UNIVERSITÄTSLEHRGANG FÜR INFORMATIONSRECHT UND RECHTSINFORMATION - RECHTSWISSENSCHAFTLICHE FAKULTÄT WIEN

BRIEFGEHEIMNIS IM STRAFRECHT UND e-MAIL IN Ö UND D
EIN MICROVERGLEICH

Lehrveranstaltung bei
Prof.DrThomas Hoeren

Max W. MOSING
Wien, Juni 2001

I. Das Briefgeheimnis in Ö aus historischer, verfassungsrechtlicher Sicht

Der Begriff des Briefgeheimnisses tauchte erstmals 1848 in der Pillersdorf´schen Verfassung (§ 20) auf, wobei darin keine Definition vorgenommen wurde[1]. Programmatisch festgehalten wurde: „Das Briefgeheimnis ist unverletzlich"! Im Dezember 1867 wurde das Staatsgrundgesetz vom Reichsrat beschlossen. Der Art 10 StGG bestimmt, dass das „Briefgeheimnis nicht verletzt" werden darf.

1958 trat die Konvention zum Schutze der Menschenrechte und Grundfreiheiten in Österreich in Kraft[2], und damit der Art 8 MRK. Dieser normiert die „Achtung des Briefverkehrs".

II. „Elektronischer Brief" (e-Mail) und Briefgeheimnis im ö Strafrecht (§ 118 StGB)

Fünfter Abschnitt
Verletzungen der Privatsphäre und bestimmter Berufsgeheimnisse
Verletzung des Briefgeheimnisses und Unterdrückung von Briefen

§ 118 StGB. (1) Wer einen nicht zu seiner Kenntnisnahme bestimmten verschlossenen Brief oder ein anderes solches Schriftstück öffnet, ist mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(2) Ebenso ist zu bestrafen, wer, um sich oder einem anderen Unbefugten Kenntnis vom Inhalt eines nicht zu seiner Kenntnisnahme bestimmten Schriftstücks zu verschaffen,

1. ein verschlossenes Behältnis, in dem sich ein solches Schriftstück befindet, öffnet oder
2. ein technisches Mittel anwendet, um seinen Zweck ohne Öffnen des Verschlusses des Schriftstücks oder des Behältnisses (Z. 1) zu erreichen.

(3) Ebenso ist zu bestrafen, wer einen Brief oder ein anderes Schriftstück (Abs. 1) vor Kenntnisnahme durch den Empfänger unterschlägt oder sonst unterdrückt.

(4) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen. Wird die Tat jedoch von einem Beamten in Ausübung seines Amtes oder unter Ausnützung der ihm durch seine Amtstätigkeit gebotenen Gelegenheit begangen, so hat der öffentliche Ankläger den Täter mit Ermächtigung des Verletzten zu verfolgen.

Brief und Schriftstück

Tatobjekt des § 118 StGB ist entweder ein „verschlossener Brief" oder ein „anderes solches Schriftstück". Unterschiede bestehen nur in der äußeren Form[3] und in der

[1] *Laurer*, Der Geheimnisschutz im österreichischen Grundrechtssystem, EuGRZ 1983, 29.

[2] BGBl 1958/210.

[3] *Mayerhofer/Rieder*, Das österreichische Strafrecht , I.Teil, Strafgesetzbuch[4], Band XI, Rz 2 zu § 118.

Kommunikationsabsicht[4], die beim Brief noch hinzukommt. Dieser Unterscheidung kommt in der Praxis keine große Bedeutung zu, allerdings sollte eigentlich im Zusammenhang mit § 118 StGB nicht nur vom „Briefgeheimnis“ sondern eigentlich vom „Schriftengeheimnis“ gesprochen werden, da dies wohl der Oberbegriff sein dürfte.

Begriff: „Brief“

Definiert wird der Brief, beziehungsweise ein Schriftstück, nach dem allgemeinen Sprachgebrauch[5]: Voraussetzung ist jedenfalls ein gedanklicher Inhalt, der in schriftlicher Form vorliegt. Bei einem gedanklichen Inhalt muss es sich nicht um ein Geheimnis in dem Sinn handeln, dass der Inhalt keinem Dritten bekannt werden soll, sondern es müssen begriffsnotwendig ein Absender und ein Empfänger vorhanden sein. Jene, zu deren Kenntnisnahme der Brief bestimmt ist, können natürlich nicht Täter im Sinn des § 118 StGB sein.

Beim Kriterium der Schriftlichkeit bietet sich als Interpretationshilfe jene Umschreibung, die beim Urkundenbegriff verwendet wird: „Schrift sind nach hM alle Zeichen, die dazu bestimmt sind, einen beliebigen Gedankeninhalt für andere lesbar zu machen. Schrift setzt somit grundsätzlich die Verwendung von Buchstaben und/oder Zahlen voraus.[...] Im Regelfall wird die schriftliche Erklärung auf Papier, Karton, Pergament oder ähnlichem angebracht sein; als Unterlage kommen aber auch andere Materialien in Betracht, wie Stoffe, Holz oder Metall. Ohne Bedeutung ist schließlich auch das verwendete Schreibmaterial; allerdings muß die Verkörperung des Gedankeninhalts von einiger Dauerhaftigkeit sein.“[6] Vergleicht man diese Definition mit dem technischen Vorgang bei den e-Mails erkennt man, dass durch das Laden der e-Mail kann ein Gedankeninhalt für den Empfänger lesbar gemacht werden. Dieser Inhalt wird mittels Buchstaben vermittelt. Auch das Erfordernis der Dauerhaftigkeit ist ebenso gegeben wie bei einem herkömmlichen Brief: Dieser wird geöffnet und nach dem Lesen entweder weiter aufbewahrt oder entsorgt. Die e-Mail wird auf den Bildschirm geholt, gelesen und danach entweder gelöscht oder in der Form eines Ausdruckes bzw. eines Datenträgers archiviert.[7]

---

[4] *Leukauf/Steininger*, Kommentar zum Strafgesetzbuch[3], Rz 4 zu § 118.

[5] *Foregger/Kodek*, StGB, MKK[7], Anm II zu § 118.

[6] *Leukauf/Steininger*, Kommentar zum StGB[3], Rz 8, 10 zu § 223.

[7] *Schmölzer*, Computer-Netzwerke und Strafrecht - eine internationale Herausforderung, in: *Terlitza/Schwarzenegger/Boric (Hrsg)*, Die internationale Dimension des Rechts, FS-Posch, Wien 1996, 334; *dies*, Strafrechtliche Aspekte zu Thema Rassismus, Neonazismus und Rechtsextremismus im Internet, in: *Stiftung Dokumentationsarchiv des österreichischen Widerstandes (Hrsg)*, Netz des Hasses, Wien 1997, 259.

Wie die Art der Übermittlung aussehen darf, ist nicht unumstritten: *Wessely* ist der Meinung, dass e-Mail vom Briefbegriff nicht erfasst seien, da die Übertragung über Datenleitungen und nicht auf Papier erfolgt.[8] *Leukauf/Steininger*[9] und *Mayerhofer/Rieder*[10] sehen hingegen keine besondere Art der Übermittlung als vom Briefbegriff zwingend vorgegeben.

Das Briefgeheimnis ist strafrechtlich nicht als solches geschützt, sondern immer nur in Abhängigkeit von einer Verschluss- oder Verwahrungsform.[11] Der Zustand des Verschlossenseins ist im Zusammenhang mit dem Öffnen zu sehen. Erst durch dieses Öffnen wird die Kenntnisnahme möglich – davor soll geschützt werden. Zu beachten ist, dass das Öffnen und nicht die Kenntnisnahme des Schriftstückes von § 118 StGB umfasst ist und pönalisiert wird. Verschlossen ist ein Schriftstück, sofern dem Eindringen ein Hindernis entgegengesetzt ist.[12] Es soll einem Dritten zumindest erschwert werden, Kenntnis zu erlangen. Dies ist wohl bei der e-Mail gegeben, da man jedenfalls ein gewisses Maß an technischem Wissen sowie meist einige Hardwarekomponenten als „Werkzeug" für dieses Eindringen benötigt, wenn die e-Mail auf dem Empfänger- oder Senderrechner liegt und gar mit einem Passwort geschützt ist. Der Brief ist zum Schutz des unbefugten Lesens verklebt. Jedermann, der sich Zugang zu diesem Brief verschaffen kann, schafft es wohl auch diesen zu öffnen – möglicherweise auch so, dass der Zugriff nicht erkannt werden kann. So wie ein gedanklicher Inhalt zu Papier gebracht und dieser in einem Kuvert verschlossen wird, so wird die e-Mail elektronisch erzeugt und in ein „elektronisches Kuvert" verpackt.[13] Dieses besteht nicht aus einem physischen Schutzumschlag und kann demnach auch nicht mechanisch aufgebrochen werden. Es wäre wohl zu eng, eine derartige Substanzverletzung für „das Öffnen" zu verlangen. § 118 StGB nennt als Objekt den „verschlossenen Brief". Diesem Erfordernis wird die codegesicherte e-Mail gerecht. Nicht nötig ist für eine verschlossene e-Mail, dass sie verschlüsselt ist. Genausowenig, wie man für ein Umhüllen einer Nachricht einen Tresor fordert, kann man mE nach für die Erfüllung des „Verschlusses" bei e-Mail eine Cheffrierung verlangen!

Beim Übertragen der e-Mail ist diese in SMTP-Pakete „verschlossen". Durch das SMTP wird die Nachricht in viele kleine „Kuverts" (Pakete) geteilt und über unterschiedliche Wege vom Sender zum Empfänger geleitet. Solange sie jedoch

[8] *Wessely*, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612.

[9] *Leukauf/Steininger*, Kommentar zum Strafgesetzbuch[3], Rz 4 zu § 118.

[10] *Mayerhofer/Rieder*, Das österreichische Strafrecht , I.Teil, Strafgesetzbuch[4], Band XI, Rz 13 zu § 118.

[11] *Zipf* in WK, Rz 1 zu § 118 StGB.

[12] *Zipf* in WK, Rz 5 zu § 118 StGB.

[13] Siehe Punkt IV.B.3.b.

beim Absender am Rechner lagert oder sich bereits beim Empfänger befindet, liegt kein derartiger Verschluss vor. Hier kann die Verschlussform eine andere sein: Ist der Zugriff auf diese - sich noch nicht bzw. nicht mehr im Übertragungsweg befindenden - e-Mails nur mittels Passwort möglich, so kommt aus diesem Grund der Schutz durch des Briefgeheimnisses zum Tragen, da ein Passwortschutz einem Kuvert gleichgesetzt werden kann. Als Ausdruck des Wunsches nach Vertraulichkeit wurde die e-Mail ja passwortgesichert gespeichert und dadurch verschlossen. Will man sie lesen, so muss der richtige Code eingegeben und damit der Verschluss wieder geöffnet werden. ME nach liegt also sowohl bei der noch beim Absender lagernden als auch bei der bereits beim Empfänger gespeicherten e-Mail, die mittels Passwort zugriffsgesichert ist, ein elektronisch verschlossener Brief im Sinn des § 118 StGB vor.

§ 118 Abs 2 StGB

Absatz 2 spricht nur von Schriftstücken, wobei diese als Überbegriff zu „Briefen" gelten.[14] Normiert wird ein Absichtsdelikt: Der Täter dringt ein, „um zu lesen". Die tatsächliche Kenntnisnahme ist nicht nötig.

Der Begriff „Behältnis"

In Z 1 wird das Öffnen eines verschlossenen Behältnisses, um an ein Schriftstück zu gelangen, unter Strafe gestellt. Unter Behältnis versteht man ein Raumgebilde, das jedoch nicht zum Betreten für Menschen gedacht ist (Aktenkoffer oder Tresor). Um diese Bestimmung auf e-Mail anzuwenden, müsste man von folgender, äußerst praxisferner, Vorstellung ausgehen: Der Täter öffnet einen mit Schloss versehenen Rechner, um die Festplatte und damit die e-Mails zu „entnehmen"! Anders könnte der Begriff des verschlossenen Behältnisses nicht erfüllt werden.

Die e-Mail ist zwar in einem „elektronischen Kuvert" verpackt - um ein Behältnis im genannten Sinn handelt es sich dabei jedoch nicht.

Verwendung eines technischen Mittels

§ 118 Abs 2 Z 2 StGB will den bestrafen, der ein technisches Mittel anwendet, um ohne Öffnen des Verschlusses „seinen Zweck" zu erreichen. Gemeint ist damit unter anderem das Durchleuchten von Briefstücken.[15] Aufgrund des technischen Unterschiedes zwischen herkömmlichem Brief und e-Mail werden letztere bei

[14] Siehe Punkt V.A.1.

[15] *Mayerhofer/Rieder*, Das österreichische Strafrecht , I.Teil, Strafgesetzbuch[4], Band XI, Rz 9 zu § 118.

Eingriffen immer so geöffnet, dass der Verschluss (Passwortschutz) beeinträchtigt wird. Die Ziffer 2 ist somit für e-Mail kaum anwendbar.

§ 118 Abs 3 StGB

§ 118 Abs 3 StGB hat eine ganz andere Zielrichtung: Während es bei Abs 1 und 2 um das Öffnen – den Siegelbruch - geht, bezieht sich Abs 3 nur auf den Schutz des korrekten Zugangs. In diesem Sinn bedeutet die Verweisung auf Abs 1 nicht, dass das Schriftstück auch verschlossen sein muss.[16] Damit fällt das Problem des Verschlusses jedenfalls weg! Abs 3 stellt auf das Recht auf Übermittlung frei von jeglichen Eingriffen Unbefugter[17] ab, indem das Unterdrücken und Unterschlagen von Schriftstücken VOR Kenntnisnahme durch den Empfänger unter Strafe gestellt wird. Für e-Mail wird diese Bestimmung immer dann relevant werden, wenn die Nachricht nicht (nur) geöffnet, sondern (auch) dem Empfänger vorenthalten wird.

§ 118 Abs 4 StGB

Nach dieser Bestimmung ist der Täter nur auf Verlangen des Absenders und/oder des Empfängers - dies kommt auf den Zeitpunkt[18] des Eingriffs an - zu verfolgen. Ist der Täter ein Beamter, so muß der StA die Ermächtigung des Geschädigten einholen.

Wie schon angedeutet bzw aus der Natur der Kommunikation bzw Übermittlung von Nachrichten, gibt es unterschiedliche Zeitpunkte, wann und wo jemand in den Kommunikationsfluss eingreifen kann, um an die Nachricht zu gelangen. Im Briefverkehr können hier folgende zeitlichen und örtlichen Sachverhalte unterschieden werden – auch wenn sie juristisch nicht unbedingt zu anderen Lösungen führen:

- der Brief ist geschrieben und liegt offen auf dem Schreibtisch (Kein Siegelbruch möglich – nur § 118 Abs 3 (Unterdrückung) denkbar.
- der Brief wurde in ein Kuvert gesteckt und dieses verklebt und zum Versand bereitgelegt – Siegelbruch und Unterdrückung möglich.
- Brief wurde in den Briefkasten geworfen – Siegelbruch und Unterdrückung möglich.
- Brief wird vom Briefträger gelesen – Siegelbruch.
- Brief wird vom Briefträger in den Empfängerbriefkasten geworfen – Siegelbruch und Unterdrückung möglich.

[16] *Zipf* in WK, Rz 22 zu § 118 StGB.

[17] *Mayerhofer/Rieder*, Das österreichische Strafrecht , I.Teil, Strafgesetzbuch[4], Band XI, Rz 11 zu § 118.

[18] *Zipf* in WK, Rz 33 zu § 118 StGB.

- Brief liegt noch ungeöffnet am Schreibtisch des Empfängers – Siegelbruch und Unterdrückung möglich.
- Brief wird gelesen in einen Tresor eingeschlossen - § 118 Abs 2 möglich.

Die Situation bei e-Mails

Zugriffe beim Absender

Wenn der Zugang zu für das Versenden gedachte e-Mails nur mittels Passwortes möglich ist, ist dadurch das Tatbestandsmerkmal eines „verschlossenen Briefes" –vgl oben - erfüllt. Wer also eine am User-Rechner liegende e-Mail öffnet (durch Laden in den Arbeitsspeicher auf dem Bildschirm sichtbar macht) oder löscht, ist nach § 118 zu bestrafen.

Eingriffe in die Strecke Absender - Provider

Ab dem Absenden ist die e-Mail in einer Form des elektronischen Kuverts - dem SMTP-Paket - verschlossen. Damit wäre das Öffnen – nach dem packet-sniffing – als Siegelbruch im Sinn des § 118 StGB zu verstehen. Wird die e-Mail „abgezweigt", sodass die Nachricht gar nicht auf dem Providerrechner angelangt, so kommt §118 Abs 3 zur Anwendung.

Zugriffe beim Provider des Absenders

Weiters kann das Briefgeheimnis am Providerrechner verletzt werden, indem eine Person, die zum Mail-Server Zugang hat, die Daten sichtbar macht oder löscht.

Eingriffe in die Strecke Provider - Provider

Hier sind unzählige Möglichkeiten des Zugriffs denkbar: Die Vorgangsweise beim Eindringen entspricht im wesentlichen oben beschriebener.

Zugriffe beim Provider des Empfängers

Einerseits kann ein Dritter direkt am Rechner das Öffnen der e-Mail durchführen. Andererseits ist aber noch eine zusätzliche Eingriffsart möglich: Für den Adressaten warten e-Mails abholbereit am Providerrechner. Autorisiert mit Account und Paßwort könnte aber jedermann via Datenleitung diese Nachrichten löschen oder abfragen! In letzterem Fall wird der Verschluss durch unerlaubtes Verwenden dieser Zugangsdaten aufgebrochen. Zu beachten könnte in diesem Zusammenhang auch das ZugangskontrollG – Umsetzung der RL 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontolldiensten in seinem engen Anwendungsbereich sein.

Eingriffe in die Strecke Provider - Empfänger
Vgl Streck Absender – Provider.

Zugriffe beim Empfänger
Hat der Empfänger seine für ihn bestimmten e-Mails abgeholt, so hat er selbst und zulässigerweise den Verschluß geöffnet. Damit hört zunächst der Briefgeheimnisschutz auf zu wirken.

Leitet der Empfänger die empfangene e-Mail jedoch weiter und ist der Zugriff wieder nur mittels Passworts möglich, so ist wiederum die Anwendbarkeit des § 118 StGB begründet.

III.“Elektronischer Brief“ (e-Mail) und Briefgeheimnis im d Strafrecht
IN § 202 d StGB sind ebenfalls „nur“ verschlossene Briefe und andere verschlossene Schriftstücke vor dem Siegelbruch geschützt. Geschütztes Rechtsgut ist zum einen der Siegel, zum anderen die Kenntnisnahme ohne Öffnung des Verschlusses. Siehe hiezu die Ausführungen zum österreichischen Recht. Bei der e-Mail ist nun ebenfalls die Frage zu stellen, ob und wann es sich bei der e-Mail um ein solches verschlossenes Schriftstück handelt.

Verschlossenes Schriftstück
Nachdem in Deutschland 1986 – also noch vor Aufkommen der großen e-Mail-Welle – bereits eine Sonderbestimmung für das Ausspähen von Daten in § 202a StGB implementiert wurde, ist nach meinen Recherchen die Frage, ob e-Mails an sich dem Briefgeheimnis nach § 202 StGB unterliegen in der Literatur in Deutschland nicht behandelt worden. Im Folgenden soll die mögliche Strafbarkeit des Providers nach § 206 StGB außer Betracht bleiben.

Zurück zum Schriftstück: Schriftstück ist nach *Lenckner*[19] jede Verkörperung eines gedanklichen Inhalts durch Schriftzeichen. Damit ist das Schriftstück an die Körperlichkeit gebunden.[20] Nach ihm sollen sonstige zur Gedankenübermittlung bestimmte Träger nunmehr von § 202a StGb geschützt sein. Daher scheitert man in der Frage des Briefgeheimnisses für e-Mail in Deutschland wohl an dem Erfordernis der Verkörperung von Gedankeninhalten, die erforderlich wäre, um dem Tatbestandsmerkmal „anderes verschlossenes Schriftstück“ gerecht zu werden. Somit kann das Lesen von e-Mails – unabhängig ob passwortgeschützt oder nicht – nicht unter § 202 StGB subsumiert werden.

[19] *Lenckner Theodor*, in *Schönke/Schröder*, Strafgesetzbuch[26] (München, 2001) 1611.
[20] Vgl auch *Lackner Karl*, Strafgesetzbuch mit Erläuterungen[22] (München 1997) 884.

E-Mails unterliegen daher in Deutschland nicht dem Briefgeheimnis, da das Verständnis – wohl auch dem Zivilrecht und dem dortigen Sachbegriff abgeleitet – von Körperlichkeit und Unkörperlichkeit in Deutschland eine andere ist, als in Österreich.

IV „Elektronischer Brief" und § 202a dStGB

Besonders interessant bei dieser Bestimmung des „Ausspähens von Daten" ist die Definition von „Daten" im Zusammenhang mit diesem Tatbestand. Daten sind nämlich in diesem Zusammenhang nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Das Ansprechen der „Übermittlung" in der Datendefinition lässt unmittelbar auf die Frage schließen, ob der deutsche Gesetzgeber hier auch die e-Mail schützen wollte. Hiezu hat man wohl den eigentlich geregelten Sachverhalt heranzuziehen: Daten, die besonders gespeichert sind, sollen vor der unbefugten Kenntnisnahme geschützt werden. Grundsätzlich ist der Datenbegriff im dStGB weit zu verstehen. Ein Geheimnis braucht ihnen nach der Definition nicht zugrunde liegen.

Gedacht war wohl bei der Übermittlung in der Definition der Daten im Abs 2 an das „Anzapfen von Netzwerkleitungen" und weniger an das Abfangen von konkreten Mitteilungen – auch wenn diese Unterscheidung wohl technisch, als auch rechtlich keine große Rolle spielen dürfte.

Sind nun e-Mails an sich – und zu welchem Zeitpunkt – besonders geschützt? Wie schon oben – in der Beurteilung nach österreichischem Recht – dargelegt, ist die e-Mail, wenn sie am Rechner des Senders oder Empfängers gespeichert ist, in der Regel wohl nicht besonders geschützt. Jeder, der Zugriff auf den Rechner und den dazugehörigen Client hat, kann die e-Mails ohne jeglichen Aufwand lesen. Anders ist es mE, wenn die e-Mails – und wohl auch der e-Mail-Client an sich – passwortgeschützt sind. Dann handelt es sich um Daten, die nicht für den unberechtigten Leser bestimmt und besonders gesichert sind. Umgeht jemand den Passwortschutz, verschafft er sich (oder auch einem anderen – man denke an die Weiterleitung) Kenntnis von Daten, die elektronisch (Arbeitsspeicher) oder magnetisch (Festplatte) gespeichert sind und die auch nicht unmittelbar wahrnehmbar sind. Somit sind mE im Falle des Passwortschutzes e-Mails sowohl am Empfänger als auch am Sender-Rechner nach § 202a dStGB geschützt.[21]

[21] Vgl allgemein *Lackner*, Strafgesetzbuch[22] , 887

Nur eine Anmerkung im Zusammenhang mit „e-Mail am Arbeitsplatz“: Es wird wohl auch der Arbeitgeber nicht allein aufgrund des Arbeitsverhältnisses gerechtfertigt sein, e-Mails – auch wenn sie an die sog Firmenadresse mitarbeiter@firma.de gehen – über den Systemadministrator zu lesen, wenn der Arbeitnehmer für das Abrufen eigene Passwörter definiert hat. ME ist dies auch als „Umgehung“ der besonderen Sicherung zu sehen. AA wohl *Lackner,* Strafgesetzbuch[22] , 888.

Juristisch/Technisch interessanter ist wohl die Frage, ob das SMTP den Anforderungen der besonderen Sicherung iSd § 202a dStGB genügt. Grundsätzlich sind ja auch Daten, wenn sie übermittelt werden gem § 202a Abs2 dStGB geschützt. Wenn man davon ausgeht, dass die besondere Sicherung aus Vorkehrungen zu bestehen hat, die objektiv geeignet sind und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf die Daten auszuschließen oder wenigstens zu erschweren,[22] hat man mit dem SMTP als Sicherung wohl Schwierigkeiten. Faktisch kann das SMTP mit der Möglichkeit, dass einzelne Daten-Pakete über völlig unterschiedliche Leitungen vom Sender zum Empfänger übermittelt werden, wohl eine objektive Sicherung bilden, aber subjektiv nutzt jemand SMTP aus Sicherheitsgründen nicht. Der Effekt, dass die Datenpakete nicht „ganz leicht“ abgefangen werden können, ist vielmehr ein „Nebeneffekt“, der nicht als Sicherung im Sinne des § 202a dStGB zu verstehen ist. Außerdem ist beim SMTP relativ leicht – mittels packet-sniffing udgl – alle Pakete abzufangen und , nachdem die Daten sonst im plain-text übermittelt werden, auch zu lesen. Damit ist wohl auch der objektive Schutz durch das SMTP äußerst gering.

Somit kommt man mE zum Schluss, dass SMTP nicht der von § 202a dStGB geforderten besonderen Sicherung entspricht. Besonders gesichert ist allerdings ohne Frage eine verschlüsselte e-Mails. Das Abfangen und entschlüsseln einer solchen Nachricht ist sicherlich unter § 202a dStGB zu subsumieren.

Abschließend kann also gesagt werden, dass die passwortgesicherten e-Mails in Österreich dem Schutz nach § 118 StGB (Briefgeheimnis) unterliegen. In Deutschland scheitert man beim Briefgeheimnis (§ 202 dStGB) für e-Mails am Erfordernis der Körperlichkeit. Nach § 202a dStGB sind nur passwortgesicherte bzw auf dem Übertragungsweg verschlüsselte e-Mails geschützt.

[22] *Lenckner* in *Schönke/Schröder*, Strafgesetzbuch[26] ,1616.