Universitätslehrgang
für Informationsrecht und Rechtsinformation
an der Rechtswissenschaftlichen Fakultät der Universität Wien

Indiskretionsdelikte und neue Medien

Zur strafrechtlichen Relevanz der Überwachung privater Kommunikation mittels „Internet Monitoring Software“

MASTER THESIS

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)

FÜR INFORMATIONSRECHT UND RECHTSINFORMATION

vorgelegt von

Mag. Patrick Geiger

begutachtet von

Ao. Univ. Prof. Dr. Susanne Reindl

im September 2003

ABKÜRZUNGSVERZEICHNIS

aA	anderer Ansicht
aaO	am angeführten Ort
Abb	Abbildung
ABGB	Allgemeines Bürgerliches Gesetzbuch
Abs	Absatz
AnwBl	Österreichisches Anwaltsblatt
AOL	America Online
Art	Artikel
BGBl	Bundesgesetzblatt
BlgNr	Beilage(n) zu den stenographischen Protokollen des Nationalrats
bzw	beziehungsweise
ca	circa
CCC	Convention on Cyber-Crime des Europarats
dh	das heißt
Dipl.-Inform.	Diplomierter Informatiker
DIR	Datenschutz und Informationsrecht
DSG	Datenschutzgesetz
ECG	E-Commerce-Gesetz
ecolex	Fachzeitschrift für Wirtschaftsrecht
EDVuR	EDV und Recht
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
ErlBem	Erläuternde Bemerkungen
EuGRZ	Europäische Grundrechte-Zeitschrift
f, ff	folgende
FH	Fachhochschule
FJ	Finanzjournal
GMat	Gesetzesmaterialien

hA	herrschende Ansicht
Hrsg	Herausgeber
iA	im Allgemeinen
idF	in der Fassung
idR	in der Regel
idS	in diesem Sinne
ieS	im engeren Sinn
insb	insbesondere
iS	im Sinne
iSv	im Sinne von
IT	Informationstechnologie
iVm	in Verbindung mit
JAP	Juristische Ausbildung und Praxisvorbereitung
JBl	Juristische Blätter
krit	kritisch
LAN	Local Area Network
leg cit	legis citatae (der zitierten Vorschrift)
lit	litera
LSK	Leitsatzkartei
MB	Megabyte
mE	meines Erachtens
mwN	mit weiteren Nachweisen
Nr	Nummer
og	oben genannte(n)
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
ÖBl	Österreichische Blätter für gewerblichen Rechtsschutz
ÖJZ	Österreichische Juristenzeitung
PC	Personal Computer
PGP	Pretty Good Privacy

RdA	Das Recht der Arbeit
RGBl	Reichsgesetzblatt
RL	Richtlinie der Europäischen Gemeinschaften
Rsp	Rechtsprechung
RV	Regierungsvorlage
Rz	Randzahl
RZ	Richterzeitung
sog	sogenannt, -e, -er, -es
SSt	Entscheidungen des österreichischen obersten Gerichtshofes in Strafsachen und Disziplinarangelegenheiten
StGB	Strafgesetzbuch
StGB-Komm	Kommentar zum Strafgesetzbuch
StGG	Staatsgrundgesetz
StRÄG	Strafrechtsänderungsgesetz
TKG	Telekommunikationsgesetz
ua	unter anderem
USD	amerikanische Dollar
uU	unter Umständen
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
vgl	vergleiche
VR	die Versicherungsrundschau
WK	Wiener Kommentar zum Strafgesetzbuch
Z	Ziffer
zB	zum Beispiel
ZfV	Zeitschrift für Verwaltung
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

INHALTSVERZEICHNIS

1 Einleitung

1.1 Die Erweiterung der Kommunikationsmöglichkeiten durch das Internet

Die in der letzten Zeit rasant vorangeschrittene globale Vernetzung hat die Möglichkeiten des Austausches von Information jedweder Art enorm erweitert. Die Übermittlung von Nachrichten via Internet ist sowohl aus dem heutigen Geschäfts- wie dem Alltagsleben nicht mehr wegzudenken. Die „herkömmliche" Post, für die sich nunmehr die Bezeichnung „Snail Mail" („Schneckenpost") herausgebildet hat, um deren verhältnismäßige Langsamkeit hervorzuheben, wurde in weiten Bereichen durch die Nachrichtenübertragung per E-Mail ersetzt, wobei neben der Geschwindigkeit und den günstigen Kosten auch die Möglichkeit, umfangreiche Dateien zu übertragen, eine große Rolle gespielt hat.

Daneben haben sich neue Formen der Kommunikation in Echtzeit herausgebildet, die vor dem Siegeszug des Internet mangels Datenübertragungskapazitäten noch weitgehend unbekannt waren, wie zB der Chat und die Videokonferenz.

1.2 Synchrone und asynchrone Kommunikation

Als synchrone Kommunikation bezeichnet man die Kommunikation in Echtzeit. Dabei stehen die ausgetauschten Informationen dem Kommunikationspartner[1] sofort – bzw mit einer minimalen Verzögerung – nach der Absendung zur Verfügung, sodass jener unmittelbar darauf reagieren kann. Beispiele dafür sind im Bereich der Nachrichtenübermittlung via Internet der Chat und die Videokonferenz, im Bereich der herkömmlichen Nachrichtenübermittlung das Telefonat. Asynchrone Kommunikation hingegen findet mit einer beliebig langen Zeitverzögerung statt, die Nachricht ist zwar vom Empfänger – allenfalls nach einer minimalen Verzögerung – abrufbar, der Absender weiß aber idR nicht, wann diese tatsächlich empfangen wird. Beispiele dafür sind die E-Mail sowie der per „Snail Mail" übermittelte Brief.

Dass die Übergänge zwischen synchroner und asynchroner Kommunikation im Rahmen der Nachrichtenübertragung durch das Internet aber fließend sind und

[1] Denkbar sind freilich auch mehrere Kommunikationspartner gleichzeitig, im Folgenden wird jedoch der Einfachkeit halber die Einzahl verwendet.

dadurch eine scharfe Abgrenzung nicht möglich ist, zeigen die „Instant Messaging Systeme“, die innerhalb weniger Jahre zu einem der beliebtesten Dienste des Internet geworden sind. Diese ermöglichen es dem User, sich entweder mittels eines Programms oder direkt über den Webbrowser bei einem zentralen Server anzumelden und potentiellen Kommunikationspartnern die Bereitschaft zur Kontaktaufnahme zu signalisieren. Dabei kann der User meistens wählen, für welche Mitglieder aus einer vorgewählten Kontaktliste er sichtbar und erreichbar sein will und jenen seinen „Online Status“ (zB „erreichbar“ oder „gerade nicht am PC“) anzeigen lassen. Versendet werden können sowohl „Online-Messages“ als auch „Offline-Messages“, bei ersteren kann der Empfänger – sofern er gerade seinen PC beobachtet – sofort reagieren und wie in einem Chat eine synchrone Kommunikation in Echtzeit führen, letztere erreichen den Empfänger wie eine E-Mail erst zu jenem Zeitpunkt, in dem er das System startet und sich erneut am Server anmeldet.

1.3 Einsatzbereiche von Chat, Instant Messaging und Videokonferenz

Neben speziellen Chat-Programmen existieren zahllose verschiedensten Themenkreisen gewidmete Chatrooms, in die sich der User über entsprechende Websites oder Programme einloggen und mit den übrigen Teilnehmern austauschen kann. Das Angebot reicht dabei von Diskussionen zu spezifischen wissenschaftlichen Fragestellungen bis zu Chatrooms, die ausschließlich der Unterhaltung ohne vorgegebene Themen dienen. Einige Unternehmen nutzen die Vorteile dieser Art der synchronen Kommunikation auch, um schnell und günstig online Customer Support anbieten zu können. Vielfach wird der Chat auch dazu genutzt, zwanglos neue Kontakte – welcher Art auch immer – zu knüpfen. Ein erheblicher Nachteil des Chat liegt darin, dass – ohne gleichzeitige Heranziehung anderer Kommunikationsmittel – die Identifikation des Kommunikationspartners kaum möglich ist.

Instant Messaging wird meist für die Nachrichtenübermittlung an einen im voraus eingeschränkten Personenkreis (Mitglieder einer „Kontaktliste“) eingesetzt und erfreut sich auch auf geschäftlicher Ebene zur unternehmensinternen Kommunikation zunehmender Beliebtheit.

Videokonferenzen bieten gegenüber dem Chat und der herkömmlichen Telefonie den Vorteil, dass die Kosten unabhängig von der Distanz zwischen den Kommunikationspartnern lediglich den Kosten einer Verbindung mit dem Internet entsprechen und die Kommunikationspartner füreinander visuell wahrnehmbar sind, wobei die Unterhaltung – je nach technischer Ausstattung und

zur Verfügung stehender Übertragungskapazität – entweder wie im Chat über die Tastatur oder wie bei einem Telefonat über Mikrofone und Lautsprecher geführt wird.

1.4 Einsatzbereiche der E-Mail

Die E-Mail ist in den letzten Jahren zum Inbegriff moderner Nachrichtenübermittlung geworden und wird sowohl im privaten wie auch im geschäftlichen Bereich zunehmend zum Ersatz des Briefverkehrs eingesetzt. Zu diesem Siegeszug hat neben der Übertragungsgeschwindigkeit und der Kostenersparnis vor allem auch der Umstand beigetragen, dass die zu versendenden Inhalte nicht mehr nur in Papierform, sondern ebenso mittels elektronischer Datenträger präsentiert, verarbeitet und archiviert werden können.

1.5 Gegenstand dieser Arbeit

Der Gesetzgeber anerkennt seit langem, dass Sender und Empfänger von Nachrichten in vielen Fällen ein berechtigtes Interesse an der Vertraulichkeit ihrer Kommunikation und am Schutz ihrer Privatsphäre haben und hat aus diesem Grund schon lange vor dem Zeitalter des Internets Straftatbestände zum Schutz des Briefgeheimnisses und des Fernmeldegeheimnisses geschaffen. Die Geheimhaltungsinteressen der User, die die Möglichkeiten des Internets zur Nachrichtenübertragung nutzen, sind oft sehr ähnlicher Natur, jedoch durch Programme, die unbemerkt sämtliche Online-Aktivitäten aufzuzeichnen vermögen, massiv bedroht.

Gegenstand dieser Arbeit ist die Untersuchung, ob die elektronische Nachrichtenübermittlung via Internet in gleicher Weise wie das Briefgeheimnis und das Fernmeldegeheimnis durch das strafrechtliche Instrumentarium gegen Angriffe anderer Privater geschützt ist und ob ein solcher Schutz überhaupt wünschenswert und notwendig erscheint.

2 Der Schutz der Vertraulichkeit von Kommunikationsvorgängen

2.1 Geheimnisschutz und Geheimnisbegriff im StGB

Das StGB fasst in seinem fünften Abschnitt unter der Überschrift „Verletzungen der Privatsphäre und bestimmter Berufsgeheimnisse“ eine Deliktsgruppe zusammen, deren Gegenstand mit dem Terminus „Geheimnisschutz“ umschrieben wird, geschützte Rechtsgüter sind die Privatsphäre und die Geheimsphäre. Da jene aber keine ausreichend präzisen bzw präzisierbaren Rechtsgüter darstellen, umfasst der Schutzbereich nur einzelne, zumeist sektoral und nach bestimmten Angriffsweisen umschriebene Ausschnitte aus der Privat- und Geheimsphäre, sodass der Strafrechtsschutz in diesem Bereich notwendigerweise fragmentarisch, formalisiert und kasuistisch bleibt[2]. *Gassauer-Fleissner* [3] sieht im Bereich des § 118 StGB (Verletzung des Briefgeheimnisses und Unterdrückung von Briefen) die Ursache für diese Kasuistik in der Umschreibung „qualifizierter krimineller Energie“ in Ansehung einer besonders verwerflichen Motivation, doch ist mE eher *Zipf* [4] zu folgen, der die strenge Formalistik der Tatbestände in diesem Bereich in der Notwendigkeit rechtsstaatlichen Kriterien genügender Deliktsumschreibungen sieht. Beispielsweise ist jemand, der über dem Schreibtisch des Briefempfängers eine Überwachungskamera installiert, um den Inhalt von Briefen, die darunter geöffnet werden, zu erfahren, von einer nicht minder kriminellen Energie beseelt als jemand, der über Dampf mit einer Stricknadel einen verschlossenen Brief öffnet, sich Kenntnis vom Inhalt verschafft und den Brief daraufhin wieder verschließt.

Eher dem Schutz der Privatsphäre sind die §§ 118, 119 (Verletzung des Telekommunikationsgeheimnisses) und 120 StGB (Mißbrauch von Tonaufnahme- oder Abhörgeräten) zuzuordnen, da sie den Austausch von Gedankenäußerungen in akustischer- oder Schriftform schützen, wobei jeweils nur ein partieller Schutz nach bestimmten Angriffsarten besteht.[5] Die §§ 118a (Widerrechtlicher Zugriff auf ein Computersystem) und 119a StGB (Missbräuchliches Abfangen von Daten) hingegen schützen allgemein „Daten“, dh nicht notwendigerweise Nachrichten bzw Kommunikationsvorgänge, wobei § 119a einen Übermittlungsvorgang voraussetzt. Die §§ 121-124 StGB schützen Berufsge-

[2] *Zipf*, WK[1] Vor § 118 Rz 1.
[3] *Gassauer-Fleissner,* Geheimhaltung, Offenbarung und Veröffentlichung von Daten in Informationsnetzen, ecolex 1997, 102.
[4] *Zipf*, aaO.
[5] *Zipf*, WK[1] Vor § 118 Rz 3.

heimnisse bzw Geschäfts- oder Betriebsgeheimnisse und damit allenfalls Aufzeichnungen über vorangegangene Kommunikationsvorgänge. Dass die unter dem fünften Abschnitt des StBG zusammengefasste Deliktsgruppe wegen der Notwendigkeit formalisierter und kasuistischer Tatbestandsumschreibungen besonders anfällig für Novellierungsbedarf aufgrund neuer technischer Möglichkeiten, in die Privat- bzw Geheimsphäre einzudringen, ist, wird schon aus der Tatsache ersichtlich, dass durch das Strafrechtsänderungsgesetz 2002 in diesem Abschnitt zwei neue Paragraphen (§§ 118a und 119a) eingefügt, einer (§ 119) geändert und einer (§ 120) ergänzt werden mussten.

Im österreichischen Recht findet sich keine Legaldefinition des Begriffs "Geheimnis", dennoch wird sowohl im UWG als auch im StGB und den arbeitsrechtlichen Bestimmungen ein Geheimnis einheitlich als Tatsache angesehen, *"die nur einem eng begrenzten, im wesentlichen geschlossenen Personenkreis bekannt sein darf und anderen nicht oder nur schwer zugänglich ist und die nach dem Willen des Berechtigten nicht über den Kreis der Eingeweihten hinausdringen soll"* [6]. Für ein Betriebs- oder Geschäftsgeheimnis ist die Definition dahingehend zu erweitern, dass der Berechtigte zusätzlich an der Geheimhaltung ein schutzwürdiges wirtschaftliches Interesse haben muss, wobei es sich um Tatsachen kommerzieller oder technischer Art handeln muss. Darüber hinaus muss die Tatsache in einer Beziehung zum Betrieb des Unternehmens stehen und für dessen Wettbewerbsfähigkeit Bedeutung haben[7].

Judikatur und Literatur vertreten für die §§ 122 bis 124 StGB und für § 11 UWG eine übereinstimmende Position, die sich nach *Burgstaller* [8] folgendermaßen zusammenfassen lässt: *„„Geschäfts- oder Betriebsgeheimnis" sind (1) unternehmensbezogene Tatsachen kommerzieller oder technischer Art, die (2) bloß einer bestimmten und begrenzten Zahl von Personen bekannt und anderen nicht oder nur schwer zugänglich sind, die weiter (3) nach dem Willen des Berechtigzen nicht über den Kreis der Eingeweihten hinausdringen sollen, wobei schließlich (4) der Geschäfts- oder Betriebsinhaber an der Nichtoffenbarung dieser Tatsachen ein wirtschaftliches Interesse haben muß."*

Leukauf/Steininger [9] beschreiben Geheimnisse als *„Tatsachen, die nur einer Person oder einem bestimmten, nicht allzu großen Kreis von Personen bekannt*

[6] *Schramböck*, Der Schutz von Betriebs- und Geschäftsgeheimnissen nach Beendigung des Arbeitsverhältnisses in Österreich und in den USA (am Beispiel des Bundesstaates Kalifornien) im Rechtsvergleich, ÖBl 2000, 3, mwN.
[7] *Schramböck*, aaO.
[8] *Burgstaller*, in: *Aicher/Funk/Korinek/Krejci/Ruppe* [Hrsg], Geheimnisschutz im Wirtschaftsleben (1980) 11, mwN.
[9] *Leukauf/Steininger*, StGB[3] § 121 Rz 16, mwN.

und anderen nicht oder nur schwer zugänglich sind und die nach dem ausdrücklichen oder erschließbaren Willen des Berechtigten auch nicht über diesen Kreis hinaus bekannt werden sollen."

Wessely [10] definiert Tatsachen als „geheim", die *„lediglich einer oder wenigen Personen außerhalb eines eine geschlossene Einheit bildenden Personenkreises bekannt sind"* [11] und hält fest, dass die Abgrenzung im Einzelfall schwierig sein kann. Als „Geheimnis im technischen Sinn" beschreibt er Nachrichten bzw Informationen, die aufgrund ihres Inhaltes geheim sind.

Im Fall des Austausches von Information schützt das Strafrecht jedoch nicht nur den Inhalt von Nachrichten, sondern ebenso das Vertrauen des Absenders und Empfängers in die Vertraulichkeit der Nachrichtenübertragung. Die §§ 118, 119, und 120 Abs 2a StGB schützen Kommunikationsvorgänge, die wegen der räumlichen Distanz der Kommunikationspartner auf Übertragungswege (zB die Post, Telekomanbieter oder das Internet) angewiesen sind. Dabei begegnet der Schutz der Vertraulichkeit der Nachrichtenübermittlung durch die og Delikte jenen Gefahren, die aus dem spezifischen gewählten Übertragungsweg resultieren. Geschützt sollen also nicht nur „Geheimnisse im technischen Sinn" sein, sondern der Kommunikationsvorgang als solcher, sodass es auf den Inhalt der Nachrichten nicht ankommt.

Schmidt [12] orientiert den strafrechtlich relevanten Geheimnisbegriff Rechtsprechung und Schrifttum folgend an drei miteinander zu kumulierenden Elementen: *„Erstens am „Geheimsein" der Tatsachen, auf die sich das Geheimnis beziehen soll; zweitens am Geheimhaltungswillen des Geheimnisträgers, und drittens an dem von diesem Willen unabhängigen, vom Erfordernis der Gerechtigkeit her bestimmten objektiven Geheimhaltungsinteresse."* „Geheim" ist demnach eine Tatsache, wenn sie *„noch im Geheimbereich des Geheimnisträgers oder der mit seinem Willen zu Mitwissern gemachten Dritten, in diesem Falle also in einem durch gegenseitige Verpflichtung oder gleichlaufende Interessen geschlossenen Kreis von „Wissenden" verborgen ist. Was über diesen Bereich hinausgelangt ist, insbesondere das, was in den geheimniszerstörenden Bereich der Öffentlichkeit (Offenkundigkeit) geraten ist, kann niemals mehr Geheimnis sein, mag ein Geheimnisträger noch so sehr an seinen* (sic!) *Geheimhaltungswillen festhalten* [...]*."* Wo kein Geheimhaltungswille besteht, könne juristisch nicht von einem „Geheimnis" gesprochen werden. Durch das

[10] *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491.
[11] Vgl zum Begriff des „Geheimnisses" sowie zur Abgrenzung ausführlich *Seiler*, Der strafrechtliche Schutz der Geheimnissphäre, 18 ff.
[12] *Schmidt*, Zur Problematik des Indiskretionsdelikts, ZStW 79, 741.

Erfordernis eines objektiven Geheimhaltungsinteresses stellt sich der strafrechtliche Geheimnisbegriff als normatives Tatbestandsmerkmal dar, wodurch es notwendig wird, den spezifisch rechtlichen Sprachgebrauch jeweils deliktsbezogen durch systematische oder teleologische Auslegung herauszuarbeiten.

Obwohl die im fünften Abschnitt des StGB zusammengefassten Delikte meist generell mit dem Terminus „Geheimnisschutz" übertitelt werden, handelt es sich aufgrund der Verschiedenartigkeit der geschützten Rechtsgüter und der Angriffsobjekte um eine sehr heterogene Deliktsgruppe[13], der kein einheitlicher Geheimnisbegriff zugrunde liegt. Für den Schutz der Vertraulichkeit der Nachrichtenübertragung ergibt sich folglich ein weiter Geheimnisbegriff, da in diesem Bereich nicht auf den Inhalt der Nachricht abgestellt wird. Der von *Schmidt* umschriebene Geheimnisbegriff kann demnach nur zur Definition eines Kernbereiches, in dem ein strafrechtlicher Schutz unbedingt notwendig erscheint, herangezogen werden. Der tatsächliche Schutz geht insbesondere dadurch, dass die entsprechenden Tatbestände Verletzungs- und Gefährdungsaspekte kombinieren und somit die Strafbarkeit oft weit in das Vorfeld der unmittelbaren Rechtsgutverletzung durch Kenntnisnahme von „geheimen" Tatsachen verlagert wird, meist über die Pönalisierung tatsächlicher Einbrüche in die Geheimnissphäre hinaus.

§ 118 StGB zB stellt bereits das Öffnen eines Briefes oder eines verschlossenen Behältnisses, in dem sich ein nicht zur Kenntnisnahme durch den Täter bestimmtes Schriftstück befindet, unter Strafe. Das Delikt ist dabei schon vor der Kenntnisnahme vom Inhalt vollendet, sofern der Täter die Absicht verfolgt, sich oder einem anderen Unbefugten Kenntnis vom Inhalt des Briefs oder Schriftstücks zu verschaffen (Absichtsdelikt ieS).[14] Um ein „Geheimnis" in dem Sinn, dass der Inhalt des Briefs oder Schriftstücks nur einem bestimmten begrenzten Personenkreis bekannt werden soll, braucht es sich nicht zu handeln, sodass es allein auf den Bruch der Vertraulichkeit ankommt.[15] Für eine Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB) genügt schon die Benützung einer Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, wiederum unabhängig vom tatsächlichen Erfolg des Angriffes auf das Rechtsgut.[16]

[13] *Zipf*, WK[1] Vor § 118 Rz 3; *Koberger*, Grenzenloser Schutz der Privatsphäre vor Tongandgeräten?, ÖJZ 1990, 330.
[14] *Leukauf/Steininger*, StGB[3] § 118 Rz 18.
[15] *Leukauf/Steininger*, StGB[3] § 118 Rz 4.
[16] Vgl zur alten Rechtslage *Leukauf/Steininger*, StGB[3] § 119 Rz 14 ff.

Für die §§ 118, 119, 119a und 120 Abs 2a StGB ergibt sich aus dem oben ausgeführten zusammenfassend, dass die dort umschriebenen Deliktstatbestände nicht nur die unbefugte Kenntnisnahme vom Inhalt der übermittelten Nachrichten bzw Daten pönalisieren, sondern vielmehr den Schutz der Vertraulichkeit des gewählten Übertragungsweges gewährleisten sollen. Die entsprechenden Delikte sind sohin selbst dann, wenn der übertragene Inhalt geheim bleibt oder gar kein „Geheimnis im technischen Sinn" darstellt, bereits mit einem Eingriff in die Kommunikationssphäre verwirklicht. Das Geheimnis ist bei diesen Delikten im Gegensatz zu den §§ 121 bis 124 StGB kein Tatbestandselement.

§ 121 StGB (Verletzung von Berufsgeheimnissen) ist als Sonderdelikt spezifisch auf die Angehörigen bestimmter Berufsgruppen und deren Hilfskräfte zugeschnitten und schützt Geheimnisse, die den Gesundheitszustand einer Person betreffen (Abs 1) bzw Geheimnisse, die einem Sachverständigen im Rahmen einer behördlichen Bestellung bekannt geworden sind (Abs 3), sofern die betroffene Person an der Geheimhaltung ein berechtigtes Interesse hat. Hier bildet das berechtigte Interesse an der Geheimhaltung – welches bei Gesundheitsdaten in der Regel gegeben sein wird – das zentrale Kriterium, geschützt wird daneben das Vertrauen in die Diskretion der genannten Berufsgruppen.

Beim durch die §§ 122 bis 124 StGB geschützten Geschäfts- und Betriebsgeheimnis ergibt sich die Schutzwürdigkeit aufgrund wirtschaftlicher Überlegungen aus dem Unternehmensbezug der geheimen Tatsachen. Hier genügt grundsätzlich bereits die mangelnde Offenkundigkeit einer unternehmensbezogenen Tatsache und das entsprechende objektive Geheimhaltungsinteresse für die Annahme eines Wirtschaftsgeheimnisses.[17]

2.2 „Indiskretionsdelikte ieS" und geschütztes Rechtsgut

Für die folgende Untersuchung ist eine Untergruppe der Indiskretionsdelikte, die im folgenden als „Indiskretionsdelikte ieS" bezeichnet wird, hervorzuheben. Darunter sind solche Delikte zu verstehen, die – losgelöst von wirtschaftlichen Überlegungen – weder den Eintritt eines Vermögensschadens, noch einen Bereicherungsvorsatz des Täters voraussetzen. Die Indiskretionsdelikte ieS bezwecken nicht den Schutz fremden Vermögens. Der Vorsatz des Täters beschränkt sich darauf, dass jener allenfalls einen Gefühlsschaden des Opfers ernstlich für möglich hält und sich damit abfindet (sog „bedingter Vorsatz"), ei-

[17] *Burgstaller*, Geheimnisschutz 15.

nen solchen aber nicht bezweckt. Zu den Indiskretionsdelikten ieS zählen § 118 StGB (Verletzung des Briefgeheimnisses und Unterdrückung von Briefen), § 119 StGB (Verletzung des Telekommunikationsgeheimnisses) und § 120 StGB (Mißbrauch von Tonaufnahme- oder Abhörgeräten). Eine weitere Gemeinsamkeit jener Deliktsgruppe ist der Schutz der Vertraulichkeit von Kommunikationsvorgängen. Die Notwendigkeit, neben dem zivilrechtlichen Persönlichkeitsschutz und dem Schutz des Briefgeheimnisses strafrechtliche Tatbestände einzuführen, die – unabhängig von einem Bereicherungsvorsatz oder einer Schädigungsabsicht des Täters – die Privatsphäre des Individuums schützen, ergab sich vor allem durch technische Entwicklungen wie Tonbandaufnahmegeräte oder Abhöranlagen, die ein Eindringen in den intimsten Bereich der Persönlichkeit eines anderen erleichtern, sowie durch die Erfindung neuer Kommunikationsmedien wie der Telefonie.

Die Indiskretionsdelikte ieS schützen die Privat- bzw Intimsphäre. Da jedoch der Inhalt der Nachricht nicht relevant ist, kann das geschützte Rechtsgut zutreffender mit dem Begriff der „Kommunikationssphäre“ umschrieben werden, wodurch auch zum Ausdruck kommt, dass ebenso das Vertrauen der Kommunikationspartner in die Exklusivität des Kommunikationsvorganges geschützt werden soll.

Da bei der Untersuchung, ob eine Nachricht strafrechtlich geschützt ist, auf die Art der Übermittlung und nicht auf deren Inhalt abzustellen ist, wird im folgenden für Inhalte, deren vertrauliche Behandlung üblicherweise von den Kommunikationspartnern gewünscht wird, der Begriff „diskretionsrelevante Inhalte“ verwendet.

2.3 Eingrenzung des Gegenstandes der Untersuchung

Im folgenden sollen nur solche Sachverhalte untersucht werden, in denen der Täter, der sich unter Verwendung des unten beschriebenen Programms „IamBigBrother“ ohne Wissen des Überwachten unbefugt Zugang zu diskretionsrelevanten Inhalten verschafft, keine über die bloße Indiskretion hinausgehenden Ziele verfolgt. Der Täter handelt nicht mit Schädigungsabsicht oder Bereicherungsvorsatz und will die ausspionierten Kommunikationsinhalte niemandem anderen zugänglich machen und will sie auch auf keine andere Art in irgendeiner Form verwerten. Nach seinem Tatplan erlangt das Opfer von der Tat keine Kenntnis.

Untersucht werden nur Tatbestände des gerichtlichen Strafrechts. Der Täter handelt im privaten Bereich, arbeitsrechtliche Aspekte werden nicht thematisiert.

3 Angriffe auf die Vertraulichkeit von Kommunikationsvorgängen via Internet durch Überwachungsprogramme („Internet Monitoring Software“)

Die Überwachung von Kommunikationsvorgängen auf dem eigenen oder auf einem fremden PC ist in der heutigen Zeit längst nicht mehr Netzwerkadministratoren, Computerexperten, Hackern oder Technikern vorbehalten. Mittlerweile wurde eine Vielzahl von Programmen entwickelt, die es auch dem „durchschnittlich begabten User“ erlauben, solche zu installieren und damit fremde Nachrichtenübermittlung zu überwachen und zu protokollieren. Für derartige Programme haben sich die Bezeichnungen „Internet Monitoring Software“ bzw „Spyware“ herausgebildet. Angeboten werden sie auf diversen Websites und stehen dort – nach Bezahlung mittels Kreditkarte – zum sofortigen Download bereit. Bezeichnend für Funktionalität und Inhalt dieser Programme sind deren Namen: „IamBigBrother“, „NetObserve“, „Spy Agent“, „Realtime-Spy“, „WebMail Spy“, „WebSite Watcher“, „iSpyNOW“, „Modem Spy“, „PC Activity Monitor Pro“, „Cyber INFORMER“, „OrvellMonitoring2003“, „CuteSpy“ oder „Perfect Keylogger“, um nur einige zu nennen. Einem ausführlichen Anwendungstest wurde als Grundlage dieser Arbeit das Programm „IamBigBrother“[18] unterzogen.

Gemeinsam ist diesen Programmen die leichte Installation und Bedienbarkeit sowie die Fähigkeit, für den Überwachten unbemerkt zu laufen, sodass sie weder in der Systemsteuerung unter der Liste der installierten Software[19] aufscheinen, noch auf der Taskleiste oder auf der Liste der zuletzt gestarteten Programme jemals sichtbar werden. Manche der erwähnten Produkte bieten jedoch die Möglichkeit, dem jeweiligen Benutzer des PCs – nach entsprechender Voreinstellung durch denjenigen, der Zugang zum Überwachungsprogramm hat – anzeigen zu lassen, dass seine Aktivitäten protokolliert werden.

[18] Online: http://www.iambigbrother.com.

[19] Beschrieben wird hier ausschließlich die Anwendung unter einem Windows Betriebssystem, auf das die meisten dieser Produkte zugeschnitten sind, selbstverständlich sind aber auch gleichartige Programme für die Anwendung unter anderen Betriebssystemen erhältlich.

Je nach Umfang, der sich freilich auch im Preis für das jeweilige Programm niederschlägt (soweit überblickbar ca zwischen 30,-- und 200,-- USD), bietet Internet Monitoring Software die nachstehenden Funktionalitäten an[20]:

„E-Mail Capturing“:	Der Inhalt aller empfangenen und versendeten E-Mails wird aufgezeichnet.
„Conversation-Logging“:	Es wird die gesamte Konversation, die in einem Chatroom oder über einen Chat-Client bzw ein Instant Messaging System läuft, aufgezeichnet.
„Remote Install“:	Das Programm wird an eine Datei angehängt, jene wird per E-Mail verschickt. Öffnet der Empfänger die Datei, installiert sich das Programm selbständig und unbemerkt auf dessen PC und führt – je nach Umfang des Programms – die übrigen beschriebenen Funktionalitäten aus. Der Überwachende gelangt durch die Funktionen „Remote Access“ oder „Log Delivery“ (siehe dazu unten) zu den Ergebnissen des Überwachungsvorgangs.
„Remote Access“:	Die Ergebnisse des Überwachungsvorgangs werden auf einem Server abgelegt und können weltweit von jedem PC mit Internetzugang abgefragt werden.
„Log Delivery”:	Die Ergebnisse des Überwachungsvorganges werden als Datei per E-Mail automatisch vom überwachten PC an eine vom Überwacher ausgewählte E-Mail Adresse verschickt, was für den Überwachten nicht sichtbar wird.
„Key-Logging“:	Jede Eingabe über die Tastatur wird protokolliert, dh alles, was der Überwachte auf der Tastatur schreibt, kann nachträglich vom Überwachenden gelesen werden.
„Screenshots“:	Die Ausgabe des Monitors wird in einer Bilddatei festgehalten, dh der Überwachende sieht nachträglich genau, was der Bildschirm zu einem bestimmten Zeitpunkt angezeigt hat.

[20] Diese Liste erhebt keinen Anspruch auf Vollständigkeit, da dem Verfasser – trotz umfangreicher Recherche – nicht alle angebotenen Produkte der vorgestellten Art bekannt sind. Aus Kostengründen war es auch nicht möglich, alle beschriebenen Funktionalitäten zu testen.

„Filterning“ von Websites:	Der Zugang zu vorausgewählten Websites wird gesperrt.
„Webcam Picture-Capturing“:	Eine an den überwachten PC angeschlossene Kamera („Webcam“) nimmt Bilder vom Überwachten (bzw je nach Ausrichtung von der unmittelbaren Ungebung des überwachten PCs) auf.
Passwortschutz:	Das Überwachungsprogramm kann nur nach Eingabe eines Passworts gestartet oder in seiner Konfiguration verändert werden.
Diverse Auflistungen:	Protokolliert werden: • alle besuchten Websites • alle gestarteten Programme • alle geöffneten Dokumente • alle ausgedruckten Dokumente

Getestet wurden im Rahmen dieser Arbeit die Funktionen „E-Mail Capturing“, „Conversation Logging“, „Remote Access“, „Key-Logging“, „Screenshots“, Passwortschutz und Diverse Auflistungen. Bei den übrigen Funktionen beziehen sich die Ausführungen auf Angaben der Hersteller.

Die Hersteller der erwähnten Produkte bezeichnen jene oft als „Parental Control Software“ oder als „Internet Security Software“, um den Anschein zu erwecken, sie seien lediglich dazu konzipiert, im Rahmen der elterlichen Erziehungsgewalt durch Überwachung die Sicherheit Minderjähriger zu gewährleisten. Beworben werden sie dann jedoch mit Slogans wie „Is Your Spouse cheating Online?“ („Betrügt Ihre Gattin/Ihr Gatte Sie online?“), woraus sich ein wahrscheinlich in der Realität wesentlich bedeutenderer Verwendungszweck erahnen lässt.

Freilich hat der Markt auf diese Entwicklung mit der Bereitstellung eines „Gegenmittels“, der sogenannten „Anti Spy Software“ reagiert. Programme mit Namen wie „Pest Patrol“, „NetCop“, „SpywareKilla“, „SpyRemover“, „Spy Sweeper“, „Spy Stopper“, „Personal Antispy“, „Keylogger Hunter“, „Keylogger Killer“, „SpywareBlaster“, „Spy Detect“ oder „Spy Sweeper“ – um nur einige zu nennen – werben damit, installierte „Spy Software“ zu erkennen und vom PC zu eliminieren, während Hersteller von „Internet Monitoring Software“ sich in der Präsentation ihrer Produkte damit brüsten, dass jene von „Anti Spy Software“ nicht erkannt und entfernt werden können. Die tatsächliche Situation entspricht wahrscheinlich dem Wettlauf zwischen Programmierern von Computerviren und Produzenten von „Anti Viren Software“, man denke dabei beispiels-

weise an den als Liebesbrief (besser: „Liebesmail“) getarnten Massen-Virus namens "Loveletter", der im Mai 2000 ganze Netzwerke lahm legte und von der damals gebräuchlichen „Anti Viren Software“ nicht erkannt und eliminiert werden konnte. Es ist anzunehmen, dass sowohl die Programmierer von „Internet Monitoring Software“ als auch die Programmierer von „Anti Spy Software“ die Entwicklung der Produkte der „Gegenseite“ beobachten und darauf mit Gegenstrategien reagieren.

3.1 Das Programm „IamBigBrother“

Das Programm „IamBigBrother“ wurde vom Verfasser erworben und einem ausführlichen Test unterzogen[21]. Erhältlich ist die Software entweder direkt über die Homepage des Herstellers (http://www.iambigbrother.com) zu einem Preis von 29,99 USD oder über diverse Vertriebsgesellschaften, die freilich einen Aufschlag auf diesen Preis verrechnen. Bezeichnet wird das Produkt als „Parental Internet Control Software“, die auf der Homepage angebotene „Flash Demo“[22] zeigt ein – offensichtlich unmündiges – Mädchen, das mit einem Unbekannten im Chat ein Treffen vereinbart. Der Unbekannte entpuppt sich im folgenden als Erwachsener, durch dessen düsteres Aussehen zu bedrohlich klingender Musik der Eindruck eines geplanten Verbrechens suggeriert wird. Weiters werden die Funktionalitäten des Programms ausführlich anhand von „Screenshots“ beschrieben. Der Erwerb erfolgt durch direkten Download und Bezahlung per Kreditkarte, die heruntergeladene Installationsdatei hat eine Größe von 3,35 MB.

Während der Installation kreiert das Programm neue Ordner, die tief in die Windows-Ordnerhierarchie hineinreichen und teilweise als Inhalt nur jeweils einen neuen Ordner enthalten (der vollständige Pfad lautet: C:\WINDOWS\system32\fonts\system\explorer\mru). Im Ordner „mru“ werden schließlich das Programm abgelegt und die Ergebnisse der Überwachungsvorgänge gespeichert. Diese Vorgehensweise hat offensichtlich den Zweck, den Ort des Programms zu verschleiern und damit dessen Auffindbarkeit zu erschweren. Unmittelbar nach der Installation steht dem User auf dem Desktop ein Dokument zur Verfügung, in dem beschrieben wird, wie man „IamBigBrother“ startet: Man öffnet das Startmenü, klickt das Feld „Ausführen“ und

[21] Die Tests erfolgten unter dem Betriebssystem Windows XP (Home Edition), die getestete Version ist IamBigBrother 9.0.

[22] Dabei handelt es sich um einen kurzen Zeichentrickfilm mit Ton, der durch die Software „Macromedia Flash Player“, die üblicherweise auf Home-PCs installiert ist, wiedergegeben wird.

gibt im erscheinenden Dialogfenster „cpanel“ ein, daraufhin erscheint die Aufforderung zur Eingabe des Passworts (in der Grundeinstellung lautet das Passwort „iambigbrother“, dieses kann jedoch jederzeit leicht geändert werden). In einem Setupprozess können die Feineinstellungen zu den unten näher beschriebenen Funktionalitäten vorgenommen werden. Danach beginnt das Programm automatisch mit jedem Start des PC zu laufen und protokolliert unbemerkt die Aktivitäten des jeweiligen Benutzers.

3.1.1 Die Aufzeichnung von Kommunikationsvorgängen mit „IamBigBrother“

3.1.1.1 E-Mail (Funktion „E-Mail Capturing“)

Bei der Aufzeichnung von E-Mails ist zu unterscheiden zwischen solchen, die mit einem E-Mail-Programm (E-Mail-Client) wie Outlook-Express versandt oder abgerufen werden und solchen, die als „Webmail“ direkt über eine Homepage in einem Browserfenster versandt oder abgerufen werden. Weiters ist zu unterscheiden, ob der E-Mail-Server vom Provider des Users (zB Chello) oder von einem Gratisanbieter (zB Hotmail) zur Verfügung gestellt wird. Eine abgesandte E-Mail wird in jedem Fall zuerst auf dem E-Mail-Server des Anbieters zwischengespeichert, für den Abruf stehen im Folgenden verschiedene Verfahren zu Verfügung. Üblicherweise werden E-Mails, die am E-Mail-Server eines Providers gespeichert sind, mit einem E-Mail-Programm abgerufen, jedoch ermöglichen fast alle Provider mittlerweile ihren Kunden, auch über Web-Mail, dh ohne Verwendung eines E-Mail-Programms über den Browser auf ihr E-Mail-Konto zugreifen zu können. Andererseits können E-Mails, die auf dem E-Mail-Server eines Gratisanbieters gespeichert sind, meistens auch über ein E-Mail-Programm abgerufen werden. Ob vor jeder Abfrage des E-Mail-Kontos erst ein Passwort eingegeben werden muss, ist bei Verwendung eines E-Mail-Programms vom User in der Konfiguration festzulegen. Erfolgt der Zugang zum E-Mail-Konto über eine Website, muss idR ein Passwort eingegeben werden, doch ist auch hier bei manchen Anbietern die Voreinstellung möglich, dass der User schon durch den Aufruf der Website direkt zu seinem E-Mail-Konto geleitet wird. Solche Einstellungen sind freilich nur auf dem PC, an dem sie vorgenommen wurden, wirksam.

„IamBigBrother“ protokolliert sowohl E-Mails, die von einem Webmail-Account über den Browser[23] verschickt oder abgerufen werden, als auch solche, die mit einem E-Mail-Programm verschickt oder abgerufen werden, beschränkt sich dabei jedoch auf bestimmte Anbieter[24]. Von der technischen Seite betrachtet wird dabei nicht der Übertragungsweg selbst oder ein bestimmtes Programm überwacht, sondern ausschließlich die Aktion am Bildschirm, dh „IamBigBrother“ ordnet die Bildschirmaktivität den einzelnen Programmen zu und hält die Bildschirmausgabe fest, wobei jedoch nicht auf die Kommunikationsschnittstellen (die sogenannten „Ports“), die den PC mit dem Internet verbinden, zugegriffen wird. Eine einlangende E-Mail wird daher immer erst dann aufgezeichnet, wenn sie am Bildschirm geöffnet wird, eine verschickte hingegen, *bevor* sie tatsächlich übermittelt wird.[25]

E-Mail-Verkehr, der über das im Privaten Bereich wohl am häufigsten eingesetzte Programm „Outlook Express“[26] abgewickelt wird, wird lückenlos aufgezeichnet. Startet der Überwachende nun „IamBigBrother“ zur Auswertung seines Überwachungsvorganges, wählt er zunächst den Tag, dessen Aktivität er angezeigt sehen möchte. Unter der Schaltfläche „Outlook Express“ sieht er zunächst, wie viele E-Mails geöffnet und versendet wurden (vgl Abb 1).

[23] Die Tests wurden unter Verwendung des Browsers Internet Explorer, Version 6.0 durchgeführt.

[24] Wird die Aktivität des Überwachten in einem bestimmten Programm, Chat oder Instant Messaging System bzw auf einer bestimmten Website nicht direkt und zur Gänze von „IamBigBrother“ aufgezeichnet, so werden jene im folgenden als „nicht protokollierte“ Dienste bezeichnet.

[25] Die Erläuterungen zur von „IamBigBrother“ angewandten Technik des Aufzeichnens erhielt der Verfasser im Wege des Schriftverkehrs per E-Mail vom 15. und 16. 7. 2003 von Herrn Dipl.-Inform. (FH) Gerrit Wiegand, dem an dieser Stelle herzlich für seine Hilfe und die prompten Antworten auf die entsprechenden Anfragen gedankt sei. Herr Dipl.-Inform. (FH) Wiegand ist Geschäftsführer der mainis IT-Service GmbH in Offenbach am Main, Deutschland, und war von 1999 bis 2001 an der Entwicklung von "quid! – Das Siegel für Qualität im Datenschutz" (einem Verfahren zur Bewertung von Datenschutz-Standards in Unternehmen, online: http://www.quid.de) als wissenschaftlicher Mitarbeiter beteiligt. Sein Tätigkeitsschwerpunkt liegt neben der Entwicklung von Internet-Lösungen im Bereich des (Arbeitnehmer-) Datenschutzes ua in Form von Publikationen und gutachterlichen Tätigkeiten („Im Netz@work“, erschienen 2003 im VSA-Verlag; „Der Chef surft mit“, online: http://www.onlinerechte-fuer-beschaeftigte.de/more/software/download/der_chef_surft_mit.pdf).

[26] Die Tests wurden unter Verwendung des Programms Outlook Express, Version 6.0 durchgeführt.

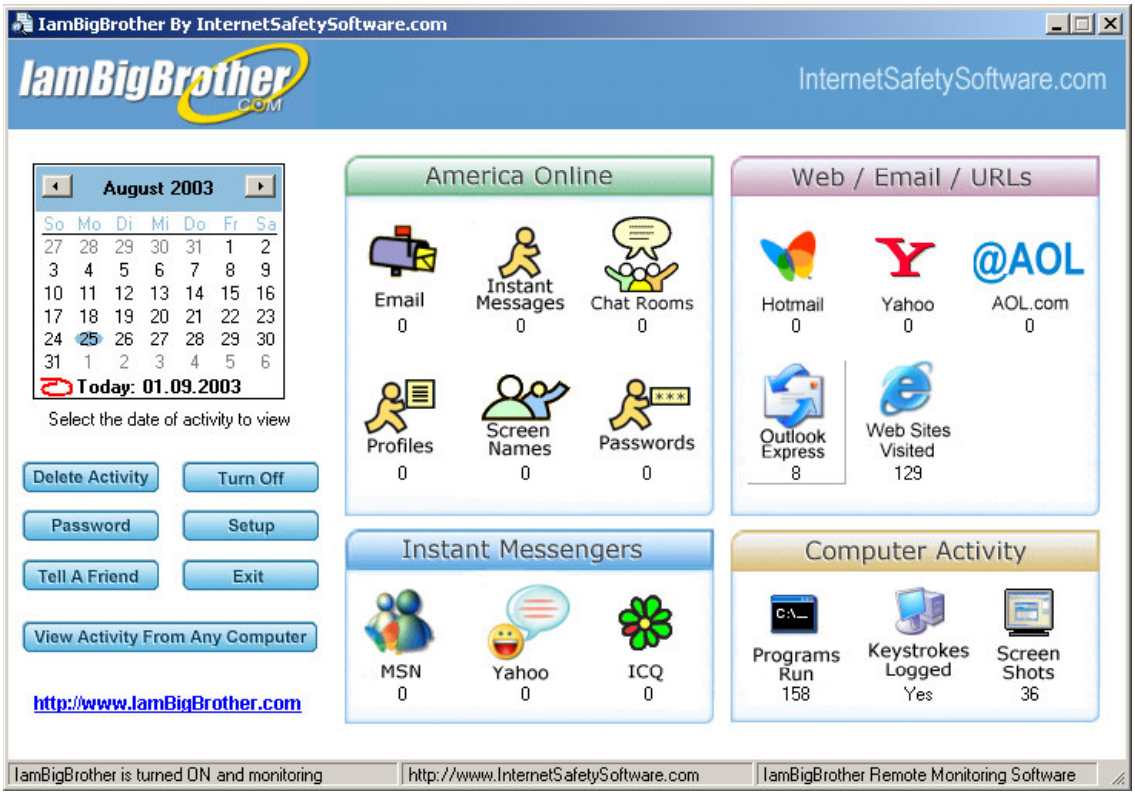

Abb 1: Die Benutzeroberfläche von „IamBigBrother“

Nach einem Klick auf diese Schaltfläche erscheint eine Liste, die in einer Spalte die jeweilige Uhrzeit, zu der die E-Mail verschickt oder geöffnet wurde, und in der nächsten die entsprechende Aktivität („Incoming Outlook Email Read“ oder „Outgoing Outlook Email Composed“) auflistet (vgl Abb 2).

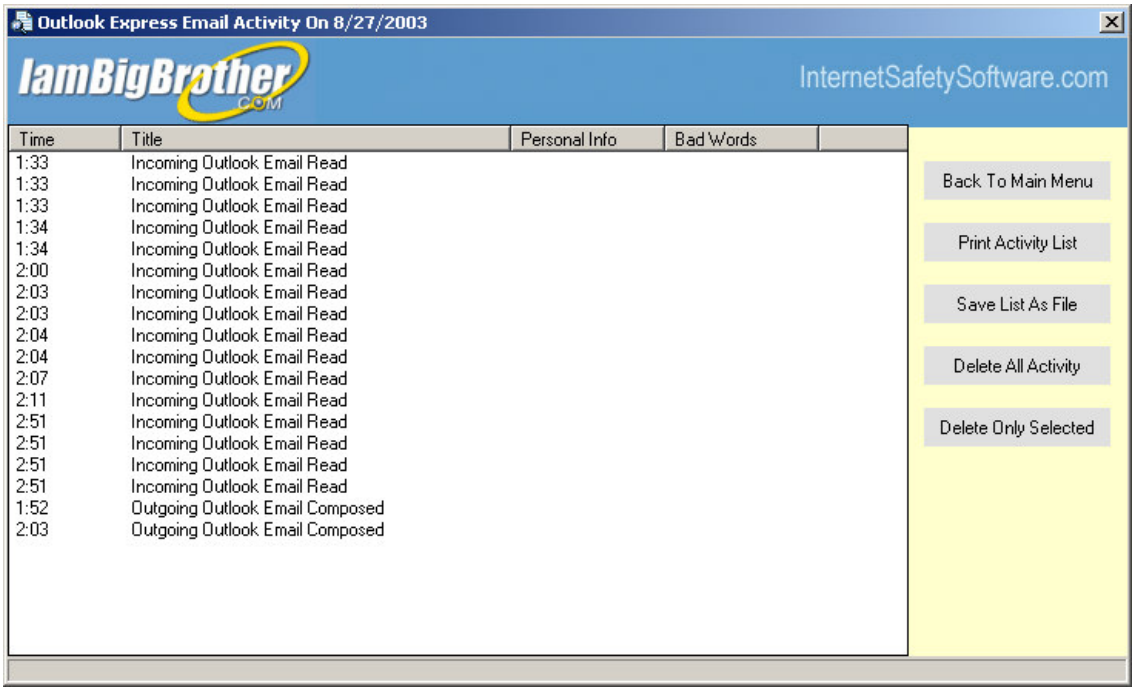

Abb 2: Liste der Aktivitäten im Programm „Outlook Express“

Durch Doppelklick in eine der Zeilen erscheint ein neues Fenster, das bei empfangenen E-Mails unter dem Absender, dem Betreff und der Uhrzeit des Empfangs den Inhalt der E-Mail anzeigt, und zwar exakt in der Formatierung und Farbgestaltung, wie sie für den Überwachten auf dem Bildschirm sichtbar war (vgl Abb 3).

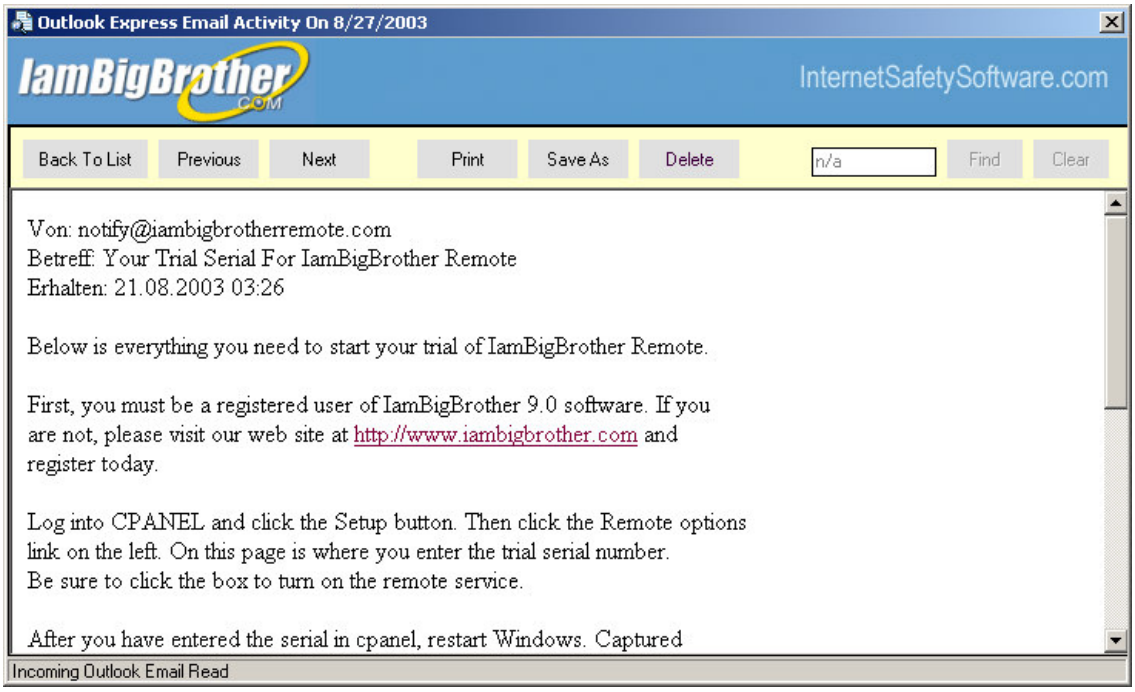

Abb 3: Aufzeichnung einer mit „Outlook Express“ empfangenen E-Mail

Ebenso verhält es sich bei verschickten E-Mails, neben dem Inhalt werden der Absender und der Betreff angegeben, der Empfänger jedoch nur, wenn er vor dem Versenden über die Tastatur eingegeben wurde, also dann nicht, wenn der Absender die „Reply“ Funktion benützt oder die E-Mail durch direktes Anklicken einer E-Mail-Adresse, die im Browser als Hyperlink angezeigt wurde, verschickt hat.

Benützt der Überwachte einen Webmail-Account zum Empfangen und Versenden seiner E-Mails, wird der Inhalt der gesamten Website (ohne Symbolleisten) im Zeitpunkt des Versendens bzw des Empfangs aufgezeichnet und – wenn auch teilweise in einem anderen Schriftbild – wiedergegeben (vgl Abb 4).

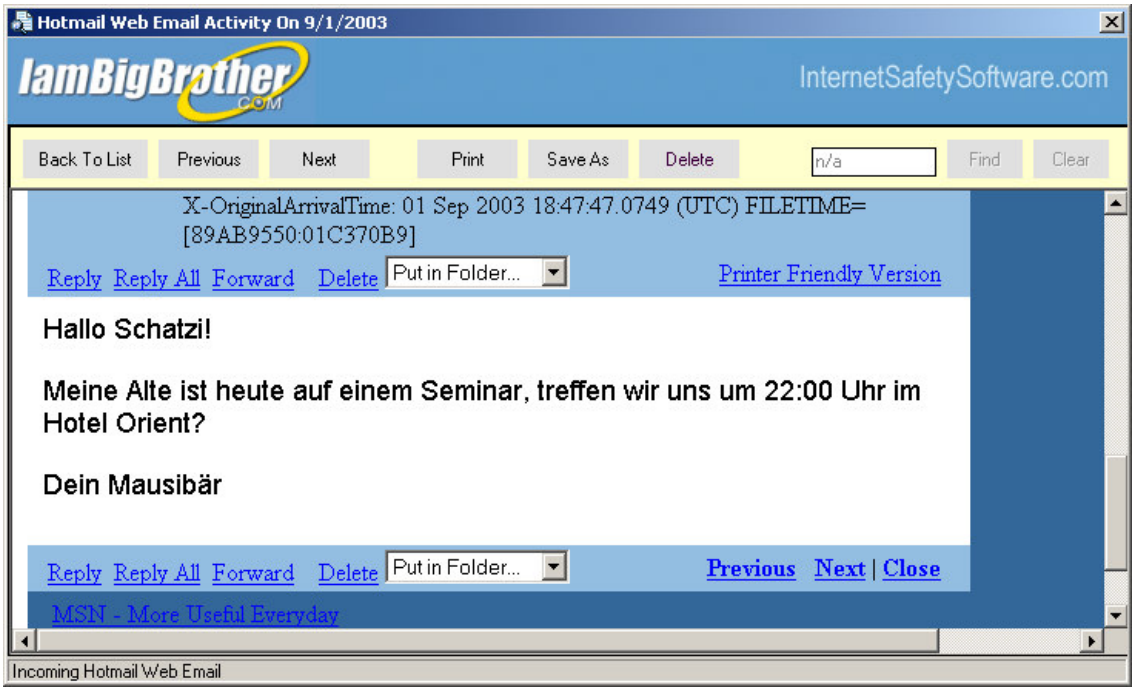

Abb 4: Aufzeichnung einer mit „Hotmail“ empfangenen E-Mail

Die Auswertung des Überwachungsvorgangs erfolgt hier wie oben beschrieben durch Auswahl der anzuzeigenden E-Mail aus einer Liste nach einem Klick auf die Schaltfläche des Webmail-Anbieters. Im Fall von „IamBigBrother“ stehen hier „Hotmail“, „Yahoo“ und „AOL“ zur Auswahl (vgl Abb 1).

3.1.1.2 Chat und Instant Messaging (Funktion „Conversation-Logging“)

„IamBigBrother“ protokolliert Konversationen, die über die Instant Messaging Systeme der Anbieter „ICQ“, „MSN“ und „Yahoo“ geführt werden und zeichnet dabei sowohl empfangene als auch abgeschickte Nachrichten auf. Die hierbei angewandte Technik entspricht der bei der Aufzeichnung von E-Mails beschriebenen. Der Überwachende sieht auf den einzelnen Schaltflächen, auf welchen das Logo des jeweiligen Dienstanbieters abgebildet wird, die Anzahl der geführten Unterhaltungen, durch Klick darauf erscheint eine Liste, die den Beginn der Konversation und den Gesprächspartner (bzw dessen „Nickname“, das ist der Name, den der Überwachte oder dessen Gesprächspartner gewählt hat) anzeigt, durch einen Doppelklick auf die ausgewählte Unterhaltung wird in sehr übersichtlicher Form der Dialog dargestellt, zu jeder Nachricht wird auch die exakte Zeit des Abschickens aufgelistet (vgl Abb 5).

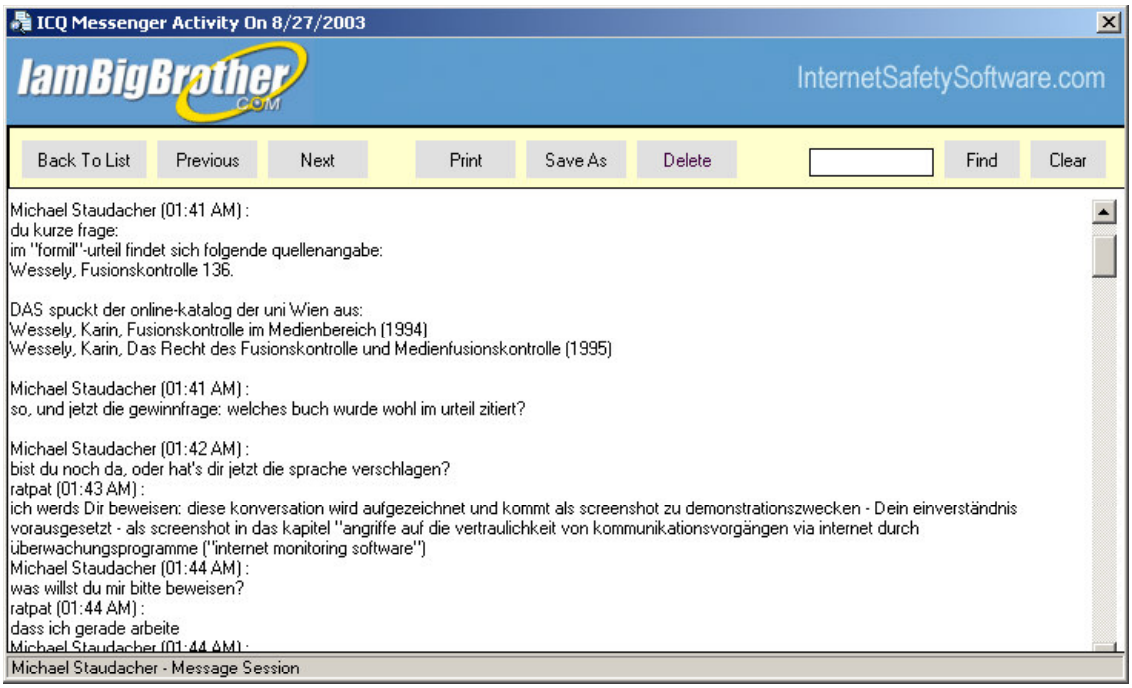

Abb 5: Auszug aus der Aufzeichnung einer über „ICQ" geführten Unterhaltung

3.1.1.3 „Key-Logging"

Über die Schaltfläche „Keystrokes Logged" gelangt der Überwachende zu einer Liste, in der alle Tastatureingaben des Überwachten aufgelistet sind, und zwar unter Angabe der Uhrzeit und des Programms bzw der Website, in dem bzw der jener etwas geschrieben hat. So kann der Überwachende auch Nachrichten, die über einen nicht protokollierten Dienst versendet wurden, nachträglich lesen. Weiters werden – fast[27] – alle vom Überwachten eingegebenen Passwörter aufgezeichnet, anhand deren Verbindung mit dem Programm bzw der Website kann der Überwacher leicht zuordnen, wozu diese Passwörter dienen. Dies eröffnet dem Überwacher natürlich die Möglichkeit, mithilfe eines so erlangten Passworts unbemerkt in E-Mail-Accounts des Überwachten einzudringen und unabhängig vom Abruf durch den Berechtigten dessen Korrespondenz zu lesen.

[27] Siehe dazu unten unter Punkt 3.2.

3.1.1.4 Screenshots („Screen Capturing“)

“IamBigBrother” ermöglicht es dem Anwender, auszuwählen, in welchen zeitlichen Abständen (alle 5, 10, 15, 30 oder 60 Minuten) Screenshots angefertigt werden sollen, diese werden „Timed Screenshots“ genannt. Auf diese Weise können Chats und über die Tastatur geführte Videokonferenzen, oder zumindest Ausschnitte daraus, festgehalten werden, die über einen nicht protokollierten Dienst geführt werden, wobei sowohl gesendete als auch empfangene Mitteilungen aufgezeichnet werden. Weiters kann eine Liste von Worten, sogenannten „Keywords“ erstellt werden, bei deren Eingabe sofort ein Screenshot angefertigt wird. Für die Protokollierung von diskretionsrelevanten Inhalten eignen sich dabei zB Grußformeln, Abschiedsformeln, Namen, Telefonnummern sowie alle generell vom Überwachten häufig in bestimmten Situationen verwendeten Ausdrücke. Bei der Auswertung wird dem Überwachenden eine Liste mit „Thumbnails“[28] unter Angabe der jeweiligen Uhrzeit, zu der diese angefertigt wurden, und der Tatsache, ob es sich um einen „Timed Screenshot“ oder um einen Screenshot handelt, der aufgrund der Eingabe eines „Keywords“ angefertigt wurde, angezeigt. In letzterem Fall wird unmittelbar unter dem „Thumbnail“ auch das eingegebene „Keyword“ gelistet.

Einen Überblick über sämtliche Aktivitäten, die der Überwachte in einem passwortgeschützten Bereich ausübt, erhält der Überwachende durch Kombination der beschriebenen Funktionalitäten, indem er die mittels der Funktion „Key-Logging“ erlangten Passwörter in die Liste der Worte, nach deren Eingabe ein Screenshot angefertigt wird, aufnimmt. Auf diese Weise werden für den Überwachenden zusätzlich die entsprechende Website bzw das Programm, in der ein Passwort verwendet wird, sowie die dazugehörige Benutzerkennung („User-Name“ oder E-Mail-Adresse) sichtbar.

3.1.2 „Remote Access“

Das Service „Remote Access“ stellt eine Zusatzfunktion des Programms dar, die nicht im Lieferumfang enthalten ist und extra beantragt werden muss. Inhabern der Vollversion wird für eine Periode von zehn Tagen ein kostenloser Test des Features angeboten, danach kostet die Nutzung der Fernabfrage 9,99 USD pro Monat. Die Ergebnisse des Überwachungsvorganges werden

[28] Das sind Bilddateien, die unter starker Verkleinerung in einer Liste angezeigt werden, um einen Überblick über eine größere Menge von Bilddateien zu ermöglichen. Ein Klick auf den „Thumbnail“ führt zur Darstellung der Bilddatei in Originalgröße.

in diesem Fall nicht mehr auf der Festplatte des überwachten PCs, sondern auf einem Server des Anbieters gespeichert und sind weltweit mit jedem Browser abrufbar. Die Umstellung muss im Setup des Programms auf dem überwachten PC vorgenommen werden und ist dort jederzeit wieder rückgängig zu machen. Der Zugang zum Server erfolgt über die website http://www.iambigbrotherremote.com durch Eingabe der E-Mail Adresse des Überwachenden und eines zugeteilten Passworts. Die Benutzeroberfläche ähnelt der des Programms und ist in der gleichen Weise zu bedienen.

Da das Programm die aufgezeichneten Dateien selbständig vom PC des Überwachten an den Server übermittelt, war zusätzlich zu testen, ob eine Firewall[29] Schutz gegen diesen Vorgang bietet. Verwendet wurde das Produkt „ZoneAlarm“[30] der Firma Zone Labs, welches kostenlos zum Download angeboten wird. „ZoneAlarm“ meldet automatisch jeden Versuch eines Programms, sich mit dem Internet zu verbinden, nennt den Namen des Programms und macht die Verbindung von einer Zustimmung des Users abhängig. Im Fall von „IamBigBrother“ meldet „ZoneAlarm“ einen Verbindungsversuch des Programms „WinI“. Lässt der User die Verbindung nicht per Mouseclick zu, werden keine Dateien übertragen und der Überwachende erhält keine Ergebnisse des Überwachungsvorgangs. Allerdings bieten die meisten Firewalls die Möglichkeit, im Voraus bei der Zulassung von Verbindungen zwischen Programmen zu differenzieren und für jedes Programm einzeln festzulegen, ob es sich mit dem Internet verbinden darf, ohne davor den User nach Erlaubnis zu fragen. Nimmt der Überwachende diese Einstellung für „IamBigBrother“ vor, wozu er anlässlich der Installation der Überwachungssoftware ja Gelegenheit hat, bemerkt dies der Überwachte nur dann, wenn er in seiner Firewall die Liste der Programme, die sich selbständig verbinden können, aufruft. Dadurch, dass sich „IamBigBrother“ dort aber „WinI“ nennt, kann er daraus keine Rückschlüsse darauf ziehen, dass er überwacht wurde.

[29] Eine Firewall (engl. "Brandmauer") ist ein Filter, der Hacker-Angriffe, Viren und unberechtigte Zugriffe auf einen einzelnen Rechner oder ein ganzes Netzwerk verhindert. Firewalls können entweder als reine Software-Lösung installiert werden, oder aber eine Kombination von Soft- und Hardware bilden. Die reine Software-Lösung ist iA auch die billigste und bietet je nach Preisklasse mehr oder weniger effektiven Schutz. Es gibt aber auch sehr ordentliche Firewalls kostenlos im Internet zum Download. (Definition von: http://www.wdr.de/themen/_komponenten_/stichwort/computer/internet/umfrage_kriminalitaet/firewall.jhtml?rubrikenstyle=computer).

[30] Online: http://www.zonelabs.com; Getestet wurde die Version 3.7.202.

3.1.3 „IamBigBrother“ und „Anty Spy Ware“

Getestet wurde im Rahmen dieser Arbeit die Gratisversion des Programms „Spy Sweeper“[31] der Firma Webroot Software. Dieses Programm war in der Lage, „IamBigBrother“ aufzuspüren und zu isolieren bzw zu eliminieren. Allerdings ist nicht davon auszugehen, dass der „durchschnittliche User“ neben „Anti Viren Software“, welche auf Überwachungsprogramme meistens nicht reagiert,[32] und einer Firewall auch regelmäßig „Anti Spy Software“ einsetzt.

3.2 Exkurs: „IamBigBrother“ und Kryptographie

Unter Kryptographie versteht man die Verschlüsselung und Entschlüsselung von Daten. Vertrauliche Inhalte werden dabei so verändert, dass sie bis zur Entschlüsselung nicht lesbar sind. Um zu untersuchen, inwieweit Kryptographie geeignet ist, die Vertraulichkeit von Nachrichten gegen mittels „Internet Monitoring Software“ durchgeführte Überwachungsmaßnahmen zu sichern, wurde vom Verfasser das populäre Programm „Pretty Good Privacy“ („PGP“)[33] installiert und getestet.

PGP verwendet ein asymmetrisches Verschlüsselungsverfahren (oftmals auch als „Public-Key-Verfahren“ bezeichnet), bei dem sowohl Sender als auch Empfänger über ein Schlüsselpaar, bestehend aus je einem öffentlichen und einem privaten Schlüssel, verfügt. Diese Schlüsselpaare wirken derart zusammen, dass eine mit dem privaten Schlüssel einer Person verschlüsselte Nachricht nur mit dem öffentlichen Schlüssel derselben Person wieder entschlüsselt werden kann. Verschlüsselt der Absender also die Nachricht mit dem öffentlichen Schlüssel des Empfängers, dann kann die Nachricht nur mit dem privaten Schlüssel des Empfängers wieder entschlüsselt werden. Der Vorteil dieses Verfahrens liegt darin, dass die Kommunikationspartner nur ihre öffentlichen Schlüssel austauschen müssen, der private Schlüssel jedoch geheim bleibt und nur für *eine* Person, nämlich den Inhaber, zugänglich sein soll.

Dem Inhaber eines privaten Schlüssels stehen mehrere Möglichkeiten zur Verfügung, sich durch die Auswahl eines geeigneten Speichermediums gegen die

[31] Online: http://www.webroot.com; Getestet wurde die Version 2.1.0.
[32] Während der Tests wurde die leistungsstarke und regelmäßig aktualisierte „Anti Viren Software“ „Norton“ der Firma Symantec verwendet. Diese reagierte nicht auf die Installation und den Betrieb von „IamBigBrother“.
[33] Getestet wurden das Produkt PGP 8.0.1 in der Freeware-Version (erhältlich über die Website http://www.pgpi.com) sowie die kostenpflichtige Version PGP Personal 8.0 (erhältlich über die Website http://www.pgp.com).

unbefugte Benutzung seines privaten Schlüssels abzusichern: Die höchste Sicherheit bietet dabei die Speicherung auf einem externen Medium wie zB einer Chipkarte, die bei Verwendung des Schlüssels in ein an den PC angeschlossenes Lesegerät eingegeben werden muss. Diese Methode bedingt freilich einen gewissen Zeitaufwand und einen nicht unerheblichen Kostenaufwand für das Lesegerät, das überdies erst installiert werden muss, und ist daher im privaten Bereich wenig verbreitet. Bequemer erscheint die Speicherung des privaten Schlüssels auf der Festplatte des Inhabers. In diesem Fall hat der Inhaber die Wahl, ob die Eingabe einer von ihm gewählten Passphrase Bedingung für jeden Ver- bzw Entschlüsselungsvorgang sein soll. Im Test zeigte sich, dass „IamBigBrother“ nicht imstande ist, diese Passphrase mittels der Funktion „Key-Logging“ aufzuzeichnen, PGP bietet demnach offensichtlich bereits einen gewissen Schutz gegen derartige Überwachungsmaßnahmen.

Durch die Funktion „E-Mail-Capturing“ jedoch werden sowohl verschickte als auch empfangene E-Mails in der verschlüsselten Form aufgezeichnet. Hat der Überwachte seinen privaten Schlüssel auf der Festplatte gespeichert und benutzt er keine Passphrase, kann der Überwachende die aufgezeichneten E-Mails auch entschlüsseln. Benutzt der Überwachende die Funktion „Remote Access“ und hat er keinen Zugriff auf den PC des Überwachten, hat er auch keinesfalls Zugang zum dessen privatem Schlüssel und kann daher vom Überwachten empfangene E-Mails nicht entschlüsseln. Da PGP seine Funktionalitäten in E-Mail-Programme wie Outlook Express integrieren kann, hat der Anwender (bei Verwendung der kostenpflichtigen Version) die Möglichkeit, die Voreinstellungen so zu definieren, dass eine abgerufene verschlüsselte E-Mail automatisch und ohne weitere Zwischenschritte beim Öffnen entschlüsselt angezeigt und eine verschickte nach Auswahl des passenden öffentlichen Schlüssels automatisch verschlüsselt wird. „IamBigBrother“ zeichnet in diesen Fällen jeweils nur den verschlüsselten Text auf und der Überwachende hat selbst dann, wenn er über das Passwort zum E-Mail-Account des Überwachten verfügt, keine Möglichkeit, Kenntnis vom Inhalt einlangender Nachrichten zu nehmen. E-Mails, die der Überwachte *versendet*, werden jedoch bereits vor der Verschlüsselung, nämlich während sie verfasst werden, mittels der Funktion „Key-Logging“ protokolliert.

Zusammenfassend ist also festzuhalten, dass Kryptographie – sofern der Überwachte die richtigen Voreinstellungen bezüglich automatischer Entschlüsselung und Notwendigkeit der Eingabe einer Passphrase wählt – für *empfangene* E-Mails einen gewissen Schutz gegen eine Überwachung mit „IamBigBrother“ bietet.

3.3 Untergruppen des Zugangs zu diskretionsrelevanten Inhalten

Für die nachfolgende sachverhalts- und tatbestandsbezogene Untersuchung des strafrechtlichen Schutzes gegen die Überwachung privater Kommunikation mittels „IamBigBrother“ sind aufgrund der engen Umschreibungen der Angriffshandlungen in den jeweiligen Deliktstatbeständen Fallgruppen zu bilden, anhand derer eine Subsumtion vorgenommen werden kann.

3.3.1 Fallgruppe I: Zugang zu direkt aufgezeichneten E-Mails und Konversationen

Diese Fallgruppe umfasst das direkte Aufzeichnen ganzer ausgehender oder einlangender E-Mails mittels „IamBigBrother“, die entweder durch ein E-Mail-Programm oder den Webbrowser versendet oder empfangen werden, ohne dass der Überwachende dazu auf ein Passwort zurückgreifen müsste. Dabei wird die Funktion „E-Mail Capturing“[34] angewandt. Weiters gehört zu dieser Fallgruppe die Aufzeichnung von mittels „Instant Messaging Systemen“ versendeten und empfangenen Nachrichten oder ganzer Dialoge, die durch die Funktion „Conversation-Logging“[35] protokolliert werden.

3.3.2 Fallgruppe II: Zugang zu einem E-Mail-Account durch ein mittels „IamBigBrother“ erlangtes Passwort

In dieser Fallgruppe ruft der Überwachende durch ein E-Mail-Programm oder den Webbrowser – unter Verwendung eines mittels der Funktion „Key-Logging“[36] erlangten Passworts – an den Überwachten versendete E-Mails ab. Hat der Überwachte selbst die E-Mails noch nicht abgerufen, erfolgt der Empfang direkt vom Mailserver des Überwachten, hat der Überwachte die entsprechenden E-Mails bereits davor empfangen, werden diese für den Überwachenden nur dann zugänglich, wenn der Überwachte sie noch nicht vom Mailserver gelöscht hat. Zu E-Mails, die der Überwachte versendet hat, gelangt der Überwachende nur dann, wenn der Überwachte jene gespeichert hat.

[34] Vgl oben unter Punkt 3.1.1.1.
[35] Vgl oben unter Punkt 3.1.1.2.
[36] Vgl oben unter Punkt 3.1.1.3.

3.3.3 Fallgruppe III: Zugang zu einem durch einen „Screenshot“ oder durch die Funktion „Key-Logging“ festgehaltenen Kommunikationsinhalt

Der Überwachende verfolgt den Inhalt einer Nachrichtenübermittlung, indem er sich eine durch die Funktion „Screen Capturing“[37] festgehaltene Bilddatei oder einen durch die Funktion „Key-Logging“[38] protokollierten Text anzeigen lässt.

4 Ist private elektronische Kommunikation strafrechtlich gegen mittels „Internet Monitoring Software“ vorgenommene Überwachungsmaßnahmen geschützt?

Im folgenden wird anhand der in Frage kommenden Tatbestände untersucht, ob der Einsatz von „IamBigBrother“ zur Aufzeichnung von diskretionsrelevanten Inhalten im privaten Bereich mit den Mitteln des geltenden Strafrechts sanktioniert werden kann. Aus praktischen Gründen muss sich die Analyse dabei hier auf die Funktionalitäten dieses Programms beschränken, da zur Vornahme der Subsumtion auch die genauen technischen Auswirkungen des Vorgehens des Täters bekannt sein müssen.

4.1 Kernstrafrecht

4.1.1 Die bereits vor der Einführung eines „Computerstrafrechts“ vorhanden gewesenen Tatbestände

Die Vertraulichkeit von Kommunikationsvorgängen, die nicht über das Internet abgewickelt werden, waren bereits vor der Entwicklung eines speziellen Computerstrafrechts durch mehrere strafrechtliche Bestimmungen gegen Indiskretionen geschützt, zu nennen ist hier vor allem der Schutz des Briefgeheimnisses (§ 118 StGB) sowie das Fernmeldegeheimnis (heute „Telekommunikationsgeheimnis“, § 119 StGB). Freilich unterliegen auch die neuen Kommunikationsmedien rechtlicher Regulierung, sodass die Parole vom „Internet als rechtsfreier Raum“ das Wunschdenken einiger Pioniere dieser Technologien geblieben ist.[39] Bisweilen wird auf die „Medienneutralität des Rechts“ verwiesen und versucht, bisher unbehandelte Rechtsfragen des Internets unter Heranziehung der

[37] Vgl oben unter Punkt 3.1.1.4.
[38] Vgl oben unter Punkt 3.1.1.3.
[39] *Brenn* [Hrsg], ECG (2002) 6.

traditionellen rechtlichen Regelungsmechanismen und Methodik zu lösen. Auch *Schmölzer* [40] führt dazu aus: *„Beim Internet handelt es sich um keinen „rechtsfreien Raum": Die geltenden Gesetze sind anzuwenden; allenfalls gilt es, im Dienste der Rechtssicherheit Lücken zu schließen und Interpretationsunsicherheiten zu beseitigen, die durch Entwicklungen im Technologiebereich entstanden sind."* Im Strafrecht ist hier jedoch große Vorsicht geboten, denn der Auslegung von Straftatbeständen sind aufgrund rechtsstaatlicher Anforderungen enge Grenzen gesteckt, eine automatische Anwendung der strafrechtlichen Normen auf neue, bislang ungeregelte technische Vorgänge, die in der sprachlichen Formulierung der entsprechenden Tatbestände keine Deckung mehr finden, ist – mag die Wertungslage auch völlig gleichartig erscheinen – wegen der strengen Auslegungsregeln und des Analogieverbots zuungunsten des Täters nicht zulässig. § 1 StGB verbietet idS nicht nur täterbelastende Analogie, sondern überhaupt jede Methode zur Ausfüllung strafrechtlicher Regelungslücken zu Lasten des Täters.[41]

4.1.1.1 Verletzung des Briefgeheimnisses und Unterdrückung von Briefen (§ 118 StGB)

Der strafrechtliche Schutz des Briefgeheimnisses, eines der ältesten Indiskretionsdelikte, war vor Inkrafttreten des StGB im Gesetz vom 9. April 1870, RGBl Nr 42, zum Schutz des Brief- und Schriftengeheimnisses enthalten, § 118 StGB ist an dessen Stelle getreten. Das Briefgeheimnis ist weiters durch Art 10 des Staatsgrundgesetzes vom 21. Dezember 1867, RGBl Nr 142, und Art 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten[42] (Recht auf Achtung des Privat- und Familienlebens) auf verfassungsrechtlicher Ebene geschützt.

4.1.1.1.1 Darstellung des Tatbestandes

§ 118 StGB unterscheidet je nach Angriffsobjekt und Angriffshandlung vier Deliktsfälle: Abs 1 pönalisiert das Öffnen eines nicht zur Kenntnisnahme durch den Täter bestimmten verschlossenen Briefes oder eines anderen solchen Schriftstückes. Nach Abs 2 macht sich der Täter strafbar, wenn er ein verschlossenes Behältnis, in dem sich ein solches Schriftstück befindet, öffnet oder ein technisches Mittel anwendet, um seinen Zweck ohne Öffnen des Ver-

[40] *Schmölzer*, in: *Jahnel/Schramm/Staudegger* [Hrsg], Informatikrecht[2] (2003) 353.
[41] *Leukauf/Steininger*, StGB[3] § 1 Rz 7.
[42] BGBl Nr 210/1958 zuletzt geändert durch BGBl III Nr 30/1998.

schlusses des Schriftstücks oder des Behältnisses zu erreichen, wobei jedoch die Absicht hinzukommen muss, sich oder einem anderen Unbefugten Kenntnis vom Inhalt des nicht zu seiner Kenntnis bestimmten Schriftstücks zu verschaffen. Abs 3 stellt das Unterschlagen oder sonstige Unterdrücken eines Briefes oder eines anderen Schriftstücks vor Kenntnisnahme durch den Empfänger unter Strafe.

Tatobjekt des § 118 StGB ist ein „verschlossener Brief" oder ein „anderes solches Schriftstück", wobei der Brief begrifflich nur eine Unterart des Schriftstücks darstellt.[43] Es ist also zu untersuchen, ob die E-Mail oder eine sonstige über das Internet vom Absender zum Empfänger übertragene Nachricht unter diese Begriffe subsumiert werden kann.

4.1.1.1.2 Interpretationsmethoden

4.1.1.1.2.1 Teleologische Interpretation

Die teleologische Interpretation stellt auf den Sinn und Zeck der Rechtsnorm ab. Die Abs 1 und 2 bezwecken den Schutz der Vertraulichkeit von durch Schriftzeichen ausgedrückten gedanklichen Inhalten[44] vor Kenntnisnahme durch Personen, für die jene Mitteilung nicht bestimmt ist. Ein Eindringen in die Privat- und Geheimsphäre durch Unbefugte soll verhindert werden, wobei es jedoch auf den Inhalt der Mitteilung nicht ankommt.[45] Abs 3 bezweckt den Schutz des Empfängers vor Vereitelung der Kenntnisnahme eines an ihn abgesandten gedanklichen Inhaltes und stellt damit auf die Sicherstellung des schriftlichen Kommunikationsvorganges als solchen ab.

Nach diesen Gesichtspunkten scheint nun die E-Mail bzw eine sonstige über das Internet übermittelte Nachricht als durch Schriftzeichen ausgedrückter gedanklicher Inhalt ebenso schützenswert wie ein verschlossener Brief oder ein anderes solches Schriftstück, da jede Kenntnisnahme durch Unbefugte ein Eindringen in die Privat- und Geheimsphäre des Absenders bzw Empfängers befürchten lässt und die Vertraulichkeit der Mitteilung verletzt. Auch bei E-Mails und sonstigen über das Internet übermittelten Nachrichten kann der Übertragungsweg und das Vertrauen der Kommunikationspartner auf den Zugang der Mitteilung beim intendierten Empfänger verschiedenen Angriffen durch Unbe-

[43] *Leukauf/Steininger*, StGB[3] § 118 Rz 4.
[44] *Leukauf/Steininger*, aaO.
[45] *Leukauf/Steininger,* aaO.

fugte ausgesetzt sein, sodass der Zweck der Norm einen strafrechtlichen Schutz der elektronischen Kommunikation zunächst nahe legen würde.

4.1.1.1.2.2 Historische Interpretation

Die historische Interpretation beleuchtet die Entstehungsgeschichte einer Rechtsnorm und orientiert sich an den subjektiven Absichten und Zweckvorstellungen des historischen Gesetzgebers. Als Hilfsmittel werden dabei in erster Linie die Gesetzesmaterialien (zB Erläuternde Bemerkungen zur Regierungsvorlage, Ausschussberichte und stenographische Protokolle zu den Sitzungen des Nationalrates) herangezogen.

Diese Interpretationsmethode führt hier nicht weiter, da zur Zeit der Entstehung der gegenständlichen Norm das Internet – zumindest in seiner heutigen Form – noch nicht existierte und dem historischen Gesetzgeber daher die Kommunikationsmöglichkeiten, die dieses zur Verfügung stellt, gar nicht bekannt bzw bewusst sein konnten.

4.1.1.1.2.3 Wortinterpretation

Im Strafrecht stellt der mögliche Wortsinn der auszulegenden Norm unstrittig die äußerste Grenze für die Auslegung dar.[46] Die Wortinterpretation richtet sich nach der Bedeutung des Wortes im allgemeinen Sprachgebrauch.

Bei E-Mails und sonstigen per Internet versendeten Nachrichten handelt es sich um Datenbündel, die durch verschiedene Technologien (zB Bildschirmausgabe oder Ausdruck) visualisiert werden und mE daher schon nach dem Wortsinn nicht unter den Begriff des „verschlossenen Briefs“ oder „sonstigen Schriftstücks“ subsumiert werden können.

4.1.1.1.3 Exkurs: Bisherige Ansätze zur dogmatischen Einordnung der E-Mail

Vernier/Ebensperger [47] gehen davon aus, dass die Bestimmung des § 118 StGB auf das Internet nicht passt, da E-Mails keine „Schriftstücke“ sind.

[46] *Leukauf/Steininger*, StGB[3] § 1 Rz 10.
[47] *Vernier/Ebensperger*, in: *Brenn* [Hrsg], ECG (2002) 119.

Gassauer-Fleissner [48] vertritt die Ansicht, dass Verletzungen der Vertraulichkeit in Netzwerken als der Verletzung des Briefgeheimnisses vergleichbare Eingriffe aufgrund der sehr konkreten Beschreibung der verpönten Tatbilder nicht dem Tatbestand des § 118 StGB zugeordnet werden können. *Laga* [49] lehnt die Subsumtion des E-Mail-Verkehrs unter das Briefgeheimnis *„im Zweifel“* ab und hält fest, dass eine E-Mail zwar verschlüsselt, aber nie „verschlossen“ sein kann.

Für *Lewisch* [50] liegt das entscheidende Abgrenzungskriterium in der Körperlichkeit, die Subsumtion der E-Mail unter den Begriff des Schriftstückes lehnt er aus diesem Grund ab. Auch nach *Triffterer* [51] besitzen Daten und Programme unabhängig von dem jeweiligen Träger keine Körperlichkeit. *Lichtenstrasser* [52] hingegen sieht die Körperlichkeit als durch die Funktion der Festplatte als „Schriftträger“ hergestellt an, gesteht jedoch ein, dass die E-Mail, solange sie sich am Übertragungsweg befindet, über keinen Schriftträger verfügt. Unter Berufung auf den Zweck des Art 8 Abs 1 EMRK, dessen innerstaatlicher Umsetzung § 118 StGB ua diene, und die GMat zu § 118 StGB behandelt sie die E-Mail als „Schriftstück“ iS jenes Straftatbestandes. Diese Subsumtion erscheint mir jedoch methodologisch verfehlt, da – wie oben ausgeführt – bei der Auslegung von strafrechtlichen Normen die teleologische und die historische Interpretation eine Überschreitung des Wortsinns nicht zu rechtfertigen vermögen.

Obereder [53] stellt zunächst eine „Verwandtschaft“ von E-Mail und Brief fest und lehnt eine Subsumtion von *einfachen* (iSv unverschlüsselten) E-Mails unter § 118 StGB ab, führt aber im folgenden dazu aus: *„„Verschlossen“ wäre ein E-Mail wohl nur dann, wenn es verschlüsselt abgesendet und vom unberechtigten Empfänger entschlüsselt wird.“* Ähnlich zurückhaltend meint *Jahnel* [54]: *„Art 10 StGG erklärt das Briefgeheimnis für unverletzlich und schützt damit die Vertraulichkeit von Briefen, dh von verschlossenen Schriftstücken, deren Inhalt Außenstehenden nicht zur Kenntnis gebracht werden darf. Da elektronische Post kein Kuvert besitzt, fallen (zumindest nicht verschlüsselte) E-Mails nicht unter den Schutz des Briefgeheimnisses. Bei verschlüsselten E-Mails ist zu überlegen, ob nicht der Verschlüsselung der Charakter eines elektronischen „Kuverts“ zukommen könnte.“* Auch Wagner[55] legt sich nicht eindeutig fest:

[48] *Gassauer-Fleissner*, ecolex 1997, 102.
[49] *Laga*, Rechtsprobleme im Internet (1998) 160.
[50] *Lewisch*, WK² § 118 Rz 5.
[51] *Triffterer*, StGB-Komm § 126a Rz 30.
[52] *Lichtenstrasser*, in: *IT-LAW.AT* [Hrsg], e-Mail – elektronische Post im Recht (2003) 138 f.
[53] *Obereder*, E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, RdA 2001, 75.
[54] *Jahnel*, Datenschutz im Internet, ecolex 2001, 84.
[55] *Wagner*, Unbefugter Zugriff auf e-Mail, ecolex 2000, 273.

„§ 118 StGB, der die Verletzung des Briefgeheimnisses unter Strafe stellt, ist auf den unbefugten Zugriff auf e-Mail nicht anwendbar, spricht er doch ausdrücklich vom „verschlossenen Brief". Darunter wird uU verschlüsselte e-Mail zu subsumieren sein, einfache e-Mail, wie sie in den meisten Unternehmen im Einsatz ist, aber sicherlich nicht." Lichtenstrasser [56] lässt den durch die Verschlüsselung zum Ausdruck kommenden Willen des Berechtigten nach Geheimhaltung und das faktische Hindernis, das durch die Verschlüsselung einer Kenntnisnahme vom Inhalt der E-Mail entgegengesetzt wird, für die Subsumtion unter den Begriff des „verschlossenen Schriftstückes" genügen. Unverschlüsselte E-Mails seien hingegen mit Postkarten zu vergleichen. ME ist jedoch auch die Verschlüsselung schon alleine aufgrund des Wortsinnes kein geeignetes Kriterium, das einen eindeutigen Bezug zu § 118 StGB herzustellen vermag. Die Anwendung von Kryptographie bringt zwar einen gewissen Geheimhaltungswillen zum Ausdruck, kommt aber begrifflich nicht einem Verschluss gleich. Zur Entschlüsselung eines Textes sind völlig andere Mittel erforderlich, als zum Öffnen eines verschlossenen Briefs oder Behältnisses. Die Entschlüsselung setzt eine intellektuelle Leistung voraus, die Öffnung eines Briefes oder Behältnisses ist hingegen ein rein mechanischer Vorgang. Da das Strafrecht im Bereich des Schutzes von Kommunikationsinhalten streng nach eng umschriebenen Angriffswegen differenziert, wäre aus diesem Grunde beispielsweise auch die Entschlüsselung des Textes einer verschlüsselten Postkarte nicht durch § 118 StGB pönalisiert.

Der – ebenso für das Zivilrecht getroffenen[57] – Gleichsetzung der unverschlüsselten E-Mail mit einer Postkarte ist mE entgegenzuhalten, dass auch ein verschlossener Brief am Postweg mit zahlreichen Personen in Berührung kommt, die diesen „abfangen" und das Briefgeheimnis verletzen könnten und dieses Risiko dem Absender durchaus bewusst ist. Weiters ist auch nach dem Inhalt der Sendung zu unterscheiden: Die Postkarte reist zwar *offener* als ein verschlossener Brief, dafür aber nicht weniger *sicher*. Da dies auch dem Absender bekannt ist, wird er für vertrauliche Inhalte die Briefform wählen. Der Absender einer E-Mail, der seinen E-Mail-Account durch ein Passwort gesichert wähnt, wird zumindest davon ausgehen, dass ein möglicher Zugriff auf die Kommunikationsinhalte neben Netzwerkadministratoren und Angestellten des Providers auf technisch besonders versierte „Hacker", bzw auf Personen, die eine gewisse kriminelle Energie aufbringen, beschränkt ist. Von einer Postkarte hingegen ist allgemein bekannt, dass jeder physische Kontakt ohne weitere Zwischen-

[56] *Lichtenstrasser*, e-Mail 139 f.

[57] *Vonkilch*, Der Einsatz elektronischer Signaturen aus versicherungsschutzrechtlicher und verbraucherschutzrechtlicher Perspektive, VR 2001, 25; *Menzel*, Elektronische Signaturen, (2000) 22.

schritte gleichzeitig die Möglichkeit verschafft, Kenntnis vom Inhalt zu nehmen, daher wird der Absender jene auch nur dann einsetzen, wenn für ihn die Vertraulichkeit des Inhaltes keine Rolle spielt.

Zusammenfassend ergibt sich daher nach der hier vertretenen Ansicht aus den obigen Ausführungen, dass ein Angriff auf E-Mails unter keinen Deliktsfall des § 118 StGB subsumiert werden kann.

4.1.1.2 Mißbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 Abs 1 und 2 StGB – die Fassung vor dem StrÄG 2002)

§ 120 Abs 1 pönalisiert die Benutzung eines Tonaufnahmegeräts oder Abhörgeräts in der Absicht, sich oder einem anderen Unbefugten durch Aufzeichnen oder Abhören Kenntnis von einer nicht öffentlichen Äußerung eines anderen zu verschaffen. Nach Abs 2 ist zu bestrafen, wer die Tonaufnahme einer nicht öffentlichen Äußerung ohne Einverständnis des Sprechenden einem Dritten zugänglich macht oder jene veröffentlicht.

Leukauf/Steininger [58] führen zu diesem Tatbestand aus: *„Tonaufnahmegerät ist jede Vorrichtung, die Töne oder Tonfolgen so konserviert, dass sie wiederholbar wiedergegeben werden können. Abhörgerät ist jede technische Vorrichtung, durch die Töne über den natürlichen Klangbereich hinaus verstärkt oder übertragen werden."* Dass § 120 Abs 1 und 2 StGB nur das gesprochene Wort schützt, ist herrschende Meinung.[59]

Da „IamBigBrother" keine Töne konserviert, verstärkt oder überträgt, sondern lediglich nicht-akustische Daten aufzeichnet, ist die Bestimmung auf den Einsatz dieses Programms eindeutig nicht anwendbar.

4.1.1.3 Sachbeschädigung (§ 125 StGB)

Zu überlegen ist, ob der Tatbestand der Sachbeschädigung möglicherweise auf die in Fallgruppe II[60] umschriebene Angriffshandlung anwendbar ist, wenn der Täter sich durch ein ohne Wissen des Überwachten aufgezeichnetes Passwort Zugang zu dessen E-Mail-Account verschafft und dort auf dem Posteingangs-

[58] *Leukauf/Steininger*, StGB[3] § 120 Rz 5 f.
[59] *Lewisch*, WK[2] § 120 Rz 1.
[60] Vgl oben unter Punkt 3.3.2.

server gespeicherte E-Mails vor Kenntnisnahme durch den Überwachten löscht.

Das Delikt pönalisiert das Zerstören, Beschädigen, Verunstalten oder Unbrauchbarmachen einer fremden *Sache*. Geschützt sind jedoch nach heute unstrittiger Auffassung nur *körperliche* [61] Sachen, Voraussetzung für eine Beschädigung ist eine Beeinträchtigung der stofflichen Unversehrtheit.[62] Manipulationen, die Schäden nur anrichten, weil sie Daten auf einem Datenträger unbrauchbar machen, sind dem Täter nur nach § 126a StGB anzulasten.[63] Nach *Triffterer* [64] ist für die Abgrenzung ausschlaggebend, dass Daten und Programme unabhängig von dem jeweiligen Träger keine Körperlichkeit besitzen. Der Datenträger selbst bleibt bei der geprüften Angriffshandlung jedoch unversehrt, sodass der Täter nicht wegen einer Sachbeschädigung verurteilt werden kann.

4.1.2 Das Strafrechtsänderungsgesetz 1987

Durch das StRÄG 1987[65] wurden erstmals computerstrafrechtliche Bestimmungen in das StGB eingeführt, die sich der EDV-spezifischen Wirtschaftskriminalität widmen. Neben § 126a StGB (Datenbeschädigung) wurde der Tatbestand des § 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch) geschaffen. Ein näheres Eingehen auf § 148a StGB erübrigt sich für diese Betrachtung, da jener nur mit Bereicherungsvorsatz begangen werden kann und daher eindeutig und ausschließlich den Bereicherungsdelikten zuzuordnen ist.

Aus der Entstehungsgeschichte dieser Tatbestände ist bekannt, dass damals, was die Zielsetzung der neuen Regelungen im Kernstrafrecht betrifft, eine Reduzierung auf Vermögensdelikte und eine Abgrenzung zum Bereich des Datenschutzes angepeilt wurde.[66]

---

[61] *Leukauf/Steininger*, StGB[3] § 125 Rz 2; *Schmölzer*, Informatikrecht[2] 347.
[62] *Bertel*, WK[2] § 125 Rz 3.
[63] *Bertel*, WK[2] § 126a Rz 9; *Triffterer*, StGB-Komm § 126a Rz 111.
[64] *Triffterer*, StGB-Komm § 126a Rz 30.
[65] BGBl 1987/605.
[66] *Jaburek/Schmölzer*, Computerkriminalität (1985) 19 ff; *Schick/Schmölzer*, Das österreichische Computer-Strafrecht – Eine Bestandsaufnahme, EDVuR 199**2**, 107.

4.1.2.1 Datenbeschädigung (§ 126a StGB)

Ebenso auf die in Fallgruppe II[67] umschriebenen Angriffshandlungen bezieht sich die Analyse des § 126a StGB, sofern der Täter Nachrichten vor Kenntnisnahme durch den Überwachten löscht. Nach dieser Bestimmung macht sich strafbar, wer automationsunterstützt verarbeitete, übermittelte oder überlassene Daten verändert, löscht, sonst unbrauchbar macht oder unterdrückt, und einen anderen dadurch schädigt.

Die Subsumtion der E-Mail unter den Begriff der „automationsunterstützt verarbeiteten oder übermittelten Daten", unter den alle auf einer Festplatte gespeicherten Daten fallen,[68] bereitet zunächst kein Problem. Auch, dass der Täter über fremde E-Mails nicht verfügen darf, ist eindeutig. Für das „Unterdrücken" ist entscheidend, dass die betreffenden Daten *„dauernd oder doch zeitweilig dem (jederzeitigen) Zugriff des Verfügungsberechtigten entzogen sind und deshalb von diesem nicht verwendet werden können"* [69]*,* was beim Löschen einer E-Mail vom Server sicherlich der Fall ist.

Fraglich ist allerdings, ob im untersuchten Fall auch der vom Tatbestand geforderte Schaden eintritt. Da dem StGB kein einheitlicher Schadensbegriff zugrunde liegt, ist der hier verwendete Schadensbegriff näher zu untersuchen und deliktsspezifisch einzugrenzen. Dabei zeigt sich, dass § 126a StGB, der als Erfolgsdelikt einzustufen ist,[70] eindeutig einen *Vermögensschaden* fordert [71] und eine Schädigung an einem sonstigen (konkreten) Recht nicht genügt.[72] Nach *Triffterer* [73] muss der Vermögensschaden unmittelbar dadurch entstehen, dass der Täter eine der im Deliktstatbestand umschriebenen Tathandlungen setzt. Geschütztes Rechtsgut des § 126a StGB ist ein spezieller *Vermögenswert*, nämlich das *„Interesse am Fortbestand und an der Verfügbarkeit von Daten"* [74]. Aufgrund jenes Interesses, das neben dem Vermögen geschützt wird, bezeichnet *Triffterer* [75] § 126a StGB als *„eigenständiges Delikt gegen Individualinteressen"*.

---

[67] Vgl oben unter Punkt 3.3.2.
[68] *Bertel*, WK^2 § 126a Rz 1.
[69] *Leukauf/Steininger*, StGB^3 § 126a Rz 12.
[70] *Weiss*, Computerstrafrecht, FJ 1998, 244; *Triffterer*, StGB-Komm § 126a Rz 18.
[71] *Bertel*, WK^2 § 126a Rz 5; *Triffterer*, aaO.
[72] *Leukauf/Steininger*, StGB^3 § 126a Rz 14; *Weiss*, FJ 1998, 244; AA *Lichtenstrasser*, e-Mail 145, die sich allerdings mit dem Schadensbegriff nicht auseinandersetzt.
[73] *Triffterer*, StGB-Komm § 126a Rz 84.
[74] *Schick/Schmölzer*, EDVuR 1992, 107.
[75] *Triffterer*, StGB-Komm § 126a Rz 21.

Daher bleibt ein Täter, der fremde E-Mails ohne den Vorsatz, einen anderen *am Vermögen* zu schädigen, löscht, nach dieser Bestimmung straflos. Handelt der Täter hingegen idS vorsätzlich, macht er sich strafbar, es wird ihm aber zusätzlich der Eintritt eines konkreten Vermögensschadens nachzuweisen sein.

4.1.3 Das Strafrechtsänderungsgesetz 2002

Die Einführung neuer materieller computerstrafrechtlicher Bestimmungen durch das StRÄG 2002[76] erfolgte im wesentlichen in Umsetzung gemeinschaftsrechtlicher und internationaler Verpflichtungen bei der Bekämpfung des Terrorismus, der organisierten Kriminalität und der Computerkriminalität. Zu nennen ist hier insbesondere die Cyber-Crime-Konvention des Europarates vom 23. 11. 2001.[77]

Titel I der CCC widmet sich Taten gegen die Sicherheit, Verfügbarkeit und rechtmäßige Nutzung von Computersystemen und unterscheidet dabei die Tatbestände des illegalen Zugriffs auf Computerdaten, des illegalen Abhörens von Daten und der (Zer-) Störung von Daten und Computern. Titel II widmet sich Angriffen auf Computerdaten und umschreibt Tatbestände der Umgehung von Sicherheitseinrichtungen (v.a. Vortäuschen falscher Zugangsberechtigungen wie beim Hacken) und des Internetbetrugs (Bereicherungsdelikte durch Nutzung von Computerdaten). Inhalt des Titel III ist die Kinderpornographie, Titel IV regelt Urheber- und verwandte Rechte.[78]

Bei einer näheren Betrachtung wird ersichtlich, dass die CCC neben der Bekämpfung der Kinderpornographie hauptsächlich den Schutz von Wirtschaftsgütern verfolgt und somit – obgleich einzelne Tatbestände auch dem Geheimnisschutz und dem Schutz der Privatsphäre zuzuordnen sind, sofern jene Bedeutung für den Schutz des Eigentums erlangen – die Indiskretionsdelikte ieS[79] keinen Eingang in die Konvention gefunden haben und Indiskretionshandlungen, die keinen wirtschaftlichen Schaden herbeiführen, nicht Gegenstand einer Harmonisierung des Strafrechtes auf diesem Gebiet geworden sind.

[76] BGBl I 2002/134.
[77] Online: http://www.coe.int; ETS N° 185; im folgenden „CCC".
[78] Vgl dazu die Präsentation *Andreaus´*, Convention on Cybercrime, vom 23. 11. 2001, online: www.e-zentrum.at/rechtsdoku/pdf/Cybercrime.ppt.
[79] Vgl dazu oben unter Punkt 2.2.

4.1.3.1 Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)

Die Tathandlung des § 118a StGB besteht darin, dass sich der Täter zu einem Computersystem, über das er nicht oder nicht alleine verfügen darf, oder zu einem Teil eines solchen, Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt. Hinzukommen muss ein dreifacher Vorsatz in Form der *Absicht* des Täters,
1) sich oder einem anderen Unbefugten von den dort gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und
2) dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht,
3) sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen.[80]

Ruft der Überwachende nun unter Verwendung eines Passwortes, das er durch den Einsatz des Überwachungsprogramms ohne Wissen des Überwachten erlangt hat (Fallgruppe II)[81], E-Mails, die am Posteingangsserver des E-Mail-Dienstanbieters des Überwachten gespeichert sind, ab, verschafft er sich dadurch Zugang zu einem Teil eines Computersystems, über das er nicht allein verfügen darf, indem er spezifische Sicherheitsvorkehrungen im Computersystem verletzt. § 74 Z 8 StGB definiert das Computersystem als *„sowohl einzelne wie auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen“*. Als „Vorrichtung“ idS sind die körperlichen Bestandteile wie Processor, Drucker, Bildschirm usw zu verstehen,[82] ein Mailserver ist von dieser Definition zweifellos erfasst. Die dort als Dateien abgespeicherten einzelnen E-Mails sind Teil des Systems und als einzelne Bestandteile des Computersystems iSd § 118a StGB zu qualifizieren.[83] Der Zugriff auf den Mailserver ist abhängig von der Übermittlung eines Passwortes, also liegt eine spezifische Sicherheitsvorkehrung vor, die der Täter durch ausspionieren des Passworts zunichte gemacht und dadurch iS des § 118a StGB verletzt hat.[84]

Eine eingehende Untersuchung, wann durch den Einsatz von „IamBigBrother“ in allen drei Fallgruppen der objektive Tatbestand hergestellt ist, wäre aufgrund der – je nach Beschaffenheit des Computersystems, der eingesetzten Sicherheitsvorkehrungen und der Art, wie der Täter zu den Ergebnissen seines

[80] *Reindl*, E-Commerce und Strafrecht (2003) 148.
[81] Vgl oben unter Punkt 3.3.2.
[82] *Reindl* 149.
[83] *Reindl* 150.
[84] *Reindl* 155 ff.

Überwachungsvorganges gelangt – zahlreichen zu bildenden Fallgruppen zwar sehr reizvoll, jedoch extrem langwierig und würde daher den Rahmen dieser Arbeit sprengen, weshalb hier – wiewohl dem Verfasser durchaus bewusst ist, dass dieses Vorgehen bei einer strafrechtlichen Subsumtion unüblich ist – mit der Untersuchung des Vorsatzes fortgefahren wird.

Die Absicht des Täters, sich von den gespeicherten Daten Kenntnis zu verschaffen, liegt zweifellos vor. Aus der Eingrenzung des Gegenstandes dieser Untersuchung folgt, dass er nicht die Absicht hat, sie einem anderen zugänglich zu machen oder sie zu veröffentlichen. Zweifelhaft erscheint, ob der Täter die Absicht verfolgt, die Daten iS des § 118a StGB zu „benützen". Eine systematische Interpretation, insbesondere ein Vergleich mit den Bestimmungen der §§ 119, 119a und 120 Abs 2a StGB, die ebenfalls durch das StRÄG 2002 eingefügt bzw abgeändert wurden, legt den Schluss nahe, dass das bloße Lesen der E-Mail einem „sich Kenntnis von Daten verschaffen" entspricht, da man sich von schriftlichen Nachrichten bzw Daten nur Kenntnis verschaffen kann, indem man sie liest. Die Absicht, sich Kenntnis von den Daten zu verschaffen, ist im Tatbestand jedoch bereits an früherer Stelle enthalten. Auch durch Wortinterpretation muss man mE zu dem Ergebnis gelangen, dass „benützen" in diesem Fall eine gewisse Verwertungshandlung bezeichnet, die über ein bloßes „Lesen" hinausgeht. Weiters fordert § 118a StGB die Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einen Nachteil zuzufügen. Um einen Vermögensvorteil geht es dem Täter hier nicht, das bloße Lesen der Daten, also die bloße Geheimnisverletzung, ist noch kein Nachteil iS des Tatbestandes. *„Wäre dem so, dann ginge allerdings die selbständige Bedeutung dieser Komponente des erweiterten Vorsatzes verloren."*[85]

Daraus folgt, dass der Überwachende, der mit bloßem Indiskretionsvorsatz handelt, nach dieser Bestimmung straffrei bleibt.

4.1.3.2 Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)

Das Fernmeldegeheimnis ist seit 1. 1. 1975 durch Art 10a des Staatsgrundgesetzes vom 21. Dezember 1867, RGBl Nr 142 idF BGBl 1974/8, und Art 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten[86] (Recht auf Achtung des Privat- und Familienlebens) auf verfassungsrechtlicher Ebene geschützt.

[85] *Reindl* 159, mwN.
[86] BGBl Nr 210/1958 zuletzt geändert durch BGBl III Nr 30/1998.

Nach § 119 StGB macht sich strafbar, wer eine Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, um sich oder einem anderen Unbefugten Kenntnis vom Inhalt einer nicht für ihn bestimmten und im Wege einer dieser Anlagen übermittelten Nachricht zu verschaffen. Der Tatbestand wurde durch das StRÄG 2002 an die – damals – aktuelle Terminologie des Telekommunikationsgesetzes 1997[87] angepasst und nimmt nun ausdrücklich Bezug auf die Definition der Telekommunikation in § 3 Z 13 des TKG 1997, die unter Telekommunikation *„den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen"* versteht. Der Informationsaustausch via E-Mail ist von dieser Definition eindeutig erfasst, der Begriff der „Nachricht" ist – entsprechend dem Begriff der „Mitteilung" der alten Rechtslage – als Vermittlung eines Gedankeninhalts zu verstehen.[88] Im Verhältnis zur alten Rechtslage wurde im wesentlichen die Überschrift von „Verletzung des Fernmeldegeheimnisses" auf „Verletzung des Telekommunikationsgeheimnisses" geändert, die „Mitteilung" wurde ersetzt durch die „Nachricht", die Übermittlung durch eine „Fernmeldeanlage" wurde ersetzt durch die Übermittlung „im Wege einer Telekommunikation oder eines Computersystems", es wird nicht mehr auf die Anbringung technischer Einrichtungen, sondern auf die Überwachung als solche abgestellt. Die „Vorrichtung" muss nicht notwendigerweise eine körperliche sein, sodass auch die Installation von für den Überwachungszweck entwickelten Programmen unter diese Bestimmung fällt.[89] Diese Qualifikation der „Vorrichtung" erhellt insbesondere aus der Tatsache, dass § 126c StGB ein Computerprogramm als taugliches Mittel zur Begehung des Delikts nach § 119 StGB anführt.

Geschütztes Rechtsgut ist hier die Vertraulichkeit des Übertragungswegs, die Kommunikationspartner sollen keine Angst haben, *„dass andere von ihren Gedanken während der Übertragungsphase erfahren, während derer sich die beteiligten Personen nicht vor Zugriffen schützen können."* [90] *„Aus dem Schutzzweck der Norm ergibt sich, dass nur Eingriffe in die Telekommunikation oder in die Übertragung im Wege des Computersystems selbst – also während der*

[87] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, das Telegraphenwegegesetz, das Fernmeldegebührengesetz und das Kabel- und Satelliten-Rundfunkgesetz geändert werden sowie ergänzende Bestimmungen zum Rundfunkgesetz und zur Rundfunkverordnung getroffen werden, BGBl I Nr 100/1997 zuletzt geändert durch BGBl I Nr 134/2002; im folgenden TKG 1997.
[88] *Leukauf/*Steininger, StGB[3] § 119 Rz 3; *Reindl* 162; ErlBem RV 1166 BlgNR XXI. GP.
[89] *Reindl* 163; *Lichtenstrasser*, e-Mail 142.
[90] *Reindl* 182.

Übertragungsvorgänge – sanktioniert werden." [91] *Schmölzer* [92] spricht in diesem Zusammenhang von *„Informationen, die sich auf einem „EDV-Transport" befinden"* und von *„im Übertragungsstadium befindlichen Daten"*. Nach Ansicht des Gesetzgebers sieht Art 3 der CCC, der durch die gegenständliche Norm umgesetzt werden sollte, *„die Kriminalisierung widerrechtlicher Überwachung nicht öffentlicher Übertragungen von Computerdaten zu und von Computersystemen oder innerhalb eines solchen Systems vor."* [93] Auch *Mosing* [94] interpretiert den Tatbestand dahingehend, dass *„nur jene e-Mail, die im Internet (ab dem Modem) unterwegs ist – nach § 119 StGB – geschützt"* wäre und der Eingriff daher bei § 119 StGB während der Übertragungsphase stattfinden müsse.

Nach *Lewisch* [95] ist auch das Anbringen einer Vorrichtung zur Kenntniserlangung von E-Mails strafbar. In seiner Kommentierung des § 119 StGB in dessen Fassung vor dem StRÄG 2002, der damals ausschließlich Eingriffe in Mitteilungen, die durch eine *Fernmeldeanlage* übermittelt wurden, pönalisierte, wollte er keine Einschränkung des Tatbestandes auf Vorrichtungen, die eine Kenntnisverschaffung in Echtzeit, also *zum Zeitpunkt der Kommunikation selbst* erlauben, vornehmen. Das Gesetz ziele auf eine umfassende Absicherung gegenüber solchen Vorrichtungen ab, *„die es dem Täter ermöglichen, nicht für ihn bestimmte – über die Fernmeldeeinrichtung übertragene – Mitteilungen zu erfahren"*, weshalb auch die Verwendung von Aufnahmevorrichtungen als tatbildlich zu deuten sei. Ein an der Telekommunikationsanlage angebrachtes *Aufnahme*gerät ermöglicht zwar kein Abhören *zum Zeitpunkt der Kommunikation selbst*, nimmt aber zu diesem Zeitpunkt – also während der Übertragungsphase – die Aufzeichnung des Nachrichteninhalts zum Zwecke einer späteren Auswertung vor. Die Funktionsweise des von *Lewisch* als taugliches Instrument zur Begehung des Deliktes beschriebenen Aufnahmegeräts unterscheidet sich von der Aufzeichnung von E-Mails mittels der Funktionen „E-Mail Capturing", „Conversation-Logging", „Key-Logging" oder der Anfertigung eines „Screenshots" dadurch, dass in letzteren Fällen der Kommunikationsinhalt entweder *vor* oder *nach* der Übertragungsphase festgehalten wird. Es erscheint daher zweifelhaft, ob das Programm „IamBigBrother" noch als verpönte „Aufnahmevorrichtung" im Sinne *Lewischs* zu qualifizieren wäre.

---

[91] *Reindl* 162.
[92] *Schmölzer*, Informatikrecht[2] 354.
[93] ErlBem RV 1166 BlgNR XXI. GP.
[94] *Mosing*, Die e-Mail-Nutzung im Lichte der anwaltlichen Verschwiegenheitspflicht, AnwBl 2001, 440.
[95] *Lewisch*, WK[2] § 119 Rz 4 ff.

Jedenfalls stellt der Wortlaut des § 119 StGB auf eine *übermittelte* Nachricht ab, sodass die Aufzeichnung einer Nachricht *vor* dem Übermittlungsvorgang schon nach dem Wortlaut der Bestimmung nicht erfasst ist.

Der Täter, der nach Fallgruppe I[96] vorgeht, macht sich daher nach der hier vertretenen Ansicht, dass im Falle des § 119 StGB der Eingriff während der Übermittlungsphase erfolgen muss, nicht strafbar, da „IamBigBrother" bei der Aufzeichnung von E-Mails und anderen Nachrichten nicht am Übertragungsweg ansetzt, sondern die Nachrichten unmittelbar vor oder nach dem Übertragungsvorgang durch Festhalten der Bildschirmausgabe protokolliert.[97]

In Fallgruppe II[98] greift der Täter mit Hilfe eines ausspionierten Passworts auf eine Nachricht zu, die noch nicht an den Empfänger übermittelt, sondern zwischengespeichert auf dem Posteingangsserver für jenen zum Abruf bereitsteht und verwendet dabei keine weitere Vorrichtung. Obwohl der Überwachende vom Zeitpunkt der Installation der Überwachungssoftware bis zum Abruf der E-Mails iS eines einheitlichen Tatplans vorgeht und die einzelnen Zwischenschritte uU als Gesamtheit zu betrachten sind, muss dennoch die Benützung der Vorrichtung zum Tatzeitpunkt – hier dem Zugriff auf den Kommunikationsinhalt – erfolgen, sodass der Täter auch in dieser Fallkonstellation straffrei bleibt. Die bloße Installation des Programms mit dem Ziel, ein Passwort auszuspionieren, ist hinsichtlich § 119 StGB ebenfalls straffrei, da das Passwort keine Nachricht ist – im Gegensatz zu § 119a StGB schützt § 119 StGB nicht sämtliche übermittelte Daten – und vor der Übertragung aufgezeichnet wird.

Für die Fallgruppe III[99] gilt das oben zu Fallgruppe I gesagte, da auch diesfalls nur Inhalte aufgezeichnet werden, die sich nicht am Übertragungsweg befinden.

4.1.3.3 Missbräuchliches Abfangen von Daten (§ 119a StGB)

§ 119a StGB ähnelt in seinem ersten Deliktsfall im Tatbild stark dem § 119 StGB, die Unterschiede liegen darin, dass das Angriffsobjekt in § 119a StGB im Wege eines Computersystems übermittelte Daten sind. Auf der subjektiven Tatseite muss der Vorsatz in Form der *Absicht* des Täters hinzukommen, die Daten selbst zu benützen, sie einem anderen, für den sie nicht bestimmt sind,

[96] Vgl oben unter Punkt 3.3.1.
[97] Vgl oben unter Punkt 3.1.1.1.
[98] Vgl oben unter Punkt 3.3.2.
[99] Vgl oben unter Punkt 3.3.3.

zugänglich zu machen oder zu veröffentlichen und sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Nach dem zweiten Deliktsfall macht sich strafbar, wer in der selben Absicht die elektromagnetische Abstrahlung eines Computersystems auffängt. § 119a StGB ist als Auffangtatbestand zu § 119 StGB konzipiert.[100]

Zur Anwendbarkeit des ersten Deliktsfalls dieser Bestimmung ist, was die äußere Tatseite betrifft, zunächst auf das zu § 119 StGB gesagte zu verweisen, wiederum sind Daten geschützt, die sich am Übertragungsweg befinden. Doch selbst bei einer Anwendung des Tatbestandes auf Daten außerhalb eines Übermittlungsprozesses scheitert die Subsumtion am geforderten Vorsatz. Die Auslegung der Worte „Nachteil" bzw „benützt" entspricht der zu § 118a StGB vorgenommenen, sodass der Täter nach dem ersten Deliktsfall dieser Bestimmung straflos bleibt.

Auch der zweite Deliktsfall ist schon für die äußere Tatseite nicht einschlägig, da „IamBigBrother" keine elektromagnetische Abstrahlung auffängt. In diesem Deliktsfall kann die „Vorrichtung" gar kein Programm sein, da Programme keine Strahlung auffangen können.

4.1.3.4 Mißbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 Abs 2a StGB)

Das StRÄG 2002 ersetzte die bis dahin geltende Strafbestimmung des § 102 TKG 1997 durch die Einfügung des Abs 2a des § 120 StGB, die Tathandlung des „Aufzeichnens" wurde übernommen und die des „Mitteilens" zum Zwecke der Anpassung an § 120 Abs 2 StGB durch „zugänglich machen oder veröffentlichen" ersetzt, wodurch nach Ansicht des Gesetzgebers der gesamte Regelungsinhalt des § 102 TKG 1997 überstellt wurde.[101]

Nach § 120 Abs 2a StGB macht sich strafbar, wer eine im Wege einer Telekommunikation übermittelte und nicht für ihn bestimmte Nachricht in der Absicht, sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen, aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht. Wiederum wird auf § 3 Z 13 TKG 1997 verwiesen, sodass E-Mails jedenfalls von dieser Bestimmung erfasst sind.

[100] ErlBem RV 1166 BlgNR XXI. GP.
[101] ErlBem RV 1166 BlgNR XXI. GP.

Wie schon zu § 119 StGB wird hier die Ansicht vertreten, dass – da wiederum auf eine *übermittelte* Nachricht abgestellt wird – schon aufgrund einer grammatikalischen Interpretation die Aufzeichnung von Nachrichten *vor* dem Übertragungsvorgang nicht vom gegenständlichen Tatbestand erfasst ist. *Lichtenstrasser* und *Mosing* [102] wollen diese Bestimmung nur dann zur Anwendung kommen lassen, *„wenn keine – angebrachte oder sonst empfangsbereit gemachte – Vorrichtung benutzt wird, sondern es sich um rein im Wege der Telekommunikation übermittelte Nachrichten, also – auch zufällig erhaltene – Gedankeninhalte, handelt."* Ein plausibles Indiz für diese Einschränkung ergäbe sich aus einer systematischen Betrachtung der Gesamtheit der durch des StRÄG 2002 eingeführten Delikte. Das Vorbereitungsdelikt des § 126c StGB[103] verbietet das Herstellen, Einführen, Vertreiben, Veräußern oder sonst zugänglich machen von Computerprogrammen, die nach ihrer besonderen Beschaffenheit ersichtlich zur Begehung der Straftaten nach den §§ 118a, 119, 119a, 126a oder 126b StGB geschaffen oder adaptiert worden sind, sofern die Begehung eines der genannten Delikte mit diesen Programmen geplant ist. § 120 Abs 2a StGB ist von dieser Aufzählung nicht erfasst, was den Schluss nahe legt, dass der Gesetzgeber nicht davon ausgehen wollte, dass dieses Delikt auch durch Verwendung einer „Vorrichtung" begangen werden kann. Allerdings hätte andererseits die Aufnahme des § 120 Abs 2a in den Katalog der Delikte, deren Vorbereitung durch § 126c StGB pönalisiert werden soll, die unhaltbare Konsequenz, dass das Vorbereitungsdelikt mit einer höheren Strafe bedroht wäre, als das entsprechende Delikt selbst. Auch eine systematische Betrachtung des gesamten § 120 StGB mit der Überschrift „Mißbrauch von Tonaufnahme- oder Abhör*geräten*" spricht aufgrund der Nennung technischer Hilfsmittel mE dafür, dass das „Aufzeichnen" iSd Abs 2a auch mittels einer „Vorrichtung", also auch eines Computerprogramms, erfolgen kann und eine weitere Einschränkung nicht gerechtfertigt ist.

Geht der Täter nach Fallgruppe II[104] vor, liegt eine bereits übermittelte Nachricht vor, diese ist auf der Mailbox des intendierten Empfängers zwischengespeichert und liegt für jenen zum Abruf bereit. Obwohl der Empfänger die E-Mail noch nicht erhalten hat, ist sie dennoch an dessen Posteingangsserver übermittelt worden. Fraglich erscheint hier, ob das Öffnen der E-Mail vom Begriff des „Aufzeichnens" erfasst ist. Will der Täter die E-Mail lesen, hat er zunächst nur den Vorsatz, sich Kenntnis vom Inhalt zu verschaffen. Allerdings wird die E-Mail bei Benützung eines Mailprogramms durch das Öffnen zwangs-

[102] *Lichtenstrasser/Mosing/Otto*, Wireless LAN - Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003, 14.
[103] Vgl unten unter Punkt 4.1.3.6.
[104] Vgl oben unter Punkt 3.3.2.

läufig als Datei auf die Festplatte geladen, wo sie auch gespeichert wird.[105] Bei einem Abruf von Webmail durch den Browser hingegen gelangt die E-Mail nur in den Arbeitsspeicher und wird nicht auf die Festplatte übertragen. Unter „Aufzeichnen" versteht der allgemeine Sprachgebrauch jedoch eine über das bloße „sich Kenntnis vom Inhalt verschaffen" oder „lesen" hinausgehende Handlung, deren Zweck in der Konservation des Inhaltes der Nachricht für einen neuerlichen Zugang zu einem späteren Zeitpunkt liegt. Das Passwort zum E-Mail-Account des Überwachten wurde durch das Programm zweifellos aufgezeichnet, die Tathandlung des Abrufs der Nachricht vom Mailserver ist jedoch mE nicht unter den Begriff des „Aufzeichnens" zu subsumieren, wenn der Täter nicht mit dem Vorsatz handelt, die Nachricht für weitergehende Zwecke zu konservieren. Auch die alternativen Tathandlungen „einem anderen Unbefugten zugänglich machen" oder „veröffentlichen" erschöpfen sich nicht in einer bloßen Kenntnisnahme vom Inhalt.

Der nach Fallgruppe II vorgehende Täter macht sich daher nach der hier vertretenen Ansicht nicht nach § 120 Abs 2a StGB strafbar.

Geht der Täter nach den Fallgruppen I und III[106] vor, benutzt er das Programm zweifellos als Werkzeug, um Inhalte im Sinne einer Konservierung zum Zwecke der späteren Auswertung aufzuzeichnen. Aufgrund der Einschränkung des Tatbestandes auf zum Zeitpunkt der Aufzeichnung bereits übermittelte Inhalte macht sich der Täter allerdings nach § 120 Abs 2a StGB nur dann strafbar, wenn er sich Zugang zu vom Überwachten *empfangenen* Nachrichten verschafft. Die Protokollierung von Nachrichten, die der Überwachte schreibt und in weiterer Folge verschickt, mittels „Key-Logging" bleibt nach dieser Bestimmung straflos.

4.1.3.5 Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)

Nach dieser Bestimmung macht sich strafbar, wer durch die Eingabe oder Übermittlung von Daten ein Computersystem, über das er nicht oder nicht alleine verfügen darf, schwer stört. Nach *Maleczky* [107] sind *damit „Computerviren erfasst, die Netzwerke lahm legen, nicht aber solche, die nur geringfügige oder bloß kurze Störungen verursachen."* Die GMat führen zum Begriff der schweren Störung aus: *„Schwer störend wird ein Angriff insbesondere dann sein, wenn er*

[105] *Reindl* 166 f.
[106] Vgl oben unter den Punkt 3.3.1 und 3.3.3.
[107] *Maleczky*, Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115.

ein Computersystem völlig lahm legt oder etwa so verlangsamt, dass der verbleibende Gebrauchswert für den Betroffenen nicht wesentlich höher liegt als bei einem regelrechten Stillstand.“ [108]

Die Installation eines Programms ist zweifellos als Eingabe von Daten zu qualifizieren. Nun führt zwar die Tatsache, dass ein bei jeder Aktivität des Überwachten zusätzlich laufendes Programm Systemressourcen verbraucht und die Processorleistung, die den übrigen ausgeführten Programmen zur Verfügung steht, vermindert, die Schwelle einer „schweren Störung“ iS der oben genannten Funktionalitätsbeeinträchtigungen ist dadurch aber jedenfalls noch nicht erreicht, wie auch beim Test von „IamBigBrother“ festgestellt werden konnte, da keine Verschlechterung der Systemleistung bemerkbar wurde. Eine schwere Störung könnte allenfalls dann erreicht werden, wenn der Überwachende das Programm auf einem fremden PC installiert hat und die aufgezeichneten Dateien nicht löscht. So könnte bei kleinen Festplatten nach längerer Zeit insbesondere durch die Ansammlung einer großen Menge von Bilddateien der Speicherplatz der Festplatte erschöpft sein und der PC für den Überwachten nahezu unbrauchbar werden. In diesem (seltenen) Fall würde sich der Täter – vorausgesetzt, es ist auch sein Vorsatz auf eine schwere Störung gerichtet – nach § 126b StGB strafbar machen.

4.1.3.6 Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)

Das Vorbereitungsdelikt des § 126c Abs 1 StGB pönalisiert das Herstellen, Einführen, Vertreiben, Veräußern oder Sonst-zugänglich-machen eines Computerprogramms, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung zumindest eines der Delikte der §§ 118a, 119, 119a, 126a oder 126b geschaffen oder adaptiert worden ist, oder einer vergleichbaren solchen Vorrichtung oder eines Computerpassworts, eines Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, wenn jene nach dem Vorsatz des Täters zur Begehung eines der oben genannten Delikte gebraucht werden sollen. Abs 2 normiert, unter welchen Bedingungen der Täter wegen tätiger Reue nicht zu bestrafen ist.

Da nach den erläuternden Bemerkungen zum StRÄG 2002[109] der bloße Besitz der erwähnten Computerprogramme und Zugangsdaten nach der Entscheidung des Gesetzgebers nicht strafbar sein soll, wird wohl auch der direkte

[108] ErlBem RV 1166 BlgNR XXI. GP.
[109] ErlBem RV 1166 BlgNR XXI. GP.

Download des Programms das Tatbestandsmerkmal des „Einführens“ nicht erfüllen, sofern der Täter nicht in der Absicht handelt, die Software auch anderen zugänglich zu machen. Fraglich erscheint, ob das Ausspionieren eines fremden Passworts jener Tathandlung zuzuordnen ist, mE ist dies jedoch zu verneinen, da der allgemeine Sprachgebrauch mit „einführen“ das Überschreiten einer Staatsgrenze verbindet.

Zur inneren Tatseite ist angesichts der obigen Ausführungen festzuhalten, dass eine Bestrafung des Täters, der lediglich mit Indiskretionsvorsatz handelt, nicht in frage kommt, da der Vorsatz, ein Delikt nach § 120 Abs 2a StGB zu begehen, im Tatbestand nicht genannt ist und die angeführten Delikte keine Strafbarkeit des Täters begründen.

4.2 Nebenstrafrecht

4.2.1 Kommunikationsgeheimnis (§§ 93 iVm 108 TKG 2003)

Die Ziele des TKG 2003[110] sind die Umsetzung der einschlägigen Europarechtlichen Richtlinien, die Gestaltung der künftigen Regulierungspolitik Österreichs und administrative Anpassungen unter Berücksichtigung der Erfahrungen bei der Vollziehung des Telekommunikationsrechtes. Die Bestimmung des § 93 TKG 2003 entspricht im Wesentlichen der des § 88 des TKG 1997 und wurde an das neue begriffliche Umfeld angepasst. Die Überschrift wurde von „Fernmeldegeheimnis“ auf „Kommunikationsgeheimnis“ geändert und die Standortdaten[111] in den Schutzbereich einbezogen.[112] Schutzgegenstand des § 88 Abs 3 TKG 1997 war eine „im Rahmen der Nutzung eines öffentlichen Telekommunikationsdienstes erfolgte Kommunikation“, § 93 Abs 3 TKG 2003 schützt nunmehr „Nachrichten und die damit verbundenen Verkehrs- und Standortdaten“. Den Begriff der „Nachricht“ definiert § 92 Abs 3 Z 7 TKG 2003 als *„jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die*

[110] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird und das Bundesgesetz über die Verkehrs-Arbeitsinspektion und das KommAustria-Gesetz geändert werden; BGBl I Nr 70/2003.
[111] Das sind gemäß der Definition des § 92 Abs 3 Z 6 TKG 2003 *„Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben“*.
[112] ErlBem RV 128 BlgNR XXII. GP.

Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können". Die E-Mail fällt daher zweifellos unter den Begriff der „Nachricht" iSd TKG 2003.

Der Abs 2 des § 93 TKG 2003 verpflichtet zur Wahrung des Kommunikationsgeheimnisses Betreiber[113] und alle Personen, die an der Tätigkeit des Betreibers mitwirken, Abs 3 verbietet das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer, ausgenommen von diesem Verbot sind Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist. Abs 4 verbietet die Aufzeichnung, Mitteilung an Unbefugte oder Verwertung von unbeabsichtigt empfangenen Nachrichten, die nicht für den tatsächlichen Empfänger bestimmt waren.

Die Strafbestimmung des § 108 TKG 2003, die in ihrem Wortlaut und der Überschrift genau dem § 103 TKG 1997 entspricht, bedroht (Z 1) *Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken*, für den Fall mit gerichtlicher Strafe, dass jene unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung machen oder ihm Gelegenheit geben, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen oder (Z 2) eine Nachricht fälschen, unrichtig wiedergeben, verändern, unterdrücken, unrichtig vermitteln oder unbefugt dem Empfangsberechtigten vorenthalten. § 108 ist ein Auffangtatbestand, der nur zur Anwendung kommt, wenn die Tat nicht nach einer anderen Bestimmung (insb den §§ 118a, 119, 119a und 120 StGB) mit strengerer Strafe bedroht ist. Weitere gerichtliche Strafbestimmungen sieht das TKG 2003 nicht vor. Der Täter einer solchen Indiskretionshandlung, der kein Betreiber iS des § 3 Z 1 TKG 2003 ist, macht sich daher nach dem TKG nicht strafbar.

Die Abs 3 und 4 des § 93 TKG 2003 hingegen verpflichten nach ihrem Sinn und Zweck jedermann zur Einhaltung der Vertraulichkeit der Kommunikation. Allerdings sieht das TKG 2003 – wie schon das TKG 1997 nach der Aufhebung von dessen § 102 – keine weitere Sanktion für Verstöße gegen diese Bestimmungen vor,[114] sodass der Täter, der die Inhalte fremder Kommunikation auf-

[113] § 3 Z 1 TKG 2003 definiert den „Betreiber" als *„ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist"*.

[114] *Parschalk/Zuser/Otto*, Telekommunikationsrecht (2002) 131; *Lichtenstrasser*, e-Mail 148.

zeichnet, zwar eindeutig rechtswidrig handelt, aber nach dem TKG nicht bestraft werden kann.

4.2.2 Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG)

4.2.2.1 Das Grundrecht auf Datenschutz

§ 1 Abs 1 des Datenschutzgesetzes[115] proklamiert in programmatischer Weise: *„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. ...“* Das DSG 2000 wurde zur innerstaatlichen Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[116] erlassen. § 1 DSG 2000 wurde als Verfassungsbestimmung beschlossen und als Grundrecht mit unmittelbarer Drittwirkung ausgestaltet. Das Grundrecht auf Datenschutz gilt somit auch im Verhältnis der Bürger untereinander.

§ 4 Z 1 DSG 2000 definiert „personenbezogene Daten“ als „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.“ Unter „sensiblen Daten“ versteht § 4 Z 2 DSG 2000 „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben“.

Für die hier vorgenommene Untersuchung stellt sich nun die Frage, ob Kommunikationsinhalte und Passwörter „personenbezogene Daten“ iS des DSG 2000 darstellen. „Da es bei einer e-Mail meist um die Kommunikation zwischen einer Person als Absender und einer anderen Person als Empfänger geht, ist

[115] Bundesgesetz über den Schutz personenbezogener Daten, BGBl I Nr 165/1999 zuletzt geändert durch BGBl I Nr 136/2001, im folgenden DSG 2000.
[116] CELEX-Dokumentnummer: 395L0046.

diese Voraussetzung regelmäßig erfüllt."[117] Der Personenbezug ergibt sich dabei aus der Erkennbarkeit der Identität des Absenders sowie dessen Kontaktdaten, zB der E-Mail-Adresse.[118] Der OGH hatte bereits zur Rechtslage vor dem DSG 2000 die Frage zu klären, ob ein fremdes Passwort ein personenbezogenes Datum darstellt und hat festgestellt, dass der Täter durch die Benutzung eines Mailboxsystems unter Verwendung eines widerrechtlich erlangten Kennworts personenbezogene Daten iS des § 3 Z 1 des damals geltenden Datenschutzgesetzes[119] widerrechtlich verwertet hatte.[120] Der Leitsatz zu dieser Entscheidung lautet: *„Kennwörter (Passwörter) für elektronische Nachrichtensysteme sind personenbezogene Daten iSd § 3 Abs 1 DSG."* Der Täter wurde nach § 49 („Geheimnisbruch") des alten Datenschutzgesetzes, der die widerrechtliche Offenbarung oder Verwertung von Daten, die dem Täter ausschließlich kraft seiner berufsmäßigen Beschäftigung mit Aufgaben der Verarbeitung anvertraut worden oder zugänglich geworden sind, pönalisierte, verurteilt. Gemäß der damals geltenden Legaldefinition verstand man unter „personenbezogenen Daten*" „auf einem Datenträger festgehaltene Angaben über bestimmte oder mit hoher Wahrscheinlichkeit bestimmbare Betroffene"*, sodass die Qualifikation des Passworts als personenbezogenes Datum auch für die aktuelle Rechtslage gelten muss.

Da der Täter, der sich mittels „IamBigBrother" Zugang zu fremden Kommunikationsinhalten verschafft, somit grundsätzlich rechtswidrig iS des DSG 2000 handelt, ist im folgenden zu untersuchen, ob jenes Gesetz auch Sanktionen für dieses Vorgehen bereithält.

4.2.2.2 Die Strafbestimmung des § 51 DSG

Nach § 51 DSG 2000 macht sich strafbar, wer personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat. Hinzukommen muss der Vorsatz in Form der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen. Der Angriffsweg ist dabei nicht näher umschrieben.

---

[117] *Jahnel*, in: *IT-LAW.AT* [Hrsg], e-Mail – elektronische Post im Recht (2003) 90.
[118] *Lichtenstrasser*, e-Mail 149 f.
[119] Datenschutzgesetz BGBl Nr 565/1978.
[120] OLG Wien 21. 11. 1989, 23 Bs 201/89 = EDVuR 1990 H 3, 111.

Dass die Verschaffung der Daten als widerrechtlich zu qualifizieren ist, ergibt sich ua aus § 1 DSG 2000 und § 93 Abs 3 TKG 2003. Das von der Strafbestimmung vorausgesetzte schutzwürdige Geheimhaltungsinteresse des Opfers ist nach Art 8 EMRK im Zusammenhalt mit der Gesamtrechtsordnung zu beurteilen[121]. Aufgrund der vorgenommen Einschränkung der hier thematisierten Angriffswege kann die Untersuchung der Tathandlung auf das „Benützen" von Daten und die Untersuchung des Vorsatzes auf die „Absicht, einem anderen einen Nachteil zuzufügen" eingeschränkt werden.

Für das „Benützen" von Daten ist auf das zu § 118a StGB ausgeführte zu verweisen, sodass unter „benützen" mE auch im Fall des § 51 DSG 2000 eine Verwertungshandlung zu verstehen ist, die über die bloße Kenntnisverschaffung hinausgeht. Die Legaldefinition des § 4 Z 9 nennt das „Benützen" gemeinsam ua mit „Ermitteln", „Erfassen", „Speichern" und „Abfragen" als Unterfall des „Verarbeitens" von Daten. Aus dem systematischen Zusammenhang ist daher zu schließen, dass durch § 51 DSG 2000 nicht sämtliche Unterfälle des „Verarbeitens" kriminalisiert wurden und die bloße Aufzeichnung von Daten mit der Absicht, sich Kenntnis vom Inhalt zu verschaffen, und die bloße Abfrage von jener Bestimmung nicht erfasst sind.

Aus den GMat zum DSG 2000[122] wird ersichtlich, dass die neue Strafbestimmung eine Einschränkung der Strafbarkeit auf die rechtswidrige Verwendung von Daten „in besonders verwerflicher Absicht" bezweckte. Fraglich erscheint schon, ob für die Absicht, einem anderen einen Nachteil zuzufügen, ein Nachteil in Form eines Gefühlsschadens ausreicht, oder ob die Absicht, einen darüber hinausgehenden Schaden am Vermögen oder anderen konkreten Rechten zu verursachen, erforderlich ist.

Da der Täter im hier untersuchten Sachverhalt allenfalls einen Gefühlsschaden des Opfers in Kauf nimmt, jedoch nicht in der *Absicht* handelt, jenem einen Nachteil zuzufügen, bleibt er auch nach § 51 DSG 2000 straffrei.

[121] *Dohr/Pollirer/Weiss*, DSG[2] (2002) § 51 Anm 6.
[122] ErlBem RV 1613 BlgNR XX. GP.

4.3 Mögliche Rechtfertigungsgründe

4.3.1 Das elterliche Erziehungsrecht

Überwachen Erziehungsberechtigte die Kommunikation ihres Kindes, so kann diese Handlung als Ausübung des Erziehungsrechtes gerechtfertigt sein, die Grenzen der elterlichen Erziehungsgewalt ergeben sich aus dem Familienrecht, insbesondere den §§ 146 ff ABGB. Eingriffe in strafrechtlich geschützte Rechtsgüter des Kindes gelten dann als gerechtfertigt, wenn sie zur Erreichung des Erziehungszwecks erforderlich sind, ein berechtigter Erziehungsanlass gegeben ist und sie sich innerhalb der Grenzen der von der Rechtsordnung anerkannten Erziehungsmaßstäbe halten.[123] *Leukauf/Steininger* [124] definieren den „berechtigten Erziehungsanlass" als *„ein bestimmtes Fehlverhalten des Kindes, das einer Erziehungsmaßregel bedarf"* und fordern als weitere Voraussetzung der Rechtfertigung ein *„diesem Anlass adäquates, zur Erreichung des angestrebten Erziehungsziels geeignetes Einwirken auf das Kind"*.

Bei einem Eingriff in das Briefgeheimnis kommt das Erziehungsrecht als Rechtfertigungsgrund in Betracht[125], *Leukauf/Steininger* [126] bezweifeln jedoch, dass dies uneingeschränkt auch in bezug auf mündige Minderjährige gelte. Jedenfalls wird ein einschlägiger Rechtfertigungsgrund für alle Formen der Überwachung von Kommunikationshandlungen des Kindes heranziehbar sein, insbesondere auch bei Eingriffen in das Telekommunikationsgeheimnis.

Da Überwachungsmaßnahmen jedoch noch kein Einwirken auf das Kind aufgrund eines Fehlverhaltens im Sinne der zivilrechtlichen Regelung dieses Rechtfertigungsgrundes darstellen und meist nur eine mehr oder minder konkrete Verdachtslage den Ausschlag für die Überwachung geben wird, scheint es in diesem Fall sachgerechter, die Grenzen der Berechtigung zu einem Eingriff in die geschützten Rechtsgüter nach den Regeln der rechtfertigenden Pflichtenkollision zu beurteilen, zumal Eltern auch die Pflicht zur Ergreifung sachgerechter Erziehungsmaßnahmen haben und für das Kindeswohl verantwortlich sind.[127]

---

[123] *Leukauf/Steininger*, StGB^3 § 3 Rz 29, mwN.
[124] *Leukauf/Steininger*, StGB^3 § 3 Rz 32.
[125] *Zipf*, WK^1 § 118 Rz 30; *Lewisch*, WK^2 § 118 Rz 32.
[126] *Leukauf/Steininger*, StGB^3 § 118 Rz 22.
[127] *Leukauf/Steininger*, StGB^3 § 3 Rz 30; *Triffterer*, AT^2 (1994) 227.

4.3.2 Die rechtfertigende Pflichtenkollision

Im Eltern-Kind Verhältnis steht die Pflicht zur Wahrung der Vertraulichkeit der Pflicht gegenüber, das Kind vor Schaden zu bewahren. Die Erfüllung der Pflicht, die sich auf das höherwertige Rechtsgut bezieht, rechtfertigt bei der Pflichtenkollision die Verletzung der minderwichtigen Pflicht, sodass eine Güterabwägung vorzunehmen ist.[128] ME ist für die Rechtfertigung von Überwachungsmaßnahmen der Eltern jedenfalls zu fordern, dass zumindest eine Verdachtslage vorliegen muss, die das Kindeswohl bedroht erscheinen lässt, wobei jedoch kein allzu strenger Maßstab anzulegen sein wird. Eine grundlose Überwachung der Kommunikation des Kindes halte ich nicht für gerechtfertigt, hingegen erscheint mir auch die Überwachung eines mündigen Minderjährigen bei Vorliegen konkreter Verdachtsmomente, die eine Gefährdung vermuten lassen, unproblematisch.

4.3.3 Rechtfertigender und entschuldigender Notstand

Der von Lehre und Rsp entwickelte Rechtfertigungsgrund des rechtfertigenden Notstandes rechtfertigt die Rettung eines höherwertigen Rechtsguts auf Kosten eines geringerwertigen, ohne dass diese Kollision auf sich ausschließenden Rechtspflichten beruht. Dabei muss ein gegenwärtiger oder unmittelbar drohender bedeutender Nachteil für das höherwertige Rechtsgut vorliegen und die Rettungshandlung das einzige angemessene Mittel zur Abwendung dieses Nachteils darstellen.[129]

Wie beim rechtfertigenden Notstand muss beim entschuldigenden Notstand, bei dem ein gleichwertiges oder auch geringerwertiges Gut gerettet wird, eine Notstandsituation und eine Notstandhandlung vorliegen, das Verhalten des Täters bleibt zwar rechtswidrig, ist aber entschuldigt, wenn jenem ein rechtsmäßiges Verhalten nicht mehr zumutbar erscheint und auch von einem mit den rechtlich geschützten Werten verbundenen Menschen kein anderes Verhalten zu erwarten wäre.[130]

Der OGH hatte sich im Rahmen des § 120 StGB mit der heimlichen Aufzeichnung von Telefongesprächen des Ehepartners mit einem Dritten zum Zwecke

[128] *Leukauf/Steininger*, StGB[3] § 3 Rz 43 ff.
[129] *Leukauf/Steininger*, StGB[3] § 3 Rz 49 ff.
[130] *Leukauf/Steininger*, StGB[3] § 10 Rz 2 ff.

der Beweisführung in einem Scheidungsverfahren auseinanderzusetzen.[131] Nach den in diesem Verfahren entwickelten Grundsätzen ist die heimliche Aufzeichnung idR auch durch das Interesse des anderen Eheteils an der Erbringung des Nachweises ehestörender Beziehungen seines Ehepartners nicht gerechtfertigt oder auch nur entschuldigt, weil der Anspruch auf Achtung des Privat- und Familienlebens eines Menschen, seiner Wohnung und seines Briefverkehrs, höherwertig ist als der hier angestrebte Zweck.[132] Dieser Grundsatz muss freilich für alle Arten der Überwachung fremder Kommunikationsvorgänge gelten.[133]

In Ausnahmesituationen kann jedoch Rechtfertigung infolge rechtfertigenden Notstands bei der Aufzeichnung fremder Kommunikation zum Zwecke der Beweisführung in einem Straf- oder Zivilverfahren in betracht kommen, wenn das Interesse an der Beweisführung das Interesse am Schutz von privaten Äußerungen überwiegt.[134]

5 Ist ein strafrechtlicher Schutz vor Angriffen gegen private elektronische Kommunikation via Internet durch andere Private wünschenswert und geboten?

Da im Ergebnis keinesfalls *Lichtenstrasser* [135], die die Ansicht vertritt, es *„werden alle denkbaren Möglichkeiten einer Störung der Übermittlung elektronischer Post bzw eines widerrechtlichen Zugriffs auf Übermittlungsinhalte strafrechtlich sanktioniert“*, gefolgt werden kann, ist im folgenden zu untersuchen, ob eine Erweiterung des strafrechtlichen Schutzes der privaten Kommunikation via Internet wünschenswert erscheint und ob aufgrund völkerrechtlicher Verträge ein dahingehender Auftrag an den Gesetzgeber vorliegt.

Parallelen zwischen der strafrechtlich geschützten herkömmlichen Kommunikation und der Nachrichtenübertragung via Internet wurden in dieser Arbeit bereits vielfach aufgezeigt. Die Möglichkeit eines Eingriffs in die Vertraulichkeit ist den Kommunikationspartnern sowohl beim Versenden von Briefen als auch bei Telefonaten sehr wohl bewusst. Der strafrechtliche Schutz des Brief- und Telekommunikationsgeheimnisses soll einerseits die Möglichkeit schaffen, Indiskre-

[131] 12 Os 143/75 = SSt 47/75 = JBl 1976, 656 = RZ 1976/73 = ÖJZ LSK 1976/53 = EvBl 1976/186; krit hiezu *Koberger*, Grenzenloser Schutz der Privatsphäre vor Tonbandgeräten?, ÖJZ 1990, 330.
[132] *Leukauf/Steininger*, StGB[3] § 120 Rz 16.
[133] *Zipf*, WK[1] § 118 Rz 29.
[134] *Leukauf/Steininger*, StGB[3] § 120 Rz 17.
[135] Lichtenstrasser, e-Mail 150.

tionshandlungen in diesem Bereich angemessen zu bestrafen und andererseits durch die generalpräventive Wirkung das Vertrauen der Kommunikationspartner in die Exklusivität der Nachrichtenübermittlung stärken. Die von anderen Autoren zum Thema des strafrechtlichen Schutzes der E-Mail angestellten Untersuchungen und die im StRÄG 2002 zum Ausdruck kommenden Bestrebungen des Gesetzgebers, eine Pönalisierung von Eingriffen in durch ein Computersystem übermittelte Nachrichten zu erwirken, sprechen für die umfassende Schutzbedürftigkeit elektronischer Kommunikation. Durch die derzeitige Gesetzeslage kommt es überdies zu unverständlichen Wertungswidersprüchen: Beispielsweise ist die Verschaffung von Kenntnis des Inhaltes einer E-Mail sowohl dann unter Strafe gestellt, wenn der Täter diese durch ein Programm abfängt, das am Übertragungsweg ansetzt, als auch dann, wenn er die elektromagnetische Abstrahlung des Computersystems auffängt. Benutzt der Täter hingegen ein Programm wie „IamBigBrother zu diesem Zweck, bleibt er straffrei.

Zusammenfassend ist daher festzuhalten, dass im Bereich des strafrechtlichen Schutzes der über das Internet übertragenen Kommunikationsinhalte offenbar eine planwidrige Regelungslücke vorliegt, die vom Gesetzgeber geschlossen werden sollte. *Zeger* [136] forderte bereits im Jahr *1992 „eine Neuregelung für die von der technischen Entwicklung überholten Paragraphen 118 (Verletzung des Briefgeheimnisses und Unterdrückung von Briefen), 119 (Verletzung des Fernmeldegeheimnisses) und 120 StGB (Mißbrauch von Tonaufnahme- oder Abhörgeräten)“*, was im Fall des § 118 StGB entweder durch eine Ausdehnung des Schutzes auf sonstige Datenträger, zB Disketten, oder durch die Aufnahme eines Absatzes, der auch die unbefugte Beschaffung von "automationsunterstützt verarbeiteten Daten unter Umgehung einer Sicherheitsmaßnahme" unter Strafe stellt, erfolgen sollte. In beiden Fällen hätte durch eine adäquate Formulierung des novellierten Tatbestandes ein umfassender Schutz erreicht werden können. Für die §§ 119 und 120 StGB schlug er vor, die Tatbestände auf den Missbrauch beliebiger technischer Geräte zur Überwachung bzw Aufzeichnung auszuweiten. Aus heutiger Sicht wäre freilich anstatt auf „technische Geräte“ auf „Vorrichtungen“ abzustellen, sodass auch Programme von diesem Begriff erfasst sind.

[136] *Zeger*, Datenschutz im Strafrecht, DIR 1992, 34; online: http://www.ad.or.at/text/161.htm.

5.1 Grundrechte

5.1.1 Das Staatsgrundgesetz

Das Staatsgrundgesetz schützt in seinen Art 10 und 10a das Briefgeheimnis sowie das Fernmeldegeheimnis. Allerdings entfalten die im StGG verbürgten Grundrechte nach hL keine unmittelbare Drittwirkung im Verhältnis der Bürger untereinander. Zur Erlangung von Effektivität in jenem Verhältnis bedürfen die Grundrechte der näheren einfachgesetzlichen Ausgestaltung.

Nach *Nowakowski* [137] gebe es eine *„verfassungsrechtlich fundierte Strafpflicht des Staates im Interesse verfassungsrechtlich gewährleisteter Grundrechte* [...]*“*. Schon *Jellinek* [138] ging von einem doppelten Zweck der Grundrechte in dem Sinn aus, dass die grundrechtlichen Verfassungsbestimmungen sowohl Verbote an die Gesetzgebung, in den angegebenen Richtungen beschränkende, neue Bestimmungen einzuführen, als auch das Gebot enthielten, bestimmte Prinzipien einer künftigen Gesetzgebung zu Grunde zu legen. Zwar sind die klassischen Grundrechte als subjektive Abwehrrechte gegen den Staat konzipiert (man spricht hier von der „negativen“ Seite der Grundrechte), doch verlangen sie nach heute hA ebenso auch ein positives Handeln des Staates, etwa auf den Gebieten des Zivil- und Strafrechts, iS einer „Schutzfunktion“[139].

Allerdings hat der VfGH[140] ausgesprochen, dass *„Art 10 des Staatsgrundgesetzes nur Briefe im eigentlichen Sinn des Wortes schützt“*. Im Zusammenhang mit einem anderen Erkenntnis des VfGH[141], in dem jener festhält: *„Läßt der völlig eindeutige und klare Wortlaut einer Verfassungsvorschrift Zweifel über den Inhalt einer Regelung nicht aufkommen, so ist eine Untersuchung, ob nicht etwa die historische oder teleologische Auslegung einen anderen Inhalt ergeben würde, nicht zulässig“*, lässt sich jedoch aus Art 10 StGG kein Auftrag an den Gesetzgeber ableiten, auch die elektronische Kommunikation zu schützen.

Der VfGH[142] hat bereits mehrfach ausgesprochen, dass er verfassungsrechtliche Begriffe in dem Sinn interpretiert, den sie im Zeitpunkt ihres Inkrafttretens

---

[137] *Nowakowski*, Die Grund- und Menschenrechte in Relation zur strafrichterlichen Gewalt, ÖJZ 1965, 282.
[138] *Jellinek*, System der subjektiven öffentlichen Rechte (1891) 91.
[139] *Loebenstein*, Die Zukunft der Grundrechte, JBl 1986, 137; *Lehne*, Grundrechte achten und schützen? Liberales Grundrechtsverständnis 1849, JBl 1985, 129.
[140] VfSlg 938.
[141] VfSlg 4442.
[142] Vgl zB VfSlg 1327, 1351, 1994, 3472.

nach der einfachgesetzlichen Rechtsordnung hatten (sog „Versteinerungstheorie“).[143] Da die Bestimmung des Art 10a zum Schutz des Fernmeldegeheimnisses per 1. 1. 1975 in Kraft trat, ist zu untersuchen, in welchem Sinne damals der Begriff des „Fernmeldeverkehrs“ verstanden wurde. IS des alten Fernmeldegesetztes[144] bezeichnete der Begriff der „Fernmeldeanlage“ *„alle technischen Anlagen zur Übertragung, Aussendung oder zum Empfang von Zeichen, Schriften, Bildern, Schallwellen oder Nachrichten jeder Art, auf Draht- und Funkweg sowie im Wege optischer oder elektromagnetischer Übertragung“.*[145] Auch der Entwurf des StGB stellte nicht auf die Begriffe „Telegraph“ und „Telephon“, sondern auf den Begriff der „Fernmeldeanlage“ ab, der durch § 1 des Fernmeldegesetzes definiert war,[146] sodass die Übermittlung von E-Mails dem Fernmeldeverkehr unterliegt.[147]

Aus der grundrechtlichen Bestimmung des Art 10a StGG kann daher ein Auftrag an den Gesetzgeber, die elektronische Kommunikation via Internet strafrechtlich zu schützen, abgeleitet werden.

5.1.2 Die EMRK

Art 8 Abs 1 EMRK garantiert jedermann die Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs. Nach Art 1 EMRK sind die Signatarsstaaten verpflichtet, allen ihrer Jurisdiktion unterstehenden Personen die in Abschnitt I der Konvention niedergelegten Rechte und Freiheiten zuzusichern. Dadurch haben die vertragsschließenden Parteien sich wechselseitig verpflichtet, die Einhaltung der in der EMRK verankerten Grundrechte gegenüber ihren Rechtsunterworfenen zu gewährleisten. Somit kommt den in der EMRK verbürgten Grundrechten Drittwirkung zu und eine Verletzung der Konvention durch einen Vertragsstaat liegt schon dann vor, wenn jener eine solche Wirkung innerstaatlich nicht gewährleistet.[148]

In der Präambel ist als Erwägungsgrund festgehalten, dass in der Wahrung *und in der Entwicklung* der Menschenrechte ein Mittel zur Erreichung des Ziels der Herbeiführung einer größeren Einigkeit unter den Mitgliedern des Europarates gesehen wird. Dadurch kommt zum Ausdruck, dass der EMRK ein evolutives

[143] *Mayer*, Entwicklungstendenzen in der Rechtsprechung des Verfassungsgerichtshofes, ÖJZ 1980, 337.
[144] BGBl 1949/170.
[145] *Lewisch*, WK^2 § 119 Rz 3, mwN.
[146] ErlBem RV 30 BlgNR XIII. GP.
[147] *Lewisch*, aaO.
[148] *Griller*, Drittwirkung und Fiskalgeltung von Grundrechten, ZfV 1983, 1.

Element inneliegt und die verbürgten Rechte dynamisch – jeweils an Hand der gegenwärtigen gesellschaftlichen Rahmenbedingungen sowie technischen Möglichkeiten und Aussichten – zu interpretieren sind. Auch der EGMR folgt in seiner Auslegung der in der EMRK gewährten Rechte einer Linie, die schlagwortartig mit "dynamischer oder evolutiver Auslegung" umschrieben werden kann. Dabei kann eine dynamische Interpretation sogar zu einer Erweiterung des sachlichen Geltungsbereiches eines Grundrechtes führen, die über die ursprünglichen Intentionen der Vertragsparteien hinausgeht.[149]

Eine nähere Analyse des Begriffs des „Briefverkehrs“ erübrigt sich somit, da die elektronische Kommunikation via Internet jedenfalls unter den Anspruch auf Achtung des Privatlebens im Sinne der Konvention fällt. Nach *Wessely* [150] ist die Datenübermittlung via Internet dem Fernmeldeverkehr zuzuordnen, da es zur Übermittlung keines Datenträgers bedarf und diese zT im Funk-, zT im Leitungsweg erfolgt. Nach der heute gebräuchlichen – auch vom StGB und dem TKG nachvollzogenen – Terminologie werden Fernmeldeverkehr und Datenübermittlung via Internet unter dem Begriff der „Telekommunikation“ zusammengefasst. Wenngleich Art 8 Abs 1 EMRK weder den Fernmeldeverkehr noch die Telekommunikation ausdrücklich nennt, hat der EGMR erstmals im Fall Klass gegen Deutschland festgestellt, dass der Fernmeldeverkehr sowohl dem Privatleben als auch dem Briefverkehr zuzurechnen ist.[151]

Zusammenfassend ist daher festzuhalten, dass aufgrund der den Staat treffenden Gewährleistungspflichten und dem Gebot der dynamisch-evolutiven Interpretation aus der EMRK durchaus ein Auftrag an den Gesetzgeber abzuleiten ist, die elektronische Kommunikation via Internet auch im Verhältnis der Bürger untereinander umfassend gegen Angriffe zu schützen. Obgleich der Gestaltungsspielraum des Gesetzgebers hinsichtlich der Durchsetzung des Grundrechtsschutzes grundsätzlich weit ist,[152] empfiehlt sich für den hier thematisierten Bereich der Einsatz des Strafrechts, um eine adäquate generalpräventive Wirkung zu erreichen.

[149] *Berka*, Die europäische Menschenrechtskonvention und die österreichische Grundrechtstradition, ÖJZ 1979, 365.
[150] *Wessely*, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612.
[151] EGMR 6. 9. 1978, EuGRZ 1979, 278.
[152] *Griller*, Der Schutz der Grundrechte vor Verletzungen durch Private, JBl 1992, 205.

5.2 Die Datenschutzrichtlinie für elektronische Kommunikation

Die Datenschutzrichtlinie für elektronische Kommunikation[153] hält in den Erwägungsgründen zunächst fest, dass die Entwicklung der Informationsgesellschaft durch die Einführung neuer elektronischer Kommunikationsdienste gekennzeichnet ist und die erfolgreiche grenzüberschreitende Entwicklung dieser Dienste zum Teil davon abhängt, inwieweit die Nutzer darauf vertrauen, dass ihre Privatsphäre unangetastet bleibt. Das Internet eröffne den Nutzern durch die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste zwar neue Möglichkeiten, bilde aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre. Zur Beseitigung von Behinderungen des Binnenmarktes der elektronischen Kommunikation sollen die von den Mitgliedstaaten erlassenen rechtlichen, ordnungspolitischen und technischen Bestimmungen zum Schutz personenbezogener Daten, der Privatsphäre und der berechtigten Interessen juristischer Personen im Bereich der elektronischen Kommunikation harmonisiert werden.

Die Erwägungsgründe nehmen ausdrücklich Bezug auf sogenannte "Spyware", "Web-Bugs", "Hidden Identifiers" und ähnliche Instrumente, die ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückverfolgen zu können und daher eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein. Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen seien Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. Das innerstaatliche Recht sollte Rechtsbehelfe für den Fall vorsehen, dass die Rechte der Benutzer und Teilnehmer nicht respektiert werden. Gegen jede – privatem oder öffentlichem Recht unterliegende – Person, die den nach dieser Richtlinie getroffenen einzelstaatlichen Maßnahmen zuwiderhandelt, sollten Sanktionen verhängt werden.

Bemerkenswert erscheint, dass die Definition der „elektronischen Post“ in Art 2 lit h der RL[154] nicht nur E-Mails, sondern auch über „Instant-Messaging-

[153] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt Nr L 201 vom 31. 7. 2002.

[154] Die RL definiert „elektronische Post“ als *„jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird“*.

Systeme“ verschickte Nachrichten erfasst. Aufgrund des bereits in der Einleitung erörterten fließenden Übergangs zwischen synchroner und asynchroner Kommunikation, die eine Differenzierung nicht sinnvoll erscheinen lässt, werden auch über einen „Chat“ verschickte Nachrichten von dieser Definition erfasst sein, obwohl solche streng gesehen nicht erst vom User „abgerufen“ werden müssen, sondern sofort am Bildschirm dargestellt werden.

Nach Art 5 Abs 1 der RL haben die Mitgliedstaaten das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer zu untersagen und die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen. Wie unter Punkt 5.1.2 bereits angesprochen ist mE eine bloße Verbotsnorm, sofern ein Verstoß dagegen keine strafrechtliche Sanktion nach sich zieht, nicht ausreichend, um die nötige generalpräventive Wirkung zu erzielen.

Die innerstaatliche Umsetzung der Richtlinie soll, soweit der Wirkungsbereich des Bundesministers für Verkehr, Innovation und Technologie betroffen war, durch den 12. Abschnitt des TKG 2003 erfolgt sein.[155] Sofern jedoch die Bestimmungen des 12. Abschnitts das Verhältnis Privater untereinander regeln und sich nicht ausschließlich an „Anbieter“[156] oder „Betreiber“[157] richten, bestehen die unter Punkt 4.2.1 aufgezeigten Defizite: Für einen Verstoß gegen die Bestimmungen der Abs 3 u 4 des § 93 TKG 2003, die das Kommunikationsgeheimnis im Verhältnis der Bürger untereinander schützen, ist keine Sanktion vorgesehen.

Die RL ist bis zum 31. Oktober 2003 innerstaatlich umzusetzen, bis zu jenem Zeitpunkt ist kein weiterer gesetzgeberischer Akt in dieser Richtung zu erwarten. Da die elektronische Kommunikation via Internet im Verhältnis zwischen Privaten – wie in dieser Arbeit aufgezeigt – auch außerhalb des TKG 2003 keineswegs umfassend gegen Angriffe geschützt ist, muss man für diesen Bereich mE von einem Umsetzungsdefizit ausgehen.

---

[155] ErlBem RV 128 BlgNR XXII. GP.

[156] § 92 Abs 3 Z 1 TKG 2003 definiert den „Anbieter“ als *„Betreiber von öffentlichen Kommunikationsdiensten“*.

[157] § 3 Z 1 TKG 2003 definiert den „Betreiber“ als *„ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist“*.

6 Gedanken zu einem möglichen neuen Tatbestand

Bei der Formulierung eines neuen Straftatbestandes ist zunächst auf die geänderte Terminologie, die sich seit dem Inkrafttreten des StRÄG 2002 und des TKG 2003 entwickelt hat, bedacht zu nehmen. Die Neufassung des § 119 StGB (Verletzung des Telekommunikationsgeheimnisses) durch das StRÄG 2002 hat den Tatbestand an die – damals aktuelle – Terminologie des TKG 1997 angepasst und verweist zur Begriffsbestimmung auf § 3 Z 13 leg cit, der die „Telekommunikation" als *„den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels dazu dienender technischer Einrichtungen"* definiert. Dadurch ist zunächst klargestellt, dass Gegenstand des Telekommunikationsgeheimnisses prinzipiell sämtliche via Internet übermittelte Nachrichten sein können. Zwar findet sich im TKG 2003 keine ausdrückliche Definition der „Telekommunikation" mehr, lediglich der „Telekommunikationsdienst" wird definiert als *„ein Kommunikationsdienst mit Ausnahme von Rundfunk"* (§ 3 Z 21 leg cit). Es ist allerdings nicht davon auszugehen, dass das Verständnis des Begriffs der „Telekommunikation" durch das TKG 2003 irgendeine Änderung erfahren hätte.

6.1 Der Ort des neuen Tatbestandes

Wie schon unter Punkt 5.1.2 erörtert, ist die Datenübermittlung via Internet, obgleich zweifellos auch Parallelen zum Briefverkehr evident sind, der Telekommunikation zuzuordnen, sodass der neue Tatbestand systematisch am ehesten nach den §§ 119 und 119a als § 119b ins StGB einzugliedern wäre. Das TKG 2003 erscheint mir weniger als passender Ort, da dessen Ziele vornehmlich im Bereich der Wettbewerbsregulierung und der Schaffung und Administration geeigneter infrastruktureller Rahmenbedingungen mit eindeutigem Schwerpunkt auf dem Gebiet der Sprachtelefonie liegen. Da ausschließlicher Schutzgegenstand des § 120 StGB (Mißbrauch von Tonaufnahme- oder Abhörgeräten) ursprünglich das *gesprochene* Wort war, wurde die Einfügung des neuen Abs 2a durch das StRÄG 2002 als dem Konzept des § 120 Abs 1 und 2 StGB widersprechend bereits kritisiert[158], sodass auch diese Bestimmung nicht als passender Ort für eine neue Regelung zum Schutz der elektronischen Kommunikation erscheint.

[158] *Schmölzer*, Informatikrecht[2] 356.

6.2 Das Angriffsobjekt

Um einen umfassenden Schutz der Kommunikationsvorgänge zu erreichen, wird es nicht ausreichend sein, auf „im Wege einer Telekommunikation oder eines Computersystems übermittelte" Inhalte als Angriffsobjekt abzustellen. Eine ausdrückliche Klarstellung, dass es ausschließlich auf die Kenntnisnahme vom Inhalt der Nachricht ankommt und nicht darauf, in welchem Stadium der Übermittlung sich diese Nachricht befindet, scheint unumgänglich. Der Begriff der „Telekommunikation" als *„technischer Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten"* erfasst begrifflich solche Nachrichten nicht, die *vor* der Übermittlung durch „E-Mail-Capturing" oder „Key-Logging" protokolliert werden. Um die Parallele zum Schutz des Briefgeheimnisses zu wahren, in dessen Rahmen auch Briefe geschützt sind, die noch nicht der Post zur Übermittlung übergeben wurden, sind Nachrichten bereits vor dem Eintritt in die Übertragungsphase zu schützen. Als Angriffsobjekt wird daher auf den Inhalt einer „im Wege einer Telekommunikation oder eines Computersystems übermittelten oder zu übermittelnden, nicht für den Täter bestimmten, Nachricht vor, während oder nach dem Übermittlungsvorgang" abzustellen sein. Durch den Begriff der „Nachricht" ist klargestellt, dass nur ein Angriff auf in Kommunikationsabsicht verfasste gedankliche Inhalte pönalisiert wird. Die Einbeziehung der Verkehrs- und Standortdaten in den strafrechtlichen Schutz kann mE unterbleiben, da dem Täter ohnehin bekannt ist, welcher PC überwacht wird und vergleichbare Informationen auch durch das Briefgeheimnis nicht geschützt sind.

6.3 Die Tathandlung

Kriminalisierte Tathandlung sollte bereits die Installation des Überwachungsprogramms bzw die Anbringung einer anderen Vorrichtung sein. Hier kann der Begriff der „Vorrichtung" iS des § 119 StGB verwendet werden, der auch Programme erfasst. Eine Einschränkung auf Programme sollte nicht erfolgen, da auch spezielle Hardware, also ein kleines Gerät, das ganz einfach direkt am Tastatur-Stecker angeschlossen wird, Kommunikationsinhalte protokollieren kann. Dieses Gerät zeichnet alle Tastaturaktivitäten auf und kann zu einem späteren Zeitpunkt ausgelesen werden.[159] Da solche Geräte bei der Aufzeichnung nicht am Übertragungsweg ansetzen und auch nicht die elektromagnetische Abstrahlung des Computersystems auffangen, ist deren Einsatz durch die bestehenden strafrechtlichen Bestimmungen nicht erfasst. Diese Verlagerung

[159] Vgl *Wiegand/Friedel*, Der Chef surft mit 9, online: http://www.onlinerechte-fuer-beschaeftigte.de/more/software/download/der_chef_surft_mit.pdf.

der Strafbarkeit in das Vorfeld des eigentlichen Angriffs auf das geschützte Rechtsgut entspricht einerseits dem System des fünften Abschnitts des StGB und ist andererseits dadurch gerechtfertigt, dass die Installation des Programms bzw die Anbringung der Vorrichtung nach dem Tatplan ohne weitere Zwischenschritte in die Aufzeichnung der Nachrichteninhalte oder Passwörter mündet. Außerdem werden auf diese Weise problemlos alle Fallgruppen der unter Punkt 3.3 aufgezeigten Angriffswege erfasst. Freilich sollte auch die Benützung einer durch eine andere Person angebrachte Vorrichtung kriminalisiert werden.

6.4 Der Vorsatz

Der Vorsatz des Täters sollte in der Absicht liegen, sich oder einem anderen Unbefugten Kenntnis vom Inhalt der Nachricht zu verschaffen. Die Absicht, die Nachrichteninhalte bzw ausspionierten Passwörter einer weiteren Verwertungshandlung zuzuführen oder dem Opfer einen über einen eventuellen Gefühlsschaden hinausgehenden Nachteil zuzufügen, ist nicht zu fordern, ebenso wenig die Verletzung einer spezifischen Sicherheitsvorkehrung. Der Tatbestand sollte dem unter Punkt 2.2 beschriebenen Konzept der Indiskretionsdelikte ieS folgen.

6.5 Das Strafmaß

Aus der Strafdrohung des § 120 Abs 1 und 2 StGB von Freiheitsstrafe bis zu einem Jahr bzw Geldstrafe bis zu 360 Tagessätzen erhellt, dass der Gesetzgeber einen Angriff auf die Vertraulichkeit des *gesprochenen* Wortes als am schwerwiegendsten wertet, wohingegen die Strafdrohungen der §§ 120 Abs 2a und 118 StGB von Freiheitsstrafe bis zu drei Monaten bzw Geldstrafe bis zu 180 Tagessätzen für die Aufzeichnung einer im Wege einer Telekommunikation übermittelten Nachricht bzw eine Verletzung des Briefgeheimnisses deutlich geringer ausfallen. Da durch die Installation eines Überwachungsprogramms oder die Anbringung einer Vorrichtung die gesamte via Internet geführte Kommunikation des Opfers über einen längeren Zeitraum hinweg aufgezeichnet wird oder sogar Passwörter ausspioniert werden, die ein jederzeitiges Eindringen in den E-Mail-Account des Opfers ermöglichen, erscheint mir in Anlehnung an die §§ 119 und 119a StGB eine Strafdrohung von sechs Monaten bzw Geldstrafe bis zu 360 Tagessätzen gerechtfertigt.

6.6 Die Verfolgbarkeit

Einem Grundzug der Strafbestimmungen gegen die Verletzung der Privatsphäre entsprechend und in Anlehnung an weitere vergleichbare legislative Maßnahmen der jüngeren Vergangenheit – zu nennen sind hier ua die §§ 118a, 119, 119a und 120 StGB sowie § 51 DSG 2000 – wäre der neue Tatbestand als Ermächtigungsdelikt auszugestalten.[160] Verletzte werden in Fällen synchroner Kommunikation jedenfalls beide Kommunikationspartner sein, wohl aber auch – aufgrund der Unzweckmäßigkeit einer Differenzierung aufgrund der fließenden Übergänge – in Fällen asynchroner Kommunikation.

6.7 Vorbereitungsdelikt und tätige Reue

Freilich wird der neue Tatbestand auch in den Katalog der in § 126c Abs 1 Z 1 und Abs 2 StGB genannten Tatbestände aufzunehmen sein, sodass die entsprechenden Vorbereitungshandlungen pönalisiert werden und tätige Reue möglich ist.

6.8 Die Überschrift

Für die Überschrift wäre der Begriff der Telekommunikation unpassend, da jener auf den *technischen* Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten und nicht auf die Kommunikations*inhalte* abstellt. Passender erscheint der Begriff der elektronischen Kommunikation, der auch einen Bezug zur Datenschutzrichtlinie für elektronische Kommunikation herstellen würde.

6.9 Der mögliche Wortlaut des neuen Tatbestandes

Der einzufügende Tatbestand könnte daher folgendermaßen lauten:

Widerrechtlicher Zugriff auf Inhalte elektronischer Kommunikation

§ 119b. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermit-

[160] Vgl auch die ErlBem RV 1166 BlgNR XXI. GP.

telten oder zu übermittelnden, nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die geeignet ist, den Inhalt dieser Nachricht vor, während oder nach dem Übermittlungsvorgang aufzuzeichnen, an einem Computersystem anbringt oder sonst empfangsbereit macht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Ebenso ist zu bestrafen, wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer in einem Computersystem, über das er nicht oder nicht alleine verfügen darf, gespeicherten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die geeignet ist, ein Passwort, einen Zugangscode oder damit vergleichbare Daten, die den Zugriff auf dieses Computersystem oder einen Teil dieses Computersystems ermöglichen, aufzuzeichnen, an einem Computersystem anbringt oder sonst empfangsbereit macht.

(3) Ebenso ist zu bestrafen, wer eine Vorrichtung, die an einem Computersystem angebracht oder sonst empfangsbereit gemacht worden ist, in der im Abs. 1 oder im Abs. 2 bezeichneten Absicht benützt.

(4) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

LITERATURVERZEICHNIS

Berka, Die europäische Menschenrechtskonvention und die österreichische Grundrechtstradition, ÖJZ 1979, 365
Brenn [Hrsg], ECG (2002)
Burgstaller, in: *Aicher/Funk/Korinek/Krejci/Ruppe* [Hrsg], Geheimnisschutz im Wirtschaftsleben (1980) 11

Dohr/Pollirer/Weiss, DSG^2 (2002)

Gassauer-Fleissner, Geheimhaltung, Offenbarung und Veröffentlichung von Daten in Informationsnetzen, ecolex 1997, 102
Griller, Der Schutz der Grundrechte vor Verletzungen durch Private, JBl 1992, 205
Griller, Drittwirkung und Fiskalgeltung von Grundrechten, ZfV 1983, 1

Jaburek/Schmölzer, Computerkriminalität (1985)
Jahnel, Datenschutz im Internet, ecolex 2001, 84
Jahnel, in: *IT-LAW.AT* [Hrsg], e-Mail – elektronische Post im Recht (2003)
Jellinek, System der subjektiven öffentlichen Rechte (1891)

Koberger, Grenzenloser Schutz der Privatsphäre vor Tongandgeräten?, ÖJZ 1990, 330

Laga, Rechtsprobleme im Internet (1998)
Lehne, Grundrechte achten und schützen? Liberales Grundrechtsverständnis 1849, JBl 1985, 129
Leukauf/Steininger, Kommentar zum Strafgesetzbuch^3 (1992)
Lewisch, in: Wiener Kommentar zum Strafgesetzbuch^2
Lichtenstrasser, in: *IT-LAW.AT* [Hrsg], e-Mail – elektronische Post im Recht (2003)
Lichtenstrasser/Mosing/Otto, Wireless LAN - Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003, 14
Loebenstein, Die Zukunft der Grundrechte, JBl 1986, 137

Maleczky, Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 115
Mayer, Entwicklungstendenzen in der Rechtsprechung des Verfassungsgerichtshofes, ÖJZ 1980, 337
Menzel, Elektronische Signaturen, (2000)

Mosing, Die e-Mail-Nutzung im Lichte der anwaltlichen Verschwiegenheitspflicht, AnwBl 2001, 440

Nowakowski, Die Grund- und Menschenrechte in Relation zur strafrichterlichen Gewalt, ÖJZ 1965, 282

Obereder, E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, RdA 2001, 75

Parschalk/Zuser/Otto, Telekommunikationsrecht (2002)

Reindl, E-Commerce und Strafrecht (2003)

Schick/Schmölzer, Das österreichische Computer-Strafrecht – Eine Bestandsaufnahme, EDVuR 1992, 107
Schmidt, Zur Problematik des Indiskretionsdelikts, ZStW 79, 782
Schmölzer, in: *Jahnel/Schramm/Staudegger* [Hrsg], Informatikrecht[2] (2003)
Schramböck, Der Schutz von Betriebs- und Geschäftsgeheimnissen nach Beendigung des Arbeitsverhältnisses in Österreich und in den USA (am Beispiel des Bundesstaates Kalifornien) im Rechtsvergleich, ÖBl 2000, 3
Seiler, Der strafrechtliche Schutz der Geheimnissphäre

Triffterer, Österreichisches Strafrecht, Allgemeiner Teil[2] (1994)
Triffterer, in: Triffterer-Kommentar zum Strafgesetzbuch

Vernier/Ebensperger, in: *Brenn* [Hrsg], ECG (2002)
Vonkilch, Der Einsatz elektronischer Signaturen aus versicherungsschutzrechtlicher und verbraucherschutzrechtlicher Perspektive, VR 2001, 25

Wagner, Unbefugter Zugriff auf e-Mail, ecolex 2000, 273
Weiss, Computerstrafrecht, FJ 1998, 244
Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491
Wessely, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612
Wiegand/Friedel, Der Chef surft mit, online: http://www.onlinerechte-fuer-beschaeftigte.de/more/software/download/der_chef_surft_mit.pdf

Zeger, Datenschutz im Strafrecht, DIR 1992, 34
Zipf, in: Wiener Kommentar zum Strafgesetzbuch[1]