätzlich gesetzlichen Schutz genießt, eine „expectation of privacy" gegeben sei und daher die Nutzung des e-Mail-Verkehrs kein Verstoß gegen die Verschwiegenheitspflicht darstelle. Ob die e-Mail-Nutzung demnach eine Verletzung der Verschwiegenheitspflicht darstellt, hängt – wenn man der Argumentation der ABA-Kommission folgt – davon ab, ob und welchen Schutz die e-Mail-(Übertragung) in Ö genießt.

Die e-Mail ist aufgrund ihrer Textlichkeit[20]) und ihrer Übertragung über Telekommunikationsinfrastruktur ein juristisches „Doppelgeschöpf". Es sind sowohl Elemente des gesetzlichen Terminus „Brief" als auch Elemente des „Fernmeldevorganges" vorhanden. Aufgrund der sich daraus ergebenden Unklarheit bei der rechtlichen Zuordnung, aber mE auch aufgrund „technischer Überlegungen", wurde vielfach davon ausgegangen, dass e-Mails ein „verwundbares Medium" und leichter zugänglich seien, als verschlossene Briefe,[21]) teilweise wurde sogar das Gleichnis zur Postkarte gezogen. Konsequenterweise wurde daraus gefolgert, dass der Schutz, der Briefen zukommt, zB § 118 StGB,[22]) auf e-Mails nicht anwendbar sei, da es sich hiebei eben nicht um „verschlossene Schriftstücke" handelt.[23]) Auf die Elemente des Fernmeldevorganges abstellend wurde in Analogie zum Fernschreiber und Telefax für die e-Mail nur § 119 StGB für anwendbar erachtet. Damit wäre nur jene e-Mail, die im Internet (ab dem Modem)[24]) unterwegs ist – nach § 119 StGB – geschützt. Dem ist mE nicht undifferenziert zu folgen.[25]) Wie *Lunzer* in seiner Arbeit bewies, sind (passwortgesicherte) e-Mails als „elektronische Kuverte" durchaus als verschlossene Schriftstücke zu qualifizieren und unterliegen somit auch dem Briefgeheimnis nach § 118 StGB.[26]) Dem ist mE zu folgen, da es –

14) Council of the bars and law societies of the European Union (CCBE), electronic communication and the internet, zitiert 25. 7. 2001, http://www.ccbe.org/uk/load/commeluk.pdf.

15) *American Bar Association,* Standing Committee on ethics and professional responsibility, Formal Opinion No 99–143 (March 10, 1999): Protecting the Confidentiality on Unencryted E-Mail, Chicago, zitiert: 25. 7. 2001, http://www.abanet.org/cpr/fo99-413.html. Vgl zur geplanten Änderung der amerikanischen Standesrechtsrichtlinien: www.abanet.org/journal/ju/01/fbroke.html, zitiert 26. 7. 2001.

16) *American Bar Association,* zitiert: 25. 7. 2001, http://www.abanet.org/cpr/fo99-413.html.

17) „The fact that ISP administrators or hackers are capable of intercepting Internet e-mails – . . . in violation of federal law – should not render the expectation of privacy in this medium . . ." *American Bar Association,* zitiert: 25. 7. 2001, http://www.abanet.org/cpr/fo99-413.html.

18) The Electronic Communications Privacy Act, zitiert 25. 7. 2001, http://floridalawfirm.com/privacy.html.

19) So *Thiele,* AnwBl 1999, 634.

20) Vgl die Diskussion um die Einführung der Textlichkeit neben der Schriftlichkeit in § 126 Abs 3 BGB.

21) *Gassauer-Fleissner,* ecolex 1997, 102; *Wagner Raoul G.,* Unbefugter Zugriff auf e-mail, ecolex 2000, 273 (273).

22) Art 10 StGG iVm Art 149 B-VG; Art 8 EMRK; § 118 StGB; § 77 UrhG.

23) *Wessely,* ÖJZ 1996, 612 (sich mE unverständlich berufend auf *Schmölzer Gabriele,* Prozessuale Zwangsmittel im Fernmeldewesen – Beschlagnahme oder Überwachung? RZ 1988, 247); *Wagner,* ecolex 2000, 273.

24) Kunstwort aus MOdulator und DEModulator: *Grömmer Walter Michael,* Fragen der EDV-Ausstattung bei Rechtsanwälten und Notaren, EDVuR 1988 H 2, 12.

25) *Lunzer Harald,* Electronic mail und Geheimnisschutz: Prozessuale und materiellrechtliche Fragestellungen (DiplArb, Graz 1998) 13ff; *Prohaska-Marchried,* Geheimnisschutz 12f; unklar: *Gassauer-Fleissner,* ecolex 1997, 102.

26) *Lunzer,* Electronic mail 31ff.

wie unten noch darzustellen sein wird – keinen sachlich gerechtfertigten Grund für die Differenzierung zwischen passwortgeschützter e-Mail und dem Brief gibt – auch was den strafrechtlichen Schutz betrifft. § 118 StGB tritt daher, um auch eine Besserstellung hintanzuhalten, beim Eingriff während der Übertragung hinter § 119 StGB zurück.

Auch für die Beurteilung auf standesrechtlicher Ebene und der Sicherheit der Verschwiegenheit ist herauszuarbeiten, ob eine sachliche Rechtfertigung für eine Differenzierung gegeben sein könnte. Hierfür sind wohl auch zuerst die technischen und erst dann die juristischen Gesichtspunkte heranzuziehen:[27] Die Konzeption des Internets lässt das Abfangen und Lesen von fremden Daten(paketen) zu. Mit Know-How und krimineller Energie lassen sich auch *bestimmte* e-Mails ausfindig machen.[28] Das gezielte Abfangen von Nachrichten und das leichte Verwischen von Spuren in der „virtuellen Welt" werden als Sicherheitsmängel bewertet, weshalb die Meinung vertreten wird, dass die „Einhaltung der anwaltlichen Verschwiegenheitspflicht, [. . .] nicht gewährleistet werden kann, [. . .]"[29] und dass „[d]as unverschlüsselte Versenden von Dokumenten [. . .] einen schuldhaften Verstoß gegen die anwaltliche Verschwiegenheitspflicht darstellen [kann]."[30] Für die Übertragung der e-Mails innerhalb des Internets wird das Simple-Mail-Transfer-Protocol (SMTP) verwendet. Aus der Geschichte des Internets ergibt sich, dass bei der Konzeption relativ wenig auf „privacy" geachtet wurde; daher wird SMTP heute von einigen als nicht sicher im Sinne der Geheimhaltung beurteilt.[31] SMTP zerteilt die Information (e-Mail) in kleine Pakete und übermittelt diese Pakete auf durchaus unterschiedlichen Wegen (unterschiedlichen Leitungen, Switches und Servern) vom Absender zum Empfänger. ME kann dieses Protokoll daher prinzipiell als *nicht unsicher beurteilt* werden. Der Ansicht, dass diese Übertragung *nicht völlig sicher ist,* ist aber trotzdem ohne Zweifel zu folgen. Es gibt nämlich durchaus die Möglichkeit die Pakete gezielt umzuleiten, sodass man als Dritter alle Pakete empfangen und die Information lesen kann (packet-sniffing). Für die Frage der Verschwiegenheitsbruches bedarf es allerdings eines direkten Vergleichs zwischen den technischen Gefahren der e-Mail-Nutzung und jenen der „snail-mail", wie die Post von Internet-Usern genannt wird. ME kann nur dann juristisch beurteilt werden, ob eine unterschiedliche Behandlung von Post- und e-Mail-Verkehr sachlich gerechtfertigt ist. Wer als Anwalt vertrauliche Mitteilungen auf einer Postkarte oder in einem offenen Kuvert verschickt, dem ist wohl eine Verletzung der Verschwiegenheitspflicht vorzuwerfen.[32] Es stellt sich daher die Frage, ob die e-Mail einer Postkarte oder einem offenen Kuvert, die beide übrigens nicht den Schutz des § 118 StGB genießen, entspricht. E-Mails sind am Server – aufgrund des Passwortschutzes der beiden Abruf-Protokolle POP3 und IMAP, als auch auf dem Übertragungsweg durch die Zerteilung in Pakete – durchaus mit dem kuvertierten und verklebten Brief vergleichbar.[33] Der Brief im verklebten Kuvert erfüllt ohne Zweifel die aktive Geheimhaltungspflicht des Rechtsanwaltes. Es sollen nun die Möglichkeiten der missbräuchlichen Kenntnisnahme der Informationen auf dem Postweg und dem Weg über das Internet erkannt und iSd Verschwiegenheitspflicht bewertet werden. Für den Außenstehenden bedarf es bei der Übertragung mittels der Post des „Einbruches" in einen Postkasten (§ 118 (2) Z 1 StGB) oder der Mitwirkung eines Postbediensteten, um an die übersendete Nachricht zu gelangen. Im Internet bedarf es ähnlicher Methoden, nämlich des „Einbruchs" in die e-Mail-Box[34] oder der Mitwirkung eines an der e-Mail-Übertragung Beteiligten. Um Einblick in die e-Mail-Box eines anderen zu erhalten, benötigt man entweder den Usernamen und das Passwort des e-Mail-Box-Inhabers oder hat – wie der Provider – Administratoren-Rechte auf dem Server, auf dem die e-Mail-Box liegt.[35] Ersteres kann durch „Ausspähen" geschehen und ist in der Praxis noch immer sehr einfach, da es nach wie vor beliebt ist, Passwörter auf gelben Zetteln neben den Bildschirm oder unter die Tastatur zu kleben. Technisch bietet sich die Möglichkeit – allerdings mit einigem Know-How – die Passwörter bei der Abfrage eines anderen im Internet „mitzuschreiben". Beim Abrufen werden nämlich die User- und Passwortdaten im plain-text (also lesbar und unverschlüsselt) vom Computer des Nutzers zu seiner e-Mail-Box gesendet. Werden nun solche Informationen zB mittels „packet-sniffing" abgefangen (Strafbarkeit nach § 119 StGB), kann aufgrund der so erlangten Daten, wie der rechtmäßige e-Mail-Box-Inhaber auf die e-Mails zugegriffen werden. Greift jemand unter Mithilfe des Providers, der ja als Administrator die Rechte hierfür hätte, direkt auf die e-Mail-Box zu, so bedient er sich gleichsam des „Postbediensteten des Internets". Dass sowohl der Postbedienstete als auch der Provider relativ leicht die Möglichkeit haben, auf die übermittelten Informationen zuzugreifen, wird man nicht bestreiten können. Die Beteiligten machen sich im Falle des Postbediensteten gem § 3 PostG iVm § 30 PostG und uU § 118 StGB, im Falle des Providers nach § 88 TKG und uU § 118 StGB strafbar. Die Strafbarkeit allein genügt allerdings mE – entgegen der Ansicht des ABA-Komi-

27) Vgl *Gassauer-Fleissner,* ecolex 1997, 103.

28) *Sagawe/Klages* zitiert 20. 12. 2000, http://www.tyskret.com/deutsch/internet/sicher9.shtml.; *Gassauer-Fleissner,* ecolex 1997, 103.

29) *Thiele,* Anwaltliche Werbung im Internet, AnwBl 1999, 402 (402); vgl aber *ders,* AnwBl 1999, 634; *Mayer-Schönberger Viktor / Pilz Michael,* E-Commerce: Rechtliche Rahmenbedingungen und Notwendigkeiten, AnwBl 1999, 217 (217).

30) *Thiele,* AnwBl 1998, 670; vgl aber *ders,* AnwBl 1999, 634.

31) *Sagawe/Klages,* zitiert 20. 12. 2000, http://www.tyskret.com/deutsch/internet/sicher9.shtml.; *Gassauer-Fleissner,* ecolex 1997, 103; *Thiele,* AnwBl 1998, 670; vgl aber *ders,* AnwBl 1999, 634; aA *Lunzer,* Electronic mail 31.

32) Vgl *Gassauer-Fleissner,* ecolex 1997, 103.

33) *Lunzer,* Electronic mail 31 ff.

34) Speicherplatz auf einem Server, in dem e-Mails gespeichert werden und dessen Inhalt mittels POP3 oder IMAP abgefragt werden kann.

35) Auf die Darstellung des echten „packet-sniffing" kann aufgrund der geringen praktischen Relevanz an dieser Stelle verzichtet werden.

tees – alleine noch nicht aus, um von einer „expectation of privacy" auszugehen, da es mE aufgrund der in Ö geltenden aktiven Geheimhaltungspflicht vielmehr auf die tatsächlichen Umstände ankommt: § 88 Abs 4 TKG stellt die Verwertung und Weitergabe von Informationen, die nicht für den tatsächlichen Empfänger bestimmt waren, unter Strafe. Diese Norm würde – nach dem ABA-Gedanken – auch eine „expectation of privacy" bedeuten, wenn der Anwalt falsche e-Mail-Adressen verwendet oder Adressen verwechselt und so Mitteilung statt an den Klienten an den Gegner übermittelt.[36]) Diese Norm will aber sich nicht den „schlampigen" Übermittler schützen, sondern stellt auf technische Übermittlungsfehler ab. Der gesetzliche Schutz verhindert also nicht immer den Bruch der aktiven Geheimhaltungspflicht.

Das „Gebot" der CCBE „confidential information" nicht in unverschlüsselten e-Mails zu versenden, hätte in der Praxis eine enorme Diskriminierung der e-Mail-Kommunikation zur Folge: Anwälte hätten jegliche Daten, die seinen Klienten betreffen, nur verschlüsselt zu versenden, wozu sie erstens mit dem Korrespondenz-Partner ein Verschlüsselungsverfahren (Kryptographie-Verfahren)[37]) vereinbaren müssten und zweitens die entsprechende Kryptographie-Software benötigen würden. Es stellt sich aber vorher noch die gar nicht triviale Frage, ob solche Verfahren überhaupt gesetzlich zulässig sind. In Ö gibt es, im Gegensatz zu anderen Staaten,[38]) kein Verbot von Kryptographiesoftware im Zusammenhang mit e-Mail-Korrespondenz: sie ist also prinzipiell rechtlich frei einsetzbar.[39]) Praktisches Hindernis beim Einsatz von e-Mail-Kryptographie ist die Voraussetzung des Vorhandenseins von kompatibler Software[40]) beim Anwalt und beim Klienten. Es ist zwar für die nichtkommerzielle Nutzung auch Kryptographie-Freeware (also kostenlose Software) erhältlich, doch meist ergibt sich daraus ein nicht unbeträchtlicher Arbeits- und auch Kostenaufwand, den nicht jeder Klient auf sich nehmen will.

Neben obgenannten Problemen stellt sich nach wie vor die Frage der sachlichen Rechtfertigung der – von der CCBE empfohlenen – unterschiedlichen Behandlung von e-Mail und Snail-Mail. Nach obiger Darstellung (einiger) Möglichkeiten, im Internet an e-Mail-Inhalte zu gelangen, stellt sich mE aufgrund der technischen Voraussetzungen, die hierfür erforderlich sind, kein größeres Risiko dar, als beim „normalen" Post-Versand. In beiden Fällen ist mit krimineller Energie der Inhalt mit ähnlichem Aufwand zugänglich, weshalb es mE nicht gerechtfertigt wäre, den e-Mail-Verkehr durch die Verschlüsselungspflicht zu diskriminieren. Dieser Meinung ist ganz offensichtlich auch der österreichische Gesetzgeber, der in § 112 ZPO wie selbstverständlich die e-Mail neben den Boten, die Post und das Telefax als zulässige Übermittlungsform bei der Gleichschriftübermittlung zwischen den Anwälten zulässt.[41]) Gerade in e-Mails mit Gleichschriften können – im Lichte der anwaltlichen Verschwiegenheit – sehr vertrauliche Informationen enthalten sein. Trotzdem verlangt der Gesetzgeber keine besondere Qualität der e-Mails, obwohl sich diese Norm ausschließlich an Rechtsanwälte wendet und beim In-Kraft-Treten des § 112 ZPO[42]) das SigG schon in Kraft war und daher kryptographische Verfahren „gesetzesbekannt" waren. Dies spricht dafür, dass der Gesetzgeber keine Diskriminierung der e-Mails wünscht. Zwar kann diese Regelungen nicht unmittelbar auf standesrechtliche Pflichten wirken, doch sind sie mE bei der Konkretisierung der Pflichten durchaus heranzuziehen. Da somit die Verschwiegenheitspflicht bei der Übermittlung von Gleichschriften mittels e-Mail gewahrt zu sein scheint, können mE gleichartige Informationen auch gegenüber anderen e-Mail-Nutzern unverschlüsselt übermittelt werden.

Als Zwischenergebnis ist also festzuhalten, dass Daten – selbst Gleichschriften – auch per e-Mail übertragbar sind, ohne dass diese Tatsache einen Bruch der Verschwiegenheitspflicht darstellt. Doch was gilt für die Übermittlung von Informationen, die aufgrund des Geheimhaltungsinteresses nicht in Eingaben – und damit auch nicht in § 112 ZPO-e-Mails – verwendet würden. Es handelt sich dabei um solche Daten, bei denen selbst die ABA von dem Vertrauen auf die Sicherheit der e-Mail-Kommunikation abrückt: „A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation." Diese Informationen bedürfen also eines noch größeren Schutzes bei der Übermittlung.

36) Vgl OBKD 10. 5. 1993, 13 Bkd 4/92, AnwBl 1994/4615 *(Strigl)*.

37) „Verschlüsselung"; „Chiffrierung": vgl *Lago Gerhard*, Rechtsprobleme im Internet (Wirtschaftskammer Österreich, 1998) 142ff; vgl *Mayer-Schönberger/Pilz*, AnwBl 1999, 217.

38) Vgl USA und Diskussion in F: vgl *Mayer-Schönberger/Pilz*, AnwBl 1999, 218.

39) *Lago*, Rechtsprobleme 155; vgl aber § 42b RL-BA.

40) Stellvertretend die Freeware „Pretty Good Privacy – PGP" zum Downloaden unter http://www.pgp.com/products/freeware/default.asp, zitiert 25. 7. 2001.

41) Vgl *Popp Friedrich*, Die neue „Zustellung" zwischen Rechtsanwälten im Zivilprozess, RdW 2000/501; zur Problematik der Unterschrift und Übertragungsfehler: *Konecny Andreas*, Direktübersendung von Gleichschriften im Konkursverfahren, ZIK 2000/245; noch vor Einführung des § 112 ZPO das Problem erkennend: *Thiele*, Form- und Fristenwahrung durch elektronische Übermittlung einer Textdatei? MR 1999, 7 (8).

42) Gem BGBl I 2000/26: § 112 ZPO seit 1. 6. 2000 in Kraft.

Abhandlungen

Die Post bietet hierfür die Übermittlung per eingeschriebenem Brief an. Dies verhindert de facto die Möglichkeit des Einbruches in den Briefkasten und bringt eine Bestätigung der Versendung und beim Postbediensteten eine Bestätigung der Übergabe mit sich. Bei sehr vertraulichen Informationen wird man annehmen dürfen, dass der Anwalt diese „eingeschrieben" übermittelt – möglicherweise gebietet das sogar das Standesrecht. Sollte dem so sein, würde das Internet sogar eine sicherere Methode anbieten, nämlich obgenannte Kryptographie-Verfahren. Hier ist es (nahezu) ausschließlich den beiden Kommunikations-Parteien möglich, die Informationen zur Kenntnis zu nehmen. Ohne jetzt näher auf den technischen Hintergrund der asymmetrischen Verschlüsselung eingehen zu wollen, verwendet der Nutzer beim Verschlüsseln mit dem „de-facto-Standard"[43] Pretty Good Privacy (PGP) und dem S/MIME-Verfahren faktisch jenes Verfahren, das im SigG geregelt ist, nur in die entgegengesetzte Richtung. Es ergibt sich allerdings aus dem SigG iVm § 3 Abs 4 Signaturverordnung, dass die Signaturerstellungsdaten nicht für die Nachrichtenverschlüsselung eingesetzt werden dürfen. Es dürfen also die Daten, mit denen die digitale Signatur erstellt und überprüft wird, nicht dazu verwendet werden, um die Nachricht selbst zu ver- bzw zu entschlüsseln; es sind also in diesem Fall zwei unabhängige Schlüsselpaare erforderlich. Dies macht die praktische Anwendbarkeit auch nicht unbedingt leichter. Sollte eine standesrechtliche Verpflichtung zur Übermittlung mittels eingeschriebenem Brief für solch vertrauliche Informationen bestehen, wäre die e-Mail iVm Kryptographie zumindest gleichwertig. Der Klient könnte allerdings in die Übermittlung per nicht eingeschriebenem Brief, wie auch in den e-Mail-Verkehr ohne Kryptographie einwilligen.[44] Beim Geheimnis handelt es sich – vgl auch § 1 DSG – um ein disponibles Rechtsgut[45] und der Klient kann somit in die etwaige Verletzung rechtmäßig einwilligen.[46] Ob die Einwilligung, die strafrechtlich und zivilrechtlich tatbestandsausschließend[47] oder zumindest als Rechtfertigungsgrund[48] verstanden wird, auch die mögliche Verletzung des Standesrechtes rechtfertigt, ist mE durchaus zu bejahen, obwohl die Standespflicht „[. . .] auf einer ganz anderen Ebene wie die [. . .] Verpflichtung aus dem Vertragsverhältnis zum Klienten"[49] liegt.[50]

Besondere Bedeutung erhält allerdings der CCBE-Guidance durch die e-Commerce-Richtlinie,[51] die in ihrem Artikel 8 Abs 2 die Mitgliedstaaten und die Kommission anhält, die Berufsvereinigungen und -organisationen zu ermutigen, Verhaltenskodizes auf Gemeinschaftsebene aufzustellen. Diese Verhaltenskodizes sollen die (standesrechtlichen) Regeln für die kommerzielle Kommunikation der „reglementierten Berufe" (im E-Commerce-Gesetz [ECG] „Angehörige geregelter Berufe")[52] europaweit möglichst einheitlich festlegen. Der CCBE-Guidance würde an sich auch nicht dem ECG und auch nicht der e-Commerce-RL widersprechen: Das ECG bezieht für geregelte Berufe die grundsätzliche Zulässigkeit nur auf Werbung und andere Maßnahmen zur Absatzförderung, worunter wohl nicht der eigentliche e-mail-Verkehr zu verstehen ist. Die e-Commerce-RL spricht zwar von der Erlaubnis für reglementierte Berufe kommerzielle Kommunikation als Teil eines Dienstes der Informationsgesellschaft einzusetzen, aber nur unter der Bedingung, dass die berufsrechtlichen Regeln eingehalten werden. Die Verpflichtung zum Einsatz von Verschlüsselungsprogrammen könnte daher – wohl unbeabsichtigt – durch die e-Commerce-RL bestärkt werden.

Zusammenfassend ist mE eine Pflicht zum Einsatz von Kryptographie beim e-Mail-Verkehr im Lichte der anwaltlichen Verschwiegenheit nicht gegeben. Es mangelt an der sachlichen Rechtfertigung für eine Diskriminierung des e-Mail-Verkehrs. Die CCBE-Empfehlung „electonic communication in the Internet" ist im Zusammenhang mit der e-Mail-Kommunikation jedenfalls zu eng und wohl auch nicht ganz praxisnah.

Dem Gedanken der American Bar Association ist mE – bis auf die Verallgemeinerung, dass gesetzlicher Schutz automatisch eine „expectation of privacy" nach sich zieht – wohl zu folgen: Solange es sich nicht um Daten mit sehr hohem Geheimhaltungsinteresse handelt, ist keine Verschlüsselung der Nachrichten verpflichtend, um die Verschwiegenheitspflicht zu wahren. Selbst bei Daten mit sehr hohem Geheimhaltungsinteresse steht es dem Klienten frei, in jegliche Form der Kommunikation einzuwilligen.

Der CCBE-Guidance könnte allerdings aufgrund der e-Commerce-RL an Bedeutung gewinnen: Die Bestärkung zu europaweiten standesrechtlichen Regelungen durch die EU-Staaten und die Kommission könnten bewirken, dass der Guidance als verbindlich anerkannt wird. Dies wäre mE nicht nur sachlich nicht gerechtfertigt, sondern würde auch den e-Mail-Einsatz beim Rechtsanwalt faktisch zum Erliegen bringen.

43) *Telekom Control*, FAQ, zitiert 26. 2. 2001, http://www.signatur.tkc.at/de/security/faq300.html.

44) Nicht als „Verzicht" zu verstehen: vgl *Resch Reinhard*, Die Einwilligung des Geschädigten (Manz, Wien 1997); vgl *Hinterhofer Hubert*, Die Einwilligung im Strafrecht (WUV, Wien 1998); vgl auch Empfehlung des Rat der Anwaltschaften der Europäischen Union (CCBE), Electronic Communication and The Internet: Guidance for European Lawyers, zitiert 25. 7. 2001, http://www.ccbe.org/uk/load/commeluk.pdf.

45) Vgl strafrechtlich: *Hinterhofer*, Einwilligung 23ff; *Fuchs*, AT[4], 119f; *Kienapfel/Höpfel*, AT[4], 20; vgl zivilrechtlich: *Resch*, Einwilligung 77ff.

46) Vgl *Feil/Wennig*, Anwaltsrecht[2], 74.

47) *Hinterhofer*, Einwilligung, 11; *Koziol*, Haftpflichtrecht I[3], 182.

48) *Hinterhofer*, Einwilligung, 11; *Foregger/Fabrizy*, Strafgesetzbuch[6], 291; *Fuchs*, AT[4], 116ff; *Kienapfel/Höpfel*, AT[4],17, 69; zivilrechtlich: *Welser* in *Koziol/Welser*, Grundriss[11] II 286.

49) *Feil/Wennig*, Anwaltsrecht[2], 47.

50) Vgl allerdings OBDK 24. 1. 1994, Bkd 65/90 AnwBl 1994/4831 *(Strigl)*; vgl auch *Prohaska-Marchried*, Geheimnisschutz 34f.

51) RL 2000/31/EG des Europäischen Parlaments und Rates vom 8. 6. 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr").

52) Zu Redaktionsschluss als Entwurf: http://www.bmj.gv.at/gesetzes/download/ecommerce.pdf, zitiert 25. 7. 2001.