**Zur Diskussion / A discuter**

# Rechtliche Zulässigkeit von «Remote Forensic Software» in der Schweiz

**ERNST PLATZ***

*Im Zuge von Ermittlungen gegen Terrorismus und organisierte Kriminalität stossen Ermittler weltweit an ihre technischen Grenzen. Verdächtige bedienen sich nämlich seit geraumer Zeit der Vorzüge der Computertechnik, welche die staatliche Überwachung zunehmend erschweren. Insbesondere der Einsatz verschlüsselter Internet-Telefonie stellt die Ermittlungsbehörden vor Schwierigkeiten. Entsprechend wachsen Begehrlichkeiten, die Personalcomputer Verdächtiger gezielt mittels Softwarewanzen, im Fachterminus «Remote Forensic Software» genannt, auszuspähen. Aus diesem Problemkreis ergeben sich eine Reihe rechtlicher und praktischer Fragestellungen, welche im nachfolgenden Beitrag beleuchtet werden sollen.*

*Au cours de leurs investigations dirigées contre le terrorisme et le crime organisé, les enquêteurs du monde entier sont confrontés à leurs limites techniques. Les suspects utilisent depuis longtemps les avantages que leur offrent les techniques informatiques rendant la surveillance des Etats de plus en plus difficile. En particulier, les autorités d'instruction sont confrontées à des difficultés dues à l'utilisation de la téléphonie cryptée par Internet. Par conséquent, les demandes d'infiltrer les micro-ordinateurs de personnes suspectes au moyen de puces informatiques, en langage technique «Remote Forensic Software», sont de plus en plus fréquentes. Ces circonstances entraînent une série de questions juridiques et d'ordre pratique qui sont mises en lumière dans le présent article.*



## I. Einleitung

### 1. Problemstellung

In der Schweiz stehen den Ermittlungsbehörden bislang verschiedene Werkzeuge zur Verfügung, um kriminelle Machenschaften im Bereich der Informatik und Telekommunikation aufzudecken. In der Vergangenheit wurden Verdächtige im Internet häufig anhand einer IP-Adresse identifiziert und mittels ihres Internetanbieters namhaft gemacht. Darauf folgte in aller Regel eine Hausdurchsuchung, im Rahmen derer die vorgefundenen Festplatten beschlagnahmt und einer forensischen Untersuchung zugeführt wurden. Eine weitere Option ist die Überwachung von Telefonanschlüssen, welche das unbemerkte Abhören von Gesprächen und des Datenverkehrs ermöglicht. Rechtsgrundlage hierfür bildet das Bundesgesetz betreffend der Überwachung des Post- und Fernmeldeverkehrs (BÜPF).

Die moderne Technik hält jedoch Möglichkeiten bereit, derlei Massnahmen zu umgehen. So erweist sich das Abhören von IP-Telefonaten als äusserst schwierig. Die Gespräche werden zunächst verschlüsselt, in mehrere Datenpakte aufgeteilt und über (zumeist im Ausland befindliche) Server dem

Empfänger übermittelt[1]. Auf die gleiche Weise lassen sich auch sensible Daten auf der Computerfestplatte verschlüsseln, sodass diese für Unberechtigte unleserlich erscheinen.

Handelsübliche kryptographische Verschlüsselungsverfahren bieten mittlerweile einen derart wirksamen Schutz vor Angriffen, dass eine Dechiffrierung mittels Kryptoanalyse oftmals mit vertretbarem Aufwand unmöglich erscheint[2]. Ein möglicher Ausweg wäre es demnach, wenn sich die Ermittler direkten Zugang in die Einflusssphäre des Nutzers verschaffen könnten, in welchem die zu untersuchenden Daten noch im Klartext vorliegen. Dieser verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze wird landläufig als Online-Durchsuchung[3] bezeichnet. Hierunter wird sowohl die einmalige Online-Durchsicht, als auch die längerfristige Online Überwachung verstanden. Diese Möglichkeiten soll nun die «Remote Forensic Software[4]» bieten. Sie kombiniert Elemente einer klassischen Hausdurchsuchung mit jenen einer verdeckten Überwachung[5]. Dies bringt für die Ermittler einerseits Vorteile mit sich, gleichzeitig tun sich jedoch auch Probleme rechtlicher und faktischer Natur auf. Während das Thema der Online-Durchsuchung in anderen Ländern für hitzige Debatten sorgt, blieb der Problemkreis in der Schweiz bis anhin von der breiten Öffentlichkeit mehrheitlich unbeachtet.

## 2. Aktuelle Situation in der Schweiz

Über die aktuelle Situation in der Schweiz zu dem Thema ist bislang wenig bekannt. Zeitungsberichten[6] zufolge soll der dem UVEK unterstehende Dienst für besondere Aufgaben (DBA) in der Vergangenheit bereits den Einsatz von Software zur Abhörung verschlüsselter VoIP-Telefonie getestet haben. Die von der Schwyzer Firma «ERA IT Solutions» hergestellte Abhörsoftware soll in der Lage sein, Antivirensoftware und Firewalls zu überwinden und die abgehörten Daten in unverdächtigen Paketen an die Ermittlungsbehörden zu versenden. Darüber hinaus wäre die Software fähig, an den Zielcomputer angeschlossene Mikrofone zu aktivieren, um Raumgespräche gezielt zu belauschen. Nach Beendigung der Abhörung liesse sich die Software unbemerkt aus der Ferne wieder deinstallieren, ohne dass der Ausgespähte hiervon Notiz nimmt. Der Leiter des Dienstes für besondere Aufgaben (DBA) räumt auf Anfrage zwar ein, dass das gegenwärtige Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) bislang keine klare Rechtsgrundlage für den Einsatz von «Remote Forensic Software» bietet, jedoch die kantonalen und die eidgenössische Strafprozessordnung deren Einsatz unter dem Titel technischer Überwachungsgeräte[7] zulassen würden[8].

Im Kanton St. Gallen wurde jedoch der Einsatz von «Remote Forensic Software» durch die Strafverfolgungsbehörden vom zuständigen Bewilligungsrichter mit der Begründung abschlägig beurteilt, der Vollzug einer Überwachung des Fernmeldeverkehrs obliege ausschliesslich dem beim UVEK angesiedelten Dienst zur Überwachung des Post- und Fernmeldeverkehrs. Im konkreten Falle handelt es sich um Ermittlungen gegen eine des Drogenhandels verdächtige Person, deren Überwachung zweier E-Mail-Adressen nicht den gewünschten Erfolg brachte. Entsprechend forderten die Strafverfolgungsbehörden die Genehmigung einer speziellen Software zwecks aktiver Überwachung des Zielrechners, da der zuständige Dienst nicht in der Lage wäre, die Überwachungsmassnahme selbst zu vollziehen.

---

[1] Der Internetprovider kann folglich keine Verbindungsdaten zu den Gesprächen aufzeichnen. Ferner ist die Verbindung über ungeschützte WLAN-Accesspoints möglich, sodass auch keine IP-Adresse zu den Verdächtigen führt.

[2] In verschiedenen Ländern unterliegen kryptografische Verfahren Nutzungs- und Exportbeschränkungen. So existierte in Frankreich von 1990 bis 1996 eine Bestimmung, welche die Deponierung der Schlüssel bei einer vertrauenswürdigen Behörde verlangte. In Grossbritannien ist am 1. Oktober 2007 eine Erweiterung des «Regulation of Investigatory Powers Act» (RIPA) in Kraft getreten, welcher sich explizit dem Umgang mit verschlüsselten Daten widmet. Abschnitt 49 des Gesetzes statuiert diesbezüglich die Herausgabepflicht der Schlüssel oder des Klartextes zu Lasten des Verdächtigen, welche bei Verweigerung mit einer Gefängnisstrafe von bis zu fünf Jahren belegt ist. Diese Bestimmung widerspricht jedoch dem allseits anerkannten Zeugnisverweigerungsrecht diametral. Die Schweiz kennt keine vergleichbaren Bestimmungen.

[3] Der Begriff erscheint in diesem Zusammenhang etwas irreführend, da sich eine Online-Durchsuchung nicht nach den Formvorschriften der herkömmlichen Hausdurchsuchung richtet. Wichtigstes Merkmal ist, dass erstere ohne das Wissen des Betroffenen durchgeführt wird, da ansonsten die Vereitelung des Untersuchungszweckes droht.

[4] Solcherlei Software wird seit Jahren bereits illegal von Hackern eingesetzte und als «Trojanisches Pferd» bzw. «Trojaner» bezeichnet. Hierunter werden Computerprogramme verstanden, welche versteckte, vom Anwender nicht gewünschte Aufgaben erfüllen (z.B. Ausspähen von Kontodaten).

[5] Als Ziel der Software können nebst Computern auch mobile Endgeräte wie Personal Digital Assistants (PDAs) oder Smartphones in Betracht kommen.

[6] «SonntagsZeitung» vom 8. Oktober 2006.

[7] Hier stellt sich die Frage, ob eine Computersoftware als Gerät im Sinne des Gesetzes anzusehen sei. Die Umschreibung als Vorrichtung wäre in diesem Zusammenhang wohl treffender.

[8] N. BERANEK ZANON, Schweizer Behörden testen Spionage-Software, SWITCHJournal, 2006, 25.

Hiermit sollte einerseits der gesamte E-Mail- und Chat-Verkehr des Verdächtigen, andererseits auch der Inhalt seiner Festplatte ausgeforscht werden. In den Erwägungen wurde diesbezüglich auf den problematischen Umstand hingewiesen, dass es sich bei ersterem Vorgang um eine Überwachung von laufenden Kommunikationsvorgängen handelt, während die zweite Massnahme eine geheime Durchsuchung von Datenträgern darstellt. Weiter nahm der Bewilligungsrichter zur Frage der Zuständigkeit wie folgt Stellung:

«Mit dem Erlass des BÜPF hat der Bund die alleinige Kompetenz für die Regelung der Überwachung des Post- und Fernmeldeverkehrs beansprucht. Er hat damit aber auch – abgesehen von den kantonal geregelten Anordnungs- und Genehmigungskompetenzen – die alleinige Verantwortung für die technischen und organisatorischen Massnahmen zur Durchführung der Überwachung übernommen.

Der Staatsanwaltschaft bzw. der kantonalen Polizei ist es in diesem Sinn verwehrt, mit eigenen technischen Mitteln in das verfassungsmässige Recht auf Achtung des Fernmeldegeheimnisses (Art. 13 Abs. 1 BV) einzugreifen. Der vom Kantonalen Untersuchungsamt angeordnete Einsatz technischer Überwachungsgeräte zur Überwachung des E-Mail- und Chat-Verkehrs von X.Y. stellt in diesem Sinn nichts anderes als eine Umgehung der vom Bundesgesetzgeber getroffenen Zuständigkeitsregeln dar. Eine Genehmigung zum Einsatz technischer Überwachungsgeräte kann deshalb – soweit mit den technischen Überwachungsgeräten der Fernmeldeverkehr überwacht werden soll – nicht erteilt werden. Hingegen bleibt ausdrücklich festzuhalten, dass die Genehmigung zur Überwachung der beiden E-Mail-Adressen … bereits mit Entscheid vom 8. November 2006 erteilt worden ist[9].»

Wie aus obigen Ausführungen hervor geht, wird die Frage nach der rechtlichen Grundlage einer Online-Durchsuchung bislang uneinheitlich beurteilt. Jedoch ist es denkbar, dass die Frage in der kommenden Strafprozessordnung des Bundes abschliessend geklärt wird.

### 3. Exkurs: Rechtliche Situation von VoIP-Diensten in der Schweiz

Gemäss BAKOM stellt die blosse Bereitstellung einer VoIP-Software (z.B. Skype), sowie der reine Betrieb eines VoIP-Dienstes noch keine meldepflichtige Fernmeldedienstleistung im Sinne des FMGs dar. Werden hingegen diese VoIP-Leistungen in Verbindung mit Internetdiensten angeboten, so greifen dieselben Pflichten wie bei klassischen Anbietern öffentlicher Telefon- oder Internetdienstleistungen. Hieraus ergibt sich insbesondere die Bindung an das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), sowie an die dazugehörige Verordnung (VÜPF). Entsprechend wären die Anbieter gehalten, mit den Strafverfolgungsbehörden zusammenzuarbeiten und von ihnen angebrachte Verschlüsselungen auszuheben[10].

## II. Grundsätzliches zur «Remote Forensic Software»

### 1. Möglichkeiten und Grenzen

Die klassische Durchsuchung birgt für die Untersuchungsbehörden verschiedene Nachteile, welche bei einer Online-Durchsuchung entfallen würden. So erfährt der Betroffene bei ersterer von dem gegen ihn geführten Ermittlungsverfahren, was ermittlungstaktische Nachteile nach sich ziehen kann. So wird unter Umständen der Kontakt zu Mittätern abgebrochen, wodurch Ermittlungsansätze verloren gehen. Ferner können Daten auch extern auf Servern im Internet abgelegt sein, so dass man derer bei einer klassischen Hausdurchsuchung ohne Benutzernamen und Passwort nicht habhaft wird. Ausserdem vereitelt häufig Verschlüsselungssoftware die Ermittlungen, da ein sicheres Passwort nach gegenwärtigem Stand der Technik nicht in realistischen Zeiträumen entschlüsselt werden kann.

Eine «Remote Forensic Software» kann indes verschiedene Funktionen übernehmen. So ist sie in der Lage, die Tastatureingaben zu protokollieren, um so an die Benutzernamen und Passwörter für verschlüsselte Daten zu gelangen. Eine «Backdoor»-Funktion erlaubt es darüber hinaus, den befallenen Rechner «fernzusteuern». Dies wiederum ermöglicht das Mitschneiden von End-to-End-Kommunikationen[11], Aktivieren von Mikrofon und Kamera, sowie die gezielte Durchsuchung des Systems nach verdächtigen Dateien. Damit diese Aktivitäten unbemerkt bleiben, manipuliert eine Rootkit-Funktion

[9] Gerichtspraxis des Kantons St. Gallen, GVP 2006, 295 f.
[10] N. BERANEK ZANON, Rechtsfragen zu VoIP im Hochschulumfeld, SWITCHJournal, 2006, 26.
[11] Z.B. Textnachrichten (Instant-Messaging), Internet-Telefonie, Videokonferenzen etc.

das Betriebssystem, sodass die «Remote Forensic Software» nicht als aktives Programm erkannt wird[12].

Die Möglichkeiten, wie eine «Remote Forensic Software» auf den Rechner eines Verdächtigen gelangen kann sind indes beschränkt. Eine Methode wäre die Übermittlung im Dateianhang einer E-Mail. Jedoch genügt das blosse Empfangen der infektiösen Botschaft noch nicht; Muss doch der Anhang in der Regel manuell geöffnet werden. Dies setzt jedoch eine gewisse Arglosigkeit des Nutzers voraus[13]. Eine weitere Möglichkeit wäre in der Ausnutzung von Sicherheitslücken14[14] des Systems zu erkennen. Jedoch bedarf dies einer eingehenden Kenntnis der auf dem Zielrechner verwendeten Software. Dies, zumal Sicherheitslücken nach ihrem Bekanntwerden von den Softwareherstellern rasch geschlossen werden[15].

Die Spähsoftware wäre zudem auf eine bestehende Internet-Verbindung angewiesen, deren Bandbreite der Spiegelung grösserer Datenmengen Grenzen setzt. Ebenso droht die Enttarnung durch Virenscanner und Firewalls, welche heutzutage die meisten Nutzer auf ihren Rechnern installiert haben dürften[16]. Um dieser Problematik zu begegnen, verlagen Untersuchungsbehörden in Deutschland zwecks Anbringung der Software die Räumlichkeiten von Verdächtigen heimlich, physisch betreten zu dürfen.

### 2. Anforderungen an die Computer-Forensik

Ohne allzu sehr auf technische Einzelheiten eingehen zu wollen, ist es dennoch sinnvoll, sich die Anforderungen an die Computer-Forensik[17] in Hinblick auf deren gerichtliche Anerkennung vor Augen zu führen. Oberstes Gebot bildet hierbei die Authentizität der zu untersuchenden Datenbestände, welche Grundlage für die Revisionsfähigkeit und damit die Verlässlichkeit der Untersuchungsmethode bildet. Insbesondere gilt es sicherzustellen, dass es zu keiner Veränderung des Untersuchungsgegenstandes kommt und keine versteckten Dateien übersehen werden. Entsprechend wird ein beschlagnahmtes Computersystem bei der Untersuchung niemals aufgestartet, da dies unweigerlich Veränderungen auf dem Datenträger mit sich bringen würde. Stattdessen wird die Festplatte ausgebaut und auf einem weiteren Datenträger ein identisches Abbild erzeugt. Dieses Abbild (in der Fachsprache Image genannt) wird sodann mittels einer kryptografischen Prüfsumme («Hash») signiert, um nachträgliche Veränderungen nachweisen zu können[18]. Erst dann kann mit der eigentlichen Auswertung der beschlagnahmten Daten mittels des Abbildes begonnen werden. Folglich erscheint die gerichtliche Verwertbarkeit der durch «Remote Forensic Software» erlangten Erkenntnisse nicht über jeden Zweifel erhaben. Dies, da keine ausreichende Gewähr für die Authentizität, mithin die Unverfälschtheit der Daten, erbracht werden kann. In ein zu untersuchendes System von aussen einzudringen und dabei gar ein Fremdprogramm einzubringen widerspricht diesem wichtigsten Grundsatz der Computerforensik[19].

## III. Rechtliche Grundlagen

### 1. Betroffene Rechtsgüter

Durch den Einsatz von «Remote Forensic Software» greift der Staat gleich in mehrere besonders geschützte Interessen des Bürgers ein. Entsprechend bedarf es einer ausdrücklichen, gesetzlichen Grundlage sowie der Beachtung des Verhältnismässigkeitsgrundsatzes und des öffentlichen Interes-

[12] Das amerikanische FBI setzte bereits eine vergleichbare Software namens CIPAV erfolgreich ein, um einen Bombendroher dingfest zu machen.
[13] Denkbar wäre es, Internet-Anbieter zu verpflichten, den ganzen Datenverkehr eines Verdächtigen über einen Proxy-Server umzuleiten und bei dessen nächstem (beliebigen) Download die Spionagesoftware unbemerkt in den heruntergeladenen Inhalt einzubringen.
[14] Zu denken ist insbesondere an Lücken in Betriebssystemen, Web-Browsern oder E-Mail-Clients.
[15] J. SCHMIDT, Technische Optionen für die Online-Durchsuchung, Heise Security, 11. März 2007, www.heise.de/security/artikel/86415.
[16] U. BUERMEYER, Die «Online-Durchsuchung». Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS, 2007, 145.
[17] Die Computer- oder IT-Forensik umschreibt die Verwendung von Software zur Ermittlung krimineller Handlungen, insbesondere zur Aufdeckung von Computerkriminalität.
[18] M. HANSE/A. PFITZMANN, Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, Deutsche Richterzeitung (DRiZ) August 2007, 225.
[19] Nach herrschender Expertenmeinung stellt bereits die Infiltration eine Modifikation des Zielsystems dar, welche die Revisionsfähigkeit und damit die gerichtliche Verwertbarkeit der Erkenntnisse in Frage stellt.

ses. So wird durch die staatliche Massnahme in Analogie zum Hausfrieden der «Computerfriede» gebrochen[20]. Die «Unverletzlichkeit des eigenen Computers» ermöglicht es dem Berechtigten, seine Datenbestände im virtuellen Raum ungestört zu beherrschen und Unberechtigte fernzuhalten[21]. Da sich auf Datenträgern oft auch private Daten befinden, geht ein Eingriff hierauf gleichzeitig mit einer Persönlichkeitsverletzung im Sinne des Datenschutzgesetzes einher. Gleichsam dürfte durch das Protokollieren von Tastatureingaben oder die Belauschung durch ein im Computer integriertes Mikrofon die Verletzung des Geheim- oder Privatbereichs vorliegen. Hinzu käme im konkreten Falle die Überwachung des Internet-, insbesondere E-MailVerkehrs, welcher vom verfassungsmässigen Fernmeldegeheimnis in gleichem Masse geschützt ist wie Telefongespräche oder Briefpost[22]. Das E-Mail unterliegt insbesondere dem Schutz des Briefgeheimnisses, sofern dieses die Anforderungen an die Qualifikation einer verschlossenen Sendung erfüllt (z.B. durch Verschlüsselung)[23]. Hieraus ergibt sich, dass dem Einsatz von «Remote Forensic Software» rein faktisch sowohl der Charakter einer klassischen Hausdurchsuchung als auch der Überwachung des Post- und Fernmeldeverkehrs sowie der einer heimlichen Beobachtung zukommen. Hieraus ergibt sich ein gewisser Regelungsbedarf zwecks Schaffung der Rechtssicherheit.

### 2. Zulässigkeit de lege lata

Seit dem 1. Januar 2002 ist das neue Bundesgesetz betreffend der Überwachung des Post- und Fernmeldeverkehrs (BÜPF) in Kraft getreten. Entsprechend verweist der Wortlaut von Art. 44 FMG nur noch auf das BÜPF, welches an die Stelle der kantonalen Strafprozessordnungen (und jene des Bundes) trat und die Anordnung von Überwachungsmassnahmen gesamtschweizerisch einheitlich regelte. Im Internetbereich entfaltete das BÜPF insoweit Geltung, als es die Teilnehmeridentifikation (inkl. Verkehrs- und Rechnungsdaten) sowie die Überwachung in Echtzeit oder rückwirkend regelt[24]. Auf das BÜPF wiederum stützen sich nunmehr die kantonalen (bzw. eidgenössische) Strafprozessordnungen bei der Umsetzung von Überwachungsmassnahmen.

Obwohl der Einsatz technischer Überwachungsgeräte im BÜPF nicht explizit geregelt wurde, ist dieser in den Strafprozessordnungen des Bundes und der Kantone enthalten. Hierbei sollen die Voraussetzungen und das Verfahren des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000 sinngemäss Anwendung finden[25]. Der hierin enthaltene Verweis auf Art. 179bis ff. StGB und damit auf das Abhören und Aufnehmen fremder Gespräche legt die Vermutung nahe, dass mit den genannten technischen Überwachungsgeräten eher Mikrofone und Aufnahmegeräte gemeint sind, als «Remote Forensic Software», welche einem ungleich umfassenderen Anwendungszweck dient. Ansonsten hätte konsequenterweise Art. 143bis StGB mit angeführt werden müssen.

Art. 179octies StGB erklärt die Überwachung des Post- und Fernmeldeverkehrs sowie den Einsatz technischer Überwachungsgeräte im Sinne von Art. 179bis ff. für straflos, sofern dies im Rahmen einer vom zuständigen Richter genehmigten amtlichen Überwachung erfolgt. Die Voraussetzungen für erstere Massnahme richten sich nach dem Bundesgesetz betreffend der Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sowie der dazugehörigen Überwachungsverordnung (VÜPF). Dieses Bundesgesetz führte neu Minimalvorschriften für die Ausgestaltung der Überwachungseingriffe durch das kantonale Prozessrecht ein[26]. Diese Minimalvorschrift liegt in den drei Voraussetzungen für die Überwachung begründet. Neben der ausdrücklichen gesetzlichen Grundlage und der Genehmigung durch den zuständigen Richter ist zudem das Vorliegen materieller Voraussetzungen zu beachten. Mithin muss die Massnahme der Verfolgung oder Verhinderung eines Verbrechens oder Vergehens dienen, dessen Schwere und Eigenart den Eingriff rechtfertigt[27].

---

[20] J. REHBERG/N. SCHMID, Strafrecht III, 8. Aufl., Zürich 2003, 150.
[21] P. WEISSENBERGER, Basler Kommentar, Strafrecht II, 2. Aufl., Basel 2007, StGB 143bis N 3.
[22] BGE 122 I 190 (bei amtlichen Überwachungen handelt sich nach Meinung des Bundesgerichts um einen schweren Grundrechtseingriff).
[23] P. VON INS/P.-R. WYDER, Basler Kommentar, Strafrecht II, 2. Aufl., Basel 2007, StGB 179 N 20 ff.
[24] U. MAURER/S. GANSER, Neuerungen bei der Überwachung des Post- und Fernmeldeverkehrs – auf Kosten des Telekommunikationskonsumenten?, sic! 2002, 129.
[25] Vgl. Art. 41 Abs. 2 StPO SZ, Art. 104 Abs. 2 StPO ZH.
[26] VON INS/WYDER (Fn. 23), StGB 179octies N 5–11.
[27] VON INS/WYDER (Fn. 23), StGB 179octies N 13.

Als Sonderproblem stellt sich zudem die Frage, inwieweit in Zusammenhang mit der Überwachung ein Hausfriedensbruch oder gar eine Sachbeschädigung gerechtfertigt werden kann. Während aus systematischer Perspektive dies zu verneinen wäre, so sprechen doch praktische Interessen dafür. Unter Umständen könnte die Überwachungsmassnahme in sehr engen Grenzen als Rechtfertigungsgrund i.S. von Art. 32 StGB dienen[28]. Analog ist auch der Einsatz von «Remote Forensic Software» mit einem virtuellen oder faktischen Hausfriedensbruch verbunden und beinhaltet im ungünstigen Falle auch eine Sach- und/oder Datenbeschädigung.

### 3. Zulässigkeit de lege ferenda

Im Juni 2007 legte der Bundesrat einen leicht angepassten Vernehmlassungsentwurf[29] für die Änderung des «Bundesgesetzes vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit» vor. In diesem kurz «BWIS-II» genannten Entwurf ist neu ein Art. 18n enthalten, welcher das geheime Durchsuchen eines Datenverarbeitungssystems vorsieht. Aus den Erläuterungen zum Entwurf geht hervor, dass die relevanten delinquenten Gruppen ihre Kommunikation gegen den Zugriff Dritter besonders sichern. Das Eindringen in die geschützten Bereiche wäre zwar mit Fachwissen möglich, jedoch ohne entsprechende Befugnis verboten[30].

Die Durchsuchung könnte nun neu auch ohne Wissen des mutmasslichen Gefährders erfolgen. Der Massnahme soll entsprechend passiver Charakter zukommen, wonach es im zu untersuchenden System weder zu Funktionsstörungen noch zur Datenbeschädigung kommen soll. Als Rechtfertigung des Eingriffs bedarf es des Verdachtes, einer konkreten und schweren Gefährdung der innern oder äusseren Sicherheit der Schweiz. Zudem müssen alle anderen Mittel der Informationsbeschaffung erfolglos geblieben sein, bzw. von Beginn weg aussichtslos oder unverhältnismässig erscheinen. Hiermit soll namentlich dem Terrorismus, verbotenem politischem oder militärischem Nachrichtendienst, dem verbotenen Handel mit Waffen, radioaktiven Materialien sowie unerlaubtem Technologietransfer begegnet werden. Da es sich bei der Durchsuchung eines Datenverarbeitungssystems um eine schwerwiegende Einschränkung handelt, hat diese wiederum den Erfordernissen von Art. 36 BV zu genügen[31].

Der Einsatz technischer Überwachungsgeräte würde hingegen in Art. 18m geregelt. Hiervon sind namentlich akustische und optische Beobachtungs- und Aufzeichnungsgeräte erfasst[32], wobei analog auf Regelung und Umfang der Bestimmung von Art. 66 Abs. 2 der Bundesstrafprozessordnung (SR 312.0) verwiesen wird. Durch die Einschränkung auf die Beobachtung nach Massgabe der Art. 179bis bis 179quater StGB ist die Qualifikation von «Remote Forensic Software» als technisches Überwachungsgerät im Sinne der Norm jedoch zu verneinen.

Der Entwurf zur Schweizerischen Strafprozessordnung seinerseits sieht in Art. 66 Abs. 1 die Überwachung des Post- und Fernmeldeverkehrs vor und verweist diesbezüglich auf das BÜPF. Im darauf folgenden Abs. 2 findet ferner der Einsatz technischer Überwachungsgeräte im Sinne von Art. 179bis ff. StGB Erwähnung, auf welchen die Voraussetzungen und das Verfahren des BÜPF sinngemäss Anwendung finden. Die Möglichkeit einer heimlichen Durchsuchung von Datenverarbeitungssystemen ist im Entwurf nicht vorgesehen. Vielmehr ist nach Art. 69 bei der Durchsuchung von Papieren und damit wohl auch von digitalen Dokumenten mit grösster Schonung der Privatgeheimnisse vorzugehen. Dabei sei dem Inhaber der Papiere womöglich Gelegenheit zu geben, sich vor der Durchsuchung über deren Inhalt auszusprechen und gegen die Durchsuchung Einsprache zu erheben. Ferner wäre bei der Durchsuchung der Wohnungsinhaber beizuziehen oder, wenn dieser abwesend ist, ein Verwandter, Hausgenosse oder Nachbar. Diese Vorgaben könnten bei einer heimliche Durchsuchung von Datenverarbeitungssystemen per Definition nicht eingehalten werden.

Folglich enthält die in Ausarbeitung befindliche Schweizerische Strafprozessordnung, im Gegensatz zum revidierten Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, keine Rechtsgrundlage für die geheime Durchsuchung von Datenverarbeitungssystemen und dem Einsatz von «Remote Forensic Software» im Speziellen. Durch die neue Schweizerische Strafprozessordnung in

[28] VON INS/WYDER (Fn. 23), StGB 179octies N 50.
[29] Die ursprüngliche Fassung datierte vom Juli 2006.
[30] Vgl. Art. 143 und 143bis StGB.
[31] Vorentwurf: Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit – Erläuternder Bericht, 61.
[32] Der Entwurf verzichtet jedoch auf die ausdrückliche Nennung von «Remote Forensic Software» als Mittel hierzu.

vorliegender Fassung würde die Rechtslage indes keine Klärung erfahren. Dies, da hierin die Bestimmungen der bisherigen Strafprozessordnungen weitgehend übernommen wurden.

### IV. Fazit

Aus den vorangegangenen Überlegungen kann geschlossen werden, dass zumindest der Status quo einschlägiger Rechtssetzung keine befriedigende Antwort auf die Frage nach der Zulässigkeit von «Remote Forensic Software» zulässt. Weder das Bundesgesetz betreffend der Überwachung des Post- und Fernmeldeverkehrs (BÜPF) noch die diversen Strafprozessordnungen äussern sich explizit hierzu. Die Qualifikation der «Remote Forensic Software» als technisches Überwachungsgerät[33] wäre in verschiedener Hinsicht problematisch. Einerseits ermöglicht die Software weitaus umfassendere Eingriffe in die Privatsphäre als die blosse Überwachung der Kommunikation. Andererseits erscheint es fraglich, ob eine Computersoftware als technisches Gerät anzusehen sei. Allenfalls müsste von einer Vorrichtung die Rede sein. Dies, zumal das BÜPF den Begriff des technischen Überwachungsgerätes gar nicht kennt. Entsprechend mangelt es den gängigen Regelungen dem Erfordernis der hinreichenden Bestimmtheit, welche insbesondere für schwerwiegende Grundrechtseingriffe unabdingbar erscheint.

Auch das sich in Revision befindliche «Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit» und die künftige Schweizerische Strafprozessordnung bieten nur bedingt Gewähr für eine ausreichende gesetzliche Grundlage. Zwar sieht ersteres Gesetz die heimliche Durchsuchung eines Datenverarbeitungssystems ausdrücklich vor, während im Entwurf zur Schweizerischen Strafprozessordnung dieser Passus fehlt. Damit dürfte diese Massnahme künftig zwar dem Schweizer Staatsschutz zur Verfügung stehen, nicht jedoch den einzelnen Staatsanwaltschaften. Art. 138 Abs. 2 E-StPO legt zwar fest, dass unter Umständen auch rechtswidrig erlangte Beweise anerkannt werden können. Dies kann jedoch aus rechtsstaatlicher Sicht nur der Ausnahmefall sein.

Weiter fällt auf, dass die Bestimmung über die heimliche Durchsuchung eines Datenverarbeitungssystems die Mittel hierzu nicht näher umschreibt. Dies könnte einerseits mit der thematisierten Spezialsoftware geschehen, jedoch auch auf dem Wege, dass zur Datenbeschaffung heimlich physisch in Räumlichkeiten eingedrungen wird. Dies insbesondere unter dem Aspekt, dass sensible Datenverarbeitungsanlagen entweder gut gegen Angriffe aus dem Internet geschützt sind oder aber mit diesem gar nicht direkt vernetzt sind. Hiermit ist ein Problemkreis ausgeklammert, welcher in der Diskussion im benachbarten Ausland besonders hitzig debattiert wird.

Ferner vermag die Regelung unter dem Titel der Überwachung des Fernmeldeverkehrs wenig zu befriedigen, da der Fernmeldeverkehr, zumindest im Falle der Online-Durchsuchung, lediglich Mittel und nicht etwa Ziel des Eingriffs darstellt. Ziel wären in casu die sich im Herrschaftsbereich des Verdächtigen befindlichen Datenbestände, und das Internet lediglich das Einfallstor hierzu. Hiermit befinden wir uns faktisch auf dem Gebiet einer klassischen Hausdurchsuchung. Die Problematik hierbei liegt jedoch in der Natur der Sache begründet, wonach eine heimliche Durchsuchung dem Betroffenen nicht zur Kenntnis gebracht würde. Dieser kann seine Interessen, mithin das rechtliche Gehör, aufgrund der Heimlichkeit der Massnahme nicht wahrnehmen, so wie dies bei einer konventionellen Durchsuchung möglich wäre. Da Datenbestände als Träger menschlicher Gedankenäusserung teils private Informationen beinhalten, müssten sie bei der Sicherstellung analog zu Schriftstücken behandelt werden. Demnach wäre dem Angeschuldigten Gelegenheit zu geben, sich über den Inhalt auszusprechen und gegen die Durchsuchung Einsprache zu erheben.

In Hinblick auf die anstehenden Rechtssetzungsvorhaben wäre es demnach wünschbar, dass diese offenen Fragen eine abschliessende Beantwortung erfahren und hiermit Rechtsklarheit geschaffen würde. Insbesondere schwere Eingriffe in die Grundrechte bedürfen klarer gesetzlicher Grundlagen, untergraben diese doch ansonsten das Vertrauen des Bürgers in das staatliche Handeln. Im konkreten Falle stellt es für die Legislative eine besondere Herausforderung dar, mit der raschen technischen Entwicklung Schritt zu halten. Hierbei handelt es sich zwar um ein schwieriges, aber dennoch realisierbares Unterfangen.

[33] Art. 179sexies StGB verwendet ebenfalls die Formulierung des «technischen Gerätes», welche im Schrifttum als missglückt angesehen wird. Offenbar fand der Begriff auch Eingang in die diversen Strafprozessordnungen, jedoch nicht in das BÜPF selbst.

**Zusammenfassung**

*Moderne Technologien und veränderte Bedrohungslagen stellen die Schweizerischen Untersuchungsbehörden vor neue Herausforderungen. Insbesondere der Einsatz verschlüsselter Internet-Telefonie droht die gängige Telefonüberwachung obsolet werden zu lassen. Zwar lässt sich auch diese Art der Kommunikation mit den notwendigen Spezialkenntnissen überwachen, jedoch ist die Handhabe der Ermittler durch eine brüchige Rechtsgrundlage eingeschränkt. Insbesondere das Ausspähen von Computersystemen und der Einsatz von «Remote Forensic Software» wurde gesetzlich bislang nicht geregelt. Dies jedoch drängt sich auf, da staatliche Eingriffe in die Privatsphäre des Bürgers einer ausdrücklichen gesetzlichen Grundlage bedürfen. Ganz offensichtlich entsprechen die gängigen Bestimmungen den Erfordernissen des digitalen Zeitalters nur ungenügend. In der Tat sind Computersysteme mittlerweile als Träger sensibler privater Daten anzusehen, welche eines besonderen Schutzes bedürfen. Problematisch hierbei ist der Umstand, dass bei den genannten Untersuchungshandlungen die Grenzen zwischen klassischer Überwachung und der Hausdurchsuchung zu verwischen drohen. Hieraus ergibt sich eine Reihe ungelöster juristischer Fragestellungen. Der Gesetzgeber hat sich der Thematik bislang jedoch eher halbherzig angenommen. Während das in Revision befindliche «Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit» (BWIS-II) die heimliche Durchsuchung von Datenverarbeitungssystemen ausdrücklich erlaubt, fehlt dieser Passus hingegen im Entwurf zur Schweizerischen Strafprozessordnung (E-StPO). Entsprechend bleibt abzuwarten, ob der Gesetzgeber in absehbarer Zeit eine umfassende Regelung der Problematik vornimmt.*

**Résumé**

*Les technologies modernes et les nouvelles menaces posent de sérieux défis aux autorités d'instructions suisses. En particulier, l'utilisation de la téléphonie cryptée par Internet risque de rendre obsolète la surveillance téléphonique telle que nous la connaissons. Bien que cette forme de communication puisse être surveillée en appliquant les connaissances techniques nécessaires, leur mise en œuvre par les enquêteurs se heurte toutefois à des bases légales lacunaires. La surveillance de systèmes informatiques et l'usage de «Remote Forensic Software» n'ont notamment pas fait à ce jour l'objet d'une réglementation légale. Elle est cependant nécessaire, dans la mesure où les interventions de l'Etat dans la sphère privée du citoyen nécessitent une base légale expresse. Manifestement, les dispositions actuelles ne répondent pas suffisamment aux exigences de l'ère de la digitalisation. En effet, les systèmes informatiques doivent être désormais considérés comme des supports de données privées sensibles nécessitant une protection spéciale. Le problème réside dans le fait que les actes d'instruction précités menacent d'effacer les limites entre une surveillance classique et la perquisition. Ainsi, de nombreuses questions juridiques demeurent sans réponse. Le législateur s'en est cependant peu préoccupé. Alors que la révision actuelle de la «loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)» autorise expressément la perquisition secrète de systèmes informatiques, une telle disposition fait en revanche défaut dans l'avant-projet de loi fédérale sur l'organisation des autorités pénales de la Confédération. Reste à voir si le législateur entreprendra dans un proche avenir une réglementation globale de ce problème.*

* lic. iur., lic. oec., Schübelbach.